Physical Layer Security Through Secure Channel Estimation

Fawad Ud Din

Department of Electrical & Computer Engineering
McGill University
Montreal

June 2021

A thesis submitted to McGill University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Abstract

Wireless communication is highly susceptible to eavesdropping attacks where a malicious user can exploit the broadcast nature of the wireless signals to eavesdrop on confidential information. At the physical layer, there are multiple possible avenues to utilize the inherent randomness of the wireless transmission medium to achieve secure communication. One of the lucrative possibilities is to use the channel state information (CSI) to establish a secure communication link because it is vital in decoding the received signal at the transmitter. This technique is commonly referred to as discriminatory channel estimation (DCE) where the channel estimation performance is intentionally degraded at the eavesdropper as compared to the legitimate nodes to achieve secure communication.

In this thesis, we capitalize on full-duplex (FD) transmissions to transmit the pilot signals to obscure the channel estimates from the eavesdropper. FD transmission severely limits the estimation performance at the eavesdropper while the legitimate nodes can acquire robust estimates. The secrecy of channel estimates from the eavesdropper provides a bandwidth-efficient security technique as the channel estimation requires less bandwidth than the data transmission. We have presented the achievable secrecy capacity analysis along with the simulation analysis to illustrate the performance improvements achieved by the proposed novel secure channel estimation.

In this thesis, we also study the impact of artificial noise (AN) to improve the secrecy achieved by the use of FD transmission of pilot signals. For a strategically located eavesdropper, we have presented novel DCE techniques where AN signals are transmitted along with pilot signals using FD transmission. The AN signals confuse the nearby eavesdropper to establish a secure and robust communication link. We have also presented novel local adaptive power allocation algorithms, where each legitimate node performs power allocation in the absence of statistical channel characteristics regarding the eavesdropping channel. We have provided an in-depth simulation analysis including a location-based simulation analysis to illustrate that the secrecy performance achieved by the proposed DCE techniques. The simulation results indicate that the proposed DCE techniques achieve robust secure communication against a strategically located eavesdropper: while the other DCE techniques are unable to avoid the leakage of information to the eavesdropper.

Résumé

La communication sans fil est très sensible aux attaques par écoute clandestine où un utilisateur malveillant peut exploiter la nature de diffusion des signaux sans fil pour écouter des informations confidentielles. Au niveau de la couche physique, il existe de multiples avenues possibles pour utiliser le caractère aléatoire inhérent du support de transmission sans fil pour obtenir une communication sécurisée. L'une des possibilités lucratives est d'utiliser les informations d'état de canal (CSI) pour établir une liaison de communication sécurisée car elle est vitale pour décoder le signal reçu au niveau de l'émetteur. Cette technique est communément appelée estimation de canal discriminatoire (DCE) où les performances d'estimation de canal sont intentionnellement dégradées au niveau du nœud espion par rapport aux nœuds légitimes pour obtenir une communication sécurisée.

Dans ce mémoire, nous capitalisons sur les transmissions en full-duplex (FD) pour transmettre les signaux pilotes afin d'obscurcir les estimations de canal par le nœud espion. La transmission FD limite considérablement les performances d'estimation au niveau du nœud espion tandis que les nœuds légitimes peuvent acquérir des estimations robustes. Le secret des estimations de canal provenant de l'écoute indiscrète fournit une technique de sécurité efficace en bande passante car l'estimation de canal nécessite moins de bande passante que la transmission de données. Nous avons présenté l'analyse réalisable de la capacité de confidentialité ainsi qu'une analyse par simulation pour illustrer les améliorations de performances obtenues par la nouvelle estimation de canal sécurisé proposées.

Dans ce mémoire, nous avons également étudié l'impact du bruit artificiel (AN) pour améliorer le secret obtenu par l'utilisation de la transmission FD de signaux pilotes. Dans le cas d'un nœud espion stratégiquement situé, nous avons présenté de nouvelles techniques DCE où les signaux AN sont transmis avec les signaux pilotes en utilisant la transmission FD. Les signaux AN confondent le nœud espion à proximité en l'empêchant d'établir une liaison de communication sécurisée et robuste. Nous avons également présenté de nouveaux algorithmes d'allocations de puissance adaptative locale, où chaque nœud légitime effectue une allocation de puissance en l'absence de caractéristiques de canal statistiques concernant le canal d'écoute. Nous avons fourni une analyse de simulation approfondie, y compris une analyse de simulation basée sur la localisation, pour illustrer les performances de confidentialité obtenues par les techniques DCE proposées. Les résultats de la simulation indiquent

que les techniques DCE proposées permettent une communication sécurisée robuste contre un écouteur malintentionné stratégiquement situé: tandis que les autres techniques DCE sont incapables d'éviter la fuite d'informations vers un écouteur clandestine.

Acknowledgments

First and foremost, I begin in the name of God the most Merciful and Beneficent, to Whom all the praise belongs for enabling me to accomplish all that I have accomplished.

I would like to express my deepest gratitude to my mentor and supervisor Professor Fabrice Labeau. His constant motivation, guidance, support, and mentorship helped me throughout the Ph.D. program. During this time, I learned a lot under his supervision both on personal terms and on work ethic.

I would also like to thank Professors Ioannis Psaromiligkos and Georges Kaddoum for being on my committee and providing valuable comments. I am also thankful to Professors Michael Rabbat and Tho Le-Ngoc from whom I learned a great deal attending their courses as a part of my Ph.D. work.

I would like to gratefully acknowledge the financial support of the McGill Engineering Doctoral Award (MEDA), Natural Science and Engineering Research Council (NSERC), and Hydro-Quebec throughout my Ph.D. program.

I would like to thank my colleagues in the lab, both past and present, for the stimulating conversations and companionship over the years. Your support both scientifically and personally was valuable in supporting me during stressful and difficult moments. A huge thank-you goes to all of my wonderful friends who have always believed in me.

Last but not the least, I would like to express my gratitude to my wife, my parents, my grandparents, and my siblings for their unconditional support and prayers though-out the Ph.D. My parents who raised me supported me and taught me to be the person I am today. My wife, Durria, for the gracious support and sacrifice though-out the Ph.D. Our son, for filling our lives with joy and commitment, especially during the global pandemic. I would also like to express my gratitude to my grandfather for instilling the values of curiosity, perseverance, and discipline in my life that enabled me to achieve my goals in my Ph.D.

Preface

All the work presented in this thesis was conducted by the author under the Ph.D. supervision of Professor Fabrice Labeau, at Telecommunications & Signal Processing Laboratory in the Department of Electrical and Computer Engineering at McGill University.

Chapter 2 presents a comprehensive literature review of the subject. A part of Chapter 2 has also been published [62]. Chapters 3, and 4 present the main contributions of this thesis. A version of Chapters 3 and 4 has been published [74, 75], or submitted for publication [98]. The author was responsible for the design of novel channel estimation techniques, novel power allocation algorithms, system models, mathematical derivations, computer simulations, and the composition of all the manuscripts and the chapters of this thesis. Professor Fabrice Labeau has supervised the whole research, provided research direction and guidance, and extensively revised all the manuscripts and the chapters of this thesis.

The detailed contributions of this thesis to the original literature are described in Section 1.2.

[62] 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.

[74] 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.

[75] F. Ud Din and F. Labeau, "In-band Full-Duplex Discriminatory Channel Estimation using MMSE," IEEE Trans. Inform. Forensic Secur., pp. 1-1, 2020.

[98] F. Ud Din and F. Labeau, "Artificial Noise Assisted In-Band Full-Duplex Secure Channel Estimation,"IEEE Trans. Veh. Technol., submitted for publication.

Contents

List of Figures

List of Acronyms

AF	Amplify and Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BCE	Blind Channel Estimation
BER	Bit Error Rate
CP	Cyclic Prefix
CSI	Channel State Information
DCE	Discriminatory Channel Estimation
FD	Full-Duplex
GSVD	Generalized Singular Value Decomposition
IC	Interference Cancellation
ICA	Independent Component Analysis
LMMSE	Linear Minimum Mean Square Error
LDPC	Low-Density Parity-Check
LS	Least Squares
LTE	Long Term Evolution
LNA	Low Noise Amplifier
MIMO	Multiple-Input and Multiple-Output
MLE	Maximum Likelihood Estimator
MSE	Mean Square Error
NOMA	Non-Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
OSTBC	Orthogonal Space-Time Block Codes
PA	Power Amplifier

PLS	Physical Layer Security
QAM	Quadrature Amplitude Modulation
RF	Radio Frequency
RSS	Received Signal Strength
SCE	Standard Channel Estimation
SI	Self-Interference
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio
STBC	Space-Time Block Codes
WARP	Wireless Open Access Research Platform
WSN	Wireless Sensor Network
ZMCSWGN	Zero Mean Circularly Symmetric White Gaussian Noise

Chapter 1

Introduction

1.1 Motivation

Recent advancements in communications technologies have resulted in an avalanche of connected devices and smart networks. These advancements have widely impacted our lives, for example, smart homes, smart cars, and smart power grids. Wireless communications have played a major role in enabling these smart devices and smart networks, commonly referred to as wireless sensor networks (WSNs). WSNs are widely employed in the oil, gas, and natural resources industry [1] as they tremendously reduce the cost, increase the network coverage, and reduce the deployment time as compared to the wired networks. The growing penetration of wireless networks has raised concerns regarding their security and privacy due to the broadcast nature of the wireless transmission medium. The security threats in wireless networks can result in colossal damage, as their applications include many sensitive governmental, military, and commercial uses [2]. The privacy and security threats in wireless communications are classified into three broad categories: jamming attack, malicious data injection, and eavesdropping. In the jamming attacks, the malicious user deliberately transmits a signal to block or jam the communication link between legitimate nodes. These attacks could make the attacked wireless network inoperable. Similarly, in the malicious data injection attacks, the attacker carefully injects false data to cause damage. In an eavesdropping attack, the adversary intercepts information over the wireless channel to acquire critical and private information. The eavesdropping attacks can be passive where the eavesdropper does not transmit any signal or active where the eavesdropper also transmits its signal. The

eavesdropping attacks on wireless networks are most prevalent due to the broadcast nature of wireless communication. This thesis will focus on providing secrecy against passive eavesdropping attacks. The passive nature of the eavesdropper makes this task challenging as it is impossible to acquire any knowledge regarding the presence and the channel characteristics of the eavesdropper.

Novel attacks on wireless communications have exposed personal information to malicious users, such as a smart video doorbell commercially known as Ring which has exposed users' WiFi credentials [3]. Similarly, another vulnerability of WiFi devices called Kr00k affected millions of devices, where the malicious user can passively eavesdrop on the transmitted wireless signal to acquire sensitive information regarding credit cards, passwords, etc. [4, 5]. Likewise, cyber attacks on critical infrastructure can result in physical damage, power outages, equipment loss, etc., where the attacker can take over the servers by establishing a peer-to-peer network among affected servers. On 23 December 2015, power outages were experienced by many customers across Ukraine, which were caused by BlackEnergy malware [6]. The election process can also be compromised by exploiting the vulnerabilities of utilized communication protocols in the voting application called Voatz to alter, stop, or expose a user's vote [7].

The current communication framework is partitioned into layers, and the encryption is commonly implemented on higher layers, for example, the application or transport layer of the communication stack. The basic idea of encryption is shown in Fig. 1.1, where a sender encrypts the secret message known as plaintext into a ciphertext by using a secret key. The ciphertext is transmitted to the receiver via a communication channel. The receiver decrypts the ciphertext using the secret key, such encryption is known as symmetric encryption. There are multiple vulnerabilities in existing encryption techniques. The major drawback of cryptographic systems is their reliance on computational hardness to decode the ciphertext by any malicious user in absence of the secret key. The recent advances in computational technology and the availability of computational resources make it easier to decipher such codes. Different vulnerabilities of communication and encryption techniques can also be exploited to eavesdrop on secure communication as shown by the Kr00k attack [4]. Recent advances in deep learning techniques have also been utilized to circumvent the existing state-of-the-art encryption technique [8]. The lower layers (physical and data link layer) of the communication stack are oblivious to any security considerations. In the face of rapidly

evolving threats to wireless devices and networks, the security must be considered on the physical layer as an additional layer of security to increase the robustness and secrecy of the existing communication schemes.

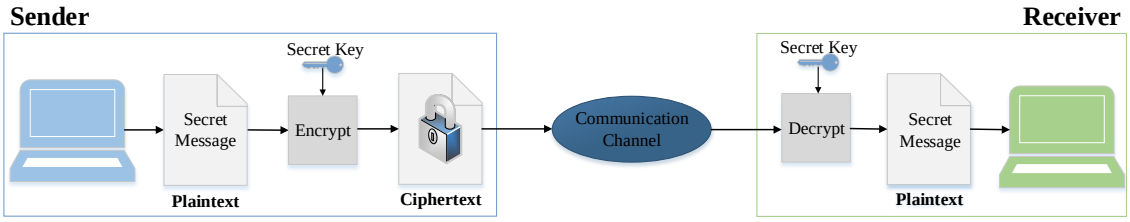


Fig. 1.1 A basic illustration of the encryption process at the legitimate sender and receiver.

At the physical layer of the communication stack, physical layer security (PLS) utilizes the randomness of the wireless transmission medium to obscure the transmitted signal from any potential eavesdropper. A basic channel model comprising of a legitimate transmitter, legitimate receiver, and an eavesdropper is shown in Fig. 1.2, where the channel between the legitimate nodes is referred to as the main channel and the channel between the legitimate transmitter and the eavesdropper as the eavesdropping channel. The fundamental properties of wireless signal transmission ensure that in most cases the signal received at the legitimate receiver via the main channel is significantly different from the signal received at the eavesdropper via the eavesdropping channel. An eavesdropper physically distant from the legitimate receiver by at least half the wavelength of the signal used for transmission is an example of such scenarios [9]. Therefore, the difference in the received signals received at the legitimate receiver and the eavesdropper is exploited in the PLS techniques to achieve secure communication, as compared to the use of a secret key in the encryption techniques. The majority of the existing PLS literature focuses on the study of the achievable secrecy rates from an information-theoretic perspective. Multiple signal processing and communication techniques have been employed to realize physical security by using secure channel codes [10, 11], and optimal beamforming design [12], but these techniques require channel state information (CSI) of the eavesdropper which is not possible for scenarios where the eavesdropper is passive. In the absence of CSI regarding the eavesdropper, blind artificial noise (AN) aided multi-antenna based physical layer security techniques [13, 14] provide a practical solution

by transmitting AN orthogonal to the legitimate channel. The major drawback of AN based physical layer security techniques is their reliance on channel estimates [15], as robustness and secrecy of channel estimates are crucial for achieving secrecy.

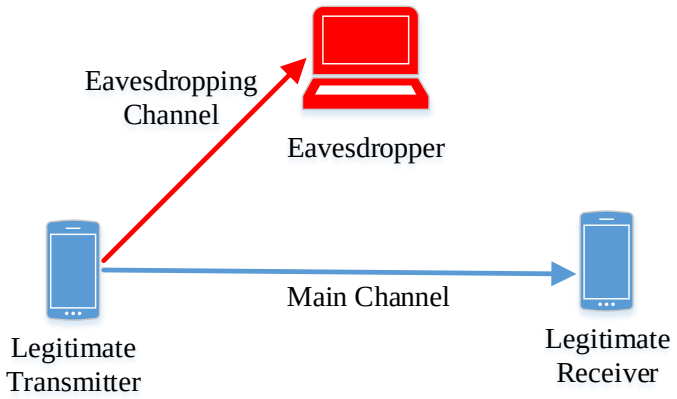


Fig. 1.2 A basic eavesdropping channel model.

CSI regarding the respective channel is also crucial in establishing a robust communication link, in addition to its importance in establishing physical layer security. In the absence of CSI, it is difficult to recover the signal randomly distorted by the wireless channel [16]. Therefore, obscuring CSI from the eavesdropper is also utilized to achieve physical layer security by discriminatory channel estimation (DCE) [17] to avoid the leakage of channel estimate to the malicious user. DCE degrades the channel estimation performance at the malicious user as compared to the legitimate receiver, and once CSI estimation is done, the link is secured. DCE is bandwidth efficient as compared to other physical layer security techniques, as the channel estimation stage consumes less bandwidth as compared to the data transmission stage. The most commonly used existing DCE schemes are presented in [17,18], where AN aided pilot signal is transmitted in multiple stages to acquire robust estimates of the channel between legitimate nodes while ensuring channel estimation deterioration at the eavesdropper. DCE presented in [17], requires that the channel between the legitimate nodes be statistically superior to the eavesdropping channel, which implies that the legitimate receiver must be closer to the transmitter than the eavesdropper. For DCE presented in [18], it can only be utilized for scenarios where the legitimate receiver does not transmit any

confidential information, which is generally not possible in most practical communication systems. These DCE techniques also require that the number of antennas at the legitimate transmitter is greater than the eavesdropper and the legitimate receiver. These conditions are difficult to ensure in practice. Therefore, the aim of this thesis is to devise novel DCE techniques to overcome the drawbacks of the existing DCE techniques.

1.2 Summary of Contributions

In this thesis, we present novel techniques to provide secure wireless communication by obscuring channel estimates from any passive eavesdropper. We propose full-duplex for transmission of the training signals from the legitimate nodes, to avoid leakage to channel estimates to the malicious user as in the absence of robust channel estimates, the malicious user is unable to decode the information robustly, where in full-duplex transmission each node simultaneously transmits and receives the signal in the same time and frequency band. We also propose a novel artificial noise assisted secure full-duplex channel estimation to enhance the channel estimation performance differentiation between a legitimate user and a malicious user by exploiting the multiple antennas and the high transmit power at the legitimate nodes. The contributions of this thesis can be summarized as:

- A comprehensive literature review of the existing physical layer security techniques for multiple-input and multiple-output systems along with their advantages and drawbacks for practical implementation.

- We propose a novel discriminatory channel estimation technique comprising of two stages to overcome the leakage of channel estimates to a malicious user by using the full-duplex transmission. In the first stage, the legitimate nodes transmit private orthogonal training signals to estimate the residual self-interference channel. In the second stage, the legitimate nodes simultaneously transmit the training signals using in-band full-duplex transmission to estimate the respective channel while causing equivocation at the eavesdropper. The proposed channel estimation technique achieves secure communication as robust channel estimation is crucial in decoding information. The limitation of the proposed full-duplex based channel estimation technique is that a strategically located eavesdropper can improve the channel estimation performance by getting close to the legitimate transmitter while increasing its distance from the legitimate receiver.

- We also propose the use of artificial noise to enhance the secrecy performance of the full-duplex aided discriminatory channel estimation against a strategically located eavesdropper. We present a novel three stages discriminatory channel estimation technique, where the first stage is responsible for self-interference channel estimation. In the second stage, the legitimate nodes simultaneously transmit a limited power training signal to acquire rough channel estimates to design orthogonal artificial noise. In the third stage, the legitimates nodes simultaneous transmits training signals along with orthogonal artificial noise to estimate the respective channel while ensuring performance deterioration at the eavesdropper.

- We present a novel local adaptive power allocation algorithm using estimated channel variances to allocate power to the training stages while keeping the allocated power secret from any potential passive eavesdropper.

- We also present a novel algorithm for the design of orthogonal artificial noise where the number receive antennas is greater than or equal to the number transmit antennas.

The contributions derived from this work are reported in following refereed conferences and journals:

[62] 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.

[74] 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.

[75] F. Ud Din and F. Labeau, "In-band Full-Duplex Discriminatory Channel Estimation using MMSE," IEEE Trans. Inform. Forensic Secur., pp. 1-1, 2020.

[98] F. Ud Din and F. Labeau, "Artificial Noise Assisted In-Band Full-Duplex Secure Channel Estimation,"IEEE Trans. Veh. Technol., submitted for publication.

1.3 Organization of the Thesis

This chapter provides motivation of the thesis. The rest of the thesis is organized into four chapters, where Chapter 2 provides a comprehensive literature review of the existing physical layer security techniques along with their advantages and drawbacks for practical implementation.

Chapter 3 presents the proposed discriminatory channel estimation technique using full-duplex transmission from the legitimate nodes to deteriorate the channel estimation performance at the eavesdropper as compared to the legitimate nodes. We provide performance comparison to the existing DCEs, along with the blind channel estimation at the eavesdropper.

Chapter 4 presents a novel orthogonal artificial noise (AN) assisted full-duplex DCE. The design of Orthogonal AN is presented for the arbitrary number of antennas at the legitimate nodes and the eavesdropper. A novel local adaptive power allocation algorithm is developed to allocate power to the training stages while keeping the allocated power secret from any potential eavesdropper. Finally, location-based simulation analysis is provided to analyze the performance of the proposed artificial noise assisted full-duplex DCE. Finally, the conclusion of this thesis along with the possible topics of future work are presented in Chapter 5.

This thesis follows the usual convention of notation, where vectors are denoted by lowercase boldface letters, and matrices are denoted by uppercase boldface letters.

Chapter 2

Background: Physical Layer Security

This chapter provides an overview of PLS and sets the stage for the forthcoming chapters. Section 2.1 provides the foundations for the physical layer security, followed by different techniques developed to achieve PLS in Sections 2.2 to 2.5. Section 2.6 presents the utilization of secure channel estimation to achieve physical layer security, which will form the basis of the contribution in this thesis. Section 2.7 provides a brief introduction of in-band full-duplex communication, as the full-duplex capability also provides a lucrative opportunity to secure the transmitted signals.

2.1 Foundation of Physical Layer Security

The foundation of physical layer security was laid by Claude Shannon in his seminal paper [19], where an information-theoretic model of secure communication was presented. Fig. 2.1 shows the secure communication scheme utilized in [19] comprising a legitimate transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper. The channel between legitimate nodes Alice-Bob is denoted as the main channel, and the channel between Alice and the eavesdropper is referred to as the wiretap channel. In this scheme, the legitimate nodes share a non-reusable secret key denoted as a vector $\boldsymbol{k}$. This thesis uses the usual convention of notation, where vectors are denoted by lowercase boldface letters, and matrices are denoted by uppercase boldface letters. To send a message $\boldsymbol{m}$, Alice encodes $\boldsymbol{m}$ to a codeword $\boldsymbol{c}$ using the shared secret key $\boldsymbol{k}$, where the message $\boldsymbol{m}$ corresponds the information that Alice wants to transmit. The eavesdropper and Bob both have access to

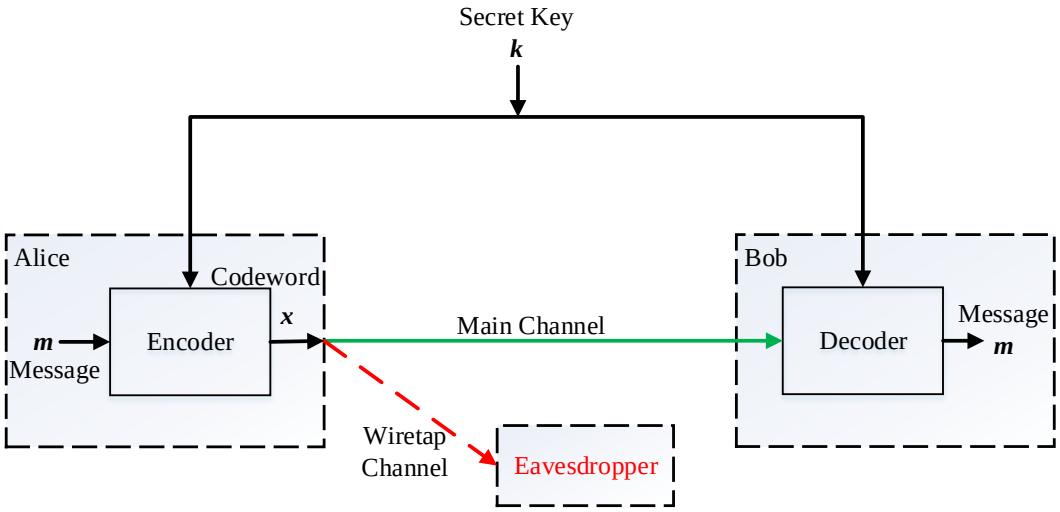


Fig. 2.1 Shannon's model for secure communication.

the codeword $\boldsymbol{c}$, as the communication channels are assumed to be noiseless. To formulate the information-theoretic condition to ensure secure communication, the equivocation at the eavesdropper is defined as $h(\boldsymbol{m}|\boldsymbol{c})$, where $h(.)$ denotes the entropy, and $h(\boldsymbol{m}|\boldsymbol{c})$ is the entropy of $\boldsymbol{m}$ given $\boldsymbol{c}$ [19]. $h(\boldsymbol{m}|\boldsymbol{c})$ represents the reduction in the uncertainty about message $\boldsymbol{m}$ after receiving the codeword $\boldsymbol{c}$ at the eavesdropper. To achieve perfect secrecy, the eavesdropper's equivocation must be equal to the a priori uncertainty about the message $\boldsymbol{m}$ before receiving the codeword $\boldsymbol{c}$, which is given as:

$$h(\boldsymbol{m}|\boldsymbol{c}) = h(\boldsymbol{m}). \tag{2.1}$$

The above equation implies that knowing the codeword $\boldsymbol{c}$ without the knowledge of the secret key $\boldsymbol{k}$ does not provide any information regarding the message $\boldsymbol{m}$ at the eavesdropper. Therefore, the entropy of the shared secret key must be greater than or equal to that of the message to ensure perfect secrecy. In other words, the length of the secret key must be equal to or greater than that of the message $\boldsymbol{m}$. To achieve this stringent condition for perfect secrecy one-time pad coding or Vernam's cipher scheme is used where every data bit is encoded (XORed) with a unique bit from the pre-shared secret key. The requirements of a non-reusable shared secret key and unrealistic assumptions of the noiseless channel make

Shannon's secrecy scheme unrealistic for practical considerations.

For noisy wireless channels, Wyner presented the wiretap channel model in [20] where the wiretap channel is assumed to be a probabilistically degraded version of the main channel. This guarantees that the signal received at the eavesdropper is statistically more distorted as compared to the signal received at the legitimate receiver. In the wiretap channel model, the message $\boldsymbol{m}$ comprising on l message symbols is encoded to a codeword $\boldsymbol{x}$ comprising of n encoded symbols, which is then transmitted over a noisy wireless channel. Bob and the eavesdropper observe their corresponding noisy versions of the transmitted signal denoted by $\boldsymbol{y}$ and $\boldsymbol{z}$, comprising of n received noisy symbols. The secrecy condition introduced by Wyner is given as:

$$\lim_{n\to\infty} \frac{1}{n} I(\boldsymbol{m}; \boldsymbol{z}) = 0, \tag{2.2}$$

where $I(\boldsymbol{m}; \boldsymbol{z})$ denotes the mutual information between $\boldsymbol{m}$ and $\boldsymbol{z}$. Therefore, the equivocation rate at the eavesdropper is given as:

$$\lim_{n\to\infty} \frac{1}{n} h(\boldsymbol{m}|\boldsymbol{z}) = \frac{1}{n} h(\boldsymbol{m}). \tag{2.3}$$

It provides a relaxed secrecy constraint as compared to Shannon's secrecy constraint presented in (2.1). The relaxed secrecy constraint presented in (2.2) has been utilized to show the existence of channel codes that can achieve the required transmission rate at a legitimate receiver while maintaining the obliged equivocation rate at the eavesdropper, as explained next.

2.2 Secrecy through Coding

Traditionally, channel coding has been utilized to increase the robustness of the communication link. In physical layer security, traditional channel coding techniques have been modified to achieve secure communication by introducing additional ambiguity during the channel coding process to make the signal undetectable to the eavesdropper. The secrecy achieving codes are referred to as wiretap codes as they exploit the wiretap channel model which guarantees that the average receive signal to noise ratio (SNR) at the legitimate receiver will be higher than the eavesdropper.

Nested code structures have been utilized to realize wiretap codes, where each distinct message $\boldsymbol{m}$ corresponds to multiple codewords instead of just one codeword in traditional channel coding. A random auxiliary message $\boldsymbol{m}'$ is used by Alice to select a codeword $\boldsymbol{x}$ comprising of n symbols [10, 11]. The random selection of codeword $\boldsymbol{x}$ based on auxiliary message $\boldsymbol{m}'$ introduces the required equivocation at the eavesdropper while Bob can decode the codeword due to its superior channel conditions. For the wiretap channel model, the signal received at Bob is given as $\boldsymbol{y}$, while the eavesdropper observes signal $\boldsymbol{z}$. Upper bound of the leaked information about the message $\boldsymbol{m}$ to the eavesdropper is given in [11] as:

$$\frac{1}{n}I(\boldsymbol{m};\boldsymbol{z}) \leq C_e - \frac{1}{n}h(\boldsymbol{m}') + \frac{1}{n}h(\boldsymbol{m}';\boldsymbol{m},\boldsymbol{z}), \tag{2.4}$$

where C_e denotes the capacity of the eavesdropper's channel. Hence, the above equation indicates that to achieve weak secrecy condition defined in (2.2), the rate of subcodebook associated to the message $\boldsymbol{m}$ should be close to the channel capacity of the eavesdropper, while the uncertainty of the eavesdropper regarding the auxiliary message $\boldsymbol{m}'$ is close to zero, such that: $\frac{1}{n}h(\boldsymbol{m}') = C_e$, and $\frac{1}{n}h(\boldsymbol{m}'|\boldsymbol{m},\boldsymbol{z}) = 0$.

