Physical Layer Security Through Secure Channel Estimation

Fawad Ud Din, and Fabrice Labeau

Department of Electrical and Computer Engineering, McGill University, 3480 University Street,
Montréal, Québec, H3A 0E9, Canada.
Emails: fawad.uddin@mail.mcgill.ca, fabrice.labeau@mcgill.ca

***Abstract*—The random nature of wireless channel can be utilized to achieve secure communications. Recently, there have been some contributions towards finding practical approaches to provide physical layer security, but robust and secure channel estimates are critical in achieving secrecy. In this paper, we propose that in-band full-duplex communication can be utilized by the legitimate transceiver pair to mask the channel estimates from the eavesdropper. The proposed secure channel estimation technique comprises of two stages. In the first stage, the self-interference channel is estimated by respective nodes. In the second stage, in-band full-duplex transmission from both legitimate nodes is utilized to achieve channel estimates at legitimate nodes while providing equivocation at the eavesdropper. The performance analysis shows that the proposed scheme provides robust channel estimation at the legitimate nodes while maintaining equivocation at the eavesdropper.**

I. Introduction

The growing penetration of smart networks and connected devices has raised concerns regarding their security and privacy. The security threats in wireless sensor networks (WSN) can result in colossal damage, as their applications include many sensitive governmental, military, and commercial usage [1]. For any large-scale implementation of WSNs, security and privacy requirements are vital to avert any major catastrophe. In current communications frameworks, secrecy is provided by encryption of the information. The major drawback of cryptographic systems is their reliance on computational hardness to decode the encryption. The recent advancements in computational technology and availability of computational resources make it easier to decipher the codeword. The physical layer security theoretically assures secure communication for certain scenarios [2]. In current communication framework, the encryption is commonly implemented on higher layers, for example, application, and transport layer of the communication stack. The lower layers (physical and data link layer) are oblivious of any security considerations. In the face of recent challenges, the security must be considered on physical layer to provide secure wireless communications.

The vast majority of literature on physical layer security is of theoretical nature. Recently there have been some contributions towards finding more practical approaches to provide secure communications [3], but robust and secure channel estimates are critical in achieving secrecy through these techniques [4]. The authors in [4] have shown that leakage of channel state information (CSI) deteriorates the performance of physical layer security techniques. In recent papers, the Discriminatory Channel Estimation (DCE) techniques have been presented to avoid the leakage of channel estimates to the eavesdropper, where channel estimation performance is degraded at the eavesdropper as compared to the legitimate transceiver pair [5], [6]. The existing DCE techniques comprise of multiple stages, wherein first stage, rough channel estimates are obtained by limiting the power of pilot signal or transmitting the pilot from receiver instead of the transmitter. Afterwards, artificial noise (AN) aided pilot signal is utilized to deteriorate the estimation performance at the eavesdropper. The rough channel estimates obtained in the first stage are utilized to transmit the AN in the null space of legitimate channel. The major drawbacks of existing DCE are leakage of rough estimates to an adversary, and robustness of rough estimates as they can deteriorate channel estimation in further re-training stages. To overcome these problems, we propose a novel secure channel estimation technique where in-band full-duplex communication has been utilized to avoid the leakage of channel estimates to any potential eavesdropper.

The proposed channel estimation technique comprises of two stages. In the first stage, the corresponding self-interference channel is estimated by both legitimate nodes by using random training symbols known to themselves only. The eavesdropper cannot acquire useful information as the pilot sequence is not known at the eavesdropper. In the second stage, in-band full-duplex training signals are transmitted from both legitimate nodes, and the two overlapping signals cause equivocation at the eavesdropper. In this paper, mean square error (MSE) has been utilized as the performance metric to analyze the estimation performance. The estimators in both stages are based on least square (LS) minimization which are shown to be equal to maximum likelihood (ML) estimators. Our simulation analysis shows that the proposed secure channel estimation technique provides robust channel estimates at the legitimate receiver while maintaining equivocation at the eavesdropper.

The remainder of this paper is organized into five sections. The section II provides the system model used in our research. The proposed secure channel estimation technique is presented in section III. The results obtained from simulation analysis are described in section IV followed by conclusions in the

section V. This paper follows usual conventions of notation, where vectors are denoted by boldface symbols, $(.)^H$, $(.)^T$, and $(.)^*$ represent conjugate transpose, transpose, and conjugate. These notations will be followed throughout this paper.

