IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 13, 2020, accepted June 21, 2020, date of publication July 1, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006281

Detection of Pilot Contamination Attack for Frequency Selective Channels

AWAIS AHMED[1], (Student Member, IEEE), MUHAMMAD ZIA[1], (Member, IEEE), IHSAN UL HAQ[2], (Member, IEEE), AND HUY-DUNG HAN[3], (Member, IEEE)

[1]Department of Electronics, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Department of Electrical Engineering, International Islamic University, Islamabad, Islamabad 45320, Pakistan
[3]Faculty of Electronics and Telecommunications, Hanoi University of Science and Technology, Hanoi 10000, Vietnam

Corresponding author: Awais Ahmed (awaisahmed@ele.qau.edu.pk)

ABSTRACT Physical layer security (PLS) provides an additional protection layer to the conventional encryption in the presence of an active eavesdropper (Eve). The detection of pilot contamination attack (PCA) on legitimate nodes by the active Eve is vital in order to mitigate the effect of the attack. In this work, we propose a novel PCA detector for the nodes, which intend to establish secure communication in time division duplex (TDD) mode over a frequency selective channel. We devise binary hypothesis from the decision directed channel estimate for PCA detection by exploiting observations of pilot sequence and random data in pilot and data phases, respectively. We also provide performance analysis of the proposed method. The comparison of simulation results and analysis demonstrates the accuracy of the analysis. The proposed detector has low probability of detection error as compared to the existing high complexity sub-space based PCA detector.

INDEX TERMS Active eavesdropping, physical layer security, pilot contamination attack, PCA detection.

I. INTRODUCTION

Wireless communication networks are widely used in military and civilian applications and have become an integral part of our lives. The security of future wireless communication systems is a key concern due to the broadcast nature of wireless channel [1]–[3]. Traditionally, the security of a communication system is achieved by conventional encryption methods at application layer, which have well-known weaknesses [4], [5]. For instance, ciphers, which were considered unbreakable in the past are now vulnerable due to exponential growth of the computational power [4], [6]. In recent years, physical layer (PHY) security has emerged as an effective approach to provide additional security at the top of conventional encryption [4], [6], [7]. Physical layer security approaches exploit characteristics of wireless channel to prevent eavesdropping [8]. Seminal work in [9] introduces secrecy capacity for wiretap channel at PHY. Following the work in [9], extensive research has been conducted to ensure secure transmission using physical layer security, such as cooperative relaying [10]–[12], interference management [13]–[15] and artificial jamming [16]. The precoder design and impact of PCA on secrecy capacity of massive multiple input multiple output (MaMIMO) is investigated in [17]–[21]. Encryption using secret key generated from the randomness of reciprocal wireless channel is investigated in [22]–[28] and references therein to secure communication from passive Eve. Similarly, secret key generation at PHY in the presence of an active Eve is investigated in [29].

The PCA poses severe security threat to the legitimate nodes due to the fact that the transmission protocol, the pilot sequences and the frame structure of communication standards are known to the legitimate nodes and eavesdroppers. An active eavesdropper can impair the channel estimation process by sending the training sequence of the legitimate user under attack in the pilot phase [30], [31]. Thus, under PCA, the legitimate node acquires sum of the channels of the legitimate user and active Eve. The legitimate user can't separate the multi-path component of legitimate node from the sum of the two channels. Consequently, a precoder design steers partial beam towards active Eve [32]. Furthermore, as a result of PCA, the correlation between the channel estimates at legitimate nodes significantly decreases, which causes higher key disagreement between legitimate nodes [33], [34]. The PCA detection is vital to take proper measures to secure physical layer communication from eavesdropping.

The associate editor coordinating the review of this manuscript and approving it for publication was Hamed Ahmadi.

Work in [35] employs the signal power distribution for PCA detection without theoretical derivation of the decision threshold. In [35], the authors also propose PCA detection with the cooperation between the legitimate users under the assumption that Eve contaminates both the downlink and uplink transmissions. The signal power based PCA detection is thoroughly investigated in [36]. In [36], the authors proposed an energy ratio based PCA detector, which exploits the fact that an active eavesdropper introduces added power in the uplink phase. Consequently, the legitimate node loses significant portion of received power in the downlink phase due to precoder design from contaminated channel state information. However, the training symbols required in both the downlink and uplink transmission makes it more complex in practical situations. Another approach in [37] detects the presence of an active eavesdropper by exploiting the received power at the legitimate node under the assumption of the closed-loop power control. The method in [38] uses likelihood ratio test by exploiting the prior knowledge of both the channel and noise covariance. Another group of PCA detectors introduce additional randomness in the pilot phase. The additional randomness can neither be replicated nor predicted by an active eavesdropper [37], [39]–[41]. However, introduction of additional randomness degrades the channel estimation of other users in the wireless network due to loss of orthogonality of pilots. In [41], the authors introduced a PCA detector by using the modified PSK symbols in the training phase for channel estimation. The presence of an active eavesdropper can be detected by examining the phase difference between the selected PSK signals. However, the detection regions and performance of the proposed method is not optimal as discussed in [41]. A subspace-based method proposed in [37] improves the performance of random PSK symbols method. The motivation behind the subspace-based method is to exploit the ratio between the largest and the second largest eigen values of received covariance matrix in the pilot phase. The ratio is compared to a predefined threshold to detect the presence of PCA. However, work in [37] lacks the criterion to compute threshold of the detector.

Works in [40], [42]–[44] use minimum description length (MDL) method for source enumeration in pilot phase observations. The sub-space method in [40], [42]–[44] involves estimation of second-order statistics and computing the eigen values, which is computationally extensive. Furthermore, the transmission of random data in pilot phase impairs the channel estimate at the legitimate nodes due to interference from random data. The performance of sub-space approaches is poor in low signal-to-noise ratio (SNR) regimes [45].

Motivation of our work stems from the fact that existing PCA detection methods transmit additional waveform in the pilot phase for PCA detection [39], [41], [46]. Furthermore, modified pilot waveform impairs channel estimation and PCA detectors have high complexity [39]–[41]. We propose two low complexity novel PCA detectors to combat Eve without modifying pilot signal. We assume that Eve is passive in data phase, which is inline with assumption in [47]. In the first method, we formulate pilot assisted binary hypothesis (PABH) from the observations in pilot phase to detect the presence of the active Eve. The pilot phase is followed by the payload, which is random symbol sequence. The second method builds upon PABH, which exploits random data to formulate decision directed binary hypothesis (DDBH) for PCA detection. The proposed PABH provides coarse PCA detection, whereas DDBH achieves enhanced performance by combining observations of pilot and data phases. The proposed detectors have low complexity and do not impose any constraint on the training length contrary to sub-space based methods such as MDL [40], [42], [43].

In DDBH, we estimate channel of the legitimate node by using estimated data symbols as a reference signal. Then, we remove the signal of the legitimate user from the observation in the pilot phase. We use residual signal to estimate the channel of active Eve. Finally, we formulate binary hypotheses from the channel estimate of the active Eve for PCA detection.

The major contributions of this manuscript are:

- We present two novel low-complexity PCA detectors using the contaminated pilot observations and decision-directed channel estimate by exploiting random payload data. The proposed detectors are simple and do not require additional feedback as compared to the existing works in [41] and [36], respectively.
- We present analysis of impact of bit error rate on the decision directed channel estimation using normalized mean square error (NMSE) as a performance metric.
- We provide performance analysis of the probability of error P_E and complexity of the proposed PCA detectors. The comparison of analytical and simulation results verifies the accuracy of the analysis. The simulation results demonstrate that the proposed methods achieve low probability of detection error and low NMSE of the channel estimation of legitimate user.
- We also compare performance of the proposed method with self-contamination based MDL method [43].

The rest of the manuscript is organized as follows. In Section II, we introduce the system model for PCA. Section III formulates our problem to illustrate the issue of PCA. In Section IV, we present performance analysis of the proposed PABH and DDBH detectors and discuss the complexity of the proposed methods in Section V. Next, we present simulations in Section VI in order to provide the efficiency of our proposed PCA detectors before concluding in Section VII.

Notations: Boldface upper-case and lower-case letters denote matrices and vectors, respectively. For any matrix $\mathbf{A}$, we use $\mathbf{A}^H$, $\mathbf{A}^T$ and $\mathbf{A}^\dagger$ to denote its Hermitian, transpose and Penrose-Moore pseudo-inverse, respectively. $\mathbf{I}_N$ denotes $N \times N$ identity matrix while $\mathbf{E}\{\mathbf{A}\}$ stands for the expectation operator of $\mathbf{A}$. Tr($\mathbf{A}$) represents the trace of matrix $\mathbf{A}$.

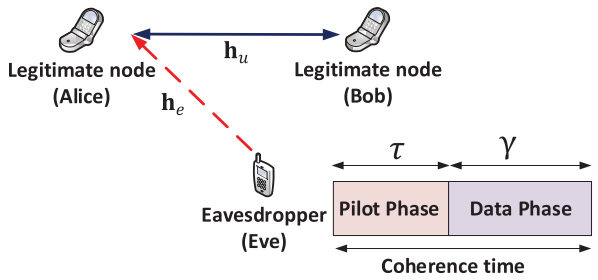

FIGURE 1. System model of pilot contamination attack for frequency selective channels.

II. SYSTEM MODEL

In this work, we consider a typical three node communication system over a frequency selective channel under OFDM signaling as shown in Fig. 1. The legitimate nodes Alice and Bob establish secure communication and an active eavesdropper (Eve) intends to decode private messages of Alice and Bob. Each node in the communication link is equipped with single antenna. Both legitimate nodes communicate in TDD manner by exploiting the property of channel reciprocity. The L-path wireless channel from Bob to Alice $\mathbf{h}_u = \sqrt{\beta_u}\,\tilde{\mathbf{h}}_u \in \mathcal{C}^{L\times 1}$ and Eve to Alice $\mathbf{h}_e = \sqrt{\beta_e}\,\tilde{\mathbf{h}}_e \in \mathcal{C}^{L\times 1}$ are uncorrelated if they are separated by more than half a carrier wavelength $\frac{\lambda}{2}$ [48], where β_u and β_e represent the large scale fading coefficients for shadowing and path loss [49]. The elements of small-scale fading coefficients vectors $\tilde{\mathbf{h}}_e$ and $\tilde{\mathbf{h}}_u$ are independent and identically distributed (i.i.d) with zero mean and variance $\frac{1}{L}$.

