Multiple antenna Physical Layer Security against Passive Eavesdroppers: A Tutorial

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 increasing use of network-connected devices places a higher risk on security and privacy of data. The characteristics of the wireless channel can be employed to provide secrecy in wireless communication, in the form of Physical Layer Security (PLS). This review paper provides a tutorial on practical PLS based on multiple antenna and relay network systems, and identifies current challenges in this important research area. The emphasis is also put on the crucial step of secure channel estimation, as well as discriminatory channel estimation (DCE), without which the practical application of PLS remains limited.**

I. Introduction

The secrecy of communication is crucial to avoid information leakage to potential adversaries. The broadcast nature of wireless communications makes it challenging to provide secure communications. The privacy and security threats in wireless communications are usually classified in three categories: eavesdropping, jamming communication, and malicious data injection. In an eavesdropping attack, the adversary intercepts information that is being communicated over the wireless channel. The eavesdropping attacks result in leakage of potentially critical and private information to the adversary. These attacks can be passive, in which the eavesdropper does not transmit any signal, or active, in which the eavesdropper also transmits its own signal. Passive eavesdropping attacks on wireless networks are most prevalent, as they are easily enabled by the broadcast nature of the wireless channel. This paper is devoted to reviewing the state of the art and current important challenges in the area security against passive eavesdropping attacks, through the use of Physical Layer Security (PLS). Although we review some of the foundational theoretical results, the main focus of this paper is on more practical ways to achieve PLS. The passive nature of the eavesdropper makes this task challenging because it is impossible for the legitimate transmitter/receiver pair to acquire any knowledge regarding the presence or channel characteristics of the eavesdropper.

PLS finds its roots with Claude Shannon [1] and A. D. Wyner [2], whose papers focused on presenting the theoretical limits of achieving secure communication. The utilization of PLS theoretically assures secrecy for certain scenarios as compared to cryptographic techniques, which rely on computation hardness of decoding process to provide security. Furthermore, PLS can be implemented as the additional layer of security in addition to cryptographic techniques to increase secrecy against more sophisticated attacks.

Based on the theoretical foundations of PLS, there have been attempts in the literature to realize PLS by utilizing different signal processing and wireless communications techniques. In this paper, we provide a tutorial on prominent practical PLS techniques and outline the challenges faced by them. We discuss in particular the PLS techniques based on the use of multiple antennas, which can been used to avoid the leakage of information to any adversary. The increases prevalence of multiple antenna systems also offers a good opportunity to exploit these systems to provide PLS. We also review secure communications techniques based on relay and cooperative systems. Finally, recognizing that a key enabler for many multiple-antenna PLS techniques is the lack of ability for the eavesdropper to obtain a good estimate of the legitimate channel, we discuss the important issue of Discriminatory Channel Estimation (DCE).

The remainder of this paper is organized as follows. Section II covers foundations of PLS techniques. Section III describes the specific use of multiple antenna systems for PLS, including in relay and cooperative systems. It also discussed in detail the crucial issue of secure channel estimation. Finally, our conclusion and future work is mentioned in Section IV. This paper follows usual conventions of notation, where vectors are denoted by boldface symbols.

II. Physical Layer Security

Physical layer security uses the physical-layer characteristics (such as diversity or independence) of the wireless channel to achieve secrecy [3]. The basic model usually considered for PLS is shown in Figure 1. In this model, the legitimate transmitter and the receiver exchange information over the main channel, while an eavesdropper passively eavesdrops on their communication via the so-called wiretap channel. By convention, the legitimate transmitter, receiver, and the eavesdropper are commonly referred to as Alice, Bob, and Eve, respectively.

The principle of PLS has been introduced by Claude Shannon in his seminal paper [1]. In [1], Shannon presented a secure communication scheme based on the use of secret keys, in which Alice and Bob share a non-reusable secret key K. Alice has to transmit message M to Bob, so it encodes M

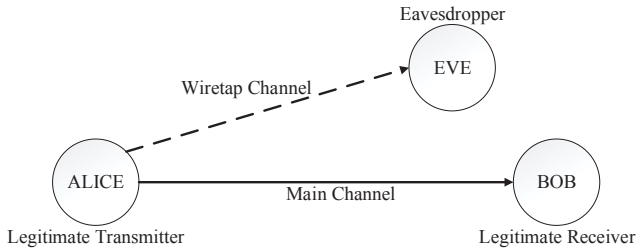

Fig. 1. Basic channel model for physical layer security, comprising of three nodes, namely, Alice (legitimate transmitter), Bob (legitimate receiver), and Eve (eavesdropper).