II. System Model

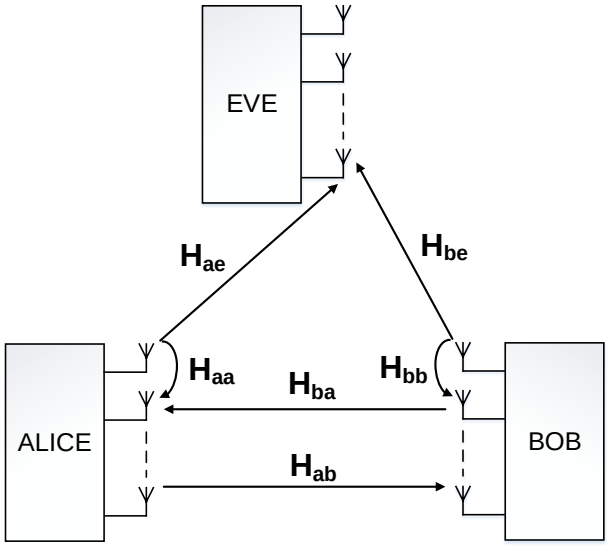

Fig. 1. Basic channel model utilized for proposed channel estimation technique, comprising of multi antenna full-duplex legitimate transmitter, legitimate transmitter, and eavesdropper commonly known as Alice, Bob, and Eve, respectively.

We consider a three node network for physical layer security as shown in Fig. 1. In this model, the legitimate transmitter and receiver exchange information over the main channel, while an eavesdropper passively eavesdrops on their communication via wiretap channel. In the literature, the legitimate transmitter, receiver, and eavesdropper are commonly referred to as Alice, Bob, and Eve, respectively. In this paper, Eve is considered to be a passive eavesdropper, where the adversary intercepts information that is being communicated over the wireless channel but does not transmit any signal. All the nodes are considered to have multiple antennas with full-duplex capabilities. It is considered that only one antenna's channel is estimated at once, it provides low complexity and simplicity. All transmissions are assumed to be drawn from the same M-ary square QAM constellation. Thus if m denotes the number of bits per symbol per dimension, we have $M = 2^{2m}$. The set of complex baseband constellation points $\left\{x_{k_I,k_Q}\right\}$ for $k_I, k_Q \in \{0, \ldots, \sqrt{M}-1\}$ are given as:

$$x_{k_I,k_Q} = \sqrt{\frac{3P}{M-1}}\left[2k_I + 1 - \sqrt{M} + j\left(2k_Q + 1 - \sqrt{M}\right)\right],$$

where $j = \sqrt{-1}$ and P indicates the transmission power.

Each receiver is assumed to experience independent zero-mean circularly symmetric additive white Gaussian noise (AWGN). All the transmissions are assumed to undergo independent flat fading channel and path-loss is modeled as the simplified path model as described in [7]. The fading for self-interference channel H_{aa}, and H_{bb} are statistically modeled as Rician fading distribution based on the experimental characterization of self-interference channel in [8]. On the other hand, inter-node channel fading distribution is statistically modeled as Rayleigh fading distribution. In this research, the phase noise is assumed to be perfectly canceled as transmit and receive chains share a common oscillator on each node. Both training stages comprise of n symbols, where n is the length of the training sequence.

III. Proposed Discriminatory Channel Estimation

A. First Stage

In the first stage, the self-interference channel is estimated by the respective nodes. Each node utilizes a random training signal which is known to itself only. The usage of a private pilot signal provides secrecy against Eve in the first stage. The existing DCE techniques limit the power of the pilot signal to limit the performance of channel estimation at Eve, but in this scheme Eve cannot use any pilot based channel estimation technique. The received signal for ith-training symbol at the respective node is given as:

$$Y_{si} = H_s X_{si} + n_{si}, \qquad i = 0, \ldots, n-1 \tag{1}$$

where, Y_{si} is the received self-interference signal. H_s indicates the self-interference channel and X_{si} is the ith random pilot signal. n_{bi} is assumed from a zero mean and variance σ_s independent and identically distributed (iid) AWGN added to the system.

