Artificial Noise Assisted In-Band Full-Duplex Secure Channel Estimation

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

***Abstract*—This paper proposes a novel secure channel estimation technique to provide security against leakage of the channel estimates to any malicious user by utilizing artificial noise (AN) along with full-duplex (FD) transmissions. AN overcomes the drawback of FD transmission, where any strategically located eavesdropper can minimize the interference signal received from the FD receiver. The proposed secure channel estimation technique comprises three stages, where the first stage is responsible for the estimation of the residual self-interference (SI) channel. The second stage acquires rough channel estimates to design AN orthogonal to the channel between legitimate transmitter-receiver for the next training stage. In the third stage, both legitimate nodes transmit orthogonal AN signals along with the known training signals using FD transmissions. For power allocation, we have presented a novel local adaptive power allocation algorithm at each legitimate node to allocate the powers to the training signals, and AN signals while ensuring equivocation at the eavesdropper. We provide the mean square error (MSE) to indicate the performance achieved by the respective nodes. We have also provided the bit error rate (BER) simulation analysis to indicate the secure communication achieved by securing the channel estimation process. The presented simulation analysis indicates that the eavesdropper is unable to decode the transmitted information while the legitimate receiver has robustly decoded the transmitted information.**

***Index Terms*—Physical Layer Security, Discriminatory Channel Estimation, Artificial Noise Injection.**

I. Introduction

Recent attacks on communication networks and cyber-physical systems have reignited the interest in physical layer security (PLS), where the randomness of the wireless transmission medium is exploited to provide secrecy at the lowest layer of the communications stack [1]. PLS can be employed as an additional layer of security, along with existing cryptographic techniques, to provide secrecy against rapidly evolving attacks on communication systems [2].

Robust and accurate channel state information (CSI) is crucial in establishing a reliable communication link, as it characterizes the overall effect of the wireless transmission medium on the transmitted signal. In the absence of knowledge regarding CSI, it is difficult to recover the transmitted signals, especially for multiple-input multiple-output (MIMO) systems where CSI is critical in decoding the spatially multiplexed data streams as shown in [3]. Therefore, Discriminatory Channel Estimation (DCE) techniques are introduced to exploit the CSI to achieve PLS by ensuring that the channel estimation performance is degraded at the malicious user as compared to the legitimate nodes [4]. Secrecy and robustness of CSI are also crucial in achieving secrecy through other PLS techniques, for instance, secure channel coding [5], [6], MIMO beamforming [7], and artificial noise (AN) aided MIMO beamforming [8], [9], where robust CSI is essential at legitimate nodes to design channel codes and beamforming matrices and the malicious user can leverage any leakage of CSI to overcome security measures specifically designed for the main channel [10]–[12]. CSI between the legitimate transmitter and the eavesdropper is also exploited by known-plaintext attack in [13], to overcome the AN orthogonal to data transmission from a MIMO system.

DCE provides an efficient method of achieving PLS because the channel estimation stage generally consumes less bandwidth as compared to the data transmission stage. Most commonly used AN-assisted multiple-stage DCE training schemes are presented in [4], [14], where it is required that the main channel must be better than the eavesdropping channel, statistical channel information regarding the eavesdropper's channel must be available at the legitimate nodes, and the number of antennas at the transmitters must be greater than the receiver to achieve secrecy. These strict restrictions are hard to meet in practice as it not possible to guarantee the location and capabilities of the potential eavesdropper. These DCE techniques utilize half-duplex wireless communication, where only one node transmits the signal while all the other nodes passively receive the transmitted signal. Recently, in-band full-duplex (FD) transmissions are utilized in DCE to simultaneously transmit the pilot sequence from the legitimate transmitter and the receiver, such that the received signal at the eavesdropper is the superposition of the two signals. The superposition of two signals at the eavesdropper results in the equivocation regarding the training signal to achieve DCE [15]–[17]. The FD-DCE techniques overcome the drawbacks of existing half-duplex based DCE techniques [4], [14], [18]–[21] as they do not require the statistical channel information regarding the eavesdropping channel, or restrict the number of antennas on the legitimate receiver. In [16], FD transmissions are utilized to achieve DCE but the residual self-interference is considered to be additive white Gaussian noise, which limits the scope of the presented DCE scheme. In [15], we have presented FD based DCE comprising of two stages, where, in the first stage, the SI channel is estimated by using a private pilot signal, followed by FD transmissions from both legitimate nodes to estimate the corresponding channels. All the FD-DCE techniques mentioned in [15], [16] require that the malicious user is not too close to the transmitter; even then

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

the eavesdropper can optimize its location to minimize the interference signal from the legitimate receiver as compared to the legitimate transmitter. As shown in Fig. 1, the eavesdropper will try to maximize its distance from legitimate receiver d_r to minimize the strength of the signal received from the legitimate receiver. The difference in d_t and d_r will generate the difference in the average strength of the signal received at the eavesdropper from the transmitter and the receiver because path loss is strongly related to the distance. In such scenarios, the eavesdropper can exploit the disparity in the average received signal strength to acquire robust channel estimates and decode the transmitted information robustly. To overcome the drawbacks of the existing FD-DCE, we present a novel DCE technique in this paper where a novel AN aided multistage FD DCE is utilized to tackle the challenge of a strategically located eavesdropper. The proposed AN aided FD (ANFD) DCE utilizes AN signals along with in-band FD transmission to achieve robust and secure communication against a strategically located eavesdropper, by utilizing AN to avoid the leakage of channel estimates to the strategically located eavesdropper.

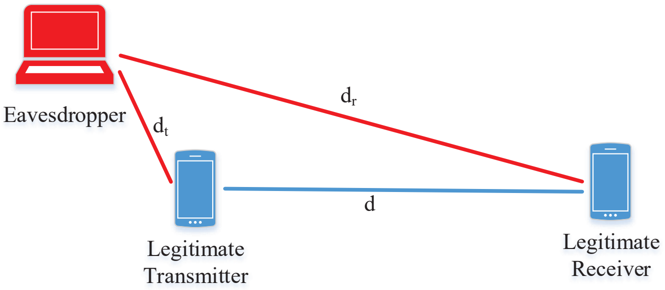

Fig. 1: Lucrative location to eavesdrop as the distance from the legitimate receiver (d_r) is greater than the legitimate transmitter (d_t).

A. Contributions and Outline

The contributions of this paper can be summarized as:

- To the best of our knowledge, the proposed novel ANFD-DCE is the first DCE scheme that provides secrecy against the strategically located eavesdropper by using AN assisted FD transmissions to secure the channel estimates. We have provided a comprehensive simulation analysis for all the possible locations of the eavesdropper to indicate the performance improvements achieved by the proposed ANFD-DCE.
- We present a novel local adaptive power allocation algorithm at both legitimate nodes in the absence of any information regarding the eavesdropping channel. The adaptive power allocation also avoids the leakage of allocated powers to any malicious user, which further degrades the channel estimation performance at the eavesdropper.
- We present a novel algorithm for the design of orthogonal AN without any constraint on the number of antennas at the legitimate nodes and the potential eavesdroppers.
- In this paper, we present an in-depth location-based simulation analysis of the proposed ANFD-DCE against the existing FD-DCE to indicate the performance enhancements achieved by the proposed ANFD-DCE. We have also analyzed the effect of increasing the number of eavesdropping antennas on achieved secrecy performance by performing simulation analysis for a different number of eavesdropping antennas.

The rest of this paper is organized into four sections. Section II provides the system model considered for the proposed AN assisted FD-DCE. Section III explains the proposed ANFD-DCE. Section IV presents a detailed simulation analysis. Finally, the conclusion of this research is presented in Section V. This paper follows the usual convention of notation, where vectors are denoted by lowercase boldface letters, and matrices are denoted by uppercase boldface letters. $\mathbb{E}\left[.\right]$ 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: $\boldsymbol{R_X} = \mathbb{E}\left[\boldsymbol{X}\boldsymbol{X}^H\right]$. $\chi^2(k)$ denotes the chi-square distribution with k degrees of freedom and $\mathcal{N}(\mu, \sigma^2)$ denotes the Gaussian distribution with μ mean and σ^2 variance. Tr$[.]$ indicates the trace operator of the matrix, and $||.||$ denotes the L^2 norm. These notations will be followed throughout this paper.

II. System Model

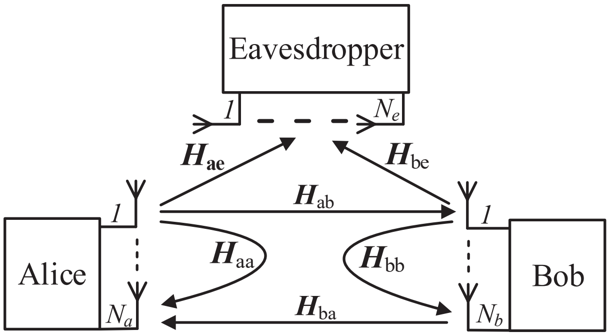

Fig. 2: Channel model consisting of multi-antenna FD legitimate transmitter (Alice), legitimate receiver (Bob), and the eavesdropper comprising of N_a, N_b, and N_e antennas, respectively.

Consider a FD MIMO channel model comprising of a legitimate transmitter (Alice), legitimate receiver (Bob), and an eavesdropper as shown in Fig. 2. All nodes are assumed to have FD capabilities. The number of antennas at Alice, Bob, and the eavesdropper are denoted as N_a, N_b, and N_e, respectively, as shown in Fig. 2. The eavesdropper is considered to be passive, as it does not transmit any signal but passively eavesdrops on the legitimate communication. All the wireless channels are considered to be flat fading and non-reciprocal, which implies that forward and reverse channel fading coefficients are independent of each other. The legitimate channel from Alice to Bob is denoted as $\mathbf{H}_{ab} \in \mathbb{C}^{N_a \times N_b}$, and from Bob to Alice is denoted by $\mathbf{H}_{ba} \in \mathbb{C}^{N_b \times N_a}$. Similarly, the eavesdropping channel from Alice to the eavesdropper is denoted by $\mathbf{H}_{ae} \in \mathbb{C}^{N_a \times N_e}$, and from Bob to the eavesdropper as $\mathbf{H}_{be} \in \mathbb{C}^{N_b \times N_e}$. The residual SI channels at Bob and Alice are denoted as $\mathbf{H}_{bb} \in \mathbb{C}^{N_b \times N_b}$, and $\mathbf{H}_{aa} \in \mathbb{C}^{N_a \times N_a}$, respectively. The total duration of each transmission block length is assumed to be T symbols comprised of multiple training stages $T_1, \ldots, T_n$ and a data transmission stage T_d. The assumptions regarding respective channels and system noises are summarized below:

- The main channel between Alice-Bob is assumed to non-reciprocal, where the elements of $\mathbf{H}_{ab}$, $\mathbf{H}_{ba}$ are assumed to independent and identically distributed (i.i.d.) random variables with zero mean and variance equal to σ_{ab}^2, and σ_{ba}^2 such that: $\sigma_{ab}^2 = \sigma_{ba}^2$. It is also assumed that the instantaneous channel variances are within the threshold: $1.2 < \frac{\sigma_{ab}^{(i)^2}}{\sigma_{ba}^{(i)^2}} < 0.8$ at every instant i as given by experimental characterization of channel reciprocity in [22]. The inequality between the instantaneous variances $\sigma_{ab}^{(i)^2}$ and $\sigma_{ba}^{(i)^2}$ is due to the hardware differences caused by the influence of AGC (Automatic Gain Control) and LNA (Low Noise Amplifier) on the power levels of the signals received at Alice and Bob.
- All inter-node channels $\mathbf{H}_{ab}$, $\mathbf{H}_{ba}$, $\mathbf{H}_{ae}$, and $\mathbf{H}_{be}$ are modeled as block Rayleigh fading channel where channel variance depends on the distance between the transmitter and the respective receiver as given by the simplified path loss model in [23][1].
- All full-duplex antennas are able to simultaneously transmit and receive by using a circulator switch as shown in [24]. The circulator switch provides considerable isolation between transmit and receive radio frequency (RF) chains [25]. To mitigate the SI at the full-duplex receiver, analog self-interference cancellation is utilized before performing analog to digital conversion. For analog cancellation, the output of the power amplifier is subtracted at the input of the low noise amplifier after suitable scaling as given in [24]. Transmit and receive RF chains are assumed to share a common oscillator, which along with analog cancellation reduces non-linear impairments caused by SI signal below the noise floor [26]. Therefore, the residual SI channels $\mathbf{H}_{aa}$, and $\mathbf{H}_{bb}$ are modeled as block Rayleigh fading channels as given by experimental characterization of SI channel in [27]. This is also a commonly utilized statistical model for characterizing the residual SI channel in the literature [15], [17], [28]–[30].
- This paper assumes that a robust timing synchronization technique for full-duplex communication has been utilized as given in [31], [32], to achieve timing synchronization especially caused by the difference in propagation delay between the SI and the desired signal. The timing synchronization techniques counteract the difference in propagation delay in a similar fashion to the time-alignment in LTE (Long Term Evolution) uplink, where a node farther from the base station (eNodeB) advances their transmission more as compared to nearby nodes such that, all the received signals are synchronized at the receiver [31], [32]. It requires that the propagation delay must be within the cyclic prefix (CP), where CP in LTE is between 4.7 and 16.7 microseconds; as we have considered the indoor wireless channel where nodes are at-most 10 meters apart from each other, the maximum possible propagation delay is approximately 33 nanoseconds. Therefore, the transmission of the SI signal is delayed by the difference in the propagation delay similar to the time-alignment in LTE (Long Term Evolution) uplink. As the propagation delay is significantly less than CP, therefore the utilization of time-alignment removes inter-symbol interference [33]. Therefore, regardless of robust synchronization and small propagation delay as compared to cyclic prefix, we have assumed that the residual synchronization offset degrades the signal to interference plus noise ratio by 1 dB as given in [34], to cater for any practical synchronization errors. The performance degradation due to the synchronization offset is modeled by increasing the variance of the noise added at the receiver by 1 dB.
- All data transmission symbols are taken M-ary Quadrature Amplitude Modulation (QAM). For the data transmission stage, the half-duplex transmission is considered, 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 the 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.
- The noise added to the received signal at all the nodes is considered to the zero mean circularly symmetric Gaussian noise (ZMCSWGN) with variance σ^2, which implies that all the nodes are operating under similar conditions like temperature, bandwidth, etc.

III. Proposed Discriminatory Channel Estimation Technique

Proposed ANFD-DCE comprises three stages, where the first stage is responsible for residual SI channel estimation by using a private orthogonal training signal as given in [15], [17]. The orthogonality of the training signals is exploited by the other legitimate node and the eavesdropper to acquire statistical information regarding respective channels. Based on the estimated channel variance both legitimate nodes perform adaptive power allocation locally, where each node assumes possible lucrative positions for the potential eavesdropper and allocates power to the forthcoming training stages to achieve PLS. The local adaptive power allocation at both legitimate nodes conceals the transmit power of the pilot signals from the eavesdropper because it is not possible for the eavesdropper

[1] The flat fading assumption considered here generalizes to the utilization of multi-carrier modulation techniques, like Orthogonal Frequency Division Multiplexing (OFDM) under frequency selective fading due to multipath environments, as long as the length of the cyclic prefix (CP) is greater than the delay spread of the channel.

to acquire the variance of the legitimate channel (between the legitimate transmitter and receiver).

In the second training stage, both the legitimate nodes simultaneously transmit the known training signals along with the AN signals to equally deteriorate all channels using in-band FD transmissions. The pilot signals acquire the rough estimates of the main channel (between the legitimate transmitter and receiver), and the AN signals avoid robust channel estimation at the eavesdropper. The legitimate FD node cancels the AN signal transmitted by itself using the SI channel information as the transmitted AN signal is perfectly known. However, the eavesdropper receives the AN signals from both the legitimate nodes. The rough channel estimate of the main channel will be utilized to design an AN signal orthogonal to the main channel for the upcoming AN assisted training stage. Finally, in the last channel estimation stage, both legitimate nodes transmit training signals to improve the estimate of their respective legitimate channels, along with the orthogonal AN signals to deteriorate the channel estimation performance at the eavesdropper.

A. First Stage: SI Channel Estimation

SI channel estimation is the first stage of the proposed DCE; it is responsible for acquiring robust estimates of the residual SI channel to be utilized in later stages for digital SI cancellation. This stage is similar to the SI channel estimation stage given in the existing FD based DCE techniques [15], [17], [30], as a private orthogonal training signal is transmitted by each legitimate node using half-duplex transmission to estimate the respective residual SI channel. The length of the training sequence is kept equal to the number of variables to be estimated [35] such that: $T_1 = N_a + N_b$, which makes blind channel estimation techniques inoperable at the eavesdropper[2]. The estimation process is the same for both legitimates nodes, without loss of generality, we will describe the estimation process at Bob; similar results and steps are valid for Alice.

At Bob: Both legitimate nodes utilize half-duplex transmissions to transmit the private orthogonal training sequence in independent time slots to avoid the interference, where Alice remains silent during Bob's transmission and vice versa. The corresponding received signal at Bob is given as:

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

where $\boldsymbol{X}_{sb} \in \mathbb{C}^{N_b \times N_b}$ is the orthogonal private training signal satisfying $\boldsymbol{X}_{sb}^{H}\boldsymbol{X}_{sb} = \boldsymbol{I}_{N_b}$, $\boldsymbol{H}_{bb}$ corresponds to the residual SI channel modeled as block Rayleigh fading channel with variance σ_{bb}^2, and $\boldsymbol{W}_{si}^{b}$ corresponds to ZMCSWGN with variance σ^2 added to the received signal. The transmitted private training signal is known at Bob as the transmit and receive radio frequency (RF) chains are on the same FD device. As the residual SI channel and noise variances are available at the legitimate node, LMMSE estimation is utilized as given in [37] to estimate $\boldsymbol{H}_{bb}$ as:

$$\begin{aligned}
\hat{\boldsymbol{H}}_{bb} &= \boldsymbol{R}_{\boldsymbol{H}_{bb}}\mathbf{X}_{sb}^{H}\left(\mathbf{X}_{sb}\boldsymbol{R}_{\boldsymbol{H}_{bb}}\mathbf{X}_{sb}^{H} + \boldsymbol{R}_{\boldsymbol{W}_{si}^{b}}\right)^{-1}\mathbf{Y}_{si}^{b}, && (2)\\
&= \frac{\sigma_{bb}^2}{\sigma_{bb}^2 + \sigma^2}\boldsymbol{X}_{sb}^{H}\boldsymbol{Y}_{si}^{b} && (3)\\
&\triangleq \boldsymbol{H}_{bb} + \Delta\hat{\boldsymbol{H}}_{bb}, && (4)
\end{aligned}$$

where $\boldsymbol{R}_{\boldsymbol{H}_{bb}} = \sigma_{bb}^2\boldsymbol{I}_{N_b}$ is the covariance of $\boldsymbol{H}_{bb}$, and $\boldsymbol{R}_{\boldsymbol{W}_{si}^{b}} = \sigma^2\boldsymbol{I}_{N_b}$ denotes the noise covariance, and $\Delta\hat{\boldsymbol{H}}_{bb}$ denotes the estimation error matrix. From [37], the correlation matrix of $\Delta\hat{\boldsymbol{H}}_{bb}$ is given as:

$$\begin{aligned}
\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{bb}\Delta\hat{\boldsymbol{H}}_{bb}^{H}\right) &= \left(\boldsymbol{R}_{\boldsymbol{H}_{bb}}^{-1} + \boldsymbol{X}_{sb}^{H}\boldsymbol{R}_{\boldsymbol{W}_{si}^{b}}^{-1}\boldsymbol{X}_{sb}\right)^{-1}, && (5)\\
&= N_b\left(\frac{1}{\sigma_{bb}^2} + \frac{1}{\sigma^2}\right)^{-1}\boldsymbol{I}_{N_b}. && (6)
\end{aligned}$$

Finally, the normalized MSE for the SI channel estimator $\hat{\boldsymbol{H}}_{bb}$ is given as:

$$\begin{aligned}
\mathcal{E}_{bb} &= \frac{\operatorname{Tr}\left[\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{bb}\Delta\hat{\boldsymbol{H}}_{bb}^{H}\right)\right]}{N_b^2}, && (7)\\
&= \left(\frac{1}{\sigma_{bb}^2} + \frac{1}{\sigma^2}\right)^{-1}. && (8)
\end{aligned}$$

At Alice: During the SI channel estimation stage Bob transmits the private training signal $\boldsymbol{X}_{sb}$, which will also be received at Alice as:

$$\boldsymbol{Y}_{s}^{a} = \boldsymbol{X}_{sb}\boldsymbol{H}_{ba} + \boldsymbol{W}_{s}^{a}, \tag{9}$$

where $\boldsymbol{H}_{ba}$ is the channel between Bob-Alice, and $\boldsymbol{W}_{s}^{a}$ is the corresponding ZMCSWGN noise with variance σ^2 added at Alice. As $\boldsymbol{H}_{ba}$ and $\boldsymbol{W}_{s}^{a}$ are independent Gaussian random variables, the received signal $\boldsymbol{Y}_{s}^{a}$ is also Gaussian distributed with zero mean, and $\boldsymbol{R}_{\boldsymbol{Y}_{s}^{a}} = \boldsymbol{X}_{sb}^{H}\boldsymbol{R}_{\boldsymbol{H}_{ba}}\boldsymbol{X}_{sb} + \boldsymbol{R}_{\boldsymbol{W}_{s}^{a}} = \left(\sigma_{ba}^2 + \sigma^2\right)\boldsymbol{I}_{N_b}$. In the absence of knowledge regarding the private training signal $\boldsymbol{X}_{sb}$, Alice exploits the orthogonality of $\boldsymbol{X}_{sb}$ to estimate the channel variance σ_{ba}^2. Alice employs Maximum Likelihood Estimator (MLE) given in [37] to estimate the variance of the channel $\boldsymbol{H}_{ba}$ because statistical information regarding σ_{ba}^2 is not available at Alice. The MLE estimator is given as:

$$\hat{\sigma}_{ba}^2 = \frac{\operatorname{Tr}\left[\left(\boldsymbol{Y}_{s}^{a}\right)^{H}\left(\boldsymbol{Y}_{s}^{a}\right)\right]}{N_a N_b} - \sigma^2. \tag{10}$$

The estimated channel variance $\hat{\sigma}_{ba}^2$ will be utilized by Alice to perform adaptive power allocation for upcoming training stages. To analyze the performance of the variance estimation at Alice, we need to calculate variance and mean of $\hat{\sigma}_{ba}^2$. The above equation (10) can also be written as:

$$\hat{\sigma}_{ba}^2 = \frac{1}{N_a N_b}\sum_{i=1}^{N_b}\sum_{j=1}^{N_a} ||\left[\boldsymbol{Y}_{s}^{a}\right]_{i,j}||^2 - \sigma^2, \tag{11}$$

where $\sum_{i=1}^{N_b}\sum_{j=1}^{N_a} ||\left[\boldsymbol{Y}_{s}^{a}\right]_{i,j}||^2$ corresponds to sum of $N_a N_b$ squares of independent Gaussian random variables. Hence, by

[2] To generalize to frequency selective fading environment with orthogonal frequency-division multiplexing (OFDM) with appropriate cyclic-prefix (CP), the minimum length of training signal must be equal to the delay spread times the number of variables as given in [36].

