IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 November 2022, accepted 12 December 2022, date of publication 15 December 2022,
date of current version 22 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3229615

RESEARCH ARTICLE

Higher Secrecy Capacity by Successive Pilot Contamination and Jamming Cancellation

AWAIS AHMED[1], (Student Member, IEEE), MUHAMMAD ZIA[1], (Member, IEEE), NAEEM BHATTI[1], (Member, IEEE), HASAN MAHMOOD[1], AND HUY-DUNG HAN[2], (Member, IEEE)

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

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

ABSTRACT We present a secure transmission method for orthogonal frequency division multiplexing (OFDM) signaling between legitimate nodes (Alice and Bob) communicating in time-division duplex (TDD) mode under an active attack. An active eavesdropper carries out pilot contamination attack in pilot phase by transmitting the pilot signal of the legitimate user and jamming attack in data phase. In the proposed method, Alice estimates the reciprocal channel between Alice and Bob by employing successive cancellation of the pilot contamination and interference from an active eavesdropper in pilot and data phases, respectively. We estimate reciprocal channels of legitimate users and eavesdropper. The precoder design at Alice from the estimated channels steers information towards Bob and artificial noise towards Eve in order to enhance the secrecy capacity of channel of the legitimate nodes. The simulation results show that the proposed method effectively estimates the channels of legitimate users and eavesdropper by removing the impact of contamination attack. Consequently, legitimate channel achieves higher secrecy capacity.

INDEX TERMS Active eavesdropping, detection, channel reciprocity, OFDM, pilot contamination attack, secrecy capacity.

I. INTRODUCTION

Security is a critical issue in wireless communication systems due to the broadcast nature of transmission medium. Wireless systems are also susceptible to pilot contamination attack (PCA) from an active eavesdropper [1]. The physical layer's (PHY) security has attracted significant attention and is regarded as an attractive alternative for securing private messages over wireless channels [2], [3], [4], [5].

Unlike wired communication links, wireless communication suffers from a risk of being eavesdropped. Recently, spatial degrees of freedom (DOF) provided by multiple antennas have also been exploited to considerably enhance the security at PHY [6], [7], especially in the presence of passive eavesdropping. One way to enhance secrecy capacity of the legitimate channel is the transmission of artificial noise signals in the null space of an estimated legitimate user channel [8], [9], [10]. Increasing the number of antennas at the base station, with the aim of exploiting additional DOF, ensures secure communication when adversary is passive. Furthermore, beamforming [11] and secret key generation techniques have been used to achieve security at PHY [12].

Active eavesdropping for wireless communication is extensively investigated, particularly, PCA, which degrades the security of the legitimate nodes and facilitates eavesdropper to steal information in [13], [14], and [15] and references therein. Most of the works on PHY security focus on the detection of PCA and little investigation is carried out on the mitigation of the impact of PCA on legitimate users [13], [15], [16]. In order to enhance the secrecy capacity of the link of the legitimate users, a reliable estimate of channel state information (CSI) of reciprocal channel at the transmitter is vital [17], [18], [19]. The precoder design for transmission reduces the information leakage towards the active Eve [1]. The gain of multiple antennas depends highly on accurate channel estimate of the legitimate node [20]. The secrecy capacity for cell-free massive multiple-input multiple-output (MIMO) network is analyzed, when network is under attack by an active eavesdropper with single antenna [21], [22], [23], [24], [25]. However, a smart jammer can actively attack the

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

pilot phase to induce pilot contamination attack and jamming attack in the data phase. Consequently, a smart jammer can induce jamming in the data phase and deteriorate the received signal-to-interference-and-noise ratio (SINR).

In practice, if an eavesdropper attacks the transmission, it is essential to quickly detect the presence of eavesdropping so that countermeasures can be taken in a timely manner [26], [27], [28], [29]. For example, the secure transmission schemes in the presence and absence of PCA are totally different. In the absence of PCA, maximal ratio transmission (MRT) beamforming maximizes the signal to noise ratio (SNR) at Bob. However, under PCA, MRT scheme results in significant information leakage towards Eve due to contaminated channel estimate [30]. Thus, to safeguard transmission under PCA, contamination free channel estimation should be evaluated [31]. Motivated by the above mentioned observations, we propose a PCA detection method in the pilot phase and jamming detection method in the data phase.

We focus on the enhancement of the secrecy capacity of the channel of the legitimate nodes in the presence of an active eavesdropper for time division duplex (TDD) communication link. The precoder design to form beam towards legitimate receiver requires good estimate of the reciprocal legitimate channel. The PCA contaminates the estimated channel, which causes information leakage towards the eavesdropper. We use the observations of the pilot and data phases to successively remove pilot contamination in pilot phase and interference in data phase from Eve in order to enhance secrecy capacity of the channel between the legitimate users.

The secrecy capacity of the forward channel under PCA is severely compromised [1]. Work in [32] and [33] focuses on the transmission of artificial noise (AN) and precoder design, respectively, to enhance the secrecy capacity under passive eavesdropping. A secure transmission method for TDD mode under active eavesdropping in [34] proposed an unified design, which combines the precoding and transmission of AN in the null space of user. Works in [32], [33], and [34] assume that transmitter has perfect CSI for precoder design and Eve is silent in data phase. In practice, acquisition of channel state information (CSI) for wireless communication systems in the presence of PCA from an Eve is a challenging task and Eve can chose to transmit jamming signal in data phase. Work in [35] assumes unused orthogonal pilots and Eve transmits jamming signal in pilot phase. The receiver in [35] exploits unused pilots to reduce the impact of contamination from the active jammer. The method in [35] fails to estimate channel when an active Eve launches PCA in the pilot phase and jamming attack in the data phase. The work in [36] adopted a proactive eavesdropping scheme, where the legitimate eavesdropper pretends to launch PCA in pilot phase. In [36], a proactive jamming scheme is adopted to improve the performance of eavesdropper during data transmission phase. The recent work in [13] proposes three phase uplink training (TPUT) method, which uses an additional auxiliary node to detect active Eve and estimate the channels of legitimate users and eavesdropper.

Unlike the previous methods that focus either on pilot contamination or jamming attacks, we propose a novel transceiver design to mitigate the impact of PCA in pilot phase and jamming attack in data phase. The proposed receiver successively removes pilot contamination in pilot phase and jamming in data phase without using an auxiliary node in [13].

A. CONTRIBUTIONS

The proposed transmitter sends short silence in data phase at a random position, which is helpful for the legitimate receiver (Alice) to successively alleviate the pilot contamination and interference for the channel estimation. The precoder design uses channel estimate after successive removal of pilot contamination and jamming signal from an active Eve and achieves higher secrecy capacity. The major contributions of this work are as follows:

- We propose a transceiver design, in which transmitter (Bob) transmits silence for short time in data phase to help receiver (Alice) mitigate the impact of PCA in pilot phase and jamming attack in data phase using successive cancellation.
- We also propose a jamming detection scheme, which detects silence from Bob and jamming attack from an active eavesdropper in data phase.
- We provide closed form expression of the probability of detection error for the proposed maximum-likelihood (ML) silence detector. The sub-space based minimum descriptor length (MDL) method detects number of sources for the detection of jamming attack.
- Simulation results reveal that the precoder design from the proposed scheme can achieve better performance in terms of secrecy capacity and can effectively combat multiple transmission strategies of Eve in the data phase.