Low-Density Parity Check (LDPC) codes have been utilized to design wiretap codes due to their excellent error-correction performance and availability of tools to analyze the decoding performance at Bob and the eavesdropper [21]. LDPC codes are utilized for secure coding in [22–24], to induce the desired equivocation at the eavesdropper while achieving channel capacity at Bob. In similar fashion polar codes are also utilized for secrecy as they are also from the family of low complexity linear block codes [25, 26]. Chaos-based modulation along with polar codes for the wiretap channel is presented in [27], where polar codes are utilized to improve secrecy performance.

The major drawback with the existing coding based secrecy approaches is the requirement of global channel state information at the transmitter, which renders them inappropriate for practical applications. Global channel state information is not possible to achieve, especially for a passive eavesdropper. To overcome the requirement of knowing the eavesdropper's channel information, the design of the wiretap code without any knowledge regarding the eavesdropping channel is presented in [28] for additive white Gaussian noise (AWGN) channels, where an auxiliary message is embedded in the message signal randomly instead of using channel information. This technique still requires robust channel estimates of the main chan-

nel to design wiretap codes. The major drawback of this secure communication technique presented in [28] is the huge communication overhead, as it requires at least 512 codeword bits to transmit 50 message bits securely. All the coding based physical layer security schemes require that the wiretap channel must be probabilistically degraded as compared to the main channel, this assumption is not valid in many practical scenarios where the eavesdropper is closer to Alice than Bob. Therefore, these drawbacks make these elegant and complex designs of wiretap codes only applicable to very restricted scenarios.

2.3 Secret Key Generation from Public Discussions over Noisy Channel

Secret key generation based physical layer security techniques exploit the independence of the main channel and the wiretap channel to provide secure communication. In [29], the authors have utilized an independent binary symmetric channel to generate a unique secret key among the legitimate transmitter and receiver. Fig. 2.2 shows the channel model used for secure key generation. The main idea is based on independence between channels and utilization of an error-free public feedback channel, where Alice transmits a sequence of binary symbols over a public noisy wireless channel, and the signals received at Bob and the eavesdropper are independent realizations of the transmitted signal due to the independence of their respective channels and system noises. The main channel and the wiretap channel are considered to be independent of each other due to differences in their fading, propagation loss, and position. In the wireless channels, the assumption of independent channels holds until the distance between legitimate nodes and the eavesdropper is greater than half the wavelength of the signal used for transmission. The independent channels result in independent observations at Bob and the eavesdropper of the signal transmitted from Alice. The information regarding correctly decoded bits at Bob is sent back to Alice via the noiseless public feedback channel. The bits decoded correctly at Bob are utilized at both the legitimate nodes to generate a mutual private secret key. The secrecy of the mutually generated key is ensured by the independence of the wiretap channel from the main channel, which makes sure that few bits are decoded correctly at Bob and not at the eavesdropper. This scheme can achieve secrecy even when the wiretap channel has superior performance than the main channel by transmitting more bits to make sure that there exists a group of bits that are correctly

decoded at Bob but not at the eavesdropper.

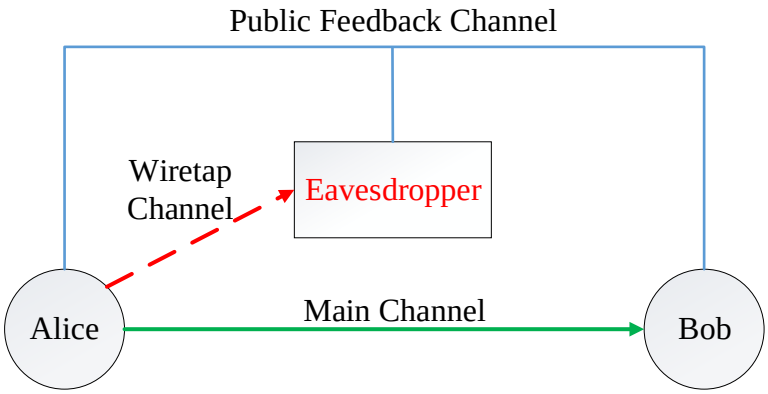


Fig. 2.2 Secret key generation channel model, consisting of three nodes and public feedback channel.

The secret key generation schemes generally consist of three distinct steps which are, key distillation, information reconciliation, and privacy amplification [30]. The key distillation step involves the generation of unique data among the legitimate transceiver pair. The information reconciliation stage utilizes error-correcting codes to reconcile information among the legitimate nodes. Finally, the privacy amplification step utilizes an encoding algorithm to increase the entropy of the received secret key from the correctly decoded bits after two steps.

There are many efforts in the literature to realize physical layer security by using different secret key generation techniques [31–33]. Real-time measurements have been conducted in different scenarios and environments to analyze the entropy of the generated secret key [31]. Their results indicate that secret key generation is most efficient in mobile node scenarios as compared to static nodes. A novel adaptive quantizer is proposed, which partitions sampled Received Signal Strength (RSS) values into variable-length blocks, after which quantization is performed on each block based on their peak values, average, and standard deviation. For static scenarios, induced randomness is employed to increase the rate of the secret key generation by exchanging random symbols by the legitimate nodes [34], but it requires perfect channel reciprocity to acquire the same secret key at both legitimate nodes. Covert key generation is presented in [35], where a novel communication protocol is presented to share the secret key in the presence of an active eavesdropper.

The real-time implementation of secret key generation utilizing the frequency selective nature of multipath fading channels has been shown in [32, 36], where multi-level quantization is performed on RSS values to generate a mutual secret key. In [33], the authors have considered a binary erasure channel to generate a secret key for a centralized network where the eavesdropper is a registered user in the network. The key generation strategy is divided into two stages, wherein the first stage pilot messages are broadcasted to the whole network until they achieve a considerable number of erasures at each node. It assumes that the information regarding erasures is available to all the users in the network by simply observing the acknowledgment feedback signals. In the second stage, each legitimate user pair generates a unique secret key based on correctly decoded bits. This work is only valid for centralized networks in which the eavesdropper is a known registered user in the network, which is not possible for many passive eavesdropping scenarios.

One of the major drawbacks of secret key generation schemes is the requirement of high communication overhead to ensure the robustness and secrecy of the established secret key [37], as it is not possible to know the bit errors at the eavesdropper for passive eavesdropping scenarios. The significance of this drawback is even greater for the scenarios where the eavesdropping channel is better than the main channel, such that the received signal-to-noise ratio (SNR) is higher at the eavesdropper as compared to Bob, which will result in fewer errors at the eavesdropper than Bob. Another drawback of secret key generation schemes is the requirement of channel reciprocity, which is not always the case for the wireless channels as shown through experiments in [38]. To overcome the requirement of channel reciprocity, round-trip channel estimates are utilized to generate the secret key [39]. However, the major challenges faced by channel estimation based secret key generation techniques are channel estimation errors, the independence of additive noise, and interference at both legitimate nodes [40]. The spatial and temporal correlation of the wireless channels also raises challenges in achieving secrecy through secret key based techniques [37].

2.4 Relay and Cooperative Methods for Secrecy

Physical layer cooperation has been widely utilized in wireless communication literature to efficiently utilize the scarce resource of wireless bandwidth. It does so by attempting to mimic the multiplexing and diversity gains of multi-antenna systems with or without

employing multiple antennas at individual nodes [41]. A relay network generally comprises a source, destination, and relays. The relay nodes cooperate with the source by transmitting the message to the destination. The relays have also been utilized in the literature to achieve secrecy. The literature is broadly classified into two categories by [2], namely *trusted relays* and *untrusted relays*.

In schemes based on *trusted relays*, the relay node helps the legitimate transmitter to achieve secrecy. In [42], the relay decodes the message, followed by the transmission of an artificial noise (AN) signal independent of the decoded secure message by the relay. The AN signal induces the required equivocation at the eavesdropper. In such a scenario, the relay node assumes full CSI regarding legitimate receiver to generate AN orthogonal to the main channel. The joint optimization of AN-aided beamforming is considered in [43, 44], where the relay optimizes its power allocation between AN and the legitimate signal. Full-duplex (FD) relay has been utilized to maximize the secrecy rate in [45]. The relay node transmits a jamming signal while utilizing the FD capabilities to simultaneously receive the information from the source. It also assumes perfect CSI of eavesdropper's channel at the relay, which enables it to optimize the AN signal. The transmitter and receiver are considered to be single antenna half-duplex systems. In [45], the authors have derived the achievable secrecy rates considering different scenarios depending on the availability of the eavesdropper's CSI and utilization of the jamming signal. Multi-relay multi-hop FD relays for secure communication are presented in [46], where the relay selection algorithm is presented to achieve physical layer security in the presence of multiple eavesdroppers. A machine learning-based power allocation technique is presented in [47], in which the relay nodes forward the received signal to the destination along with the transmission of orthogonal artificial noise. The proposed algorithm requires global channel information regarding all the nodes, including the eavesdropper.

Untrusted relays cooperate in transmitting the message to the destination while potentially eavesdropping on the data [48,49]. There are multiple techniques where the information is concealed from the relay node to achieve secrecy in such scenarios. In [50], the authors have proposed the utilization of the amplify-and-forward (AF) cooperation scheme only, because, in such a scheme the relay node only amplifies the received signal and then forwards it, without decoding the received signal at the relay node. This approach is based on the ethical imposition that relay will not attempt to decode the data. To overcome this limitation, the utilization of a full-duplex destination is presented in [51], where the full-duplex

destination forwards a jamming signal towards the relay while the source is transmitting. Afterward, the known jamming signal is subtracted from the signal received from the relay. The source-based jamming is presented to provide secrecy against full-duplex untrusted relay in [52], where the source transmits a jamming signal along with the secret message to cause equivocation at the untrusted relay.

The cooperative jamming schemes have high transmission overhead and complexity as they require collaboration among multiple nodes. The transmission of a jamming signal requires power and bandwidth, which are critical resources in every wireless network. Most importantly, these schemes require robust channel estimates for beamforming to design an artificial noise signal orthogonal to the main channel (between Alice and Bob). The eavesdropper can exploit the pilot signals to acquire robust channel estimates, which can be utilized by the eavesdropper to overcome the artificial noise signal by using a known-plaintext attack given in [53]. These are the major drawbacks of relay-based secrecy schemes for achieving physical layer security.

2.5 Multi-Antenna Systems for Physical Layer Security

The utilization of multi-antenna systems has drastically increased in the last decade to achieve significant performance improvements. The availability of multiple antennas and spatial channels provide a lucrative opportunity to utilize some antennas or transmission streams to transmit data while utilizing the remaining antennas to secure the transmitted signal. Multi-antenna beamforming, artificial noise aided transmission, and other multiple-antenna-based techniques are designed to exploit the additional resources antennas for physical layer security.

Fig. 2.3 shows a typical channel model employed in existing multi-antenna based physical layer security systems consisting of Alice, Bob, and the eavesdropper equipped with N_a, N_b, and N_e antennas, respectively. $\boldsymbol{H}_{ab} \in \mathbb{C}^{N_a \times N_b}$ represents the corresponding channel from Alice to Bob (main channel), and $\boldsymbol{H}_{ae} \in \mathbb{C}^{N_a \times N_e}$ corresponds to the eavesdropping channel from Alice to the eavesdropper. Therefore, the signals received by Bob and the eavesdropper

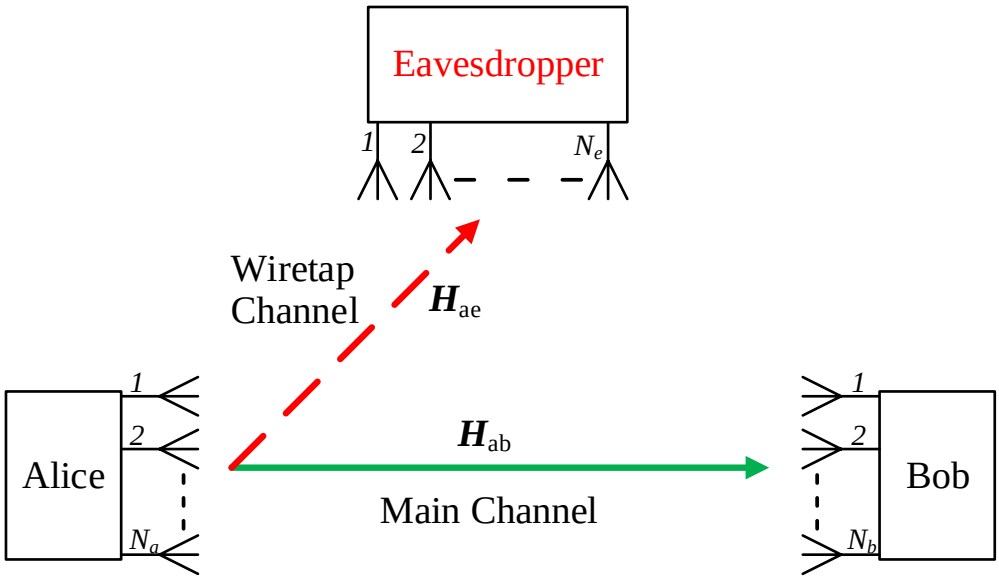


Fig. 2.3 Basic MIMO channel model for physical layer security comprising of Alice, Bob, and the eavesdropper with N_a, N_b, and N_e antennas, respectively.

are given as:

$$\boldsymbol{Y}_b = \boldsymbol{X}_d \boldsymbol{H}_{ab} + \boldsymbol{W}_b, \tag{2.5}$$

$$\boldsymbol{Y}_e = \boldsymbol{X}_d \boldsymbol{H}_{ae} + \boldsymbol{W}_e, \tag{2.6}$$

where $\boldsymbol{X}_d \in \mathbb{C}^{N \times N_a}$ is the signal transmitted by Alice, N corresponds to the length of the data transmission frame or the time slots utilized to transmit the signal, $\boldsymbol{W}_r$, and $\boldsymbol{W}_e$ are corresponding noise signals added to each signal, and they are assumed to be zero-mean circularly symmetric complex additive white Gaussian noise with variances σ_b^2 and σ_e^2, respectively. Secrecy capacity is the most commonly utilized metric in MIMO-based physical layer security systems to design novel transmission strategies while ensuring that the eavesdropper is unable to decode the secret message. Based on the wiretap model [54],

secrecy capacity for a MIMO system is defined as:

$$C_s = C_b - C_e, \tag{2.7}$$

$$= \max_{\boldsymbol{X}_d} \left[I(\boldsymbol{X}_d; \boldsymbol{Y}_b) - I(\boldsymbol{X}_d; \boldsymbol{Y}_e) \right], \tag{2.8}$$

where C_b, and C_e represent the respective channel capacity at Bob and the eavesdropper, respectively. The first work on MIMO based secure communication was presented in [12], where space-time block codes are utilized to achieve secure communication. It is shown in [12] that, the proposed secure space-time block codes achieve near-perfect secrecy capacity for the channel unaware eavesdropper, where the eavesdropper does not have any knowledge regarding the eavesdropping channel $\boldsymbol{H}_{ae}$. For the channel-aware eavesdropper, the transmit SNR is constrained to the channel-averaged Chernoff error exponent, which results in a sub-optimum communication strategy. Upper bounds of secrecy capacity for MIMO based physical layer security techniques are presented in [55–58], using generalized singular value decomposition (GSVD). The requirement of instantaneous CSI regarding the eavesdropper $\boldsymbol{H}_{ae}$ at Alice is the major drawback of these techniques, as it is impossible to estimate $\boldsymbol{H}_{ae}$ at Alice for a passive eavesdropper.

For the cases where the eavesdropper's CSI is not available at Alice, artificial noise orthogonal to the legitimate channel is utilized to achieve secrecy in [59]. The impact of imperfections in the estimated main channel $\boldsymbol{H}_{ab}$ due to the estimation errors on AN-aided beamforming is presented in [13]. Alice splits its power to transmit data symbols and artificial noise. There are different approaches to optimize the power allocation between AN and data symbols depending on channel information available at Alice. The received signals at Bob and eavesdropper for AN-aided physical layer security techniques are given as:

$$\boldsymbol{Y}_b = \boldsymbol{X}_d \boldsymbol{H}_{ab} + \boldsymbol{Z} \boldsymbol{H}_{ab} + \boldsymbol{W}_b \tag{2.9}$$

$$\boldsymbol{Y}_e = \boldsymbol{X}_d \boldsymbol{H}_{ae} + \boldsymbol{Z} \boldsymbol{H}_{ae} + \boldsymbol{W}_e \tag{2.10}$$

where $\boldsymbol{Z}$ indicates the orthogonal AN signal transmitted from the transmitter to induce equivocation at the eavesdropper. To design the orthogonal AN signal, the number of antennas at Alice must be greater than Bob such that: $N_a > N_b$. AN-aided transmission is shown to improve secrecy performance in non-orthogonal multiple access (NOMA) networks [60].

A practical secure communication approach based on AN aided MIMO beamforming is presented in [14], by using the ZFBF (Zero-Forcing Beamforming) feature present in the 802.11ac standard to generate multiple orthogonal blinding streams. Alice uses a single stream to transmit the data, and all the other streams are utilized to transmit the orthogonal blinding streams with Bob considered to be a single antenna receiver. The Gram–Schmidt orthogonalization process has been employed to create orthogonal blinding streams. Random symbols are transmitted on these orthogonal streams to decrease the received signal-to-interference-plus-noise ratio (SINR) at the eavesdropper. Experimental results indicate that the SINR differentiation is achieved between the legitimate nodes and the eavesdropper for indoor scenarios by utilizing WARP (Wireless Open Access Research Platform) nodes at RICE University. For outdoor scenarios, the SINR differentiation between the legitimate nodes and the eavesdropper is diminished due to the absence of multi-path fading.

MIMO beamforming-based schemes provide an attractive opportunity for physical layer security as many devices now have multiple antennas available at their disposal, but there are several downsides to such schemes. The major drawback of multi-antenna based security techniques is their dependence on channel estimates [15]. For an optimized transmission system, the channel estimates of the eavesdropper are also required which is not possible. Blind orthogonal AN-aided transmission schemes also require statistical information regarding the eavesdropper to achieve robust secrecy capacity. The crucial issue with such schemes lies in obtaining channel estimates because if the eavesdropper can get hold of these estimates, then the information can be compromised by utilizing known plain-text attacks [53], which implies that channel estimates are critical in achieving secrecy. The importance of robust and secure channel estimates for multi-antenna based secure communication emphasizes that secure channel estimation is essential to achieve secure communication.

2.6 Discriminatory Channel Estimation

Robust and accurate CSI is crucial in establishing a reliable communication link, as CSI 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 signal as it has been randomly distorted by the wireless channel, especially for MIMO systems where CSI is critical in decoding the spatially multiplexed data streams as shown in [16,

61]. Therefore, CSI is also exploited to achieve PLS by Discriminatory Channel Estimation (DCE) techniques, where channel estimation performance is degraded at the malicious user as compared to the legitimate nodes [17]. As indicated in previous sections, the robustness of CSI is crucial at the legitimate nodes in achieving secrecy through existing physical layer security techniques, for instance, to design secure channel codes [11,26], MIMO beamforming matrices [12], and orthogonal AN-signal for AN-aided MIMO beamforming [13,14]. DCE can be utilized to enable the application of wiretap channel codes based PLS to the scenarios where the wiretap channel is better than the main channel. Similarly, the secrecy of CSI is also crucial as the eavesdropper can exploit the leaked information regarding CSI to overcome the different existing physical layer security techniques [15, 62, 63], for example, to obtain the secret key [39], cancel the orthogonal AN-signal from the relay node [42], and overcome AN-aided transmission by known-plaintext attacks [53]. In [15], the impact of CSI on MIMO beam-forming based secrecy schemes is presented, by analyzing the impact of CSI leakage to the eavesdropper on the achievable secrecy capacity. The results indicate that DCE significantly improves the secrecy capacity rate as compared to the conventional channel estimation techniques. The significance of the secrecy of CSI is one of the bases of this thesis as it provides a foundation in achieving secure communication through other existing PLS techniques.

DCE provides an efficient way of achieving physical layer security because the channel estimation stage consumes less bandwidth as compared to the data transmission stage so that the overhead of PLS is focused on a shorter fraction of the total duration of the communication. The most commonly used AN-assisted multiple-stage DCE training schemes are presented in [17, 18]. The most prevalent schemes proposed for DCE are feedback-and-retraining [17] and two-way training [18]. These schemes utilize a rough estimation stage followed by the AN-assisted training stage. The system model is the same as mentioned in the previous section for multi-antenna systems. Fig. 2.3 shows the basic channel model comprising of Alice, Bob, and the eavesdropper utilized typically in the DCE schemes.

First, we consider the feedback-and-retraining training scheme [17]. It comprises of multiple stages. In the first stage, the power of the training signal is restrained to limit the estimation performance at the receiving nodes, these estimates are referred to as the rough

channel estimates. The training signal sent by Alice in the first stage is given as:

$$\boldsymbol{X}_0 = \sqrt{\frac{P_0 T_0}{N_t}} \boldsymbol{C}_0, \tag{2.11}$$

where $\boldsymbol{C}_0 \in \mathbb{C}^{T_0 \times N_t}$ is the pilot signal satisfying $\boldsymbol{C}_0^H \boldsymbol{C}_0 = \boldsymbol{I}_{N_t}$, P_0 indicates the power of the pilot signal, and T_0 is the training length. During the first stage, the signals received at Bob $\boldsymbol{Y}_{b0}$ and the eavesdropper $\boldsymbol{Y}_{e0}$ are given as:

$$\boldsymbol{Y}_{b0} = \boldsymbol{X}_0 \boldsymbol{H}_{ab} + \boldsymbol{W}_{b0}, \tag{2.12}$$

$$\boldsymbol{Y}_{e0} = \boldsymbol{X}_0 \boldsymbol{H}_{ae} + \boldsymbol{W}_{e0}. \tag{2.13}$$

where $\boldsymbol{W}_{b0}$ and $\boldsymbol{W}_{e0}$ are the corresponding additive noise during the initial stage. Based on these observations Bob estimates the channel $\hat{\boldsymbol{H}}_{ab0}$ and sends the channel estimates back to Alice. These channel estimates are critical for the precoding weights in the second stage. The eavesdropper can intercept these channel estimates and utilize them for the cancellation of artificial noise to acquire robust channel estimates. Linear minimum mean square estimation (LMMSE) is utilized by Bob to estimate the channel coefficients.

The second stage is known as the feedback-and-retraining stage, where $\hat{\boldsymbol{H}}_{ab0}$ is utilized by Alice to place the AN in the null space of the main channel $\hat{\boldsymbol{H}}_{ab0}$. The signal transmitted by Alice in this stage is given as:

$$\boldsymbol{X}_1 = \sqrt{\frac{P_1 T_1}{N_t}} \boldsymbol{C}_1 + \boldsymbol{Z}_1 \boldsymbol{N}_{\hat{\boldsymbol{H}}_{ab0}}, \tag{2.14}$$

where $\boldsymbol{C}_1$ is the training signal, $\boldsymbol{N}_{\hat{\boldsymbol{H}}_{ab0}}$ corresponds to the left null-space of $\hat{\boldsymbol{H}}_{ab0}$, and $\boldsymbol{Z}_1$ is AN. In this scenario, special care should be taken in determining the AN power as the null-space $\boldsymbol{N}_{\hat{\boldsymbol{H}}_{ab0}}$ based on the imperfect channel estimates can potentially do more harm than good by causing interference at Bob. Finally, the received signals at Bob and the eavesdropper are given as:

$$\boldsymbol{Y}_{b1} = \boldsymbol{X}_1 \boldsymbol{H}_{ab} + \boldsymbol{W}_{b1}, \tag{2.15}$$

$$\boldsymbol{Y}_{e1} = \boldsymbol{X}_1 \boldsymbol{H}_{ae} + \boldsymbol{W}_{e1}. \tag{2.16}$$

The AN degrades the channel estimation at the eavesdropper as compared to Bob. This concept is further extended with m-retraining stages to improve the estimates of the main channel $\boldsymbol{H}_{ab}$. In each stage i, the channel estimate $\hat{\boldsymbol{H}}_{ab(i-1)}$ of the previous stage $i-1$ is utilized to design the orthogonal AN, where $i = 1, 2, ...m$ indicates the current retraining stage. Lastly, space-time block codes (STBC) are utilized to transmit the data symbols to demonstrate that Bob decodes the information robustly while the eavesdropper is unable to decode the data symbols due to the inferior channel estimates.

The major drawback of the feedback-and-retraining DCE [17] is the leakage of channel estimates to the eavesdropper in the initial training stage, where a more capable eavesdropper can acquire robust channel estimates by exploiting its superior eavesdropping channel as compared the main channel, such that variance of $\boldsymbol{H}_{ae}$ is greater than $\boldsymbol{H}_{ab}$. Therefore, feedback-and-retraining DCE is only effective for the wiretap channel presented by Wyner [20]. The requirement of statistical information regarding the eavesdropper's CSI at the legitimate node for power allocation is not possible in the passive eavesdropping scenarios. It also requires that the number of antennas at Bob and the eavesdropper is less than Alice which is hard to guarantee for practical scenarios. These drawbacks limit the practical applications of the feedback-and-retraining DCE as it is not possible for the legitimate nodes to impose such restrictions on the eavesdropper.

The other notable DCE scheme is the *two-way training scheme* [18], where Bob sends the initial training signal instead of Alice, to overcome the leakage of the channel estimates in the first stage by the feedback-and-retraining DCE. This scheme comprises two stages where, in the first stage, Bob transmits a pilot signal to provide the reverse channel estimate to Alice. The signal received at Alice in the initial training stage is given as:

$$\boldsymbol{Y}_{a0}^{(2)} = \boldsymbol{X}_{0}^{(2)} \boldsymbol{H}_{ba} + \boldsymbol{W}_{a0}^{(2)}. \tag{2.17}$$

This information can also be overheard by the eavesdropper as:

$$\boldsymbol{Y}_{e0}^{(2)} = \boldsymbol{X}_{0}^{(2)} \boldsymbol{H}_{be} + \boldsymbol{W}_{e0}^{(2)}, \tag{2.18}$$

where publicly known pilot $\boldsymbol{X}_{0}^{(2)}$ can be utilized to acquire an estimate of $\boldsymbol{H}_{be}$. This research assumes that Alice is the only legitimate transmitter, hence the estimate of $\boldsymbol{H}_{be}$ will not provide any advantage in decoding the secret message transmitted from Alice. Therefore,

the two-way DCE does not provide secrecy to the signals transmitted by Bob, which limits the benefit of this research as most of the existing communication systems require both nodes to exchange messages with each other. Alice utilizes channel reciprocity to acquire the channel estimate $\hat{\boldsymbol{H}}_{ab} = \hat{\boldsymbol{H}}_{ba}^{T}$, where $(.)^{T}$ indicates the transpose function, to design the AN signal in the null space of $\hat{\boldsymbol{H}}_{ab}$. In the second stage, the pilot signal is transmitted from Alice along with the orthogonal AN signal to improve the estimated main channel while maintaining equivocation at the eavesdropper.

Two-way training DCE scheme also considers non-reciprocal channels where an additional round trip training signal is echoed from Alice. The first stage is the same as mentioned in the case of reciprocal channels, where Bob transmits the training signal $\boldsymbol{X}_{0}^{(2)}$ which is utilized by Alice to acquire the channel estimate $\hat{\boldsymbol{H}}_{ba}$. In the second stage, Alice transmits a private training signal $\boldsymbol{X}_{a1}^{(2)}$, the signal received by Bob is given as:

$$\boldsymbol{Y}_{b1}^{(2)} = \boldsymbol{X}_{a1}^{(2)}\boldsymbol{H}_{ab} + \boldsymbol{W}_{b1}^{(2)}. \tag{2.19}$$

Bob re-transmits $\boldsymbol{Y}_{b1}^{(2)}$ back to Alice after a constant amplification of α. The echoed signal received at Alice is given as:

$$\boldsymbol{Y}_{a2}^{(2)} = \alpha\boldsymbol{Y}_{b1}^{(2)}\boldsymbol{H}_{ba} + \boldsymbol{W}_{a2}^{(2)}, \tag{2.20}$$

$$= \alpha\boldsymbol{X}_{a1}^{(2)}\boldsymbol{H}_{ab}\boldsymbol{H}_{ba} + \alpha\boldsymbol{W}_{b1}^{(2)}\boldsymbol{H}_{ba} + \boldsymbol{W}_{a2}^{(2)}, \tag{2.21}$$

where Alice acquires a rough estimate of $\boldsymbol{H}_{ab}$ from $\boldsymbol{Y}_{a2}^{(2)}$ by using the knowledge of the private training signal $\boldsymbol{X}_{a1}^{(2)}$, and reserve channel $\boldsymbol{H}_{ba}$ estimated in the initial stage. Alice suffers from noise amplification as shown in the above equation by $\alpha\boldsymbol{W}_{b1}^{(2)}\boldsymbol{H}_{ba}$. In the third stage, orthogonal AN is added to the training signal which is transmitted from Alice based on the rough estimates of $\hat{\boldsymbol{H}}_{ab}$.

The major drawback of the two-way training DCE [18] is that it does not provide secrecy to the signals transmitted by Bob. Like the feedback-and-retraining DCE, it also requires that the number of antennas at Alice must be greater than Bob, and the variance of $\boldsymbol{H}_{ae}$ must be less than $\boldsymbol{H}_{ab}$. The two-way training requires statistical information regarding the eavesdropping channel for power allocation which is not possible the passive eavesdropping scenarios. For non-reciprocal channels, noise amplification during rough channel estimation limits its performance. These drawbacks severely limit the utilization and applications of the

two-way training DCE.