using the definition of Chi-Squared random distribution it can be shown that:

$$\sum_{i=1}^{N_b}\sum_{j=1}^{N_a} || \left[\boldsymbol{Y}_s^a\right]_{i,j} ||^2 \sim \left(\sigma_{ba}^2+\sigma^2\right)\chi^2\left(N_aN_b\right).$$

As the mean of $\mathbb{E}\left[\chi^2\left(N_aN_b\right)\right] = N_aN_b$, which implies that $\hat{\sigma}_{ba}^2$ provides an unbiased estimate of σ_{ba}^2. As $\hat{\sigma}_{ba}^2$ is an unbiased estimator, therefore its MSE $\mathcal{E}_{\hat{\sigma}_{ba}^2}$ is equal to the variance of the estimator which is given as:

$$\mathcal{E}_{\hat{\sigma}_{ba}^2} = \mathbb{E}\left[\left(\hat{\sigma}_{ba}^2-\mathbb{E}\left[\hat{\sigma}_{ba}^2\right]\right)^2\right], \tag{12}$$

$$= \mathbb{E}\left[\left(\frac{\sigma_{ba}^2+\sigma^2}{N_aN_b}\chi^2\left(N_aN_b\right)-\left(\sigma^2+\sigma_{ba}^2\right)\right)^2\right], \tag{13}$$

$$= \left(\frac{\sigma^2+\sigma_{ba}^2}{N_aN_b}\right)^2\mathbb{E}\left[\left(\chi^2\left(N_aN_b\right)-N_aN_b\right)^2\right], \tag{14}$$

where $N_aN_b = \mathbb{E}\left[\chi^2\left(N_aN_b\right)\right]$, which simplifies the right side of the above equation as the variance of $\chi^2\left(N_aN_b\right)$. Using the variance of $\chi^2\left(N_aN_b\right)$, MSE of estimator $\hat{\sigma}_{ba}^2$ is given as:

$$\mathcal{E}_{\hat{\sigma}_{ba}^2} = \frac{2(\sigma_{ba}^2+\sigma^2)^2}{N_aN_b}. \tag{15}$$

The above equation indicates that the MSE on the estimation at Alice of the variance of the Bob-Alice channel depends on the square of the sum of noise and channel variances. In the communication system the noise variance is very low for reliable communication, and the channel variance based on path-loss will also be very low for example, the free space path loss at 1 meter for carrier frequency 900 MHz would be -31.54 dB [23]. Hence, without the loss of generality, we assume that the $\mathcal{E}_{\hat{\sigma}_{ba}^2}$ would be negligible.

At the eavesdropper: In the SI channel estimation stage, the eavesdropper will also receive the private orthogonal training signal $\boldsymbol{X}_{sb}$ as:

$$\boldsymbol{Y}_s^e = \boldsymbol{X}_{sb}\boldsymbol{H}_{be}+\boldsymbol{W}_s^e, \tag{16}$$

where $\boldsymbol{H}_{be}$ is the channel between Bob and the eavesdropper, and $\boldsymbol{W}_s^e$ is the corresponding noise at the eavesdropper. As the training signal is private, it cannot be utilized to acquire an estimate of $\boldsymbol{H}_{ae}$. However, the orthogonality of the $\boldsymbol{X}_{sb}$ can be exploited by the eavesdropper to acquire the variance of $\boldsymbol{H}_{ae}$ as:

$$\hat{\sigma}_{be}^2 = \frac{\text{Tr}\left[\left(\boldsymbol{Y}_s^e\right)\left(\boldsymbol{Y}_s^e\right)^H\right]}{N_eN_b}-\sigma^2. \tag{17}$$

Similar to the MSE for variance estimation at Alice, MSE for $\hat{\sigma}_{be}^2$ will be equal to: $2(\sigma_{be}^2+\sigma^2)^2/(N_bN_e)$.

B. Second Stage: Rough Channel Estimation

This stage is responsible for acquiring rough channel estimates of the main channel ($\boldsymbol{H}_{ab}$, and $\boldsymbol{H}_{ba}$) while causing performance deterioration at the eavesdropper with the transmission of the omnidirectional AN signals.

At Bob: Bob transmits a globally known training signal along with a random AN signal in the second stage. The transmitted AN signal is known at Bob as the transmit and receive radio frequency chains are on the same device. Therefore, Bob cancels the transmitted AN signal by using the SI channel information. The eavesdropper receives the random artificial noise signal from both the legitimate nodes. The signal transmitted by Bob is given as:

$$\boldsymbol{X}_b^{(1)} = \sqrt{x_1}\boldsymbol{V}_b+\boldsymbol{B}, \tag{18}$$

where $\boldsymbol{V}_b$ is the pilot signal, and $\boldsymbol{B}$ is the random artificial noise signal drawn from $\mathcal{N}(\boldsymbol{0}, \frac{a_1}{N_b}\boldsymbol{I}_{T_2})$. The variance of the training signal x_1, and the artificial noise a_1 are determined through a run in each node of the adaptive power allocation scheme described in power allocation section for the proposed ANFD-DCE. In order to minimize the leakage of channel estimates, while keeping the length of the training signal at a minimum, the length of the training signal in the second stage is set to $T_2 = \max(N_a, N_b)$, to ensure that the reception at the eavesdropper is completely superimposed by two signals. Similarly, the signal transmitted by Alice is given as: $\boldsymbol{X}_a^{(1)} = \sqrt{x_1}\boldsymbol{V}_a+\boldsymbol{A}$, where $\sqrt{x_1}\boldsymbol{V}_a$ is the pilot signal with variance x_1 and $\boldsymbol{A}$ is the AN signal drawn from $\mathcal{N}(\boldsymbol{0}, \frac{a_1}{N_a}\boldsymbol{I}_{T_2})$. The signal received at Bob after digital SI cancellation during the second stage is given as:

$$\boldsymbol{Y}_b^{(1)} = \boldsymbol{X}_a^{(1)}\boldsymbol{H}_{ab}+\boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb}+\boldsymbol{W}_b^{(1)}, \tag{19}$$

$$= \left(\sqrt{x_1}\boldsymbol{V}_a+\boldsymbol{A}\right)\boldsymbol{H}_{ab}+\left(\sqrt{x_1}\boldsymbol{V}_b+\boldsymbol{B}\right)\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}, \tag{20}$$

where $\boldsymbol{W}_b^{(1)}$ is the additive ZMCSWGN and $\Delta\hat{\boldsymbol{H}}_{bb}$ is the residual SI after digital SI cancellation. The LMMSE estimator is used to estimate $\boldsymbol{H}_{ab}$ as the channel and noise variances are available at Bob. LMMSE estimator is given as [37]:

$$\hat{\boldsymbol{H}}_{ab}^{(1)} = \boldsymbol{R}_{\boldsymbol{H}_{ab}}\sqrt{x_1}\boldsymbol{V}_a^H\big(x_1\boldsymbol{V}_a\boldsymbol{R}_{\boldsymbol{H}_{ab}}\boldsymbol{V}_a^H + \boldsymbol{R}_{\boldsymbol{W}_1}\big)^{-1}\mathbf{Y}_b^{(1)}, \tag{21}$$

where $\boldsymbol{W}_1 = \boldsymbol{A}\boldsymbol{H}_{ab}+\boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb}+\boldsymbol{W}_b^{(1)}$, and using the independence of residual SI, AN, and additive noise; $\boldsymbol{R}_{\boldsymbol{W}_1}$ is given as:

$$\boldsymbol{R}_{\boldsymbol{W}_1} = \mathbb{E}\Bigg[\Big(\boldsymbol{A}\boldsymbol{H}_{ab}+\boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb}+\boldsymbol{W}_b^{(1)}\Big) \Big(\boldsymbol{A}\boldsymbol{H}_{ab}+\boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb}+\boldsymbol{W}_b^{(1)}\Big)^H\Bigg], \tag{22}$$

$$= N_b\Bigg(a_1\sigma_{ab}^2+\mathcal{E}_{bb}\big(x_1c+a_1\big)+\sigma^2\Bigg)\boldsymbol{I}_{T_2}, \tag{23}$$

where $c = N_b/T_2$. Substituting $\boldsymbol{R}_{\boldsymbol{W}_1}$ in (21), the LMMSE estimator can be simplified as:

$$\hat{\boldsymbol{H}}_{ab}^{(1)} = \frac{\sigma_{ab}^2\sqrt{x_1}\mathbf{V}_a^H}{\sigma_{ab}^2(x_1+a_1)+\mathcal{E}_{bb}\big(x_1c+a_1\big)+\sigma^2}\mathbf{Y}_b^{(1)}. \tag{24}$$

To analyze the channel estimation performance, the normalized MSE at Bob for the rough channel estimation stage is derived as [37]:

$$\mathcal{E}_{ab}^{(1)} = \frac{\left(\boldsymbol{R}_{\boldsymbol{H}_{ab}}^{-1} + x_1 \boldsymbol{V}_a^H \boldsymbol{R}_{\boldsymbol{W}_1}^{-1} \boldsymbol{V}_a\right)^{-1}}{N_a N_b} \tag{25}$$

$$= \left(\frac{1}{\sigma_{ab}^2} + \frac{x_1}{a_1 \sigma_{ab}^2 + \mathcal{E}_{bb}\left(x_1 c + a_1\right) + \sigma^2} \right)^{-1} \tag{26}$$

At the eavesdropper: During the rough channel estimation stage, the received signal at the eavesdropper is given as:

$$\boldsymbol{Y}_e^{(1)} = \boldsymbol{X}_a^{(1)} \boldsymbol{H}_{ae} + \boldsymbol{X}_b^{(1)} \boldsymbol{H}_{be} + \boldsymbol{W}_e^{(1)}, \tag{27}$$

$$= (\sqrt{x_1} \boldsymbol{V}_a + \boldsymbol{A}) \boldsymbol{H}_{ae} + (\sqrt{x_1} \boldsymbol{V}_b + \boldsymbol{B}) \boldsymbol{H}_{be} + \boldsymbol{W}_e^{(1)}, \tag{28}$$

where $\boldsymbol{W}_e^{(1)}$ denotes the ZMCSWGN with variance σ^2. $\boldsymbol{V}_a$ and $\boldsymbol{V}_b$ are globally known but x_1, $\boldsymbol{A}$, and $\boldsymbol{B}$ are not known globally. The eavesdropper can utilize the estimated channel variances $\hat{\sigma}_{ae}^2$ and $\hat{\sigma}_{be}^2$ to estimate the total transmitted power $P_1 = x_1 + a_1$. However, the eavesdropper can not estimate x_1 and the variance of AN signals from Alice and Bob because it will require the information regarding the channel variance of the legitimate channel σ_{ab}^2. Although the eavesdropper has statistical knowledge regarding $\boldsymbol{H}_{ae}$ and $\boldsymbol{H}_{be}$ to acquire the statistical knowledge regarding $\boldsymbol{H}_{ab}$, it needs to estimate the angle of arrival which is not possible without robust channel estimates [38]. Therefore, the least squares (LS) estimator is utilized to estimate $\boldsymbol{H}_{ae}$ by the eavesdropper as the variance of the pilot and AN signal is not available at the eavesdropper. It is assumed without loss of generality that the eavesdropper is close to Alice as compared to Bob which implies that SNR of the signal received from Alice (SNR_{ae}) is greater than that from Bob (SNR_{be}), and $\boldsymbol{H}_{ae}$ can be estimated while considering the signal received from Bob as noise. Finally, the LS estimator of $\boldsymbol{H}_{ae}$ is given as:

$$\hat{\boldsymbol{H}}_{ae}^{(1)} = \left[\sqrt{P_1} \boldsymbol{V}_a\right]^{\dagger} \boldsymbol{Y}_e^{(1)}, \tag{29}$$

$$= \boldsymbol{V}_1^{\dagger} \boldsymbol{Y}_e^{(1)}, \tag{30}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta \hat{\boldsymbol{H}}_{ae}^{(1)}. \tag{31}$$

To evaluate the channel estimation performance, the MSE of $\hat{\boldsymbol{H}}_{ae}^{(1)}$ is given as:

$$\mathbb{E}\left(\Delta \hat{\boldsymbol{H}}_{ae}^{(1)} \Delta \hat{\boldsymbol{H}}_{ae}^{(1)^H}\right) = \mathbb{E}\left[\boldsymbol{H}_{ae} \boldsymbol{H}_{ae}^H - 2 \boldsymbol{H}_{ae} \boldsymbol{Y}_e^{(1)^H} \boldsymbol{V}_1^{\dagger^H} + \boldsymbol{V}_1^{\dagger} \boldsymbol{Y}_e^{(1)} \boldsymbol{Y}_e^{(1)^H} \boldsymbol{V}_1^{\dagger^H}\right]. \tag{32}$$

Therefore, the normalized MSE for the LS estimator at the eavesdropper during the second stage is given as:

$$\mathcal{E}_{ae}^{(1)} = \sigma_{ae}^2 \left(1 - \sqrt{\frac{x_1}{P_1}}\right)^2 + \frac{a_1 \sigma_{ae}^2 + \sigma_{be}^2 (x_1 c + a_1) + \sigma^2}{P_1}. \tag{33}$$

C. Third Stage: Orthogonal AN aided Channel Estimation

In this stage, Orthogonal AN (OAN) aided training signals are transmitted from both legitimate nodes simultaneously using FD transmissions to improve the channel estimates, while causing equivocation at the eavesdropper.

