Abstract—This paper considers a pilot spoofing attack scenario in a massive MIMO system. A malicious user tries to disturb the channel estimation process by sending interference symbols to the basestation (BS) via the uplink. Another legitimate user counters by sending random symbols. The BS does not possess any partial channel state information (CSI) and distribution of symbols sent by malicious user \textit{a priori}. For such scenario, this paper aims to separate the channel directions from the legitimate and malicious users to the BS, respectively. A blind channel separation algorithm based on estimating the characteristic function of the distribution of the signal space vector is proposed. Simulation results show that the proposed algorithm provides good channel separation performance in a typical massive MIMO system.

Index Terms—Massive MIMO, pilot spoofing attack, blind channel separation.

I. INTRODUCTION

Massive multiple-input multiple-output (MMIMO) systems [1], [2] exhibit excellent potentials for opposing passive eavesdropping attacks by using physical-layer security techniques [3]. Most of these physical-layer security techniques however rely on knowledge of channel state information (CSI), which is commonly estimated in the training phase of a MMIMO system. It is well known that MMIMO is vulnerable to active pilot spoofing attacks that aim to disturb the CSI estimation process [4]. This spoofing-attack vulnerability presents a weak spot for implementing physical-layer security techniques in MMIMO.

Signal processing methods have been recently proposed to counter pilot spoofing attacks in MMIMO systems. In particular, Refs. [4]–[13] propose attack detection methods that determine whether a pilot spoofing attack is conducted or not. Among these works, in [5] and [6], the BS performs attack detection by comparing the statistical properties of its observations with partial CSI known \textit{a priori}. The proposed methods of [7]–[10] make the legitimate user send random pilot symbols to the BS. The randomness of the pilot symbols reduces the effect of pilot contamination, and allows the BS to detect the attack by determining the number of sources from which its observations come. With slighty difference, refs. [11] and [12] utilizes the randomness of data. Refs. [13] and [4] give detection methods performed by the legitimate user.

On the other hand, there are also efforts focusing on estimating the channels of the legitimate and malicious users [14]–[18]. The proposed methods all utilize different forms of asymmetry between the legitimate and malicious users. In [14] and [15], the BS could communicate with the legitimate user via a aided channel that the malicious user cannot access. In [16]–[18], the BS firstly uses independent component analysis (ICA) for separating channels, and then employ asymmetry to match these separated channels with users. To be more specific, in [16], it is assumed that some partial CSI (e.g., the path loss values) is known to the BS \textit{a priori}, and that the \textit{a priori} partial CSI of the legitimate user is different from that of the malicious user. The BS identifies channels by using the CSI difference. In [17] and [18], the asymmetry is based on the restriction that the legitimate user can send encrypted information to the BS while the malicious user cannot do that. We notice that for enabling the ICA separation method, the malicious user is assumed to send information following certain statistical distribution that is known to the BS and independent with symbols of legitimate user [16]–[18]. This assumption may not always true in practical scenarios.

Against this background, we focus on separating the channel directions from the BS to the legitimate user and the malicious user upon positive detection of such attacks has been made. In specific, we consider attack scenario in which:

1) No partial CSI is available to the BS \textit{a priori}. Both the legitimate and malicious user channels are totally unknown to the BS.

2) The malicious user is free to impersonate the legitimate user. For instance, the malicious user may overhear the symbols sent by the legitimate user, and sends symbols according to its overheard signals. The employed distribution is unknown to the BS.

With channel direction separation, the BS can separately beamform to the legitimate user and the malicious user, and further employ some asymmetry configurations (e.g., higher layer authentication protocols) to distinguish between them.

We propose a blind channel separation algorithm in which the BS quantizes its observations, and obtains the empirical distribution of quantized observations for channel separation. We observe that this empirical distribution is determined by the channel directions and the distribution of the data symbols. As such, the channel directions can be extracted from the empirical distribution observed by the BS, and hence achieving...
channel separation. In addition, the proposed algorithm is based on FFT, making it easy to be implemented in practice.