The rest of the work is organized as follows. In Section II, we present the system model for PCA. In Section III, we propose successive pilot contamination and jamming cancellation method. Section IV presents the precoding scheme to enhance secrecy capacity. In Section V, we provide the performance of the proposed method and its comparison with TPUT based method, while Section VI summarizes the main result of this work.

NOTATIONS

We represent matrices and vectors by bold-face uppercase and bold-face lowercase letters, respectively. We use the superscripts H, $\dagger$ and T, for hermitian, pseudoinverse and transpose, respectively. We use $\mathbf{I}_N$ to denote $N \times N$ identity matrix. Note that $\mathcal{C}$ is set of complex numbers.

II. SYSTEM MODEL

In the considered model, the legitimate nodes, Alice and Bob, communicate over a multipath wireless channel in TDD mode in the presence of an active Eve over frequency selective channel as shown in Fig. 1. Each node is equipped with single antenna and extension to multiple antennas is straight

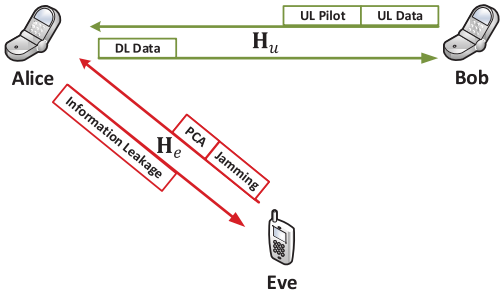


FIGURE 1. PCA model from an active Eve.

forward. The L-path wireless reciprocal user channel between legitimate nodes, Alice and Bob, is $\mathbf{h}_u \in \mathcal{C}^{L\times 1}$, whereas the wireless reciprocal channel between Eve and Alice is $\mathbf{h}_e \in \mathcal{C}^{L\times 1}$. Note that OFDM waveform converts L-path frequency selective channel into N flat-fading sub-carriers. Alice intends to transmit private message to Bob over a wireless channel in the presence of an active Eve. We denote signal direction from Bob to Alice, *up-link* direction and signal from Alice to Bob, *down-link* (reverse) direction. Bob transmits training to Alice for channel estimation and Alice designs precoder using user channel estimate $\hat{\mathbf{h}}_u$ to transmit private message to Bob (reverse direction). We assume that up-link transmission phase comprises of up-link pilot phase and up-link data transmission phase. The up-link transmission phase is followed by downlink data transmission phase. Note that the main objective of eavesdropper is to eavesdrop the downlink data transmission. Consequently, Eve launches PCA in the pilot phase. Furthermore, eavesdropper can either keep silent or transmit jamming signal in the up-link data transmission phase to further impair the signal. In the downlink data transmission phase, the eavesdropper is passive and focuses on receiving the information leakage due to PCA and jamming in uplink data phase.

In training phase, Eve transmits pilot sequence identical to the pilot sequence from Bob to Alice with the intention to steel secure message. In the presence of PCA, Alice estimates the superposition of the channels $\mathbf{h}_u$ and $\mathbf{h}_e$.

Consequently, precoder design using the estimated channel from contaminated observation by Alice implicitly steers partial beam towards Eve. Bob transmits data to Alice after pilot phase as shown in Fig. 2. In the data phase from Bob to Alice, Eve has freedom to either transmit jamming signal or become passive (silent). Furthermore, jamming signal of Eve in data phase can be random noise or M-point quadrature amplitude modulation (M-QAM) constellation.

The estimate of the channel eigen vector in pilot phase under PCA is $\hat{\mathbf{H}}_u^p = \mathbf{H}_u + \mathbf{H}_e + \Delta\mathbf{H}^p$, where $\mathbf{H}_u = \mathbf{F}\mathbf{h}_u \in \mathcal{C}^{N\times 1}$ and $\mathbf{H}_e = \mathbf{F}\mathbf{h}_e \in \mathcal{C}^{N\times 1}$, $\Delta\mathbf{H}^p = \mathbf{F}\Delta\mathbf{h}^p \in \mathcal{C}^{N\times 1}$ and $\mathbf{F}$ is the Fourier transform matrix.

We assume that Eve and Bob transmit pilot signal with unit energy. Let C and C_e be the capacities of the channel from Bob to Alice and Eve to Alice, respectively. Then, secrecy capacity is $C_s = \max\{0, C - C_e\}$. The secrecy capacity between Alice and Bob deteriorates in the event of PCA detection.

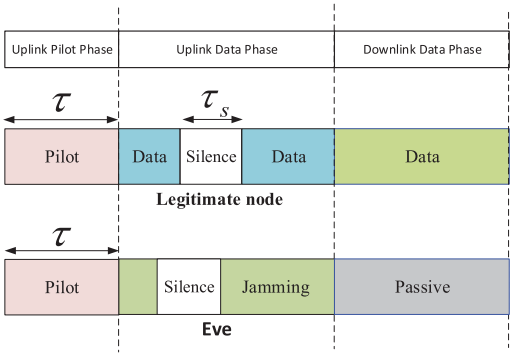


FIGURE 2. PCA model and transmission protocol from Bob to Alice in TDD mode for OFDM modulation.

A. UPLINK PILOT PHASE

The matrix model of the observation at Alice in response to the pilot sequence $\mathbf{s}_p \in \mathcal{C}^{\tau\times 1}$ under PCA is

$$\mathbf{Y}_p = \mathbf{H}_u\mathbf{s}_p^T + \mathbf{H}_e\mathbf{s}_p^T + \mathbf{W}, \tag{1}$$

where $\mathbf{W} \in \mathcal{C}^{N\times\tau}$ is the AWGN matrix. The elements of the noise matrix are independent and identically distributed (i.i.d.) with zero mean and variance σ^2. The least square (LS) channel estimate at Alice in pilot phase under PCA is

$$\begin{aligned}\hat{\mathbf{H}}_u^p &= \mathbf{H}_u\mathbf{s}_p^T\frac{\mathbf{s}_p^*}{\|\mathbf{s}_p\|^2} + \mathbf{H}_e\mathbf{s}_p^T\frac{\mathbf{s}_p^*}{\|\mathbf{s}_p\|^2} + \mathbf{W}\frac{\mathbf{s}_p^*}{\|\mathbf{s}_p\|^2}\\ &= \mathbf{H}_u + \mathbf{H}_e + \Delta\mathbf{H}^p,\end{aligned} \tag{2}$$

where $\Delta\mathbf{H}^p$ is estimation error vector of $\mathbf{H}_u+\mathbf{H}_e$ and $\|\cdot\|$ is the ℓ_2-norm. Note that $\mathbf{H}_u$ and $\mathbf{H}_e$ are independent and identically distributed. Next, we propose method to remove contribution of $\mathbf{H}_e$ from the estimate $\hat{\mathbf{H}}_u^p$ in (2). The proposed method reduces information leakage to Eve in the down-link direction to improve secrecy capacity of the legitimate channel.