At Bob: To design an OAN signal in the left null space of the legitimate channel, it is required that the number of receive antennas must be less than the number of transmit antennas.

In order to design an AN orthogonal to the legitimate channel, we consider two scenarios. First, where $N_a = N_b$: in this scenario Bob splits the $N_b \times N_a$ channel $\boldsymbol{H}_{ba}$ into two as: $\boldsymbol{H}_{ba} = [\boldsymbol{H}_{ba1} \boldsymbol{H}_{ba2}]$, where $\boldsymbol{H}_{ba1}$ and $\boldsymbol{H}_{ba2}$ has dimensions $N_b \times N_{a1}$, and $N_b \times N_{a2}$, respectively, such that $N_{a1} < N_b$, and $N_{a2} < N_b$. The training signal transmitted from Bob is given as:

$$\boldsymbol{X}_b^{(2)} = \begin{bmatrix} \boldsymbol{X}_{b,1}^{(2)} \\ \boldsymbol{X}_{b,2}^{(2)} \end{bmatrix} = \begin{bmatrix} \sqrt{x_2} \boldsymbol{V}_b + \boldsymbol{B}_1 \boldsymbol{N}_{ba1}^H \\ \sqrt{x_2} \boldsymbol{V}_b + \boldsymbol{B}_2 \boldsymbol{N}_{ba2}^H \end{bmatrix}, \tag{34}$$

where x_2 is the variance of the training signals, $\boldsymbol{B}_1$, and $\boldsymbol{B}_2$ are the zero-mean Gaussian noise with variance a_2/N_b, $\boldsymbol{N}_{ba1}^H$, and $\boldsymbol{N}_{ba2}^H$ corresponds to the left-null space of the sub-channels $\boldsymbol{H}_{ba1}$, and $\boldsymbol{H}_{ba2}$, respectively. As the number of antennas are equal at both nodes, the same process is repeated at Alice. For the second scenarios where $N_a \neq N_b$, the node with fewer antennas splits the channel into sub-channels as indicated for the previous scenario. We have provided the algorithm for generation of training signal in Algorithm 1, where $N_a > N_b$. In this algorithm, channel $\hat{\boldsymbol{H}}_{ba} \in \mathbb{C}^{N_b \times N_a}$ is partitioned such that $N_a^{(t)} < N_b$, as it is required to generate OAN. This process is repeated until the training signal is generated to estimate $\boldsymbol{H}_{ba}$. We have provided the details for generation of OAN aided training signal at Bob for $N_a > N_b$, similar approach is used to generate the training for $N_b > N_a$, and at Alice.

Lastly, as the design of OAN require forward channel estimates, we assume that null space of the channel matrix is sent from Bob to Alice and Alice to Bob instead of transferring forward channel estimates to avoid the leakage of CSI to the eavesdropper. In order to simplify the analysis, we will consider $N_a = N_b$, and the estimation of $\boldsymbol{H}_{ab1}$, similar results and analysis would be valid for $N_a \neq N_b$, and $\boldsymbol{H}_{ab2}$, respectively. The received signals at Bob in this stage after digital SI cancellation are given as:

$$\mathbf{Y}_b^{(2)} = \left(\sqrt{x_2} \boldsymbol{V}_a + \mathbf{A}_1 \mathbf{N}_{ab1}^H\right) \mathbf{H}_{ab1} + \left(\sqrt{x_2} \boldsymbol{V}_b + \mathbf{B}_1 \mathbf{N}_{ba1}^H\right) \Delta \hat{\mathbf{H}}_{bb1} + \mathbf{W}_b^{(2)}, \tag{35}$$

where $\boldsymbol{N}_{ab1}^H$ is the null space of the channel $\boldsymbol{H}_{ab1}^{(1)}$, $\boldsymbol{A}_1$ is the zero mean Gaussian noise with variance a_2/N_a, and $\mathbf{W}_b^{(2)}$ is the ZMCSWGN with variance σ^2 added at Bob during the OAN assisted channel estimation stage. The signals received

Algorithm 1: Orthogonal AN aided training signal generation for $N_a > N_b$ at Bob.

```
Input  : $\hat{\boldsymbol{H}}_{ba}, x_2, \boldsymbol{V}_b, b$
Output: $\boldsymbol{X}_b^{(2)}$
$N_{ad} \leftarrow N_a$, $n_{st} \leftarrow 1$;
while $N_{ad} \neq 0$ do
    if $N_{ad} < N_b$ then
        $n_{end} \leftarrow N_a$
    else
        $n_d \leftarrow 2$;
        $N_a^{(t)} \leftarrow \lfloor N_{ad}/n_d \rfloor$;
        while $N_a^{(t)} \leq N_b$ do
            $n_d \leftarrow n_d + 1$;
            $N_a^{(t)} \leftarrow \lfloor N_{ad}/n_d \rfloor$;
        end
        $n_{end} \leftarrow n_{st} + N_a^{(t)} - 1$
    end
    if $n_{st} = 1$ then
        $\boldsymbol{N}_{ba} \leftarrow null([\hat{\boldsymbol{h}}_{ba}^{n_{st}}, \dots, \hat{\boldsymbol{h}}_{ba}^{n_{end}}]^H)$;
        $\boldsymbol{X}_b^{(2)} \leftarrow \sqrt{x_2}\boldsymbol{V}_b + \boldsymbol{B}_{n_{st}}\boldsymbol{N}_{ba}^H$,
            $\boldsymbol{B}_{n_{st}} \sim \mathcal{N}(\mathbf{0}, \frac{a_2}{N_b}\boldsymbol{I})$;
    else
        $\boldsymbol{N}_{ba} \leftarrow null([\hat{\boldsymbol{h}}_{ba}^{n_{st}}, \dots, \hat{\boldsymbol{h}}_{ba}^{n_{end}}]^H)$;
        $\boldsymbol{X}_b^{(2)} \leftarrow \left(\boldsymbol{X}_b^{(2)} | (\sqrt{x_2}\boldsymbol{V}_b + \boldsymbol{B}_{n_{st}}\boldsymbol{N}_{ba}^H)\right)$,
            $\boldsymbol{B}_{n_{st}} \sim \mathcal{N}(\mathbf{0}, \frac{a_2}{N_b}\boldsymbol{I})$;
    end
    $N_{ad} \leftarrow N_{ad} - (n_{end} - n_{st} + 1)$;
    $n_{st} \leftarrow n_{end} + 1$
end
```

at Bob during both channel estimation stages are given as:

$$\begin{aligned}\mathbf{Y}_2 &= \begin{bmatrix}\mathbf{Y}_b^{(1)}\\ \mathbf{Y}_b^{(2)}\end{bmatrix},\\ &= \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_a\\ \sqrt{x_2}\boldsymbol{V}_a\end{bmatrix}\mathbf{H}_{ab1} + \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_b\\ \sqrt{x_2}\boldsymbol{V}_b\end{bmatrix}\Delta\hat{\mathbf{H}}_{bb1}+\\ &\quad\begin{bmatrix}\boldsymbol{A}\boldsymbol{H}_{ab1}+\boldsymbol{B}\Delta\hat{\boldsymbol{H}}_{bb1}+\mathbf{W}_b^{(1)}\\ \mathbf{A}_1\mathbf{N}_{ab1}^H\Delta\hat{\mathbf{H}}_{ab1}^{(1)}+\mathbf{B}_1\mathbf{N}_{ba1}^H\Delta\hat{\mathbf{H}}_{bb1}+\mathbf{W}_b^{(2)}\end{bmatrix},\\ &=\mathbf{X}_a\mathbf{H}_{ab1}+\mathbf{X}_b\Delta\mathbf{H}_{bb1}+\mathbf{W}_b\end{aligned}\tag{36}$$

LMMSE estimator is utilized to estimate $\mathbf{H}_{ab1}$ as:

$$\begin{aligned}\hat{\mathbf{H}}_{ab1}^{(2)} =&\sigma_{ab}^2 N_{b1}\mathbf{X}_b^H\big(N_{b1}(\sigma_{ab}^2+\mathcal{E}_{bb})\mathbf{X}_b\mathbf{X}_b^H\\ &+\mathbf{R}_{\boldsymbol{W}_b}\big)^{-1}\boldsymbol{Y}_2,\end{aligned}\tag{37}$$

$$\begin{aligned}=&\sigma_{ab}^2 N_{b1}\left(\mathbf{I}_{N_b}+N_{b1}(\sigma_{ab}^2+\mathcal{E}_{bb})\mathbf{X}_b^H\mathbf{R}_{\boldsymbol{W}_b}^{-1}\mathbf{X}_b\right)^{-1}\\ &\mathbf{X}_b^H\mathbf{R}_{\boldsymbol{W}_b}^{-1}\boldsymbol{Y}_2.\end{aligned}\tag{38}$$

where (37) is converted to (38)by using matrix identity: $\mathbf{B}^H(\mathbf{A}+\mathbf{B}\mathbf{B}^H)^{-1} = (\mathbf{I}+\mathbf{B}^H\mathbf{A}^{-1}\mathbf{B})^{-1}\mathbf{B}^H\mathbf{A}^{-1}$, and $\mathbf{R}_{\boldsymbol{W}_b}$ corresponds to the covariance of $\boldsymbol{W}_b$, which can be calculated as:

$$\begin{aligned}\mathbf{R}_{\boldsymbol{W}_b} =&\mathbb{E}\left[\boldsymbol{W}_b\boldsymbol{W}_b^H\right],\\ =&\begin{bmatrix}mN_{b1}\mathbf{I}_{T_1} & \mathbf{0}\\ \mathbf{0} & kN_{b1}\mathbf{I}_{T_2}\end{bmatrix},\end{aligned}\tag{39}$$

where $m = \sigma^2+a_1\left(\mathcal{E}_{bb}+\sigma_{ab}^2\right)$, and $k = \sigma^2+a_2\left(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb}\right)$. Exploiting the independence between the corresponding null-space and estimation error, the covariance of $\mathbf{N}_{ab1}^H\Delta\hat{\mathbf{H}}_{ab1}^{(1)}$, and $\mathbf{N}_{ba1}^H\Delta\hat{\mathbf{H}}_{bb1}^{(1)}$ can be calculated as [4]: $(N_{b1})\mathcal{E}_{ab}^{(1)}\boldsymbol{I}_{N_{b1}}$, and $(N_{b1})\mathcal{E}_{bb}\boldsymbol{I}_{N_{b1}}$, respectively, as $N_a = N_b$. Substituting $\mathbf{R}_{\boldsymbol{W}_b}$ in $\hat{\mathbf{H}}_{ab1}^{(2)}$ we get:

$$\begin{aligned}\hat{\mathbf{H}}_{ab1}^{(2)} =&\frac{\sigma_{ab}^2}{1+(\sigma_{ab}^2+\mathcal{E}_{bb})\left(\frac{x_1}{m}+\frac{x_2}{k}\right)}\\ &\left[\frac{\mathbf{X}_b^{(1)^H}}{m}\quad\frac{\mathbf{X}_b^{(2)^H}}{k}\right]\boldsymbol{Y}_2,\end{aligned}\tag{40}$$

$$\triangleq\boldsymbol{H}_{ab1}+\Delta\hat{\mathbf{H}}_{ab1}^{(2)}.\tag{41}$$

The MSE for $\hat{\mathbf{H}}_{ab1}^{(2)}$ is given as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}(\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)})^H\right] =&\mathbb{E}\left[(\boldsymbol{H}_{ab1}-\hat{\boldsymbol{H}}_{ab1}^{(2)})\boldsymbol{H}_{ab1}^H\right]-\\ &\mathbb{E}\left[(\boldsymbol{H}_{ab1}-\hat{\boldsymbol{H}}_{ab1}^{(2)})\hat{\boldsymbol{H}}_{ab1}^{(2)^H}\right]\end{aligned}\tag{42}$$