The authors in [64], have presented a novel semi-blind two-way training scheme for the reciprocal channels. A random whitening sequence is transmitted in the initial training stage, to prevent the pilot contamination attacks, where an adversary jams the part of the known pilot signal to deteriorate the performance of channel estimation. The signal transmitted in the AN-aided training stage is similar to the two-way training DCE, where AN-aided pilot is transmitted by Alice. The channel estimation at Bob is based on the whitening-rotation-based semi-blind channel estimator to overcome the effects of imperfect artificial noise due to the channel estimation errors in the initial training stage. The semi-blind two-way training scheme provides protection against pilot contamination attacks and improves the channel estimation performance by using the whitening-rotation-based semi-blind channel estimator. The applications of semi-blind two-way DCE are limited to the reciprocal channels only. The semi-blind two-way training scheme suffers from the similar drawbacks like its predecessor the two-way training DCE, as it does not provide secrecy to the information transmitted by Bob, it requires that the number of antennas at the Alice must be greater than Bob, it requires statistical information regarding the eavesdropping channel, and it requires that the main channel $\boldsymbol{H}_{ab}$ must be better than the eavesdropping channel $\boldsymbol{H}_{ae}$.

The design of AN for a two-way training based DCE is considered in [65], using the joint optimization among the legitimate nodes for the covariance matrix of the AN-signal, pilot signal power, and the linear estimator employed at Bob to minimize the estimation error at Bob while maintaining the estimation error above a certain threshold at the eavesdropper. Joint optimization between legitimate nodes relaxes the requirement of a higher number of antennas at Alice than Bob, as the direction of AN-signal is computed using the optimal linear channel estimator at Bob, and the estimated channel in the initial training stage. The optimization problem is divided into two sub-problems to ease the overhead required to optimize the parameters at both the legitimate nodes, simultaneously. The major drawback of the proposed DCE [65] is the requirement of a huge communication overhead to perform iterative optimization between Alice and Bob. Other significant drawbacks of this DCE are that, it is only valid for the reciprocal channels, it requires statistical information regarding the eavesdropping channel, and it also requires that the main channel must be better than the eavesdropping channel to achieve secure communication.

Another solution to overcome the requirement of a higher number of transmit antennas

at Alice as compared to Bob in feedback-and-retraining DCE is given in [66], where an antenna grouping strategy is considered. The initial training stage is the same as given in feedback-and-retraining DCE [17]. In the second stage, for the scenario where Bob has a greater number of antennas than Alice, then the antennas at Bob are grouped and each antenna group has a dedicated DCE turn. The proposed scheme utilizes a variable-length pilot based on the ratio of total number antenna to the number of turns. The drawback of the antenna grouping strategy is the use of the fixed number of antenna groups. The other drawbacks are similar to the drawbacks of feedback-and-retraining DCE [17] that, it leaks channel estimates to the eavesdropper in the initial training stage, it requires statistical CSI regarding the eavesdropper for optimal power allocation, and it also requires that the main channel must be better than the eavesdropping channel.

DCE is also considered for MIMO decode-and-forward cooperative system in [67]. In the first phase, the source node transmits an omnidirectional AN signal, while relay transmits the pilot signal for relay-destination channel estimation. Then in the second phase, the source transmits the training signal for source-relay channel estimation while the destination transmits AN signal into null space of relay-destination channel, based on channel estimation in the first phase. Finally, the authors have presented optimization for power allocation between the training signals and the AN. The presented DCE for cooperative network lacks the analysis of system-level performance to indicate the secrecy performance achieved by the DCE in the considered relay network. In the cooperative network, the multiple transmissions from the legitimate transmitter and the relay node can be exploited by the eavesdropper. The presented DCE requires that the number of antennas at the legitimate destination must be greater than the relay node. An informed eavesdropper can optimize its location to overcome the AN-signal transmitted by the legitimate transmitter and the relay node.

2.6.1 Summary of drawbacks of existing DCE schemes

All of the existing DCE techniques require that the main channel must be better than the eavesdropping channel, that statistical channel information regarding the eavesdropper's channel must be available at the legitimate nodes, and that 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. All of the mentioned DCE techniques consider half-duplex

nodes, where only one node transmits the signal while all the other nodes passively receive the transmitted signal. In this thesis, we will explore an additional degree of freedom by utilizing in-band full-duplex transmissions to address the shortcomings of the existing DCE techniques. In the next section, we have provided a brief overview of the full-duplex system.

2.7 In-Band Full-Duplex Communication

As already mentioned in the previous chapter, in an in-band full-duplex communication system each node simultaneously transmits and receives the signal in the same time and frequency band to improve the efficiency of the utilized channel resources. The major challenge faced by full-duplex systems is the self-interference (SI) added to the receiver by the self transmitted signal. The recent advancements in signal processing techniques and electronic devices have provided multiple solutions to minimize the self-interference, analog self-interference cancellation, especially has attracted a lot of attention as it can achieve robust self-interference cancellation [68,69]. Analog self-interference cancellation is shown in Fig. 2.4, where a circulator switch is utilized to simultaneously transmit and receive [70]. The circulator switch provides considerable isolation between transmit and receive radio frequency (RF) chains [71]. In Fig. 2.4, $\boldsymbol{X}$ and $\boldsymbol{Y}$ indicate the transmit and the receive baseband signals, respectively. 'TX' indicates the transmit RF chain while 'RX' indicates receive RF chain. For analog cancellation, the output of the power amplifier (PA) at the transmit radio frequency (RF) chain is subtracted at the input of the low noise amplifier (LNA) at the receive RF chain after suitable scaling as given in [70]. Transmit and receive RF chains are assumed to share a common oscillator as they are on the same device, which along with analog cancellation reduces non-linear impairments caused by the self-interference signal below the noise floor [72].

The efficient minimization of SI enables the utilization of in-band full-duplex devices to approximately double the channel capacity. The lucrative opportunity to simultaneously transmit and receive signals in the same frequency and time band is also exploited to achieve PLS by transmitting a jamming signal while receiving the transmission from the legitimate transmitter [73,74]. In this thesis, we will explore the use of in-band full-duplex transmissions to achieve DCE.

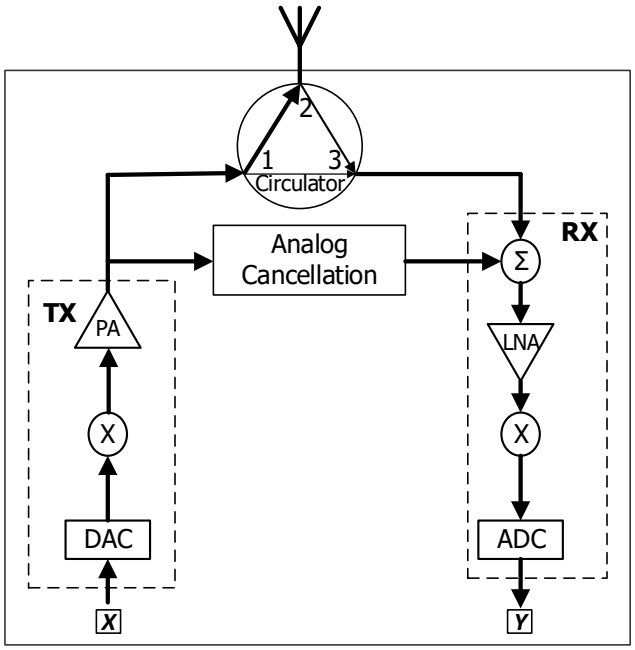


Fig. 2.4 Simple illustration of analog self-interference cancellation in a full-duplex node.

2.8 Summary

In this chapter, we have provided a brief overview of physical layer security foundations along with different approaches to realize the physical layer security. The review of existing physical layer security literature reveals the strong reliance of different physical layer security techniques on robust and secure channel estimates. Therefore, obscuring the channel estimates from the eavesdropper by using DCE techniques present a lucrative opportunity to realize physical layer security. DCE is also bandwidth-efficient as the channel estimation stage is generally shorter than the data transmission stage. Our contributions in the upcoming chapters of this thesis provide innovative solutions to the open problems faced by the existing DCE techniques.

Chapter 3

In-Band Full-Duplex Discriminatory Channel Estimation using MMSE

3.1 Introduction

As mentioned in Chapter 2, CSI is crucial in establishing a secure communication link. Therefore, DCE techniques provide an efficient way to achieve secure communication by providing the secrecy against leakage of channel estimates to the eavesdropper. This chapter proposes an innovative Full-Duplex aided DCE (FD-DCE) to overcome the drawbacks of the existing DCE techniques, which require that the main channel must be better than the eavesdropping channel, availability of statistical information regarding eavesdropping channel at the legitimate transmitter, etc.. In the proposed FD-DCE, the legitimate transmitter and receiver employ in-band full-duplex transmissions to estimate their respective channels while maintaining equivocation at the eavesdropper[1]. Unlike existing DCE techniques [17, 18], the proposed FD-DCE method does not require any information regarding the eavesdropper. 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, the full-duplex transmission has been used to induce ambiguity at the eavesdropper while acquiring channel estimates at the legitimate nodes. Some existing techniques for in-band full-duplex channel estimation have been presented in [77, 78], but the existing works are oblivious to the secrecy requirements to achieve discriminatory channel estimation

[1]The proposed FD-DCE presented in this chapter was presented in [75, 76].

performance at the eavesdropper as compared to the legitimate receiver.

The proposed channel estimation technique comprises of two stages. The first stage is responsible for the estimation of the SI channel, as we have used the channel aware SI cancellation technique for full-duplex stage due to its superior performance as compared to channel unaware cancellation [68]. 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 SI signal. Therefore, the utilization of independent stages for SI and inter-node channel estimation enables robust SI channel estimates by avoiding interference from the other node while preventing the leakage of channel estimates by using a private training signal in the first stage. Hence, the improved SI cancellation in the second stage due to superior SI channel estimation.

Section 3.2 provides the system model considered for the proposed FD-DCE. Section 3.3 explains the proposed FD-DCE. Sections 3.4, and 3.5 presents the detailed performance analysis of the proposed FD-DCE along with a comparison to the existing DCE techniques to highlight the performance improvements achieved by the proposed FD-DCE.

3.2 System Model

Consider a FD multiple-input multiple-output (MIMO) channel model consisting of a legitimate transmitter (Alice), legitimate receiver (Bob), and an eavesdropper as shown in Fig. 3.1. 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. 3.1. 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 the forward and backward channel coefficient will be different at the legitimate nodes due to the difference in their multipath and hardware differences caused by the different components at Alice and Bob. The proposed DCE techniques in this thesis can be applied to reciprocal channels as well because channel reciprocity will further facilitate the implementation of the proposed DCE techniques. The

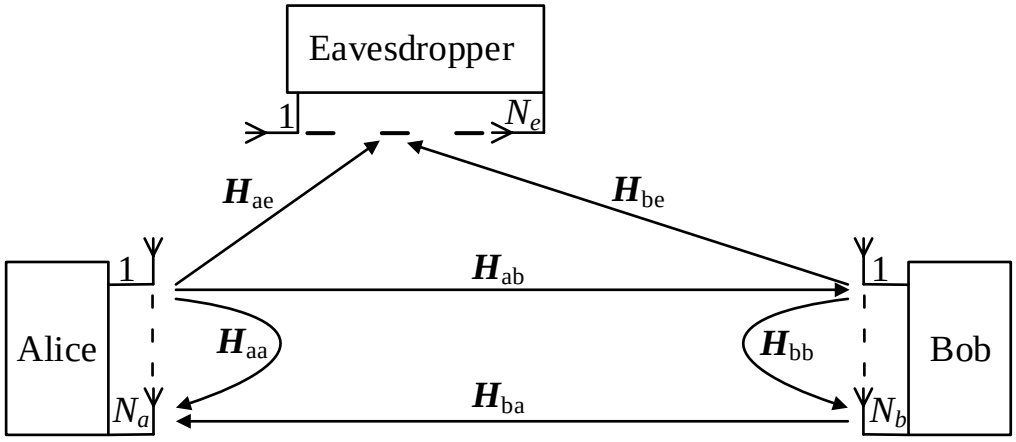


Fig. 3.1 Basic channel model utilized for the proposed FD-DCE technique, comprising multiple antenna full-duplex legitimate transmitter, legitimate receiver, and the eavesdropper, where legitimate transmitter and receiver are commonly known as Alice, and Bob, respectively.

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:

- 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 [79][2].

- All full-duplex antennas are able to simultaneously transmit and receive by using a circulator switch as shown in [70]. The circulator switch provides considerable isolation

[2]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.

between transmit and receive radio frequency (RF) chains [71]. 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 [70]. 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 [72]. 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 [68]. This is also a commonly utilized statistical model for characterizing the residual SI channel in the literature [75, 76, 80–82].

- This thesis assumes that a robust timing synchronization technique for full-duplex communication has been utilized as given in [83, 84], 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 [83, 84]. 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 uplink. As the propagation delay is significantly less than CP, therefore the utilization of time-alignment removes inter-symbol interference [85]. Lastly, it is assumed that robust the timing synchronization is achieved by using state-of-the-art blind synchronization technique [86, 87] to avoid the leakage of channel estimates in the synchronization stage to the eavesdropper.

- 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 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 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.

- In this thesis, all nodes are assumed to be static. The proposed DCE techniques can also be applied to achieve physical layer security for mobile nodes given in [88]: as the proposed DCE utilizes a minimum length of the 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 the proposed DCE.

3.3 Proposed Full-Duplex Discriminatory Channel Estimation Technique

3.3.1 First Stage

The first stage of the proposed channel estimation is responsible for the estimation of SI channels, to be utilized in the later stage for the cancellation of the SI signal. A private random training signal, known to the transmitting node only, is transmitted to estimate the respective SI channels by both legitimate nodes. A pilot based channel estimation technique is utilized for estimation as the transmitter and receiver RF chains are on the same full-duplex device. Independent time slots have been utilized for transmission of private training signals by both nodes to avoid 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 [89].

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 [90]. The estimation process is the same for both legitimates nodes, so the steps and performance for Bob will be described here; the same steps and results are valid for Alice.

To design a private training signal at Bob, a random $N_b \times N_b$ matrix $\boldsymbol{X}$ is generated, which is then orthogonalized by using Gram-Schmidt process [91] to get $\boldsymbol{X}_{sb}$, where $\boldsymbol{X}_{sb}^H \boldsymbol{X}_{sb} = \boldsymbol{I}_{N_b}$[3]. 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 $\boldsymbol{Y}_{si}^b \in \mathbb{C}^{N_b \times N_b}$ at Bob for self-inference channel estimation is given as:

$$\boldsymbol{Y}_{si}^b = \boldsymbol{X}_{sb} \boldsymbol{H}_{bb} + \boldsymbol{W}_{si}^b, \tag{3.1}$$

where $\boldsymbol{W}_{si}^b$ is ZMCSWGN with covariance matrix $\sigma^2 \boldsymbol{I}_{N_b}$. 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 [92] is employed for channel estimation as:

$$\hat{\boldsymbol{H}}_{bb} = \sigma_{bb}^2 \mathbf{X}_{sb}^H \left(\sigma_{bb}^2 \mathbf{X}_{sb} \mathbf{X}_{sb}^H + \sigma^2 \mathbf{I}_{N_b} \right)^{-1} \mathbf{Y}_{si}^b, \tag{3.2}$$

$$\triangleq \boldsymbol{H}_{bb} + \Delta \hat{\boldsymbol{H}}_{bb}, \tag{3.3}$$

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

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

$$\boldsymbol{Y}_{si}^e = \boldsymbol{X}_{sb} \boldsymbol{H}_{be} + \boldsymbol{W}_{si}^e, \tag{3.4}$$

where $\boldsymbol{W}_{si}^e$ is ZMCSWGN. 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

[3]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 $\boldsymbol{X}_{sa}$.

channel estimation techniques [93, 94]. The number of symbols received at the eavesdropper is critical for these techniques, as their performance deteriorates with the decrease in the number of observed symbols [75, 93, 94], 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. In the proposed FD-DCE, the length of the private training signal is kept 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.

3.3.2 Second Stage

In the second stage, inter-node channels are estimated while utilizing the SI channel information from the first stage to cancel the SI 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. The length of the training sequence is set to $T_2 = \max\{N_a, N_b\}$, to assure that the reception at the eavesdropper is completely superimposed by two signals while using the minimum number of training symbols.

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:

$$[\boldsymbol{X}_a]_{i,k} = \sqrt{\frac{1}{T_2}} e^{-j2\pi(k-1)i/N_a}, \tag{3.5}$$

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 the Gram-Schmidt process as mentioned in the first stage. Finally, the received signal at Bob in the second stage is given as:

$$\boldsymbol{Y}_b = \boldsymbol{X}_a \boldsymbol{H}_{ab} + \boldsymbol{X}_b \boldsymbol{H}_{bb} + \boldsymbol{W}_b, \tag{3.6}$$

where $\boldsymbol{W}_b$ is the additive system noise. 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:

$$\boldsymbol{Y}_b^{dc} = \boldsymbol{X}_a\boldsymbol{H}_{ab} + \boldsymbol{X}_b\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b, \tag{3.7}$$

$$= \boldsymbol{X}_a\boldsymbol{H}_{ab} + \boldsymbol{W}_b^{dc}, \tag{3.8}$$

where $\Delta\hat{\boldsymbol{H}}_{bb}$ corresponds to the estimation error as given in (3.3), and $\boldsymbol{W}_b^{dc} = \boldsymbol{X}_b\Delta\hat{\boldsymbol{H}}_{bb}+\boldsymbol{W}_b$ is the corresponding residual interference plus noise signal. In order to estimate the channel $\boldsymbol{H}_{ab}$, Bob uses the LMMSE criterion given in [92] as the corresponding channel and noise variances are available, as LMMSE outperforms the other data aided estimation techniques for example, Least Squares (LS), and wiener filter channel estimation [92]. The LMMSE estimator for channel $\boldsymbol{H}_{ab}$ is given as:

$$\hat{\boldsymbol{H}}_{ab} = \sigma_{ab}^2\boldsymbol{X}_a^H\left(\sigma_{ab}^2\boldsymbol{X}_a\boldsymbol{X}_a^H + \boldsymbol{R}_{\boldsymbol{W}_b^{dc}}\right)^{-1}\boldsymbol{Y}_b^{dc}, \tag{3.9}$$

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

$$\boldsymbol{R}_{\boldsymbol{W}_b^{dc}} = \mathbb{E}\left[\boldsymbol{X}_b\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\boldsymbol{X}_b^H\right] + \sigma^2\boldsymbol{I}, \tag{3.10}$$

$$= \left(\frac{N_b}{T_2}\mathcal{E}_{bb} + \sigma^2\right)\boldsymbol{I}_{T_2} \tag{3.11}$$

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

$$\mathcal{E}_{bb} = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\}]}{N_b^2}. \tag{3.12}$$

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 (3.9) can be simplified as:

$$\hat{\boldsymbol{H}}_{ab} = \frac{\sigma_{ab}^2}{(N_a\sigma_{ab}^2 + N_b\mathcal{E}_{bb})/T_2 + \sigma^2}\boldsymbol{X}_a^H\boldsymbol{Y}_b^{dc}, \tag{3.13}$$

$$\triangleq \boldsymbol{H}_{ab} + \Delta\hat{\boldsymbol{H}}_{ab}, \tag{3.14}$$

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:

$$\boldsymbol{Y}_e = \boldsymbol{X}_a\boldsymbol{H}_{ae} + \boldsymbol{X}_b\boldsymbol{H}_{be} + \boldsymbol{W}_e, \tag{3.15}$$

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 $\mathcal{CN}\left(\boldsymbol{0}, \sigma^2\boldsymbol{I}_{T_2}\right)$. The eavesdropper can take advantage of the 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 [95]. 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[4], it is assumed 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 $\boldsymbol{Z}_e = \boldsymbol{X}_b\boldsymbol{H}_{be} + \boldsymbol{W}_e$ as interference plus noise signal in the above equation (3.15). By applying the LMMSE criterion, the eavesdropper can obtain the estimate of $\boldsymbol{H}_{ae}$ as:

$$\hat{\boldsymbol{H}}_{ae} = \sigma_{ae}^2\boldsymbol{X}_a^H\left(\sigma_{ae}^2\boldsymbol{X}_a\boldsymbol{X}_a^H + \boldsymbol{R}_{\boldsymbol{Z}_e}\right)^{-1}\boldsymbol{Y}_e, \tag{3.16}$$

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

$$\hat{\boldsymbol{H}}_{ae} = \frac{\sigma_{ae}^2}{(N_a\sigma_{ae}^2 + N_b\sigma_{be}^2)/T_2 + \sigma^2}\boldsymbol{X}_a^H\boldsymbol{Y}_{\boldsymbol{e}}, \tag{3.17}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}. \tag{3.18}$$

To further improve the accuracy of channel estimates, the eavesdropper can use 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

[4]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.

techniques given in [94,96,97], 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.

3.4 Performance Analysis of Proposed Channel Estimation Technique

3.4.1 Mean Square Error

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

At Bob

The normalized MSE for the first stage is given as:

$$\mathcal{E}_{bb} = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\}]}{N_b^2}, \tag{3.19}$$

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 [92] as:

$$\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{bb}(\Delta\hat{\boldsymbol{H}}_{bb})^H\} = \left(\boldsymbol{R}^{-1}_{\boldsymbol{H}_{bb}} + \boldsymbol{X}^H_{sb}\boldsymbol{R}^{-1}_{\boldsymbol{W}^b_{si}}\boldsymbol{X}_{sb}\right)^{-1}, \tag{3.20}$$

where $\boldsymbol{R}_{\boldsymbol{H}_{bb}}$ is the covariance of the channel $\boldsymbol{H}_{bb}$, and $\boldsymbol{R}_{\boldsymbol{W}^b_{si}}$ is the noise covariance matrix. Using the error correlation matrix given in (3.20), $\mathcal{E}_{bb}$ can be simplified as:

$$\mathcal{E}_{bb} = \left(\frac{1}{\sigma^2_{bb}} + \frac{1}{\sigma^2}\right)^{-1}. \tag{3.21}$$

MSE for $\hat{\boldsymbol{H}}_{ab}$ using the error correlation matrix from [92] is given as:

$$\mathcal{E}_{ab} = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ab}(\Delta\hat{\boldsymbol{H}}_{ab})^H\}]}{N_a N_b}, \tag{3.22}$$

$$= \frac{N_b \mathrm{Tr}\left[\left(\frac{1}{\sigma_{ab}^2}\boldsymbol{I}_{N_a} + \left(\frac{1}{\sigma^2+\mathcal{E}_{bb}}\right)\boldsymbol{X}_a^H\boldsymbol{X}_a\right)^{-1}\right]}{N_a N_b}, \tag{3.23}$$

$$= \left(\frac{1}{\sigma_{ab}^2} + \frac{1}{\sigma^2+\mathcal{E}_{bb}}\right)^{-1}. \tag{3.24}$$

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:

$$\mathcal{E}_{ae} = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ae}(\Delta\hat{\boldsymbol{H}}_{ae})^H\}]}{N_a N_e}, \tag{3.25}$$

$$= \frac{\mathrm{Tr}\left[\frac{1}{\sigma_{ae}^2}\boldsymbol{I}_{N_a} + \left(\frac{1}{\sigma_{be}^2+\sigma^2}\right)\boldsymbol{X}_a^H\boldsymbol{X}_a\right]}{N_a}, \tag{3.26}$$

$$= \left(\frac{1}{\sigma_{ae}^2} + \frac{1}{\sigma_{be}^2+\sigma^2}\right)^{-1}. \tag{3.27}$$

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.

3.4.2 Secrecy Capacity

In this section, the secrecy performance of the proposed FD-DCE is analyzed based on the MSE provided in the previous section. To analyze the secrecy performance of the proposed

FD-DCE utilize the secrecy capacity which is defined as [30]:

$$C_s = \frac{1}{T_d} \left[C_b - C_e \right]^+, \tag{3.28}$$

where C_b, C_e corresponds to the channel capacity at Bob and the eavesdropper respectively, T_d indicates the length of the data transmission stage, and the notation $[x]^+$ means $\max\{x, 0\}$.

Following the channel estimation using the proposed FD-DCE, Alice transmits T_d data symbols to Bob using half-duplex transmission, i.e. Alice transmits the data signal while Bob remains silent. The signals received by Bob and the eavesdropper are given as:

$$\boldsymbol{Y}_b^d = \boldsymbol{X}_d \boldsymbol{H}_{ab} + \boldsymbol{W}_b^d, \tag{3.29}$$

$$\boldsymbol{Y}_e^d = \boldsymbol{X}_d \boldsymbol{H}_{ae} + \boldsymbol{W}_e^d, \tag{3.30}$$

where $\boldsymbol{X}_d \in \mathbb{C}^{T_d \times N_a}$ are data symbols transmitted by Alice, and $\boldsymbol{W}_b^d$, and $\boldsymbol{W}_e^d$ denote ZMCSWGN with variance σ^2. It can be seen from the above equation that half-duplex data transmission represents a better opportunity for eavesdropping as compared to the full-duplex transmission, because the eavesdropper receives only one signal from Alice while Bob remains silent.

To derive the channel capacity at Bob, the received signal $\boldsymbol{Y}_b^d$ can also be written in vector form as:

$$\boldsymbol{y}_b^d = \left(\boldsymbol{I}_{T_d} \otimes \boldsymbol{H}_{ba} \right) \boldsymbol{x}_d + \boldsymbol{w}_b^d, \tag{3.31}$$

where $\otimes$ denotes the Kronecker product, $\boldsymbol{H}_{ba} = \boldsymbol{H}_{ab}^T$,[5] $\boldsymbol{x}_d = \text{vec}\left(\boldsymbol{X}_d\right)$, and $\boldsymbol{w}_b^d = \text{vec}\left(\boldsymbol{W}_b^d\right)$. We have considered a scenario where CSI is not available at the transmitter, therefore to achieve channel capacity the data transmission signal $\boldsymbol{x}_d$ is taken from Gaussian distribution with covariance: $\mathbb{E}[\boldsymbol{x}_d \boldsymbol{x}_d^H] = \frac{P}{N_a} \boldsymbol{I}_{N_a T_d}$ [98], where P is the available power for data transmission. To derive a lower bound on achievable channel capacity at Bob, the mutual information conditioned on the estimated channel is given as [98]:

$$I(\boldsymbol{x}_d; \boldsymbol{y}_b^d | \hat{\boldsymbol{H}}_{ba}) = h(\boldsymbol{x}_d | \hat{\boldsymbol{H}}_{ba}) - h(\boldsymbol{x}_d | \boldsymbol{y}_b^d, \hat{\boldsymbol{H}}_{ba}). \tag{3.32}$$

[5]Here, $\boldsymbol{H}_{ba} = \boldsymbol{H}_{ab}^T$ does not indicate reciprocity of the channel; it is used for the ease of notation such that: $\boldsymbol{y}_b^d = \text{vec}(\boldsymbol{Y}_b^d)$.