to codeword X by utilizing the pre-shared secret key K. Eve and Bob both have access to X and it is assumed that all the communication channels are noiseless. For such system, Shannon formulated that information theoretical secrecy is given as $\mathbb{H}(M|X)$, which denotes the entropy of M given X. This is also known as the eavesdropper's equivocation, which can be roughly understood as a measure of the degree to which the eavesdropper is confused. In order to achieve perfect secrecy, the eavesdropper's equivocation must be equal to the a-priori uncertainty about the message M before receiving X, i.e.

$$\mathbb{H}(M|X) = \mathbb{H}(M). \tag{1}$$

This equation implies that knowing *X* does not provide any information regarding message *M*, or *X* is statistically independent of *M*. It also means that for perfect secrecy $I(M|X) = 0$, i.e. that the mutual information between *M* and *X* must be zero. It is also been shown by Shannon that perfect secrecy can be achieved only if: $\mathbb{H}(K) \geq \mathbb{H}(M)$, which means that the entropy of the secret key must be greater than or equal to that of the message. It implies that the length of the secret key must be at least equal to or greater than that of the message being transmitted. To achieve this stringent condition one-time pad coding or Vernam's cipher scheme can be used for secure communication: every data bit is encoded (XORed) with a unique bit from the pre-shared secret key. This makes Shannon's secrecy scheme impractical because of the unrealistic constraints imposed by the generation, utilization, and sharing of a non-reusable secret key and because of the communication overhead involved.

A relaxed condition for secrecy was presented by Wyner [2], in which the wiretap channel is assumed to be a probabilistically degraded version of the main, legitimate channel. This guarantees that the received signal at the eavesdropper is statistically more distorted than the received signal at the legitimate receiver. The wiretap channel model has been used to modify the physical layer coding to increase the secrecy of the communication, using codes referred to as wiretap codes. In the literature, a nested code structure has been used to realize wiretap codes [4]. The major drawback with coding-based secrecy approaches is the requirement of global channel state information at the transmitter, which is nearly impossible to obtain for practical applications, in particular regarding the knowledge by the transmitter of a passive eavesdropper's channel conditions.

Given these limitations, the next section focuses on practical PLS techniques and challenges faced by them.

III. Multiple Antenna Systems for Physical Layer Security

The utilization of multiple antenna systems has drastically increased in the last decade due to the performance improvements they offer. The Multiple Input Multiple Output (MIMO) capabilities are also used to achieve secrecy.

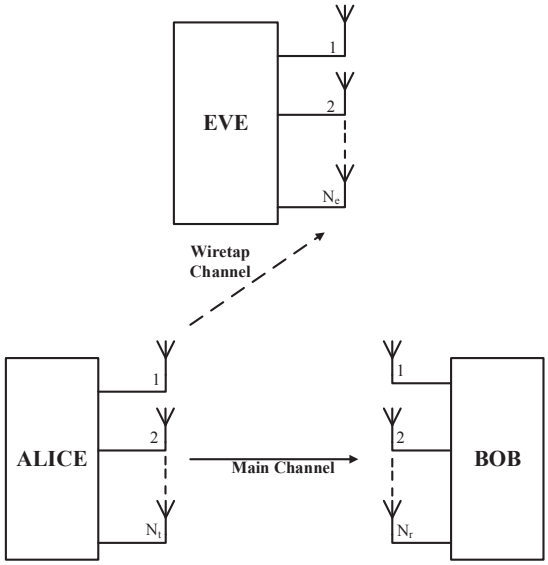

Fig. 2. Basic MIMO wiretap channel comprising of Alice, Bob and Eve with N_t , N_r, and N_e antennas, respectively.