An OFDM waveform with N_s subcarriers converts single frequency selective channel into N_s parallel sub-channels [50], [51]. The legitimate node (Bob) transmits pilot sequence to Alice for channel estimation in pilot phase. Alice exploits channel reciprocity and designs precoder using channel estimate to focus data transmission towards Bob. The pilot sequence sent by Bob to Alice is publicly known and an active Eve contaminates pilot phase observations of Alice by transmitting the pilot sequence of Bob to Alice in order to impair channel estimation and alter precoder design. As a direct consequence of PCA, Alice estimates the sum $\mathbf{H}_u+\mathbf{H}_e$, where $\mathbf{H}_u = \mathbf{F}\mathbf{h}_u$, $\mathbf{H}_e = \mathbf{F}\mathbf{h}_e$, and $\mathbf{F} \in \mathcal{C}^{N_s\times N_s}$ is Fast Fourier Transform (FFT) matrix. The precoder design from the estimate of the sum $\mathbf{H}_u + \mathbf{H}_e$ alters the beam in data phase from Alice to Bob. Thus, private information leaks towards Eve. The PCA detection, which is helpful to mitigate the impact of PCA, is imperative to achieve secure communication. In the next section, we present the proposed PCA detection method.

III. PROBLEM FORMULATION

In this section, we present low-complexity PABH and DDBH PCA detectors for the detection of attack by an active Eve. In the pilot phase, Bob transmits training sequence to Alice and Alice acquires CSI to design precoder to transmit secure data from Alice to Bob. The matrix model of the received signal $\mathbf{Y}_p$ in frequency domain is

$$\mathbf{Y}_p = \sqrt{P_n}\,\mathbf{H}_u\mathbf{x}_p^T + I_e\sqrt{P_e}\,\mathbf{H}_e\mathbf{x}_p^T + \mathbf{W}_p, \tag{1}$$

where $\mathbf{x}_p \in \mathcal{C}^{\tau\times 1}$ is the training sequence, $I_e \in \{0,1\}$ is an indicator function, $\mathbf{W}_p \in \mathcal{C}^{N_s\times\tau}$ is the AWGN matrix with elements having zero mean and variance σ^2. Note that P_n and P_e are the powers of Bob and Eve, respectively. The energy of the pilot sequence $\|\mathbf{x}_p\|^2 = \tau$ is the ℓ_2-norm of the pilot sequence $\mathbf{x}_p$ of length τ. The binary hypotheses $\mathcal{H}_0$ (Eve is not active) and $\mathcal{H}_1$ (Eve is active) using pilot phase least square (LS) channel estimate $\widehat{\mathbf{H}}_u^p$ from Bob to Alice is

$$\begin{aligned}
\mathcal{H}_0 : \widehat{\mathbf{H}}_u^p &= \mathbf{Y}_p\frac{\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2} = \sqrt{P_n}\,\mathbf{H}_u\mathbf{x}_p^T\frac{\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2} + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2}\\
&= \sqrt{P_n}\,\mathbf{H}_u + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\tau}.\\
\mathcal{H}_1 : \widehat{\mathbf{H}}_u^p &= \mathbf{Y}_p\frac{\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2} = \sqrt{P_n}\,\mathbf{H}_u\mathbf{x}_p^T\frac{\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2}\\
&\quad + \sqrt{P_e}\,\mathbf{H}_e\frac{\mathbf{x}_p^T\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2} + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\|\mathbf{x}_p\|^2}\\
&= \sqrt{P_n}\,\mathbf{H}_u + \sqrt{P_e}\,\mathbf{H}_e + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\tau}.
\end{aligned} \tag{2}$$

Notice that the channel estimate under $\mathcal{H}_0$ consists of modified noise and legitimate channel. Whereas, under $\mathcal{H}_1$, observation consists of one more term, which is Eve's channel. In addition, the major interference signal under $\mathcal{H}_1$ is the contaminated pilot signal from Eve instead of the error in channel estimation due to noise.

OFDM transforms L-path frequency selective channel into N_s flat-fading channels. Thus, in frequency domain, each path-gain has zero mean and variance $\sigma_H^2 = \frac{\beta_u}{N_s}$. Therefore, distributions of $\widehat{\mathbf{H}}_u^p$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are $\widehat{\mathbf{H}}_u^p|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_n\beta_u}{N_s} + \frac{\sigma^2}{N_s\tau})\mathbf{I}_{N_s}\right)$ and $\widehat{\mathbf{H}}_u^p|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_n\beta_u}{N_s} + \frac{P_e\beta_e}{N_s} + \frac{\sigma^2}{N_s\tau})\mathbf{I}_{N_s}\right)$, respectively. Furthermore, time domain channel estimate can be obtained by applying inverse FFT (IFFT) operation $\mathbf{F}^H$ on the frequency domain channel estimate $\widehat{\mathbf{H}}_u^p$ as $\widehat{\mathbf{h}}_u^p = \mathbf{F}^H\widehat{\mathbf{H}}_u^p$. The time domain channel $\mathbf{h}_u^p$ has L flat-fading paths, where gains are i.i.d. with Gaussian distribution of zero mean and variance $\sigma_h^2 = \frac{\beta_u}{L}$. Thus, distributions of $\widehat{\mathbf{h}}_u^p$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are $\widehat{\mathbf{h}}_u^p|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_n\beta_u}{L} + \frac{\sigma^2}{L\tau})\mathbf{I}_L\right)$ and $\widehat{\mathbf{h}}_u^p|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_n\beta_u}{L} + \frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau})\mathbf{I}_L\right)$, respectively. In PABH detector, we formulate binary hypothesis using channel estimate $\widehat{\mathbf{h}}_u^p$ from Bob to Alice. Next, we present binary hypotheses for data-aided PCA detection. In data-aided PCA detection phase, we use pilot assisted channel estimate to decode data.

The pilot phase is followed by payload data in data phase from Bob to Alice and Eve remains silent in the payload data phase. The assumption that Eve remains silent in the payload data phase is inline with [47]. The motivation behind PCA stems from the fact that an active Eve contaminates the channel estimate of legitimate node to steer valuable

information towards the eavesdropper. The best strategy for Eve is to remain silent during the data phase as transmission of random jamming symbols in data phase also increases self-interference at the eavesdropper. The self-interference degrades the signal to interference plus noise ratio (SINR) resulting in lower information rate of Eve. In addition, the probability of Eve detection significantly increases when Eve remains active in the data phase [52]. Since channels from Bob to Alice and Eve to Alice are independent, contaminated channel estimate $\widehat{\mathbf{H}}_u^p$ in pilot phase can decode payload data. We use decoded data as reference to further improve pilot phase channel estimate $\widehat{\mathbf{H}}_u^p$ from Bob to Alice. The matrix model of the received signal $\mathbf{Y}_d$ of Alice in data phase is

$$\mathbf{Y}_d = \sqrt{P_n}\,\mathbf{H}_u\mathbf{x}_d^T + \mathbf{W}_d, \tag{3}$$

where $\mathbf{x}_d \in \mathcal{C}^{\gamma\times 1}$ is the random data sequence and $\mathbf{W}_d \in \mathcal{C}^{N_s\times\gamma}$ is AWGN matrix with mean zero and covariance matrix $\sigma^2\mathrm{I}$. The coherent estimate of data vector $\mathbf{x}_d$ using pilot phase channel estimate is

$$\widehat{\mathbf{x}}_d^T = \left(\widehat{\mathbf{H}}_u^p\right)^\dagger \mathbf{Y}_d = \alpha\left(\sqrt{P_n}\,\mathbf{H}_u + \sqrt{P_e}\,\mathbf{H}_e + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\tau}\right)^H \left(\sqrt{P_n}\,\mathbf{H}_u\mathbf{x}_d^T + \mathbf{W}_d\right) = \alpha P_n\|\mathbf{H}_u\|^2\mathbf{x}_d^T + \widetilde{\mathbf{w}}_d, \tag{4}$$

where

$$\widetilde{\mathbf{w}}_d = \alpha\sqrt{P_nP_e}\mathbf{H}_e^H\mathbf{H}_u\mathbf{x}_d^T + \frac{\alpha\sqrt{P_n}}{\tau}\mathbf{x}_p^T\mathbf{W}_p^H\mathbf{H}_u\mathbf{x}_d^T + \alpha\sqrt{P_n}\mathbf{H}_u^H\mathbf{W}_d + \alpha\sqrt{P_e}\mathbf{H}_e^H\mathbf{W}_d + \frac{\alpha}{\tau}\mathbf{x}_p^T\mathbf{W}_p^H\mathbf{W}_d \tag{5}$$

and $\alpha = \|\sqrt{P_n}\,\mathbf{H}_u + \sqrt{P_e}\,\mathbf{H}_e + \frac{\mathbf{W}_p\mathbf{x}_p^*}{\tau}\|^{-2}$. Due to central limit theorem, $\widetilde{\mathbf{w}}_d \in \mathcal{C}^{\gamma\times 1}$ is AWGN matrix with mean zero and covariance matrix $\tilde{\sigma}_d^2\mathrm{I}_\gamma$. The estimate $\widehat{\mathbf{x}}_d$ of data symbols is reliable due to poor correlation between $\mathbf{H}_u$ and $\mathbf{H}_e$ ($\epsilon = \mathbf{H}_u^H\mathbf{H}_e$). We use hard decision $\tilde{\mathbf{x}}_d = \mathrm{dec}(\widehat{\mathbf{x}}_d)$ as reference to estimate $\mathbf{H}_u$ in data phase. In moderate and high SNR regimes, $\tilde{\mathbf{x}}_d = \mathbf{x}_d$. Thus, decision directed LS estimate of $\mathbf{H}_u$ is

$$\widehat{\mathbf{H}}_u^d = \frac{\mathbf{Y}_d\,\tilde{\mathbf{x}}_d}{\gamma} = \sqrt{P_n}\,\mathbf{H}_u + \frac{\mathbf{W}_d\,\tilde{\mathbf{x}}_d}{\gamma}. \tag{6}$$