The last term in the above equation can be shown equal to zeros by using the independence between the estimation error and the LMMSE estimate. After performing numerical simplifications the normalized MSE of $\hat{\mathbf{H}}_{ab1}^{(2)}$ is given as:

$$\mathcal{E}_{ab}^{(2)} =\frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}(\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)})^H\}]}{N_aN_{b1}},\tag{43}$$

$$\begin{aligned}=&\Bigg(\frac{1}{\mathcal{E}_{ab}^{(1)}}\\ &+\frac{m^2x_2}{(m+x_1\mathcal{E}_{bb})\left[x_2m\mathcal{E}_{bb}+(m+x_1\mathcal{E}_{bb})\,k\right]}\Bigg)^{-1}.\end{aligned}\tag{44}$$

The above relation indicates that the MSE improves with the utilization of the AN aided channel estimation stage at Bob.

At the eavesdropper: The signals received at the eavesdropper during the OAN assisted channel estimation stages are:

$$\boldsymbol{Y}_e^{(2)} = \begin{bmatrix}\boldsymbol{X}_{a,1}^{(2)}\\ \boldsymbol{X}_{a,2}^{(2)}\end{bmatrix}\boldsymbol{H}_{ae}+\begin{bmatrix}\boldsymbol{X}_{b,1}^{(2)}\\ \boldsymbol{X}_{b,2}^{(2)}\end{bmatrix}\boldsymbol{H}_{be}+\begin{bmatrix}\boldsymbol{W}_{e,1}^{(2)}\\ \boldsymbol{W}_{e,2}^{(2)}\end{bmatrix},\tag{45}$$

$$\begin{aligned}=&\begin{bmatrix}\sqrt{x_2}\boldsymbol{V}_a\\ \sqrt{x_2}\boldsymbol{V}_a\end{bmatrix}\boldsymbol{H}_{ae}+\begin{bmatrix}\sqrt{x_2}\boldsymbol{V}_b\\ \sqrt{x_2}\boldsymbol{V}_b\end{bmatrix}\boldsymbol{H}_{be}+\\ &\begin{bmatrix}\boldsymbol{A}_1\boldsymbol{N}_{ab1}^H\boldsymbol{H}_{ae}+\boldsymbol{B}_1\boldsymbol{N}_{ba1}^H\boldsymbol{H}_{be}+\boldsymbol{W}_{e,1}^{(2)}\\ \boldsymbol{A}_2\boldsymbol{N}_{ab2}^H\boldsymbol{H}_{ae}+\boldsymbol{B}_2\boldsymbol{N}_{ba2}^H\boldsymbol{H}_{be}+\boldsymbol{W}_{e,2}^{(2)}\end{bmatrix}.\end{aligned}\tag{46}$$

As already mentioned, $\boldsymbol{V}_a$ and $\boldsymbol{V}_b$ are globally known but x_2, $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{B}_1$,and $\boldsymbol{B}_2$ are not known globally. To utilize the signals received in the OAN assisted training stage for the estimation of $\boldsymbol{H}_{ae}$, the eavesdropper utilizes LS estimation by exploiting the global pilot sequences and the sums of the total transmitted power as:

$$\begin{aligned}\hat{\boldsymbol{H}}_{ae}^{(2)} &= \begin{bmatrix}\sqrt{P_2}\boldsymbol{V}_a \\ \sqrt{P_2}\boldsymbol{V}_a\end{bmatrix}^{\dagger} \boldsymbol{Y}_e^{(2)}, && (47)\\ &= \boldsymbol{V}_2^{\dagger}\boldsymbol{Y}_e^{(2)}, && (48)\\ &\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}^{(2)}, && (49)\end{aligned}$$

where $P_2 = x_2 + a_2$ is the sum of the total power transmitted in the third stage. Therefore, the overall sequential LS estimate of $\boldsymbol{H}_{ae}$ is given as:

$$\begin{aligned}\hat{\boldsymbol{H}}_{ae} &= \begin{bmatrix}\sqrt{P_1}\boldsymbol{V}_a \\ \sqrt{P_2}\boldsymbol{V}_a \\ \sqrt{P_2}\boldsymbol{V}_a\end{bmatrix}^{\dagger} \begin{bmatrix}\boldsymbol{Y}_e^{(1)} \\ \boldsymbol{Y}_e^{(2)}\end{bmatrix}, && (50)\\ &= \hat{\boldsymbol{H}}_{ae}^{(1)} + \frac{2P_2}{P_1+2P_2}\left(\hat{\boldsymbol{H}}_{ae}^{(2)} - \hat{\boldsymbol{H}}_{ae}^{(1)}\right), && (51)\\ &\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}. && (52)\end{aligned}$$

The MSE for $\hat{\boldsymbol{H}}_{ae}$ is given as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] =&\mathbb{E}\Bigg[\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}\right)\\ &\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}\right)^{H}\Bigg]. && (53)\end{aligned}$$

The above equation can be computed as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] =&\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}\right] - \frac{4P_2}{P_1+2P_2}\\ &\mathbb{E}\Bigg[\boldsymbol{H}_{ae}\hat{\boldsymbol{H}}_{ae}^{(2)^H} - \boldsymbol{H}_{ae}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\\ &- \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(2)^H} + \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\Bigg]\\ &- \frac{4P_2^2}{(P_1+2P_2)^2}\mathbb{E}\Bigg[\hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(2)^H}\\ &- \hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(1)^H} - \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(2)^H}\\ &+ \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\Bigg]. && (54)\end{aligned}$$

Finally, the normalized MSE $\mathcal{E}_{ae}^{(2)}$ is given as:

$$\begin{aligned}\mathcal{E}_{ae}^{(2)} =&\mathcal{E}_{ae}^{(1)} + \frac{4P_2}{(P_1+2P_2)^2}\Bigg(\frac{\sigma^2}{2} + \frac{a_2\left(\sigma_{ae}^2+\sigma_{be}^2\right)}{2}\\ &- \sigma_{ae}^2\left(\sqrt{\frac{x_2}{P_2}} - \sqrt{\frac{x_1}{P_1}}\right)(P_1+2P_2) + P_1\sqrt{\frac{x_1x_2}{P_1P_2}}\\ &\left(\sigma_{ae}^2 + c\sigma_{be}^2\right) - \frac{P_1+P_2}{P_1}\Big(x_1\left(\sigma_{ae}^2+c\sigma_{be}^2\right)\\ &+ a_1(\sigma_{ae}^2+\sigma_{be}^2) + \sigma^2\Big) + x_2\left(\sigma_{ae}^2+c\sigma_{be}^2\right)\Bigg). && (55)\end{aligned}$$

The above equation indicates that the eavesdropper can reduce the normalized MSE by utilizing the signals received in the third stage, depending on the parameters selected by the legitimate nodes.

D. Power Allocation

Both legitimate nodes perform power allocation after estimating the variance of the channel between them. For optimal power allocation, each node assumes that the estimated variance and the power allocation algorithms are the same at the other node.

To limit the channel estimation performance at the malicious user, the channel statistics of the eavesdropper's channel are required at the legitimate node. We have considered a passive eavesdropper, where the legitimate nodes do not have any information regarding the eavesdropper's channel. In the absence of statistical information regarding the eavesdropper, each legitimate node assumes all possible lucrative locations for the potential eavesdropper which can be exploited by the eavesdropper. These locations are used to acquire channel variance between the legitimate nodes and the eavesdropper by using a statistical path-loss model to calculate the achievable channel estimation performance at the eavesdropper. For the location of the eavesdropper, it is assumed that no malicious node can be within d_b units of the legitimate node, which implies that d_b represents the radius of a circular boundary around the legitimate node Bob. Possible lucrative locations for the eavesdropper are shown in Fig. 3, where the dotted area indicates the lucrative position for the eavesdropper to acquire robust estimates regarding $\boldsymbol{H}_{be}$, as it is close to Bob.

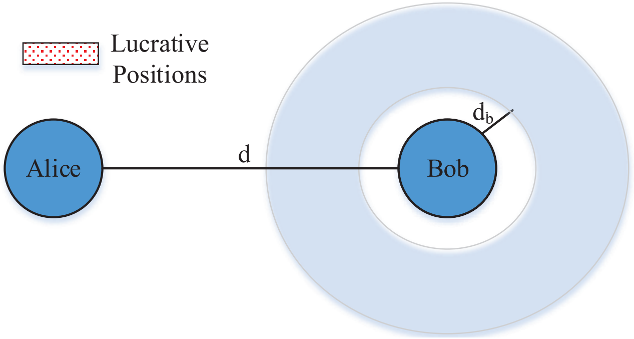

Fig. 3: Possible lucrative locations for any potential eavesdropper.

To analyze the performance of the eavesdropper at the lucrative positions, Bob generates points in the circle where the radius is greater than d_b and less than $d/2$. Bob can calculate the variance of the channels $\boldsymbol{H}_{ae}$, and $\boldsymbol{H}_{be}$, by using the estimated legitimate channel variance and the specified path-loss model. The calculated variances are utilized to estimate the achievable statistical performance at Bob by using $\mathcal{E}_{ab}^{(2)}$ as given in (44) and at the eavesdropper by using $\mathcal{E}_{ae}^{(2)}$ as given in (55). From [35], [39], the received SNR for MIMO system with channel estimation error is given as:

$$SNR_{ae} = \frac{P\left(\sigma_{ae}^2 - \mathcal{E}_{ae}^{(2)}\right)}{\sigma^2 + P\mathcal{E}_{ae}^{(2)}}, \tag{56}$$

where P denotes the power used for data transmission. The detailed derivation and explanation of the above relation can be found in [35], [39]. It can be seen from (56), that the received SNR is directly related to the channel variance. Hence, in order to select the optimal location for eavesdropping on Bob, we select the position where the variance of channel $\boldsymbol{H}_{ae}$ is maximum and out of those position where $\boldsymbol{H}_{be}$ channel variance is minimum, which results in less interference for the eavesdropper during channel estimation stage. Based on the selected eavesdropper location and MSE the power allocation tries to optimize the following condition:

$$\min_{\substack{\mathcal{E}_{ae}^{(2)} \geq \gamma \\ x_1+a_1 \leq P_{avg} \\ x_2+a_2 \leq P_{avg}}} \quad \mathcal{E}_{ab}^{(2)}, \tag{57}$$

where $\mathcal{E}_{ae}^{(2)}$ and $\mathcal{E}_{ab}^{(2)}$ for ANFD-DCE are given in (55) and (44), respectively and P_{avg} is the average transmission power available for each channel training stage, which corresponds to the maximum transmit power of the transmission device. Brute-force search algorithm is used to get the values of x_1, x_2, a_1 and a_2, which satisfies the above conditions. If the value of γ is selected such that: $\nexists(x_1, x_2, a_1, a_2) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$, then it is decreased by a small value ϵ until $\exists(x_1, x_2, a_1, a_2) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$.