II. SYSTEM MODEL

Assuming that pilot spoofing attack detection has been performed to validate the existence of a malicious user, we consider the system model depicted in Fig. 1. The BS is equipped with $M$ antennas, while the legitimate and malicious users have a single antenna each. The uplink and the corresponding downlink channels satisfy reciprocity. We assume that the channel separation process is performed within the coherent time of the channels, and use the $M \times 1$ vectors $h$ and $g$ to specify the channels from the legitimate user and malicious user to the BS, respectively. In the uplink, the legitimate and malicious users send random symbols $A$ and $B$ at power $P_1$ and $P_2$ to the BS, respectively. We use $P_A$ and $P_B$ for denoting the stochastic distributions of random symbols $A$ and $B$ over finite alphabets $A$ and $B$, respectively. For arbitrary $a \in A$ and $b \in B$, we assume the joint distribution of $A$ and $B$ satisfies $P_{A,B}(a,b) > 0$ whenever $P_A(a) > 0$ and $P_B(b) > 0$. This assumption indicates $A$ and $B$ are independent with each other, but $B$ cannot be definitely determined by $A$. In practical, it corresponds to a fact that the malicious user sends $B$ according to its observed version of $A$. Nevertheless, the malicious user cannot get $A$ exactly due to the channel fading and noise.

The received symbol of the BS is specified by
\[ y = \sqrt{P_i}h_iA_i + \sqrt{P_i}g_iB_i + w_i, \]
where $w$ is the noise vector, whose elements are i.i.d. circular-symmetric complex Gaussian (CSCG) random variables with zero mean and variance $\sigma^2$. Whenever needed, we use $\beta_1$ and $\beta_2$ for denoting the path losses of channels from the legitimate and malicious users to the BS, respectively. The BS does not know $\beta_1$, $\beta_2$, $P_1$, $P_2$, $h$, $g$ and $P_{12}$ a priori.

Assuming the uplink channel described by (1) is used $n$ times, within the coherent time of the channel, for the $i$th instant of use, (1) gives rise to
\[ y_i = \sqrt{P_i}h_iA_i + \sqrt{P_i}g_iB_i + w_i, \]
for $i = 1, 2, \ldots, n$. Stacking the $n$ equations in (2) into a matrix form, we obtain
\[ Y = [h, g] \begin{bmatrix} A \sqrt{P_1} \\ B \sqrt{P_2} \end{bmatrix} + W \]
where $Y = [y_1, y_2, \ldots, y_n]$, $W = [w_1, w_2, \ldots, w_n]$, $A = [A_1, A_2, \ldots, A_n]$, and $B = [B_1, B_2, \ldots, B_n]$. Let $S$ be the $M \times 2$ signal subspace matrix whose columns form an orthonormal basis that spans the column space of $[h, g]$. Then, we project $Y$ onto the signal subspace and get from (3)
\[ Z = \frac{1}{\sqrt{M}}S^TY = [z_1', z_2'] \begin{bmatrix} A \sqrt{P_1} \\ B \sqrt{P_2} \end{bmatrix} + N \]
where $[z_1', z_2'] = \frac{1}{\sqrt{M}}S^T[h, g]$, $N = \frac{1}{\sqrt{M}}S^TW$, and the elements of $N$ are i.i.d. Gaussian random variables with zero mean and variance $\frac{\sigma^2}{M}$. Clearly, $N$ is independent of $[z_1', z_2']$. It is argued in [19] that this independence and the Gaussianity of $N$ imply that
\[ [h, g] = \sqrt{MS}[z_1', z_2'] \]
would be a reasonable estimator for the channel pair $[h, g]$ if $[z_1', z_2']$ could be found. In practice $S$ is not known a priori, but can be estimated from the singular value decomposition $Y = U \Sigma V^T$ with orthogonal matrices $U \in \mathbb{R}^{M \times M}$, $V \in \mathbb{R}^{n \times n}$ and $M \times n$ diagonal singular value matrix $\Sigma$. Then $S$ can well approximated by the first two left singular vectors in $U$ when $M$ is large in the MIMO system [19].

