Detection and Localization of the Eavesdropper in MIMO Systems

LINA NING¹, BIN LI¹, (Member, IEEE), CHENGLIN ZHAO¹, YIWEN TAO¹, AND XIANG WANG²

¹School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
²Beijing Jianyi Corporation, Ltd., Beijing 100089, China

Corresponding author: Bin Li (binli@bupt.edu.cn)

This work was supported in part by the Young Talents Invitation Program of China Institute of Communications under Grant QT2017001, in part by the Natural Science Foundation of China under Grant U1805262, and in part by the 2019 Industrial Internet Innovation Development Project of Ministry of Industry and Information Technology of China Comprehensive Security Defense Platform Project for Industrial/Enterprise Networks.

ABSTRACT The pilot spoofing attack (PSA) is one kind of active eavesdropping that happens in the channel training phase, in which an intelligent eavesdropper transmits identical pilot sequences synchronously with the legitimate user to spoof the transmitter. This attack leads to the estimated channel being a mix of a legitimate channel (the channel from the transmitter to the legitimate user) and an eavesdropper channel (the channel from the transmitter to the eavesdropper). And as a result, confidential information is leaked to the eavesdropper during the data transmission phase. Especially when the eavesdropper utilizes sufficiently large power, the channel rate at the legitimate user end decreases observably and increases dramatically at the eavesdropper. To against the active PSA, we propose a new effective scheme called the spatial spectrum method (SSM) which can be applied in situations in which the eavesdropper attacks not only the transmitter but also the legitimate user in multiple-input multiple-output (MIMO) communication systems. Specifically, this method utilizes the spatial spectrums that are attained by the uplink training phase to detect the eavesdropper. Besides it also can locate the legitimate user and the eavesdropper by identifying the direction-of-arrival (DOA) of the legitimate user and the eavesdropper based on the symmetry of the uplink and downlink channels in a time-division-duplex (TDD) system and estimating the geographical distance between the legitimate user and the eavesdropper. Consequently, the secure transmission of secret information can be guaranteed by utilizing spatial information, such as by adopting beamforming technology. Numerical results show that our method can effectively detect and locate the eavesdropper.

INDEX TERMS Physical layer security, spatial spectrum method, pilot spoofing attack, multiple-input and multiple-output.

I. INTRODUCTION

Confidential information may suffer the threat of eavesdropping when it is transmitted in the wireless medium due to the openness and broadcast nature of wireless communication. Cryptography technology is a traditional method to protect secret information by encrypting the confidential message to an unreadable message. However, this method consumes more resources (such as secret key distribution and management [1], [2]) and the encrypted message may be cracked with sufficiently advanced computational capabilities. To protect secret information, researchers have begun to pay increased attention to physical layer security (PLS) [3]–[6], which utilizes the characteristics of the wireless channel to improve the legitimate channel rate with lower complexity than cryptographic technology.

PLS is a promising method for ensuring the security of the information; hence, many studies have been dedicated to investigating effective PLS technologies. The most popular of these are artificial noise (AN) [7]–[9] and beamforming technologies [10]–[13]. To confuse eavesdroppers, the transmitter can add AN to the transmission signal and reduce the channel rate of the eavesdropper. Beamforming can achieve a positive secrecy rate even if the eavesdropping channel is stronger than the legitimate channel [14]–[16]. However, most works on PLS assume that the channel state information (CSI) is...
perfectly or at least partially known, which is impossible in practice.

As the CSI is critical to realize secure transmission, a channel training phase should be implemented before the data transmission phase. During the training phase, as the reciprocity of the uplink and downlink channels in a time-division-duplex (TDD) system, the transmitter estimates the channel based on the received pilot information that is transmitted by the legitimate user. However in a wiretap channel (which consists of a transmitter, a legitimate user and an eavesdropper) [17], [18], the eavesdropper can also attain the pilot signal due to the nature of the pilot signal (as it is repeatedly use and publicly known). Therefore, during the training phase, the eavesdropper broadcasts the pilot signal simultaneously with the legitimate user, resulting in an estimated channel that consists of a combination of the legitimate channel and the eavesdropping channel. When the transmitter transmits confidential messages through the estimated channel during the data transmission phase, the information rate may decrease for legitimate user and increase for the eavesdropper. This active attack is called the pilot spoofing attack (PSA) and it may cause terrible consequences. For example, in the worst case, the eavesdropper can obtain all confidential messages by improving its own transmit power and reducing the information rate at the legitimate user end to zero.

A. RELATED WORKS AND MOTIVATION

The PSA was first studied in [19], which mainly analyzed the damage caused by a PSA. Subsequently, various studies have been done on detecting PSA. One representative method involves modifying the pilot sequences [20]–[24]. References [20] and [21] adopted two random phase-shift keying (PSK) symbols and newly designed stochastic signals as the pilot signal. References [22] and [23] proposed an effective detection method by adding a random sequence into the pilot sequences rather than redesigning pilot signals. Reference [24] adjusted the training length and the transmit power of the pilot sequences to detect PSA. However, altering the pilot sequences is not practical as pilot signals are used not just for channel estimation but also for eliminating the interference of the legitimate users by applying orthogonal pilot sequences. Ref. [25] designed a three-phase uplink training method (TPUT) to detect the eavesdropper efficiently by introducing a trusted user. An energy ratio detector (ERD) method was introduced in [26], in which the author utilized the unequal power of the transmitter and the legitimate user to detect PSA when the eavesdropper conducts PSA. In a later study, the authors studied a two-way training method (TWTD) in the multiple-input single-output (MISO) system [27], this method not only has a good detection performance but also can estimate the legitimate channel and the eavesdropping channel (if PSA happens). However, this method assumed that the adversary only conducts the uplink training attack and would be ineffective if the adversary also conducts the downlink training attack. Moreover, given the limited training length, the channel estimation accuracy and the detection reliability would be seriously degraded in the low signal-to-noise ratio (SNR) regime. Most importantly, most of the above studies focus on the MISO case, and their results may be less effective for the more popular multiple-input multiple-output (MIMO) scenarios, due to the significantly increased training overhead and less attractive reliability.

B. OUR WORK AND CONTRIBUTIONS

In this paper, we propose a new scheme to combat the PSA by using the nature of the spatial spectrum in TDD MIMO systems. In our model, we propose a two-way channel training based scheme to detect the presence of the eavesdropper (Eve) and locate the positions of the legitimate user (Bob) and Eve. We assume that Eve is highly intelligent and can also launch the downlink training attack when it detects the transmitter executing downlink training, as shown in Fig.1. The new method utilizes the spectrum peak value to detect Eve. Besides, the transmitter (Alice) can locate Bob and Eve (the direction-of-arrivals (DOAs) of Bob and Eve and the geographical distance of the Alice-Bob and Alice-Eve). Such as, it can obtain the DOAs of Bob and Eve by recognizing which peak values come from Eve with the symmetry of the uplink and downlink channels in a TDD system, which makes the latter beamforming becomes possible.