The MIMO channel model considered in the PLS literature is shown in Figure 2. The transmitter features N_t antenna elements and the receiver comprises of N_r antennas. The corresponding channel from Alice to Bob is represented by N_t x N_r matrix $\mathbf{H}_{ab}$. The received signals at Bob $\mathbf{Y}_b$ and eavesdropper $\mathbf{Y}_e$ are given by

$$\begin{aligned} \mathbf{Y}_b &= \mathbf{H}_{ab}\mathbf{X} + \mathbf{n}_b \\ \mathbf{Y}_e &= \mathbf{H}_{ae}\mathbf{X} + \mathbf{n}_e, \end{aligned} \tag{2}$$

where $\mathbf{n}_r$ and $\mathbf{n}_e$ are corresponding noise signals added to each signal, and they are assumed to be zero-mean independent circularly symmetric complex additive white Gaussian noise with variances σ_r^2 and σ_e^2 respectively.

a) Coding-based approaches: The first work on MIMO-based secure communication was presented in [5], where space-time block codes are used to achieve secure communication. The performance metrics used are Low Probability of Intercept (LPI) which imposes a constraint on eavesdropper's channel capacity and Low Probability of Detection (LPD) which constrains the ability of an eavesdropper to detect the presence of the signal. To achieve zero channel capacity for the eavesdropper, it uses precoding based on channel

information regarding the main and wiretap channel. Secrecy is achieved through the fact that the main and wiretap channel are assumed to be independent. For LPD, the transmit SNR is constrained to the channel-averaged Chernoff error exponent, which also results in a sub-optimum communication strategy. The major drawback of this technique is again the assumption regarding the knowledge of the eavesdropper's CSI at the transmitter, which is again impractical in the case of a passive eavesdropper.

b) Artificial Noise: For the cases where the eavesdropper's CSI is not known at the transmitter, artificial noise is used to achieve secrecy [6], [7]. Alice splits its power to transmit data symbol and artificial noise (AN). 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 the legitimate receiver and eavesdropper are given as

$$\begin{aligned} \mathbf{Y}_b &= \mathbf{H}_{ab}\mathbf{X} + \mathbf{H}_{ab}\mathbf{Z} + \mathbf{n}_b \\ \mathbf{Y}_e &= \mathbf{H}_{ae}\mathbf{X} + \mathbf{H}_{ae}\mathbf{Z} + \mathbf{n}_e, \end{aligned} \tag{3}$$

where $\mathbf{Z}$ indicates the AN signal transmitted from the transmitter to induce equivocation at the eavesdropper. Secrecy capacity is used as the performance metric; it is the difference between the capacity of the main channel and the capacity of the wiretap channel:

$$\begin{aligned} C_s &= \max_{\mathbf{Q}_a} I(\mathbf{X};\mathbf{Y}_r) - I(\mathbf{X};\mathbf{Y}_e) \\ &= \max_{\mathbf{Q}_a} \log\,|\mathbf{I} + \mathbf{H}_{ab}\mathbf{Q}_a\mathbf{H}_{ab}^H| - \log\,|\mathbf{I} + \mathbf{H}_{ae}\mathbf{Q}_a\mathbf{H}_{ae}^H|, \end{aligned} \tag{4}$$

where $\mathbf{Q}_a$ is the total covariance of transmitted signal. The aim is to maximize the secrecy capacity given in Equation (4).

A practical secure communication approach based on MIMO beamforming is presented in [8], where authors have described a novel scheme for achieving PLS for the scenario where no CSI is available regarding the eavesdroppers at the legitimate transmitter. It uses ZFBF (Zero-Forcing Beam-Forming) present in 802.11ac standard to generate multiple orthogonal blinding streams. The optimal weight $\mathbf{W}$ for pre-coding corresponds to the pseudo-inverse of channel matrix $\mathbf{H}$ as:

$$\mathbf{W} = \mathbf{H}^{\dagger} = \mathbf{H}^H \left(\mathbf{H}\mathbf{H}^H\right)^{-1}. \tag{5}$$

The transmitter uses a single stream to transmit the data, and all the other streams are used to transmit the orthogonal blinding streams. A Gramm-Schimdt orthogonalization process is used to create pseudo channel matrix $\mathbf{H}^{'}$, which contains the legitimate receiver's channel vector $\mathbf{H}_{ab}$ along with the pseudo channel vectors orthogonal to the legitimate receiver's channel. In a first step, $\mathbf{H}_{ab}$ is padded with a truncated (M-1)xN identity matrix $\mathbf{I}$ to obtain matrix $\bar{\mathbf{H}}$, which is called the preliminary channel. Then, Gram-Schmidt orthogonalization is performed on the preliminary channel matrix as described in [8] to get $\mathbf{H}^{'}$. Afterwards, pre-coding is performed using the pseudo channel matrix $\mathbf{H}^{'}$ used instead of $\mathbf{H}$ in equation (5). These blinding streams comprise of artificial noise which is orthogonal to the legitimate receiver's channel. The random symbols are transmitted on these orthogonal streams to decrease the received Signal to Interference plus Noise Ratio (SINR) at the eavesdroppers. Experimental results [8] confirm this SINR performance using WARP (Wireless Open Access Research Platform) nodes at RICE University.