Since $A$ and $B$ may have the same distribution, $[z_1', z_2']$ cannot be uniquely determined by $Y$ without knowledge of $\beta_1$, $\beta_2$, $P_1$, $P_2$, $A$, and $B$. As will be argued in the next section, it is however possible to estimate $[h, g]$ via (5), up to a permutation between the two columns and up to a phase ambiguity on each column. As a result, we will be able to separate the beamforming directions from the BS to the legitimate and malicious users based on channel reciprocity.

III. BLIND CHANNEL DIRECTION SEPARATION

First, with our assumption on $P_{A,B}$, the columns of $[z_1', z_2']$ are $2 \times 1$ random vectors that range over the alphabet $Z = \{ az_1' + bz_2' : a \in A, b \in B \}$.

The main idea of our channel separation scheme is to use $Z$ to obtain $[z_1', z_2']$ up to a column permutation, and then achieve the desired separation of channel directions via (5).

To explain how we may obtain $[z_1', z_2']$ from $Z$, let us start by considering an example where both the legitimate and malicious users send BPSK symbols. That is,
\[ Z = \begin{bmatrix} z_1' + z_2', -z_1' + z_2', z_1' - z_2', -z_1' - z_2' \end{bmatrix}^{\top} \]
\[ v_A \ v_B \ v_C \ v_D \]
It is clear that
\[ v_A - v_B = 2z_1', \quad v_C - v_D = 2z_2' \]
This indicates that every point in $Z$ is connected to another point in $Z$ by a line segment along the direction of $z_1'$. Fig. 2 denotes this observation geometrically. We will refer to this property as $z_1'$ covers $Z$. Similarly, it is easy to see that $v_A - v_C = 2z_2'$, $v_B - v_D = 2z_1'$, and hence $z_2'$ also covers $Z$. On
the other hand, we have that only \( v_A - v_D = 2z'_1 + 2z'_2 \) and \( v_B - v_C = 2z'_2 - 2z'_1 \). Thus, \( z'_1 + z'_2 \) covers only \( v_A \) and \( v_D \), \( z'_2 - z'_1 \) covers only \( v_B \) and \( v_C \). Neither \( z'_1 + z'_2 \) nor \( z'_2 - z'_1 \) covers \( Z \). Note that the above cases exhaust the differences between all pairs of points in \( Z \). In summary, among all the pairwise differences, \( z'_1 \) and \( z'_2 \) cover \( Z \), but \( z'_1 + z'_2 \) and \( z'_2 - z'_1 \) do not. As a result, we may obtain \( z'_1 \) and \( z'_2 \) from \( Z \) by finding out all pairwise differences that cover \( Z \). It turns out that this observation extends to the general case as summarized in the proposition below:

**Proposition 1.** Consider the general alphabet

\[
Z = \{az'_1 + bz'_2 : a \in \mathcal{A}, b \in \mathcal{B}\}
\]

where \( \mathcal{A} \) and \( \mathcal{B} \) are finite and with cardinalities at least 2. Each vector in \( \{\exp \{i\theta_1\} z'_1, \exp \{i\theta_2\} z'_2\} \) cover more points of \( Z \) than vector of the form \( c_1 z'_1 + c_2 z'_2 \) where \( c_1 \) and \( c_2 \) are both nonzero, \( \theta_1 \) and \( \theta_2 \) characterize the phase ambiguity.

Proposition 1 allows us to obtain \( [z'_1, z'_2] \) by finding two pairwise differences of vectors in \( Z \) that cover most points of \( Z \). We will give a practical algorithm to do so later. With Proposition 1, the problem of channel separation now reduces to that of estimating the alphabet \( Z \) from the observation \( Y \).