The estimate of the signal from Bob to Alice in pilot phase observation in (1) is

$$\widehat{\mathbf{Y}}_{pu} = \widehat{\mathbf{H}}_u^d\,\mathbf{x}_p^T = \left(\sqrt{P_n}\,\mathbf{H}_u + \frac{\mathbf{W}_d\,\tilde{\mathbf{x}}_d}{\gamma}\right)\mathbf{x}_p^T. \tag{7}$$

We can estimate the contribution of Eve to the observation of Alice in pilot phase by subtracting the estimate of Bob $\widehat{\mathbf{Y}}_{pu}$ from (1) as follows:

$$\widehat{\mathbf{Y}}_{pe} = \sqrt{P_e}\,I_e\mathbf{H}_e\mathbf{x}_p^T + \mathbf{W}_p + \frac{\mathbf{W}_d\tilde{\mathbf{x}}_d\mathbf{x}_p^T}{\gamma}. \tag{8}$$

We assume that in moderate and high SNR regime, $\tilde{\mathbf{x}}_d = \mathbf{x}_d$. Then, the binary hypothesis from the LS estimate of the Eve's channel using residue signal $\widehat{\mathbf{Y}}_{pe}$ is

$$\mathcal{H}_0 : \widehat{\mathbf{H}}_e^d = \widehat{\mathbf{Y}}_{pe}\frac{\mathbf{x}_p}{\|\mathbf{x}_p\|^2} = \frac{\mathbf{W}_p\mathbf{x}_p}{\tau} + \frac{\mathbf{W}_d\mathbf{x}_d}{\gamma},$$

$$\mathcal{H}_1 : \widehat{\mathbf{H}}_e^d = \widehat{\mathbf{Y}}_{pe}\frac{\mathbf{x}_p}{\|\mathbf{x}_p\|^2} = \sqrt{P_e}\,\mathbf{H}_e + \frac{\mathbf{W}_p\mathbf{x}_p}{\tau} + \frac{\mathbf{W}_d\mathbf{x}_d}{\gamma}. \tag{9}$$

The distribution of $\widehat{\mathbf{H}}_e^d$ under hypothesis $\mathcal{H}_0$ is $\widehat{\mathbf{H}}_e^d|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{\sigma^2}{N_s\tau} + \frac{\sigma^2}{N_s\gamma})\mathbf{I}_{N_s}\right)$. Similarly, the distribution of Eve's channel estimate $\widehat{\mathbf{H}}_e^d$ under hypothesis $\mathcal{H}_1$ is $\widehat{\mathbf{H}}_e^d|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_e\beta_e}{N_s} + \frac{\sigma^2}{N_s\tau} + \frac{\sigma^2}{N_s\gamma})\mathbf{I}_{N_s}\right)$. Note that under $\mathcal{H}_0$, the estimate of Eve's channel consists of noise terms (Eve's channel estimation error), which is function of noise variance, training length τ in pilot phase and payload data length γ in data phase used for channel estimation of LU. Note that under $\mathcal{H}_1$ in (9), the Eve's channel estimate has significant term, which corresponds to Eve's channel $\mathbf{H}_e$. The distributions of time domain channel estimate $\widehat{\mathbf{h}}_e^d$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ for DDBH are $\widehat{\mathbf{h}}_e^d|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma})\mathbf{I}_L\right)$ and $\widehat{\mathbf{h}}_e^d|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma})\mathbf{I}_L\right)$, respectively.

A. IMPACT OF CHANNEL LENGTH

Now, we evaluate the variance $\tilde{\sigma}_d^2$ of the elements of effective noise $\widetilde{\mathbf{w}}_d$, which affects data decoding (bit errors) and channel estimation error. The elements of channel vectors $\mathbf{H}_u$ and $\mathbf{H}_e$ are independent and identically distributed with mean zero and variance $\frac{1}{L}$. The correlation term $\mathbf{H}_e^H\mathbf{H}_u = \sum_i^L \mathbf{H}_e^*(i)\mathbf{H}_u(i)$ in $\widetilde{\mathbf{w}}_d$ is a random variable, which is the sum of L random variables. Note that $\mathbf{H}_e^*(i)\mathbf{H}_u(i)$ has zero mean and variance $\frac{1}{L^2}$. Due to central limit theorem, the distribution of correlation $\mathbf{H}_e^H\mathbf{H}_u$ converges to normal distribution with mean zero and variance $\frac{1}{L}$. For two point constellation, only real part of correlation affects the bit errors. Thus, variance of real component is $\mathcal{R}\{\mathbf{H}_e^H\mathbf{H}_u\} = \frac{1}{2L}$. The elements of $\mathbf{W}_p$ are also i.i.d. with zero mean and variance $\frac{\sigma^2}{L}$. The product vector $\mathbf{W}_p^H\mathbf{H}_u \in C^{\tau\times 1}$ is vector of i.i.d. random variable of mean zero and variance $\frac{\sigma^2}{L}$ each. Thus, random variable $\frac{1}{\tau}\mathbf{x}_p^T\mathbf{W}_p^H\mathbf{H}_u$ has mean zero and variance $\frac{\sigma^2}{\tau L}$. The variance of real component $\mathcal{R}\{\frac{1}{\tau}\mathbf{x}_p^T\mathbf{W}_p^H\mathbf{H}_u\}$ is $\frac{\sigma^2}{2\tau L}$. Due to central limit theorem, distribution of $\mathbf{H}_u^H\mathbf{W}_d$ and $\mathbf{H}_e^H\mathbf{W}_d$ also converges to normal distribution with mean zero and variance $\frac{\sigma^2}{2L}$. Furthermore, each element of vector of random variables $\frac{1}{\tau}.\mathbf{x}_p^T\mathbf{W}_p^H\mathbf{W}_d$ has normal distribution with zero mean and variance $\frac{\sigma^4}{2\tau L}$. Using variance of each term of $\widetilde{\mathbf{w}}_d$, the variance of each element of vector of random variables $\widetilde{\mathbf{w}}_d$ is

$$\tilde{\sigma}_d^2 = \frac{1}{2L} + \frac{\sigma^2}{2L} + \frac{\sigma^2}{2\tau L} + \frac{\sigma^2}{2L} + \frac{\sigma^4}{2\tau L} = \frac{1}{2L}\left(1 + 2\sigma^2 + \frac{\sigma^2}{\tau} + \frac{\sigma^4}{\tau}\right). \tag{10}$$

The variance $\tilde{\sigma}_d^2$ of the elements of effective noise vector $\widetilde{\mathbf{w}}_d$ is inversely proportional to the channel taps L. In high SNR regime, $\lim_{\sigma^2\to 0}\tilde{\sigma}_d^2 \to \frac{1}{2L}$ causes BER and NMSE floor. For large L, either due to muli-path components or large antennas, $\|\mathbf{H}_u\| \to 1$ and $\mathbf{H}_e^H\mathbf{H}_u \to 0$.

The following proposition describes the impact of the bit errors on the normalized mean square error (NMSE) of the user channel estimate.

Proposition 1: The NMSE of the decision directed least square channel estimate under probability of bit error p is

$$NMSE_\gamma = \sum_{k=0}^{\gamma} \left(\frac{4k^2}{\gamma^2} + \frac{\sigma^2}{\gamma}\right)\binom{\gamma}{k} p^k\,(1-p)^{\gamma-k}, \quad (11)$$

where γ is block size of the decoded bits $\tilde{\mathbf{x}}_d = dec(\widehat{\mathbf{x}}_d)$ used as reference for decision directed channel estimation.

Proof: The performance of decision-directed channel estimation depends on the number of errors in the decoded data $\tilde{\mathbf{x}}_d$ used as a reference to estimate user channel $\mathbf{H}_u$. We assume that each bit in the decoded data is independent from the other bits in the decoded block. In moderate SNR regime, probability of error is low and probability that all bits in the frame are erroneous is almost zero for large block size γ. Let p be probability of bit error. Thus, the probability of k errors $p_r(k)$ in γ independent bits using Bernoulli distribution is

$$p_r(k) = \binom{\gamma}{k} p^k (1-p)^{\gamma-k}, \quad k = 0, 1, \cdots \gamma, \quad (12)$$

where $\binom{\gamma}{k} = \frac{\gamma!}{k!(\gamma-k)!}$. The decision-directed LS channel estimate of legitimate user under bit error is

$$\widehat{\mathbf{H}}_u^d = \frac{\mathbf{Y}_d\,\tilde{\mathbf{x}}_d}{\gamma} = \frac{\sqrt{P_n}\,\mathbf{H}_u \mathbf{x}_d^T \tilde{\mathbf{x}}_d}{\gamma} + \frac{\mathbf{W}_d \tilde{\mathbf{x}}_d}{\gamma}, \quad (13)$$

where $\mathbf{x}_d$ is the transmitted data vector and $\tilde{\mathbf{x}}_d$ is the decoded data vector. The length of decoded vector $\tilde{\mathbf{x}}_d$ used as reference for training is γ. The channel estimation error for error free decoding ($k = 0$) is

$$\Delta\mathbf{H}(0) = \mathbf{H}_u^d - \widehat{\mathbf{H}}_u^d = \widetilde{\mathbf{w}}. \quad (14)$$

The NMSE of the channel estimation for $k = 0$ errors is $\text{NMSE}(0) = \frac{\sigma^2}{\gamma}$. For one error, $\mathbf{x}_d^T \tilde{\mathbf{x}}_d = \gamma - 2$. The channel estimation error in the presence of $k = 1$ error is

$$\Delta\mathbf{H}(1) = \mathbf{H}_u^d - \frac{(\gamma-2)\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}} = \frac{2\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}}. \quad (15)$$

The NMSE of the channel estimation for $k = 1$ error is $\text{NMSE}(1) = \frac{4}{\gamma^2} + \frac{\sigma^2}{\gamma}$. The channel estimation error in the presence of $k = 2$ error is

$$\Delta\mathbf{H}(2) = \mathbf{H}_u^d - \frac{(\gamma-4)\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}} = \frac{4\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}}. \quad (16)$$

In general, the channel estimate in the presence of k errors can be expressed as

$$\Delta\mathbf{H}(k) = \mathbf{H}_u^d - \frac{(\gamma-2k)\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}} = \frac{2k\mathbf{H}_u^d}{\gamma} - \widetilde{\mathbf{w}}. \quad (17)$$

The NMSE of the channel estimation for k errors is

$$\text{NMSE}(k) = \frac{4k^2}{\gamma^2} + \frac{\sigma^2}{\gamma}. \quad (18)$$

Thus, the weighted NMSE from (12) and (18) is

$$\begin{aligned}\text{NMSE}_\gamma &= \sum_{k=0}^{\gamma} \big(\text{NMSE}(k)\big) p_r(k) \\ &= \sum_{k=0}^{\gamma} \left(\frac{4k^2}{\gamma^2} + \frac{\sigma^2}{\gamma}\right)\binom{\gamma}{k} p^k\,(1-p)^{\gamma-k}. \quad (19)\end{aligned}$$

□

In Section VI, Fig. 5, we present comparison of analytical and Monte Carlo NMSE. Next, we present our proposed PABH and DDBH PCA detectors and provide performance analysis.