As the pilot signal is known at the receiver, LS estimation is utilized to estimate the self-interference channel. LS is one of the simplest estimation techniques as it does not require any statistical information regarding received signal. LS estimation minimizes the squared distance as:

$$\min_{H_s} \sum_{i=0}^{n-1} \left(Y_{si} - H_s X_{si}\right)^2 \tag{2}$$

The minimization is performed by taking the derivative with respect to H_s. Finally, the LS estimator is given as:

$$\hat{H}_s^{LS} = \frac{\sum_{i=0}^{n-1} Y_{si} X_{si}}{\sum_{i=0}^{n-1} X_{si}^2} \tag{3}$$

ML estimator can also be utilized as the noise is assumed to be iid AWGN. In [9], the author has shown that for given iid AWGN scenario LS estimate is equal to ML estimate, which implies that statistical information regarding noise does not provide any benefit in the estimation process.

B. Second Stage

In the second stage, full-duplex transmission provides the required equivocation at the eavesdropper while delivering pilot sequences for channel estimation at both participating nodes, it also saves the bandwidth and communication overhead which is wasted in existing AN based training schemes. Full-duplex is utilized for secure communication in [10],

where the authors have presented achievable secrecy sum rates. The full-duplex communication is considered for channel estimation only because it does not provide optimal utilization of resources in scenarios, where higher bandwidth is required for transmission of data from Alice to Bob as compared to the other way round. We can increase the data rate from Alice to Bob by utilizing multiple-input, multiple-output (MIMO) based spatial multiplexing techniques, as compared to full-duplex. The received signals, at respective nodes in this stage, are given as:

$$Y_{ai} = H_{ba}X_{bi} + H_{aa}X_{ai} + n_{ai}, \;\; i = 0, \ldots, n-1 \tag{4}$$

$$Y_{bi} = H_{bb}X_{bi} + H_{ab}X_{ai} + n_{bi}, \;\; i = 0, \ldots, n-1 \tag{5}$$

$$Y_{ei} = H_{be}X_{bi} + H_{ae}X_{ai} + n_{ei}, \;\; i = 0, \ldots, n-1 \tag{6}$$

where, Y_{ai}, Y_{bi}, and Y_{ei} indicates respective ith received signals at Alice, Bob, and Eve. X_{ai} and X_{bi} are ith pilot signals transmitted by Alice and Bob simultaneously. These equations indicate that received signal at Eve has two unknown channel coefficients H_{be} and H_{ae}. Although pilot signals X_{bi} and X_{ai} are known to Eve, the absence of channel information makes it hard for Eve to extract any information from the received signal.

Alice and Bob acquire channel estimates by utilizing LS estimation algorithm and the self-interference channel estimates from the previous stage. LS estimation at Bob is given as:

$$\min_{H_{ab}} \sum_{i=0}^{n-1} \left(Y_{bi} - H_{ab}X_a i - \hat{H}_{bb}X_{bi} \right)^2 \tag{7}$$

$$\hat{H}_{ab}^{LS} = \frac{\sum_{i=0}^{n-1} Y_{bi}X_{ai} - \hat{H}_{bb}X_{ai}X_{bi}}{\sum_{i=0}^{n-1} X_{ai}^2} \tag{8}$$

where, $\hat{H}_{bb}^{LS}$ is estimated in the previous stage. To find ML estimate of H_{ab}, likelihood for received signal can be expressed as:

$$\mathcal{L}(Y_b|H_{ab}) = \log\left(2\pi\sigma_b^2\right)^{-\frac{n}{2}} - \frac{\sum_{i=0}^{n-1}\left(Y_{bi} - H_{ab}X_{ai} - H_{bb}X_{bi}\right)^2}{2\sigma_s^2} \tag{9}$$

After maximizing likelihood, ML estimate for H_{ab} is given as:

$$\hat{H}_{ab}^{ML} = \frac{\sum_{i=0}^{n-1} Y_{bi}X_{ai} - \hat{H}_{bb}X_{ai}X_{bi}}{\sum_{i=0}^{n-1} X_{ai}^2} \tag{10}$$

As in previous stage the ML estimate turns out to be same as LS estimate. Finally, the same process is repeated at Alice to acquire estimate $\hat{H}_{ba}$.

