In-Band Full-Duplex Discriminatory Channel Estimation using MMSE

Fawad Ud Din, *Member, IEEE,* and Fabrice Labeau, *Senior Member, IEEE*

***Abstract*—This paper proposes full-duplex transmissions from legitimate nodes to achieve channel estimation performance deterioration at an eavesdropper as compared to the legitimate receiver. The proposed discriminatory channel estimation (DCE) technique comprises of two stages where, in the first stage, the self-interference channel is estimated by the respective legitimate nodes. Followed by in-band full-duplex transmission from both legitimate nodes for channel estimation at legitimate nodes, while providing equivocation at the eavesdropper due to the superposition of two signals. The discrimination of channel estimation performance provides secrecy against the passive eavesdropper while delivering information to the legitimate receiver. We provide the mean square error (MSE) to indicate the performance achieved by linear minimum mean square error (LMMSE) estimators. We have also provided bit error rate (BER), and secrecy capacity analysis to indicate the performance of secure communication achieved by securing the channel estimates from the eavesdropper. The BER analysis shows that for proposed DCE, BER at the eavesdropper is close to 0.1 while the legitimate node is able to robustly decode the information. Finally, simulation results show that the proposed DCE outperforms existing DCE techniques for the considered scenario.**

***Index Terms*—Channel Estimation, Physical Layer Security, Full-Duplex, Discriminatory Channel Estimation, MIMO, MSE, LS.**

I. Introduction

WIRELESS COMMUNICATIONS have been extensively utilized to provide access to remote locations. Wireless communications are also widely employed in smart homes, smart grids, and health-care monitoring networks. The broadcast nature of wireless communication has raised concerns regarding its security, and privacy. The security threats in wireless networks can result in significant damage, as their applications include many sensitive governmental, military, and commercial usage [1]. In current communications systems, the secrecy is provided by utilizing cryptographic techniques to encrypt the information which is implemented at the higher layers of the communication stack [2]. To combat the secrecy challenges at the lowest layer of the communication protocol stack, physical layer security (PLS) has been proposed which provides secure communication by utilizing the inherent randomness of wireless transmission media [3]. PLS should be utilized as an additional layer of security on top of the existing encryption techniques at higher layers [2], as the recent attacks have shown to overcome the existing encryption techniques to attack the wireless networks and eavesdrop on the users [4], [5]. Security threats in wireless communications are broadly classified into two categories: first, active attacks, where a malicious user jams, or injects false data into the legitimate communication. Second, passive attacks, where a malicious user passively eavesdrops on legitimate communication. The eavesdropping attacks are most prevalent in wireless communications due to its broadcast nature. In this paper, we will focus on eavesdropping attacks where a malicious user passively listens to the legitimate communication.

The majority of the existing PLS literature focuses on the study of the achievable secrecy rates from an information-theoretic perspective which requires channel state information (CSI) of the malicious user to either design appropriate secure channel codes [6], [7], or optimal beamforming design [8] for secure communication which is not possible for scenarios where the eavesdropper is passive. In the absence of CSI regarding the eavesdropper, artificial noise (AN) aided multi-antenna based PLS techniques [9], [10] provide a practical solution by transmitting AN orthogonal to the legitimate channel, the major drawback of AN based PLS techniques is their dependence on channel estimates [11], as robustness and secrecy of channel estimates is crucial as they can be utilized by the eavesdropper via known-plaintext attacks to cancel the AN signal [12]. To avoid the leakage of channel estimate to the malicious user, discriminatory channel estimation (DCE) has been utilized, through which channel estimation performance at the malicious users is intentionally degraded as compared to the legitimate receiver.

The most commonly used schemes to achieve DCE are feedback-and-retraining [13], and two-way training [14]. Feedback-and-retraining DCE consists of multiple stages, where, in the first stage, the power of the training signal is limited to allow the receiving nodes to acquire only rough estimates regarding the corresponding channels. This is followed by multiple retraining stages, where an AN-assisted training signal is utilized to further refine the channel estimates. This scheme ignores the possibility that the malicious receiver can acquire robust channel estimates in the first stage based on its channel characteristics. To overcome the leakage of channel estimates in the first channel estimation stage, two-way training is proposed in [14], where the legitimate receiver transmits the training signal instead of the legitimate transmitter in the first training stage; this scheme is well suited for the reciprocal channels. In the second stage, an AN-aided pilot signal is utilized to acquire channel estimates at the legitimate receiver. For non-reciprocal channels, in the second stage, the legitimate transmitter transmits a training signal known to itself only. The received signal at the legitimate receiver is re-transmitted

The authors are with the Department of Electrical and Computer Engineering, McGill University, Montréal, QC H3A-0G4, Canada (email: fawad.uddin@mail.mcgill.ca; fabrice.labeau@mcgill.ca). This work was supported by Hydro-Québec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/Hydro-Québec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14)

after amplification to acquire the forward channel estimates at the legitimate transmitter. Finally, AN-aided pilot signals are utilized to improve the channel estimates. Two-way training DCE is suitable for reciprocal channels, but for non-reciprocal channels it suffers from noise amplification [15]. As feedback-and-retraining [13], and two-way training [14] DCE utilize orthogonal AN signal to secure the transmission of pilot signal, they require that number of receive antennas at the legitimate node and the eavesdropper must be less than the number of transmit antennas at the legitimate transmitter, and the eavesdropping channel (between the legitimate transmitter and the eavesdropper) must be worse off than the legitimate channel (between legitimate nodes). These drawbacks make feedback-and-retraining DCE vulnerable to attack by an eavesdropper with a higher number of antennas or having better channel than the legitimate receiver. Different variations of these two DCE schemes are presented in [16]–[19], which suffer from the same drawbacks as mentioned for feedback-and-retraining, and two-way training DCE.

To overcome the drawbacks of AN based DCEs, the full-duplex system is also utilized to achieve DCE. Theoretical insights regarding the use of full-duplex communication for securing wireless communications is provided in [20], where the author has also presented the use of full-duplex transmissions to achieve DCE where, single full-duplex transmission is utilized to estimate the self-interference and intended channel simultaneously, and the residual self-interference is considered to be additive white Gaussian noise, which limits the estimation performance for the channel based on experimental characterizations of full-duplex channel [21] to the residual self-interference irrespective of the length or power of the training signal. In [20], only single antenna full-duplex devices are considered and it lacks the analysis on the effect of DCE on achievable secrecy performance. In [22], single antenna based full-duplex transmission is proposed to secure the leakage of channel estimates to the eavesdropper; however this system ignores the leakage of statistical information regarding the legitimate channel to the eavesdropper, which could be utilized to implement a more advanced estimator (i.e. Minimum Mean Square Error (MMSE) estimator) to estimate the corresponding channels. The use of single antenna-based transmission makes it bandwidth inefficient for multiple-input multiple-output (MIMO) systems.

To overcome the drawbacks of existing DCE schemes, we propose the utilization of full-duplex MIMO communication for securing the channel estimates, where the legitimate transmitter and receiver employ in-band full-duplex transmissions to estimate their respective channels while maintaining equivocation at the eavesdropper. The proposed DCE does not require any information regarding the eavesdropper as it is required by existing DCEs [13], [14]. The proposed channel estimation technique assumes channels between legitimate nodes to be non-reciprocal. It is bandwidth efficient as compared to other schemes because, instead of artificial noise, full-duplex transmission has been used to induce ambiguity at the eavesdropper while acquiring channel estimates at the legitimate nodes. The existing works for in-band full-duplex channel estimation have been presented in [23], [24], but the existing works are oblivious of the secrecy requirements to achieve discriminatory channel estimation performance at the eavesdropper as compared to the legitimate receiver.