The first term on the right hand side of the above equation indicates the entropy of the data signal $\boldsymbol{x}_d$ as $\boldsymbol{x}_d$ is independent of $\hat{\boldsymbol{H}}_{ba}$. Hence, the entropy is given as: $h(\boldsymbol{x}_d|\hat{\boldsymbol{h}}_{ba}) = \mathbb{E}[\log_2|\pi e\frac{P}{N_a}\boldsymbol{I}_{N_aT_d}|]$. The upper bound for the second term in (3.32) can be obtained by using the LMMSE estimation to estimate $\boldsymbol{x}_d$ given $\boldsymbol{y}_b^d$ and $\hat{\boldsymbol{H}}_{ba}$. Therefore, using MSE for the LMMSE estimation [92], the entropy is given as:

$$h(\boldsymbol{x}_d|\boldsymbol{y}_b^d, \hat{\boldsymbol{H}}_{ba}) \leq \mathbb{E}\left[\left|\pi e(\boldsymbol{R}_{\boldsymbol{x_d}}^{-1} + \boldsymbol{H}^H\boldsymbol{R}_{\boldsymbol{w}}^{-1}\boldsymbol{H})^{-1}\right|\right], \tag{3.33}$$

where $\boldsymbol{R}_{\boldsymbol{x_d}}$ denotes the covariance matrix of $\boldsymbol{x}_d$, $\boldsymbol{H} = (\boldsymbol{I}_{T_d} \otimes \hat{\boldsymbol{H}}_{ba})$, and $\boldsymbol{R}_{\boldsymbol{w}}$ represents the covariance of $\boldsymbol{w} = (\boldsymbol{I}_{T_d} \otimes \Delta\hat{\boldsymbol{H}}_{ba})\boldsymbol{x}_d + \boldsymbol{w}_b^d$. Exploiting the independence between $\Delta\hat{\boldsymbol{H}}_{ba}$, $\boldsymbol{x}_d$, and $\boldsymbol{w}_b^d$, $\boldsymbol{R}_{\boldsymbol{w}}$ is given as:

$$\boldsymbol{R}_{\boldsymbol{w}} = \mathbb{E}[\boldsymbol{w}_b^d\boldsymbol{w}_b^{d^H}] + \mathbb{E}[\boldsymbol{H}\boldsymbol{x}_d\boldsymbol{x}_d^H\boldsymbol{H}^H]. \tag{3.34}$$

Substituting the values of $\mathbb{E}[\boldsymbol{w}_b^d\boldsymbol{w}_b^{d^H}]$ and $\mathbb{E}[\boldsymbol{x}_d\boldsymbol{x}_d^H]$ in the above equation we get:

$$\begin{aligned}\boldsymbol{R}_{\boldsymbol{w}} =& \sigma^2\boldsymbol{I}_{T_dN_b} + \frac{P}{N_a}\mathbb{E}\Big[\big(\boldsymbol{I}_{T_d} \otimes \Delta\hat{\boldsymbol{H}}_{ba}\big)\big(\boldsymbol{I}_{T_d} \otimes \Delta\hat{\boldsymbol{H}}_{ba}^H\big)\Big], &(3.35)\\ =& \sigma^2\boldsymbol{I}_{T_dN_b} + \frac{P}{N_a}\Big(\boldsymbol{I}_{T_d} \otimes \mathbb{E}\big[\Delta\hat{\boldsymbol{H}}_{ba}\Delta\hat{\boldsymbol{H}}_{ba}^H\big]\Big), &(3.36)\end{aligned}$$

substituting $\mathbb{E}\big[\Delta\hat{\boldsymbol{H}}_{ba}\Delta\hat{\boldsymbol{H}}_{ba}^H\big] = N_a\mathcal{E}_{ab}\boldsymbol{I}_{N_b}$ in the above equation we get:

$$\boldsymbol{R}_{\boldsymbol{w}} = \big(\sigma^2 + P\mathcal{E}_{ab}\big)\boldsymbol{I}_{T_dN_b}. \tag{3.37}$$

Putting values of respective covariance matrices in (3.33), it can be simplified as:

$$\begin{aligned}h(\boldsymbol{x}_d|\boldsymbol{y}_b^d, \hat{\boldsymbol{H}}_{ba}) \leq& \mathbb{E}\left[\log_2\left((\pi e)^{T_dN_a}\Big|\boldsymbol{I}_{T_d} \otimes \frac{N_a}{P}\boldsymbol{I}_{N_a} + \boldsymbol{I}_{T_d} \otimes \frac{\hat{\boldsymbol{H}}_{ba}^H\hat{\boldsymbol{H}}_{ba}}{\sigma^2 + P\mathcal{E}_{ab}}\Big|\right)\right], &(3.38)\\ =& T_d\mathbb{E}\left[\log_2\left((\pi e)^{T_dN_a}\Big|\frac{N_a}{P}\boldsymbol{I}_{N_a} + \frac{\hat{\boldsymbol{H}}_{ba}^H\hat{\boldsymbol{H}}_{ba}}{\sigma^2 + P\mathcal{E}_{ab}}\Big|\right)\right]. &(3.39)\end{aligned}$$

Therefore, mutual information $I(\boldsymbol{x}_d; \boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba})$ is given as:

$$\begin{aligned} I(\boldsymbol{x}_d; \boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}) \geq & T_d \mathbb{E}\big[\log_2 \big|\boldsymbol{I}_{N_a} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ba}^H \hat{\boldsymbol{H}}_{ba}}{\sigma^2 + P\mathcal{E}_{ab}}\big|\big], \\ \triangleq & C_b^-, \end{aligned} \tag{3.40}$$

where C_b^- represent the lower bound on the channel capacity at Bob. Using the identity $|\boldsymbol{I}_a + \boldsymbol{AB}| = |\boldsymbol{I}_b + \boldsymbol{BA}|$, where a and b are the number of rows in $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, the lower bound on channel capacity can also be given as:

$$C_b^- = T_d \mathbb{E}\big[\log_2 \big|\boldsymbol{I}_{N_b} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ba}\hat{\boldsymbol{H}}_{ba}^H}{\sigma^2 + \mathcal{E}_{ab}P}\big|\big]. \tag{3.41}$$

In order to find an upper bound on channel capacity, the mutual information is expanded as:

$$I(\boldsymbol{x}_d; \boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}) = h(\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}) - h(\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}, \boldsymbol{x}_d). \tag{3.42}$$

The first term on the right hand side $h(\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba})$ of the above equation is lower bounded by covariance of $\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}$ as:

$$h(\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}) \leq \mathbb{E}[\log_2 |\pi e \boldsymbol{R}_{\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}}|], \tag{3.43}$$

$$= T_d \mathbb{E}\bigg[\log_2 \Big((\pi e)^{T_d N_b} \big|\frac{P}{N_a}\hat{\boldsymbol{H}}_{ba}\hat{\boldsymbol{H}}_{ba}^H + \left(P\mathcal{E}_{ab} + \sigma^2\right)\boldsymbol{I}_{N_b}\big|\Big)\bigg]. \tag{3.44}$$

For second term on the right hand side of (3.42), $h(\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}, \boldsymbol{x}_d) = \mathbb{E}[|\pi e \boldsymbol{R}_{\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}, \boldsymbol{x}_d}|]$, where covariance matrix is given as:

$$\boldsymbol{R}_{\boldsymbol{y}_b^d|\hat{\boldsymbol{H}}_{ba}, \boldsymbol{x}_d} = \mathbb{E}\Big[\boldsymbol{I}_{T_d} \otimes \left(\Delta\hat{\boldsymbol{H}}_{ba}\boldsymbol{x}_d\boldsymbol{x}_d^H\Delta\hat{\boldsymbol{H}}_{ba}^H\right) + \boldsymbol{w}_b\boldsymbol{w}_b^H\Big], \tag{3.45}$$

$$= \boldsymbol{I}_{T_d} \otimes (\sigma^2 + \mathcal{E}_{ab}\boldsymbol{x}_d^H\boldsymbol{x}_d)\boldsymbol{I}_{N_b}. \tag{3.46}$$

Combining (3.44) and (3.46), we get:

$$I(\boldsymbol{x}_d; y_b^d|\hat{\boldsymbol{H}}_{ba}) \leq T_d\mathbb{E}\Big[\log_2\Big|\boldsymbol{I}_{N_b} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ba}\hat{\boldsymbol{H}}_{ba}^H}{\sigma^2 + P\mathcal{E}_{ab}}\Big|\Big] + T_d N_b\mathbb{E}\Big[\log_2\Big(\frac{\sigma^2 + P\mathcal{E}_{ab}}{\sigma^2 + \boldsymbol{x}_d^H\boldsymbol{x}_d\mathcal{E}_{ab}}\Big)\Big], \tag{3.47}$$

$$= C_b^- + T_d N_b\mathbb{E}\big[\log_2\big(\frac{\sigma^2 + P\mathcal{E}_{ab}}{\sigma^2 + \boldsymbol{x}_d^H\boldsymbol{x}_d\mathcal{E}_{ab}}\big)\big],$$

$$= C_b^+. \tag{3.48}$$

Similarly, the lower bound on channel capacity at the eavesdropper is given as:

$$I(\boldsymbol{x}_d; \boldsymbol{y}_e^d|\hat{\boldsymbol{H}}_{ea}) \geq T_d\mathbb{E}\left[\log_2\big|\boldsymbol{I}_{N_e} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ea}\hat{\boldsymbol{H}}_{ea}^H}{\sigma^2 + P\mathcal{E}_{ae}}\big|\right] = C_e^-. \tag{3.49}$$

Likewise, for the upper bound of channel capacity at the eavesdropper:

$$I(\boldsymbol{x}_d; \boldsymbol{y}_e^d|\hat{\boldsymbol{H}}_{ea}) \leq C_e^- + T_d N_e\mathbb{E}\left[\log_2\big(\frac{\sigma^2 + P\mathcal{E}_{ae}}{\sigma^2 + \boldsymbol{x}_d^H\boldsymbol{x}_d\mathcal{E}_{ae}}\big)\right] = C_e^+. \tag{3.50}$$

Finally, using upper and lower bound on channel capacities at Bob and the eavesdropper, we formulate the lower and upper bound on secrecy capacity as:

$$C_s^- = \frac{1}{T_d}[C_b^- - C_e^+]^+, \tag{3.51}$$

$$C_s^+ = \frac{1}{T_d}[C_b^+ - C_e^-]^+. \tag{3.52}$$

To analyze the secrecy capacity achieved by each DCE scheme we provide simulation analysis to calculate average secrecy capacity as: $C_s = (C_s^- + C_s^+)/2$ for different antennas at Bob and the eavesdropper. We have used the same transmission power in the training stage as well as the data transmission stage, which makes it impractical to assume $P \to \infty$ because it will cause the self-interference in the full-duplex channel estimation stage close to ∞.

3.4.3 Effect of Full-Duplex Data Transmission on Secrecy Capacity

This section illustrates the effect of full-duplex transmission on the secrecy capacity. The signals received by Bob and the eavesdropper during full-duplex data transmission stage are

given as:

$$\boldsymbol{Y}_b^d = \boldsymbol{X}_d^{(a)}\boldsymbol{H}_{ab} + \boldsymbol{X}_d^{(b)}\boldsymbol{H}_{bb} + \boldsymbol{W}_b^d, \tag{3.53}$$

$$\boldsymbol{Y}_e^d = \boldsymbol{X}_d^{(a)}\boldsymbol{H}_{ae} + \boldsymbol{X}_d^{(b)}\boldsymbol{H}_{be} + \boldsymbol{W}_e^d, \tag{3.54}$$

where $\boldsymbol{X}_d^{(a)}$ and $\boldsymbol{X}_d^{(b)}$ are the data symbols transmitted by Alice and Bob. Following the same step to derive channel capacity given in the previous section, the lower bound on channel capacity at Bob is given as:

$$C_{b,f}^{-} = T_d\mathbb{E}\big[\log_2\big|\boldsymbol{I}_{N_b} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ba}\hat{\boldsymbol{H}}_{ba}^H}{\sigma^2 + (\mathcal{E}_{ab} + \mathcal{E}_{bb})\,P}\big|\big]. \tag{3.55}$$

It can be seen by comparing the above equation with C_b^- given in (3.41), that $C_{b,f}^- < C_b^-$ due to the additional self-interference signal. Similarly, the lower bound on channel capacity at the eavesdropper is given as:

$$C_{e,f}^{-} = T_d\mathbb{E}\big[\log_2\big|\boldsymbol{I}_{N_e} + \frac{\frac{P}{N_a}\hat{\boldsymbol{H}}_{ea}\hat{\boldsymbol{H}}_{ea}^H}{\sigma^2 + (\mathcal{E}_{ae} + \sigma_{be}^2)\,P}\big|\big]. \tag{3.56}$$

The comparison of $C_{e,f}^-$ with C_e^- given in (3.49) shows that: $C_{e,f}^- < C_e^-$ due the additional interference signal transmitted from Bob. As $\mathcal{E}_{bb} = \frac{\sigma^2\sigma_{bb}^2}{\sigma^2+\sigma_{bb}^2}$, therefore $\mathcal{E}_{bb} < \sigma_{be}^2$, which implies that residual self-interference is less than the path-loss between Bob and the eavesdropper. Hence, it can shown that:

$$C_b^- - C_{b,f}^- < C_e^- - C_{e,f}^-. \tag{3.57}$$

The above relation indicates that loss in channel capacity due to full-duplex data transmission is greater at the eavesdropper as compared to the legitimate receiver, due to the discriminatory channel estimation at the eavesdropper as compared to Bob. Lastly, the upper bound on channel capacity is shown to be close to the lower bound in the previous section because: $\sigma^2 + P(\mathcal{E}_{ae} + \sigma_{be}^2)$ is greater than and close to $\sigma^2 + \boldsymbol{x}_d^{a^H}\boldsymbol{x}_d^a\mathcal{E}_{ae} + \boldsymbol{x}_d^{b^H}\boldsymbol{x}_d^b\sigma_{be}^2$. Therefore, secrecy capacity for full-duplex data transmission C_s^{FD} is greater than the half-duplex C_s as: $C_s^{FD} > C_s$.

3.5 Simulation Analysis and Results

This section presents the simulation analysis to demonstrate the secrecy performance achieved by the proposed FD-DCE scheme. MIMO wireless system is considered as mentioned in Section 3.2, 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 3.3. 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 [79], which implies that we have considered an indoor office environment as our simulation scenario. Therefore, path-loss for the receiver d meters away from the transmitter is given as:

$$P_r = P_t K \left(\frac{d_0}{d}\right)^{\alpha} \tag{3.58}$$

where P_r is the received power, P_t is the transmitted power, K is a constant factor, and α is path loss exponent. SNR in all the figures corresponds to the receive SNR at the legitimate node (Bob). For simulation analysis, we have utilized 10^5 independent realizations of random channels. The variance of the SI channel is considered as given by experimental evaluations in [68]. 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 the same, which implies that transmit SNR is same for all nodes. All data transmission symbols are taken from 64-ary QAM constellation. We have assumed that the residual synchronization offset degrades the signal to interference plus noise ratio by 1 dB as given in [99], 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.

For data transmission, we have utilized half-duplex transmission as mentioned in Sec-

tion 3.4.2. 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 [100]. To show the performance of the blind channel estimation technique, we utilize state of the art blind channel estimation technique for STBC [94] 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 [94]. 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 FD-DCE, as the original channel is not available at the eavesdropper.

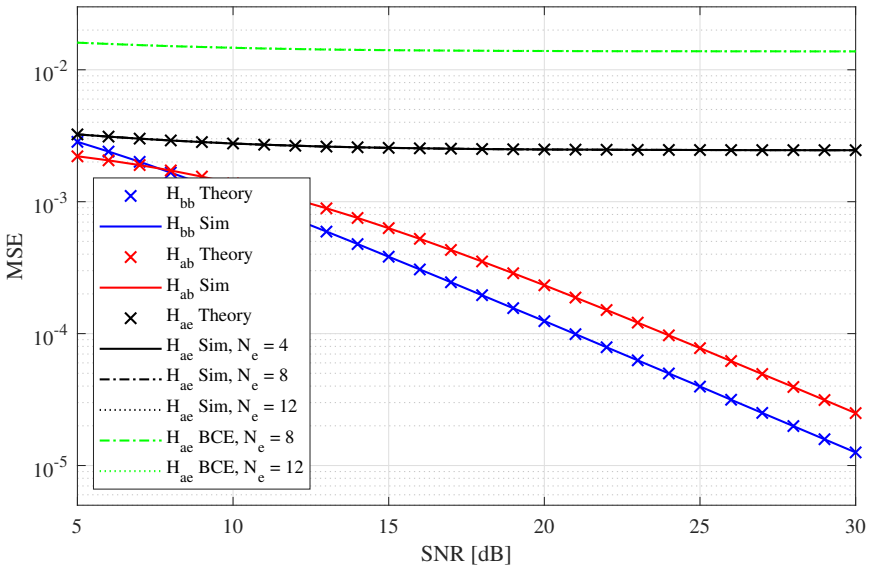


Fig. 3.2 MSE for $\boldsymbol{H}_{bb}$, $\boldsymbol{H}_{ab}$, and $\boldsymbol{H}_{ae}$, where $N_a = 4$, and $N_b = 4$.

The performance of FD-DCE is shown in Fig. 3.2, 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 3.4.1, i.e., $\boldsymbol{H}_{bb}$ Theory, $\boldsymbol{H}_{ab}$ Theory, and $\boldsymbol{H}_{ae}$ Theory, are obtained from (3.21), (3.24), and (3.27), 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. 3.2. 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 SI signal.

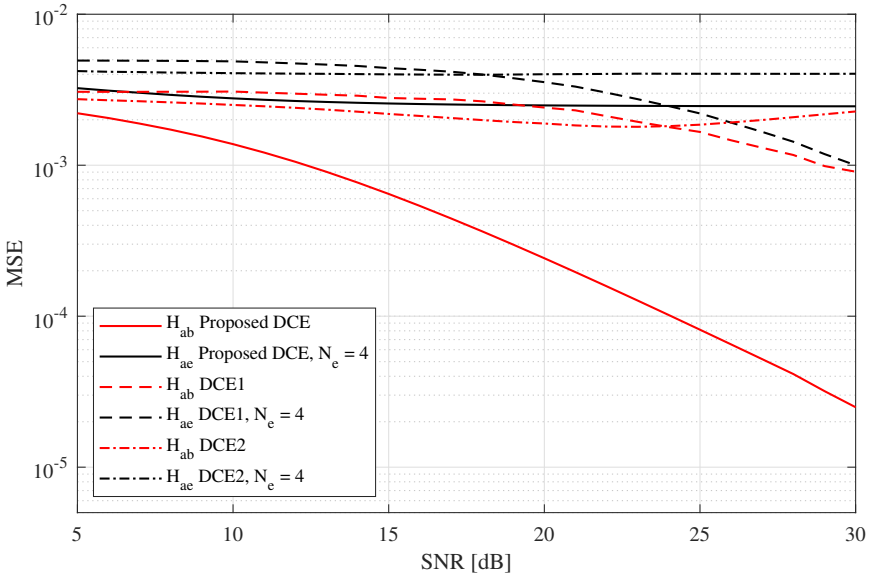


Fig. 3.3 MSE comparison with two prominent DCE schemes, DCE1 presented in [17], and DCE2 [18], where $N_a = 4$, $N_b = 4$, and $N_e = 4$.

Fig. 3.3 provides the performance comparison of FD-DCE scheme against two prominent DCE schemes presented in [17], and [18], denoted here as DCE1, and DCE2, respectively. For the implementation of DCE1 and DCE2, statistical information regarding the eaves-

dropper'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 [17, 18] 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. 3.2 that, MSE remains the same for the different number of receive antennas. Fig. 3.3 shows that DCE1 keeps MSE at the eavesdropper higher than the FD-DCE because the eavesdropping variance is utilized in power allocation which is not available for FD-DCE. 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.

In Fig. 3.4, C_s of the system is indicated based on the estimation error at Bob and the eavesdropper. C_s represents the average secrecy capacity as mentioned in Section 3.4.2, we have considered average secrecy capacity to illustrate the performance improvements achieved by the FD-DCE efficiently as the difference in secrecy capacity between FD-DCE and existing DCE techniques is the same for lower and upper bound on secrecy capacity. The transmission model is considered as mentioned in Section 3.4.2. 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. 3.4 shows that increasing the number of antennas at the eavesdropper decreases the secrecy capacity. It can be seen

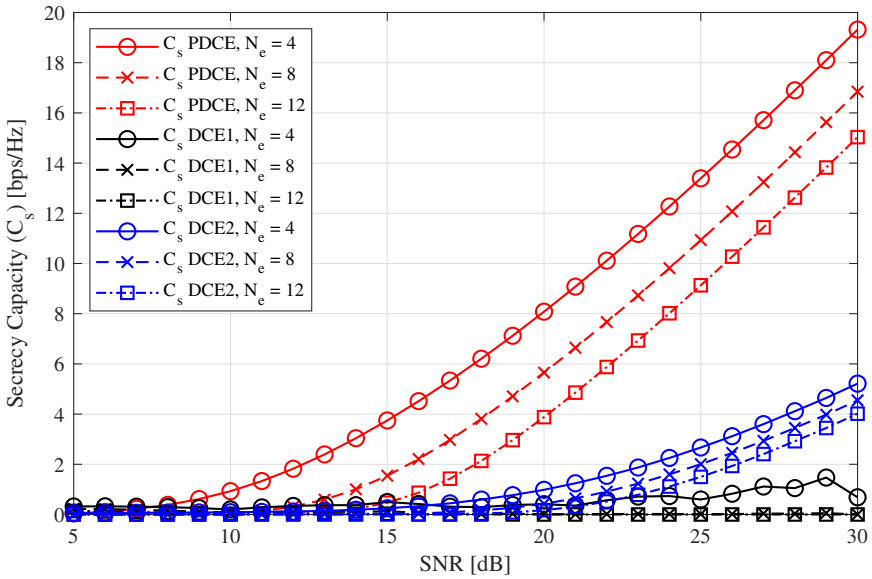


Fig. 3.4 Secrecy Capacity achieved by using proposed DCE against DCE1 and DCE2.

from the relation of C_e given in (3.50), that an increase in N_e results in the increase of the channel capacity C_e. C_s for FD-DCE 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 FD-DCE, while existing DCE techniques are unable to provide secure communication.

Finally, in Fig. 3.5 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 FD-DCE, 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

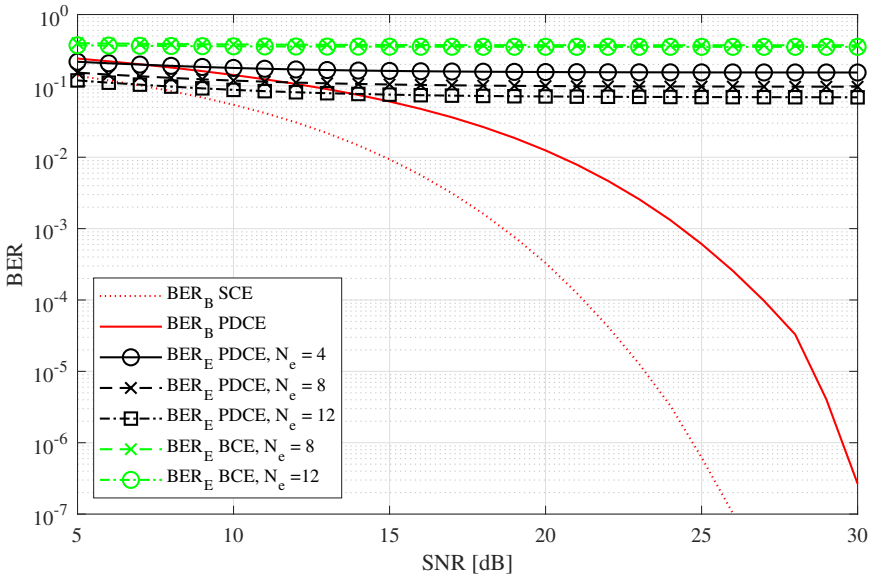


Fig. 3.5 BER achieved at Bob and the eavesdropper for different channel estimation techniques against transmit SNR, for rate 1/2 OSTBC.

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 (3.25). Fig. 3.5 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. 3.3 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. 3.5, 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 FD-DCE.

3.6 Summary

In this chapter, 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 FD-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 chapter, 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 the proposed FD-DCE technique as compared to other existing DCE techniques.

The secrecy of the pilot sequence using FD is optimal for the scenarios where the eavesdropper is equidistant from Alice and Bob, as the channel estimation performance for Alice-eavesdropper channel improves as the eavesdropper moves closer to Alice as compared to Bob. Therefore, it is critical to analyze the effect of a strategically located eavesdropper on FD-DCE. In the next chapter, we present the effect of the eavesdropper's location on the achieved secrecy and also explore the innovative solution to further enhance the secrecy achieved by the DCE techniques.

Chapter 4

Artificial Noise Aided Full-Duplex Discriminatory Channel Estimation

4.1 Introduction

In the previous chapter a novel discriminatory channel estimation (DCE) is presented, where in-band full-duplex (FD) transmissions are utilized to simultaneously transmit the pilot sequence from the legitimate nodes, 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. The full-duplex discriminatory channel estimation (FD-DCE) technique presented in the previous chapter requires that the malicious user is not too close to the transmitter; even then 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. 4.1, 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 FD-DCE, in this chapter we present two novel artificial noise (AN) assisted DCE techniques where AN aided multistage full-duplex DCE is utilized to tackle

the challenge of a strategically located passive eavesdropper.

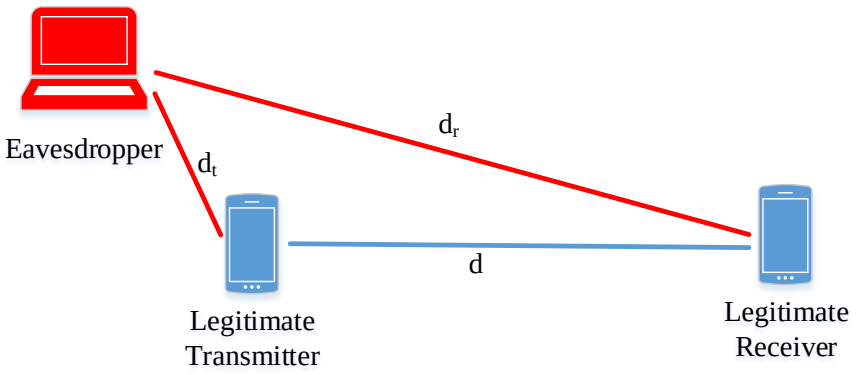


Fig. 4.1 Lucrative location to eavesdrop as the distance from the legitimate receiver (d_r) is greater than the legitimate transmitter (d_t).

First, we propose ANFD-DCE, which comprises of three stages, where the first stage is responsible for residual SI channel estimation by using a private orthogonal training signal as given in Section 3.3. 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 secure communication. 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 to acquire the variance of the legitimate channel (between the legitimate transmitter and receiver). In the second training stage, FD transmissions are utilized to simultaneously transmit the known training signals from both the legitimate nodes to acquire a rough estimate of the legitimate channel. The rough channel estimate of the main channel will be utilized to design an artificial noise signal orthogonal to the main channel for the upcoming AN assisted training stage. The eavesdropper can exploit the estimated channel statistical information to acquire the power of the training signal, and utilize the linear minimum mean square error (LMMSE) estimation to acquire the respective channel estimates. Finally, in the last channel estimation stage, both legitimate nodes transmit training signals to improve the estimate of their respective legitimate channels, along with orthogonal AN signals to deteriorate the channel estimation performance at the eavesdropper.

In ANFD-DCE, the eavesdropper can utilize the rough channel estimation stage to acquire the robust channel estimates using the LMMSE estimator. To overcome this drawback of the ANFD-DCE, we propose a novel double artificial noise aided full-duplex (DANFD) discriminatory channel estimation[1], where an AN signal is transmitted in the rough channel estimation stage to overcome the drawback of the ANFD-DCE. DANFD-DCE also comprises three stages where the first stage is responsible for SI channel estimation, followed by the rough channel estimation stage and the AN aided channel estimation stage. The performance analysis indicates that the DANFD-DCE achieves robust secure communication as compared to the ANFD-DCE and the FD-DCE presented in Chapter 3.

The same channel model is utilized in this chapter, as presented in Section 3.2. The rest of this chapter is organized into three sections. Section 4.2 explains the proposed ANFD-DCE. Section 4.3 presents the novel DANFD-DCE and the summary of this chapter is presented in Section 4.4.

4.2 Artificial Noise aided Full-Duplex Discriminatory Channel Estimation Technique

4.2.1 First Stage: SI Channel Estimation

SI channel estimation is the first stage of the artificial noise aided full-duplex (ANFD)-DCE; it is responsible for acquiring robust estimates of 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 FD-DCE technique given in Section 3.4, 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 [89] such that: $T_1 = N_a + N_b$, which makes blind channel estimation techniques inoperable at the eavesdropper. 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.

[1]The proposed DANFD-DCE technique presented in this chapter was presented in [101].

At Bob

As mentioned in the previous chapter, the corresponding received signal at Bob is given as:

$$\boldsymbol{Y}_{si}^{b} = \boldsymbol{X}_{sb}\boldsymbol{H}_{bb} + \boldsymbol{W}_{si}^{b}, \tag{4.1}$$

and the corresponding LMMSE estimator is given as:

$$\hat{\boldsymbol{H}}_{bb} = \boldsymbol{R}_{\boldsymbol{H}_{bb}}\mathbf{X}_{sb}^{H}\left(\mathbf{X}_{sb}\boldsymbol{R}_{\boldsymbol{H}_{bb}}\mathbf{X}_{sb}^{H} + \boldsymbol{R}_{\boldsymbol{W}_{si}^{b}}\right)^{-1}\mathbf{Y}_{si}^{b}, \tag{4.2}$$

using $\boldsymbol{R}_{\boldsymbol{H}_{bb}} = \sigma_{bb}^{2}\boldsymbol{I}_{N_b}$ and $\boldsymbol{R}_{\boldsymbol{W}_{si}^{b}} = \sigma^{2}\boldsymbol{I}_{N_b}$, the above can be simplified as:

$$\hat{\boldsymbol{H}}_{bb} = \frac{\sigma_{bb}^{2}}{\sigma_{bb}^{2}+\sigma^{2}}\boldsymbol{X}_{sb}^{H}\mathbf{Y}_{si}^{b} \tag{4.3}$$

$$\triangleq \boldsymbol{H}_{bb} + \Delta\hat{\boldsymbol{H}}_{bb}, \tag{4.4}$$

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

$$\mathcal{E}_{bb} = \frac{\mathrm{Tr}\left[\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{bb}\Delta\hat{\boldsymbol{H}}_{bb}^{H}\right)\right]}{N_b^{2}}, \tag{4.5}$$

$$= \left(\frac{1}{\sigma_{bb}^{2}} + \frac{1}{\sigma^{2}}\right)^{-1}. \tag{4.6}$$

At Alice

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

$$\boldsymbol{Y}_{s}^{a} = \boldsymbol{X}_{sb}\boldsymbol{H}_{ba} + \boldsymbol{W}_{s}^{a}, \tag{4.7}$$

where $\boldsymbol{W}_{s}^{a}$ 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 $\boldsymbol{R}_{\boldsymbol{Y}_{s}^{a}} = \boldsymbol{X}_{sb}^{H}\boldsymbol{R}_{\boldsymbol{H}_{ba}}\boldsymbol{X}_{sb} + \boldsymbol{R}_{\boldsymbol{W}_{s}^{a}} = \left(\sigma_{ba}^{2}+\sigma^{2}\right)\boldsymbol{I}_{N_b}$. Alice employs Maximum Likelihood Estimator (MLE) given in [92] 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:

$$\hat{\sigma}_{ba}^2 = \frac{\mathrm{Tr}\left[\left(\boldsymbol{Y}_s^a\right)^H\left(\boldsymbol{Y}_s^a\right)\right]}{N_a N_b} - \sigma^2. \tag{4.8}$$

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 the variance and mean of $\hat{\sigma}_{ba}^2$. The above equation (4.8) can also be written as:

$$\hat{\sigma}_{ba}^2 = \frac{1}{N_a N_b}\sum_{i=1}^{N_b}\sum_{j=1}^{N_a} |\left[\boldsymbol{Y}_s^a\right]_{i,j}|^2 - \sigma^2, \tag{4.9}$$

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

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

As the mean of $\mathbb{E}\left[\chi^2\left(N_a N_b\right)\right] = N_a N_b$, 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:

$$\mathcal{E}_{\hat{\sigma}_{ba}^2} = \mathbb{E}\left[\left(\hat{\sigma}_{ba}^2 - \mathbb{E}\left[\hat{\sigma}_{ba}^2\right]\right)^2\right], \tag{4.10}$$

$$= \mathbb{E}\left[\left(\frac{\sigma_{ba}^2 + \sigma^2}{N_a N_b}\chi^2\left(N_a N_b\right) - \left(\sigma^2 + \sigma_{ba}^2\right)\right)^2\right], \tag{4.11}$$

$$= \left(\frac{\sigma^2 + \sigma_{ba}^2}{N_a N_b}\right)^2 \mathbb{E}\left[\left(\chi^2\left(N_a N_b\right) - N_a N_b\right)^2\right], \tag{4.12}$$

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 $\hat{\sigma}^2_{ba}$ is given as:

$$\mathcal{E}_{\hat{\sigma}^2_{ba}} = \frac{2(\sigma^2_{ba} + \sigma^2)^2}{N_aN_b}. \tag{4.13}$$

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 [79]. Hence, without the loss of generality, we assume that the $\mathcal{E}_{\hat{\sigma}^2_{ba}}$ 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:

$$\boldsymbol{Y}^e_{si} = \boldsymbol{X}_{sb}\boldsymbol{H}_{be} + \boldsymbol{W}^e_{si}, \tag{4.14}$$

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

$$\hat{\sigma}^2_{be} = \frac{\mathrm{Tr}\left[\left(\boldsymbol{Y}^e_{si}\right)\left(\boldsymbol{Y}^e_{si}\right)^H\right]}{N_eN_b} - \sigma^2. \tag{4.15}$$

The estimated channel variance $\hat{\sigma}^2_{be}$ will be exploited by the eavesdropper to utilize LMMSE based estimation for acquiring robust estimates. Similar to the MSE for variance estimation at Alice, MSE for $\hat{\sigma}^2_{be}$ will be equal to: $2(\sigma^2_{be} + \sigma^2)^2/(N_bN_e)$.