B. PCA DETECTION

Now, we present the proposed PABH and DDBH detectors. We treat PCA detection as a binary hypothesis problem using likelihood ratio test. The proposed PABH and DDBH detectors use pilot assisted channel estimate $\widehat{\mathbf{H}}_u^p$ in (2) and Eve's channel estimate $\widehat{\mathbf{H}}_e$ by fusing pilot and data phase observations in (2) and (9), respectively. The binary vector hypotheses in (2) and (9) have Gaussian distribution with zero mean and differ in variances. For simplicity and without loss of generality, we consider σ_0^2 and σ_1^2 as the variances under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. For PABH detector,

$$\sigma_0^2 = \frac{P_n\beta_u}{L} + \frac{\sigma^2}{L\tau} \text{ and } \sigma_1^2 = \frac{P_n\beta_u}{L} + \frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau}. \quad (20)$$

Similarly, in the case of DDBH,

$$\sigma_0^2 = \frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma} \text{ and } \sigma_1^2 = \frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma}. \quad (21)$$

We consider $\mathbf{z} = \widehat{\mathbf{h}}_u^p$ and $\mathbf{z} = \widehat{\mathbf{h}}_e^d$ for PABH and DDBH, respectively. The distributions of $\mathbf{z}$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are [53]

$$\begin{aligned} f_{\mathbf{z}|\mathcal{H}_0}(\mathbf{z}) &= \frac{1}{\sqrt{(2\pi\sigma_0^2)^L}}\exp\left(-\frac{\|\mathbf{z}\|^2}{2\sigma_0^2}\right), \\ f_{\mathbf{z}|\mathcal{H}_1}(\mathbf{z}) &= \frac{1}{\sqrt{(2\pi\sigma_1^2)^L}}\exp\left(-\frac{\|\mathbf{z}\|^2}{2\sigma_1^2}\right). \quad (22)\end{aligned}$$

The likelihood ratio test for binary detection is

$$\frac{\frac{1}{\sqrt{(2\pi\sigma_1^2)^L}}\exp\big(-\frac{E}{2\sigma_1^2}\big)}{\frac{1}{\sqrt{(2\pi\sigma_0^2)^L}}\exp\big(-\frac{E}{2\sigma_0^2}\big)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \nu, \quad (23)$$

where $\nu = \frac{p_1}{p_0} = 1$ is the ratio of a-priori probabilities $p_0 = 0.5$ and $p_1 = 0.5$ of $\mathcal{H}_0$ and $\mathcal{H}_1$. Note that $E = \|\mathbf{z}\|^2$ is the ℓ_2-norm of the channel estimate from Bob to Alice for PABH and channel estimate from Eve to Alice for DDBH. We write (23) as

$$-\frac{L}{2}\ln\left(\sigma_1^2\right) + \frac{L}{2}\ln\left(\sigma_0^2\right) - \frac{E}{2\sigma_1^2} + \frac{E}{2\sigma_0^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} 0. \quad (24)$$

After re-arranging (24), we have

$$E \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta = L\left(\frac{\sigma_0^2\sigma_1^2}{\sigma_1^2-\sigma_0^2}\right)\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right). \tag{25}$$

The proposed detectors compare the norm of the estimated channel at the legitimate receiver with the threshold in (25) to detect the presence of PCA. For PABH detector, $\sigma_0^2 = \frac{P_n\beta_u}{L} + \frac{\sigma^2}{L\tau}$ and $\sigma_1^2 = \frac{P_n\beta_u}{L} + \frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau}$. Thus, PCA detection threshold for PABH detector is

$$\eta_p = \frac{1}{P_e\beta_e}\left(P_n\beta_u + \frac{\sigma^2}{\tau}\right)\left(P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}\right) \times\ln\left(\frac{P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}}{P_n\beta_u + \frac{\sigma^2}{\tau}}\right). \tag{26}$$

Similarly, for DDBH $\sigma_0^2 = \frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma}$ and $\sigma_1^2 = \frac{P_e\beta_e}{L} + \frac{\sigma^2}{L\tau} + \frac{\sigma^2}{L\gamma}$. The PCA detection threshold for DDBH detector is

$$\eta_d = \frac{1}{P_e\beta_e}\left(\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right)\left(P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right) \times\ln\left(\frac{P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}{\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}\right). \tag{27}$$

Note that in high SNR regime, for PABH, $\lim_{\sigma^2\to 0} \eta_p = \frac{P_n\beta_u(P_n\beta_u+P_e\beta_e)}{P_e\beta_e}\ln\left(\frac{P_n\beta_u+P_e\beta_e}{P_n\beta_u}\right) = 1.386$ for $P_n = P_e = 1$ and $\beta_u = \beta_e = 1$. Whereas, $\lim_{\sigma^2\to 0} \eta_d = 0$ for DDBH detector. The detection thresholds η_p and η_d are independent of degrees of freedom L. Next, we provide performance analysis of the proposed PCA detectors in terms of the probability of error.

IV. PERFORMANCE ANALYSIS

Now, we present the performance analysis of proposed detectors in terms of probability of error P_E. The norm of the estimated channel $\chi = \|\mathbf{z}\|^2$ is chi-square random variable of degrees $2L$. Let $E_0 = E|\mathcal{H}_0$ and $E_1 = E|\mathcal{H}_1$ be the instantaneous norms of channel estimates under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. An event of "miss detection" occurs when PCA detector fails to detect the presence of pilot contamination attack on Alice [54]. The probability of miss detection P_M for PABH is

$$P_M = P\left(E_1 = E|\mathcal{H}_1 < \eta_p = \frac{1}{P_e\beta_e}\left(P_n\beta_u + \frac{\sigma^2}{\tau}\right) \times\left(P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}\right)\ln\left(\frac{P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}}{P_n\beta_u + \frac{\sigma^2}{\tau}}\right)\right). \tag{28}$$

Similarly, an event of "false detection" occurs when PCA detector detects Eve in the absence of PCA on Alice [54]. The probability of false alarm P_F for PABH is

$$P_F = P\left(E_0 = E|\mathcal{H}_0 > \eta_p = \frac{1}{P_e\beta_e}\left(P_n\beta_u + \frac{\sigma^2}{\tau}\right) \times\left(P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}\right)\ln\left(\frac{P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}}{P_n\beta_u + \frac{\sigma^2}{\tau}}\right)\right). \tag{29}$$

The probability of miss detection P_M for DDBH is

$$P_M = P\left(E_1 = E|\mathcal{H}_1 < \eta_d = \frac{1}{P_e\beta_e}\left(\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right) \times\left(P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right)\ln\left(\frac{P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}{\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}\right)\right). \tag{30}$$

The probability of false alarm P_F for DDBH is

$$P_F = P\left(E_0 = E|\mathcal{H}_0 > \eta_d = \frac{1}{P_e\beta_e}\left(\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right) \times\left(P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}\right)\ln\left(\frac{P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}{\frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}}\right)\right). \tag{31}$$

Now, we derive the probability of miss P_M and probability of false alarm P_F for PABH and DDBH as a function of detection threshold η. The probability density functions $f_{\chi|\mathcal{H}_0}(x)$ and $f_{\chi|\mathcal{H}_1}(x)$ under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ for PABH and DDBH have Gaussian distribution. Note that $\eta = \eta_p$ in (26) and $\eta = \eta_d$ in (27) are detection thresholds for PABH and DDBH, respectively. Furthermore, σ_0^2 and σ_1^2 for PABH and DDBH are given in (20) and (21), respectively. The probability of miss P_M is

$$\begin{aligned} P_M &= \int_0^{\eta} f_{\chi|\mathcal{H}_1}(x)dx = \int_0^{\eta} \frac{2^n\, x^{\frac{n}{2}-1}}{\sigma_1^n 2^{\frac{n}{2}}\Gamma(\frac{1}{2}n)}\exp\left(-\frac{x}{\sigma_1^2}\right)dx \\ &= 1 - \exp\left(-\frac{\eta}{\sigma_1^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_1^2}\right)^k. \end{aligned} \tag{32}$$

Similarly, the probability of false alarm as a function of threshold η can be evaluated as:

$$\begin{aligned} P_F &= \int_{\eta}^{\infty} f_{\chi|\mathcal{H}_0}(x)dx = \int_{\eta}^{\infty} \frac{2^n\, x^{\frac{n}{2}-1}}{\sigma_0^n 2^{\frac{n}{2}}\Gamma(\frac{1}{2}n)}\exp\left(-\frac{x}{\sigma_0^2}\right)dx \\ &= 1 - \int_0^{\eta} \frac{2^n}{\sigma_0^n 2^{\frac{n}{2}}\Gamma(\frac{1}{2}n)} x^{\frac{n}{2}-1}\exp\left(-\frac{x}{\sigma_0^2}\right)dx \\ &= 1 - \left(1 - \exp\left(-\frac{\eta}{\sigma_0^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_0^2}\right)^k\right) \\ &= \exp\left(-\frac{\eta}{\sigma_0^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_0^2}\right)^k. \end{aligned} \tag{33}$$