A. Contributions and Outline

The proposed channel estimation technique comprises of two stages. The first stage is responsible for the estimation of the self-interference channel, as we have used the channel aware self-interference cancellation technique for full-duplex stage due to its superior performance as compared to channel unaware cancellation [21]. The legitimate nodes transmit orthogonal private random training signals using independent time slots. The orthogonality of the private training signal is also exploited by all the nodes to acquire statistical channel information regarding respective channels. In the second stage, both legitimate nodes simultaneously transmit known training signals to estimate the corresponding channels by utilizing a linear minimum mean square error (LMMSE) estimator while canceling the self-interference signal. The contributions of this work are:

- We present a novel DCE technique, which to the best of our knowledge, is the first practical DCE scheme which does not require any statistical information regarding the passive eavesdropper's channel, and also do not restrict the number of receive antennas at the legitimate receiver. This is in contrast with existing DCE techniques which require that the number of receive antennas at the legitimate receiver to be less than the number of transmit antennas, and in which statistical information regarding the eavesdropper's channel is used in allocating the power to the training signal [13], [14], [25]. For the number of antennas at the eavesdropper, we have provided the simulation analysis to indicate that, for the given channel model, increasing the number of eavesdropping antennas does not improve the Bit Error Rate (BER) required for robust communication.
- For the proposed DCE, we present the secure channel estimation for a multiple antenna system, in which orthogonal private pilot signals have been designed to be transmitted simultaneously from multiple antennas while keeping them secret from the eavesdropper. In this paper, the length of the training signal is limited to the minimum, which prevents the leakage of channel estimates by blind channel estimation at the eavesdropper, particularly in the first stage. Lastly, multiple antenna system has been utilized for the derivation of the performance metrics, which increases the complexity of the presented analysis.
- In this paper, we present an in-depth analysis of proposed full-duplex aided discriminatory channel estimation. Half-duplex transmissions are utilized for the data transmission stage to indicate the secrecy performance achieved while the legitimate receiver is not transmitting. We have provided the secrecy capacity analysis that can be achieved by using the proposed discriminatory channel estimation. Simulation analysis has been provided to indicate the secrecy performance achieved by exploiting state of the art blind channel estimation technique at

the eavesdropper. Lastly, for the first time, we have provided a quantitative comparison against existing DCE techniques, which shows that the proposed DCE achieves better secrecy while consuming less power.

The rest of this paper is organized into five sections. Section II provides the system model considered for the proposed DCE. Section III explains the proposed DCE. Sections IV, and V presents the detailed performance analysis. Finally, the conclusion of this research is presented in Section VI. This paper follows the usual convention of notation, where vectors are denoted by lowercase boldface letters, and matrices are denoted by uppercase boldface letters. $\mathbb{E}[.]$ represents expectation operator, $(.)^H$ represents conjugate transpose, $\boldsymbol{I}_n$ corresponds to $n \times n$ identity matrix, $j = \sqrt{-1}$ is the imaginary unit, and $|.|$ is the determinant operator. $\boldsymbol{R_X}$ represents covariance of random matrix $\boldsymbol{X}$ which is defined as: $\boldsymbol{R_X} = \mathbb{E}\left[\boldsymbol{X}\boldsymbol{X}^H\right]$. The notation $[x]^+$ mean $\max(x, 0)$. These notations will be followed throughout this paper.

II. System Model

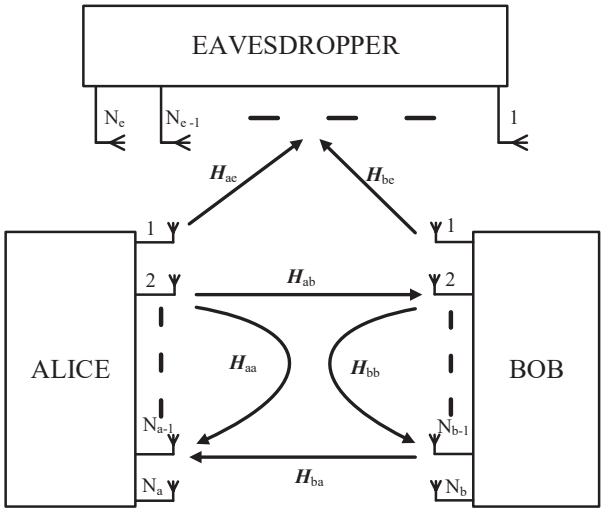

Fig. 1. Basic channel model utilized for proposed DCE technique, comprising of multiple antenna full-duplex legitimate transmitter, legitimate receiver, and the eavesdropper, where legitimate transmitter and receiver are commonly known as Alice, and Bob, respectively.

Consider a MIMO system comprising of two legitimate users, Alice, and Bob, along with a passive eavesdropper with N_e receive antennas as shown in Fig. 1. Legitimate nodes are assumed to be full-duplex nodes with N_a, and N_b full-duplex antennas at Alice and Bob, respectively. All full-duplex antennas simultaneously transmit and receive signals by using circulator switches as shown in [26]. All channels are assumed to be non-reciprocal wireless channels, meaning forward and reserve channel fading coefficients are independent, where channels between Alice, and Bob are denoted as $\mathbf{H}_{ab} \in \mathbb{C}^{N_a \times N_b}$, and $\mathbf{H}_{ba} \in \mathbb{C}^{N_b \times N_a}$. The eavesdropping channels are $\mathbf{H}_{ae} \in \mathbb{C}^{N_a \times N_e}$ between Alice, and the eavesdropper, and $\mathbf{H}_{be} \in \mathbb{C}^{N_b \times N_e}$ between Bob, and the eavesdropper. All the inter-node channels $\mathbf{H}_{ab}, \mathbf{H}_{ba}, \mathbf{H}_{ae}$, and $\mathbf{H}_{be}$ are assumed to undergo block Rayleigh fading with respective variances $\sigma^2_{ab}, \sigma^2_{ba}, \sigma^2_{ae}, \sigma^2_{be}$ given by the simplified path-loss model described in [27]. The flat fading assumption generalizes to the utilization of multi-carrier modulation technique, like Orthogonal Frequency Division Multiplexing (OFDM) under frequency selective fading environments, as long as the length of the cyclic prefix (CP) is greater than the delay spread of the channel. In this paper, all nodes are assumed to be static. Proposed DCE can also be applied to achieve physical layer security for mobile nodes given in [28], as proposed DCE utilizes a minimum length of training sequence it can be easily adapted for application to mobile nodes with minimal overhead. For mobile nodes, short coherence time due to mobility of the nodes will also provide better protection against blind channel estimation attacks on proposed DCE.

The self-interference channels are denoted as $\mathbf{H}_{bb} \in \mathbb{C}^{N_b \times N_b}$, and $\mathbf{H}_{aa} \in \mathbb{C}^{N_a \times N_a}$. The self-interference channels correspond to residual self-interference after analog cancellation. Full-duplex devices are assumed to share an oscillator for the transmitter, and receiver radio frequency (RF) chains, as both of them are on the same full-duplex device. For analog cancellation, the self-interference cancellation signal is taken from the output of Power Amplifier at the transmitter and subtracted at the input of Low Noise Amplifier at the receiver as given in [26]. The use of analog cancellation along with a shared oscillator removes non-linear transmitter and receiver impairments below the noise floor, where the main part of the residual self-interference signal is linear [29]. Finally, these residual self-interference channels $\mathbf{H}_{bb}$, and $\mathbf{H}_{aa}$ are modeled as block Rayleigh fading channel as given by experimental characterization of the self-interference channel in [21]. This is a widely adopted channel model for the self-interference channel in the full-duplex based physical layer security systems [25], [30]. As we have considered passive eavesdropper, any information regarding the eavesdropper's channel is not available at the legitimate nodes. Existing works on DCE assume the availability of some statistical information regarding the eavesdropper's channel at legitimate nodes, which is impractical for passive eavesdropping scenarios [13], [14], [25].

This paper assumes that timing synchronization is achieved by using existing state of the art timing and frequency synchronization techniques for full-duplex communication as given in [31]–[33], where the residual synchronization offset degrades the signal to interference plus noise ratio by 1 dB as given in [32]. To model the performance degradation due to the synchronization offset, we have increased the variance of the noise added at the receiver by 1 dB. The total duration of each block length is assumed to be T symbols comprised of two training stages T_1, T_2, and a data transmission stage T_d. All the transmission symbols are taken M-ary Quadrature Amplitude Modulation (QAM). For the data transmission stage, we have considered half-duplex transmission, where only Alice transmits the data while Bob passively receives the signal transmitted by Alice. The half-duplex data transmission signifies an easier scenario for the eavesdropping as it represents secrecy performance of the proposed DCE without any interference, jamming, or artificial noise in the

data transmission stage. It also represents a practical scenario, where Alice has data to be transmitted while Bob does not have any data ready for transmission.