4.2.2 Second Stage: Rough Channel Estimation

This stage is responsible for acquiring rough channel estimates to design AN orthogonal to the main channel ($\boldsymbol{H}_{ab}$, and $\boldsymbol{H}_{ba}$) for transmission in the AN aided training stage. Alice and Bob transmit $\boldsymbol{X}_a^{(1)} = \sqrt{x_1}\boldsymbol{V}_a^{(1)}$, and $\boldsymbol{X}_b^{(1)} = \sqrt{x_1}\boldsymbol{V}_b^{(1)}$ using in-band FD transmissions, where x_1 is the variance of the training signals determined through a run in each node of the adaptive power allocation scheme described in Section 4.2.4, and $\boldsymbol{V}_a^{(1)}$, and $\boldsymbol{V}_b^{(1)}$ are globally known orthogonal training signals such that: $\boldsymbol{V}_a^{(1)^H}\boldsymbol{V}_a^{(1)} = \boldsymbol{I}_{N_a}$, and $\boldsymbol{V}_b^{(1)^H}\boldsymbol{V}_b^{(1)} = \boldsymbol{I}_{N_b}$. Finally, 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.

At Bob

The received signal at Bob is given as:

$$\boldsymbol{Y}_b^{(1)} = \boldsymbol{X}_a^{(1)}\boldsymbol{H}_{ab} + \boldsymbol{X}_b^{(1)}\boldsymbol{H}_{bb} + \boldsymbol{W}_b^{(1)}, \tag{4.16}$$

where $\boldsymbol{W}_b^{(1)}$ is ZMCSWGN with covariance $\sigma^2\boldsymbol{I}_{T_2}$. The received signal at Bob after digital SI cancellation is given as: $\boldsymbol{Y}_1 = \boldsymbol{Y}_b^{(1)} - \boldsymbol{X}_b^{(1)}\hat{\boldsymbol{H}}_{bb}$. LMMSE is used to estimate $\boldsymbol{H}_{ab}$ as given in [92] by exploiting the estimated statistical information as:

$$\hat{\boldsymbol{H}}_{ab} = \sigma_{ab}^2 N_b \mathbf{X}_b^{(1)^H}\left(\sigma_{ab}^2 N_b \mathbf{X}_b^{(1)}\mathbf{X}_b^{(1)^H} + \boldsymbol{R}_{\boldsymbol{W}^{(1)}}\right)^{-1}\mathbf{Y}_1, \tag{4.17}$$

where $\boldsymbol{R}_{\boldsymbol{W}^{(1)}}$ denotes the covariance matrix of $\boldsymbol{W}^{(1)} = \boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}$. $\boldsymbol{R}_{\boldsymbol{W}^{(1)}}$ is given as: $N_b\left(\mathcal{E}_{bb}x_1c + \sigma^2\right)\boldsymbol{I}_{T_2}$, since $\boldsymbol{X_b^{(1)}}\boldsymbol{X_b^{(1)^H}} = x_1c\boldsymbol{I}_{N_b}$, where $c = \frac{N_b}{T_2}$. Therefore, the above equation can be simplified as:

$$\hat{\boldsymbol{H}}_{ab} = \frac{\sigma_{ab}^2}{\left(\sigma^2 + \left(\sigma_{ab}^2 + \mathcal{E}_{bb}c\right)x_1\right)}\boldsymbol{X}_b^{(1)^H}\boldsymbol{Y}_1, \tag{4.18}$$

$$\triangleq \boldsymbol{H}_{ab} + \Delta\hat{\boldsymbol{H}}_{ab}^{(1)}. \tag{4.19}$$

To analyze the channel estimation performance, the MSE at Bob for the rough channel

estimation stage is derived as [92]:

$$\begin{aligned}\mathcal{E}_{ab}^{(1)} =& \frac{\mathrm{Tr}\left[\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{ab}^{(1)}\Delta\hat{\boldsymbol{H}}_{ab}^{(1)^H}\right)\right]}{N_a N_b},\\ =& \frac{N_a \mathrm{Tr}\left[\left(\frac{1}{\sigma_{ab}^2}\boldsymbol{I}_{N_b} + \left(\frac{1}{\sigma^2 + x_1\mathcal{E}_{bb}c}\right)\boldsymbol{X}_b^{(1)^H}\boldsymbol{X}_b^{(1)}\right)^{-1}\right]}{N_a N_b},\\ =& \left(\frac{1}{\sigma_{ab}^2} + \frac{x_1}{\sigma^2 + x_1\mathcal{E}_{bb}c}\right)^{-1}. \end{aligned} \tag{4.20}$$

At the eavesdropper

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

$$\boldsymbol{Y}_e^{(1)} = \boldsymbol{X}_a^{(1)}\boldsymbol{H}_{ae} + \boldsymbol{X}_b^{(1)}\boldsymbol{H}_{be} + \boldsymbol{W}_e^{(1)}, \tag{4.21}$$

where $\boldsymbol{W}_e^{(1)}$ denotes the ZMCSWGN with variance σ^2. The eavesdropper utilizes the estimated channel variances $\hat{\sigma}_{ae}^2$ and $\hat{\sigma}_{be}^2$ to acquire the variance x_1 with which the training signal is transmitted by the legitimate nodes. 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}). Similar to Bob, LMMSE estimator is utilized to estimate $\boldsymbol{H}_{ae}$ by the eavesdropper as:

$$\hat{\boldsymbol{H}}_{ae} = \frac{\sigma_{ae}^2}{\left(\sigma^2 + \left(\sigma_{ae}^2 + \sigma_{be}^2 c\right)x_1\right)}\boldsymbol{X}_a^{(1)^H}\boldsymbol{Y}_e^{(1)}, \tag{4.22}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}^{(1)}. \tag{4.23}$$

The normalized MSE for the above estimator is given as:

$$\mathcal{E}_{ae}^{(1)} = \frac{\mathrm{Tr}\left[\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}\right)\right]}{N_b N_e}, \\ = \left(\frac{1}{\sigma_{ae}^2} + \frac{x_1}{\sigma^2 + x_1\sigma_{be}^2 c}\right)^{-1}. \tag{4.24}$$

4.2.3 Third Stage: AN aided Channel Estimation

In this stage, AN 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 AN 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 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:

$$\boldsymbol{X}_b^{(2)} = \begin{bmatrix}\boldsymbol{X}_{b1}^{(2)} \\ \boldsymbol{X}_{b2}^{(2)}\end{bmatrix} = \begin{bmatrix}\sqrt{x_2}\boldsymbol{V}_b^{(2)} + \boldsymbol{B}_1\boldsymbol{N}_{ba1}^H \\ \sqrt{x_2}\boldsymbol{V}_b^{(2)} + \boldsymbol{B}_2\boldsymbol{N}_{ba2}^H\end{bmatrix}, \tag{4.25}$$

where x_2 is the variance of the training signals, $\boldsymbol{V}_b^{(2)}$ is the globally known orthogonal training signal such that: $\boldsymbol{V}_b^{(2)^H}\boldsymbol{V}_b^{(2)} = \boldsymbol{I}_{N_b}$, $\boldsymbol{B}_1$, and $\boldsymbol{B}_2$ are the zero-mean Gaussian noise with variance a/N_{b1}, and, a/N_{b2}, respectively. $\boldsymbol{N}_{ba1}^H$, and $\boldsymbol{N}_{ba2}^H$ corresponds to the left-null space of the sub-channels $\hat{\boldsymbol{H}}_{ba1}$, and $\hat{\boldsymbol{H}}_{ba2}$, respectively. The length of the training signal is equal to T_2 as in the previous stage to ensure that the eavesdropper receives a superposition of two signals. As the number of antennas are equal at both nodes, the same process is repeated at Alice. For the second scenario 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 into $[\hat{\boldsymbol{h}}_{ba}^{1}, \ldots, \hat{\boldsymbol{h}}_{ba}^{N_a^{(t)}}] \in \mathbb{C}^{N_b \times N_a^{(t)}}$ such that $N_a^{(t)} < N_b$, as it is required to generate orthogonal AN. This process is repeated until the training signal is generated to estimate $\boldsymbol{H}_{ba}$. A similar approach is used to generate the training for $N_b > N_a$, and at Alice.

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

Input : $\hat{\boldsymbol{H}}_{ba}, x_2, \boldsymbol{V}_b^{(2)}, b$
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**
    $\boldsymbol{N}_{ba} \leftarrow null([\hat{\boldsymbol{h}}_{ba}^{n_{st}}, \ldots, \hat{\boldsymbol{h}}_{ba}^{n_{end}}]^H)$;
    $\boldsymbol{X}_b^{(2)} \leftarrow \sqrt{x_2}\boldsymbol{V}_b^{(2)} + \boldsymbol{B}_{n_{st}}\boldsymbol{N}_{ba}^H$, $\boldsymbol{B}_{n_{st}} \sim \mathcal{N}(\boldsymbol{0}, b\boldsymbol{I})$;
  else
    $\boldsymbol{N}_{ba} \leftarrow null([\hat{\boldsymbol{h}}_{ba}^{n_{st}}, \ldots, \hat{\boldsymbol{h}}_{ba}^{n_{end}}]^H)$;
    $\boldsymbol{X}_b^{(2)} \leftarrow \left(\boldsymbol{X}_b^{(2)} | (\sqrt{x_2}\boldsymbol{V}_b^{(2)} + \boldsymbol{B}_{n_{st}}\boldsymbol{N}_{ba}^H)\right)$, $\boldsymbol{B}_{n_{st}} \sim \mathcal{N}(\boldsymbol{0}, b\boldsymbol{I})$;
  end
  $N_{ad} \leftarrow N_{ad} - (n_{end} - n_{st} + 1)$;
  $n_{st} \leftarrow n_{end} + 1$
end

Lastly, as the design of AN 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. For example, if $\boldsymbol{H}_{ab}$ is 4×4 which is divided into two parts $\boldsymbol{H}_{ab1}$ and $\boldsymbol{H}_{ab2}$ with dimensions 4×2 and

4×2. Hence, the null space $\boldsymbol{N}_{ba1}$ is 2×4, and as $\boldsymbol{N}_{ba1}^{H}\boldsymbol{H}_{ab1} = \mathbf{0}$, it will result in 8 unknown channel coefficients and 4 equations. Therefore, the solution to this problem is not finite. Furthermore, it can be explored in the future works to consider the use of full duplex to transmit the null space to improve the secrecy of the null space. 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 are given as:

$$\mathbf{Y}_b^{(2)} = \left(\sqrt{x_2}\boldsymbol{V}_a^{(2)} + \mathbf{A}_1\mathbf{N}_{ab1}^{H}\right)\mathbf{H}_{ab1} + \left(\sqrt{x_2}\boldsymbol{V}_b^{(2)} + \mathbf{B}_1\mathbf{N}_{ba1}^{H}\right)\mathbf{H}_{bb1} + \mathbf{W}_b^{(2)}, \tag{4.26}$$

where $\boldsymbol{N}_{ab1}^{H}$ is the null space of the channel $\hat{\boldsymbol{H}}_{ab1}^{(1)}$, $\boldsymbol{A}_1$ is the zero mean Gaussian noise with variance a, and $\mathbf{W}_b^{(2)}$ is the ZMCSWGN with variance σ^2 added at Bob during the AN assisted channel estimation stage. After SI cancellation, the signals received at Bob during both channel estimation stages are given as:

$$\mathbf{Y}_2 = \begin{bmatrix}\mathbf{Y}_b^{(1)}\\ \mathbf{Y}_b^{(2)}\end{bmatrix}, \tag{4.27}$$

$$= \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_a^{(1)}\\ \sqrt{x_2}\boldsymbol{V}_a^{(2)}\end{bmatrix}\mathbf{H}_{ab1} + \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_b^{(1)}\\ \sqrt{x_2}\boldsymbol{V}_b^{(1)}\end{bmatrix}\Delta\hat{\mathbf{H}}_{bb1} + \begin{bmatrix}\mathbf{W}_b^{(1)}\\ \mathbf{A}_1\mathbf{N}_{ab1}^{H}\Delta\hat{\mathbf{H}}_{ab1}^{(1)} + \mathbf{B}_1\mathbf{N}_{ba1}^{H}\Delta\hat{\mathbf{H}}_{bb1} + \mathbf{W}_b^{(2)}\end{bmatrix}, \tag{4.28}$$

$$= \mathbf{X}_a\mathbf{H}_{ab1} + \mathbf{X}_b\Delta\mathbf{H}_{bb1} + \mathbf{W}_b \tag{4.29}$$

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

$$\hat{\mathbf{H}}_{ab1}^{(2)} = \sigma_{ab}^2 N_{b1}\mathbf{X}_b^{H}\left(N_{b1}(\sigma_{ab}^2 + \mathcal{E}_{bb})\mathbf{X}_b\mathbf{X}_b^{H} + \mathbf{R}_{\boldsymbol{W}_b}\right)^{-1}\boldsymbol{Y}_2, \tag{4.30}$$

$$= \sigma_{ab}^2 N_{b1}\left(\mathbf{I}_{N_b} + N_{b1}(\sigma_{ab}^2 + \mathcal{E}_{bb})\mathbf{X}_b^{H}\mathbf{R}_{\boldsymbol{W}_b}^{-1}\mathbf{X}_b\right)^{-1}\mathbf{X}_b^{H}\mathbf{R}_{\boldsymbol{W}_b}^{-1}\boldsymbol{Y}_2. \tag{4.31}$$

where (4.30) is converted to (4.31) by using matrix identity:

$$\mathbf{B}^{H}(\mathbf{A} + \mathbf{B}\mathbf{B}^{H})^{-1} = (\mathbf{I} + \mathbf{B}^{H}\mathbf{A}^{-1}\mathbf{B})^{-1}\mathbf{B}^{H}\mathbf{A}^{-1}, \tag{4.32}$$

and $\mathbf{R}_{\boldsymbol{W}_b}$ corresponds to the covariance of $\boldsymbol{W}_b$, which can be calculated as:

$$\begin{aligned}\mathbf{R}_{\boldsymbol{W}_b} =&\mathbb{E}\left[\boldsymbol{W}_b\boldsymbol{W}_b^H\right],\\ =&\begin{bmatrix}\sigma^2 N_{b1}\mathbf{I}_{T_2} & \mathbf{0}\\ \mathbf{0} & N_{b1}\left(\sigma^2+a(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb})\right)\mathbf{I}_{T_2}\end{bmatrix}.\end{aligned} \tag{4.33}$$

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 [17]: $(N_{b1})\mathcal{E}_{ab}^{(1)}\boldsymbol{I}_{N_{b1}}$, 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:

$$\begin{aligned}\hat{\mathbf{H}}_{ab1}^{(2)} =&\frac{\sigma_{ab}^2}{1+(\sigma^2+\mathcal{E}_{bb})\left(\frac{x_1}{\sigma^2}+\frac{x_2}{\sigma^2+a(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb})}\right)}\begin{bmatrix}\frac{\mathbf{X}_b^{(1)^H}}{\sigma^2} & \frac{\mathbf{X}_b^{(2)^H}}{\sigma^2+a(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb})}\end{bmatrix}\boldsymbol{Y}_2, &(4.34)\\ \triangleq&\boldsymbol{H}_{ab1}+\Delta\hat{\mathbf{H}}_{ab1}^{(2)}. &(4.35)\end{aligned}$$

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

$$\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}(\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)})^H\right] =\mathbb{E}\left[(\boldsymbol{H}_{ab1}-\hat{\boldsymbol{H}}_{ab1}^{(2)})\boldsymbol{H}_{ab1}^H\right]-\mathbb{E}\left[(\boldsymbol{H}_{ab1}-\hat{\boldsymbol{H}}_{ab1}^{(2)})\hat{\boldsymbol{H}}_{ab1}^{(2)^H}\right] \tag{4.36}$$

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. Using the estimator mentioned in (4.30), the above equation can be further simplified as:

$$\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)^H}\right] = \boldsymbol{R}_{\boldsymbol{H}_{ab1}}-\boldsymbol{R}_{\boldsymbol{H}_{ab1}}\boldsymbol{X}_b^H\left(\boldsymbol{X}_b\left(\boldsymbol{R}_{\boldsymbol{H}_{ab1}}+\boldsymbol{R}_{\Delta\hat{\boldsymbol{H}}_{bb1}}\right)\boldsymbol{X}_b^H+\boldsymbol{R}_{\boldsymbol{W}_b}\right)^{-1}\boldsymbol{X}_b\boldsymbol{R}_{\boldsymbol{H}_{ab1}}, \tag{4.37}$$

using identity $\boldsymbol{A}^{-1}-\boldsymbol{A}^{-1}\boldsymbol{U}(\boldsymbol{B}^{-1}+\boldsymbol{V}\boldsymbol{A}^{-1}\boldsymbol{U})^{-1}\boldsymbol{V}\boldsymbol{A}^{-1}=(\boldsymbol{A}+\boldsymbol{U}\boldsymbol{B}\boldsymbol{V})^{-1}$, the above relation can be expressed as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)^H}\right] =&\left(\boldsymbol{R}_{\boldsymbol{H}_{ab1}}^{-1}+\boldsymbol{X}_b^H\left(\boldsymbol{R}_{\boldsymbol{W}_b}+\boldsymbol{X}_b\boldsymbol{R}_{\Delta\hat{\boldsymbol{H}}_{bb1}}\boldsymbol{X}_b^H\right)^{-1}\boldsymbol{X}_b\right)^{-1}, &(4.38)\\ =&\left(\boldsymbol{R}_{\boldsymbol{H}_{ab1}}^{-1}+\frac{\boldsymbol{X}_b^H}{\mathcal{E}_{bb}N_{b1}}\left(\frac{\boldsymbol{R}_{\boldsymbol{W}_b}}{\mathcal{E}_{bb}N_{b1}}+\boldsymbol{X}_b\boldsymbol{X}_b^H\right)^{-1}\boldsymbol{X}_b\right)^{-1}, &(4.39)\end{aligned}$$

using $(\boldsymbol{A}+\boldsymbol{B}\boldsymbol{B}^H)^{-1}=\boldsymbol{A}^{-1}\boldsymbol{B}(\boldsymbol{I}+\boldsymbol{B}^H\boldsymbol{A}^{-1}\boldsymbol{B})^{-1}$, the above equation can be written as:

$$\mathbb{E}\Big[\Delta\hat{\boldsymbol{H}}^{(2)}_{ab1}\Delta\hat{\boldsymbol{H}}^{(2)^H}_{ab1}\Big]=\Big(\boldsymbol{R}^{-1}_{\boldsymbol{H}_{ab1}}+\boldsymbol{X}_b^H\boldsymbol{R}^{-1}_{\boldsymbol{W}_b}\boldsymbol{X}_b\left(\boldsymbol{I}+\mathcal{E}_{bb}N_{b1}\boldsymbol{X}_b^H\boldsymbol{R}^{-1}_{\boldsymbol{W}_b}\boldsymbol{X}_b\right)^{-1}\Big)^{-1}, \tag{4.40}$$

using (4.33), the above equation simplifies as:

$$\mathbb{E}\Big[\Delta\hat{\boldsymbol{H}}^{(2)}_{ab1}\Delta\hat{\boldsymbol{H}}^{(2)^H}_{ab1}\Big]=\left(\boldsymbol{R}^{-1}_{\boldsymbol{H}_{ab1}}+\left(\frac{x_1}{\sigma^2N_{b1}}+\frac{x_2}{fN_{b1}}\right)\left(\boldsymbol{I}+\mathcal{E}_{bb}\left(\frac{x_1}{\sigma^2}+\frac{x_2}{f}\right)\boldsymbol{I}\right)^{-1}\right)^{-1}, \tag{4.41}$$

$$=N_{b1}\left(\frac{1}{\sigma^2_{ab}}+\left(\frac{\sigma^2 f}{x_1 f+x_2\sigma^2}+\mathcal{E}_{bb}\right)^{-1}\right)^{-1}\boldsymbol{I}, \tag{4.42}$$

where $f=\sigma^2+a\left(\mathcal{E}^{(1)}_{ab}+\mathcal{E}_{bb}\right)$ and $\boldsymbol{R}_{\boldsymbol{H}_{ab1}}=\sigma^2_{ab}N_{b1}\boldsymbol{I}$. Therefore, after performing algebraic simplifications the normalized MSE of $\hat{\mathbf{H}}^{(2)}_{ab1}$ is given as:

$$\mathcal{E}^{(2)}_{ab}=\frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}^{(2)}_{ab1}(\Delta\hat{\boldsymbol{H}}^{(2)}_{ab1})^H\}]}{N_aN_{b1}}, \tag{4.43}$$

$$=\left(\frac{1}{\mathcal{E}^{(1)}_{ab}}+\frac{\sigma^4x_2}{(\sigma^2+x_1\mathcal{E}_{bb})\left[x_2\sigma^2\mathcal{E}_{bb}+(\sigma^2+x_1\mathcal{E}_{bb})\left(\sigma^2+a(\mathcal{E}^{(1)}_{ab}+\mathcal{E}_{bb})\right)\right]}\right)^{-1}. \tag{4.44}$$

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

At the eavesdropper

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

$$\boldsymbol{Y}^{(2)}_e=\begin{bmatrix}\boldsymbol{X}^{(2)}_{a,1}\\ \boldsymbol{X}^{(2)}_{a,2}\end{bmatrix}\boldsymbol{H}_{ae}+\begin{bmatrix}\boldsymbol{X}^{(2)}_{b,1}\\ \boldsymbol{X}^{(2)}_{b,2}\end{bmatrix}\boldsymbol{H}_{be}+\begin{bmatrix}\boldsymbol{W}^{(2)}_{e,1}\\ \boldsymbol{W}^{(2)}_{e,2}\end{bmatrix}, \tag{4.45}$$

$$=\begin{bmatrix}\sqrt{x_2}\boldsymbol{V}^{(2)}_a\\ \sqrt{x_2}\boldsymbol{V}^{(2)}_a\end{bmatrix}\boldsymbol{H}_{ae}+\begin{bmatrix}\sqrt{x_2}\boldsymbol{V}^{(2)}_b\\ \sqrt{x_2}\boldsymbol{V}^{(2)}_b\end{bmatrix}\boldsymbol{H}_{be}+\begin{bmatrix}\boldsymbol{A}_1\boldsymbol{N}^H_{ab1}\boldsymbol{H}_{ae}+\boldsymbol{B}_1\boldsymbol{N}^H_{ba1}\boldsymbol{H}_{be}+\boldsymbol{W}^{(2)}_{e,1}\\ \boldsymbol{A}_2\boldsymbol{N}^H_{ab2}\boldsymbol{H}_{ae}+\boldsymbol{B}_2\boldsymbol{N}^H_{ba2}\boldsymbol{H}_{be}+\boldsymbol{W}^{(2)}_{e,2}\end{bmatrix}, \tag{4.46}$$

$$=\boldsymbol{X}_a\boldsymbol{H}_{ae}+\boldsymbol{X}_b\boldsymbol{H}_{be}+\boldsymbol{W}^{(2)}_e. \tag{4.47}$$

As already mentioned, $\boldsymbol{V}_a^{(2)}$ and $\boldsymbol{V}_b^{(2)}$ are globally known but x_2, $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, $\boldsymbol{B}_1$,and $\boldsymbol{B}_2$ are not known globally. It is not possible for the eavesdropper to estimate x_2 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 [102]. However, the eavesdropper can estimate the sum of total transmitted power as: $P_e = x_1 + a$ by calculating the variance of the received signal $\boldsymbol{Y}_e^{(2)}$. To utilize the signals received in AN assisted training stage for the estimation of $\boldsymbol{H}_{ae}$, the eavesdropper can utilize LS estimation by exploiting the global pilot sequences as:

$$\hat{\boldsymbol{H}}_{ae}^{(2)} = \begin{bmatrix} \sqrt{P_e}\boldsymbol{V}_a^{(2)} \\ \sqrt{P_e}\boldsymbol{V}_a^{(2)} \end{bmatrix}^{\dagger} \boldsymbol{Y}_e^{(2)}, \tag{4.48}$$

$$= \boldsymbol{V}\boldsymbol{Y}_e^{(2)}, \tag{4.49}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}^{(2)}, \tag{4.50}$$

where $[.]^{\dagger}$ denotes the pseudo-inverse operator such that: $\boldsymbol{Z}^{\dagger} = (\boldsymbol{Z}^H\boldsymbol{Z})^{-1}\boldsymbol{Z}^H$. Finally, $\hat{\boldsymbol{H}}_{ae}^{(2)}$ can be combined with the estimate acquired in the rough channel estimation stage $\hat{\boldsymbol{H}}_{ae}^{(1)}$ by using sequential LS estimation as given in [92] as:

$$\hat{\boldsymbol{H}}_{ae} = \begin{bmatrix} \boldsymbol{X}_a^{(1)} \\ \sqrt{P_e}\boldsymbol{V}_a^{(2)} \\ \sqrt{P_e}\boldsymbol{V}_a^{(2)} \end{bmatrix}^{\dagger} \begin{bmatrix} \boldsymbol{Y}_e^{(1)} \\ \boldsymbol{Y}_e^{(2)} \end{bmatrix}, \tag{4.51}$$

$$= \frac{1}{x_1 + 2P_e}\boldsymbol{X}_a^{(1)^H}\boldsymbol{Y}_e^{(1)} + \frac{1}{x_1 + 2P_e}\begin{bmatrix} \boldsymbol{V}_a^{(2)^H} & \boldsymbol{V}_a^{(2)^H} \end{bmatrix}\boldsymbol{Y}_e^{(2)}, \tag{4.52}$$

$$= \frac{x_1}{x_1 + 2P_e}\hat{\boldsymbol{H}}_{ae}^{(1)} + \frac{2P_e}{x_1 + 2P_e}\hat{\boldsymbol{H}}_{ae}^{(2)}, \tag{4.53}$$

$$= \hat{\boldsymbol{H}}_{ae}^{(1)} + \frac{2P_e}{x_1 + 2P_e}\left(\hat{\boldsymbol{H}}_{ae}^{(2)} - \hat{\boldsymbol{H}}_{ae}^{(1)}\right), \tag{4.54}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}, \tag{4.55}$$

where, the LMMSE estimate for $\hat{\boldsymbol{H}}_{ae}^{(1)}$ given in (4.22) will be used by the eavesdropper instead of the LS estimate due to its superior performance. In the rough channel estimation stage,

the LMMSE estimator is utilized as the statistical characteristics of the received signal $\boldsymbol{Y}_e^{(1)}$, are known at the eavesdropper. The MSE for $\hat{\boldsymbol{H}}_{ae}$ is given as:

$$\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] = \mathbb{E}\left[\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}\right)\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}\right)^{H}\right]. \tag{4.56}$$

Substituting $\hat{\boldsymbol{H}}_{ae}$ and simplifying the above is given as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] = \mathbb{E}\Bigg[&\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)^{H}\Bigg]- \\ &\frac{2P_e}{x_1+2P_e}\mathbb{E}\Bigg[\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\hat{\boldsymbol{H}}_{ae}^{(2)}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)^{H}\Bigg]- \\ &\frac{2P_e}{x_1+2P_e}\mathbb{E}\Bigg[\left(\hat{\boldsymbol{H}}_{ae}^{(2)}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)^{H}\Bigg]+ \\ &\frac{4P_e^2}{(x_1+2P_e)^2}\mathbb{E}\Bigg[\left(\hat{\boldsymbol{H}}_{ae}^{(2)}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\hat{\boldsymbol{H}}_{ae}^{(2)}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)^{H}\Bigg].\end{aligned} \tag{4.57}$$