IV. Simulation Analysis and Results

In this section, simulation analysis is presented to demonstrate the secrecy performance achieved by the proposed ANFD-DCE scheme. We have considered the MIMO wireless system as mentioned in Section II, where $N_a = 4$, $N_b = [3, 4, 6]$, and $N_e = [4, 8, 12]$ at Alice, Bob, and the 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 $d_{ref} = 1m$, and path loss exponent is 1.6 for simplified path-loss channel model given in [23], which implies that we have considered indoor office environment as our simulation scenario. The variance of the residual SI channel is considered as given by experimental evaluations in [27]. As the estimation performance is highly dependent on the system noise denoted by σ^2, for the simulation analysis σ^2 is varied between 10^{-4} to 4×10^{-6} depending on the SNR. The SNR in all figures corresponds to the received SNR at the legitimate node, all the corresponding SNR can be calculated by using the respective channel variances. All the data transmission symbols are taken from the 16-ary QAM constellation.

A. Location-Based Simulation Analysis

For location-based simulation analysis, we have considered all the possible lucrative locations for the eavesdropper in a circle around the legitimate transmitter (Alice), with a radius of 2 to 2.6 meters with a step of $0.2m$ from Alice; as the closest eavesdropper can get to Alice is equal to the radius of the circular boundary around Alice $d_b = 2m$. At each radius, we have considered 18 locations for the eavesdropper to capture the effect of different locations on the performance achieved by the eavesdropper. Each location of the eavesdropper is shown on the coordinate plane, where each unit is equal to one meter. For the optimization algorithm given in Section III-D, we have utilized $\gamma = 1.5 \times 10^{-2}$ for $d_b = 2m$. First, we present the location-based analysis of the existing FD-DCE [15] scheme followed by the results of the proposed ANFD-DCE to better illustrate the performance improvements.

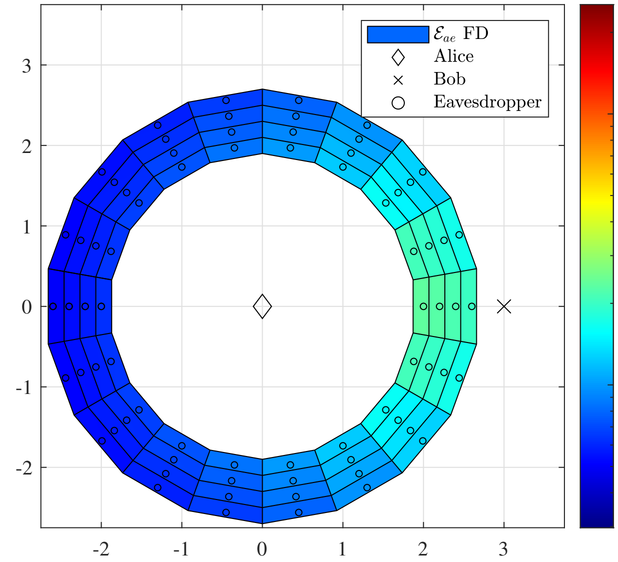

Fig. 4: MSE for the existing FD-DCE [15] for different locations of the eavesdropper on a coordinate plane for 16 dB SNR at the legitimate receiver, while MSE for FD-DCE at Bob is: $\mathcal{E}_{ab} = 9.43 \times 10^{-5}$.

Fig. 4 presents the MSE analysis of the FD-DCE scheme. Alice and Bob are located at (0,0) and (3,0) on the coordinate plane, respectively. The location of the eavesdropper is indicated by the circles and the color of each tile indicates the MSE of the channel $\boldsymbol{H}_{ae}$ at the respective circled position. Fig. 4 shows that for FD-DCE without AN the eavesdropper can acquire robust channel estimate as the eavesdropper is close to the Alice as compared to Bob.

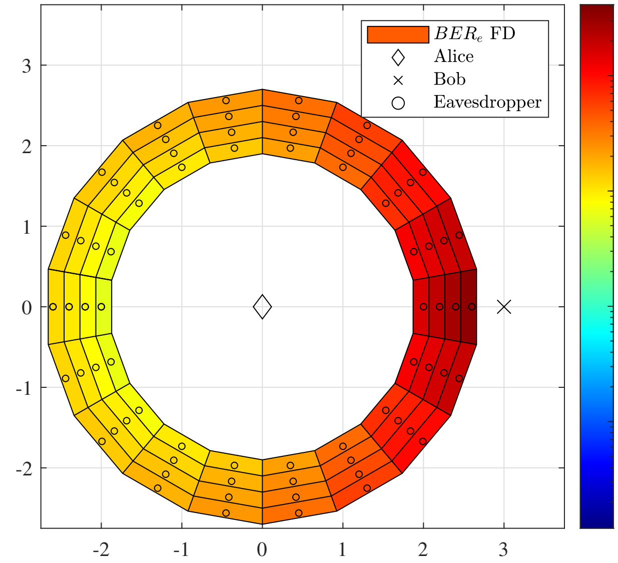

Fig. 5: BER for FD-DCE [15] at different locations of the eavesdropper for 16 dB SNR at the legitimate receiver, while BER at Bob is: $BER_{ab} = 2.1 \times 10^{-5}$.

To indicate the effect of MSE on the system level performance, we have presented BER analysis for each location. We have utilized a rate $1/2$ Orthogonal Space Time Block Codes (OSTBC) with four transmit antennas for 16-QAM signal as given in [40]. The receivers utilize channel estimated in the previous stage to estimate the signal transmitted by Alice. Fig. 5, shows the BER achieved by the eavesdropper at different locations for FD-DCE. BER simulation analysis indicates that performance at the eavesdropper improves as it is located away from Bob. Finally, the BER analysis in Fig. 5 shows that the FD-DCE achieves secure communication if the eavesdropper is located in between the legitimate node, and the BER at the eavesdropper improves as it moves away from the FD legitimate receiver Bob.

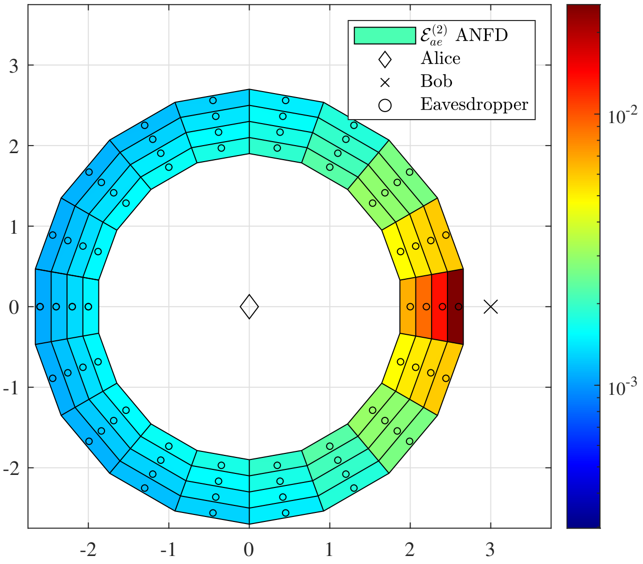

Fig. 6: MSE at different locations of the eavesdropper in the third stage for 16 dB SNR at Bob, while MSE at Bob in the third stage is: $\mathcal{E}^{(2)}_{ab} = 1.43 \times 10^{-4}$.

MSE for ANFD-DCE at the eavesdropper shown in Fig. 6 corresponds to the MSE achieved after the third stage using the sequential LS estimator denoted as $\mathcal{E}^{(2)}_{ae}$. We have considered the MSE at the eavesdropper after the third as it provides a significant performance improvement over the second stage due to the sequential LS estimator utilized in the third stage. The comparison of MSE performance at the eavesdropper for FD-DCE in Fig. 4 to the proposed ANFD-DCE in Fig. 6 shows that the ANFD-DCE reduces the leakage of channel estimates to the eavesdropper as it moves away from the FD legitimate receiver Bob.

Fig. 7 shows BER achieved by ANFD-DCE for the channel estimated in the third stage for each location of the eavesdropper. BER analysis indicates that ANFD-DCE improves the secrecy of the communication by maintaining the BER at the eavesdropper close to 0.1. It also indicates that as compared to the BER achieved by the FD-DCE in Fig. 5, the proposed ANFD-DCE establishes secure communication for the optimal eavesdropping location where the eavesdropper can robustly decode the information for the FD-DCE. This figure also indicates that BER at the eavesdropper improves as it moves away from Bob. However, the BER decreases as the eavesdropper moves away from Alice due to the increase in path loss for data transmission, although MSE improves for the eavesdropper as shown in Fig. 4.

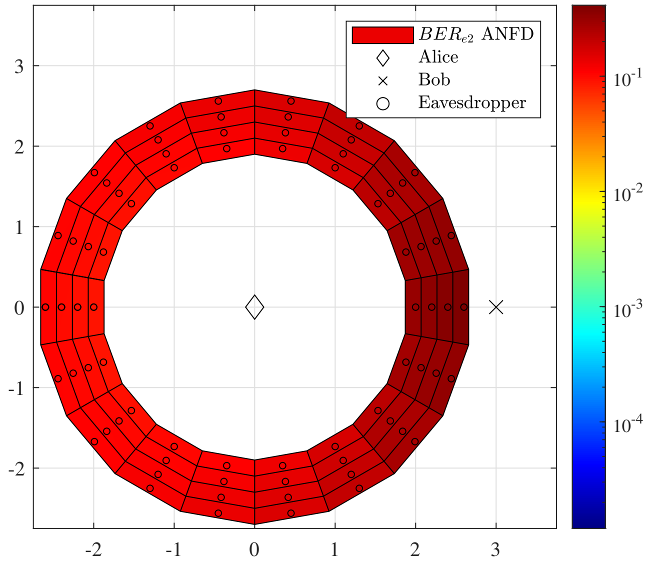

Fig. 7: BER at different locations of the eavesdropper in the third stage for 16 dB SNR at the legitimate receiver, while BER at Bob for channel estimated in the third stage is: $BER^{(2)}_{ab} = 2.97 \times 10^{-4}$.

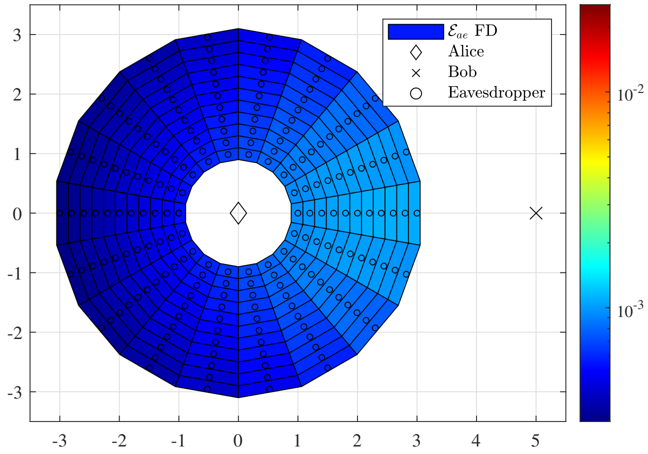

Fig. 8: MSE for the existing FD-DCE [15] for different locations of the eavesdropper on a coordinate plane for 17 dB SNR at the legitimate receiver, while MSE for FD-DCE at Bob is: $\mathcal{E}_{ab} = 2.43 \times 10^{-5}$.