Towards that end, further notice that the columns of \( n \) random vectors that have the same distribution of the \( 2 \times 1 \) random vector \( n \), whose elements are two independent Gaussian random variables with zero mean and variance \( \frac{1}{2} \). If the columns of \( [z'_1, z'_2] \)

\[
\begin{bmatrix}
A \sqrt{T_1} \\
B \sqrt{T_2}
\end{bmatrix}
\]

are i.i.d. random vectors that have the same distribution as the generic \( 2 \times 1 \) random vector \( z' \), then the columns of \( Z \), given in (4), are i.i.d. random vectors that have the same distribution as that of \( z = z' + n \). Let \( F_z \), \( F_{z'} \), and \( F_n \) denote the distributions of \( z \), \( z' \), and \( n \), respectively. Then, because \( z' \) and \( n \) are independent, we have

\[
\Phi_{F_z}(\omega) = \Phi_{F_{z'}}(\omega) \cdot \Phi_{F_n}(\omega),
\]

where \( \Phi_{F}(\omega) \) denotes the characteristic function of the distribution \( F \), and \( \omega = [\omega_1, \omega_2]^T \) is the \( 2 \times 1 \) frequency vector. Note that the noise variance parameter \( \sigma^2 \) is a characteristic of the receiver circuitry and can be measured a priori. We may assume that its value is known, and thus

\[
\Phi_{F_n}(\omega) = \exp \left\{ -\frac{\sigma^2}{2M} |\omega|^2 \right\}
\]

is also known. On the other hand, \( F_z \) can be approximated by the empirical distribution of \( Z \) obtained directly from the observation \( Y \) as in (4). Hence the distribution \( F_{z'} \) of \( z' \) can be estimated using (6).

For ease of discussion, let us use \( z \) to denote a generic column in the matrix \( Z \). To estimate \( F_z \) efficiently, we quantize \( z = [z_1, z_2]^T \) and use Fast Fourier Transform (FFT) to obtain the characteristic function of the quantized version of \( z \) as described as follows. Consider \( m \) quantization levels \( \bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m \), and the corresponding quantization intervals \( B(\bar{u}_1), B(\bar{u}_2), \ldots, B(\bar{u}_m) \):

\[
-\alpha = \bar{u}_1 < \bar{u}_2 < \bar{u}_3 < \cdots < \bar{u}_{m-1} = \alpha < \bar{u}_m.
\]

\[
B(\bar{u}_j) = \begin{cases}
(\infty, \bar{u}_1], & j = 1 \\
(\bar{u}_{j-1}, \bar{u}_j], & j = 2, 3, \ldots, m-1 \\
[\bar{u}_m, \infty), & j = m
\end{cases}
\]

where \( \bar{u}_j - \bar{u}_{j-1} = \Delta \) for \( j = 2, 3, \ldots, m \). The elements \( z_1 \) and \( z_2 \) are respectively quantized to \( \bar{z}_1 \) and \( \bar{z}_2 \) according to:

\[
\bar{z}_1 = \sum_{j=1}^{m} \bar{u}_1 1(\{z_1 \in B(\bar{u}_j)\}) + \sum_{j=1}^{m} \bar{u}_1 1(\{z_2 \in B(\bar{u}_j)\})
\]

\[
\bar{z}_2 = \sum_{j=1}^{m} \bar{u}_1 1(\{z_2 \in B(\bar{u}_j)\}) + \sum_{j=1}^{m} \bar{u}_1 1(\{z_2 \in B(\bar{u}_j)\})
\]

where \( 1(\cdot) \) denotes the indicator function, \( \Re \{\cdot\} \) and \( \Im \{\cdot\} \) takes the real part and imaginary part of its input, respectively.