The first term on right side of the above equation is the MSE of $\boldsymbol{H}_{ae}^{(1)}$ given in (4.24). The second term on the right hand side can be simplified using the orthogonality principle of the LMMSE estimator as:

$$\mathbb{E}\Bigg[\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\hat{\boldsymbol{H}}_{ae}^{(2)}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)^{H}\Bigg] = \mathbb{E}\Bigg[\left(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\right)\hat{\boldsymbol{H}}_{ae}^{(2)^H}\Bigg], \tag{4.58}$$

because $\mathbb{E}\big[\big(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\big)\hat{\boldsymbol{H}}_{ae}^{(1)^H}\big]=0$. Therefore, the MSE of $\hat{\boldsymbol{H}}_{ae}$ can be simplified as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] =&\mathbb{E}[\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}] - \frac{4P_e}{x_1+2P_e}\mathbb{E}\Bigg[\big(\boldsymbol{H}_{ae}-\hat{\boldsymbol{H}}_{ae}^{(1)}\big)\hat{\boldsymbol{H}}_{ae}^{(2)^H}\Bigg] \\ &+\frac{4P_e^2}{(x_1+2P_e)^2}\mathbb{E}\Bigg[\left(\hat{\boldsymbol{H}}_{ae}^{(1)}-\hat{\boldsymbol{H}}_{ae}^{(2)}\right)\left(\hat{\boldsymbol{H}}_{ae}^{(1)}-\hat{\boldsymbol{H}}_{ae}^{(2)}\right)^{H}\Bigg].\end{aligned} \tag{4.59}$$

To compute the second term on the right hand side of the above equation, $\mathbb{E}\big[\big(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}^{(1)}\big)\hat{\boldsymbol{H}}_{ae}^{(2)^H}\big]$ can be simplified using the variance of the estimators $\hat{\boldsymbol{H}}_{ae}^{(1)}$ and $\hat{\boldsymbol{H}}_{ae}^{(2)}$ as:

$$\mathbb{E}\big[\big(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}^{(1)}\big)\hat{\boldsymbol{H}}_{ae}^{(2)^H}\big] = N_e\bigg(\sqrt{\frac{x_2}{P_e}}\sigma_{ae}^2 - gx_1\sqrt{\frac{x_2}{P_e}}(\sigma_{ae}^2 + c\sigma_{be})\bigg)\boldsymbol{I}_{N_a}, \tag{4.60}$$

where $g = \sigma_{ae}^2/(\sigma^2 + (\sigma_{ae}^2 + \sigma_{be}^2 c)x_1)$. Similarly, to compute the third term on the right hand side of (4.59), $\mathbb{E}\big[\big(\hat{\boldsymbol{H}}_{ae}^{(1)} - \hat{\boldsymbol{H}}_{ae}^{(2)}\big)\big(\hat{\boldsymbol{H}}_{ae}^{(1)} - \hat{\boldsymbol{H}}_{ae}^{(2)}\big)^H\big]$ can be simplified using the variance and covariance of $\hat{\boldsymbol{H}}_{ae}^{(1)}$ and $\hat{\boldsymbol{H}}_{ae}^{(2)}$ as:

$$\begin{aligned}\mathbb{E}\big[\big(\hat{\boldsymbol{H}}_{ae}^{(2)} - \hat{\boldsymbol{H}}_{ae}^{(1)}\big)\big(\hat{\boldsymbol{H}}_{ae}^{(2)} - \hat{\boldsymbol{H}}_{ae}^{(1)}\big)^H\big] &= \mathbb{E}\Big[\hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(2)^H} + \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(1)^H} - 2\hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\Big], \qquad (4.61)\\ &= N_e\bigg(\frac{x_2(\sigma_{ae}^2 + \sigma_{be}^2 c)}{P_e} + \frac{a\,(\sigma_{ae}^2 + \sigma_{be}^2) + \sigma^2}{2P_e}\\ &\quad + g^2x_1\big(x_1(\sigma_{ae}^2 + \sigma_{be}^2 c) + \sigma^2\big)\\ &\quad - 2gx_1\sqrt{\frac{x_2}{P_e}}(\sigma_{ae}^2 + \sigma_{be}^2 c)\bigg)\boldsymbol{I}_{N_a}. \qquad (4.62)\end{aligned}$$

Finally, substituting back in (4.59), the normalized MSE of $\hat{\boldsymbol{H}}_{ae}$ is given as:

$$\begin{aligned}\mathcal{E}_{ae}^{(2)} =& \mathcal{E}_{ae}^{(1)} + \frac{4P_e}{(x_1 + 2P_e)^2}\bigg(-(x_1 + 2P_e)\sqrt{\frac{x_2}{P_e}}\sigma_{ae}^2 + \frac{a(\sigma_{ae}^2 + \sigma_{be}^2) + \sigma^2}{2} + P_e g^2 x_1^2\sigma^2\\ &+ \big(\sigma_{ae}^2 + \sigma_{be}^2 c\big)\Big(gx_1^2\sqrt{\frac{x_2}{P_e}} + x_2 + P_e g^2 x_1^2\Big)\bigg). \qquad (4.63)\end{aligned}$$

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.

4.2.4 Power Allocation

Both legitimate nodes perform power allocation after estimating the variance of 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 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 legitimate node Bob. Possible lucrative locations for the eavesdropper are shown in Fig. 4.2, 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.

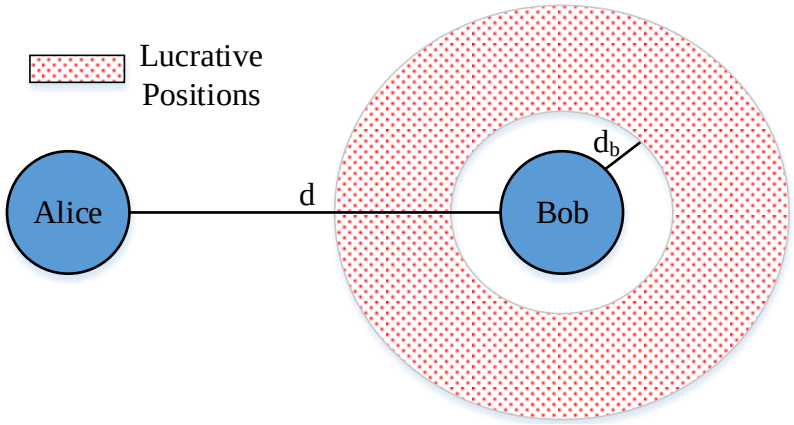


Fig. 4.2 Possible lucrative locations for any potential eavesdropper.

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. 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 (4.44) and at the eavesdropper by using $\mathcal{E}_{ae}^{(2)}$ as given in (4.63). In order to find the best possible location for eavesdropping, we consider the received signal to noise ratio (SNR) at the eavesdropper where achievable channel estimation is given by $\mathcal{E}_{ae}^{(2)}$. From [89, 98], the received SNR for MIMO system with orthogonal channel

estimation error is given as:

$$SNR_{ae} = \frac{P\left(\sigma_{ae}^2 - \mathcal{E}_{ae}^{(2)}\right)}{\sigma^2 + P\mathcal{E}_{ae}^{(2)}}, \tag{4.64}$$

where P denotes the power used for data transmission. The detailed derivation and explanation of the above relation can be found in [89, 98]. It can be seen from (4.64), that the received SNR is directly related to the channel variance and inversely to the channel estimation error, and in practical communication systems the channel variance is greater than the channel estimation error. Hence, the optimal eavesdropping location is closest to Bob, which is d_b away from Bob in the direction opposite to Alice to minimize the interference signal received from Alice.Based on the selected eavesdropper location and MSE, the power allocation tries to optimize the following condition:

$$\min_{\substack{\mathcal{E}_{ae}^{(2)} \geq \gamma \\ x_1 \leq P_{avg} \\ x_2 + a \leq P_{avg}}} \quad \mathcal{E}_{ab}^{(2)}, \tag{4.65}$$

where 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, and a, which satisfies the above conditions. If the value of γ is selected such that: $\nexists(x_1, x_2, a) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$, then it is decreased by a small value ϵ until $\exists(x_1, x_2, a) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$, to ensure that the value of γ is selected such that $\exists(x_1, x_2, a) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$.

4.2.5 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 3.2, where $N_a = 4$, $N_b = 4$, and $N_e = [4, 8]$ 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 [79], which implies that

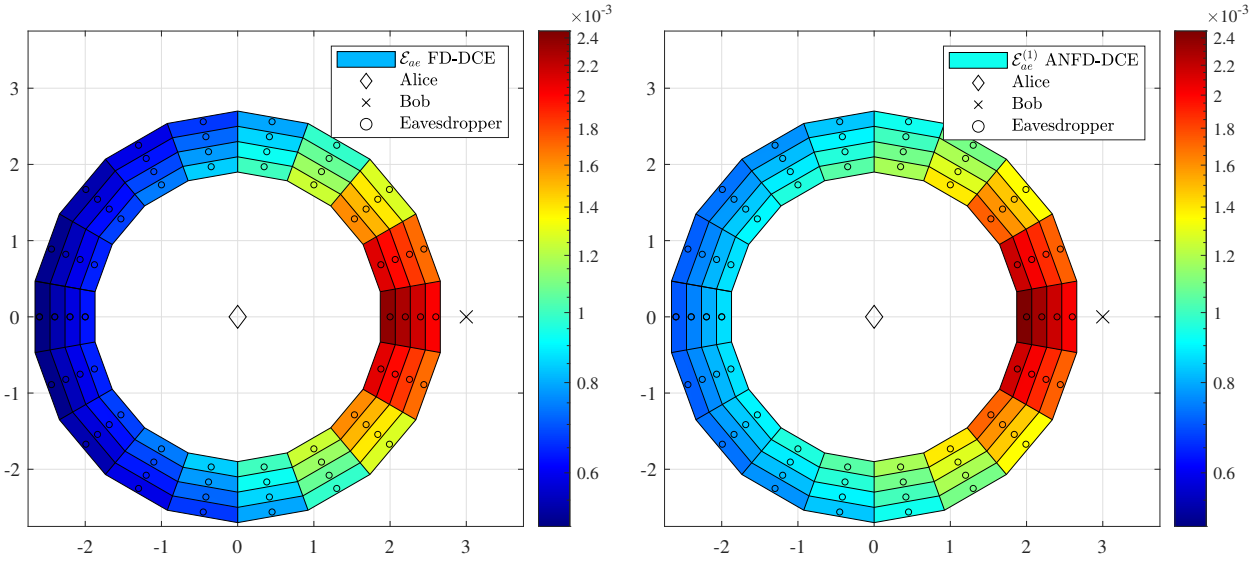
we have considered indoor office environment as our simulation scenario. The variance of self-interference channel is considered as given by experimental evaluations in [68]. As the estimation performance is highly dependent on the system noise denoted by σ^2, for the simulation analysis σ^2 is varied between 10^{-4} to 4×10^{-6} depending on the SNR. The SNR in all figures corresponds to the receive 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 16-ary QAM constellation.

Location-Based Performance 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 4.2.4, we have utilized $\gamma = 8.8 \times 10^{-4}$ for $d_b = 2m$.

Fig. 4.3 presents the MSE analysis of the FD-DCE scheme presented in the previous chapter along with the ANFD-DCE. Alice and Bob are located at (0,0) and (3,0) on the coordinate plane, respectively. The location of the eavesdropper is indicated by circles and the color of each tile indicates the MSE of the channel $\boldsymbol{H}_{ae}$ at the respective circled position. MSE for ANFD-DCE at the eavesdropper shown in Fig. 4.3b corresponds to the MSE achieved after the second stage using the LMMSE estimator denoted as $\mathcal{E}_{ae}^{(1)}$. MSE at the eavesdropper for ANFD-DCE after the AN aided channel estimation stage is omitted as it does not improve the system level BER performance, it will be further explained through the in-depth analysis presented in Section 4.2.5. The comparison of MSE performance at the eavesdropper for FD-DCE shown in Fig. 4.3a against ANFD-DCE shown in Fig. 4.3b shows that ANFD-DCE reduces the leakage of channel estimates to the eavesdropper as it moves away from the FD legitimate receiver Bob.

To indicate the effect of MSE on the system-level performance, we have presented the BER analysis for each location in Fig. 4.3. We have utilized a rate 1/2 Orthogonal Space-Time Block Codes (OSTBC) with four transmit antennas for the 16-QAM signal as given



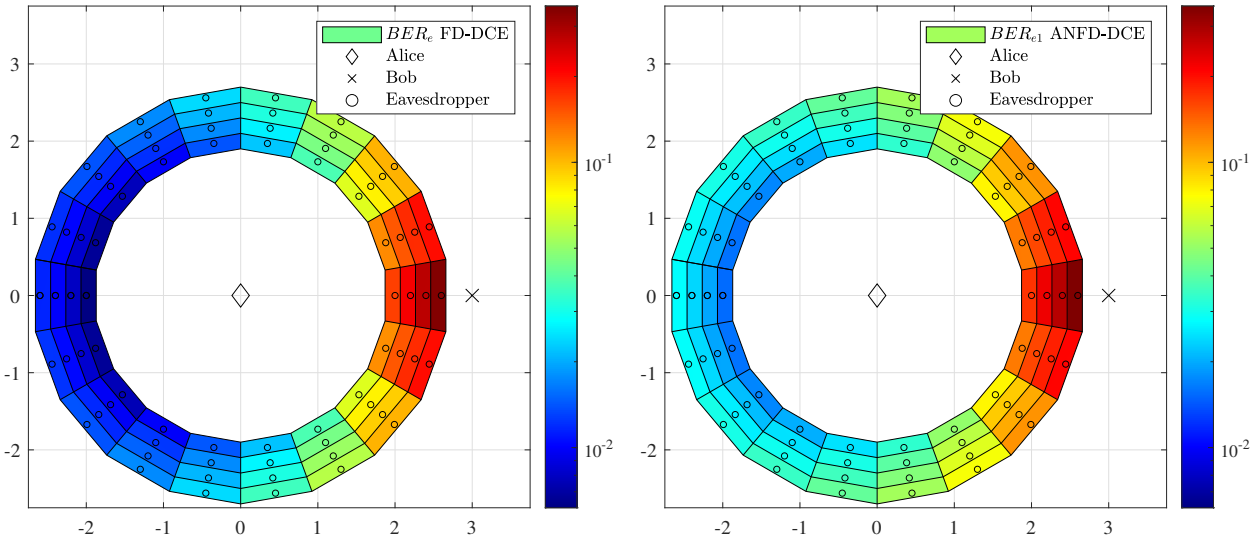
(a) FD-DCE (b) ANFD-DCE

Fig. 4.3 MSE at different locations of the eavesdropper for 16 dB SNR at the legitimate receiver, MSE for FD-DCE at Bob is: $\mathcal{E}_{ab} = 9.43 \times 10^{-5}$, and for ANFD-DCE is: $\mathcal{E}_{ab}^{(1)} = 1.12 \times 10^{-4}$.

in [100]. The receivers utilize the channel estimated in the previous stage to estimate the signal transmitted by Alice. Fig. 4.4 shows the BER achieved by the eavesdropper at different locations for FD-DCE and ANFD-DCE, where Fig. 4.4a shows the BER performance for FD-DCE and Fig. 4.4b shows BER for the channel estimated in the second stage for each location of the eavesdropper. BER analysis indicates that ANFD-DCE improves the secrecy of the communication by increasing the BER at the eavesdropper. This figure also indicates that BER at the eavesdropper improves as it moves away from Bob. However, 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. 4.3.

Performance 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 receive SNR at the eavesdropper as given in (4.64). The optimal location for eavesdropping on Alice is $d_b = 2m$ away from Alice in the opposite direction of the legitimate receiver to minimize the interference received during the channel



(a) FD-DCE (b) ANFD-DCE

Fig. 4.4 BER at different locations of the eavesdropper for 16 dB SNR at the legitimate receiver, BER at Bob for FD-DCE is: $BER_b = 2.12 \times 10^{-5}$, and for ANFD-DCE is: $BER_b = 10^{-4}$.

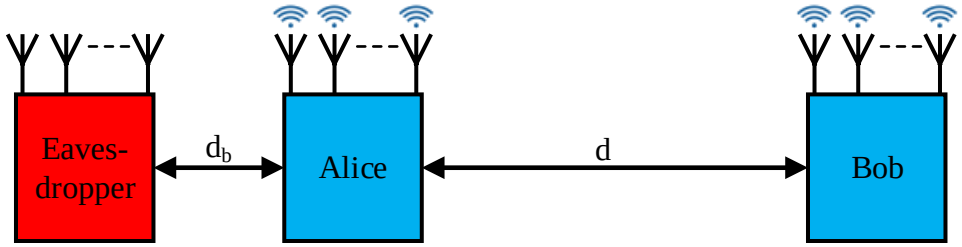


Fig. 4.5 Optimal location for any potential eavesdropper.

estimation stage as shown in Fig. 4.5. Therefore, the distance between Bob and the eavesdropper is considered to 5 meters as we have considered $d = 3m$. For the considered position we have provided MSE and BER comparisons with the FD-DCE techniques.

Fig. 4.6 shows the average power allocation to the training signals x_1, and x_2, and the AN a, where the horizontal axis represents the SNR at the legitimate receiver in dB, and the vertical axis corresponds to power in dBm. We have considered the maximum transmit power to be $30dBm$. In FD-DCE, each legitimate node utilizes all the available power to

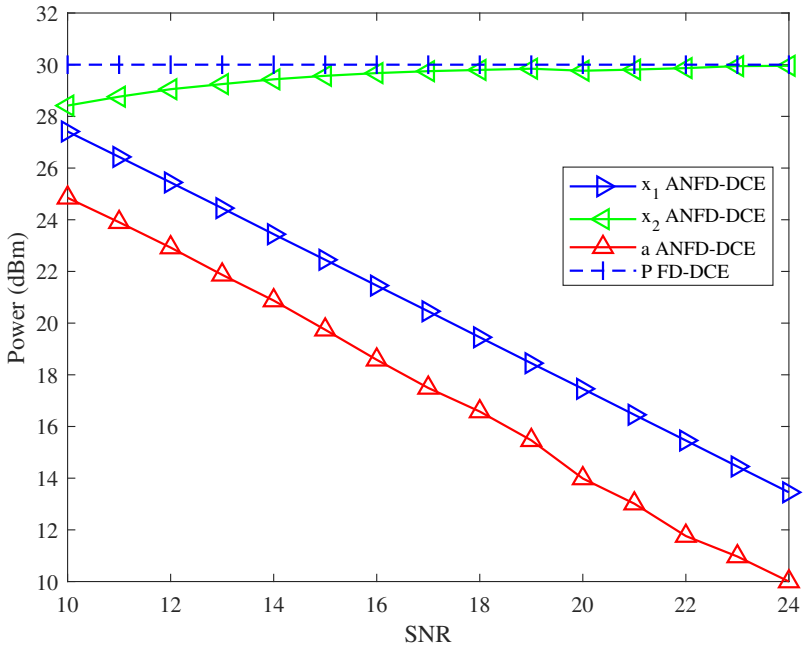


Fig. 4.6 Average power allocation for training signals and AN for legitimate nodes, while $N_a = N_b = 4$.

transmit the training signal. The results indicate that the power allocation to the rough channel estimation stage x_1 varies as the SNR increases to ensure that the MSE at the eavesdropper can be maintained above the threshold γ. The power allocated to AN also decreases as it requires less AN to maintain the threshold as the MSE at the eavesdropper in the rough channel estimation stage increases. The power allocated to x_2 is close to the maximum transmit power, to improve the channel estimates at the legitimate users as the AN ensures the equivocation at the eavesdropper.

The achievable average secrecy capacity for the proposed ANFD-DCE, along with the comparison to FD-DCE is presented in Fig. 4.7, using the relations of secrecy capacity derived in Section 3.4.2, as the LMMSE estimator is utilized by the eavesdropper in the rough channel estimation stage. We have conducted simulation analysis for the different number of antennas at the eavesdropper $N_e = [4, 8]$. These results indicate that the proposed ANFD-DCE improves the secrecy capacity as compared to the FD-DCE.

The MSE analysis for the ANFD-DCE along with the comparison to the FD-DCE is presented in Fig. 4.8, where the vertical axis corresponds to MSE and the horizontal axis indicates the received SNR at the legitimate node. For Fig. 4.8, we have considered equal

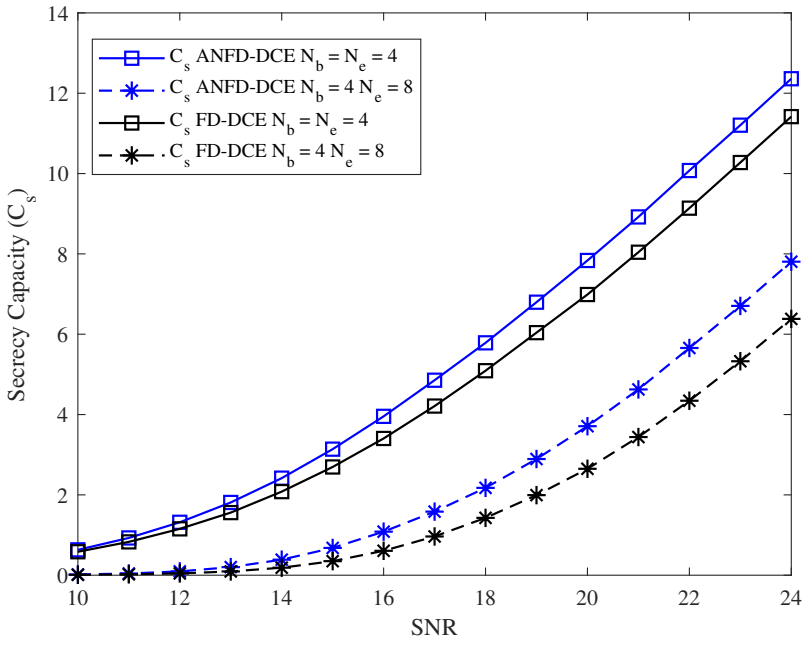


Fig. 4.7 Average Secrecy Capacity ANFD-DCE and FD-DCE, while $N_a = N_b = 4$.

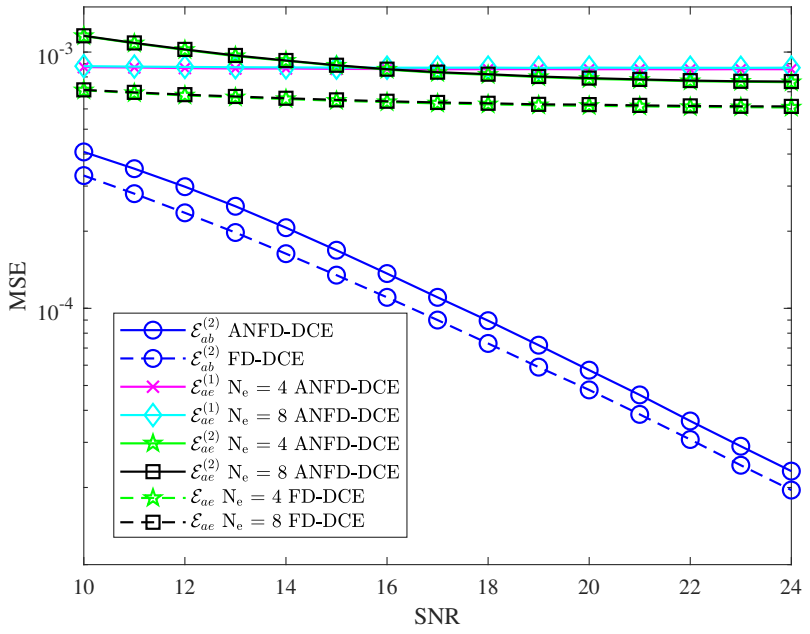


Fig. 4.8 MSE for ANFD-DCE and FD-DCE, while $N_a = N_b = 4$, and $N_e = [4, 8]$.

number of antennas at the legitimate nodes such that $N_a = N_b = 4$. These results indicate that the proposed AN assisted FD-DCE maintains higher MSE at the eavesdropper as compared to the FD-DCE technique. Meanwhile, MSE of the legitimate channel $\boldsymbol{H}_{ab}$ is higher for the proposed ANFD-DCE as compared to the FD-DCE, as the use of AN also affects the estimation performance for the legitimate channel. Fig. 4.8 shows that increasing the number of eavesdropping antennas N_e does not affect the MSE at the eavesdropper. We have presented MSE at the eavesdropper after the second stage $\mathcal{E}_{ae}^{(1)}$, and the third stage $\mathcal{E}_{ae}^{(2)}$. The comparison of $\mathcal{E}_{ae}^{(1)}$ to $\mathcal{E}_{ae}^{(2)}$ indicates that $\mathcal{E}_{ae}^{(1)}$ becomes less than $\mathcal{E}_{ae}^{(2)}$ as the second stage improves as the variance of AN decreases with increase in SNR.

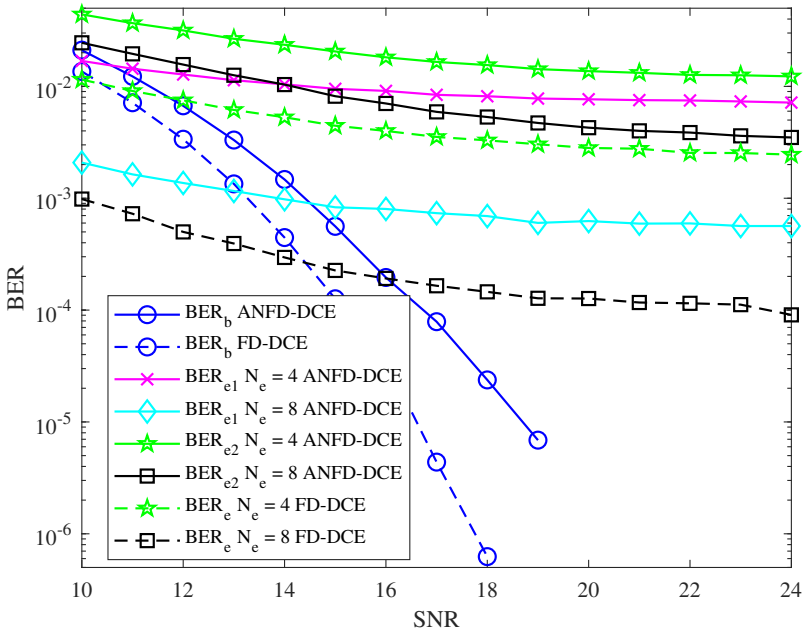


Fig. 4.9 BER for ANFD-DCE and FD-DCE, while $N_a = N_b = 4$.

In Fig. 4.9, we have shown the BER achieved at all nodes on the vertical axis against the received SNR at the legitimate node on the horizontal axis. The BER analysis clearly illustrates that the proposed ANFD-DCE improves the secrecy achieved as compared to the FD-DCE. For ANFD-DCE, we have shown the corresponding BER for the channel estimated in the second stage denoted as BER_{e1}, and for the third stage denoted as BER_{e2}. The comparison of BER_{e1} to BER_{e2} shows that the BER after the second is lower than the third stage, even though as shown in Fig. 4.8 the MSE for the channel estimated in the third

stage less than the second stage at high SNR. The superior BER performance of the channel estimated in the second stage than the third stage is due to the superior performance of the LMMSE estimator as compared to the LS estimator [103].

4.3 Double Noise aided Full-Duplex Discriminatory Channel Estimation Technique

This section presents an improved double artificial noise aided full-duplex (DANFD) discriminatory channel estimation (DCE) by using artificial noise in the rough channel estimation stage in addition to the artificial noise aided channel estimation stage. The proposed DANFD-DCE exploits the full-duplex transmission to cancel the artificial noise in the second stage as contrast to the eavesdropper as the artificial noise signal is not known at the eavesdropper. The DANFD-DCE also comprises three stages, where the SI channel estimation stage is similar to the ANFD-DCE as mentioned in Section 4.2.1. Like the ANFD-DCE, the eavesdropper and the respective legitimate nodes estimate their respective channel variances in the SI channel estimation stage. The following channel estimation stages are described below.

4.3.1 Second Stage: Artificial Noise Aided Rough Channel Estimation

The second stage acquires a rough estimate of the main channel ($\boldsymbol{H}_{ab}$ and $\boldsymbol{H}_{ba}$) while causing equivocation at the eavesdropper with the transmission of the AN signal.