III. PROPOSED METHOD

In order to design unified precoder for secure transmission from Alice to Bob [34], which transmits signal towards Bob and AN towards Eve, Alice needs estimate of reciprocal channel $\mathbf{H}_u$. However, acquisition of CSI for wireless communication systems under PCA from Eve is a challenging task. In this section, we present transmission framework at Bob and successive contamination removal method at Alice to estimate channel $\mathbf{H}_u$ between Alice and Bob.

In our proposed transmission approach, in up-link data phase, Bob remains silent for a short duration τ_s at random position in time known to Alice in order to assist Alice to estimate Eve's channel $\mathbf{H}_e$ as shown in Fig. 2. Note that Alice preserves observations of the pilot phase for successive contamination cancellation. Once, estimate of Eve's channel is known to Alice, we can remove pilot contamination from Eve in pilot phase and estimate user channel $\mathbf{H}_u$. Estimate of channel between Bob and Alice is vital for securing information from Alice to Bob in the down-link direction. In up-link data phase, Eve may decide to be silent (passive)

to reduce the probability of detection or to transmit jamming signals at random positions for effective interference to Alice. Alice preserves observation in pilot phase and follows the following steps in up-link data phase to estimate reciprocal channel between Alice and Bob:

1) Alice detects jamming signal from Eve during Bob's silent period τ_s (silence detection) in up-link data phase. If Eve transmits jamming signal in silent period τ_s of Bob, Alice estimates Eve's channel $\mathbf{H}_e$ and performs successive cancellation to estimate channel $\mathbf{H}_u$ between Alice and Bob.
2) If Eve is also silent during the silent period τ_s of Bob, Alice searches for the time slot, where Eve is silent and estimates user channel $\hat{\mathbf{H}}_u$.
3) If Alice fails to find time segment where Bob transmits data to Alice and Eve is silent, channel estimation fails.

We remove contribution of Eve's channel from the pilot phase channel estimate $\hat{\mathbf{H}}_u^p = \mathbf{H}_u + \mathbf{H}_e + \Delta\mathbf{H}^p$ and decode up-link data using preserved observations of data phase. Now, we present binary hypothesis to detect Eve during silent period of Bob in data.

A. ACTIVE EVE AND SILENT BOB DETECTION

In this section, we present Eve's detection when Bob is silent for τ_s symbols in up-link data phase. Alice assumes prior knowledge of the location of Bob's silence for τ_s symbols. Since Bob is silent, decision directed channel estimate is either noise or Eve's channel $\mathbf{H}_e$. We use channel estimate of Eve to construct the binary hypothesis $\mathcal{H}_0$ (silent Eve) and $\mathcal{H}_1$ (Eve transmitting jamming signal) from the observation. The matrix observation $\mathbf{Y}_s \in \mathcal{C}^{N\times\tau_s}$ at Alice in up-link data phase, when Bob remains silent for τ_s symbols is

$$\begin{aligned}\mathcal{H}_0 &: \mathbf{Y}_s = \mathbf{W}_s,\\ \mathcal{H}_1 &: \mathbf{Y}_s = \mathbf{H}_e\mathbf{s}_J^T + \mathbf{W}_s,\end{aligned} \tag{3}$$

where $\mathbf{W}_s \in \mathcal{C}^{N\times\tau_s}$ is the AWGN matrix. The elements of AWGN matrix $\mathbf{W}_s$ are i.i.d. with zero mean and variance σ^2. The estimate of $\mathbf{s}_J$ using contaminated channel estimate $\hat{\mathbf{H}}_u^p$ in (2) and observation $\mathbf{Y}_s$ is

$$\begin{aligned}\widehat{\mathbf{s}}_J^T &= \left(\widehat{\mathbf{H}}_u^p\right)^\dagger \mathbf{Y}_d\\ &= \alpha\left(\mathbf{H}_e + \mathbf{H}_u + \frac{\mathbf{W}\mathbf{s}_p^*}{\tau}\right)^H\\ \left(\mathbf{H}_e\mathbf{s}_J^T + \mathbf{W}_s\right) &= \alpha\|\mathbf{H}_e\|^2\mathbf{s}_J^T + \widetilde{\mathbf{w}}_s,\end{aligned} \tag{4}$$

where

$$\begin{aligned}\widetilde{\mathbf{w}}_s = \alpha\mathbf{H}_u^H\mathbf{H}_e\mathbf{s}_J^T + \frac{\alpha}{\tau}\mathbf{s}_p^T\mathbf{W}^H\mathbf{H}_e\mathbf{s}_J^T\\ + \alpha\mathbf{H}_e^H\mathbf{W}_s + \alpha\mathbf{H}_u^H\mathbf{W}_s + \frac{\alpha}{\tau}.\mathbf{s}_p^T\mathbf{W}^H\mathbf{W}_s,\end{aligned} \tag{5}$$

and $\alpha = \|\ \mathbf{H}_e + \mathbf{H}_u + \frac{\mathbf{W}\mathbf{s}_p^*}{\tau}\ \|^{-2}$ and $\mathbf{H}_e^H\mathbf{H}_e = \|\mathbf{H}_e\|^2 \approx 1$ for large channel order L. Note that, due to central limit theorem, $\widetilde{\mathbf{w}}_s \in \mathcal{C}^{\tau_s\times 1}$ is AWGN matrix of zero mean and variance $\tilde{\sigma}_s^2$. Furthermore, the jamming signal estimate $\widehat{\mathbf{s}}_J$ is reliable due to poor correlation between legitimate channel and Eve's channel. Next, we discuss the impact of channel length L on the performance of up-link data symbols estimate $\widehat{\mathbf{s}}_J$.

1) IMPACT OF CHANNEL TAPS L ON JAMMING SIGNAL ESTIMATE

We provide insight on the impact of channel taps L on the performance of jamming data decoding in terms of bit error rate (BER). We evaluate the variance of elements of effective noise $\widetilde{\mathbf{w}}_s$ obtained in (5) as follows:

1) The first term of $\widetilde{\mathbf{w}}_s$ depends on the correlation of user channel $\mathbf{H}_u$ and Eve's channel vector $\mathbf{H}_e$. Note that elements of legitimate channel $\mathbf{H}_u$ and Eve's channel $\mathbf{H}_e$ are i.i.d with mean zero and variance $\frac{1}{L}$. Consequently, the correlation term $\mathbf{H}_u^H\mathbf{H}_e = \sum_i^L \mathbf{H}_u^*(i)\mathbf{H}_e(i)$ is sum of L random variables. Each element of $\mathbf{H}_u^*(i)\mathbf{H}_e(i)$ is zero mean with variance $\frac{1}{L^2}$. Note that, due to central limit theorem, the distribution of channel correlation term $\mathbf{H}_u^H\mathbf{H}_e$ converges to normal distribution with zero mean and variance $\frac{1}{L}$. For simplicity, we consider two-point constellation of data symbols. Thus, only real part of the correlation term affects the performance of data decoding errors. The variance of only the real component of correlation term is $\mathcal{R}\{\mathbf{H}_u^H\mathbf{H}_e\} = \frac{1}{2L}$. Figure 3 presents the comparison of analytical and simulation results of correlation term. From Figure 3, we observe that the estimate $\widehat{\mathbf{s}}_J$ of jamming symbols is reliable for large channel order L due to poor correlation between $\mathbf{H}_u$ and $\mathbf{H}_e$. Furthermore, large correlation between legitimate and eavesdropper channel for small channel order L results in error floor.
2) The elements of $\mathbf{W}$ are also independent and identically distributed with mean zero and variance $\frac{\sigma^2}{L}$. Next, the product term $\mathbf{W}^H\mathbf{H}_e \in C^{\tau\times 1}$ is a vector of independent random variables of zero mean and variance $\frac{\sigma^2}{L}$ each. Furthermore, random variable $\frac{1}{\tau}\mathbf{s}_p^T\mathbf{W}^H\mathbf{H}_e$ is zero mean and variance $\frac{\sigma^2}{\tau L}$. For two point constellation, the variance of only real component of $\mathcal{R}\{\frac{1}{\tau}\mathbf{s}_p^T\mathbf{W}^H\mathbf{H}_e\}$ is $\frac{\sigma^2}{2\tau L}$.
3) The distributions of both $\mathbf{H}_u^H\mathbf{W}_s$ and $\mathbf{H}_e^H\mathbf{W}_s$ converges to normal distribution with zero mean and variance $\frac{\sigma^2}{2L}$, due to central limit theorem.
4) Each element of vector of random variables $\frac{1}{\tau}.\mathbf{s}_p^T\mathbf{W}^H\mathbf{W}_s$ has normal distribution with zero mean and variance $\frac{\sigma^4}{2\tau L}$.

The variance of each element of the vector of random variables $\widetilde{\mathbf{w}}_s$ is

$$\begin{aligned}\tilde{\sigma}_s^2 &= \frac{1}{2L} + \frac{\sigma^2}{2L} + \frac{\sigma^2}{2\tau L} + \frac{\sigma^2}{2L} + \frac{\sigma^4}{2\tau L}\\ &= \frac{1}{2L}\left(1 + 2\sigma^2 + \frac{\sigma^2}{\tau} + \frac{\sigma^4}{\tau}\right).\end{aligned} \tag{6}$$

From (6), it is clear that the variance of effective noise vector $\widetilde{\mathbf{w}}_s$ is inversely proportional to the channel taps L.

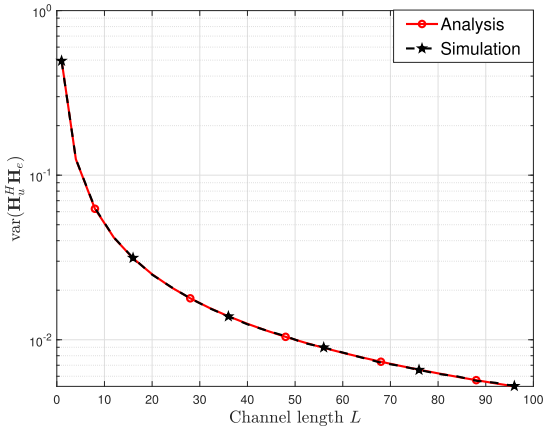


FIGURE 3. Variance of $H_u^H H_e$ as a function of channel order L.

In high SNR regime, $\lim_{\sigma^2\to 0} \tilde{\sigma}_s^2 \to \frac{1}{2L}$ causes BER and NMSE floor for small L. Furthermore, for large L, either due to muli-path components or large antennas, $\|\mathbf{H}_u\| \to 1$ and $\mathbf{H}_u^H\mathbf{H}_e \to 0$.

2) DECISION-DIRECTED DATA ESTIMATE

The jamming signal $\mathbf{s}_J$ can be random noise denoted by noise jamming (NJ) or valid constellation (M-QAM) points denoted by data jamming (DJ). The estimate of signal used as a reference for the decision directed estimation of Eve's channel in data phase is

$$\mathbf{x}_J = \begin{cases} \mathrm{dec}(\hat{\mathbf{s}}_J) & \text{if } \mathbf{s}_J \text{ from M-QAM (DJ)} \\ \hat{\mathbf{s}}_J & \text{if } \mathbf{s}_J \text{ is noise signal (NJ)} \end{cases} \tag{7}$$

Thus, decision directed LS estimate of Eve's channel $\mathbf{H}_e$ is

$$\begin{aligned} \mathcal{H}_0 : \widehat{\mathbf{H}}_e^d &= \frac{\mathbf{W}_s\mathbf{x}_J^*}{\tau_s}. \\ \mathcal{H}_1 : \widehat{\mathbf{H}}_e^d &= \mathbf{H}_e + \frac{\mathbf{W}_s\mathbf{x}_J^*}{\tau_s}. \end{aligned} \tag{8}$$

where superscript d represents up-link data phase. The estimate of reciprocal channel $\mathbf{H}_e$ can be improved by increasing the silence time τ_s of Bob. The distributions of $\widehat{\mathbf{H}}_e^d$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are $\widehat{\mathbf{H}}_e^d|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{\sigma^2}{N\tau_s})\mathbf{I}_N\right)$ and $\widehat{\mathbf{H}}_e^d|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{1}{N} + \frac{\sigma^2}{N\tau_s})\mathbf{I}_N\right)$, respectively. Furthermore, the time domain channel estimate of Eve is $\widehat{\mathbf{h}}_e^d = \mathbf{F}^H\widehat{\mathbf{H}}_e^d$, where $\mathbf{F}^H$ is the inverse FFT (IFFT). Thus, the distributions of $\widehat{\mathbf{h}}_e^d$ under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are $\widehat{\mathbf{h}}_e^d|\mathcal{H}_0 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{\sigma^2}{L\tau_s})\mathbf{I}_L\right)$ and $\widehat{\mathbf{h}}_e^d|\mathcal{H}_1 \sim \mathcal{CN}\left(\mathbf{0}, (\frac{1}{L} + \frac{\sigma^2}{L\tau_s})\mathbf{I}_L\right)$, respectively. For simplicity and without loss of generality, let σ_0^2 and σ_1^2 be the variances under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. For the proposed silence detector,

$$\sigma_0^2 = \frac{\sigma^2}{L\tau_s} \text{ and } \sigma_1^2 = \frac{1}{L} + \frac{\sigma^2}{L\tau_s}. \tag{9}$$

The maximum likelihood (ML) energy detector compares the norm of channel estimate $\widehat{\mathbf{h}}_e^d$ with the detection threshold η [37] as follows:

$$E \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta = L\left(\frac{\sigma_0^2\sigma_1^2}{\sigma_1^2 - \sigma_0^2}\right)\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right). \tag{10}$$

The detection threshold of the proposed detector by putting σ_0^2 and σ_1^2 from (9) in (10) is

$$\eta = \left(\frac{\sigma^2}{\tau_s}\right)\left(1 + \frac{\sigma^2}{\tau_s}\right)\ln\left(\frac{1 + \frac{\sigma^2}{\tau_s}}{\frac{\sigma^2}{\tau_s}}\right). \tag{11}$$

Note that the detection threshold of (11) minimizes the probability of detection error

$$\begin{aligned} P_E = \frac{1}{2}(P_F + P_M) &= \frac{1}{2}\exp\left(-\frac{\eta}{\sigma_0^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_0^2}\right)^k \\ &+ \frac{1}{2} - \frac{1}{2}\exp\left(-\frac{\eta}{\sigma_1^2}\right)\sum_{k=0}^{L-1}\frac{1}{k!}\left(\frac{\eta}{\sigma_1^2}\right)^k, \end{aligned} \tag{12}$$

under the binary hypotheses $\mathcal{H}_1$ and $\mathcal{H}_0$.