The main contributions of our work are summarized as follows:

- Our scheme provides a new spatial spectrum method (SSM) to detect and locate Eve based on a two-way channel training scheme. The new method works not only in the scenario in which Eve only launches uplink spoofing attack but also in new scenarios in which Eve launches both uplink and downlink spoofing attacks. Besides, the SSM need not redesign the pilot signals or insert the safe pilot sequence into pilot signals as in [20]–[24].
The SSM utilizes the information of the spatial to detect the TSA and it can dramatically improve the detection probability in low SNR conditions. What’s more, it can save training length compared to existing methods in MIMO scenarios; alternatively, it can obtain higher detection probabilities under the same training length than existing methods.

The greatest contribution of our work is that it can locate the position of Bob and Eve even in low SNR conditions which enables the latter beamforming from Alice to Bob becomes possible. It also can improve the secrecy capacity of the system by trapping waves in the direction of Eve.

The rest of this paper is organized as follows. Section II introduces the system model and the damages caused by PSA. Section III introduces the detection process of the malicious eavesdropper. Section IV illustrates the process for locating the eavesdropper. In section V, we introduce the simulation set-up and analyze the numerical results. Finally, the conclusions are drawn in section VI.

Notations: Bold lowercase and uppercase letters represent vectors and matrices, respectively, i.e., \( \mathbf{a} \) and \( \mathbf{A} \). \((\cdot)^T\) and \((\cdot)^\dagger\) represent the transpose and Hermitian transpose, respectively. The Euclidean norm of a vector or a matrix is denoted by \( \| \cdot \| \). The absolute value of a scalar is denoted by \( | \cdot | \). \( \mathbb{C}^{m \times n} \) represents a complex space of the dimension \( n \times m \), and \( \mathbf{I}_{n \times n} \) denotes an \( n \)-by-\( n \) identity matrix. \( \mathcal{C}_N(0, \sigma^2) \) denotes the distribution of a circularly symmetric complex Gaussian (CSCG) random variable with mean zero and variance \( \sigma^2 \). The distribution of a Gaussian random variable with zero mean and variance \( \sigma^2 \) is denoted as \( \mathcal{N}(0, \sigma^2) \). \( P_r(\cdot) \) denotes the probability measure.

II. SYSTEM MODEL AND PROBLEM STATEMENT

This analysis adopts a wiretap channel model and we adopt the polar coordinate system as shown in Fig.1, Alice is selected as the origin, Bob’s location is denoted as \( (D_{ab}, \theta_b) \), Eve’s location is denoted as \( (D_{ae}, \theta_e) \), and they respectively equipped with \( n_t, n_r, n_e \) \( (n_t = n_r \geq 2, n_e \geq 2) \) antennas. The downlink channel and the uplink channel are assumed to be reciprocal as this scheme operates in a TDD system. What’s more, we assume that the channels are block fading and that the CSI remains constant during the training length. In order to achieve data secure transmission, Alice should estimate the channel during the training phase.

Next we will briefly introduce the PSA and the damage it may cause. During the uplink training phase, each antenna of Bob broadcasts pilot signal \( x_p(n), n = 1, \ldots, N_1' \), \( \sum_{n=1}^{N_1'} |x_p(n)|^2 = N_1' \), \( N_1' \) is the pilot length of each antenna. And then Alice estimates each channel between that antenna of Bob and the antenna of its own \( \mathbf{h}_i \in \mathbb{C}^{n_r \times 1} \) \( \forall i \in \{1, 2, \ldots, n_r\} \). Hence to estimate the CSI of the legitimate channel (the channel between Alice and Bob) \( \mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{n_r}] \in \mathbb{C}^{n_r \times n_t} \), the total training length of uplink training is \( N_1 = n_rN_1' \). The illegitimate channel (the channel between Alice and Eve) is denoted by \( \mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{n_e}] \in \mathbb{C}^{n_r \times n_e} \), \( \mathbf{g}_i \in \mathbb{C}^{n_r \times 1} \). Each entry of \( \mathbf{H} \) and \( \mathbf{G} \) is assumed to be an independent and identically distributed (i.i.d) CSCG random variable. If Eve launches PSA in the uplink training process, the received signal at Alice is:

\[
y_{a,i}(n) = \left( \sqrt{P_B/n_t}h_i + \sqrt{P_E/n_e}g_i \right)x_p(n) + u(n),
\]

where \( P_B \) and \( P_E \) denote the power budgets of Bob and Eve, respectively. \( y_{a,i}(n), u(n) \in \mathbb{C}^{n_r \times 1} \). \( u(n) \) represents CSCG noise vector and each entry is i.i.d with zero mean and variance \( \sigma_u^2 \), i.e., \( u(n) \sim \mathcal{C}_N(0, \sigma_u^2) \).

The estimated CSI based on the least square (LS) method [28] is denoted by \( \hat{\mathbf{h}}_i \), when Alice isn’t aware of the PSA, the estimated CSI will be misguided and given by:

\[
\hat{\mathbf{h}}_i = \sqrt{P_B/n_t}h_i + \sqrt{P_E/n_e}g_i + \tilde{e}_i,
\]

where \( \tilde{e}_i \) is the estimation error. The estimated legitimate channel \( \hat{\mathbf{H}} = [\hat{\mathbf{h}}_1, \hat{\mathbf{h}}_2, \ldots, \hat{\mathbf{h}}_{n_r}] \) is contaminated by \( \mathbf{G} \) if PSA happens.

In the data transmission phase, Alice transmits signal \( x_d = \mathbf{W}s, \mathbf{x}_d \in \mathbb{C}^{n_r \times 1} \). \( s \) is the data symbols, the precoding matrix \( \mathbf{W} \) is:

\[
\mathbf{W} = \begin{bmatrix} \hat{\mathbf{h}}_1 & \hat{\mathbf{h}}_2 & \cdots & \hat{\mathbf{h}}_{n_r} \end{bmatrix}
\]

(3)

The received signal at Bob and Eve are:

\[
y_b = \sqrt{P_A/n_r}\mathbf{H}^\dagger\mathbf{W}s + v_b.
\]

(4)

\[
y_e = \sqrt{P_A/n_e}\mathbf{G}^\dagger\mathbf{W}s + v_e.
\]

(5)

where \( P_A \) is the power budget of Alice. \( v_b \) and \( v_e \) are the CSCG noises at Bob and Eve, respectively, i.e., \( v_b \sim \mathcal{C}_N(0, \sigma_v^2) \), \( v_e \sim \mathcal{C}_N(0, \sigma_v^2) \).