III. Proposed Channel Estimation Technique

A. First Stage

The first stage of the proposed channel estimation is responsible for the estimation of self-interference channels, to be utilized in the later stage for cancellation of the self-interference signal. A private random training signal, known to the transmitting node only, is transmitted to estimate the respective self-interference channels by both legitimate nodes. Pilot based channel estimation technique is utilized for estimation as transmitter and receiver RF chains are on the same full-duplex device. Independent time slots have been utilized for transmission of private training signal by both nodes to avoid the interference from each other, which implies that Alice remains silent while Bob is transmitting, and vice versa. The length of the first stage is $T_1 = T_a + T_b$, where T_a and T_b is the length of the training sequence transmitted by Alice and Bob, respectively. To utilize the bandwidth efficiently, the length of the training sequence is kept to the minimum such that $T_a = N_a$, and $T_b = N_b$, where all the antennas transmit simultaneously, so that the number of received training symbols is equal to the number of variables to be estimated [34]. To generalize to frequency selective fading with OFDM transmissions, the minimum length of training signal must be equal to the delay spread times the number of antennas as given in [35]. The estimation process is same for both legitimates nodes, so we will describe the steps and performance for Bob, same steps and results are valid for Alice.

To design a private training signal at Bob, a random $N_b \times N_b$ matrix $\mathbf{X}$ is generated, which is then orthogonalized by using Gram-Schmidt process [36] to get $\boldsymbol{X}_{sb}$, where $\boldsymbol{X}_{sb}^H \boldsymbol{X}_{sb} = \boldsymbol{I}_{N_b}$, because $\boldsymbol{X}_{sb}$ is a unitary matrix[1]. The orthogonality of the training signal cancels the interference caused by multiple transmit antennas, while the randomness of the training sequence keeps it private from the eavesdropper.

The received signal $\boldsymbol{Y}_{si} \in \mathbb{C}^{N_b \times N_b}$ at Bob for self-inference channel estimation is given as:

$$\boldsymbol{Y}_{si} = \boldsymbol{X}_{sb}\boldsymbol{H}_{bb} + \boldsymbol{W}_{si}, \tag{1}$$

where $\boldsymbol{X}_{sb}$ is a $N_b \times N_b$ full-rank matrix representing the private random training signal used in the first stage, $\boldsymbol{H}_{bb}$ is the corresponding residual self-interference channel, and $\boldsymbol{W}_{si}$ is zero mean circularly symmetric white Gaussian noise (ZMCSWGN) with $\sigma_{si}^2 \boldsymbol{I}_{N_b}$ variance.

As the signal $\boldsymbol{X}_{sb}$ is orthogonal, it can also be utilized to estimate the variance σ_{bb}^2 of the channel $\boldsymbol{H}_{bb}$. Hence, the LMMSE criterion [37] is employed for channel estimation as:

$$\hat{\boldsymbol{H}}_{bb} = \sigma_{bb}^2 \mathbf{X}_{sb}^H \left(\sigma_{bb}^2 \mathbf{X}_{sb}\mathbf{X}_{sb}^H + \sigma_{si}^2 \mathbf{I}_{N_b}\right)^{-1} \mathbf{Y}_{si}, \tag{2}$$

$$\triangleq \boldsymbol{H}_{bb} + \Delta\hat{\boldsymbol{H}}_{bb}, \tag{3}$$

[1]Alice utilizes the same process as Bob to generate the private training signal used in the first stage, where a random $N_a \times N_a$ matrix is generated at Alice, which is orthogonalized to get private training signal $\boldsymbol{X}_{sa}$.

where $\Delta\hat{\boldsymbol{H}}_{bb}$ is the self-interference channel estimation error.

During the first stage, the signal received from Bob at the eavesdropper is given as:

$$\boldsymbol{Y}_{e1} = \boldsymbol{X}_{sb}\boldsymbol{H}_{be} + \boldsymbol{W}_{ei}, \tag{4}$$

where $\boldsymbol{H}_{be}$ is the channel between Bob-eavesdropper, and $\boldsymbol{W}_{ei}$ is ZMCSWGN with $\sigma_{ei}^2 \boldsymbol{I}_{N_b}$ variance. In contrast to [22], the eavesdropper can acquire the variance of the Alice-eavesdropper channel σ_{ae}^2 and the Bob-eavesdropper channel σ_{be}^2 by using the orthogonality of the private training signal $\boldsymbol{X}_{sb}$. The knowledge of channel variance at the eavesdropper enables it to utilize the LMMSE channel estimation criterion in the subsequent stages. As the pilot sequence is kept private from Alice and the eavesdropper, the eavesdropper can only rely on blind channel estimation techniques [38], [39]. The number of symbols received at the eavesdropper is critical for the use of blind channel estimation techniques, as their performance deteriorates with the decrease in the number of observed symbols [22], [38], [39], such that the normalized MSE is close to 1 for the case where the number of received symbols equal to the number of unknown channel coefficients. As in this research, we have kept the length of the private training signal equal to the number of unknown channel coefficients, hence it makes blind channel estimation techniques inoperable on the signal received at the eavesdropper in the first stage.

B. Second Stage

In the second stage, inter-node channels are estimated while utilizing the self-interference channel information from the first stage to cancel the self-interference signal. As the nodes are synchronized, both legitimate nodes simultaneously start transmitting the known training signals using in-band full-duplex transmissions. At the eavesdropper, channel estimation performance is degraded due to the superposition of two training signals transmitted from the legitimate nodes. As in the previous stage, the length of the training sequence should be kept equal to the number of receive antennas, to minimize the leakage of channel estimates, but the length of the training signal in the second stage is set to $T_2 = \max\{N_a, N_b\}$, to assure that the reception at the eavesdropper is completely superimposed by two signals.

The training sequences are designed to be orthogonal to different transmit antennas on each node. The orthogonal training signal is achieved by using a circularly shifted training signal at different antennas. The training signal transmitted from Alice is given by $\boldsymbol{X}_a$, where its (i,k)th component is given as:

$$[\boldsymbol{X}_a]_{i,k} = \sqrt{\frac{1}{T_2}} e^{-j2\pi(k-1)i/N_a}, \tag{5}$$

where, $\boldsymbol{X}_a^H \boldsymbol{X}_a = \boldsymbol{I}_{N_a}$. Similarly, the training signal transmitted from Bob is denoted as $\boldsymbol{X}_b$, where $[\boldsymbol{X}_b]_{i,k} = \sqrt{1/T_2} e^{-j2\pi(k-2)i/N_b}$. The training signal can also be generated using other orthogonalization techniques like, Gram-Schmidt process as mentioned in the first stage. Finally, the received signal at Bob in the second stage is given as:

$$\boldsymbol{Y}_b = \boldsymbol{X}_a\boldsymbol{H}_{ab} + \boldsymbol{X}_b\boldsymbol{H}_{bb} + \boldsymbol{W}_b, \tag{6}$$

where $\boldsymbol{H}_{ab}$ denotes the channel between Alice-Bob, and $\boldsymbol{W}_b$ is the ZMCSWGN with i.i.d. entries that are drawn from $\mathcal{CN}\left(\mathbf{0}, \sigma_b^2 \boldsymbol{I}_{T_2}\right)$. After performing digital SI cancellation based on channel estimates $\hat{\boldsymbol{H}}_{bb}$ obtained in the first stage, the resultant received signal is given as:

$$\boldsymbol{Y} = \boldsymbol{X}_a \boldsymbol{H}_{ab} + \boldsymbol{X}_b \Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b, \tag{7}$$