At Bob

As compared to the ANFD-DCE, Bob transmits a globally known training signal along with a random artificial noise signal in the second stage. The random artificial noise signal can be cancelled at full-duplex legitimate nodes as the transmit and receive radio frequency chains are on the same device, whereas the eavesdropper receives the random artificial noise signal from both the legitimate nodes. The signal transmitted by Bob is given as:

$$\boldsymbol{X}_b^{(1)} = \sqrt{x_1}\boldsymbol{V}_b^{(1)} + \boldsymbol{B}, \tag{4.66}$$

where $\boldsymbol{V}_b^{(1)}$ is the pilot signal, and $\boldsymbol{B}$ is the random artificial noise signal drawn from $\mathcal{N}(\mathbf{0}, \frac{a_1}{N_b}\boldsymbol{I}_{T_2})$. 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 DANFD-DCE. T_2 is the length of the training signal which is kept equal to $T_2 = max(N_a, N_b)$, to ensure that the reception at the eavesdropper is superimposed by two signals. Similarly, the signal transmitted by Alice is given as: $\boldsymbol{X}_a^{(1)} = \sqrt{x_1}\boldsymbol{V}_a^{(1)} + \boldsymbol{A}$, where $\sqrt{x_1}\boldsymbol{V}_a^{(1)}$ is the pilot signal with variance x_1 and $\boldsymbol{A}$ is the AN signal drawn from $\mathcal{N}(\mathbf{0}, \frac{a_1}{N_a}\boldsymbol{I}_{T_2})$. The signal received at Bob after digital SI cancellation during the second stage is given as:

$$\mathbf{Y}_b^{(1)} = \boldsymbol{X}_a^{(1)}\boldsymbol{H}_{ab} + \boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}, \tag{4.67}$$

$$= \big(\sqrt{x_1}\boldsymbol{V}_a^{(1)} + \boldsymbol{A}\big)\boldsymbol{H}_{ab} + \big(\sqrt{x_1}\boldsymbol{V}_b^{(1)} + \boldsymbol{B}\big)\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}, \tag{4.68}$$

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 [92]:

$$\hat{\boldsymbol{H}}_{ab}^{(1)} = \boldsymbol{R}_{\boldsymbol{H}_{ab}}\sqrt{x_1}\mathbf{V}_a^{(1)^H}\left(x_1\mathbf{V}_a^{(1)}\boldsymbol{R}_{\boldsymbol{H}_{ab}}\mathbf{V}_a^{(1)^H} + \boldsymbol{R}_{\boldsymbol{W}_1}\right)^{-1}\mathbf{Y}_b^{(1)}, \tag{4.69}$$

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:

$$\boldsymbol{R}_{\boldsymbol{W}_1} = \mathbb{E}\left[\left(\boldsymbol{A}\boldsymbol{H}_{ab} + \boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}\right)\left(\boldsymbol{A}\boldsymbol{H}_{ab} + \boldsymbol{X}_b^{(1)}\Delta\hat{\boldsymbol{H}}_{bb} + \boldsymbol{W}_b^{(1)}\right)^H\right], \tag{4.70}$$

$$= N_b\left(a_1\sigma_{ab}^2 + \mathcal{E}_{bb}\big(x_1c + a_1\big) + \sigma^2\right)\boldsymbol{I}_{T_2}, \tag{4.71}$$

where $c = N_b/T_2$. Substituting $\boldsymbol{R}_{\boldsymbol{W}_1}$ in (4.69), the LMMSE estimator can be simplified as:

$$\hat{\boldsymbol{H}}_{ab}^{(1)} = \frac{\sigma_{ab}^2}{\sigma_{ab}^2(x_1 + a_1) + \mathcal{E}_{bb}\big(x_1c + a_1\big) + \sigma^2}\sqrt{x_1}\mathbf{V}_b^{(1)^H}\mathbf{Y}_b^{(1)}. \tag{4.72}$$

MSE for $\hat{\boldsymbol{H}}_{ab}^{(1)}$ is given as:

$$\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{ab}^{(1)}\Delta\hat{\boldsymbol{H}}_{ab}^{(1)^H}\right) = \left(\boldsymbol{R}_{\boldsymbol{H}_{ab}}^{-1} + \sqrt{x_1}\mathbf{V}_a^{(1)^H}\boldsymbol{R}_{\boldsymbol{W}_1}^{-1}\sqrt{x_1}\mathbf{V}_a^{(1)}\right)^{-1} \tag{4.73}$$

$$= N_b\left(\frac{1}{\sigma_{ab}^2}\boldsymbol{I}_{N_a} + \frac{x_1}{a_1\sigma_{ab}^2 + \mathcal{E}_{bb}\big(x_1c + a_1\big) + \sigma^2}\mathbf{V}_a^{(1)^H}\mathbf{V}_a^{(1)}\right)^{-1}, \tag{4.74}$$

Therefore, normalized MSE of $\hat{\boldsymbol{H}}_{ab}^{(1)}$ is given as:

$$\mathcal{E}_{ab}^{(1)} = \left(\frac{1}{\sigma_{ab}^2} + \frac{x_1}{a_1\sigma_{ab}^2 + \mathcal{E}_{bb}\big(x_1c + a_1\big) + \sigma^2}\right)^{-1} \tag{4.75}$$

At the Eavesdropper

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

$$\boldsymbol{Y}_e^{(1)} = \boldsymbol{X}_a^{(1)}\boldsymbol{H}_{ae} + \boldsymbol{X}_b^{(1)}\boldsymbol{H}_{be} + \boldsymbol{W}_e^{(1)}, \tag{4.76}$$

$$= (\sqrt{x_1}\boldsymbol{V}_a^{(1)} + \boldsymbol{A})\boldsymbol{H}_{ae} + (\sqrt{x_1}\boldsymbol{V}_a^{(1)} + \boldsymbol{B})\boldsymbol{H}_{be} + \boldsymbol{W}_e^{(1)}, \tag{4.77}$$

where $\boldsymbol{W}_e^{(1)}$ denotes the ZMCSWGN with variance σ^2. 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 is unable to get a estimate of x_1 or a_1. Therefore, 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:

$$\hat{\boldsymbol{H}}_{ae}^{(1)} = \left[\sqrt{P_1}\boldsymbol{V}_a^{(1)}\right]^{\dagger}\boldsymbol{Y}_e^{(1)}, \tag{4.78}$$

$$= \boldsymbol{V}_1^{\dagger}\boldsymbol{Y}_e^{(1)}, \tag{4.79}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}^{(1)}. \tag{4.80}$$

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

$$\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}\right) = \mathbb{E}\left[\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}^{(1)}\right)\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}^{(1)}\right)^H\right] \tag{4.81}$$

$$= \mathbb{E}\Big[\left(\boldsymbol{H}_{ae} - \boldsymbol{V}_1^{\dagger}\boldsymbol{Y}_e^{(1)}\right)\left(\boldsymbol{H}_{ae} - \boldsymbol{V}_1^{\dagger}\boldsymbol{Y}_e^{(1)}\right)^H\Big] \tag{4.82}$$

$$= \mathbb{E}\left[\boldsymbol{H}_{ae}\boldsymbol{H}_{ae}^H - 2\boldsymbol{H}_{ae}\boldsymbol{Y}_e^{(1)^H}\boldsymbol{V}_1^{\dagger^H} + \boldsymbol{V}_1^{\dagger}\boldsymbol{Y}_e^{(1)}\boldsymbol{Y}_e^{(1)^H}\boldsymbol{V}_1^{\dagger^H}\right] \tag{4.83}$$

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

$$\mathcal{E}_{ae}^{(1)} = \frac{\mathrm{Tr}\left[\mathbb{E}\left(\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}\right)\right]}{N_b N_e},$$

$$= \sigma_{ae}^2\left(1 - \sqrt{\frac{x_1}{P_1}}\right)^2 + \frac{a_1\sigma_{ae}^2}{P_1} + \frac{\sigma_{be}^2\left(\frac{x_1 N_b}{T_2} + a_1\right)}{P_1} + \frac{\sigma^2}{P_1}. \tag{4.84}$$

4.3.2 Third Stage: Artificial Noise Channel Estimation

The third stage for DANFD-DCE is similar to ANFD-DCE, where AN orthogonal to the main channel is transmitted along with the pilot signals using in-band FD transmissions from both the legitimate nodes. To design an orthogonal AN signal, we have utilized the Algorithm 1 given in the previous section, where the channel is partitioned into multiple parts to achieve orthogonal AN. For notational simplicity, we will consider $N_a = N_b$, and the estimation of $\boldsymbol{H}_{ab1}$.

At Bob

The signal received at Bob after digital SI cancellation during the third stage is given as:

$$\mathbf{Y}_b^{(2)} = \left(\sqrt{x_2}\boldsymbol{V}_a^{(2)} + \mathbf{A}_1\mathbf{N}_{ab1}^H\right)\mathbf{H}_{ab1} + \left(\sqrt{x_2}\boldsymbol{V}_b^{(2)} + \mathbf{B}_1\mathbf{N}_{ba1}^H\right)\Delta\hat{\mathbf{H}}_{bb1} + \mathbf{W}_b^{(2)}. \tag{4.85}$$

Therefore, the signals received at Bob during both channel estimation stages are given as:

$$\begin{aligned}\mathbf{Y}_2 =& \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_a^{(1)}\\ \sqrt{x_2}\boldsymbol{V}_a^{(2)}\end{bmatrix}\mathbf{H}_{ab1} + \begin{bmatrix}\sqrt{x_1}\boldsymbol{V}_b^{(1)}\\ \sqrt{x_2}\boldsymbol{V}_b^{(2)}\end{bmatrix}\Delta\hat{\boldsymbol{H}}_{bb1}\\ &+\begin{bmatrix}\boldsymbol{A}\boldsymbol{H}_{ab1} + \boldsymbol{B}\Delta\hat{\boldsymbol{H}}_{bb1} + \mathbf{W}_b^{(1)}\\ \mathbf{A}_1\mathbf{N}_{ab1}^H\Delta\hat{\mathbf{H}}_{ab1}^{(1)} + \mathbf{B}_1\mathbf{N}_{ba1}^H\Delta\hat{\boldsymbol{H}}_{bb1} + \mathbf{W}_{b,1}^{(2)}\end{bmatrix}, \qquad (4.86)\\ =&\mathbf{X}_a\mathbf{H}_{ab1} + \mathbf{X}_b\Delta\hat{\mathbf{H}}_{bb1} + \mathbf{W}_b \qquad (4.87)\end{aligned}$$

LMMSE estimator is utilized to estimate $\mathbf{H}_{ab1}$ as given in (4.31):

$$\hat{\mathbf{H}}_{ab1}^{(2)} = \sigma_{ab}^2 N_{b1}\left(\mathbf{I}_{N_b} + N_{b1}(\sigma_{ab}^2+\mathcal{E}_{bb})\mathbf{X}_b^H\mathbf{R}_{\boldsymbol{W}_b}^{-1}\mathbf{X}_b\right)^{-1}\mathbf{X}_b^H\mathbf{R}_{\boldsymbol{W}_b}^{-1}\boldsymbol{Y}_2, \qquad (4.88)$$

where $\mathbf{R}_{\boldsymbol{W}_b}$ corresponds to the covariance of $\boldsymbol{W}_b$, which can be calculated as:

$$\begin{aligned}\mathbf{R}_{\boldsymbol{W}_b} =& \mathbb{E}\left[\boldsymbol{W}_b\boldsymbol{W}_b^H\right],\\ =&\begin{bmatrix}N_{b1}\Big(\sigma^2 + a_1\big(\mathcal{E}_{bb}+\sigma_{ab}^2\big)\Big)\mathbf{I}_{T_1} & \mathbf{0}\\ \mathbf{0} & N_{b1}\left(\sigma^2 + a_2(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb})\right)\mathbf{I}_{T_2}\end{bmatrix}. \qquad (4.89)\end{aligned}$$

Finally, substituting $\mathbf{R}_{\boldsymbol{W}_b}$ in $\hat{\mathbf{H}}_{ab1}^{(2)}$ we get:

$$\begin{aligned}\hat{\mathbf{H}}_{ab1}^{(2)} =& \frac{\sigma_{ab}^2}{1+(\sigma_{ab}^2+\mathcal{E}_{bb})\Big(\frac{x_1}{\sigma^2+a_1\left(\mathcal{E}_{bb}+\sigma_{ab}^2\right)} + \frac{x_2}{\sigma^2+a_2\left(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb}\right)}\Big)}\\ &\begin{bmatrix}\dfrac{\mathbf{X}_b^{(1)^H}}{\sigma^2+a_1\big(\mathcal{E}_{bb}+\sigma_{ab}^2\big)} & \dfrac{\mathbf{X}_b^{(2)^H}}{\sigma^2+a_2\big(\mathcal{E}_{ab}^{(1)}+\mathcal{E}_{bb}\big)}\end{bmatrix}\boldsymbol{Y}_2, \qquad (4.90)\\ \triangleq& \boldsymbol{H}_{ab1} + \Delta\hat{\mathbf{H}}_{ab1}^{(2)}. \qquad (4.91)\end{aligned}$$

Using the derivation of MSE given in the previous Section 4.2, MSE for $\hat{\mathbf{H}}_{ab1}^{(2)}$ using DANFD-DCE is given as:

$$\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}(\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)})^H\right] = \left(\boldsymbol{R}_{\boldsymbol{H}_{ab1}}^{-1} + \left(\frac{x_1}{mN_{b1}} + \frac{x_2}{kN_{b1}}\right)\left(\boldsymbol{I} + \mathcal{E}_{bb}\left(\frac{x_1}{m} + \frac{x_2}{k}\right)\boldsymbol{I}\right)^{-1}\right)^{-1}, \quad (4.92)$$

$$= N_{b1}\left(\frac{1}{\sigma_{ab}^2} + \left(\frac{mk}{x_1k + x_2m} + \mathcal{E}_{bb}\right)^{-1}\right)^{-1}\boldsymbol{I}_{N_a}, \quad (4.93)$$

where $k = \sigma^2 + a_2\left(\mathcal{E}_{ab}^{(1)} + \mathcal{E}_{bb}\right)$, $m = \sigma^2 + a_1\left(\mathcal{E}_{bb} + \sigma_{ab}^2\right)$, and $\boldsymbol{R}_{\boldsymbol{H}_{ab1}} = N_{b1}\sigma_{ab}^2\boldsymbol{I}_{N_a}$. Therefore, after performing algebraic simplifications the normalized MSE of $\hat{\mathbf{H}}_{ab1}^{(2)}$ is given as:

$$\mathcal{E}_{ab}^{(2)} = \frac{\mathrm{Tr}[\mathbb{E}\{\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)}(\Delta\hat{\boldsymbol{H}}_{ab1}^{(2)})^H\}]}{N_aN_{b1}}, \quad (4.94)$$

$$= \left(\frac{1}{\mathcal{E}_{ab}^{(1)}} + \frac{m^2x_2}{(m + x_1\mathcal{E}_{bb})\left[x_2m\mathcal{E}_{bb} + (m + x_1\mathcal{E}_{bb})\,k\right]}\right)^{-1}. \quad (4.95)$$

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

At the eavesdropper

The signals received at the eavesdropper during the AN assisted channel estimation stage for DANFD-DCE are:

$$\boldsymbol{Y}_e^{(2)} = \begin{bmatrix}\boldsymbol{X}_{a,1}^{(2)}\\ \boldsymbol{X}_{a,2}^{(2)}\end{bmatrix}\boldsymbol{H}_{ae} + \begin{bmatrix}\boldsymbol{X}_{b,1}^{(2)}\\ \boldsymbol{X}_{b,2}^{(2)}\end{bmatrix}\boldsymbol{H}_{be} + \begin{bmatrix}\boldsymbol{W}_{e,1}^{(2)}\\ \boldsymbol{W}_{e,2}^{(2)}\end{bmatrix}, \quad (4.96)$$

$$= \begin{bmatrix}\sqrt{x_2}\boldsymbol{V}_a^{(2)}\\ \sqrt{x_2}\boldsymbol{V}_a^{(2)}\end{bmatrix}\boldsymbol{H}_{ae} + \begin{bmatrix}\sqrt{x_2}\boldsymbol{V}_b^{(2)}\\ \sqrt{x_2}\boldsymbol{V}_b^{(2)}\end{bmatrix}\boldsymbol{H}_{be} + \begin{bmatrix}\boldsymbol{A}_1\boldsymbol{N}_{ab1}^H\boldsymbol{H}_{ae} + \boldsymbol{B}_1\boldsymbol{N}_{ba1}^H\boldsymbol{H}_{be} + \boldsymbol{W}_{e,1}^{(2)}\\ \boldsymbol{A}_2\boldsymbol{N}_{ab2}^H\boldsymbol{H}_{ae} + \boldsymbol{B}_2\boldsymbol{N}_{ba2}^H\boldsymbol{H}_{be} + \boldsymbol{W}_{e,2}^{(2)}\end{bmatrix}, \quad (4.97)$$

$$= \boldsymbol{X}_a\boldsymbol{H}_{ae} + \boldsymbol{X}_b\boldsymbol{H}_{be} + \boldsymbol{W}_e^{(2)}, \quad (4.98)$$

where $\boldsymbol{V}_a^{(2)}$ and $\boldsymbol{V}_b^{(2)}$ 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 AN assisted training stage for the estimation of $\boldsymbol{H}_{ae}$, the eavesdropper can utilize LS estimation by exploiting the global pilot sequences and the sums

of the total transmitted power as:

$$\hat{\boldsymbol{H}}_{ae}^{(2)} = \begin{bmatrix} \sqrt{P_2}\boldsymbol{V}_a^{(2)} \\ \sqrt{P_2}\boldsymbol{V}_a^{(2)} \end{bmatrix}^{\dagger} \boldsymbol{Y}_e^{(2)}, \tag{4.99}$$

$$= \boldsymbol{V}_2^{\dagger}\boldsymbol{Y}_e^{(2)}, \tag{4.100}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}^{(2)}, \tag{4.101}$$

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:

$$\hat{\boldsymbol{H}}_{ae} = \begin{bmatrix} \sqrt{P_1}\boldsymbol{V}_a^{(1)} \\ \sqrt{P_2}\boldsymbol{V}_a^{(2)} \\ \sqrt{P_2}\boldsymbol{V}_a^{(2)} \end{bmatrix}^{\dagger} \begin{bmatrix} \boldsymbol{Y}_e^{(1)} \\ \boldsymbol{Y}_e^{(2)} \end{bmatrix}, \tag{4.102}$$

$$= \hat{\boldsymbol{H}}_{ae}^{(1)} + \frac{2P_2}{P_1 + 2P_2}\left(\hat{\boldsymbol{H}}_{ae}^{(2)} - \hat{\boldsymbol{H}}_{ae}^{(1)}\right), \tag{4.103}$$

$$\triangleq \boldsymbol{H}_{ae} + \Delta\hat{\boldsymbol{H}}_{ae}. \tag{4.104}$$

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

$$\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] = \mathbb{E}\left[\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}\right)\left(\boldsymbol{H}_{ae} - \hat{\boldsymbol{H}}_{ae}\right)^{H}\right]. \tag{4.105}$$

The above equation can be computed using the similar steps as mentioned for ANFD-DCE as:

$$\begin{aligned}\mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}\Delta\hat{\boldsymbol{H}}_{ae}^{H}\right] = \mathbb{E}\left[\Delta\hat{\boldsymbol{H}}_{ae}^{(1)}\Delta\hat{\boldsymbol{H}}_{ae}^{(1)^H}\right] - \frac{4P_2}{P_1 + 2P_2}\mathbb{E}\Big[\boldsymbol{H}_{ae}\hat{\boldsymbol{H}}_{ae}^{(2)^H} \\ - \boldsymbol{H}_{ae}\hat{\boldsymbol{H}}_{ae}^{(1)^H} - \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(2)^H} + \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\Big] - \\ \frac{4P_2^2}{(P_1 + 2P_2)^2}\mathbb{E}\Big[\hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(2)^H} - \hat{\boldsymbol{H}}_{ae}^{(2)}\hat{\boldsymbol{H}}_{ae}^{(1)^H} \\ - \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(2)^H} + \hat{\boldsymbol{H}}_{ae}^{(1)}\hat{\boldsymbol{H}}_{ae}^{(1)^H}\Big].\end{aligned} \tag{4.106}$$

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

$$\begin{aligned}\mathcal{E}_{ae}^{(2)} =&\mathcal{E}_{ae}^{(1)} + \frac{4P_2}{(P_1+2P_2)^2}\Bigg(\frac{\sigma^2}{2} + \frac{a_2\left(\sigma_{ae}^2+\sigma_{be}^2\right)}{2} - \sigma_{ae}^2\Big(\sqrt{\frac{x_2}{P_2}} - \sqrt{\frac{x_1}{P_1}}\Big)(P_1+2P_2)\\ &+ P_1\sqrt{\frac{x_1x_2}{P_1P_2}}\left(\sigma_{ae}^2+c\sigma_{be}^2\right) - \frac{P_1+P_2}{P_1}\left(x_1\left(\sigma_{ae}^2+c\sigma_{be}^2\right) + a_1(\sigma_{ae}^2+\sigma_{be}^2) + \sigma^2\right)\\ &+ x_2\left(\sigma_{ae}^2+c\sigma_{be}^2\right)\Bigg). \end{aligned} \tag{4.107}$$

4.3.3 Power Allocation for DANFD-DCE

Power allocation is performed after the first stage (SI channel estimation stage) at each legitimate node. As mentioned for the ANFD-DCE, each node assumes that the estimated variance and the power allocation algorithms are the same at the other node. The optimal location of the eavesdropping is considered as mentioned in Section 4.2.4. Therefore, for DANFD-DCE the power allocation tries to optimize the following condition:

$$\min_{\substack{\mathcal{E}_{ae}^{(2)}\geq\gamma\\ x_1+a_1\leq P_{avg}\\ x_2+a_2\leq P_{avg}}} \quad \mathcal{E}_{ab}^{(2)}, \tag{4.108}$$

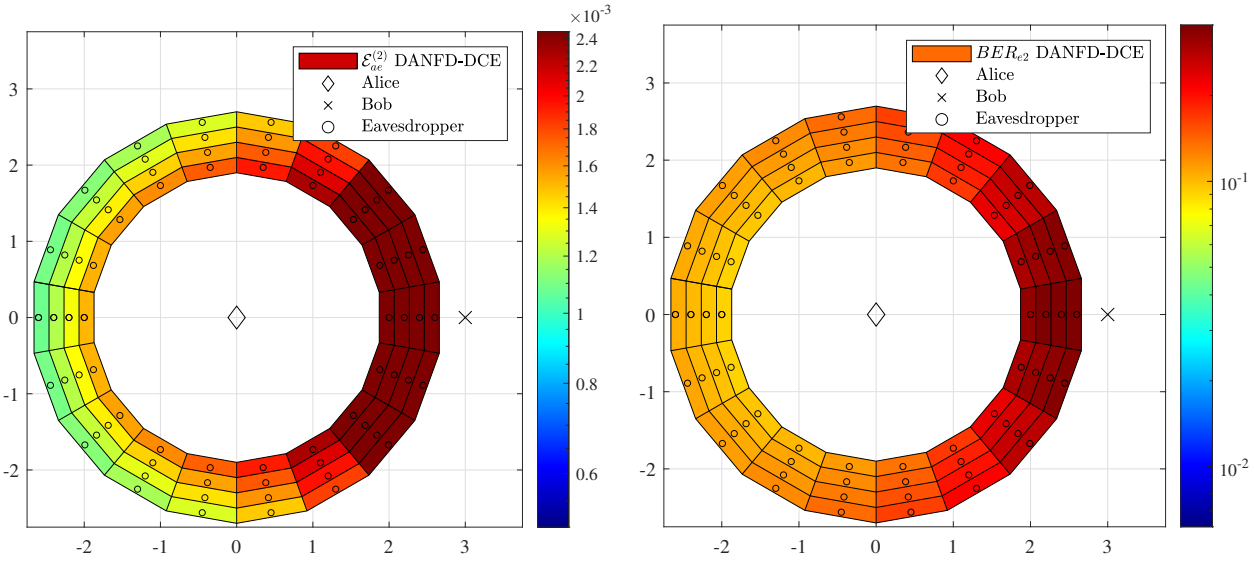
where $\mathcal{E}_{ae}^{(2)}$ and $\mathcal{E}_{ab}^{(2)}$ for DANFD-DCE are given in (4.107) and (4.95), respectively. Brute-force search algorithm is used to get the values of x_1, x_2, a_1 and a_2, which satisfies the above conditions. The value of γ is selected such that: $\exists(x_1,x_2,a) \mid \mathcal{E}_{ae}^{(2)} \geq \gamma$, as mentioned for ANFD-DCE.

4.3.4 Simulation Analysis and Results

In this section, simulation analysis is presented to demonstrate the robust secrecy performance achieved by the proposed DANFD-DCE scheme along with the comparisons to the ANFD and FD-DCE techniques. We have considered the MIMO wireless system as mentioned in Section 3.2, where $N_a = 4$, $N_b = [3,4,6]$, and $N_e = [4,8,12]$ at Alice, Bob, and the eavesdropper, respectively.

Location-Based Performance Analysis

First, we have considered the same boundary around Alice $d_b = 2m$ and distance between Alice-Bob $d = 3m$ as for ANFD-DCE to provide a performance comparison to the ANFD and FD-DCE techniques. For the power allocation algorithm given in Section 4.3.3, we have utilized $\gamma = 1.5 \times 10^{-3}$ for $d_b = 2m$. Fig. 4.10 shows the performance of the DANFD-DCE, where Fig. 4.10a indicates the MSE, and Fig. 4.10b shows the BER for each location of the eavesdropper.

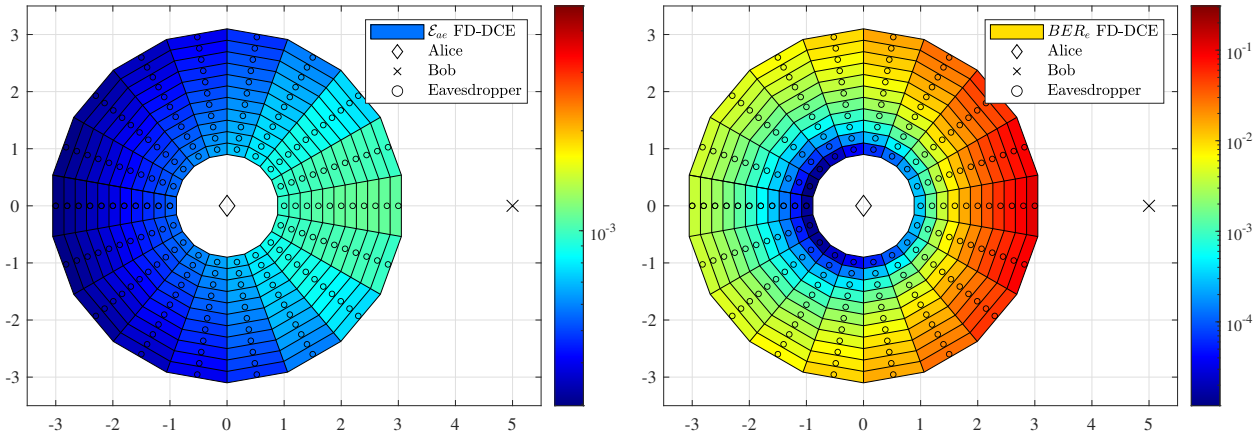


(a) MSE (b) BER

Fig. 4.10 Performance of DANFD-DCE at different locations of the eavesdropper for 16 dB SNR at the legitimate receiver, MSE for DANFD-DCE at Bob is: $\mathcal{E}_{ab}^{(2)} = 1.4 \times 10^{-4}$, and BER at Bob is: $BER_b = 2.97 \times 10^{-4}$.

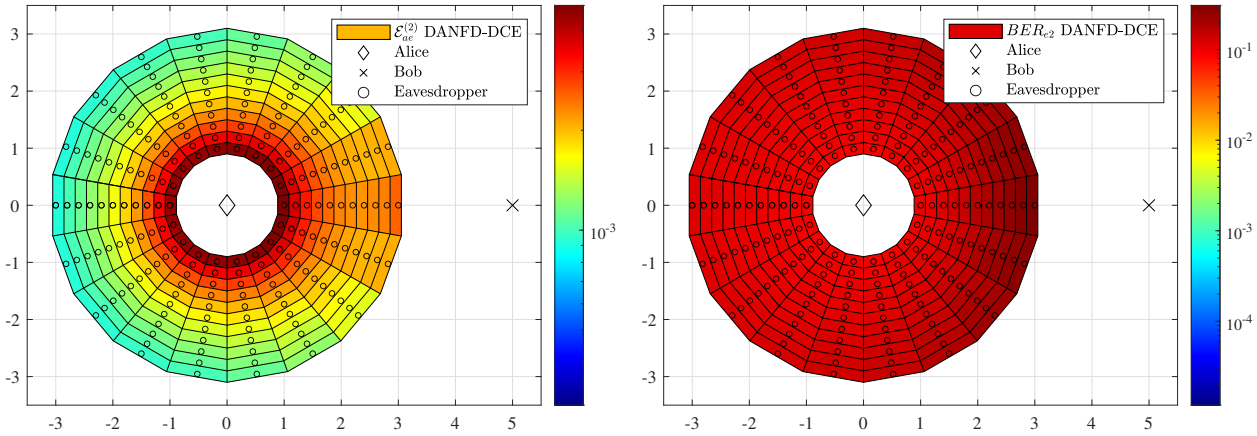
Fig. 4.10 indicates that for the given scenario, the DANFD-DCE achieves robust security because even for the optimal eavesdropping locations the BER is close to 0.1. Fig. 4.10a also shows that the MSE for the eavesdropper improves as it moves away from Bob however the BER in Fig. 4.10b shows that the eavesdropper can not decode the transmitted message robustly. We have considered the MSE and BER 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.

We have also considered $d_b = 1m$ in Fig. 4.11 and Fig. 4.12, to further analyze the effect of



(a) MSE (b) BER

Fig. 4.11 Performance of FD-DCE at different locations of the eavesdropper for 17 dB SNR at the legitimate receiver, MSE for FD-DCE at Bob is: $\mathcal{E}_{ab}^{(2)} = 2.4 \times 10^{-5}$, and BER at Bob is less than 10^{-5}.