If hypothesis $\mathcal{H}_1$ is true, we have estimate $\hat{\mathbf{H}}_e^d$ in (8) and proceed to estimate the legitimate channel $\widehat{\mathbf{H}}_u^p$ in pilot phase for secure transmission. First, we estimate pilot phase contamination of Eve using $\hat{\mathbf{H}}_e^d$ and remove the contamination of Eve in pilot phase in (1). The estimate of pilot contamination from Eve and residue signal in pilot phase are

$$\widehat{\mathbf{Y}}_{pe} = \hat{\mathbf{H}}_e^d\mathbf{s}_p^T = \mathbf{H}_e\mathbf{s}_p^T + \frac{\mathbf{W}_s\mathbf{x}_J\mathbf{s}_p^T}{\tau_s} \text{ and} \tag{13}$$

$$\widehat{\mathbf{Y}}_{pu} = \mathbf{Y}_p - \widehat{\mathbf{Y}}_{pe} = \mathbf{H}_u\mathbf{s}_p^T + \mathbf{W} - \frac{\mathbf{W}_s\mathbf{x}_J\mathbf{s}_p^T}{\tau_s}, \tag{14}$$

respectively. The LS estimate of the channel from Bob to Alice using residue observation $\widehat{\mathbf{Y}}_{pu}$ is

$$\widehat{\mathbf{H}}_u = \widehat{\mathbf{Y}}_{pu}\frac{\mathbf{s}_p^*}{\|\mathbf{s}_p\|^2} = \mathbf{H}_u + \frac{\mathbf{W}\mathbf{s}_p^*}{\tau} - \frac{\mathbf{W}_s\mathbf{x}_J}{\tau_s}. \tag{15}$$

If hypothesis $\mathcal{H}_1$ is false, we search for the segments in data phase where Eve is silent in the next sub-section.

B. SILENT EVE DETECTION

If Eve remains silent during the silent period τ_s of Bob in data phase, Alice searches for the segment in data phase where Eve is silent to obtain decision directed estimate of the legitimate channel $\widehat{\mathbf{H}}_u$ using contaminated channel estimate of pilot phase in (2). The binary hypothesis $\mathcal{H}_0$ (silent Eve) and $\mathcal{H}_1$ (jamming Eve) from the observation matrix $\mathbf{Y}_d \in \mathcal{C}^{N\times\tau_d}$ at Alice to detect the silence of Eve is:

$$\begin{aligned} \mathcal{H}_0 : \mathbf{Y}_d &= \mathbf{H}_u\mathbf{s}_d^T + \mathbf{W}_d \\ \mathcal{H}_1 : \mathbf{Y}_d &= \mathbf{H}_u\mathbf{s}_d^T + \mathbf{H}_e\mathbf{s}_J^T + \mathbf{W}_d, \end{aligned} \tag{16}$$

where $\mathbf{W}_d \in \mathcal{C}^{N\times\tau_d}$ is the AWGN matrix. The elements of AWGN matrix $\mathbf{W}_d$ are i.i.d. with zero mean and variance σ^2. We use minimum description length (MDL) method for source enumeration to search for segment where Eve is

silent in the up-link data phase [15]. The sub-space based MDL method detects the number of source by estimating the second-order statistics (correlation matrix) and computing its eigen values.

Under $\mathcal{H}_0$, the proposed scheme estimates the payload data of Bob using contaminated pilot estimate in (2) as

$$\hat{\mathbf{s}}_d^T = (\hat{\mathbf{H}}_u^p)^H \mathbf{Y}_d = \mathbf{s}_d^T + \widetilde{\mathbf{w}}_d, \tag{17}$$

where $\widetilde{\mathbf{w}}_d = (\hat{\mathbf{H}}_e^p)^H \mathbf{H}_u \mathbf{s}_d + (\hat{\mathbf{H}}_u^p + \hat{\mathbf{H}}_e^p)^H \mathbf{W}_d$. Now, we obtain decision directed estimate of the legitimate channel using $\hat{\mathbf{s}}_d$ as follows:

$$\widehat{\mathbf{H}}_u^d = \frac{\mathbf{Y}_d \hat{\mathbf{x}}_d^*}{\tau_d} = \mathbf{H}_u + \frac{\mathbf{W}_d \hat{\mathbf{x}}_d^*}{\tau_d}, \tag{18}$$

where $\hat{\mathbf{x}}_d = \text{dec}(\hat{\mathbf{s}}_d)$. In the event of failure to detect the silence of Eve, Alice terminates the current transmission. Next, we design the precoder using the estimated legitimate channel for secure transmission.

IV. PRECODING FOR DOWNLINK DATA TRANSMISSION

The precoder (pre-equalizer) design $\mathbf{f} = \frac{\hat{\mathbf{H}}_u^d}{\|\hat{\mathbf{H}}_u^d\|}$ using reciprocal channel estimate in (15) or (18) minimizes information leakage to the active Eve. The amount of information leakage is proportional to the correlation between Eve's channel $\mathbf{H}_e$ and legitimate channel $\mathbf{H}_u$. In moderate and high SNR regime, little leakage significantly lowers secrecy capacity C_s of the legitimate channel. We address this problem by transmission of AN in null space of estimate of reciprocal channel [34]. Thus, fractions of the unit power η and $1-\eta$ are allocated for information and AN, respectively. In simulation section, we present impact of AN on the secrecy capacity of the legitimate nodes.

Let $\mathbf{z} = [z_1, z_2, \cdots, z_{N-1}]^T \sim \mathcal{CN}(\mathbf{0}, I_{N-1})$ be the i.i.d. Gaussian noise vector of length $N-1$. Alice transmits AN in the null space $\mathbf{V} = \text{null}(\hat{\mathbf{H}}_u^d)$ of the data-aided channel estimate $\hat{\mathbf{H}}_u^d$. Thus, $\sqrt{1-\eta}\mathbf{V}\mathbf{z}$ is AN in the null space of signal. The precoded information with AN in the null space of $\hat{\mathbf{H}}_u^d$ transmitted by Alice to Bob in down-link data phase is

$$\mathbf{p} = \underbrace{\sqrt{\eta}\,\mathbf{f}\,s}_{\text{information}} + \underbrace{\sqrt{(1-\eta)}\,\mathbf{V}\,\mathbf{z}}_{\text{AN}}. \tag{19}$$

The ergodic capacities of channels of Alice and Eve are

$$C = \mathbf{E}\left[\log_2(1 + \frac{\eta\|\mathbf{H}_u^H\mathbf{f}\|^2}{\sigma^2})\right] \text{ and}$$
$$C_e = \mathbf{E}\left[\log_2(1 + \frac{\eta\|\mathbf{H}_e^H\mathbf{f}\|^2}{(1-\eta)\|\mathbf{H}_e^H\mathbf{V}\,\mathbf{z}\|^2 + \sigma^2})\right], \tag{20}$$

respectively. The secrecy capacity of the link between Alice and Bob is $C_s = \max\{0, C - C_e\}$. Next, we present comparison of the present simulation and analytical results of the proposed method.