Assuming Bob and Eve apply maximal ratio combining (MRC) to combine the received signals at different antennas, the average SNRs at Bob and Eve are:

\[
\text{SNR}_b = \frac{P_A}{n_r\sigma_v^2} \| \mathbf{H}^\dagger\mathbf{W} \|^2.
\]

(6)

\[
\text{SNR}_e = \frac{P_A}{n_e\sigma_v^2} \| \mathbf{G}^\dagger\mathbf{W} \|^2.
\]

(7)

If there is no PSA, \( \hat{\mathbf{h}}_i \approx \sqrt{P_B}h_i \), so \( \mathbf{W}_i = \hat{\mathbf{h}}_i/\| \hat{\mathbf{h}}_i \| \approx \hat{\mathbf{h}}_i/\| \mathbf{h}_i \| \). In this situation SNR\(_b\) can achieve to the maximum as the antennas are aligned to Bob. When Eve exists, the \( \mathbf{W} \) would not perfectly point to Bob, which leads to a decrease in SNR\(_b\) and an increase in SNR\(_e\). Especially when \( P_E \) is large enough the SNR at Eve will be larger than that at Bob, which means that Bob will get a negative secrecy rate. What’s more, the pilot length of channel training phase \( N_1 = n_rN_1' \) will be greatly increased in MIMO systems and this is impossible in practical applications as this will lead to a decrease of the data transmission length.

From the analysis above, it is critical to detect PSA and guarantee secure transmission. To do so, we propose an SSM.
by exploiting the spatial spectrums to detect Eve by a given threshold and locate Eve by comparing spatial spectrums attained respectively at Alice and Bob ends as shown in Fig. 1. The advantage of SSM is that the spatial information (the geographic location, i.e., the DOA and the distance) can be estimated with only one transmit antenna during the training process, which saves the training time and energy consumption compared to the method above. Hence, the channel model of the legitimate and the illegitimate channel are modeled as [29]:

\[
\begin{align*}
\mathbf{h} &= \sum_{l=1}^{L} \eta_{hl} \mathbf{a}(\theta_{hl}), \\
\mathbf{g} &= \sum_{l=1}^{L} \eta_{el} \mathbf{a}(\theta_{el}),
\end{align*}
\]

which represents the propagation over \(L\) paths, \(\eta_{hl}\) and \(\eta_{el}\) denote the large-scale fading coefficients, \(\mathbf{a}(\theta_{hl})\) and \(\mathbf{a}(\theta_{el})\) are the array steering vectors of Bob and Eve, respectively; \(\theta(\theta) = \left[1, e^{-2\pi d \sin \theta_1/d}, \ldots, e^{-2\pi(n-1)d \sin \theta_L/d}\right]^T\), \(\theta \in (-\frac{\pi}{2}, \frac{\pi}{2})\), \(\theta_{hl}\) and \(\theta_{el}\) respectively denote the DOAs of Bob and Eve. The detailed process of our method is as follows: in the first stage, Bob sends pilot signals with one antenna and then Alice detects if PSA happens based on the received signals. In the second stage, Alice either launches the downlink training with one antenna if PSA happens or it directly estimates the channel. If Eve was detected, Bob estimates the spatial spectrum and feeds back the results to Alice. The localization of Bob and Eve (identify the DOA of Bob and Eve and get the geographical distance of Alice-Bob and Alice-Eve) will down at Alice end.

III. DETECTING THE EAVESDROPPER BASED ON THE SPATIAL SPECTRUM

From the analysis in section II, we can see PSA would cause serious damage to data transmission, which has motivated researchers to find effective methods to cope with PSA. In this paper, we focus on an SSM to detect Eve during the pilot training phase. In this phase, the antenna works in omnidirectional emission mode and Bob would use only one single antenna to launch the uplink training. Different from other two-way training method, this idea only needs uplink training in the detection process. The downlink training process is required only when Eve is detected, otherwise, we can directly estimate the channel and transmit confidential information.

In this section, we define two hypotheses \(\mathcal{H}_0\) and \(\mathcal{H}_1\). \(\mathcal{H}_0\) denotes that Alice is not under PSA and \(\mathcal{H}_1\) means that Eve conducts the PSA. Next, we will introduce the spatial spectrum detection method in detail.

To realize secure transmission, Bob transmits the assigned pilot signals with one antenna, Eve also broadcasts the same pilot signals with one antenna synchronously with Bob to spoof Alice if PSA happens. The received signal under \(\mathcal{H}_0\) and \(\mathcal{H}_1\) are respectively denoted by:

\[
\begin{align*}
2\mathcal{H}_0 : \mathbf{y}_a(n) &= \sqrt{P_B}\mathbf{h}\mathbf{x}(n) + \mathbf{u}(n), \\
\mathcal{H}_1 : \mathbf{y}_a(n) &= \left(\sqrt{P_B}\mathbf{h} + \sqrt{P_E}\mathbf{g}\right)x(n) + \mathbf{u}(n).
\end{align*}
\]

Alice obtains the spatial spectrum of the received signal based on spatial matched filtering [30]:

\[
S_A(\theta) = \mathbf{a}^H(\theta) \mathbf{E}_\alpha \mathbf{y}_a(n) \mathbf{a}(\theta).
\]

The spatial spectrum \(S_A(\theta)\) will reach its peaks when \(\theta\) is aligned to the DOAs of the incoming signals from (12) [31], i.e., \(\theta = \theta_{hl}\) or \(\theta = \theta_{el}\) (if PSA happens). In a narrow band channel model, the losses of reflective and scattering paths are relatively high; hence, the line-of-sight (LOS) path usually dominates in the multipath. And the spatial peaks caused by the non-line of sight paths are usually very low or may be submerged in noise. Hence, the channel model in our analysis equivalent to \(\mathbf{h} \rightarrow \eta_{hl}\mathbf{a}(\theta_{hl})\) and \(\mathbf{g} \rightarrow \eta_{el}\mathbf{a}(\theta_{el})\) [32], [33]. \(\eta_{hl} \in \{\eta_{hl}|l = 1, \ldots, L\}\), \(\eta_{el} \in \{\eta_{el}|l = 1, \ldots, L\}\). \(\eta_{lb} = D_{ab}^{-d/2}\) and \(\eta_{ae} = D_{ae}^{-d/2}\) represent the large-scale fading coefficients for the LOS path of the and illegitimate channels, respectively, whereby \(d\) is the path loss exponent. The spatial spectrum is an important step in our algorithm, and there is no need to estimate the channel by inversion in our model, which greatly reduces the complexity of the algorithm. The complexity based on (12) is \(2n^2_l + n\).