$$= \boldsymbol{X}_a \boldsymbol{H}_{ab} + \boldsymbol{W}, \tag{8}$$

where $\Delta\hat{\boldsymbol{H}}_{bb}$ corresponds to the estimation error as given in (3), and $\boldsymbol{W} = \boldsymbol{X}_b \Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b$ is the corresponding residual interference plus noise signal. In order to estimate the channel $\boldsymbol{H}_{ab}$, Bob uses the LMMSE criterion given in [37] as the corresponding channel and noise variances are available. The LMMSE estimator for channel $\boldsymbol{H}_{ab}$ is given as:

$$\hat{\boldsymbol{H}}_{ab} = \sigma_{ab}^2 \boldsymbol{X}_a^H \left(\sigma_{ab}^2 \boldsymbol{X}_a \boldsymbol{X}_a^H + \boldsymbol{R}_{\boldsymbol{W}}\right)^{-1} \boldsymbol{Y}, \tag{9}$$

where $\boldsymbol{R}_{\boldsymbol{W}} = \mathbf{E}\left[\mathbf{W}\mathbf{W}^{\mathbf{H}}\right]$ corresponds to the covariance of matrix $\boldsymbol{W}$. Using the independence between the estimation error in the first stage and the noise added in the second stage, $\boldsymbol{R}_{\boldsymbol{W}}$ is given as:

$$\boldsymbol{R}_{\boldsymbol{W}} = \mathbf{E}\left[\mathbf{X_b}\boldsymbol{\Delta}\hat{\mathbf{H}}_{\mathbf{bb}}(\boldsymbol{\Delta}\hat{\mathbf{H}}_{\mathbf{bb}})^{\mathbf{H}}\mathbf{X}_{\mathbf{b}}^{\mathbf{H}}\right] + \sigma_{\mathbf{b}}^{\mathbf{2}}\mathbf{I}, \tag{10}$$

$$= \left(\frac{N_b}{T_2} MSE_1 + \sigma_b^2\right) \boldsymbol{I}_{T_2} \tag{11}$$

where $\boldsymbol{X}_b \boldsymbol{X}_b^H = (N_b/T_2)\boldsymbol{I}_{T_2}$, and MSE_1 corresponds to the variance of the estimation error in the first stage at Bob given as:

$$MSE_1 = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\}]}{N_b^2}. \tag{12}$$

Finally using the orthogonality of training signal $\boldsymbol{X_a}\boldsymbol{X_a}^H = (N_a/T_2)\boldsymbol{I}_{T_2}$, the above equation (9) can be simplified as:

$$\hat{\boldsymbol{H}}_{ab} = \frac{\sigma_{ab}^2}{(N_a\sigma_{ab}^2 + N_b MSE_1)/T_2 + \sigma_b^2} \boldsymbol{X}_a^H \boldsymbol{Y}, \tag{13}$$

$$\triangleq \boldsymbol{H}_{ab} + \Delta\hat{\boldsymbol{H}}_{ab}, \tag{14}$$

where $\Delta\hat{\boldsymbol{H}}_{ab}$ is the inter-node channel estimation error.

At the eavesdropper, the received signal in the second stage is given as:

$$\boldsymbol{Y}_e = \boldsymbol{X}_a \boldsymbol{H}_{ae} + \boldsymbol{X}_b \boldsymbol{H}_{be} + \boldsymbol{W}_e, \tag{15}$$

where $\boldsymbol{H}_{ae}$ is the channel between Alice and the eavesdropper, and $\boldsymbol{H}_{be}$ denotes the channel between Bob, and the eavesdropper, and $\boldsymbol{W}_e$ is ZMCSWGN drawn from $\mathcal{CN}\left(\mathbf{0}, \sigma_e^2 \boldsymbol{I}_{T_2}\right)$. The eavesdropper can take advantage of the signal-to-noise ratio (SNR) disparity between the signals received from Alice and Bob to acquire the channel estimates, as the pilot signals are known globally. Interference Cancellation (IC) can be applied to acquire the estimates of the channel with higher receive SNR while considering the weaker signal as interference [40]. The SNR between Alice and the eavesdropper is denoted as SNR_A, and SNR between Bob and the eavesdropper is denoted as SNR_B. Without loss of generality[2], we assume that $SNR_A > SNR_B$ which implies that the eavesdropper is closer to the legitimate transmitter Alice, as compared to Bob. Therefore, the eavesdropper can acquire the estimate of $\boldsymbol{H}_{ae}$ by considering $\boldsymbol{Z} = \boldsymbol{X}_b \boldsymbol{H}_{be} + \boldsymbol{W}_e$ as interference plus noise signal in the above equation (15). By applying the LMMSE criterion, the eavesdropper can obtain the estimate of $\boldsymbol{H}_{ae}$ as:

$$\hat{\boldsymbol{H}}_{ae} = \sigma_{ae}^2 \boldsymbol{X}_a^H \left(\sigma_{ae}^2 \boldsymbol{X}_a \boldsymbol{X}_a^H + \boldsymbol{R}_{\boldsymbol{Z}}\right)^{-1} \boldsymbol{Y}_e, \tag{16}$$

where $\boldsymbol{R}_{\boldsymbol{Z}} = \mathbb{E}\left[\boldsymbol{Z}\boldsymbol{Z}^H\right]$ corresponds to the correlation of interference plus noise signal denoted as $\boldsymbol{Z}$. By exploiting the independence between channel $\boldsymbol{H}_{be}$ and the additive noise $\boldsymbol{W}_e$, the above equation can be simplified as:

$$\hat{\boldsymbol{H}}_{ae} = \frac{\sigma_{ae}^2}{(N_a\sigma_{ae}^2 + N_b\sigma_{be}^2)/T_2 + \sigma_e^2} \boldsymbol{X}_a^H \boldsymbol{Y_e}, \tag{17}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}. \tag{18}$$

To further improve the accuracy of channel estimates, the eavesdropper can use the blind channel estimation techniques during the data transmission stage. As Alice uses space-time block codes to transmit the information, the eavesdropper can utilize blind channel estimation techniques given in [39], [41], [42], but all of these blind estimation techniques require cooperation from the transmitter, as the channel rotation ambiguities cannot be solved without assistance from the transmitter.

IV. Performance Analysis of Proposed Channel Estimation Technique

A. Mean Square Error

MSE is utilized to analyze the performance of the proposed discriminatory channel estimation technique.

1) At Bob: The MSE for the first stage is given as:

$$MSE_1 = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\}]}{N_b^2}, \tag{19}$$

as N_b^2 corresponds to the number of channel coefficients estimated. Error correlation matrix $\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\}$ is given in [37] as:

$$\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\} = \left(\boldsymbol{R}_{\boldsymbol{H}_{bb}}^{-1} + \boldsymbol{X}_{sb}^H \boldsymbol{R}_{\boldsymbol{W}_{si}}^{-1} \boldsymbol{X}_{sb}\right)^{-1}, \tag{20}$$

where $\boldsymbol{R}_{\boldsymbol{H}_{bb}}$ is the covariance of the channel $\boldsymbol{H}_{bb}$, and $\boldsymbol{R}_{\boldsymbol{W}_{si}}$ is the noise covariance matrix. Using the error correlation matrix given in (20), MSE_1 can be simplified as:

$$MSE_1 = \left(\frac{1}{\sigma_{bb}^2} + \frac{1}{\sigma_{si}^2}\right)^{-1}. \tag{21}$$

MSE for $\hat{\boldsymbol{H}}_{ab}$ using the error correlation matrix from [37] is given as:

$$MSE_2 = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ab}(\Delta\hat{\boldsymbol{H}}_{ab})^H\}]}{N_a N_b}, \tag{22}$$

$$= \frac{N_b \mathrm{Tr}\left[\left(\frac{1}{\sigma_{ab}^2}\boldsymbol{I}_{N_a} + \left(\frac{1}{\sigma_b^2 + MSE_1}\right)\boldsymbol{X}_a^H \boldsymbol{X}_a\right)^{-1}\right]}{N_a N_b},$$

$$= \left(\frac{1}{\sigma_{ab}^2} + \frac{1}{\sigma_b^2 + MSE_1}\right)^{-1}. \tag{23}$$

[2]This assumption implies that the eavesdropper strategically locates itself closer to the legitimate transmitter (Alice) than the legitimate receiver (Bob), such that the signal received from Alice is stronger than the signal received from Bob at the eavesdropper.