We have also considered $d_b = 1m$ to further analyze the effect of the boundary around Alice on the performance achieved by the respective DCE techniques. For the power allocation algorithm of the ANFD-DCE, we have utilized $\gamma = 4.5 \times 10^{-3}$ for $d_b = 1m$. The distance between the legitimate nodes is $5m$, and the eavesdropper is located in a circle around Alice with a radius from $1m$ to $3m$ with a step of $0.2m$.

The MSE and BER for the FD-DCE are presented in Fig. 8, and Fig. 9, respectively. These results show that the

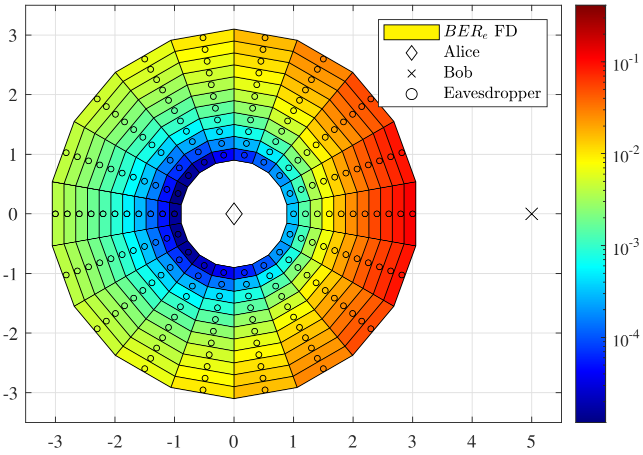

Fig. 9: BER for FD-DCE [15] at different locations of the eavesdropper for 17 dB SNR at the legitimate receiver, while BER at Bob is less than 10^{-5}.

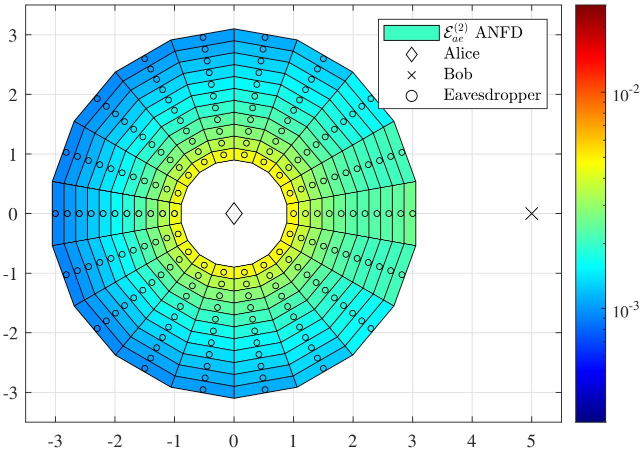

Fig. 10: MSE at different locations of the eavesdropper in the third channel estimation stage for 17 dB SNR at Bob, while MSE at Bob in the third stage is: $\mathcal{E}_{ab}^{(2)} = 5.15 \times 10^{-5}$.

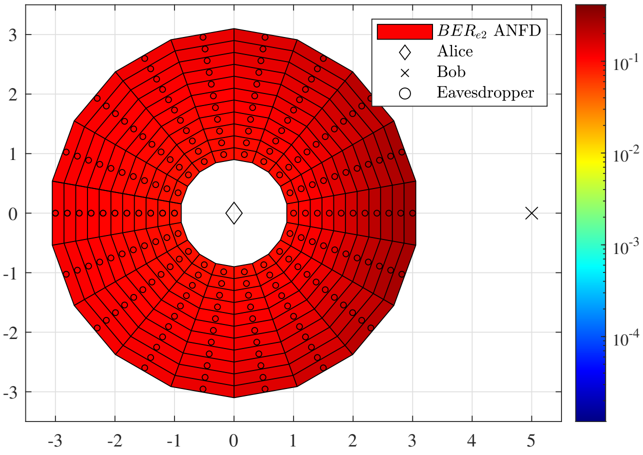

Fig. 11: BER at different locations of the eavesdropper for 17 dB SNR at the legitimate receiver, while BER at Bob for channel estimated in the third stage is: $BER_{ab}^{(2)} = 7.5 \times 10^{-5}$.

FD-DCE is unable to achieve secure communication for the eavesdropper located on the opposite side of Bob, especially if the eavesdropper is located close to Alice. However, the FD-DCE achieves equivocation for the eavesdropper located between Alice and Bob, especially if the boundary around Alice d_b is greater than $1.5m$.

For the proposed ANFD-DCE, the MSE and BER analysis are shown in Fig. 10, and Fig. 11, respectively. The ANFD-DCE achieves robust secure communication as the BER at the eavesdropper remains close to 0.1, while BER at Bob is less than 10^{-4}. These results indicate that the FD-DCE [17] is unable to avoid the leakage of information to the strategically located eavesdropper.

B. Simulation Analysis for Optimal Location of Eavesdropping

To provide an in-depth performance analysis, we have considered the optimal location for eavesdropping on Alice, by considering the received SNR at the eavesdropper as given in (56). The optimal location for eavesdropping on Alice is the location with a radius of d_b in the opposite direction of the legitimate receiver to minimize the interference received during the channel estimation stage. For the considered position we have provided MSE and BER comparisons with the existing FD-DCE technique.

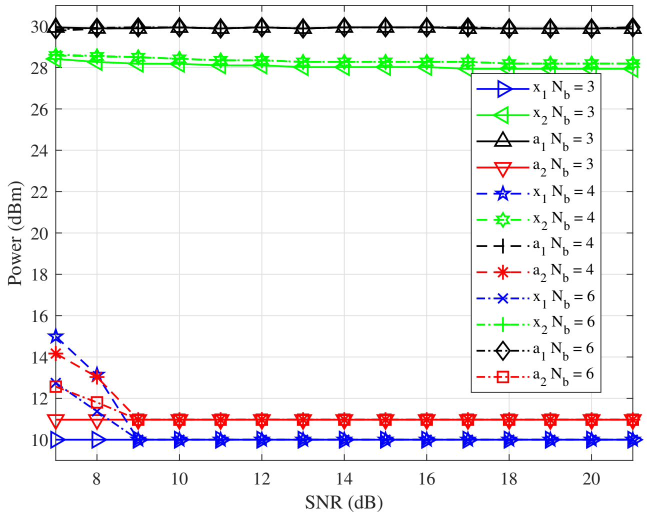

Fig. 12: Average power allocation for training signals and AN for legitimate nodes, while $N_b = [3, 4, 6]$, and $N_a = 4$.

First, we have provided the results for $d_b = 2m$ and the distance between Alice and Bob is $3m$. Fig. 12 shows the average power allocation to the training signal x_1, and x_2, and the AN a_1, and a_2 where the horizontal axis represents the received SNR at the legitimate receiver in dB, and the vertical axis corresponds to power in dBm. We have considered average power P_{avg} to be $30dBm$. We have included the power allocation for the different number of antennas at Bob. These results indicate that for the proposed ANFD-DCE, the power allocated to the training signal in the second stage (Rough Channel Estimation Stage) is kept to a minimum to avoid the leakage of channel estimates while using AN to cause equivocation at the eavesdropper. These results also show that the power allocation differs slightly for the different number of antennas, as the variance of the AN signals is normalized to the number of transmit antennas. The MSE analysis for the proposed ANFD-DCE along with the comparison to the existing FD-DCE is presented in Fig. 13, and 14, where the vertical axis corresponds to MSE and the horizontal axis indicates the received SNR at the legitimate node. For Fig. 13, we have considered equal number of antennas at the legitimate nodes such that $N_a = N_b = 4$. These results indicate that the proposed ANFD-DCE achieves higher MSE at the eavesdropper as compared to the existing FD-DCE technique. Meanwhile, MSE of the legitimate channel $\boldsymbol{H}_{ab}$ is also higher for proposed ANFD-DCE as compared to FD-DCE, as the use of AN also limits the estimation performance for the legitimate channel. Fig. 13 shows that increasing the number of eavesdropping antennas N_e does not affect the MSE at the eavesdropper. This figure also shows that for the ANFD-DCE, the channel estimation performance improves with the usage of sequential LS estimator in the third at the eavesdropper. Therefore, we have used the MSE at the eavesdropper in the third stage for the location-based performance analysis and the rest of this section.

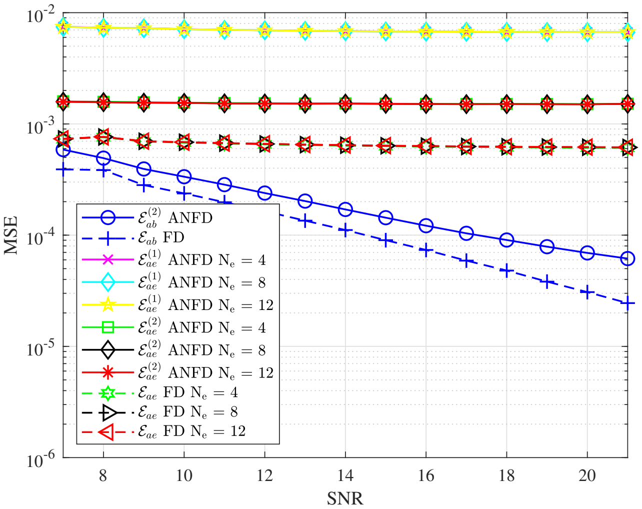

Fig. 13: MSE for ANFD-CE and FD-CE [17], while $N_a = N_b = 4$, and $N_e = [4, 8, 12]$.

Fig. 14 shows MSE for scenario where $N_a \neq N_b$, and $N_e = 4$, as MSE remains the same for the different number of antennas at the eavesdropper as shown in Fig. 13. The slight variation of MSE at Bob $\mathcal{E}_{ab}^{(2)}$ for the different number of antennas N_b can be attributed to the difference in power allocation as shown in Fig. 12. MSE analysis shows that decreasing the number of antennas at Bob improves the channel estimation performance at the eavesdropper as it implies that the eavesdropper receives less interference from Bob during the channel estimation. Finally, a comparison of MSE at the legitimate node for the proposed ANFD-DCE against FD-DCE [17] indicates that the proposed ANFD-DCE performs close to the existing scheme while maintaining higher MSE at the eavesdropper.

In Fig. 15, and Fig. 16 we have shown the BER achieved at all nodes on the vertical axis against the received SNR at

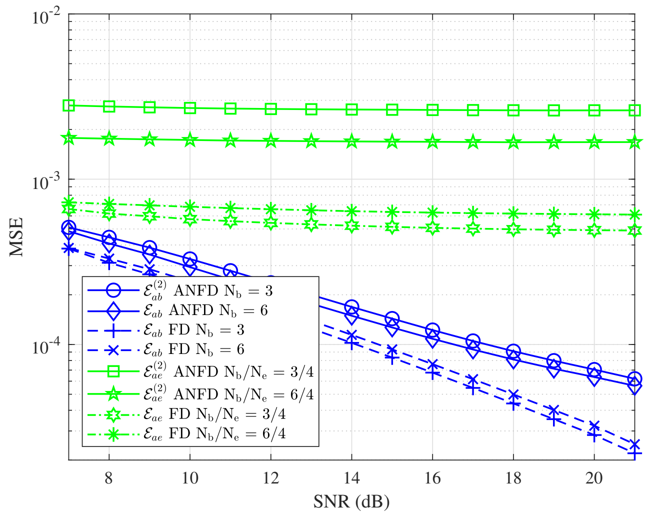

Fig. 14: MSE for ANFD-DCE and FD-DCE [17], while $N_a \neq N_b$ such that: $N_a = 4$, $N_b = [3, 6]$, and $N_e = 4$.