V. SIMULATION

Now, we evaluate the proposed successive contamination removal method to enhance the secrecy capacity of the channel of the legitimate nodes by mitigating the impact of PCA in pilot phase and jamming attack in data phase. In simulation setup, we consider model in Fig. 2. An OFDM system transmits signal over block fading frequency selective channel. We use Rayleigh fading channel of length $L = 16$, pilot length $\tau = 64$, silence symbols length $\tau_s = 40$ and data length $\tau_d = 40$. We evaluate secrecy capacity of the reverse reciprocal channel from Alice to Bob and NMSE of the channel estimates for two transmission strategies of an active Eve. In pilot phase, Eve initiates pilot contamination attack on Alice. In up-link data phase, we consider the scenarios, when Eve is silent (Sil.) or transmit jamming signal to impair Bob to Alice transmission. In up-link data phase, we consider a valid constellation and random noise denoted by data jamming (DJ) and noise jamming (NJ), respectively, as jamming signals.

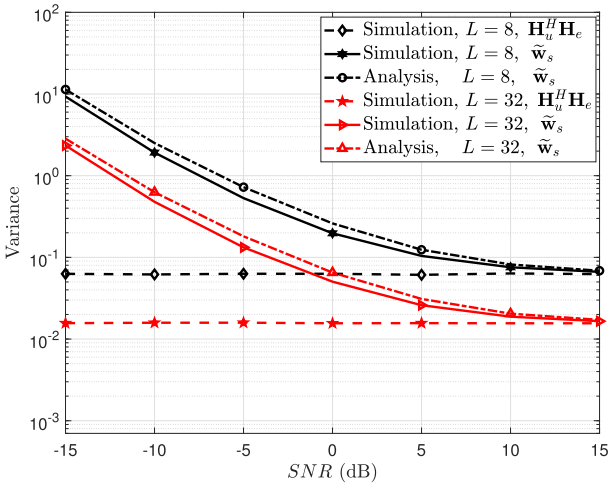


FIGURE 4. The comparison of variance of the $\boldsymbol{H_u^H H_e}$ and $\widetilde{\mathbf{w}}_s$.

Fig. 4 compares simulation results of $\tilde{\sigma}_s^2$ with the analysis in (6) for $L = 8$ and $L = 32$. Note that the small gap between the analytical and simulation of $\tilde{\sigma}_s^2$ is due to the approximation of gaussian distribution. Fig. 4 also shows that correlation term of $\mathbf{H}_u^H\mathbf{H}_e$ is the dominant term in moderate to high SNR regime. In high SNR regime, for small multi-path components, $\lim_{\sigma^2\to 0} \tilde{\sigma}_s^2 \to \frac{1}{2L}$. Consequently, BER and NMSE suffers from error floor. However, for large degrees of freedom L, $\|\mathbf{H}_u\| \to 1$ and $\mathbf{H}_u^H\mathbf{H}_e \to 0$.

Next, we investigate the statitsical distribution of correlation between legitimate channel $\mathbf{H}_u$ and $\mathbf{H}_e$ in Fig. 5. We present the comparison of probability density function (PDF) of real component $\mathcal{R}\{\mathbf{H}_u^H\mathbf{H}_e\}$ and normal fit using the MATLAB distribution fitting. Fig. 5 illustrates that Gaussian distribution appropriately fits the acquired correlation term. Next, we present the performance of coherent jamming signal estimate obtained in (7) in terms of bit error rate (BER). Fig. 6 shows that the decision-directed data estimate approaches the true jamming data. Thus, as SNR approaches 0 dB for large channel length, $\text{dec}(\widehat{\mathbf{s}}_J) \to \mathbf{s}_J$. It is also clear from Fig. 6 that BER suffers from error floor when the number of channel paths L are small. The error floor is a direct consequence of the correlation between legitimate and Eve's channels $\mathbf{H}_u$

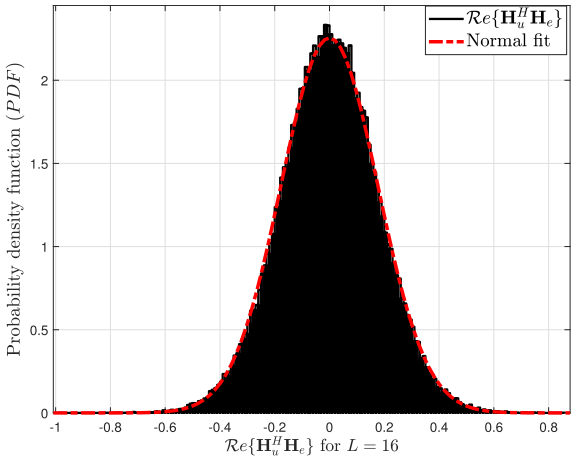


FIGURE 5. Distribution of real component $\mathcal{R}\{\mathbf{H}_e^H\mathbf{H}_u\}$ and normal fit using MATLAB distribution fitting.

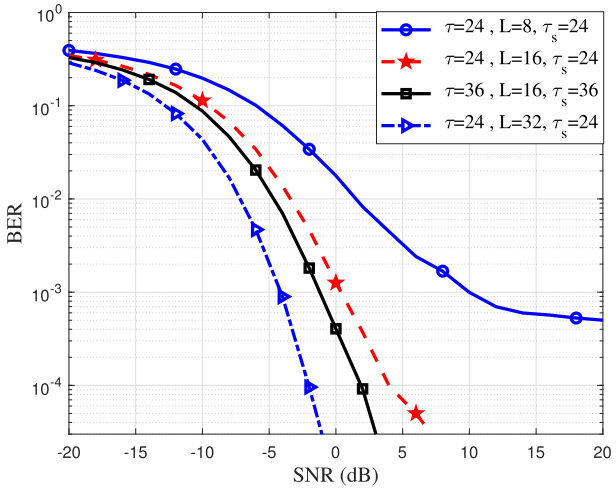


FIGURE 6. Bit Error Rate (BER) of hard decision jamming data estimate by varying pilot length τ, silence symbols length τ_s and varying degrees of freedom L.

and $\mathbf{H}_e$, respectively. The performance of decision-directed jamming data estimate directly impacts the performance of channel estimation method.

Fig. 7 presents NMSE of the channel estimate from Bob to Alice when Eve transmits NJ and DJ signals in up-link data phase in addition to PCA in pilot phase. The conventional method in Fig. 7 denotes the NMSE of the contaminated channel estimate in (2). Note that, due to equal transmit power of legitimate node and Eve, the NMSE suffers from severe performance degradation. Simulation results in Fig. 7 demonstrates that the proposed successive contamination removal approach effectively mitigates the effect of the pilot contamination and jamming in data phase. Note that estimate of channel from Bob to Alice is poor in the event of NJ due to the fact that Eve transmits random noise for jamming instead of constellation points. We also compare NMSE of channel estimate of the proposed method with method in [13], which uses auxiliary node. Fig. 7 shows that NMSE of our method without using auxiliary node is comparable to the method in [13].