To acquire the channel information Eve can rely on blind channel estimation techniques as the pilot signal transmitted in the first stage is not known to Eve. The blind channel estimation techniques do not perform at par with pilot based channel estimation techniques and they also require some prior statistical information regarding the transmitted signal [11]. Another drawback of blind channel estimation techniques is that they are inherently prone to phase ambiguity errors because it is not possible to achieve robust estimates of phase. In next section, we have utilized state-of-the-art blind channel estimation technique at Eve to acquire the best possible channel estimates.

IV. Performance Analysis

To evaluate the performance of the proposed secure channel estimation technique we have utilized MSE as the performance metric. The MSE is also given as the sum of bias-squared and variance of the estimator [9]:

$$\begin{aligned} MSE &= \mathbb{E}\left[\left(\hat{h} - h\right)^2\right] \\ &= bias(\hat{h})^2 + var(\hat{h}) \end{aligned} \tag{11}$$

where, h is the true value of the parameter, and $\hat{h}$ corresponds to the estimated value of the parameter h. First, we have calculated the theoretical values for MSE by utilizing the given random distribution and their parameters, followed by simulation analysis.

To calculate MSE for the 1st stage, the bias of $\hat{H}_s$ is given as:

$$\begin{aligned} \mathbb{E}\left[\hat{H}_s\right] &= \mathbb{E}\left[\frac{\sum_{i=0}^{n-1} Y_{si}X_{si}}{\sum_{i=0}^{n-1} X_{si}^2}\right] \\ &= H_s \end{aligned} \tag{12}$$

Hence, $\hat{H}_s$ provides unbiased estimate and the variance of the estimator corresponds to the MSE. Variance of $\hat{H}_s$ is given as:

$$\begin{aligned} var\left[\hat{H}_s\right] &= \mathbb{E}\left[\left(\hat{H}_s - \mathbb{E}\left[\hat{H}_s\right]\right)^2\right] \\ &= \mathbb{E}\left[\left(\frac{\sum_{i=0}^{n-1} Y_{si}X_{si}}{\sum_{i=0}^{n-1} X_{si}^2} - H_s\right)^2\right] \\ &= \sigma_s^2 = MSE\left(\hat{H}_s\right) \end{aligned} \tag{13}$$

The equation (13) shows that MSE of for $\hat{H}_s$ depends on the variance of the noise added to the received signal at respective node. A similar analysis is also conducted for estimation process in the second stage, mean of $\hat{H}_{ab}$ is given as:

$$\mathbb{E}\left[\hat{H}_{ab}\right] = \mathbb{E}\left[\frac{\sum_{i=0}^{n-1} Y_{bi}X_{ai} - \hat{H}_{bb}X_{ai}X_{bi}}{\sum_{i=0}^{n-1} X_{ai}^2}\right] \tag{14}$$

Substituting mean of $\hat{H}_s$ from (12) into above equation yields $\mathbb{E}[\hat{H}_{ab}] = H_{ab}$. It shows that $\hat{H}_{ab}$ provides an unbiased estimate. The variance of $\hat{H}_{ab}$ is given as:

$$\begin{aligned} var\left[\hat{H}_{ab}\right] &= \mathbb{E}\left[\left(\hat{H}_{ab} - \mathbb{E}\left[\hat{H}_{ab}\right]\right)^2\right] \\ &= \mathbb{E}\left[\left(\frac{\sum_{i=0}^{n-1} Y_{bi}X_{ai} - \hat{H}_{bb}X_{ai}X_{bi}}{\sum_{i=0}^{n-1} X_{ai}^2} - H_{ab}\right)^2\right] \\ &= \sigma_s^2 + \sigma_{ab}^2 = MSE\left(\hat{H}_{ab}\right) \end{aligned} \tag{15}$$

It indicates that MSE is the sum of two variances, as the estimate of $\hat{H}_{ab}$ is composed of difference between two Gaussian random variables.