2) At the eavesdropper: MSE is calculated to evaluate the performance of IC based LMMSE estimation. Based on assumption that $SNR_A > SNR_B$, MSE for $\hat{\boldsymbol{H}}_{ae}$ is given as:

$$MSE_e = \frac{\text{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ae}(\Delta\hat{\boldsymbol{H}}_{ae})^H\}]}{N_a N_e}, \tag{24}$$

$$= \frac{\text{Tr}\left[\frac{1}{\sigma_{ae}^2}\boldsymbol{I}_{N_a} + \left(\frac{1}{\sigma_{be}^2+\sigma_e^2}\right)\boldsymbol{X}_a^H\boldsymbol{X}_a\right]}{N_a}, \tag{25}$$

$$= \left(\frac{1}{\sigma_{ae}^2} + \frac{1}{\sigma_{be}^2+\sigma_e^2}\right)^{-1}. \tag{26}$$

The above equation shows the normalized MSE at each antenna of the eavesdropper. It also indicates that the MSE is dependent on the variance of the weaker signal along with the noise added to the system. It can also be observed from the above equation that, the normalized MSE at each receive antenna of the eavesdropper is independent of the number of antennas at the eavesdropper (N_e) so that a more equipped eavesdropper does not provide any advantage during the channel estimation at the eavesdropper.

B. Secrecy Capacity

Secrecy capacity is utilized as a performance metric to analyze the secrecy of communication, it is vastly utilized in PLS literature as the performance metric. Secrecy capacity is given as [2]:

$$C_s = C_b - C_e, \tag{27}$$

where C_b, and C_e corresponds to the channel capacity at Bob and the eavesdropper, respectively.

For data transmission stage, we considered half-duplex communication where Alice transmits the signal which is received by Bob and Eve as:

$$\boldsymbol{Y}_b^d = \boldsymbol{X}_d\boldsymbol{H}_{ab} + \boldsymbol{W}_b^d, \tag{28}$$

$$\boldsymbol{Y}_e^d = \boldsymbol{X}_d\boldsymbol{H}_{ae} + \boldsymbol{W}_e^d, \tag{29}$$

where $\boldsymbol{X}_d \in \mathbb{C}^{T_d\times N_a}$ are data symbols transmitted from Alice, and $\boldsymbol{W}_b^d$, and $\boldsymbol{W}_e^d$ denote ZMCSWGN with variance σ_{bd}^2, and σ_{ed}^2 at Bob, and the eavesdropper, respectively. Half-duplex transmission represents an easier scenario for the eavesdropper than a full-duplex case because, in half-duplex, the eavesdropper receives only one signal from Alice while Bob remains silent. Half-duplex data transmission stage also corresponds to the practical scenario where Bob does not have any data to transmit, as there is no guarantee that Alice and Bob will always have the same amount of data to transmit. To derive the channel capacity at Bob and the eavesdropper, we will first calculate the mutual information at each node so that channel capacity can be achieved by maximizing the mutual information. Mutual information for the given scenario, where the perfect channel state information is not available, can be written as [43]:

$$I(\boldsymbol{X}_d;\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) = h(\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) - h(\boldsymbol{Y}_b^d|\boldsymbol{X}_d,\hat{\boldsymbol{H}}_{ab}), \tag{30}$$

where $h(.)$ indicates the respective mutual entropies, and $\hat{\boldsymbol{H}}_{ab} = \boldsymbol{H}_{ab} + \Delta\hat{\boldsymbol{H}}_{ab}$ is the estimated channel. For simplicity in the derivation of channel capacity, we have assumed the transmitted signal $\boldsymbol{X}_d$ to be Gaussian distributed. Hence, $h(\boldsymbol{X}_b^d|\hat{\boldsymbol{H}}_{ab})$ is given as:

$$h(\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) \leq \mathbb{E}\left[\log_2|\pi e\boldsymbol{R}_{\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}}|\right], \tag{31}$$

where $\boldsymbol{R}_{\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}}$ corresponds to the covariance of $\left(\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}\right)$. The estimation error $\Delta\hat{\boldsymbol{H}}_{ab}$ for LMMSE estimator is known to be orthogonal to estimate $\hat{\boldsymbol{H}}_{ab}$ [37], hence the above equation can be simplified as:

$$h(\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) = \mathbb{E}\Big[\log_2\Big|\pi e\big(\hat{\boldsymbol{H}}_{ab}\boldsymbol{Q}\hat{\boldsymbol{H}}_{ab}^H + \big(\sigma_{bd}^2 + MSE_2P\big)\boldsymbol{I}_{N_a}\big)\Big|\Big], \tag{32}$$

where $\boldsymbol{Q} = \mathbb{E}\left[\boldsymbol{X}_d^H\boldsymbol{X}_d\right]$, and P indicates the total power available for data transmission.. Similarly, $h(\boldsymbol{Y}_b^d|\boldsymbol{X}_d,\hat{\boldsymbol{H}}_{ab})$ is given as:

$$h(\boldsymbol{Y}_b^d|\boldsymbol{X}_d,\hat{\boldsymbol{H}}_{ab}) \leq \mathbb{E}\left[\log_2|\pi e\left(\sigma_{bd}^2 + MSE_2P\right)\boldsymbol{I}_{N_a}|\right]. \tag{33}$$

By combining the above equations (32), and (33), we get:

$$I(\boldsymbol{X}_d;\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) = \mathbb{E}\left[\log_2\left|\boldsymbol{I}_{N_a} + \frac{\hat{\boldsymbol{H}}_{ab}\hat{\boldsymbol{H}}_{ab}^H\boldsymbol{Q}}{\sigma_{bd}^2 + MSE_2P}\right|\right]. \tag{34}$$

Using Singular Value Decomposition (SVD) for decoding in MIMO channels [43], the above equation can be expressed as:

$$I(\boldsymbol{X}_d;\boldsymbol{Y}_b^d|\hat{\boldsymbol{H}}_{ab}) = \mathbb{E}\left[\log_2\left|\boldsymbol{I}_{N_a} + \frac{\boldsymbol{\Lambda}\boldsymbol{Q}}{\sigma_{bd}^2 + MSE_2P}\right|\right], \tag{35}$$

where $\boldsymbol{\Lambda}_{ab} = \text{diag}\left(\lambda_{ab}^{(1)},\ldots,\lambda_{ab}^{(N_t)}\right)$, and $\hat{\boldsymbol{H}}_{ab}\hat{\boldsymbol{H}}_{ab}^H = \boldsymbol{U}_{ab}\boldsymbol{\Lambda}_{ab}\boldsymbol{V}_{ab}$. In absence of the channel state information at the transmitter, the optimal $\boldsymbol{Q}$ is given as $\boldsymbol{Q} = (P/N_a)\boldsymbol{I}_{N_a}$. From the mutual information given above, the channel capacity is given as [43]:

$$C_b = \sum_{i=1}^{N_a}\mathbb{E}\left[\log_2\left(1 + \frac{P/N_a}{\sigma_{bd}^2 + MSE_2P}\lambda_{ab}^{(i)}\right)\right]. \tag{36}$$

Same steps can be repeated for the eavesdropper to get the channel capacity as:

$$C_e = \sum_{i=1}^{N_a}\mathbb{E}\left[\log_2\left(1 + \frac{P/N_a}{\sigma_{ed}^2 + MSE_eP}\lambda_{ae}^{(i)}\right)\right], \tag{37}$$

where MSE_e denotes the channel estimation at the eavesdropper, and $\boldsymbol{\Lambda}_{ae} = \text{diag}\left(\lambda_{ae}^{(1)},\ldots,\lambda_{ae}^{(N_t)}\right)$, for $\hat{\boldsymbol{H}}_{ae}\hat{\boldsymbol{H}}_{ae}^H = \boldsymbol{U}_{ae}\boldsymbol{\Lambda}_{ae}\boldsymbol{V}_{ae}$. Secrecy capacity using C_b and C_e is given as:

$$C_s = \left[C_b - C_e\right]^+. \tag{38}$$

In the next section, we have provided a simulation analysis to analyze the secrecy capacity for the considered channel model. We have also performed the simulation analysis for the different number of receive antennas at the eavesdropper to show the effect of the higher number of eavesdropping antennas than at the legitimate nodes on the secrecy capacity.