According to the new scheme of the SSM method, \(S_A(\theta)\) can be estimated by a finite pilot length \(N_1 = N'_1\) which significantly reduces the training length compared to the training length \(N_1 = n_1N'_1\) in the time domain, i.e.,

\[
\hat{S}_A(\theta) = \frac{1}{N_1} \sum_{n=1}^{N_1} \left| \mathbf{a}^H(\theta) \mathbf{y}_a(n) \right|^2.
\]

From (13), for a fixed \(\theta\), \(y'_a(n) = \mathbf{a}^H(\theta) \mathbf{y}_a(n)\) follows a CSCG random variable. And then \(\left|y'_a(n)\right|^2\) is a non-central Chi-square distribution with 2 degrees of freedom. Based on the central limit theorem (CLT), \(\hat{S}_A(\theta)\) can be approximated by a Gaussian random variable for a given \(\theta\) when the sampling point \(N_1\) (the degree-of-freedom is \(2N_1\)) is sufficiently large.

If \(\mathcal{H}_0\) is true, one major peak \(\hat{S}_A(\theta_{hl})\) can be observed. If \(\mathcal{H}_1\) is true, two major peaks \(\hat{S}_A(\theta_{hl}), \hat{S}_A(\theta_{el})\) can be observed. In addition, some fake smaller peaks \(\hat{S}_A(\theta)\) \((i = 1, 2, \ldots)\) also can be observed, i.e., aroused by the noise or oscillation effects in the spatial spectrum. Based on the analysis above, when the number of degrees of freedom \(2N_1\) is large, \(\hat{S}_A(\theta_{hl}), \hat{S}_A(\theta_{el})\) follow Gaussian distributions, i.e., \(\hat{S}_A(\theta_{hl}) \sim N'\left(\mu_{hl}, \sigma^2_{hl}\right), \hat{S}_A(\theta_{el}) \sim N'\left(\mu_{el}, \sigma^2_{el}\right)\):

\[
\begin{aligned}
\mu_{m} &= n_1\sigma^2_{at} + \beta_m, \\
\sigma^2_{m} &= \frac{1}{N_1} (n^2_u\sigma^4_{at} + 2n_1\sigma^2_{at}\beta_{m}),
\end{aligned}
\quad m = i, b, e.
\]
where
\[
\begin{align*}
\beta_i &= \sqrt{\mathbb{E}_{\eta_b|H}(\theta_i) a(\theta_b) + \sqrt{\mathbb{E}_{\eta_a|H}(\theta_i) a(\theta_e)}^2,} \\
\beta_b &= \sqrt{\mathbb{E}_{\eta_b|H} + \sqrt{\mathbb{E}_{\eta_a|H}(\theta_i) a(\theta_e)}^2,} \\
\beta_c &= \sqrt{\mathbb{E}_{\eta_b|H}(\theta_i) a(\theta_b) + \sqrt{\mathbb{E}_{\eta_a|H}(\theta_e)}^2}.
\end{align*}
\]
(15)

Then we derive the threshold \( \gamma \) based on the false alarm probability \( P_{fa} \):
\[
P_{fa} = P_r (\text{card}(B) = 2 | H_0) \\
\approx \left( \int_{-\infty}^{+\infty} f_1(x)dx \right) \left( \int_{-\infty}^{+\infty} f_0(x)dx \right) \\
= (1 - F_1(\gamma) ) (1 - F_0(\gamma) ) ,
\]
(16)

where \( B = \{ \hat{S}_A(\theta_m) | \hat{S}_A(\theta_m) > \gamma, m = b, e, i \} \) denotes the set of detected peaks and \( \text{card}(\cdot) \) denotes the number of elements in the set. \( f_0(\gamma) \) and \( F_0(\gamma) \) are the PDF and CDF, respectively, of \( \hat{S}_A(\theta)_m \) \( \gamma \) is derived from the different fake peaks \( \hat{S}_A(\theta) \) with a given \( P_{fa} \). Then the detection threshold is \( \gamma = \max{\{\gamma\}} \).

The hypothesis test problem is:
\[
H_0 : \text{card}(B) < 2, \\
H_1 : \text{card}(B) = 2
\]
(17)

Based on the threshold \( \gamma \), we can obtain the detection probability \( P_d \) of Eve as follows:
\[
P_d = P_r (\text{card}(B) = 2 | H_1) \\
\approx \left( \int_{-\infty}^{+\infty} f_1(x)dx \right) \left( \int_{-\infty}^{+\infty} f_2(x)dx \right) \\
= (1 - F_1(\gamma) ) (1 - F_2(\gamma) ) ,
\]
(18)

where \( f_2(\gamma) \) and \( F_2(\gamma) \) are the PDF and CDF of \( \hat{S}_A(\theta) \). In fact, we have excluded a special case in the above derivation, whereby Bob and Eve are spatially close to each other. I.e., if Bob and Eve have the same DOAs, or if the DOAs of them are very close, then our method will have difficulty in detecting pilot spoofing attack.

After the PSA detection process, we execute the downlink training process to locate Bob and Eve if PSA happens; otherwise, we will directly estimate the location of Bob and transmit confidential information.

IV. LOCALIZATION OF THE EAVESDROPPER
A. IDENTIFICATION OF THE EAVESDROPPER

If we detect the PSA happens, then we obtain two DOAs according to the \( \hat{\theta} = \arg \max \hat{S}_A(\theta) \). Then we further identify the two incoming signals as being transmitted by Eve by executing the downlink training phase based on the symmetry of the uplink and downlink channels in a time-division-duplex (TDD) system. In this paper, we consider the case where Alice and Bob are both under the PSA; this means Eve also launches PSA during the downlink training process as in Fig.1 (it is obvious our method also applies for the case where Eve keeps silent during the downlink training process). Therefore, during the downlink training phase, Bob can detect two peaks \( \hat{S}_a(\theta_a) \) and \( \hat{S}_b(\theta_e) \) that arise by the incoming signals from Alice and Eve. \( \theta_a \) and \( \theta_e \) are separately the DOAs of the incoming signal from Alice and Eve at the Bob end. As with \( \hat{S}_a(\theta_b) \), \( \hat{S}_b(\theta_e) \) and \( \hat{S}_e(\theta_e) \) also follow Gaussian distributions, i.e., \( \hat{S}_a(\theta_a) \sim \mathcal{N}(\mu_a, \sigma_a^2) \), \( \hat{S}_b(\theta_e) \sim \mathcal{N}(\mu_e, \sigma_e^2) \).