The general form of the detection threshold

$$\eta = L\left(\frac{\sigma_0^2\sigma_1^2}{\sigma_1^2-\sigma_0^2}\right)\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right) \tag{34}$$

minimizes the probability of PCA detection error

$$\begin{aligned} P_E = \frac{1}{2}(P_F + P_M) &= \frac{1}{2}\exp\left(-\frac{\eta}{\sigma_0^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_0^2}\right)^k \\ &+ \frac{1}{2} - \frac{1}{2}\exp\left(-\frac{\eta}{\sigma_1^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_1^2}\right)^k, \end{aligned} \tag{35}$$

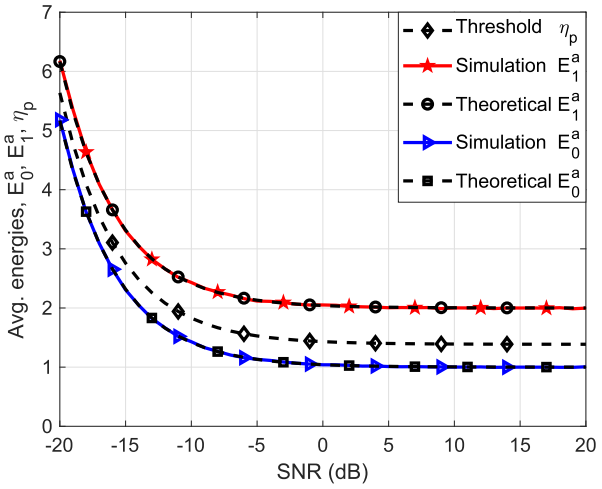

FIGURE 2. Comparison of expected channel norms E_0^a under hypothesis $\mathcal{H}_0$, expected channel norm E_1^a under hypothesis $\mathcal{H}_1$ and detection threshold η_p of PABH for $\tau = 24$ and $L = 8$..

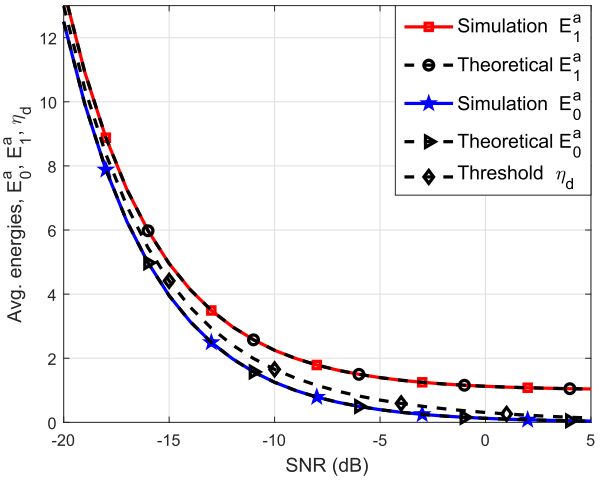

FIGURE 3. Comparison of expected channel norms E_0^a under hypothesis $\mathcal{H}_0$, expected channel norm E_1^a under hypothesis $\mathcal{H}_1$ and detection threshold η_d of DDBH for $\tau = 24$, $\gamma = 12$ and $L = 8$.

of the PCA under binary hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$. Next, we provide the performance comparison in terms of channel norms for proposed PABH and DDBH detectors.

A. CHANNEL NORM

The proposed PABH and DDBH detectors compare detection threshold with the norm-square of the estimated channels $\widehat{\mathbf{h}}_u^p$ and $\widehat{\mathbf{h}}_e^d$, respectively. The expectation of the channel norm-square under the PABH hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are

$$E_0^a = \mathbf{E}\left[\mathbf{z}^H\mathbf{z}|\mathcal{H}_0\right] = \mathbf{E}\left[\mathrm{Tr}\{\mathbf{z}\mathbf{z}^H|\mathcal{H}_0\}\right] = P_n\beta_u + \frac{\sigma^2}{\tau} \text{ and}$$
$$E_1^a = \mathbf{E}\left[\mathbf{z}^H\mathbf{z}|\mathcal{H}_1\right] = \mathbf{E}\left[\mathrm{Tr}\{\mathbf{z}\mathbf{z}^H|\mathcal{H}_1\}\right] = P_n\beta_u + P_e\beta_e + \frac{\sigma^2}{\tau}, \quad (36)$$

respectively.

Fig. 2 provides comparison of analytical and simulation channel norm-square under $\mathcal{H}_0$ and $\mathcal{H}_1$ and detection threshold η_p. In the simulation setup for Fig. 2, we consider $P_n = P_e = 1$, $\beta_u = \beta_e = 1$, the number of training symbols $\tau = 24$ and channel length $L = 8$. It is clear from Fig. 2 that the simulation results agree with the analytical results. The asymptotic (high SNR when $\sigma^2 \to 0$) values of E_0^a and E_1^a are $\lim_{\sigma^2\to 0} E_0^a = 1$ and $\lim_{\sigma^2\to 0} E_1^a = 2$, respectively. Similarly, asymptotic value of detection threshold $\lim_{\sigma^2\to 0} \eta_p = 1.386$. The expectation of the channel norm-square under the DDBH hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ are $E_0^a = \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}$ and $E_1^a = P_e\beta_e + \frac{\sigma^2}{\tau} + \frac{\sigma^2}{\gamma}$, respectively. Fig. 3 compares analytical and simulation norm-square under $\mathcal{H}_0$ and $\mathcal{H}_1$ and detection threshold η_d for DDBH. In the simulation setup for Fig. 3, we also consider $P_n = P_e = 1$, $\beta_u = \beta_e = 1$, the number of training symbols $\tau = 24$ and channel length $L = 8$. Fig. 3 shows that the simulation results agree with the analytical results. The asymptotic (high SNR when $\sigma^2 \to 0$) values of E_0^a and E_1^a are $\lim_{\sigma^2\to 0} E_0^a = 0$ and $\lim_{\sigma^2\to 0} E_1^a = 1$, respectively, for DDBH. Similarly, asymptotic value of detection threshold $\lim_{\sigma^2\to 0} \eta_d = 0$.

V. COMPLEXITY

In this section, we discuss the computational complexity of the proposed PCA detectors and comparison with the computational complexity of the self-contamination based MDL method in [43]. We express the computational complexity in terms of the upper bound on floating point operations (FLOPs). Note that each FLOP denotes one scalar complex multiplication or addition. For the sake of simplicity, we don't distinguish between the complex and real-valued multiplications.

First, we calculate the computational complexity of the self-contamination (SC) based MDL method. SC based MDL method uses signal and noise sub-spaces to detect the presence of PCA and requires only uplink training. The MDL method constructs covariance matrix from the observation and performs eigen value decomposition of the covariance matrix, which requires $\mathcal{O}(N_s^2\tau) + \mathcal{O}(N_s^3)$ FLOPs. There are N_s iterations in SC-based MDL method to detect PCA from the eigen values of the covariance matrix. The complexity of N_s iterations is $N_s\mathcal{O}(\log(N_s)) + N_s\mathcal{O}(N_s)$ FLOPs. Thus, computation complexity of the SC based MDL PCA detector is $\mathcal{O}(N_s^2\tau) + \mathcal{O}(N_s^3)$.

Now, we calculate the computational complexity of proposed PABH and DDBH methods. The proposed PABH based PCA detector uses observation of the training symbols. The proposed PABH method performs vector multiplication in (2), therefore requiring $\mathcal{O}(N_s\tau)$ FLOPs. The proposed DDBH method exploits additional payload data for PCA detection. In DDBH method, we first estimate the payload data $\hat{\mathbf{x}}_d$ in (4) which performs $\mathcal{O}(N_s\gamma)$ multiplications. Next, the DDBH estimates the channel of legitimate node using the hard decision estimated data as reference in (6). The complexity of decision directed channel estimate is $\mathcal{O}(N_s\gamma)$. Next, we estimate the signal of the legitimate user in (7), which

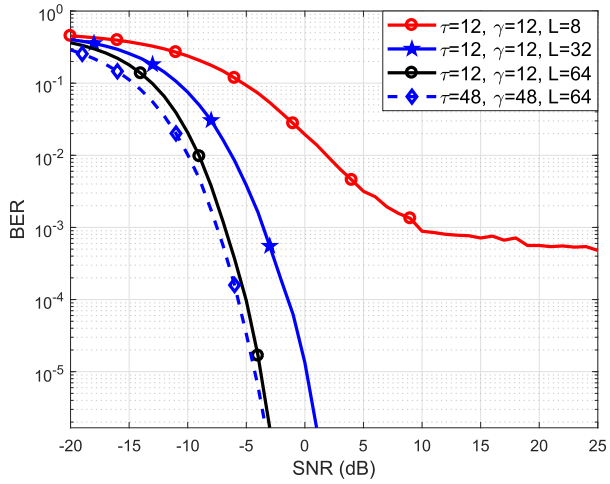

FIGURE 4. Bit error rate (BER) of hard decision data estimate by varying pilot length τ, data length γ and degrees of freedom L.

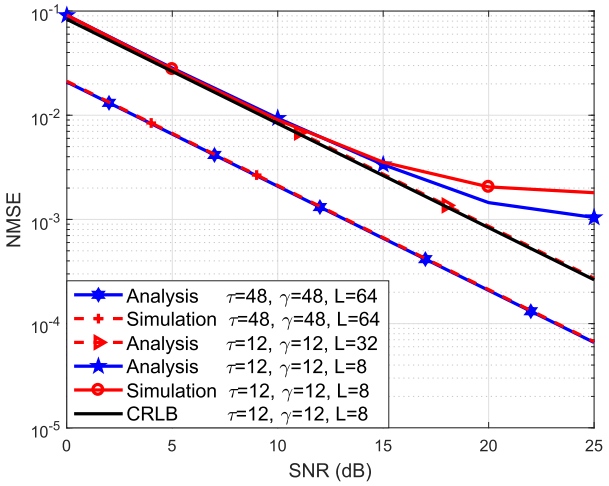

FIGURE 5. NMSE versus SNR for proposed channel estimation method by varying training length τ, data length γ and degrees of freedom L.

consumes $\mathcal{O}(N_s\tau)$ FLOPs. The channel estimate of Eve using the residual signal in (9) consumes $\mathcal{O}(N_s\tau)$ FLOPs. Thus, the computational complexity of the proposed DDBH method is $\mathcal{O}(N_s\tau) + \mathcal{O}(N_s\gamma)$. The above complexity expressions reveal that for a given τ and γ, the computational complexity of MDL increases exponentially by a factor of N_s^3, whereas the complexity of the proposed PABH and DDBH method increase linearly with N_s.