V. Simulation Analysis and Results

This section presents the simulation analysis to demonstrate the secrecy performance achieved by the proposed DCE (PDCE) scheme. MIMO wireless system is considered as mentioned in Section II, where $N_a = 4$, and $N_b = 4$ at Alice, and Bob, respectively. For the considered MIMO channel model, the length of the first and second channel estimation stage is $T_1 = 8$, and $T_2 = 4$, as given in Section III. The number of eavesdropping antennas N_e is chosen from $[4, 8, 12]$ to indicate the effect of increasing the number of antennas at the eavesdropping performance. Distances between nodes are considered in meters for an indoor office environment where, $d_{ab} = 2$ m, $d_{ae} = 1.5$ m, and $d_{be} = 1.6$ m, denotes the distance between Alice-Bob, Alice-eavesdropper, and Bob-eavesdropper, respectively. All channel coefficients are drawn from quasi-static Rayleigh fading distribution where variance for inter-node channels is based on the distance from the transmitter for 2.4 GHz transmission frequency with reference distance $d_0 = 1$ m, and path loss exponent is 1.6 for simplified path-loss channel model given in [27], which implies that we have considered an indoor office environment as our simulation scenario. For simulation analysis, we have utilized 10^5 independent realizations of random channels. The variance of the self-interference channel is considered as given by experimental evaluations in [21]. Training signals $\boldsymbol{X}_{sb}, \boldsymbol{X}_a$, and $\boldsymbol{X}_b$ are considered to be normalized to unit average power, such that $\boldsymbol{X}_{sb}^H \boldsymbol{X}_{sb} = \boldsymbol{I}_{N_b}, \boldsymbol{X}_a^H \boldsymbol{X}_a = \boldsymbol{I}_{N_a}$, and $\boldsymbol{X}_b^H \boldsymbol{X}_b = \boldsymbol{I}_{N_b}$. The variance of system noise added to all nodes is considered to be same, which implies that transmit SNR is same for all nodes. All data transmission symbols are taken from 64-ary QAM constellation. SNR in all the figures corresponds to the transmit SNR. The values of the transmit SNR are chosen to compensate for path-loss, i.e. for the legitimate channel, the transmitted power is attenuated by approximately 25dB after reaching the legitimate receiver.

For data transmission, we have utilized half-duplex transmission as mentioned in Section IV-B. In each data transmission stage, 200 data symbols are transmitted from Alice. For transmission of data symbols, we have utilized a rate $1/2$ Orthogonal Space-Time Block Codes (OSTBC) with four transmit antennas for a 64-QAM signal as given in [44]. To show the performance of the blind channel estimation technique, we have utilized state of the art blind channel estimation technique for STBC [39] to estimate $\boldsymbol{H}_{ae}$, where Independent Component Analysis (ICA) is utilized by exploiting the higher-order statistics of the transmitted STBC signal. The considered Blind Channel Estimation (BCE) is suitable for use at the eavesdropper as it does not require any modification at the transmitter. As ICA is utilized, the BCE requires the knowledge of the transmission channel to resolve the residual phase rotation ambiguities [39]. For the used rate $1/2$ OSTBC with four transmit antennas, the BCE has to resolve among 8 different phase rotations. For the resolution of phase rotations, we have utilized the channel estimated at the eavesdropper during PDCE, as the original channel is not available at the eavesdropper.

The performance of PDCE is shown in Fig. 2, where we plot MSE against the transmit SNR. The theoretical performance is calculated by substituting the relevant statistical information to the MSE expressions evaluated in section IV-A, i.e., $\boldsymbol{H}_{bb}$ Theory, $\boldsymbol{H}_{ab}$ Theory, and $\boldsymbol{H}_{ae}$ Theory, are obtained from (21), (23), and (26), respectively. The comparison of theoretical and simulation performance shows the correctness of the statistical analysis. For $\boldsymbol{H}_{ae}$, the simulation results also indicate that the average MSE performance does not depend on the number of receive antennas. MSE of $\boldsymbol{H}_{ae}$ also indicates that even for high transmit SNR the estimation error at the eavesdropper will be equal to the variance of the channel $\boldsymbol{H}_{be}$. MSE for the estimation of $\boldsymbol{H}_{ae}$ using BCE is also shown in Fig .2. For BCE, the number of receive antennas must be greater than the number of transmit antennas $N_e > N_a$, hence BCE can not be utilized for $N_e = 4$. As for BCE at the eavesdropper, MSE is the same for $N_e = 8$ and $N_e = 12$. MSE curve for BCE of $\boldsymbol{H}_{ae}$ indicates that despite using 200 transmitted symbols for channel estimation, its MSE is close to 0.01 which is close to the variance of the channel $\boldsymbol{H}_{ae}$. Therefore, there is no advantage of using BCE in terms of MSE performance of $\boldsymbol{H}_{ae}$. This figure clearly shows that the MSE at the eavesdropper is kept around 10^{-2}, while the MSE at the legitimate is significantly improved. As later shown in BER analysis, to decode the transmitted signal robustly, the MSE error should be close to 10^{-4}. MSE for $\boldsymbol{H}_{bb}$ can also be interpreted as the performance of the legacy LMMSE channel estimator without a self-interference signal.

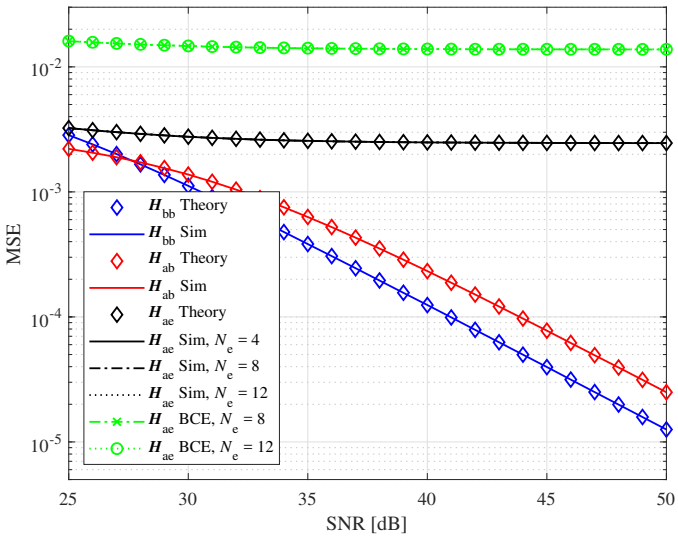

Fig. 2. MSE for $\boldsymbol{H}_{bb}$, $\boldsymbol{H}_{ab}$, and $\boldsymbol{H}_{ae}$, where $N_a = 4$, and $N_b = 4$.

Fig. 3 provides the performance comparison of PDCE scheme against two prominent DCE schemes presented in [13], and [14], denoted here as DCE1, and DCE2, respectively. For the implementation of DCE1 and DCE2, statistical information regarding the eavesdropper's channel is required at the legitimate node for optimal power allocation, which is not possible for the considered passive eavesdropping scenario. For the sake of comparison, we have assumed that the statistical information regarding the eavesdropper's channel is available at the legitimate nodes. DCE1 and DCE2 have utilized a parameter γ, which sets the limit on achievable

MSE at the eavesdropper. For the considered case, where the channel between Alice and the eavesdropper is better than the legitimate channel, it not possible to maintain a constant γ, so we have used the greatest possible value for γ at each SNR. The total power transmitted by all channel estimation techniques is considered to be the same. The system model given in [13], [14] requires $N_a > N_b$ to design orthogonal AN signal, whereas we have used $\boldsymbol{Q}_{ab} = \left[\boldsymbol{h}_{ab}^{(1)}\boldsymbol{h}_{ab}^{(2)}\boldsymbol{h}_{ab}^{(3)}\right]$, where $\boldsymbol{h}_{ab}^{(r)}$ corresponds to the channel vector at r-th receive antenna, to design AN noise signal which will not be perfectly orthogonal to $\boldsymbol{H}_{ab}$. For simplicity, we have shown the MSE at the eavesdropper for $N_e = 4$, because as shown in Fig. 2 that, MSE remains the same for the different number of receive antennas. Fig. 3 shows that DCE1 keeps MSE at the eavesdropper higher than the PDCE because the eavesdropping variance is utilized in power allocation which is not available for PDCE. For high SNR, DCE1 is unable to avoid the leakage of channel estimation, as the eavesdropper can acquire robust estimates from the first training stage of DCE1. Similarly, DCE2 avoids leakage of channel estimates to the eavesdropper but the performance of the legitimate channel is also degraded. DCE2 requires more SNR and bandwidth as compared to other techniques as it comprises of four transmission stages. It also suffers from noise amplification because the private channel training signal is transmitted by Alice which is amplified and sent back to Alice by Bob.