Then we derive the threshold \( \gamma \) based on the false alarm probability \( P_{fa} \):
\[
P_{fa} = P_r (\text{card}(B) = 2 | H_0) \\
\approx \left( \int_{-\infty}^{+\infty} f_1(x)dx \right) \left( \int_{-\infty}^{+\infty} f_0(x)dx \right) \\
= (1 - F_1(\gamma) ) (1 - F_0(\gamma) ) ,
\]
(16)

where \( B = \{ \hat{S}_A(\theta_m) | \hat{S}_A(\theta_m) > \gamma, m = b, e, i \} \) denotes the set of detected peaks and \( \text{card}(\cdot) \) denotes the number of elements in the set. \( f_0(\gamma) \) and \( F_0(\gamma) \) are the PDF and CDF, respectively, of \( \hat{S}_A(\theta)_m \). \( \gamma \) is derived from the different fake peaks \( \hat{S}_A(\theta) \) with a given \( P_{fa} \). Then the detection threshold is \( \gamma = \max{\{\gamma\}} \).

The hypothesis test problem is:
\[
H_0 : \text{card}(B) < 2, \\
H_1 : \text{card}(B) = 2
\]
(17)

Based on the threshold \( \gamma \), we can obtain the detection probability \( P_d \) of Eve as follows:
\[
P_d = P_r (\text{card}(B) = 2 | H_1) \\
\approx \left( \int_{-\infty}^{+\infty} f_1(x)dx \right) \left( \int_{-\infty}^{+\infty} f_2(x)dx \right) \\
= (1 - F_1(\gamma) ) (1 - F_2(\gamma) ) ,
\]
(18)

where \( f_2(\gamma) \) and \( F_2(\gamma) \) are the PDF and CDF of \( \hat{S}_A(\theta) \). In fact, we have excluded a special case in the above derivation, whereby Bob and Eve are spatially close to each other. I.e., if Bob and Eve have the same DOAs, or if the DOAs of them are very close, then our method will have difficulty in detecting pilot spoofing attack.

After the PSA detection process, we execute the downlink training process to locate Bob and Eve if PSA happens; otherwise, we will directly estimate the location of Bob and transmit confidential information.
Then, we have
\[
\begin{align*}
\left(\hat{S}_A (\theta_b) - \hat{S}_B (\theta_a)\right) &\sim N \left(0, \sigma_b^2 + \sigma_a^2\right), \\
\left(\hat{S}_A (\theta_b) - \hat{S}_B (\theta_a)\right) &\sim N \left(\mathbb{P}_B \eta_{ab}^2 \eta_{ab}^2 - \mathbb{P}_E \eta_{ab}^2 \eta_{ab}^2, \sigma_b^2 + \sigma_a^2\right), \\
\left(\hat{S}_A (\theta_e) - \hat{S}_B (\theta_a)\right) &\sim N \left(\mathbb{P}_B \eta_{ea}^2 \eta_{ea}^2 - \mathbb{P}_E \eta_{ea}^2 \eta_{ea}^2, \sigma_e^2 + \sigma_a^2\right), \\
\left(\hat{S}_A (\theta_e) - \hat{S}_B (\theta_e)\right) &\sim N \left(\mathbb{P}_E \eta_{ea}^2 \eta_{ea}^2 - \mathbb{P}_E \eta_{ea}^2 \eta_{ea}^2, \sigma_e^2 + \sigma_e^2\right).
\end{align*}
\]

(23)

In order to identify the DOA of Eve, the test statistics are designed as:
\[
\begin{align*}
\Delta_1 &= \left|\hat{S}_A (\theta_b) - \hat{S}_B (\theta_a)\right|, \\
\Delta_2 &= \left|\hat{S}_A (\theta_b) - \hat{S}_B (\theta_a)\right|, \\
\Delta_3 &= \left|\hat{S}_A (\theta_e) - \hat{S}_B (\theta_a)\right|, \\
\Delta_4 &= \left|\hat{S}_A (\theta_e) - \hat{S}_B (\theta_e)\right|.
\end{align*}
\]

(24)

Then the problem of identifying the DOA of Eve based on (24) is becoming which is the minimum value \(\Delta_{\min}\) among the four test statistics \(\Delta_1, \Delta_2, \Delta_3,\) and \(\Delta_4\).

If \(\Delta_1\) is the minimum value, then we can correctly identify the DOA of Eve at the Alice end as \(\theta_a\) and the DOA of Eve at the Bob end as \(\theta_e\):
\[
\Delta_{\min} = \Delta_1 \Rightarrow \begin{cases} 
S_A (\theta_b) = \hat{S}_A (\theta_b), \\
S_A (\theta_e) = \hat{S}_A (\theta_e), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e).
\end{cases}
\]

(25)

If \(\Delta_2\) is the minimum value, then we can correctly identify the DOA of Eve at the Alice end as \(\theta_a\) and falsely recognize the DOA of Eve at the Bob end as \(\theta_e\):
\[
\Delta_{\min} = \Delta_2 \Rightarrow \begin{cases} 
S_A (\theta_b) = \hat{S}_A (\theta_b), \\
S_A (\theta_e) = \hat{S}_A (\theta_e), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_b).
\end{cases}
\]

(26)

If \(\Delta_3\) is the minimum value, then we can falsely recognize the DOA of Eve at the Alice end as \(\theta_b\) and correctly identify the DOA of Eve at the Bob end as \(\theta_e\):
\[
\Delta_{\min} = \Delta_3 \Rightarrow \begin{cases} 
S_A (\theta_b) = \hat{S}_A (\theta_e), \\
S_A (\theta_e) = \hat{S}_A (\theta_b), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e).
\end{cases}
\]

(27)

If \(\Delta_4\) is the minimum value, then we can falsely recognize the DOA of Eve at the Alice end as \(\theta_e\) and falsely recognize the DOA of Eve at the Bob end as \(\theta_a\):
\[
\Delta_{\min} = \Delta_4 \Rightarrow \begin{cases} 
S_A (\theta_b) = \hat{S}_A (\theta_e), \\
S_A (\theta_e) = \hat{S}_A (\theta_b), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e).
\end{cases}
\]

(28)