The quantized version of \( z \) is then \( \bar{z} = [\bar{z}_1, \bar{z}_2]^T \). Write \( \bar{U} = \{\bar{u}_1 + i\bar{u}_1, \bar{u}_1 + i\bar{u}_2, \ldots, \bar{u}_m + i\bar{u}_m\} \). Then the alphabet of \( \bar{z} \) is \( U' \). We will denote it and enumerate its elements as \( \bar{Z} = \{\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m\} \).

Let \( \bar{Z} = [\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_n] \), where the \( i \)th column \( \bar{z}_i \) is the quantized version of the \( i \)th column of \( Z \). Next, obtain the pmf of the columns of \( Z \) as

\[
\Delta F_{\bar{z}}(\bar{u}_j) = \frac{1}{n} \sum_{i=1}^{n} 1(\bar{z}_i = \bar{u}_j)
\]

for \( j = 1, 2, \ldots, m^4 \). Thus, the characteristic function of the empirical distribution \( \Delta F_{\bar{z}} \) is

\[
\Phi_{\Delta F_{\bar{z}}}(\omega) = \sum_{j=1}^{m^4} \Delta F_{\bar{z}}(\bar{u}_j) \exp \{-i\bar{u}_j^T \omega\}.
\]

Similarly, let \( \bar{Z}' = [\bar{z}'_1, \bar{z}'_2, \ldots, \bar{z}'_n] \), where the \( j \)th column \( \bar{z}_j' \) is the quantized version of the \( j \)th column of \( [z'_1, z'_2] \)

\[
\begin{bmatrix}
A \sqrt{T_1} \\
B \sqrt{T_2}
\end{bmatrix}
\]

. To do this quantization step, we employ quantization alphabet \( \bar{Z}' = \{\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m\} \). Then, the empirical pmf of the columns of \( \bar{Z}' \) is

\[
\Delta F_{\bar{z}'}(\bar{u}_j) = \frac{1}{n} \sum_{i=1}^{n} 1(\bar{z}'_i = \bar{u}_j)
\]

for \( j = 1, 2, \ldots, m^4 \).
Using $\Phi_{\Delta F'_k}(\omega)$ in place of $\Phi_{F'_k}(\omega)$ and $\Delta F'_k$ in place of $F'_k$ in (6), we obtain the estimator

$$
\hat{\Delta F'_k} = \Phi^{-1} \left( \frac{\Phi_{\Delta F'_k}(\omega)}{\Phi_{F'_k}(\omega)} \right)
$$

(10)

for $\Delta F'_k$, where $\Phi^{-1}$ denotes the inverse Fourier Transform with respect to (8). Note that the forward and inverse Fourier Transforms in (10) can be efficiently implemented using FFT and inverse FFT, respectively.

Remark 1 The asymptotic accuracy of this estimator is guaranteed by the law of large number (LLN). Intuitively, as $n \to \infty$, $\alpha \to \infty$, $\Delta F'_k$ and $\Delta F'_k$ respectively converges to $F'_k$ and $F'_k$ in probability according to LLN. Notice that $\Phi(-)$ and $\Phi^{-1}(-)$ are orthogonal transformations, which are able to keep the convergence of its input. We would obtain that $\hat{\Delta F'_k}$ converges to $F'_k$ and $F'_k$.

On the other hand, it is observed that partitions $D$ and $D$ correspond to the LDPRs given by (11) over the random variables with symbol alphabets of the legitimate and malicious users, and imposes no restrict on statistic dependence between symbols of the legitimate and malicious users.

IV. PERFORMANCE EVALUATION

In this section, we present some simulation results to evaluate the performance of the proposed blind channel separation (BCS) scheme. We start by describing the metric that we employ to measure the channel separation performance.

Suppose that $d$ is an uplink channel direction vector obtained by some channel estimation algorithm. By reciprocity, downlink beamforming is performed based on $d$. Then the leakage-to-direct power ratio (LDPR) $\frac{\|d\|^2}{\|d\|^2}$ measures the ratio of the power leaked to the malicious user to the power directed towards the legitimate user if $d$ is employed to perform beamforming. Clearly, $\frac{\|d\|^2}{\|d\|^2}$ is the LDPR value when the channel direction estimation is perfect.