In order to validate the secrecy achieved by the proposed scheme, we have utilized the blind channel estimation scheme given in [12] at Eve in the first stage. In [12] the statistical independence among sources in space-time block coded (STBC) system has been utilized to acquire channel estimates blindly. We have also used STBC based Alamouti scheme to transmit the signal [13]. The blind channel estimation technique requires that the receiver node has more antennas than transmitting node, for the channel estimation at Eve we have considered two transmit antennas and four receive antennas. This corresponds to the worst case scenario as the state of the art blind channel estimation technique has been utilized at Eve along with additional resources to aid the blind channel estimation at Eve as compared to Bob. The major drawback of this technique is that it requires some prior information regarding the signal to resolve the phase ambiguity at the receiver. The phase ambiguity arises in all blind channel estimation techniques as they can be locked with wrong phase rotation. Finally, the channel blindly estimated in the first stage is utilized in LS estimation by Eve to estimate the channel between Alice and Eve.

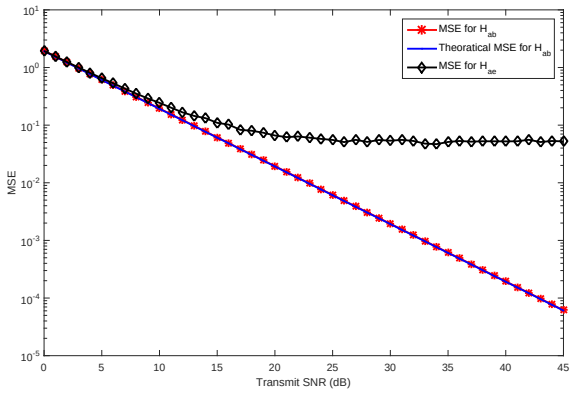

Fig. 2. MSE for H_{ab} and H_{ae} obtained by using proposed channel estimation technique against transmit SNR where H_{ab} and H_{ae} correspond to channel between Alice-Bob and Alice-Eve respectively.

For the simulation analysis, the channel coefficients for inter-node channels are drawn from a Rayleigh block fading channel model with zero mean and unit variance. The self-interference channel coefficients are drawn from a Rician fading distribution with K=35 as, presented in [8] based on the experimental characterization of the self-interference channel. For path-loss, simplified path-loss has been utilized with the path-loss exponent of '1.75' for indoor office space. The distance between the legitimate pair is assumed to be 3 meters, and Eve is 2.25 meters from both nodes. The full-duplex antennas are separated by 10 centimeters. We have utilized 16-QAM modulation for transmission, and system noise is considered to be circularly symmetric zero mean

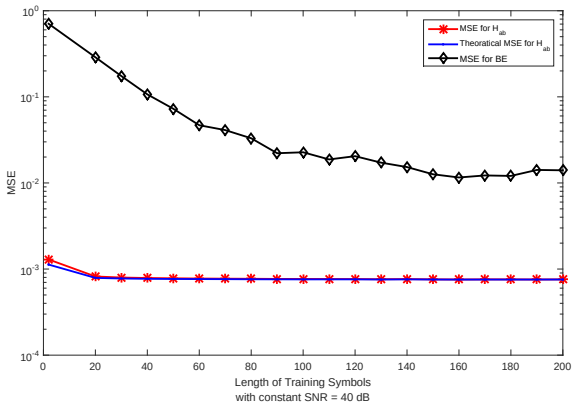

Fig. 3. MSE obtained by using proposed channel estimation technique against the length of pilot symbol used at constant transmit SNR of '30dB', where H_{ab} and H_{ae} corresponds to channel between Alice-Bob and Alice-Eve respectively.

AWGN. The variance of additive noise in the system is varied to conduct the simulation at different SNRs. The SNR and length of training symbol is considered to be same in both stages of channel estimation. Fig. 2 shows MSE for channel estimates against the transmit SNR values for the scenario where training sequence is composed of 60 symbols. These results indicate that proposed secure channel estimation provides robust channel estimates at Bob as MSE of H_{ab} is close to theoretical MSE measured from (15). The MSE of H_{ae} indicates proposed secure channel estimation technique maintains significant equivocation at Eve. In the simulations, MSE at Eve cannot be minimized lower than 10^{-2} because of the limitation of the steepest descent method utilized in blind estimation technique. Finally, the simulation results show that Eve cannot acquire useful channel estimate even with additional antennas and state-of-the-art blind channel estimation algorithm.