According to (25), (26), (27) and (28), if \(\Delta_{\min} = \Delta_1\) or \(\Delta_{\min} = \Delta_2\), the incoming signals at the Alice end would have a correct judgment; if \(\Delta_{\min} = \Delta_3\) or \(\Delta_{\min} = \Delta_4\), the incoming signals at the Bob end would have a correct judgment, as follows:
\[
\begin{align*}
\Delta_{\min} = \Delta_1 &\Rightarrow \left\{ 
S_A (\theta_b) = \hat{S}_A (\theta_b), \\
S_A (\theta_e) = \hat{S}_A (\theta_e), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e)
\right\}, \\
\Delta_{\min} = \Delta_2 &\Rightarrow \left\{ 
S_A (\theta_b) = \hat{S}_A (\theta_b), \\
S_A (\theta_e) = \hat{S}_A (\theta_e), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_b)
\right\}, \\
\Delta_{\min} = \Delta_3 &\Rightarrow \left\{ 
S_A (\theta_b) = \hat{S}_A (\theta_e), \\
S_A (\theta_e) = \hat{S}_A (\theta_b), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e)
\right\}, \\
\Delta_{\min} = \Delta_4 &\Rightarrow \left\{ 
S_A (\theta_b) = \hat{S}_A (\theta_e), \\
S_A (\theta_e) = \hat{S}_A (\theta_b), \\
S_B (\theta_a) = \hat{S}_B (\theta_a), \\
S_B (\theta_e) = \hat{S}_B (\theta_e)
\right\}.
\end{align*}
\]

(29)

(30)

To obtain the ratio of the correct recognition of \(\hat{S}_A (\theta_b)\) and \(\hat{S}_A (\theta_e)\) or \(\hat{S}_B (\theta_a)\) and \(\hat{S}_B (\theta_e)\), we use the minimum error probability method. As the recognition method of \(\hat{S}_B (\theta_a)\) and \(\hat{S}_B (\theta_e)\) is similar to that of \(\hat{S}_A (\theta_b)\) and \(\hat{S}_A (\theta_e)\), we will only discuss the ratio of correct recognition \(P_c\) of \(\hat{S}_B (\theta_a)\) and \(\hat{S}_A (\theta_a)\), i.e., \(P_e = 1 - P_c\). \(P_e\) is the minimum error probability of recognizing \(\hat{S}_A (\theta_b)\) and \(\hat{S}_A (\theta_e)\) as in (31), as shown at the bottom of the page. In (31), \(f_{\Delta_1}(\chi), f_{\Delta_2}(\chi), f_{\Delta_3}(\chi),\) and \(f_{\Delta_4}(\chi)\) are the PDFs of \(\Delta_1, \Delta_2, \Delta_3,\) and \(\Delta_4\), respectively. \(F_{\Delta_1}(\cdot), F_{\Delta_2}(\cdot), F_{\Delta_3}(\cdot),\) and \(F_{\Delta_4}(\cdot)\) are the CDFs of \(\Delta_1, \Delta_2, \Delta_3,\) and \(\Delta_4\), respectively. \(\gamma'\) is the decision threshold that minimizes the above \(P_e\), which can be determined based on \(\frac{\partial P_e}{\partial \gamma'} = 0\).

There is more than one minimum value among \(\Delta_1, \Delta_2, \Delta_3,\) and \(\Delta_4\) in some special situations, such as \(\Delta_{\min} = \Delta_1 = \Delta_2, \Delta_{\min} = \Delta_1 = \Delta_3, \Delta_{\min} = \Delta_1 = \Delta_4\) and so on. It may occur when Eve exactly stays on a circle centered on Alice’s location and with a radius of \(D_{ab}\), i.e., \(D_{ae} = D_{ab}\) and \(P_E = P_B\) or when Eve exactly stays on a circle centered on Bob’s location with a radius of \(D_{ab}\), i.e., \(D_{be} = D_{ab}\) and \(P_E = P_B\), or when Eve is located along the central axis between Alice and Bob, i.e., \(D_{ae} = D_{be}\) and \(P_E = P_B\). However, these situations are rare in practical applications due to the randomness of the location distribution. Thus, our proposed scheme can potentially be used to recognize Eve (i.e., determine the DOAs of Bob and Eve).

**B. GEOGRAPHIC DISTANCES**

To achieve secure data transmission in the data transmission phase, we locate Bob and Eve by estimating the geographic distances \(D_{ab}, D_{ae},\) and \(D_{be}\) after obtaining the DOAs of
Bob and Eve. Then, we have two methods to estimate the geographic distances.

1) DEDUCTION METHOD
We can estimate the geographic distances according to the relationship between spatial spectrum and geographic distance, such as from (12) we can obtain:

$$S_A(\theta) = P_B D_{ab} a(\theta) a^\dagger (\theta_a) a(\theta_b) a(\theta) + P_B D_{ac} a(\theta) a(\theta_c) a(\theta) + n_1 \sigma^2 + \sqrt{P_B P_E D_{ac}^{-c/2}} D_{ac}^{-c/2} a(\theta) a(\theta_c) a(\theta) + \sqrt{P_B P_E D_{ab}^{-c/2}} D_{ab}^{-c/2} a(\theta) a(\theta_b) a(\theta) .$$

(32)

Based on (32), the geographic distances $D_{ab}, D_{ae}$, and $D_{be}$ are (33), as shown at the bottom of this page, where

$$\alpha_1 = \left| \frac{1 - e^{2\pi n_1 d(\sin \theta_b - \sin \theta_c)/\lambda}}{1 - e^{2\pi d(\sin \theta_b - \sin \theta_c)/\lambda}} \right|^2 ,$$

$$\alpha_2 = \frac{1}{2} \left| \frac{1 - e^{2\pi n_1 d(\sin \theta_b - \sin \theta_c)/\lambda}}{1 - e^{2\pi d(\sin \theta_b - \sin \theta_c)/\lambda}} \right|^2 ,$$

$$\alpha_3 = \left| \frac{1 - e^{2\pi n_1 d(\sin \theta_c - \sin \theta_c)/\lambda}}{1 - e^{2\pi d(\sin \theta_c - \sin \theta_c)/\lambda}} \right|^2 ,$$

$$\alpha_4 = \frac{1}{2} \left| \frac{1 - e^{2\pi n_1 d(\sin \theta_c - \sin \theta_c)/\lambda}}{1 - e^{2\pi d(\sin \theta_c - \sin \theta_c)/\lambda}} \right|^2 .$$

(34)

Therefore we can estimate the geographic distances $D_{ab}, D_{ae}$, and $D_{be}$ through the equation set (33).

2) NEAREST NEIGHOR METHOD
To achieve secure data transmission in the data transmission phase, we can estimate $D_{ab}$ with fingerprint-based localization [34] by matching the received signal spatial spectrum peaks against the information in the fingerprint database. Then, we can locate Eve according to the triangle rule.