VI. NUMERICAL RESULTS

In this section, we present the performance of proposed PABH and DDBH detectors in comparison with MDL detector. We also provide comparison of analytical and simulation results of the proposed methods. The impact of training length and data length on the performance of the proposed PCA detectors is also investigated. In our simulation setup, the small scale fading channels from Bob to Alice and Eve to Alice are modeled as Rayleigh fading and the elements of channel vector are i.i.d. The samples drawn from Gaussian random variable for channel realization have zero mean and the variance $\frac{1}{L}$. In addition, the large-scale fading coefficients β_u and β_e are considered as 1, i.e. $\beta_u = \beta_e = 1$.

First, we present the performance of the coherent data estimate using the contaminated pilot phase channel estimate in (4) in terms of bit error rate (BER). Fig. 4 shows that the hard decision data estimate using contaminated pilot based channel estimation approaches the true payload data. That is, $\text{dec}(\widehat{\mathbf{x}}_d) \rightarrow \mathbf{x}_d$ as SNR approaches 0 dB under the large number of channel paths. However, BER suffers from severe error floor when the number of channel paths L are small. The problem of error floor is caused by the correlation among the legitimate and Eve channels $\mathbf{H}_u$ and $\mathbf{H}_e$, respectively. The performance of the hard decision data estimate directly impacts the performance of the proposed channel estimation method.

Fig. 5 presents the performance of proposed channel estimation method at legitimate nodes in terms of NMSE. The simulation results in Fig. 5 demonstrate that proposed data-aided channel estimation effectively estimates the channel of legitimate node even in the presence of PCA. Furthermore, we compare NMSE of Cramer-Rao lower bound (CRLB) with the NMSE of the proposed channel estimation method [55]. Note that NMSE for CRLB is $\frac{\sigma^2}{\gamma}$. Fig. 5 shows that NMSE of the proposed method approaches CRLB in moderate to high SNR regime for large channel paths. Moreover, performance of the proposed method can be improved at low SNR regime by increasing the number of payload data. Note that the NMSE suffers from error floor when the number of channel paths L are small. The error floor in terms of NMSE is the direct consequence of error floor in hard decision data estimate due to correlation between legitimate node's channel $\mathbf{H}_u$ and Eve's channel $\mathbf{H}_e$ as shown in Fig. 4. For large channel length, $L = 32$ and 64, small correlation between legitimate channel and Eve's channel results in subtle gap between CRLB and simulation results. Next, we present probability of PCA detection error of the proposed pilot assisted PCA detector (PABH detector) and comparison with analytical results using $\tau = 24$ training symbols.

Fig. 6 presents performance of PABH detector for $L = 8$, 16 and 32 degrees of freedom. The probability of detection error of PABH method decreases by increasing SNR. Note that probability of detection error of PABH method suffers from error floor in high SNR regime. The asymptotic performance (SNR $\rightarrow \infty$) improves by increasing the degrees of freedom (channel path L). The comparison of Monte Carlo results of probability of error with analysis in (35) in Fig. 6 validates the accuracy of the analysis. In Fig. 7, we evaluate performance of the proposed PABH PCA detector as a function of training length τ ranging from 1 to 25 symbols and number of channel paths $L = 8$ and 16. From Fig. 7, we observe that more training symbols improve probability of error. However, transmission of very long training results into error floor due to the fact that large training

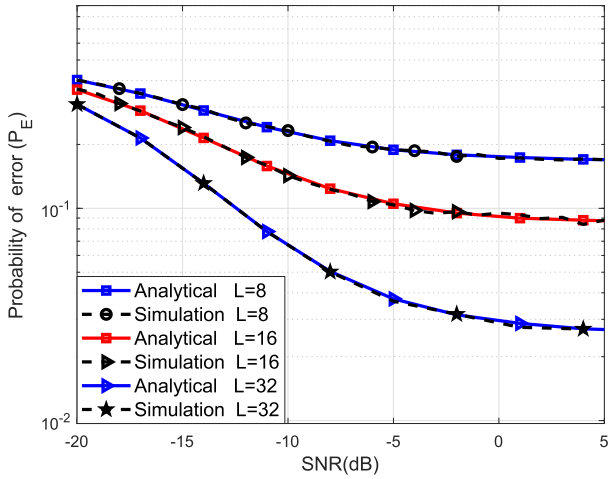

FIGURE 6. Comparison of PABH analytical and Monte Carlo P_E for pilot length $\tau = 24$.

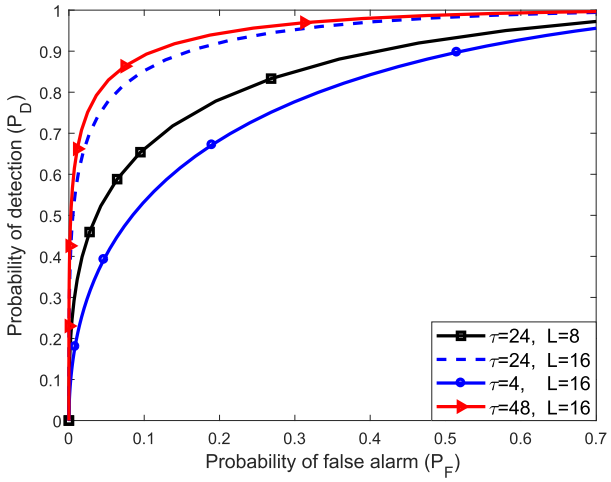

FIGURE 8. ROC of the proposed PABH for training length $\tau = 24$ and 48 and $L = 8$ and 16.

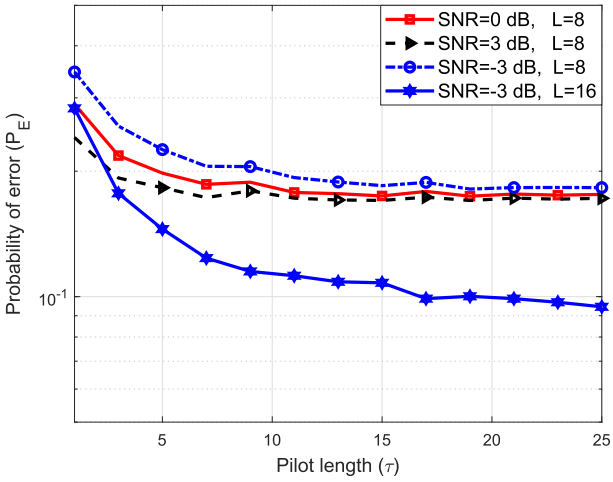

FIGURE 7. Impact of Training Length τ on PABH probability of error P_E.

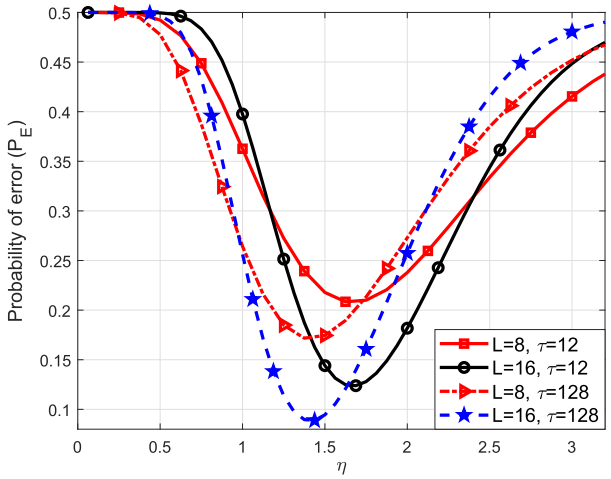

FIGURE 9. Probability of Error of proposed PABH as a function of Eta η for $SNR = -5$dB.

length lowers variance of estimation error $\frac{\sigma^2}{\tau}$ and variance of PABH hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ becomes independent of noise variance σ^2.

In Fig. 8, we illustrate the receiver operating characteristic (ROC) curve, which is a function of probability of false alarm P_F and probability of detection P_D. In Fig. 8, we set the training and contamination power of Bob and Eve to 1, that is, $P_n = P_e = 1$. We present ROC curves by varying the number of pilot bits $\tau = 4,\ 24$ and 48 and channel lengths $L = 8$ and 16. We observe from Fig. 8 that the proposed method can detect PCA with good accuracy. In addition, larger number of training bits can improve the performance of the proposed method.

Fig. 9 presents the impact of threshold η on the performance of the proposed PABH method in terms of probability of error at SNR $= -5$dB. Fig. 9 shows that P_E is a convex function of threshold η. Note that the threshold from exhaustive search, which minimizes probability of error agrees with threshold η using (26). In addition, the probability of error decreases by increasing channel length L for a given threshold η. The detection threshold η changes by changing the number of pilot symbols in the training phase. The performance of the proposed method has error floor in high SNR regime.

The pilot phase is always followed by payload data. We decode payload data using the contaminated channel estimate due to the fact that $\mathbf{H}_u$ and $\mathbf{H}_e$ are independent. Thus, contribution of $\mathbf{H}_e$ in $\hat{\mathbf{H}}_u$ in (2) has subtle impact on the decoding of payload data. We use decoded data as reference to estimate $\mathbf{H}_u$ and estimate Eve's channel to formulate DDBH for PCA detection. Now, we provide performance of DDBH PCA detector in terms of probability of error, ROC curve and comparison with MDL method. We also provide comparison of simulation and analytical results.

We present the impact of the training and payload length on P_E of the proposed DDBH PCA detector in Fig. 10. In simulation setup, we use $P_n = P_e = 1$ and $L = 32$. Fig. 10 shows that probability of error improves by increasing pilot length and payload data length. However, gain in the performance

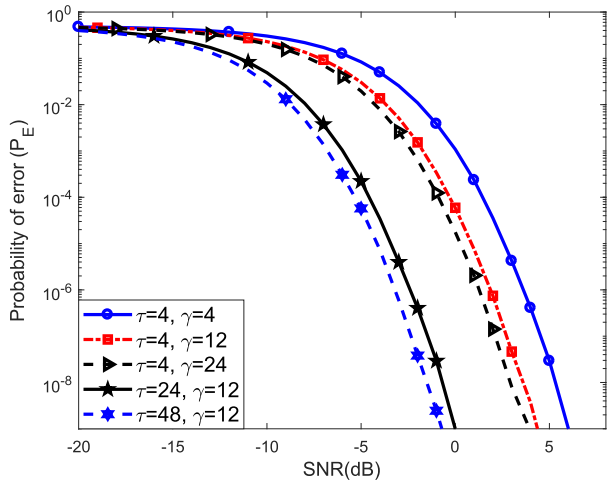

FIGURE 10. Impact of training length τ and data length γ on DDBH P_E for $L = 32$.