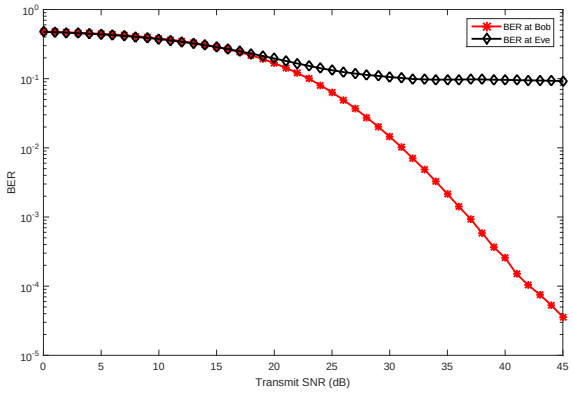

Fig. 4. System BER at Bob and Eve against SNR by utilizing Alamoti-STBC transmission along with proposed channel estimation technique.

To further investigate the performance of our proposed secure channel estimation technique we have performed simu-

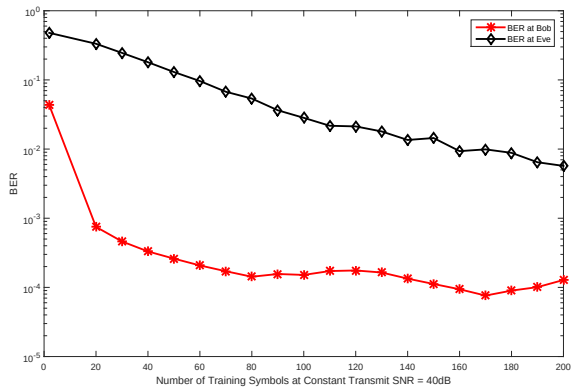

Fig. 5. System BER at Bob and Eve against the length of pilot sequence at constant SNR of 30dB.

lation analysis to study the effect of pilot sequence size on the performance. The results obtained for the MSE for different pilot sequence length are shown in Fig. 3, where the SNR is set to be 30dB in both training stages. These results indicate that increasing the pilot length improves the performance at Eve but the MSE cannot be improved less than 10^{-2} pertaining to the limitations of blind estimation algorithms. These results also indicate some mismatch between theoretical and simulation-based MSE for short length of the pilot symbol sequence, which is caused by the randomness of the noise signal.

To show the impact of the proposed channel estimation techniques on the system BER we have conducted the system level simulation analysis to evaluate the BER at the respective receiver. We have utilized Alamouti transmission strategy for two transmit antennas and one receive antenna. In Alamouti technique channel estimates are required at the receiver only. The results in Fig. 4 indicate that even with the best effort channel estimates Eve can not minimize its BER lower than 10^{-2}.

Fig. 5 shows the effect of pilot sequence length on BER of Bob and Eve, where the SNR is set to be 30dB. The results indicate that BER is reduced by increasing the pilot sequence length because MSE has been decreased with increasing the length. These results imply that the proposed channel estimation technique performs well for the scenarios where channel coherence time is small. The BER results provide the understanding of worst case scenario as additional resources are employed for channel estimation at Eve and physical layer secrecy is not utilized in the transmission of information, still, by using secure channel estimation, the performance at Eve is degraded as compared to Bob. In future, the secure transmission will be considered along with secure channel estimation to provide the better understanding of the proposed channel estimation technique.

V. Conclusions

We have presented a novel two-stage secure channel estimation technique to avoid the leakage of channel estimates to the adversary. We have designed LS-based estimator for self-interference channel estimation in the first stage. In the second stage, LS-based estimator has been presented for inter-node channel estimation in presence of the self-interference. We have analyzed the performance of channel estimation technique by utilizing MSE as the performance metric. Finally, we have presented system level BER analysis by utilizing proposed channel estimation technique to show the impact of securing the channel estimates.

VI. Acknowledgment

This work was supported by Hydro-Quebec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/HydroQuebec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14).

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] Y. Zou and J. Zhu, *Physical-layer security for cooperative relay networks*. Springer, 2016.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[8] 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.

[9] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall International Editions, 1993.

[10] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[11] E. De Carvalho and D. T. Slock, "Cramer-rao bounds for semi-blind, blind and training sequence based channel estimation," in *First IEEE Sig. Processing Workshop on Sig. Processing Advances in Wireless Commun.,*. IEEE, 1997, pp. 129–132.

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

[13] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Commun.*, vol. 16, no. 8, pp. 1451–1458, 1998.