Now, let $[h_1, h_2]$ be the channel direction vectors estimated using the blind channel separation scheme described in Section III. Since we do not know whether $h_1$ or $h_2$ corresponds to $h$, we consider the minimum between the LDPRs of the two possibilities $^1$:

$$
\text{LDPR}(h, g) = \min \left\{ \frac{\|g\|^2}{\|g\|^2} \right\},
$$

(11)

Note that the LDPR in (11) is a function of the channel vectors $[h, g]$. In the simulation, we generate 10,000 instances of the channel vectors based on the block Rayleigh fading model. That is, the elements of $h$ and $g$ are chosen as i.i.d. CSCG random variables with 0 mean and variance 1. We then average the LDPRs given by (11) over the 10,000 channel instances.

In the simulation, we set $P_1 = P_2$. The legitimate user sends equally likely random BPSK symbols, i.e., $P_A(-1) =$

$^1$The channels could be identified by some asymmetry measures, which is beyond the scope of this paper due to space limitation. We indeed assume perfect channel identification herein.
achieved by perfect CSI. For the per-antenna SNR reaches 12 dB. In contrast, the LDPR close to perfect LDPR performance within 1dB when \( M = 128 \) versus the SNR in an MMIMO system with 128 antennas at the BS, respectively. Also plotted in the figure are the LDPR values obtained by ICA scheme and by using perfect CSI information, respectively.

For the MMIMO system with \( M = 64 \), we observe from the first subfigure of Fig. 3 that the proposed algorithm achieves LDPR close to perfect LDPR performance within 1dB when the per-antenna SNR reaches 12 dB. In contrast, the LDPR achieved by traditional ICA scheme is 3dB worse than that achieved by perfect CSI. For \( M = 128 \), we observe from the second subfigure of Fig. 3 that the proposed algorithm provides almost perfect LDPR performance when the per-antenna SNR reaches 4dB. Meanwhile, it outperforms ICA scheme up to 5dB. It indicates the proposed scheme is effective to separate channel directions when the malicious and legitimate symbols are dependent, and its distributions are unknown to the BS. Due to space limitation, we cannot present more results.

Fig. 3: Average LDPR obtained by the proposed blind channel separation algorithm in an MMIMO system respectively with 64 and 128 antennas at the BS.

The malicious user sends BPSK symbols according to \( P_{BI}(+1) = \frac{1}{2}, P_{BI}(-1) = \frac{1}{2} \). The case of 500 random BPSK symbols (\( n = 500 \)) is simulated. The proposed BCS scheme is performed according to Section III.A.

For the MMIMO system with \( M = 64 \), we observe from the first subfigure of Fig. 3 that the proposed algorithm achieves LDPR close to perfect LDPR performance within 1dB when the per-antenna SNR reaches 12 dB. In contrast, the LDPR achieved by traditional ICA scheme is 3dB worse than that achieved by perfect CSI. For \( M = 128 \), we observe from the second subfigure of Fig. 3 that the proposed algorithm provides almost perfect LDPR performance when the per-antenna SNR reaches 4dB. Meanwhile, it outperforms ICA scheme up to 5dB. It indicates the proposed scheme is effective to separate channel directions when the malicious and legitimate symbols are dependent, and its distributions are unknown to the BS. Due to space limitation, we cannot present more results.

V. CONCLUSIONS

We have proposed a blind channel direction separation algorithm to differentiate the channel directions from a legitimate user and a malicious user to the BS in the uplink of a massive MIMO system. With channel reciprocity, the BS then will be able to use the channel directions to beamform to the legitimate and malicious users separately and further verify their identities by use of higher layer authentication protocols.

Extensions of the proposed channel separation to the cases of multiple legitimate and malicious users are of interest.

REFERENCES