(a) MSE (b) BER

Fig. 4.12 Performance of DANFD-DCE at different locations of the eavesdropper for 17 dB SNR at the legitimate receiver, MSE for DANFD-DCE at Bob is: $\mathcal{E}_{ab}^{(2)} = 5.15 \times 10^{-5}$, and BER at Bob is: $BER_b = 7.8 \times 10^{-5}$.

the boundary around Alice on the performance achieved by the respective DCE techniques. For the power allocation algorithm of the DANFD-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 results for FD-DCE are presented in Fig. 4.11, where Fig. 4.11a shows the MSE of the eavesdropper at

the different location around Alice. These results show that the 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 $1.5m$. We have omitted the results for ANFD-DCE as it is unable to provide robust decoding at Bob, where the BER is equal to 0.05. For the DANFD-DCE, the performance analysis is shown in Fig. 4.12. The DANFD-DCE achieves robust secure communication as the BER at the eavesdropper remains close to 10^{-1}, while BER at Bob is less than 10^{-4}.

Performance Analysis for Optimal Location of Eavesdropping

This section provides an in-depth performance analysis of the DANFD-DCE along with the comparisons to the ANFD-DCE and FD-DCE. First, we have considered the same scenario as mentioned for ANFD-DCE, where the distance between Alice and the eavesdropper is $2m$ while Alice and Bob are $3m$ apart as shown in Fig. 4.5.

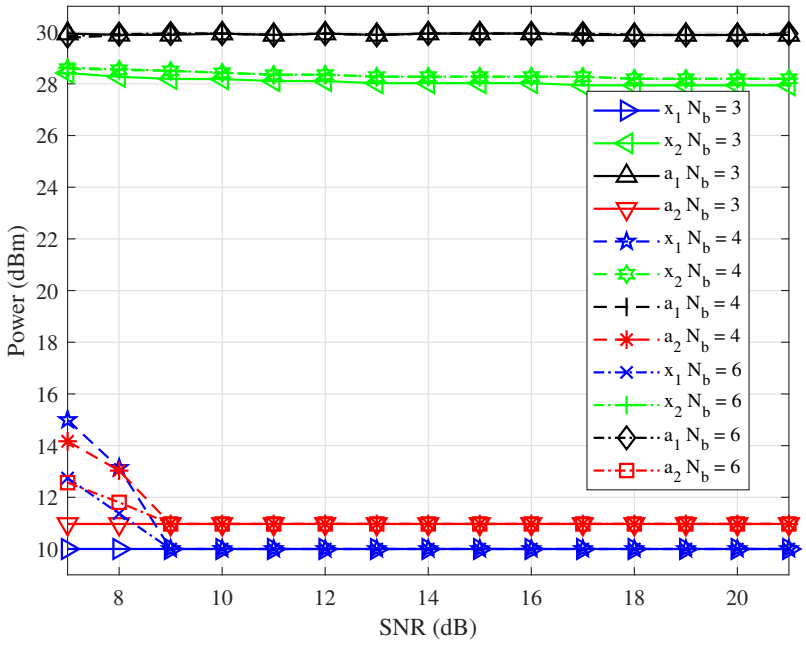
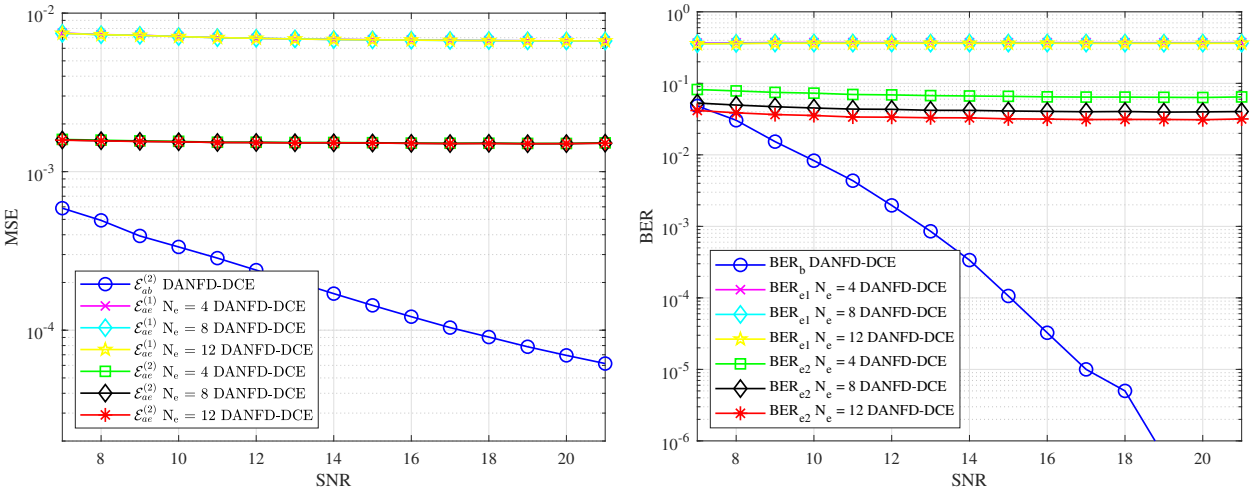


Fig. 4.13 Average power allocation for DANFD-DCE while $N_a = 4$, and $N_b = [3, 4, 6]$.

Fig. 4.13 shows the average power allocation for DANFD-DCE to the training signal

x_1, and x_2, and the AN signals a_1, and a_2 where horizontal axis represents the SNR at the legitimate receiver in dB, and vertical axis corresponds to power in dBm. The maximum transmission power is considered to be $30dBm$. We have provided the results for different number of antennas at Bob: $N_b = [3, 4, 6]$ while $N_a = 4$ at Alice. These results indicate that for the DANFD-DCE, the power allocated to the training signal in the second stage (AN aided 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 with respect to the number of transmit antennas.

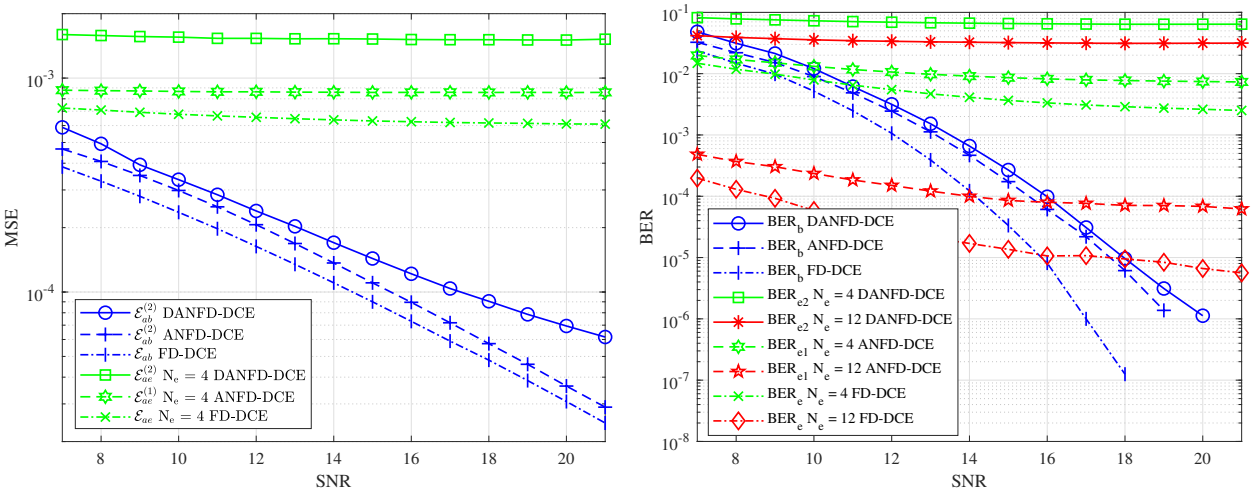


(a) MSE (b) BER

Fig. 4.14 MSE and BER for DANFD-DCE at different SNR, while $N_a = N_b = 4$, and $N_e = [4, 8, 12]$.

MSE and BER for the optimal eavesdropping location at different SNR is shown in Fig. 4.14, where $N_a = N_b = 4$. These results indicate that Bob is able to robustly decode the transmitted signal while the eavesdropper is unable to decode that information as the BER remains close to 0.1 even at high SNRs. Fig. 4.14 also shows the impact of increasing the number of eavesdropping antennas on the MSE and BER, as MSE remains the same however the BER improves slightly with the increase in the number of eavesdropping antennas. Fig. 4.14a shows that the MSE at the eavesdropper improves by using the signal received in the third stage to estimate the channel $\boldsymbol{H}_{ae}$ by the sequential LS estimator. Fig. 4.14b shows that improved MSE results in the improved BER at the eavesdropper. Therefore, the

eavesdropper will use the channel estimated in the third stage for MSE and BER.

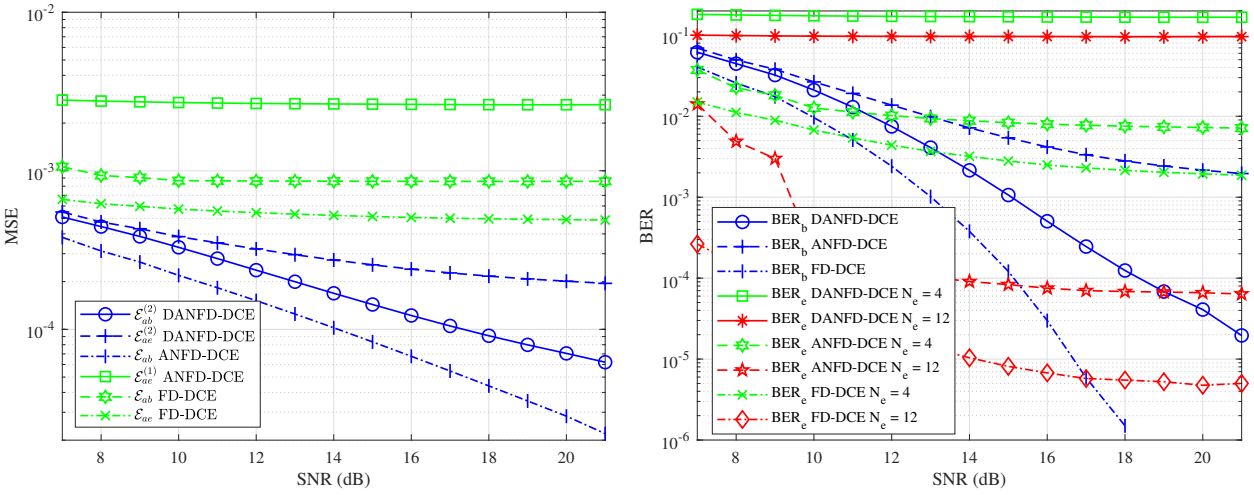


(a) MSE (b) BER

Fig. 4.15 MSE and BER for DANFD-DCE, ANFD-DCE, and FD-DCE, while $N_a = N_b = 4$, and $N_e = [4, 12]$.

The comparison of the DANFD-DCE to ANFD-DCE and FD-DCE is presented in Fig. 4.15. In Fig. 4.15a, we have shown the MSE at the eavesdropper with 4 eavesdropping antennas as the MSE remains the same for the different number of antennas. Fig. 4.15a shows that the DANFD-DCE maintains the highest MSE at the eavesdropper among the three DCE techniques by using extra AN, which also results in the higher MSE at Bob as compared to ANFD-DCE and FD-DCE. The BER analysis indicates that the DANFD-DCE achieves robust secrecy performance as compared to ANFD-DCE and FD-DCE. We have omitted the results for the eavesdropper with 8 antennas due to space limitations as the BER for $N_e = 8$ will be in between the curves given for $N_e = 4$ and $N_e = 8$ for each DCE technique.

Fig. 4.16 shows the effect of different number of antennas at Bob $N_b = [3, 6]$ on the performance achieved by each DCE. The performance improves for the eavesdropper as the number of antennas at Bob increases, because the eavesdropper receives more training signals from Alice as shown in the Algorithm 1, to ensure the AN signal is orthogonal to the main channel. Fig. 4.16b shows that for ANFD-DCE, Bob is unable to decode the transmitted signal while the eavesdropper has robustly decoded the signal as the BER is close to 10^{-4}. For $N_b = 6$, the performance of ANFD-DCE and FD-DCE improves at the legitimate node



(a) MSE for $N_b = 3$.

(b) BER for $N_b = 3$.

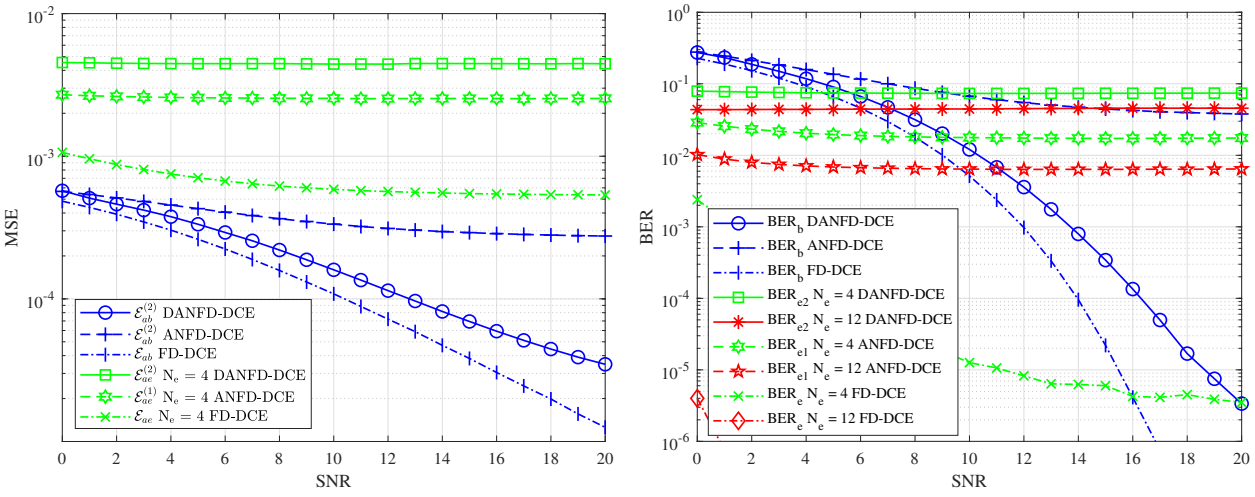
(c) MSE for $N_b = 6$.

(d) BER for $N_b = 6$.

Fig. 4.16 MSE and BER for ANFD-DCE, ANFD-DCE, and FD-DCE, while $N_a = 4$, $N_b = [3, 6]$, and $N_e = [4, 12]$

but the eavesdropper is also able to decode the information.

Fig. 4.17 shows the performance of the DCE techniques for the optimal eavesdropping location with $d_b = 1m$ around Alice, where $d_{ae} = 1m$, $d_{be} = 6m$, and $d_{ab} = 5m$. For the power allocation algorithm of the ANFD-DCE, we have utilized $\gamma = 2.6 \times 10^{-3}$ for $d_b = 1m$. 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}. The results also



(a) MSE (b) BER

Fig. 4.17 MSE and BER for DANFD-DCE, ANFD-DCE, and FD-DCE, while $N_a = N_b = 4$, and $N_e = [4, 12]$.

indicate that the ANFD-DCE keep BER at the eavesdropper close to 10^{-2} but it fails to establish a robust communication link between the legitimate nodes. Finally, the DANFD-DCE achieves robust secure communication as the BER at Bob is less than 10^{-4} while the BER at the eavesdropper is close to 10^{-1}, even with 12 eavesdropping antennas. These results show that the DANFD-DCE is able to establish a robust and secure communication link by avoiding the leakage of the channel estimates to the eavesdropper.

Effect of AN on FD based DCE

The location-based analysis presented in Section 4.2.5 and 4.3.4 provides new sights regarding the drawback of FD-DCE as it is unable to achieve secure communication for the eavesdropper located opposite to legitimate receiver but close to the legitimate transmitter. The use of AN aided DANFD-DCE solves this problem by using AN signal to protect the leakage of channel estimate. The AN signal causes equivocation at the eavesdropper where the in-band FD transmission from the legitimate receiver can not achieve equivocation due to high path-loss. However, as shown in Fig. 4.11 the FD-DCE achieves considerable secrecy for the scenarios where the eavesdropper is located in between the legitimate nodes. Therefore, the FD-DCE presented in Chapter 3 can be coupled with directional antennas or RF shield to restrict the direction of transmitted signals to achieve secure communication.

4.4 Summary

In this chapter, we have presented two novel AN assisted FD-DCE techniques. First, a novel artificial noise aided full-duplex (ANFD) DCE is presented where an orthogonal AN signal is utilized in the third stage to overcome the drawbacks of FD-DCE presented in Chapter 3. The ANFD-DCE technique comprises three stages responsible for estimation of SI channel, rough channel estimates for orthogonal AN design, and AN assisted training in the first, second, and third stage, respectively. Second, a novel double artificial noise aided full-duplex (DANFD) DCE is presented to overcome the leakage of channel estimates to a strategically located adversary by transmitting an AN signal in the second stage also known as the rough channel estimation stage. The proposed DANFD-DCE technique also comprise three stages similar to ANFD-DCE. 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 the performance improvements achieved by the proposed ANFD and DANFD-DCE as compared to the FD-DCE for different locations of the eavesdropper. The second part of the simulation analysis provides an extensive performance comparison of the DANFD, ANFD, and FD-DCE for the optimal eavesdropping location.

Chapter 5

Conclusions and Future Work

In this thesis, we have studied the secrecy of wireless communication from an eavesdropper. The applications of wireless communication have significantly increased from e-commerce, social media, smart connected cars to telemedicine over the last decade. Therefore, it is pivotal to avoid the leakage of crucial personal information to any malicious user as email passwords, credit card numbers, personal health information, and other critical information is exchanged over the wireless medium. This thesis presents novel techniques to utilize full-duplex transmissions to secure wireless communication on the physical layer (the lowest layer of the communication stack) by obscuring the channel estimates from any potential passive eavesdropper. The presented performance analysis shows that the proposed channel estimation techniques limit the decoding capability at the eavesdropper to avoid the leakage of confidential information while the legitimate receiver can robustly decode the received message. This chapter presents a summary of the thesis and future research directions.

5.1 Thesis Summary

In chapter 2, we have provided an overview of physical layer security foundations along with different approaches to realize the physical layer security and their reliance on robust and secure channel estimates. Afterward, chapter 2 provides a review of the existing discriminatory channel estimation (DCE) techniques, where the legitimate nodes obscure the channel estimates from the eavesdropper to achieve secure communication. DCE techniques provide a bandwidth-efficient opportunity to realize physical layer security as the channel estima-

tion stage is generally shorter than the data transmission stage. Finally, the open research problems of the existing DCE techniques mentioned in chapter 2 serve as the foundation for presented novel DCE techniques in this thesis.

In Chapter 3, we have presented a novel in-band full-duplex based two-stage FD-DCE technique to overcome the drawbacks of the existing DCE techniques while avoiding the leakage of channel estimates. We have presented the design of private orthogonal training signals in the first stage of the FD-DCE to acquire the self-interference (SI) channel estimates. The secrecy of training signals for the SI channel estimation prevents the leakage of channel estimates in the first stage. Subsequently, the proposed FD-DCE limits the channel estimation at the eavesdropper in the second stage by simultaneously transmitting the globally known training signals from both the legitimate nodes. In Chapter 3, we have provided the performance analysis of a passive eavesdropper located between the legitimate nodes. Mean square error (MSE) analysis is provided for each estimation stage at every node to demonstrate that the FD-DCE provides robust channel estimation at the legitimate nodes while limiting the estimation performance at the eavesdropper. For system-level performance evaluation, we have provided the achievable secrecy capacity and the bit error rate (BER) to show that the proposed FD-DCE achieves robust and secure communication while overcoming the drawbacks of the existing DCE techniques.

Chapter 4 studies the use of artificial noise (AN) along with in-band FD transmission to enhance the secrecy achieved by DCE against a strategically located eavesdropper. We have also presented the novel local adaptive power allocation algorithm for AN aided DCE techniques to keep the power allocation secret from the eavesdropper. MSE and BER simulation analysis provided to show the performance improvement achieved by adding the AN to the transmission of training signals. Location-based simulation analysis is presented in chapter 4 by showing the MSE and BER for each location of the eavesdropper, for a fixed position of the legitimate nodes. The location-based analysis shows that the in-band FD transmission of AN along with the pilot signals achieves robust secure communication for different locations of the eavesdropper. The location-based performance analysis also shows that FD-DCE can achieve secrecy for the eavesdropper located in-between the legitimate node, and its secrecy performance drops otherwise. The FD-DCE can be coupled with directional antennas or the radio frequency shields to limit the leakage of the wireless signal in unwanted directions. Therefore, the appropriate DCE technique can be selected based on

the scenario. For example, as DANFD-DCE achieves robust DCE but requires more power than ANFD-DCE, and ANFD-DCE requires more bandwidth and power to provide security against the strategically located eavesdropper than the FD-DCE.

5.2 Future Work

There are several avenues for future works by considering the different properties of the eavesdroppers and the legitimate nodes.

5.2.1 Active Eavesdropping

In this thesis, we have considered a passive eavesdropping scenario, where the eavesdropper passively eavesdrops on legitimate communication. On the other hand, an active eavesdropper also transmits the signals to cause performance deterioration at the legitimate nodes. One promising direction is to explore the impact of jamming signals from an active eavesdropper on the legitimate channel estimation and the achievable secrecy performance. For the active eavesdropping scenario, the legitimate nodes can acquire the channel statistics from the signals transmitted by the eavesdropper. Therefore, the optimal power allocation and training signal design algorithms can be designed to achieve secure communication. However, special attention should be paid to detect and cancel the jamming signal transmitted by the eavesdropper by using techniques like MUSIC (MUltiple SIgnal Classification).

5.2.2 Multiple Collaborative Nodes

In this thesis, we have considered two legitimate nodes and one eavesdropper. One future direction can be to explore the possibility of collaboration among multiple half-duplex and FD legitimate nodes. For multiple legitimate nodes, the cooperation between multiple FD and half-duplex can be considered to design and transmit the training sequence and AN signals to further enhance the secrecy performance of the DCE techniques. Similarly, another future direction can be to explore the impact of the multiple collaborative eavesdroppers on the secrecy performance. For example, triangulation can be used by multiple eavesdroppers to estimate the power allocation coefficients for AN assisted FD-DCE techniques.

5.2.3 Cross-Layer Design

One important future direction is to explore the cross-layer design of the communication system using proposed in-band FD-DCE techniques at the physical layer for channel estimation. Different PLS techniques can be employed depending on the security requirements of the transmitted message. Similarly, the use of appropriate in-band FD-DCE can be selected based on available transmission power, secrecy requirement, and other parameters.

Bibliography

[1] M. Reza Akhondi, A. Talevski, S. Carlsen, and S. Petersen, "Applications of wireless sensor networks in the oil, gas and resources industries," in *Porc. 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 10)*, Apr. 2010, pp. 941–948.

[2] 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 & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[3] "Ring video doorbell pro under the scope," https://www.bitdefender.com/files/News/CaseStudies/study/294/Bitdefender-WhitePaper-RDoor-CREA3949-en-EN-GenericUse.pdf?clickid=S7Ayccy-2xyOUCjwUx0Mo3cjUki18UW1i3gaUA0&irgwc=1&MPid=10078&cid=aff%7Cc%7CIR, accessed: 2020-06-03.

[4] "ESET INTERNET SECURITY: A serious vulnerability deep inside wi-fi encryption," https://www.eset.com/int/kr00k/, accessed: 2020-06-03.

[5] T. Mavroeidakos and V. Chaldeakis, "Threat landscape of next generation iot-enabled smart grids," in *IFIP International Conference on Artificial Intelligence Applications and Innovations*. Springer, 2020, pp. 116–127.

[6] M. L. Robert, J. A. Michael, and C. Tim, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), Washington DC, Tech. Rep., Mar. 2016.

[7] M. A. Specter, J. Koppel, and D. Weitnzer, "The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in us federal elections," *Preprint available at: https://internetpolicy. mit. edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public. pdf*, 2020.

[8] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-deepsca: Cross-device deep learning side channel attack," in *Proceedings of the 56th Annual Design Automation Conference 2019*, 2019, pp. 1–6.

[9] J. Wallace, M. Jensen, A. Swindlehurst, and B. Jeffs, "Experimental characterization of the mimo wireless channel: data acquisition and analysis," *IEEE Transactions on Wireless Communications*, vol. 2, no. 2, pp. 335–343, 2003.

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

[11] 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 Processing Magazine*, vol. 30, no. 5, pp. 41–50, 2013.

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

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

[14] 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.

[15] 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. Magazine*, vol. 53, no. 12, pp. 19–25, 2015.

[16] 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 Transactions on Wireless Communications*, vol. 6, no. 3, pp. 805–810, 2007.

[17] 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 Processing*, vol. 58, no. 12, pp. 6223–6237, 2010.

[18] 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 Processing*, vol. 61, no. 10, pp. 2724–2738, 2013.

[19] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical J.*, vol. 28, no. 4, pp. 656–715, 1949.

[20] A. D. Wyner, "The wire-tap channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[21] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 532–540, 2011.

[22] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 551–564, 2011.

[23] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled ldpc codes for the bec wiretap channel," in *Proc. IEEE Int. Symposium on Information Theory Proceedings (ISIT 11)*, Aug. 2011, pp. 2393–2397.

[24] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channel," in *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*. IEEE, 2009, pp. 834–838.

[25] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[26] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.

[27] K. Ito, Y. Masuda, and E. Okamoto, "A chaos MIMO-based polar concatenation code for secure channel coding," in *2019 International Conference on Information Networking (ICOIN)*. IEEE, 2019, pp. 262–267.

[28] T. Pinto, M. Gomes, J. P. Vilela, and W. K. Harrison, "Polar coding for physical-layer security without knowledge of the eavesdropper's channel," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[29] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

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

[31] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[32] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Select. Areas in Commun.*, vol. 31, no. 9, pp. 1779–1790, 2013.

[33] C. Fragouli, V. M. Prabhakaran, L. Czap, and S. N. Diggavi, "Wireless network security: Building on erasures," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1826–1840, 2015.

[34] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[35] M. Tahmasbi and M. R. Bloch, "Covert secret key generation with an active warden," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1026–1039, 2019.

[36] L. Wang, H. An, H. Zhu, and W. Liu, "Mobikey: Mobility-based secret key generation in smart home," *IEEE Internet of Things Journal*, 2020.

[37] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[38] S. Haile, "Investigation of channel reciprocity for ofdm tdd systems," Master's thesis, University of Waterloo, 2009.

[39] D. Qin and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," *IEEE Transactions on information forensics and security*, vol. 11, no. 12, pp. 2693–2705, 2016.

[40] A. Badawy, "Practical secrecy at the physical layer: Key extraction methods with applications in cognitive radio," Ph.D. dissertation, Politecnico di Torino, 2017.

[41] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity-Part I and part II," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1948, 2003.

[42] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[43] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for ofdma decode-and-forward relay networks," *IEEE Trans. Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, 2011.

[44] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 359–371, 2012.

[45] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 10, pp. 2095–2107, 2015.

[46] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. S. Evans, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1216–1232, 2019.

[47] J. Xing, T. Lv, and X. Zhang, "Cooperative relay based on machine learning for enhancing physical layer security," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2019, pp. 1–6.

[48] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[49] ——, "The role of an untrusted relay in secret communication," in *Proc. IEEE Int. Symposium on Information Theory (ISIT 08)*, Jul. 2008, pp. 2212–2216.

[50] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2536–2550, 2013.

[51] R. Zhao, X. Tan, D.-H. Chen, Y.-C. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11 511–11 524, 2018.

[52] S. Atapattu, N. Ross, Y. Jing, and M. Premaratne, "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Communications Letters*, vol. 23, no. 5, pp. 842–846, 2019.

[53] 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.

[54] A. Wyner and J. Ziv, "The Rate-Distortion Function for Source Coding with Side Information at the Decoder," *IEEE Trans. on Information Theory*, vol. 22, no. 1, pp. 1–10, 1976.

[55] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wiretap channel," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 2471–2475.

[56] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[57] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part ii: The mimome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[58] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[59] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[60] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[61] J. Huang and S. Signell, "On performance of adaptive modulation in MIMO systems using orthogonal space-time block codes," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4238–4247, 2009.

[62] 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 Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 516–531, 2016.

[63] 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.

[64] 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. Communications*, vol. 62, no. 7, pp. 2400–2410, 2014.

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI) 14)*, 2014, pp. 359–372.

[70] 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.

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

[72] 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.

[73] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE transactions on information forensics and security*, vol. 10, no. 3, pp. 574–583, 2015.

[74] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE communications letters*, vol. 19, no. 4, pp. 525–528, 2015.

[75] 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.

[76] ——, "In-band full-duplex discriminatory channel estimation using mmse," *IEEE Trans. Inform. Forensic Secur.*, pp. 1–1, 2020.

[77] 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.

[78] 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.

[79] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[80] 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.

[81] 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.

[82] 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. on Information Forensics and Security*, vol. 13, no. 11, pp. 2788–2800, 2018.

[83] 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.

[84] 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.

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

[86] B. Park, H. Cheon, E. Ko, C. Kang, and D. Hong, "A blind ofdm synchronization algorithm based on cyclic correlation," *IEEE Signal Processing Letters*, vol. 11, no. 2, pp. 83–85, 2004.

[87] T. Fusco and M. Tanda, "Blind synchronization for ofdm systems in multipath channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1340–1348, 2009.

[88] 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.

[89] 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.

[90] 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.

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

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

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] F. Ud Din and F. Labeau, "Artificial noise assisted in-band full-duplex secure channel estimation," *IEEE Trans. Veh. Technol., submitted for publication.*

[102] 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.

[103] Liu Kewen and Xing Ke, "Research of MMSE and LS channel estimation in OFDM systems," in *The 2nd International Conference on Information Science and Engineering*, 2010, pp. 2308–2311.