MIMO beamforming based schemes provide an attractive opportunity for practical PLS as most communication systems have multiple antennas available at their disposal, but a primary condition for them to work is the spatial independence of channels among users. In practice, the channels can also be correlated, depending on the location of Eve. Additionally, the major challenge of MIMO PLS techniques is their dependence on channel estimates [9]. For an optimized system, the channel estimates of Eve are also required, which is not possible. Even for blind jamming schemes, the channel estimates for Bob must be accurate otherwise the AN signal would interfere with Bob's signal. Another crucial challenge with such schemes is the secrecy of channel estimates because if Eve can get hold of these estimates, then the information can be compromised by utilizing known plain-text attacks [10], which means that channel estimates are critical in achieving secrecy. The importance of channel estimates for multiple antenna based secure communication emphasizes that secure channel estimation is required for secrecy in MIMO beamforming schemes.

A. Relay and Cooperative Methods for Secrecy

Physical layer cooperation has been widely used in wireless communication systems to efficiently use the scarce resource that is the wireless bandwidth. It does so by attempting to mimic the multiplexing and diversity gains of multiple antenna systems without employing multiple antennas at individual nodes [11]. A relay network generally comprises of a source, destination, and relays. The relay nodes cooperate with the source by transmitting the message to the destination. Relays have also been used in the literature to achieve secrecy. Existing systems can typically be classified into two categories [12], namely *trusted relays*, and *untrusted relays*.

In schemes based on *trusted relays*, the relay nodes help the legitimate transmitter to achieve secrecy. In [13], the message is decoded at the relay node, after what an Artificial Noise (AN) signal independent of the decoded secure message is transmitted by the relay. The AN signal induces the required equivocation at the eavesdropper. In such scenario, the relay node is assumed to have full CSI regarding the legitimate receiver to generate AN orthogonal to the secure channel. The joint optimization of AN beamforming is considered in [14], [15], where the relay optimizes its power allocation between AN and legitimate signal transmission. Full-duplex (FD) relays have been used to maximize the secrecy rate in [16]: The relay node transmits jamming signal while utilizing the FD capabilities to simultaneously receive the information from the source. It is assumed that the relay knows perfectly the CSI of the eavesdropper, which enables it to optimize the AN signal. In this context, the transmitter and receiver are assumed to be single antenna half-duplex systems.

Untrusted relays cooperate in transmitting the message to the destination while eavesdropping on the data [17]. There are multiple techniques where the information can be concealed from the relay node to achieve secrecy. In [18], the authors have proposed the utilization of amplify-and-forward (AF) cooperation scheme only, as in this case the relay node only amplifies the received signal and forwards it. The signal is not decoded at the relay so no eavesdropping can possibly be done, but this approach is based only on the ethical imposition that relays will not attempt to decode the data. To overcome this shortcoming authors have proposed the utilization of a full-duplex destination, which forwards a jamming signal towards the relay while the source is transmitting. The known jamming signal is afterward subtracted from the signal received from the relay. Joint beamforming based secure communication in the presence of untrusted relays is presented in [19].

The major challenges faced by cooperative jamming schemes are the high transmission overhead and the complexity. The transmission of a jamming signal requires power and bandwidth, which are critical resources in every wireless network. These schemes also require robust channel estimates for beam-forming so that nulling can be achieved at Eve. The channel estimation process can be compromised as Eve is also able to receive pilot training symbols. These challenges render relay-based secrecy schemes impractical but provide opportunity to further explore the use of relay networks.