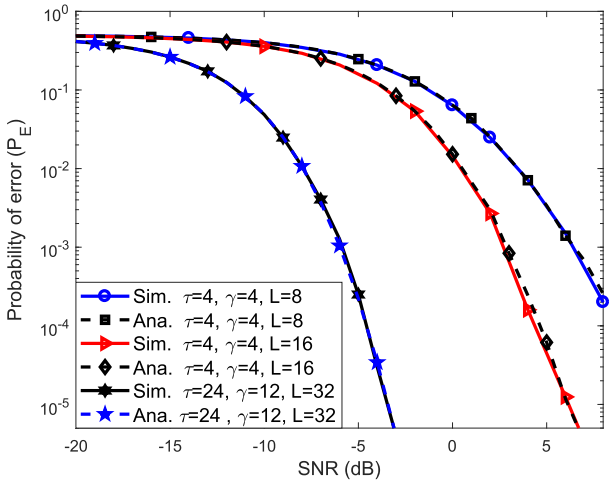

FIGURE 11. Comparison of analytical and Monte Carlo DDBH P_E for various training lengths τ, data length γ and channel length L.

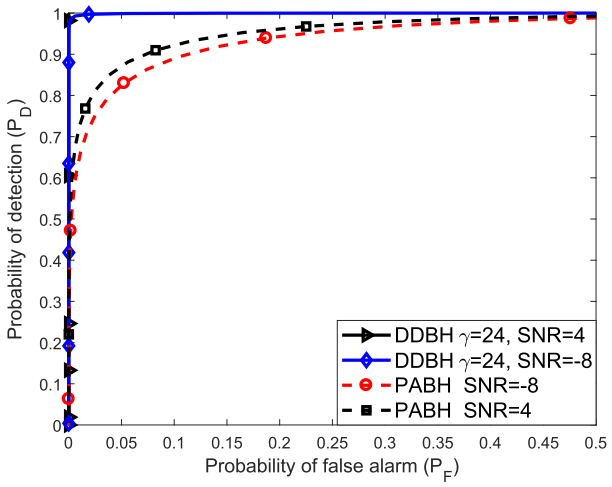

FIGURE 12. ROC comparison of PABH and DDBH for training length $\tau = 48$ and data length $\gamma = 24$ at SNR= -4, and 8 and $L = 8$ and 16 at SNR = -8dB.

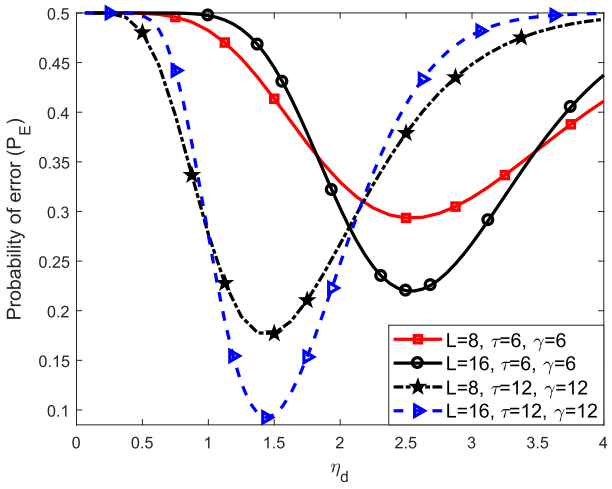

FIGURE 13. Probability of error of proposed DDBH as a function of Eta η for SNR = -8dB.

does not increase linearly with training or payload size. For example, for payload $\gamma = 12$, there is marginal performance gain by increasing training length from $\tau = 24$ to $\tau = 48$.

Fig. 11 demonstrates accuracy of the analysis of the proposed DDBH PCA detector. The comparison of the exact analysis in (35) with Monte Carlo results verifies the accuracy of the analysis.

ROC curve is a commonly metric used to evaluate the performance of a detection method. We compare ROC curve of the proposed PABH and DDBH PCA detectors in Fig. 12. In simulation setup, Bob and Eve transmit unit power in training and data modes ($P_n = P_e = 1$), $\tau = 48$ and $\gamma = 24$. From Fig. 12, we observe that the proposed DDBH PCA detector can accurately detect PCA in low SNR regime. Furthermore, fewer payload symbols significantly improve the performance of PCA detector.

Fig. 13 presents the impact of threshold η on the performance of the proposed DDBH method in terms of probability of error at SNR $= -8$dB. Fig. 13 depicts that P_E is a convex function of threshold η. We also notice that the optimal value of the threshold η_d, which achieves minimum probability of error P_E agrees with analytical threshold in (27). Furthermore, the probability of error decreases by increasing the channel length L and threshold η_d is not function of channel order L. Now, we compare performance of the proposed PABH and DDBH detectors with sub-space based MDL detector in [43] in terms of probability of detector error P_E and probability of detection P_D.

Fig. 14 compares probability of error P_E of the proposed PCA detectors with self contamination based MDL method, which uses sub-space approach for PCA detection. In simulation setup, we use $P_e = P_n = 1$. From Fig. 14, it is clear that the proposed DDBH PCA detector has lower probability of error as compared to the existing MDL method and PABH PCA detector in all SNR regimes. The performance of the proposed PABH method is better than existing MDL method in low SNR regime. Note that sub-space based approaches

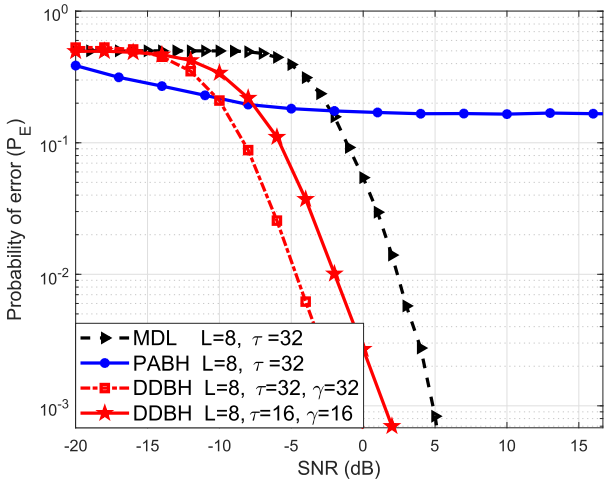

FIGURE 14. Probability of error comparison of PABH and DDBH detector with MDL method.

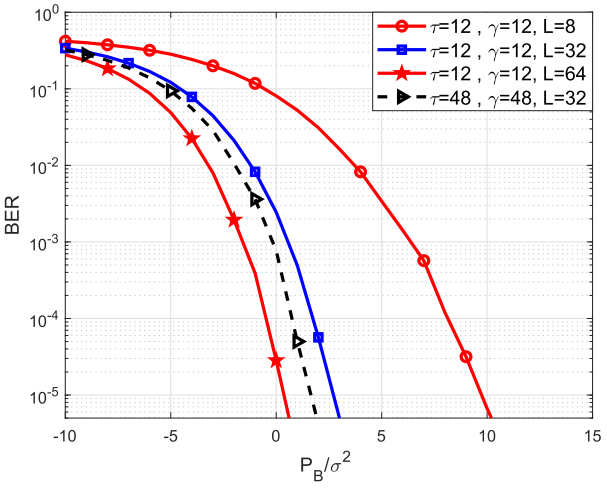

FIGURE 16. Bit error rate of hard-decision data estimate by varying user power for $\frac{P_e}{\sigma^2} = 5$dB.

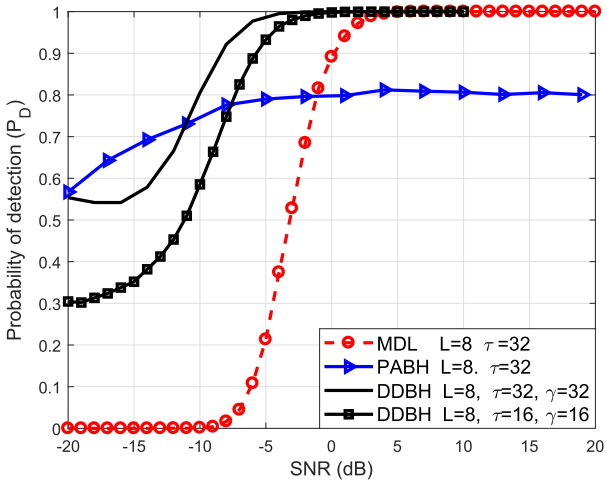

FIGURE 15. Probability of detection comparison of PABH and DDBH detector with MDL method.

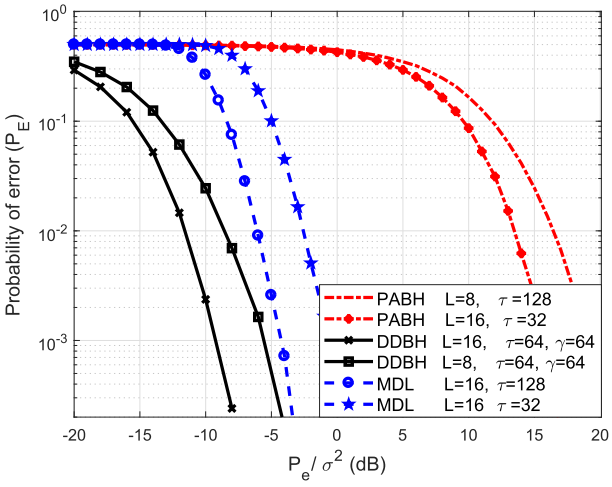

FIGURE 17. Probability of error comparison of PABH and DDBH detector with MDL method.

have higher computational complexity as compared to PABH and DDBH PCA detectors, which have linear complexity.