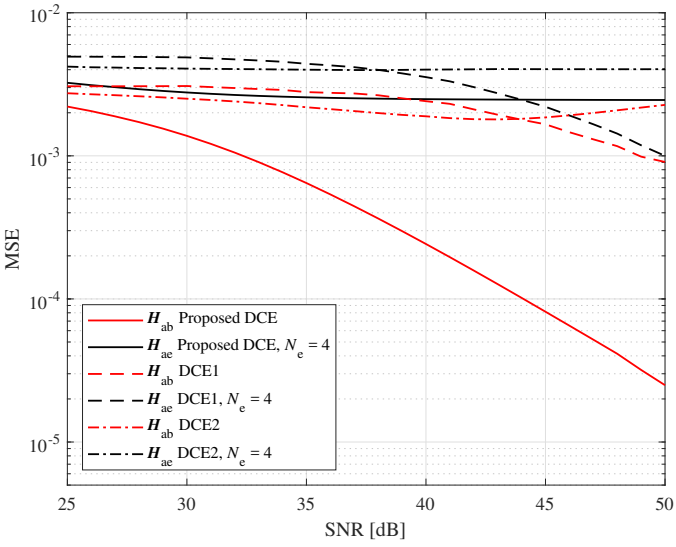

Fig. 3. MSE comparison with two prominent DCE schemes, DCE1 presented in [13], and DCE2 [14], where $N_a = 4$, $N_b = 4$, and $N_e = 4$.

In Fig. 4, C_s of the system is indicated based on the estimation error at Bob and the eavesdropper. The transmission model is considered as mentioned in Section IV-B. The variance of estimation error is equal to the MSE achieved by that DCE scheme. We have calculated C_s for the different number of eavesdropping antennas N_e, where the number of antennas at Alice and Bob, channel variances and received noise remains the same. Fig. 4 shows that increasing the number of antennas at the eavesdropper decreases the secrecy capacity. It can be seen from the relation of C_e given in (37), that an increase in N_e results in the increase of $\lambda_{ae}^{(i)}$, which increases the channel capacity C_e. C_s for PDCE shows that secure communication is possible even when the ratio between transmit (N_a) at Alice and receive (N_e) antennas at the eavesdropper is $1:3$, under the assumption of Gaussian input symbols. For DCE1, C_s is close to one when $N_e = 4$, and it reduces to zero for $N_e = 8$ and $N_e = 12$. For DCE2, the max achievable C_s is close to 5 bps/Hz when $N_e = 4$, which is very low for the considered Gaussian input sequence. These results indicate that secure communication can be achieved by using PDCE, while existing DCE techniques are unable to provide secure communication.

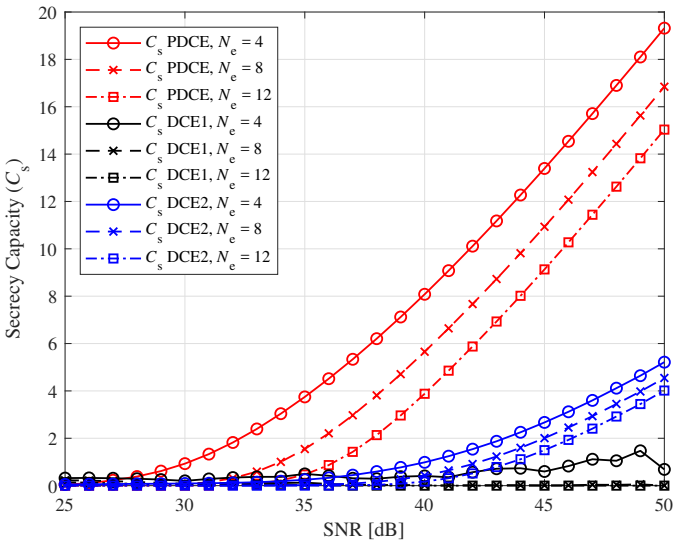

Fig. 4. Secrecy Capacity achieved by using proposed DCE against DCE1 and DCE2.

Finally, in Fig. 5 we have shown the Bit Error Rate (BER) achieved by the different channel estimation schemes at Bob and the eavesdropper represented as BER_B, and BER_E, respectively. The receiver utilizes the channel estimated by respective channel estimation technique to decode the signal transmitted by Alice. The horizontal axis indicates the transmit SNR for the data transmission phase while utilizing the channel estimates acquired for the same transmit SNR. For comparison, we have provided BER at Bob for standard channel estimation (SCE), where standard LMMSE estimator is utilized for the estimation of $\boldsymbol{H}_{ab}$. The BER results show that for PDCE, BER at the eavesdropper decreases with the increase in the number of receive antennas N_e. For $N_e = 4$, BER is greater than 0.1 which implies that the eavesdropper is unable to acquire any useful information as the maximum value for BER is 0.5. It can be better understood from the example that if we assume the transmission rate to be 1 Mbps (Megabits per second), then there would be 10^5 bits in error every second. Therefore, such a high number of errors at the physical layer will make the received information useless. Even for $N_e = 12$, the eavesdropper is unable to acquire robust information as its BER is still close to 0.1, because increasing the number of eavesdropping antennas does not improve the channel estimates as shown in (24). Fig. 5 also shows that Bob performs 6 dB away from standard LMMSE channel

estimation which corresponds to the additional training stage and transmission of training signal from both nodes. The BER for DCE1 and DCE2 remains close to 0.1 for Bob and the eavesdropper, even at the high SNRs. Similarly, Fig. 3 also shows that MSE at Bob and the eavesdropper is very high for DCE1 and DCE2 to establish any reliable communication link. We have also provided the BER performance achieved by BCE in Fig. 5, where BER at the eavesdropper for $N_e = 8$, and $N_e = 12$. It also shows that the BER achieved by BCE is worse of than the BER for IC-based channel estimation at the eavesdropper. These results show that a reliable communication link can be established between legitimate nodes while providing secrecy against the passive eavesdropper by using PDCE.

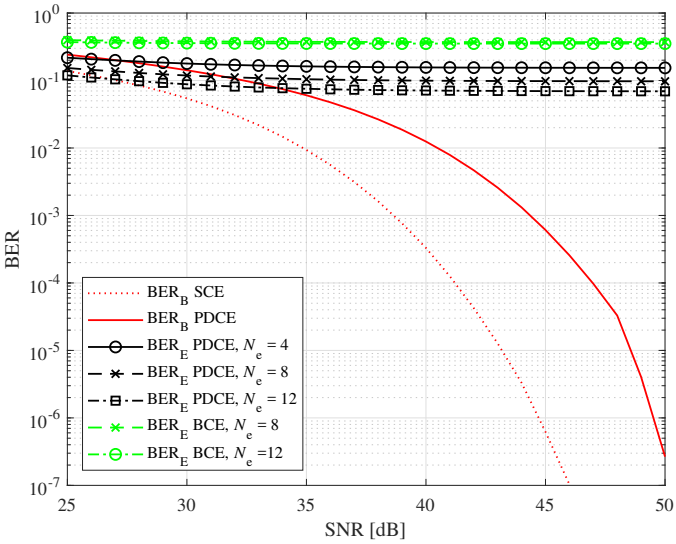

Fig. 5. BER achieved at Bob and the eavesdropper for different channel estimation techniques against transmit SNR, for rate $1/2$ OSTBC.