B. Discriminatory Channel Estimation for Physical Layer Security

As we have shown above, channel estimation is an important aspect of many PLS schemes, be it because an accurate estimate of the legitimate channel is required at the transmitter, or because the legitimate channel state information is required not to be known at the eavesdropper. DCE is a technique where channel estimation performance at the eavesdropper is intentionally degraded as compared to the legitimate receiver. DCE provides the basis for any other security scheme especially multiple antenna based techniques, as they rely on the absence of channel estimates at Eve. The existing techniques in DCE are based on insertion of AN signal along with training signal to achieve ambiguity at Eve. The most prevalent schemes proposed for DCE are feedback-and-retraining [20] and two-way training [21]. These schemes use a rough estimation stage followed by AN-assisted secure training stage.

The system model is the same as mentioned in the previous section for multiple antenna systems: Figure 2 shows the basic channel model used in DCE schemes. First, we consider the feedback-and-retraining training scheme [20]; it comprises of two stages. In the first stage, the power of the training signal is controlled to limit the estimation performance at the receiving nodes; these estimates are known as the rough channel estimates. The training signal sent by Alice is given as

$$\mathbf{X}_0 = \sqrt{\frac{P_0 T_0}{N_t}}\mathbf{C}_0, \tag{6}$$

where $\mathbf{C}_0 \in \mathbb{C}^{T_0 \times N_t}$ is the pilot signal matrix satisfying $\mathrm{Tr}(\mathbf{C}_0^H \mathbf{C}_0) = N_t$, P_0 indicates the pilot signal power, and T_0 is the training length. So, the received signals at Bob $\mathbf{Y}_{b0}$ and Eve $\mathbf{Y}_{e0}$ are given as:

$$\mathbf{Y}_{b0} = \mathbf{X}_0\mathbf{H}_{ab} + \mathbf{n}_b \tag{7}$$

$$\mathbf{Y}_{e0} = \mathbf{X}_0\mathbf{H}_{ae} + \mathbf{n}_e, \tag{8}$$

where $\mathbf{H}_{ab}$ and $\mathbf{H}_{ae}$ correspond to the channel matrix between Alice-Bob, and Alice-Eve respectively. $\mathbf{n}_b$ and $\mathbf{n}_e$ are the corresponding AWGN during the initial stage. Based on these observations Bob estimates the channel $\hat{\mathbf{H}}_{ab0}$ via Linear minimum mean square estimation (LMMSE) and sends the channel estimates back to Alice. These channel estimates are of critical importance, as the precoding weights in the second stage are based on them. Eve can intercept these channel estimates; if these estimates are accurate enough, Eve can try and use them for cancellation of artificial noise to acquire robust channel estimates. Note that one of the aspects that the authors in [20] do not consider is the problem of secure transmission of these channel estimates.

The second stage is known as the feedback-and-retraining stage. In this stage, the rough estimate $\hat{\mathbf{H}}_{ab0}$ received from Bob in the first stage is used by Alice to place some AN in the null space of Alice-Bob channel $\mathbf{H}_{ab}$. The signal transmitted by Alice in this stage is given as:

$$\mathbf{X}_1 = \sqrt{\frac{P_1 T_1}{N_t}}\mathbf{C}_1 + \mathbf{Z}_1\mathbf{K}^{\mathbf{H}_{ab}}_{\hat{\mathbf{H}}_{ab0}}, \tag{9}$$

where $\mathbf{C}_1$ is the training signal, $\mathbf{K}^{\mathbf{H}_{ab}}_{\hat{\mathbf{H}}_{ab0}}$ is the precoding matrix based on $\hat{\mathbf{H}}_{ab0}$ for AN $\mathbf{Z}_1$. In this scenario, special care should be taken in determining the AN power as the channel estimates are not robust. Finally the received signals at Bob and Eve are given as:

$$\mathbf{Y}_{b1} = \mathbf{X}_1\mathbf{H}_{ab} + \mathbf{n}_{b1} \tag{10}$$

$$\mathbf{Y}_{e1} = \mathbf{X}_1\mathbf{H}_{ae} + \mathbf{n}_{e1}. \tag{11}$$

These pilot symbols are used in estimating the channel coefficients by using LMMSE. The AN provides us the guarantee that the channel estimates at Bob are better as compared to Eve. This concept is further elaborated with k retraining stages to improve the channel estimates. In each i stage, the channel estimate $\hat{\mathbf{H}}_{ab(i-1)}$ of the previous $(i-1$-th) stage is used to add the AN, where $i = 1, 2, ...k$ indicates the current retraining stage. The major drawback of this technique is high bandwidth requirement for k retraining stages.