In Fig. 15, we compare probability of detection P_D for PABH, DDBH and MDL PCA detectors as a function of SNR. As depicted in Fig. 15, the proposed DDBH PCA detector achieves significant performance gain in all SNR regimes over the self-contamination based MDL detector. Clearly, MDL approach achieves better performance as compared to PABH PCA detector in moderate and high SNR regime. However, in low SNR regime, PABH PCA detector performs better than MDL approach.

So far, we have presented the performance of proposed detectors using $P_n = P_e = 1$. However, transmit power of Eve is not limited to unity. Therefore, in Fig. 16, we evaluate the impact of user and Eve power on bit error rate of hard-decision directed data estimate. In the simulation setup, we fix SNR of Eve to $\frac{P_e}{\sigma^2} = 5$dB and evaluate bit error rate by varying $\frac{P_n}{\sigma^2}$ from -10dB to 15dB. Fig. 16 demonstrates that proposed decision directed data estimate is reliable even when Eve attacks with more power than Bob.

In Fig. 17, we evaluate probability of error by varying transmit power of Eve. In simulation setup, we fix SNR of Bob to $\frac{P_n}{\sigma^2} = 10$dB and evaluate probability of error P_E by varying $\frac{P_e}{\sigma^2}$ from -20dB to 20dB. The simulation results demonstrate that DDBH PCA detector performs better that MDL approach and PABH PCA detector. The existing MDL detection method [40] is better than PABH detection in all SNR regimes. Fig. 17 suggests that the probability of detection error decreases by increasing the power of Eve for the fixed noise variance. Eve spends more power on pilot contamination attack, the performance degrades drastically. In low SNR regime, the eigen values corresponding to the noise sub-space are comparable to the eigen values of signal subspace. Consequently, MDL method has poor performance in low SNR regime.

Finally, Fig. 18 compares the performance of proposed detectors in terms of probability of detection as a function

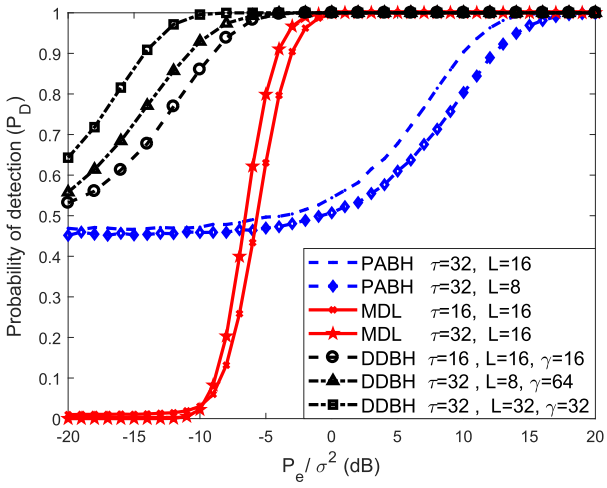

FIGURE 18. **Probability of detection comparison of PABH and DDBH detector with MDL method.**

of $\frac{P_e}{\sigma^2}$ by fixing $\frac{P_n}{\sigma^2} = 10$dB. From Fig. 18, we observe that our PABH PCA detector achieves performance gain in low SNR regime as compared to self-contamination based MDL approach. It is worth noting that MDL approach offers performance gain as compared to PABH detector in moderate and high SNR regimes. However, the proposed DDBH PCA detector outperforms MDL method in all SNR regimes.

VII. CONCLUSION

In this work, we presented two novel PABH and DDBH PCA detectors for frequency selective channels, which exploit the pilot and data phase observations. The proposed detectors have low complexity as compared to the existing sub-space based MDL detector. Furthermore, the proposed DDBH method estimates the channels of the legitimate user and Eve for PCA detection, which is useful for precoder design to enhance secrecy capacity. We also provided performance analysis of the proposed PCA detectors. The comparison of simulation results and analysis verified our analysis. The simulation results demonstrated that the proposed DDBH PCA detector outperforms sub-space based MDL detector, especially in low SNR regime.

REFERENCES

[1] T. Q. Duong, X. Zhou, and H. V. Poor, *Trusted Communications With Physical Layer Security for 5G and Beyond*, vol. 76. Edison, NJ, USA: IET, 2017.

[2] 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.

[3] Y. Gao, S. Hu, W. Tang, Y. Li, Y. Sun, D. Huang, S. Cheng, and X. Li, "Physical layer security in 5G based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26350–26357, 2018.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[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] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Oct. 2015, pp. 1–5.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Proc. IEEE Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, Jun. 2009.

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

[10] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple Amplify-and-Forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[11] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.

[12] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[13] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[14] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[15] D. Tubail, M. El-Absi, S. S. Ikki, W. Mesbah, and T. Kaiser, "Artificial noise-based physical-layer security in interference alignment multipair two-way relaying networks," *IEEE Access*, vol. 6, pp. 19073–19085, 2018.

[16] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[17] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[18] L. Shao, "Coordinated multicell beamforming and power allocation for massive MIMO: A large system analysis," *Signal Process.*, vol. 164, pp. 41–47, Nov. 2019.

[19] F. Rezaei and A. Tadaion, "Multi-layer beamforming in uplink/downlink massive MIMO systems with multi-antenna users," *Signal Process.*, vol. 164, pp. 58–66, Nov. 2019.

[20] Y. Chen, X. Gao, X.-G. Xia, and L. You, "A robust precoding for RF mismatched massive MIMO transmission," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[21] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[22] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[23] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18–33, Jan. 2019.

[24] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[25] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[26] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement under an active attack in MU-TDD systems with large antenna arrays," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 1849–1855.

[27] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE Trans. Mobile Comput.*, vol. 18, no. 3, pp. 507–519, Mar. 2019.

[28] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[29] A. Ahmed, M. Zia, and I. ul Haq, "Secret key acquisition under pilot contamination attack," *AEU Int. J. Electron. Commun.*, vol. 110, Oct. 2019, Art. no. 152865.

[30] P. Ting, C.-K. Wen, and J.-T. Chen, "An efficient CSI feedback scheme for MIMO-OFDM wireless systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2012–2015, Jun. 2007.
[31] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 4868–4873.
[32] H. Quoc Ngo, E. G. Larsson, and T. L. Marzetta, "Massive MU-MIMO downlink TDD systems with linear precoding and downlink pilots," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 293–298.
[33] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Vulnerabilities of massive MIMO systems to pilot contamination attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1251–1263, May 2019.
[34] 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.
[35] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in *Proc. IEEE 25th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2014, pp. 585–589.
[36] Q. Xiong, Y.-C. Liang, K. Hung 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.
[37] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[38] J.-M. Kang, C. In, and H.-M. Kim, "Detection of pilot contamination attack for multi-antenna based secrecy systems," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.
[39] 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.
[40] J. K. Tugnait, "Detection of pilot spoofing attack over frequency selective channels," in *Proc. IEEE Stat. Signal Process. Workshop (SSP)*, Jun. 2018, pp. 737–741.
[41] D. Kapetanovic, 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.
[42] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.
[43] 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.
[44] J. K. Tugnait, "Detection and mitigation of pilot spoofing attack," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, Oct. 2017, pp. 1667–1671.
[45] A. Badawy, T. Salman, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Estimating the number of sources in white Gaussian noise: Simple eigenvalues based approaches," *IET Signal Process.*, vol. 11, no. 6, pp. 663–673, Aug. 2017.
[46] 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.
[47] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdroppers," *IEEE Commun. Mag.*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.
[48] A. F. Molisch, *Wireless Communications*, vol. 34. Hoboken, NJ, USA: Wiley, 2012.
[49] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
[50] K. Jallouli, M. Mazouzi, A. B. Ahmed, A. Monemi, and S. Hasnaoui, "Multicore MIMO-OFDM LTE optimizing," in *Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC)*, Dec. 2018, pp. 166–170.
[51] A. Ahmed, Z. Muhammad, H. Mahmood, and N. A. Saqib, "Partial automatic repeat request transceiver for bandwidth and power efficient multiple-input-multiple-output orthogonal frequency division multiplexing systems," *IET Commun.*, vol. 9, no. 4, pp. 476–486, Mar. 2015.
[52] X. Tian, M. Li, and Q. Liu, "Random-training-assisted pilot spoofing detection and security enhancement," *IEEE Access*, vol. 5, pp. 27384–27399, 2017.
[53] J. Proakis and M. Salehi, *Digital Communications*. New York, NY, USA: McGraw-Hill, 2007.
[54] M. Barkat, *Signal Detection Estimation*. Norwood, MA, USA: Artech House, 2005.
[55] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

AWAIS AHMED (Student Member, IEEE) received the B.S. degree from the Center for Advanced Studies in Engineering (CASE), Pakistan, in 2010, and the M.Phil. degree from the Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan, in 2013, where he is currently pursuing the Ph.D. degree in communications and signal processing.

MUHAMMAD ZIA (Member, IEEE) received the M.S. degree in electronics and the M.Phil. degree from the Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan, in 1991 and 1999, respectively, and the Ph.D. degree in electrical engineering from the Department of Electrical and Computer Engineering, University of California at Davis, Davis, CA, USA, in 2010. He is currently with the Department of Electronics, Quaid-i-Azam University, as an Associate Professor.

IHSAN UL HAQ (Member, IEEE) received the M.Sc. degree in physics (electronics) from Bahauddin Zakariya University, Pakistan, in 1998, the M.Phil. degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 2004, and the Ph.D. degree in information and electronic engineering from Beihang University, Beijing, China, in 2009. He is currently with the Department of Electrical Engineering, International Islamic University, as an Associate Professor.

HUY-DUNG HAN (Member, IEEE) received the B.S. degree from the Faculty of Electronics and Telecommunications, Hanoi University of Science and Technology, Vietnam, in 2001, the M.Sc. degree from the Technical Faculty, University of Kiel, Germany, in 2005, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of California, Davis, in 2012. He is currently with the Department of Electronics and Computer Engineering, School of Electronics and Telecommunications, Hanoi University of Science and Technology. His research interests include wireless communications and signal processing, with current emphasis on blind and semi-blind channel equalization for single and multicarrier communication systems and convex optimization.