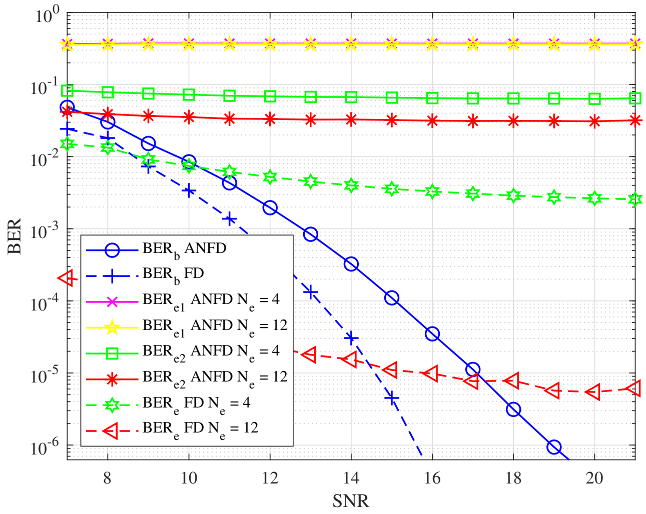

Fig. 15: BER for ANFD-DCE and FD-DCE [17], while $N_a = N_b = 4$, and $N_e = [4, 12]$.

the legitimate node on the horizontal axis. In Fig. 15 presents results for the scenario where $N_a = N_b = 4$. This figure shows that the BER at the eavesdropper improves with the increase in the number of eavesdropping antennas. However, the proposed ANFD-DCE maintains the BER higher than 10^{-2} at the eavesdropper even for $N_e = 12$. As for the existing FD-DCE, BER for the eavesdropper with $N_e = 4$ is better than the legitimate node at the low SNR due to less path-loss as compared to Bob. For the existing FD-DCE, BER for the eavesdropper with $N_e = 12$ is less than 10^{-5} at high SNR, which implies that the existing FD-DCE becomes unable to achieve secure communication with a three times increase in the number of eavesdropping antennas. The gap in BER at Bob for ANFD-DCE as compared to the existing FD-DCE shows the effect of AN on legitimate communication. Fig. 15 also shows that for the ANFD-DCE use of the sequential LS estimator in the third stage results in the improved BER at the eavesdropper. Therefore, the eavesdropper will use the channel

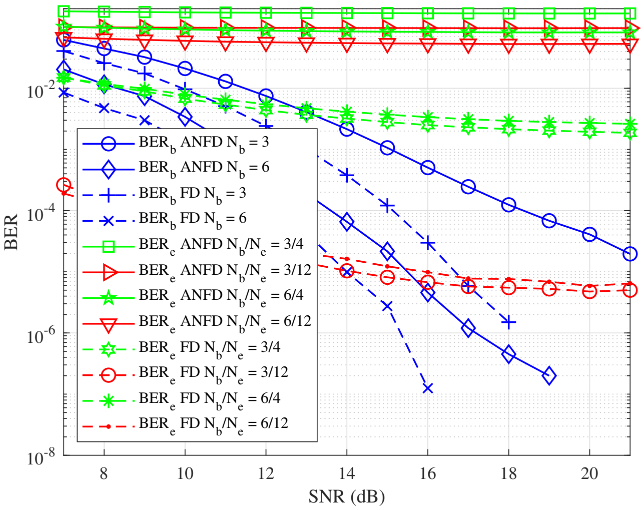

Fig. 16: BER for ANFD-DCE and FD-DCE [17], while $N_a \neq N_b$ such that: $N_a = 4$, $N_b = [3, 6]$, and $N_e = [4, 12]$.

estimated in the third stage for MSE and BER.

In Fig. 16, we have presented the BER for the scenario $N_a \neq N_b$. This figure shows that the BER at Bob improves with an increase in the number of antennas at Bob. The difference in BER is greater for ANFD-DCE as the variance of the AN signals increases because it is normalized to the number of antennas. This figure also shows that the eavesdropper does not show significant variation in the BER due to an increase in the number of antennas at Bob.

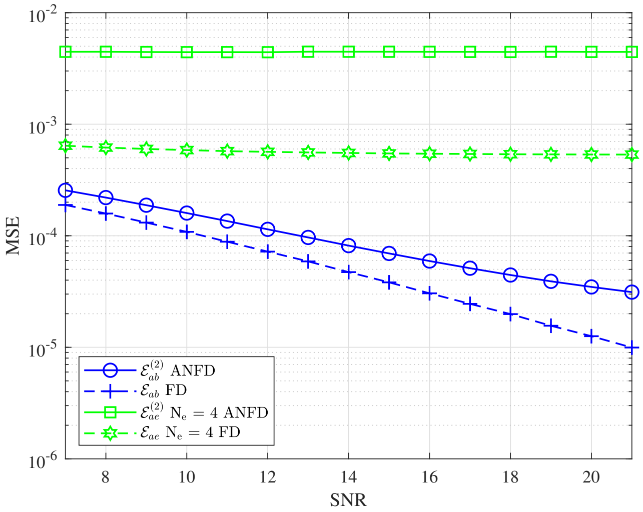

Fig. 17: MSE for ANFD-DCE and FD-DCE [17], while $d_b = 1m$, $N_a = N_b = 4$, and $N_e = [4, 12]$.

Fig. 17, and Fig. 18 shows the performance of the DCE techniques for the optimal eavesdropping location with $d_b = 1m$ around Alice, and the distance between the legitimate nodes is $5m$. The results show that the FD-DCE is unable to achieve secure communication as the eavesdropper is able to robustly decode the received signal with BER less than 10^{-4}. We have omitted the BER results for the FD-DCE at the eavesdropper with $N_e = 12$, as it remains below 10^{-6}. The proposed ANFD-DCE achieves robust secure communication as the BER at Bob is less than 10^{-5} while the BER at the eavesdropper is close to 10^{-1}, even with 12 eavesdropping antennas. These results show that the ANFD-DCE can establish a robust and secure communication link by avoiding the leakage of the channel estimates to the eavesdropper. Finally, these simulation results demonstrate that the proposed ANFD-DCE provides secure communication against a strategically located passive eavesdropper with three times more antennas than the legitimate transmitter by using AN signals along with FD transmissions.

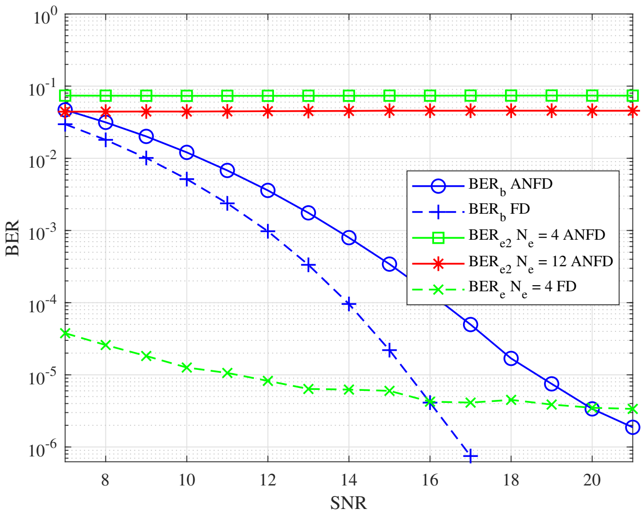

Fig. 18: BER for ANFD-DCE and FD-DCE [17], while $d_b = 1m$, $N_a = N_b = 4$, and $N_e = [4, 12]$.

V. Conclusion

In this paper, we have presented a novel ANFD-DCE, to overcome the leakage of channel estimates to a strategically located adversary. The proposed ANFD-DCE comprises three stages responsible for estimation of SI channel, rough channel estimates for orthogonal AN design, and orthogonal AN assisted training in the first, second, and third stages, respectively. We have provided MSE for each stage to analyze the achievable statistical performance. The simulation analysis is divided into two parts, where the first part provides location-based analysis to demonstrate that the proposed ANFD-DCE provides better secrecy performance than the existing FD-DCE for different locations of the eavesdropper. The second part of simulation analysis shows that for optimal eavesdropping location, the proposed ANFD-DCE outperforms the existing FD-DCE for a range of SNR values.

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] C. Wang, E. K. Au, R. D. Murch, W. H. Mow, R. S. Cheng, and V. Lau, "On the performance of the MIMO zero-forcing receiver in the presence of channel estimation error," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 805–810, 2007.

[4] 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, 2010.

[5] 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, 2013.

[6] O. O. Koyluoglu and H. El Gamal, “Polar Coding for Secure Transmission and Key Agreement,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1472–1483, 2012.

[7] A. O. Hero III, “Secure Space-Time Communication,” *IEEE Trans Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[8] N. Anand, S.-J. Lee, and E. W. Knightly, “STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming,” in *Proc. IEEE Int. Conf. on Computer Commun. (INFOCOM 12)*, Mar. 2012, pp. 720–728.

[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, 2011.

[10] 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, 2015.

[11] 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, 2016.

[12] 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)*. IEEE, 2018, pp. 1–6.

[13] 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.

[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, 2013.

[15] F. Ud Din and F. Labeau, “Physical Layer Security Through Secure Channel Estimation,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–5.

[16] Y. Hua, “Advanced Properties of Full-Duplex Radio for Securing Wireless Network,” *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 120–135, 2019.

[17] F. Ud Din and F. Labeau, “In-band full-duplex discriminatory channel estimation using mmse,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3283–3292, 2020.

[18] 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, 2014.

[19] T.-Y. Liu, Y.-C. Chen, and Y.-W. P. Hong, “Artificial Noise Design for Discriminatory Channel Estimation in Wireless MIMO Systems,” in *Proc. IEEE Global Commun. Conf. (GLOBECOM 14)*, Dec. 2014, pp. 3032–3037.

[20] C.-J. Chun, J.-H. Lee, and H.-M. Kim, “Discriminatory Channel Estimation in MIMO Decode-and-Forward Relay Systems with Cooperative Jamming,” in *Proc. IEEE Int. Conf. Commun. Workshops (ICC 16)*, May 2016, pp. 266–271.

[21] J. Bezanilla and J. Via, “Antenna Grouping for General Discriminatory Channel Estimation,” in *Porc. International Conf. Wireless Commun. & Signal Processing (WCSP 15)*, Oct. 2015, pp. 1–5.

[22] S. Haile, “Investigation of channel reciprocity for OFDM TDD systems,” Master’s thesis, University of Waterloo, 2009.

[23] A. Goldsmith, *Wireless Communications*. Cambridge university press, 2005.

[24] D. Bharadia, E. McMilin, and S. Katti, “Full Duplex Radios,” in *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4. ACM, 2013, pp. 375–386.

[25] N. Reiskarimian, J. Zhou, and H. Krishnaswamy, “A CMOS passive LPTV nonmagnetic circulator and its application in a full-duplex receiver,” *IEEE J. Solid-State Circuits*, vol. 52, no. 5, pp. 1358–1372, 2017.

[26] 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.

[27] 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, 2012.

[28] I. Krikidis, H. A. Suraweera, P. J. Smith, and C. Yuen, “Full-duplex relay selection for amplify-and-forward cooperative networks,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381–4393, 2012.

[29] 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, 2017.

[30] 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. Inf. Forensics Security*, vol. 13, no. 11, pp. 2788–2800, 2018.

[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)*. IEEE, 2017, pp. 883–887.

[32] 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, 2015.

[33] S. Sesia, I. Toufik, and M. Baker, *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons, 2011.

[34] 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.

[35] 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, 2003.

[36] 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, 2003.

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

[38] J. Li, J. Conan, and S. Pierre, “Joint estimation of channel parameters for MIMO communication systems,” in *2005 2nd International Symposium on Wireless Communication Systems*. IEEE, 2005, pp. 22–26.

[39] T. Yoo and A. Goldsmith, “Capacity and Power Allocation for Fading MIMO Channels with Channel Estimation Error,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, 2006.

[40] 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, 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.