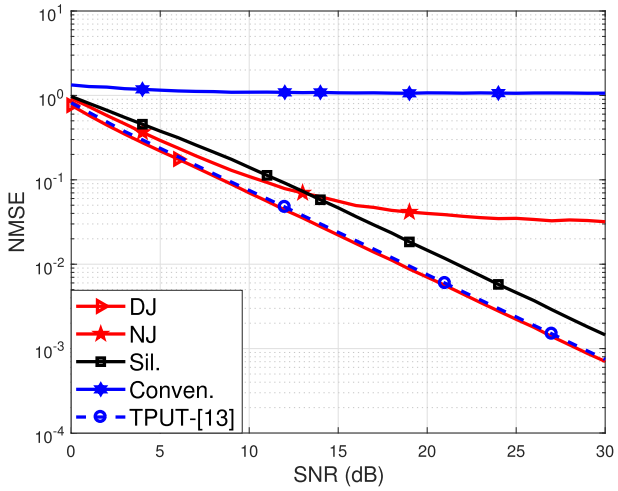


FIGURE 7. NMSE versus SNR for multiple Eve strategies.

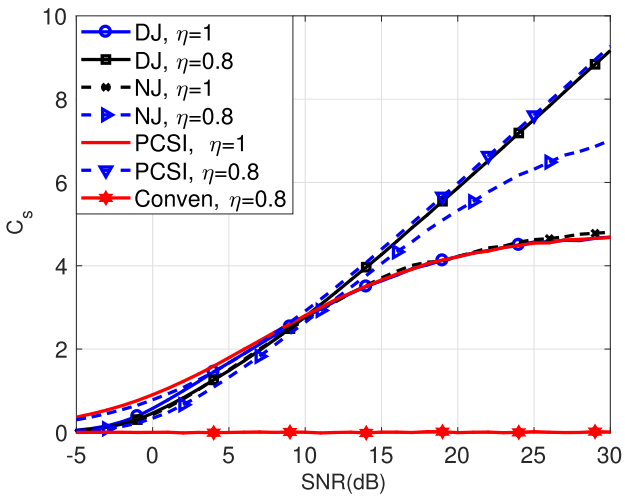


FIGURE 8. Secrecy capacity of the proposed method with variable power of AN.

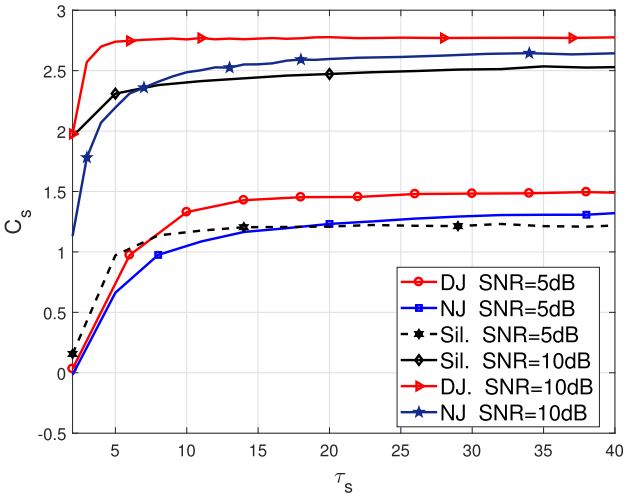


FIGURE 9. Impact of silent period τ_s on the secrecy capacity of legitimate channel.

Fig. 8 presents the efficacy of the proposed method and impact of AN on the secrecy capacity of the channel

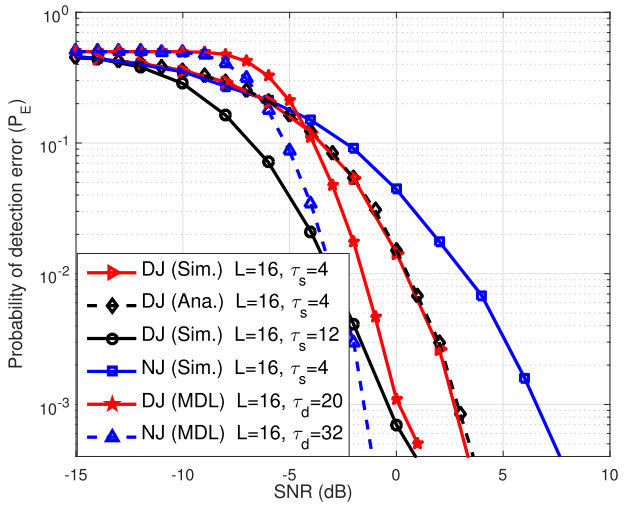


FIGURE 10. Probability of detection error P_E comparison of proposed detectors for channel length $L = 16$, pilot length $\tau = 4$ and variable silent length τ_S and data length τ_d.

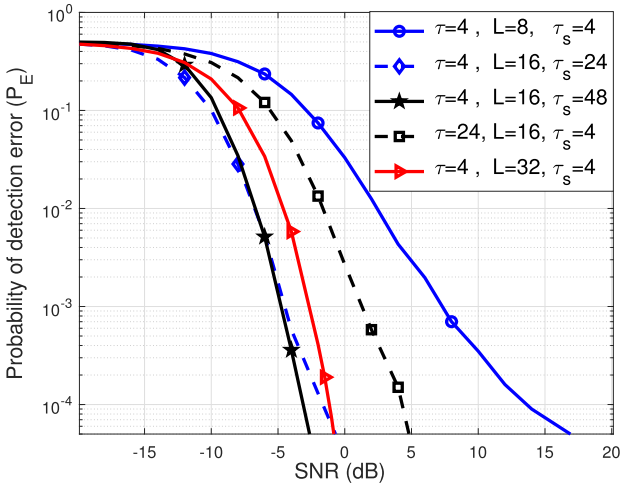


FIGURE 11. Probability of detection error P_E comparison of proposed detector for varying channel length L, varying pilot length τ and variable silent length τ_S.

between the legitimate nodes. The proposed successive contamination removal achieves significant enhancement in the secrecy capacity. The secrecy capacity of the conventional pilot assisted channel estimation approaches to zero due to equal transmit power of Alice and Eve over independent channels. The secrecy capacity with perfect CSI (PCSI) serves as benchmark. The secrecy capacity of the proposed method approaches the secrecy capacity with PCSI when Eve transmits DJ signals. The secrecy capacity of the legitimate nodes is poor under NJ due to poor channel estimate in Fig. 7. Fig. 8 also provides secrecy capacity of the proposed method with AN. The transmission of AN in the null space of the estimated legitimate channel significantly improves the secrecy capacity. Fig. 9 presents the impact of silence period τ_s of Bob in data phase on the secrecy capacity of the channel between Bob and Alice. Fig. 9 reveals that only limited number of silent symbols τ_s can offer significant performance improvement. It is clear from Fig. 9 that $\tau_s \leq 10$ achieves saturation of the secrecy capacity of the legitimate channel. Fig. 10 compares the analytical (12) and simulation results of the proposed active Eve detector under DJ when Bob is silent for τ_s period in data phase using the channel estimate in (8). The comparison reveals that simulation and analysis agree under DJ attack. We also observed that the performance of the proposed detector is poor for NJ as compared to the DJ. Fig. 10 also presents the performance of MDL based source enumerator to detect the silent period of Eve in the data phase, when Bob transmits data. It is clear from Fig. 10 that the proposed MDL detector can reliably detect the number of sources in low SNR regime. Furthermore, the performance the MDL and proposed ML detectors improves by increasing the number of silent symbols τ_s and payload symbols τ_d. Fig. 11 presents impact of degrees of freedom L, pilot length τ and silence period τ_s on the detection of Eve.