The other notable DCE scheme is the two-way training scheme, where Bob sends the initial training signal instead of Alice; it is most efficient for reciprocal channel scenarios because Alice can estimate the Alice-Bob channel due to reciprocity without leaking any information regarding Alice-Eve channel This scheme also comprises of two stages. In the first stage, Bob transmits a pilot signal to provide reverse channel estimate to Alice. This information can also be overheard by Eve, but it will not provide any advantage as it will provide to Eve the Bob-Eve channel information which is not

useful. In the second stage, AN is added to the null space of the estimated channel. This stage provides refinement to the channel estimates obtained in the initial stage. This scheme also considers non-reciprocal channels where an additional round trip training signal is echoed from Alice. The reverse training stage is the same as in the case of reciprocal channels. In the second stage, Alice transmits a training signal known to itself only. The signal received by Bob is retransmitted back after amplification. Finally, as the signal received at Alice from Bob has channel components of both forward and reverse channels, Alice acquires a rough estimate of the forward channel, as the reserve channel is already known to Alice. The estimate is mentioned as a rough estimate because it contains noise from multiple receivers and other distortions. In the third stage, AN is added to the transmitted training signal, based on the forward channel estimates from the previous stage.

The authors in [22] have presented a novel semi-blind two-way training scheme. They have considered reciprocal channels only. In their design, the reverse training signal is a random whitening sequence. The scheme has two stages, where, in the first stage, Bob transmits a random whitening sequence for reverse channel estimation. The random training sequence helps in prevention of pilot contamination attacks where an adversary jams the part of known pilot signal to deteriorate the performance of channel estimation. Alice uses Whitening Rotation based semi-blind estimation. In the second stage, AN is inserted in the pilot signal as mentioned in the two-way training scheme. The forward channel estimates are refined in the second stage by utilizing pilot based estimation.

The design of AN specifically for DCE is considered in [23]. This design is based on the joint optimization of AN covariance matrix, pilot signal power, and linear estimation at Bob. In [24], an antenna grouping strategy is considered to relax the condition of a higher number of transmit antennas as compared to receiver or eavesdropper. In case Bob has a larger number of antennas than Alice, they are grouped and each antenna group has a dedicated DCE turn. The proposed scheme uses variable length pilots, based on the ratio of total number of antenna to the number of turns.

DCE is also considered for MIMO decode-and-forward cooperative systems in [25]. In the first phase, the source node transmits an omnidirectional AN signal, while the 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 AN signal into the null space of the relay-destination channel, based on channel estimation in the first phase. Finally, the authors have presented optimization for power allocation between training signals and AN. In [9], the impact of CSI on MIMO beam-forming based secrecy schemes has been studied. The authors have also considered the impact of CSI leakage on secrecy capacity. A two-way training scheme has been used to perform DCE. The results indicate that DCE has superior secrecy rate as compared to the conventional channel estimation techniques. Finally, the same paper shows that DCE provides better secrecy capacity than other PLS techniques while maintaining lower communication overhead. In [26], authors have used full-duplex transmissions from Bob to provide secure communications. A secure channel training technique has been used for estimation of self-interference channel at Bob, by using a private training sequence known to Bob only. In the data transmission stage, Alice transmits the data stream while Bob transmits AN to Eve. The AN from Bob generates the required equivocation at Eve, as the channel from Bob to Eve is unknown at Eve.

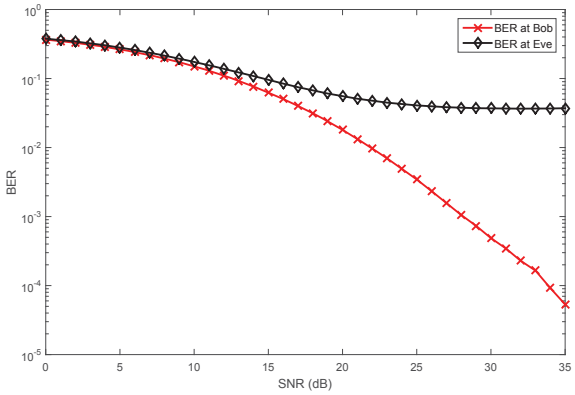

Fig. 3. System BER at Bob and Eve against SNR by utilizing Alamouti-STBC transmission along with proposed channel estimation technique.