Fingerprint-based localization includes two steps: populating the fingerprint database and fingerprint matching. The fingerprint database should be constructed in advance. In our method, as we have recognized Bob and obtained its DOA, we can locate Bob if we obtain the geographic distance $D_{ab}$. Fingerprint-based localization estimates the location of Bob by exploring the relationship of the geographic distance $D$ and the spatial spectrum peaks $S(\theta)$. The signal fingerprint form used in this paper is as follows:

$$F(D) = \langle [D_1, S_1(\theta)] \ldots [D_J, S_J(\theta)] \rangle ,$$

where $F(D)$ is the signal fingerprint with geographic distance $D$, $J$ is the number of the reference location and $S_j$ is the spatial spectrum peak at location $D_j$.

The second step in fingerprint-based localization is fingerprint matching. In this paper, we adopt the nearest neighbor algorithm to select the closest fingerprint. The nearest neighbor algorithm measures the Euclidean distances between the received spatial spectrum peak and each reference location in the fingerprint database, i.e.,

$$\text{dist}_j = \left( \hat{S}_A(\theta_b) - S_j(\theta) \right)^2 .$$

(36)

Then, the geographic distance of $\hat{D}_{ab}$ can be obtained by the nearest fingerprint $\min(\text{dist}_j)$.

When we finish the positioning of Bob, we will obtain a triangle that consists of Alice, Bob and Eve. Then, we can

$$D_{ab}^{c/2} = \sqrt{S_A(\theta_b) - P_B D_{ac}^{-c/2} a_1 P_E D_{ac}^{-c/2} a_2 - n_1 \sigma^2 - \sqrt{P_B D_{ac}^{-c/2}} a_2} ,$$

$$D_{ae}^{c/2} = \sqrt{S_A(\theta_a) - P_B D_{ae}^{-c/2} a_1 P_E D_{ae}^{-c/2} a_2 - n_1 \sigma^2 - \sqrt{P_B D_{ae}^{-c/2}} a_2} ,$$

$$D_{be}^{c/2} = \sqrt{S_B(\theta_c) - P_B D_{ae}^{-c/2} a_3 P_E D_{ae}^{-c/2} a_4 - n_2 \sigma^2 - \sqrt{P_B D_{ae}^{-c/2}} a_4} ,$$

$$D_{ab}^{c/2} = \sqrt{S_B(\theta_a) - P_E D_{be}^{-c/2} a_3 P_B D_{be}^{-c/2} a_4 - n_2 \sigma^2 - \sqrt{P_E D_{be}^{-c/2}} a_4} .$$

(33)
Algorithm

1: Bob broadcasts the pilot signal in the uplink training process.
2: Alice estimates the spatial spectrum peak values $S_A(\theta_b)$, $S_A(\theta_e)$ if PSA happens.
3: Detects if Eve exists or not. If exists goes to 4, otherwise, it goes to 7.
4: Alice sends the pilot signal in the downlink training process.
5: Bob estimates the spatial spectrum peak value $S_B(\theta_b)$ and $S_B(\theta_e)$ and feedbacks them to Alice.
6: Alice identifies which is Eve by comparing $S_A(\theta_b)$, $S_A(\theta_e)$ with $S_B(\theta_b)$ and $S_B(\theta_e)$.
7: Alice estimates geographic distances $D_{ab}$, $D_{ae}$, $D_{be}$.

**FIGURE 3.** Detection probability versus $P_E$, under $n_t = 32$, $N_1 = 100$ and $P_B = 10dB$.

use the triangle rule to deduce the distance between Alice and Eve $D_{ae}$.

Based on the above elaborations, our designed method is illustrated by the following flowchart.

**V. SIMULATION RESULTS**

In this section, we execute computer simulations and provide numerical results to validate our theoretical analysis in an MIMO system with $n_t = n_r = n_e = 32$ antennas. All simulation results are obtained from 10000 Monte Carlo runs. Generally, we set the path loss index to be 3. The transmission power budgets of Alice and Bob are set to 10 dB, and the noise variance is normalized to 1, i.e., $\sigma_n^2 = \sigma_e^2 = 1$. Without special instructions, the locations of Alice, Bob, and Eve are fixed, and the distances between Alice and Bob and between Alice and Eve are $D_{ab} = 10m$ and $D_{ae} = 13m$, respectively. We conduct several simulations to evaluate the detection and localization performance (identifying the DOA and the geographic distance of Bob and Eve) under different conditions.

As in Fig. 3, we can investigate the detection performance of our SSM method and the other TWTD method under different power budgets of Eve $P_E$. This validates our theoretical analysis, as the simulation results almost overlap with those of the theoretical analysis. The detection probability $P_d$ improves with increasing power $P_E$. This means that the risk of being detected increases as Eve’s power increases, although this also improves the eavesdropping rate. Fig. 3 evaluates the detection performance under different false alarm probabilities $P_{fa} = 0.01, 0.1$, and Fig. 3 shows that a larger false alarm probability can lead to a higher detection probability. Fig. 3 also compares the detection performance of our SSM and the TWTD method for different cases. The SSM suppresses the TWTD method when $P_E$ is greater than -4dB. This is reasonable, as the spatial peak value suppresses the interference noise by spectrum decomposition in the spatial domain and hence improves the SNR of the received signal. Moreover, the training length of each antenna for the TWTD method in the MIMO scenario is much smaller than that observed in [27] when the total training length is fixed. Hence, the TWTD method may not be suitable for MIMO scenarios, which may require a large training length, which itself is unrealistic.

Fig. 4 evaluates the detection performance of the proposed SSM method and the other TWTD method for $P_E = -3.7dB$ under different training lengths $N_1$. It is easy to observe that the simulation results overlap with the theoretical results, which further validates the accuracy of our theoretical analysis. In Fig. 4, we can see that the detection performance of the SSM method and the TWTD method increase with increasing training length $N_1$ and that even with a limited $N_1$.
the SSM can obtain perfect detection performance. Moreover, unlike the TWTD method, the SSM method does not require downlink training in the detection process, which reduces the training length. The downlink training length of the TWTD method \(N_2 = N_1\). Therefore, our method has great promise in practical applications because the training length is considerable in practical applications.

Fig. 5 shows the ratio of correct recognition under SNR which changes from 0dB to 10dB. It shows that the ratio of correct recognition increases with increasing SNR and the recognition performance can achieve a satisfying result even when \(\text{SNR} = 0\)dB. We also can observe the accuracy of the theoretical analysis, as its result match the simulation result well.