VI. Conclusion

In this paper, we have presented a novel in-band full-duplex based two-stage secure channel estimation technique to avoid the leakage of channel estimates to the adversary. We have analyzed the proposed DCE technique by utilizing MSE as the performance metric. The simulation analysis indicates that MSE at the eavesdropper cannot be improved beyond the variance of the eavesdropper's channel. In this paper, we have also provided the performance comparison to the existing DCE schemes. The performance comparison shows that proposed DCE achieves superior performance with less SNR and bandwidth. Finally, we have also presented system performance by providing secrecy capacity, and BER analysis indicating significant performance differentiation between the legitimate receiver and the eavesdropper by utilizing proposed channel estimation technique as compared to other existing DCE techniques.

References

[1] 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, 2014.

[2] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University Press, 2011.

[3] Y. Zou and J. Zhu, *Physical-layer security for cooperative relay networks*, ser. Wireless Networks. Springer International Publishing, 2016.

[4] M. Agarwal, S. Biswas, and S. Nandi, "Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 581–584, Apr. 2015.

[5] Y. Li, Y. Huang, R. Xu, S. Seneviratne, K. Thilakarathna, A. Cheng, D. Webb, and G. Jourjon, "Deep Content: Unveiling video streaming content from encrypted Wi-Fi traffic," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 2018, pp. 1–8.

[6] E. Magli, M. Grangetto, and G. Olmo, "Joint source, channel coding, and secrecy," *EURASIP J. Inform. Secur.*, vol. 2007, p. 13, 2007.

[7] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[8] A. O. Hero III, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[9] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[10] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using Zero-Forcing beamforming," in *2012 Proceedings IEEE INFOCOM*, Mar. 2012, pp. 720–728.

[11] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W. P. Hong, and E. A. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[12] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems,," in *Proc. Internet Society Network and Distributed System Security Symposium (NDSS 14)*, Feb. 2014.

[13] T.-H. Chang, W.-C. Chiang, Y.-W. P. Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223–6237, Dec. 2010.

[14] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2724–2738, May 2013.

[15] F. Ud Din and F. Labeau, "Multiple antenna physical layer security against passive eavesdroppers: A tutorial," in *2018 IEEE Canadian Conference on Electrical Computer Engineering (CCECE)*, 2018, pp. 1–6.

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

[17] T.-Y. Liu, Y.-C. Chen, and Y.-W. P. Hong, "Artificial noise design for discriminatory channel estimation in wireless MIMO systems," in *2014 IEEE Global Communications Conference*, Dec. 2014, pp. 3032–3037.

[18] C.-J. Chun, J.-H. Lee, and H.-M. Kim, "Discriminatory channel estimation in MIMO decode-and-forward relay systems with cooperative jamming," in *2016 IEEE International Conference on Communications Workshops (ICC)*, May 2016, pp. 266–271.

[19] J. Bezanilla and J. Via, "Antenna grouping for general discriminatory channel estimation," in *2015 International Conference on Wireless Communications Signal Processing (WCSP)*, Oct. 2015, pp. 1–5.

[20] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 120–135, Jan. 2019.

[21] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[22] F. Ud Din and F. Labeau, "Physical layer security through secure channel estimation," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–5.

[23] A. Masmoudi and T. Le-Ngoc, "A maximum-likelihood channel estimator for self-interference cancelation in full-duplex systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5122–5132, Jul. 2016.

[24] J. Wang, H. Yu, F. Shu, J. Lu, R. Chen, J. Li, and D. N. K. Jayakody, "Sum-MSE gain of DFT-Based channel estimator over frequency-domain LS one in full-duplex OFDM systems," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1231–1240, Jun. 2019.

[25] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Secret channel training to enhance physical layer security with a full-duplex receiver," *IEEE Trans. Inform. Forensic Secur.*, vol. 13, no. 11, pp. 2788–2800, Nov. 2018.

[26] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4. ACM, Sep. 2013, pp. 375–386.

[27] A. Goldsmith, *Wireless Communications*, 1st ed. Cambridge university press, Aug. 2005.

[28] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7849–7864, Dec. 2018.

[29] A. Masmoudi and T. Le-Ngoc, "Self-interference cancellation limits in full-duplex communication systems," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[30] S. Dang, G. Chen, and J. P. Coon, "Outage performance analysis of full-duplex relay-assisted device-to-device systems in uplink cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4506–4510, May 2017.

[31] M. Chung, L. Liu, O. Edfors, D. K. Kim, and C.-B. Chae, "Robust timing synchronization for full duplex communications: Design and implementation," in *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Nov. 2017, pp. 883–887.

[32] S. Shaboyan, E. Ahmed, A. S. Behbahani, W. Younis, and A. M. Eltawil, "Frequency and timing synchronization for in-band full-duplex ofdm system," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–7.

[33] M. Chung, M. S. Sim, J. Kim, D. K. Kim, and C.-B. Chae, "Prototyping real-time full duplex radios," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 56–63, Sep. 2015.

[34] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 951–963, Apr. 2003.

[35] I. Barhumi, G. Leus, and M. Moonen, "Optimal training design for MIMO OFDM systems in mobile wireless channels," *IEEE Trans. Signal Process.*, vol. 51, no. 6, pp. 1615–1624, Jun. 2003.

[36] F. Stephen, I. Arnold, and S. Lawrence, *Linear Algebra*. Prentice Hall 4th ed., 2003.

[37] S. M. Kay, *Fundamentals of Statistical Signal Processing: Practical Algorithm Development*. Pearson Education, 2013, vol. 3.

[38] C. Shin, R. W. Heath, and E. J. Powers, "Blind channel estimation for MIMO-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 670–685, Mar. 2007.

[39] V. Choqueuse, A. Mansour, G. Burel, L. Collin, and K. Yao, "Blind channel estimation for STBC systems using higher-order statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 495–505, Feb. 2011.

[40] Y. Saito, A. Benjebbour, Y. Kishiyama, and T. Nakamura, "System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sep. 2013, pp. 611–615.

[41] S. Shahbazpanahi, A. B. Gershman, and J. H. Manton, "Closed-form blind MIMO channel estimation for orthogonal space-time block codes," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4506–4517, Dec. 2005.

[42] W.-K. Ma, B.-N. Vo, T. N. Davidson, and P.-C. Ching, "Blind ML detection of orthogonal space-time block codes: Efficient high-performance implementations," *IEEE Trans. Signal Process.*, vol. 54, no. 2, pp. 738–751, Feb. 2006.

[43] T. Yoo and A. Goldsmith, "Capacity and optimal power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.

[44] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456–1467, Jul. 1999.

Fawad Ud Din received the B.S. degree in electrical engineering from the University of Engineering and Technology, Taxila, Pakistan, in 2011, and master's in communication engineering from Aalto University, Espoo, Finland, in 2013. Currently, he is working towards his Ph.D. degree at McGill University, Montréal, Canada. His research interests include physical layer security, statistical signal processing, and wireless communications.

Fabrice Labeau is the Deputy Provost (Student Life and Learning) at McGill University, where he also holds the NSERC/Hydro-Québec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid. His research interests are in applications of signal processing. He has (co-)authored more than 200 papers in refereed journals and conference proceedings in these areas.

He is the Director of Operations of STARaCom, an interuniversity research center grouping 50 professors and 500 researchers from 10 universities in the province of Quebec, Canada. He is President of the Institute of Electrical and Electronics Engineers (IEEE) Sensors Council, Senior Past President of the IEEE Vehicular Technology Society, and the past chair of the Montreal IEEE Section.

He was a recipient in 2015 and 2017 of the McGill University Equity and Community Building Award (team category), of the 2008 and 2016 Outstanding Service Award from the IEEE Vehicular Technology Society and of the 2017 W.S. Read Outstanding Service Award form IEEE Canada. He was recognized in 2018 "Ambassadeur Accrédité" for the Montreal Convention Center. He is a "champion" for Engineers Canada's 30 by 30 initiative and a member of Engineers Canada's Indigenous Participation in Engineering working group.