The literature review mentioned above indicates that channel estimates play a critical role in the secrecy of the system. The utilization of DCE is critical in securing the leakage of channel estimates. The feedback-and-retraining based DCE schemes ignore the scenarios where Eve can acquire robust channel estimates despite the limited power. Similarly, two-way training based DCE schemes are based on reciprocal channels, and the round trip retraining for non-reciprocal channel estimation suffers from noise amplification. To overcome these drawbacks, It is possible to use full-duplex communication in [27], where Alice and Bob use in-band full-duplex transmissions to estimate their respective channels while maintaining equivocation at Eve. The secure estimation process is completed in two stages: first, self-interference channels are estimated, followed by estimation of the inter-node channels. For estimation of the self-interference channel,a private training sequence known to respective nodes only has been used. Least-Squares (LS) estimation is used at legitimate nodes whereas, at Eve, pilot based estimation techniques can not be employed as the training sequence is not known at Eve; blind channel estimation techniques should be employed at Eve for estimation of channels between Alice and Bob to Eve, which does not perform at par with pilot based techniques [26]. In the second stage, in-band full-duplex training signals are transmitted from both legitimate nodes for estimation of the channel between Alice and Bob. The legitimate nodes perform the LS estimation while performing self-interference cancellation based on estimates acquired in the first stage. Eve also attempts to estimate the channel based on channel estimates acquired by

blind estimation during the first stage. To analyze the secrecy performance, we have considered multiple antenna systems as shown in Figure 2. The channel estimation is based on the proposed secure channel estimation technique followed by Alamouti's Space Time Block Code (STBC) transmission for two transmit antennas and one receive antenna. The Bit Error Rate (BER) at Bob and Eve indicate that, in this example, Eve can not minimize its BER lower than 10^{-2}.

DCE-based techniques provide an attractive opportunity to provide secure communication with less overhead as compared to other AN-based techniques, because they add AN only in the channel estimation phase. The DCE based techniques are still in their infancy and require robust theoretical analysis to establish for instance lower bounds on performance.

IV. Conclusion

This paper provides a tutorial regarding the PLS and emerging practical techniques used to achieve secrecy. The MIMO based techniques provide solutions to the numerous existing challenges in PLS. Relay networks can also assist in securing the communication between legitimate pair. However, the dependence of multiple antenna and relay based secrecy techniques on robust channel estimates is their vulnerability. The utilization of secure channel estimates techniques promise solutions for robust secure communications. The DCE based techniques have potential to provide practical PLS. Quantitative studies are required to compare the performance of DCE with other secrecy techniques. Further work should also aim to combine DCE with MIMO based secrecy techniques to provide robust and secure communication.

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

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

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

[4] 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.

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

[6] 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.

[7] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On Artificial-Noise Aided Transmit Design for Multi-User MISO Systems with Integrated Services," *IEEE Trans. on Vehicular Technology*, vol. 66, no. 9, pp. 8179–8195, 2017.

[8] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE Int. Conf. on Computer Commun. (INFOCOM 12)*, Mar. 2012, pp. 720–728.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] M.-N. Nguyen, N.-P. Nguyen, D. B. Da Costa, H.-K. Nguyen, and R. T. De Sousa, "Secure Cooperative Half-Duplex Cognitive Radio Networks With k-th Best Relay Selection," *IEEE Access*, vol. 5, pp. 6678–6687, 2017.

[16] 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.

[17] G. Luo, J. Li, Z. Liu, X. Tao, and F. Yang, "Physical Layer Security with Untrusted Relays in Wireless Cooperative Networks," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 17)*, Mar. 2017, pp. 1–6.

[18] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Information Theory*, vol. 57, no. 1, pp. 137–155, 2011.

[19] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *IEEE Trans. Signal Processing*, vol. 60, no. 1, pp. 310–325, 2012.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, "Channel training design in full-duplex wiretap channels to enhance physical layer security," in *Proc. IEEE Int. Conf. on Commun. (ICC 17)*, May 2017, pp. 1–6.

[27] F. Ud Din and F. Labeau, "Physical layer security through secure channel estimation," in *Proc. IEEE 87th Vehicular Technology Conference (VTC 18-Spring) In-Press*, June 2018.