Fig. 6 evaluates the ratio of correct recognition \(P_c\) under the power budgets of Eve \(P_E\) which changes from 5dB to 13dB. The locations of Alice, Bob, and Eve are fixed and the distances of Alice-Bob and Alice-Eve are \(D_{ab} = D_{ae} = 10\)m. It can be observed that the ratio of correct recognition \(P_c\) decreases when \(P_E \approx 10\)dB. We also can observe that the ratio of correct recognition is below 0.5 when \(P_E = P_B = 10\)dB. This means that we cannot recognize Bob from Eve. This is because Eve and Bob are located on the same circle centered on Alice, and so any recognition of Eve would be invalid. However, the ratio of correct recognition achieves satisfactory results when \(P_E\) is not approximately equal to \(P_B\).

As Eve and Bob are randomly distributed (\(D_{ab} \neq D_{ae}\) in most situations) we believe that our method would yield good performance even if \(P_E = P_B\).

Fig. 7 shows the mean square error (MSE) of the geographic distance estimation methods (the deduction method and the fingerprint-based method) for \(\theta_B = \pi/3, \theta_E = \pi/6\). The figure shows that the fingerprint-based method would have better performance for low SNRs and the deduction method would have better performance in better environments. Fig. 7 also indicates that both methods can yield good performance in estimating geographic distances.

VI. CONCLUSION

In this paper, we studied the PSA problem in a MIMO system. Since this attack could cause considerable damage, we propose an SSM method to address the problem. First, the new method can effectively detect the eavesdropper by using the spatial spectrum peaks and improve the detection accuracy by effectively suppressing the interference noise. Second, this method utilizes the differences between the peaks attained in the uplink training phase and the downlink training phase to identify the eavesdropper. In addition, this method can obtain the relative geographic locations of Alice, Bob and Eve, making secure transmission possible. The most important contribution of our work is that it can not only detect if PSA occurs but also obtain the locations of Alice, Bob and Eve. Numerical results validate the effectiveness of the SSM and demonstrate that our method can dramatically improve the detection performance even with a limited sampling length over that of a TWTD method. The simulation results also demonstrate the accuracy of the estimated geographical distance. Hence, this method has great promise for realizing secure transmission with DOAs and geographical distances by using beamforming technology.

REFERENCES

[1] R. Di Pietro, L. V. Mancini, and S. Jajodia, “Efficient and secure keys management for wireless mobile communications,” in Proc. 2nd ACM Int. Workshop Princ. Mobile Comput. (POMC), 2002, pp. 66–73.
[2] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proc. Symp. Secure Privacy, 2003, pp. 197–213.
[3] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge, U.K.: Cambridge Univ. Press, 2011.
[4] X. Zhou, Y. Zhang, and L. Song, Physical Layer Security in Wireless Communications. Boca Raton, FL, USA: CRC Press, 2016.
[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.
[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.
[7] X. Zhang, X. Zhou, and M. R. McKay, “On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels,” IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[8] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, “Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks,” IEEE Trans. Signal Process., vol. 63, no. 1, pp. 206–220, Jan. 2015.
[9] R. Zhang, L. Song, Z. Han, and B. Jiao, “Physical layer security for two-way untrusted relaying with friendly jammers,” IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3693–3704, Oct. 2012.
[10] B. Li, Z. Zhou, W. Zou, X. Sun, and G. Du, “On the efficient beamforming training for 60 GHz wireless personal area networks,” IEEE Trans. Wireless Commun., vol. 12, no. 2, pp. 504–515, Feb. 2013.

[11] B. Li, Z. Zhou, H. Zhang, and A. Nallanathan, “Efficient beamforming training for 60-GHz millimeter-wave communications: A novel numeri- cal optimization framework,” IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 703–717, Feb. 2014.

[12] J. Zhu, R. Schober, and V. K. Bhargava, “Secure transmission in multicell massive MIMO systems,” IEEE Wireless Commun., vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[13] F. Zhu, F. Gao, M. Yao, and H. Zou, “Joint information- and jamming-beamforming for physical layer security with full duplex base station,” IEEE Trans. Signal Process., vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[14] 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.

[15] A. Khisti and G. Wornell, “Secure transmission with multiple antennas II: The MIMOME wiretap channel,” 2010, arXiv:1006.5879. [Online]. Available: http://arxiv.org/abs/1006.5879

[16] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2008, pp. 524–528.

[17] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[18] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May 1978.

[19] X. Zhou, B. Maham, and A. Hjorungnes, “Pilot contamination for active eavesdropping,” IEEE Trans. Wireless Commun., vol. 11, no. 3, pp. 903–907, Mar. 2012.

[20] D. Kapetanović, G. Zheng, K.-K. Wong, and B. Ottersten, “Detection of pilot contamination attack using random training and massive MIMO,” in Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Sep. 2013, pp. 13–18.

[21] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang, “A semiblind two-way training method for discriminatory channel estimation in MIMO systems,” IEEE Trans. Commun., vol. 62, no. 7, pp. 2400–2410, Jul. 2014.

[22] 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.

[23] J. K. Tugnait, “Detection and identification of spoofed pilots in TDD/SDMA systems,” IEEE Wireless Commun. Lett., vol. 6, no. 4, pp. 550–553, Aug. 2017.

[24] J. Xie, Y.-C. Liang, J. Fang, and X. Kang, “Two-stage uplink training for pilot spoofing attack detection and secure transmission,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2017, pp. 1–6.

[25] X. Liu, B. Li, H. Chen, Z. Sun, Y.-C. Liang, and C. Zhao, “Detecting pilot spoofing attack in MISO systems with trusted user,” IEEE Commun. Lett., vol. 23, no. 2, pp. 314–317, Feb. 2019.

[26] 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.

[27] Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Han, “Secure transmission against pilot spoofing attack: A two-way training-based scheme,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 1017–1026, May 2016.

[28] S. M. Kay, Fundamentals of Statistical Processing: Estimation Theory, vol. 1. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.

[29] Y. R. Ramadan, A. S. Ibrahim, and M. M. Khairy, “RF beamforming for secrecy millimeter wave MISO-OFDM systems,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2016, pp. 1–6.

[30] M. S. Bartlett, An Introduction to Stochastic Processes: With Special Reference to Methods and Applications. Cambridge, U.K.: CUP Archive, 1978.

[31] T. Li and Y. Tang, “Frequency estimation based on modulation FFT and MUSIC algorithm,” in Proc. 1st Int. Conf. Pervas. Comput., Signal Process. Appl., Sep. 2010, pp. 525–528.

[32] M. N. Alotaih and K. A. Handi, “Switched phased-array transmission architecture for secure millimeter-wave wireless communication,” IEEE Trans. Commun., vol. 64, no. 3, pp. 1303–1312, Mar. 2016.

[33] W.-Q. Wang and Z. Zheng, “Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications,” IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1383–1396, Jul. 2018.

[34] Q. D. Vo and P. De, “A survey of fingerprint-based outdoor localization,” IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 491–506, 1st Quart., 2016.