VI. CONCLUSION

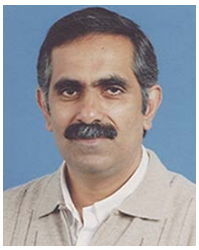
In this work, we presented the secure transmission and successive cancellation of contamination and jamming from Eve at physical layer of an OFDM system. The proposed successive contamination removal approach effectively mitigates the impact of PCA by exploiting observations of pilot and data phases. The precoder design from successive contamination removal based channel estimate substantially reduces information leakage to the Eve, which significantly enhances the secrecy capacity of channel of the legitimate nodes. We also observed that transmission of AN in null-space of legitimate channel for point-to-point link can also significantly improve the secrecy capacity of the legitimate channel.

REFERENCES

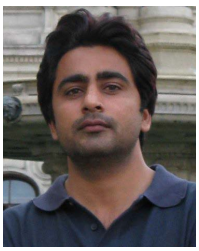
[1] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[3] J. D. V. Sanchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes, "Physical layer security for 5G wireless networks: A comprehensive survey," in *Proc. 3rd Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2019, pp. 122–129.
[4] W. Khalid, H. Yu, D.-T. Do, Z. Kaleem, and S. Noh, "RIS-aided physical layer security with full-duplex jamming in underlay D2D networks," *IEEE Access*, vol. 9, pp. 99667–99679, 2021.
[5] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.
[6] Y. L. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Net.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.
[7] 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.
[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[9] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.
[10] T.-Y. Liu, S.-C. Lin, and Y.-W. P. Hong, "On the role of artificial noise in training and data transmission for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 516–531, Mar. 2017.
[11] C. D. T. Thai, "Beamforming and jamming for physical-layer security with different trust degrees," *AEU Int. J. Electron. Commun.*, vol. 128, Jan. 2021, Art. no. 153458.

[12] 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.
[13] X. Liu, B. Li, H. Chen, Z. Sun, Y.-C. Liang, and C. Zhao, "Detecting pilot spoofing attack in MISO systems with trusted user," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 314–317, Feb. 2019.
[14] A. Santorsola, M. Zoli, A. N. Barreto, V. Petruzzelli, and G. Calo, "Effect of radio channel and antennas on physical-layer-security key exchange," *IEEE Access*, vol. 9, pp. 162175–162189, 2021.
[15] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.
[16] 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.
[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz) (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.
[18] P. Pasangi, M. Atashbar, and M. M. Feghhi, "Blind downlink channel estimation of multi-user multi-cell massive MIMO system in presence of the pilot contamination," *AEU Int. J. Electron. Commun.*, vol. 117, Apr. 2020, Art. no. 153099.
[19] A. A. Nasir, H. D. Tuan, H. H. Nguyen, and N. M. Nguyen, "Physical layer security by exploiting interference and heterogeneous signaling," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 26–31, Oct. 2019.
[20] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.
[21] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, "Physical layer security in cell-free massive MIMO," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[22] X. Zhang, D. Guo, K. An, and B. Zhang, "Secure communications over cell-free massive MIMO networks with hardware impairments," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1909–1920, Jun. 2020.
[23] J. Choi, J. Joung, and B. C. Jung, "Space–time line code for enhancing physical layer security of multiuser MIMO uplink transmission," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3336–3347, Sep. 2021.
[24] H. Jung and I.-H. Lee, "Distributed null-steering beamformer design for physical layer security enhancement in Internet-of-Things networks," *IEEE Syst. J.*, vol. 15, no. 1, pp. 277–288, Mar. 2021.
[25] A. Chorti, A. N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.
[26] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.
[27] W. Xu, C. Yuan, S. Xu, H. Q. Ngo, and W. Xiang, "On pilot spoofing attack in massive MIMO systems: Detection and countermeasure," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1396–1409, 2021.
[28] J. Qiu, K. Xu, X. Xia, Z. Shen, W. Xie, D. Zhang, and M. Wang, "Secure transmission scheme based on fingerprint positioning in cell-free massive MIMO systems," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 8, pp. 92–105, 2022.
[29] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmWave grant-free IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 658–670, 2021.
[30] K.-W. Huang and H.-M. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 345–359, Jan. 2021.
[31] X. Liu, Y. Tao, C. Zhao, and Z. Sun, "Detect pilot spoofing attack for intelligent reflecting surface assisted systems," *IEEE Access*, vol. 9, pp. 19228–19237, 2021.
[32] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[33] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.
[34] 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. 3380–3900, Jul. 2016.
[35] H. Akhlaghpasand, E. Bjornson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 1, pp. 182–186, Jan. 2020.
[36] X. Lu, W. Yang, Y. Cai, and X. Guan, "Proactive eavesdropping via covert pilot spoofing attack in multi-antenna systems," *IEEE Access*, vol. 7, pp. 151295–151306, 2019.
[37] A. Ahmed, M. Zia, I. U. Haq, and H.-D. Han, "Detection of pilot contamination attack for frequency selective channels," *IEEE Access*, vol. 8, pp. 123966–123978, 2020.

AWAIS AHMED (Student Member, IEEE) received the B.S. degree from the Center for Advanced Studies in Engineering (CASE) University, 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 a Professor.



NAEEM BHATTI (Member, IEEE) received the M.Sc. and M.Phil. degrees in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 2002 and 2004, respectively, and the Ph.D. degree in informatics from the Vienna University of Technology, Vienna, Austria, in 2012. He is currently with the Department of Electronics, Quaid-i-Azam University, as an Associate Professor.

HASAN MAHMOOD received the M.S. degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1991, the M.S. degree in electrical engineering from the University of Ulm, Germany, in 2002, and the Ph.D. degree in electrical engineering from the Stevens Institute of Technology, Hoboken, NJ, USA, in 2007. From 1994 to 2000, he was with the Department of Electronics, Quaid-i-Azam University, as a Faculty Member, where he is currently with the Department of Electronics as a Professor.

HUY-DUNG HAN (Member, IEEE) received the B.S. degree from the Faculty of Electronics and Telecommunications, Hanoi University of Science and Technology, Hanoi, 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 at Davis, Davis, in 2012. He is currently with the School of Electronics and Telecommunications, Department of Electronics and Computer Engineering, Hanoi University of Science and Technology. His research interests include the area of wireless communications and signal processing, with current emphasis on blind and semi-blind channel equalization for single and multi-carrier communication systems and convex optimization.