Achieving Secure Communication Through Pilot Manipulation

Morteza Soltani*, Tunçer Baykaş*, Hüseyin Arslan*,
*School of Engineering and Natural Sciences, Istanbul Medipol University,
Istanbul, Beykoz, 34810, Turkey.

***Abstract*—Raising concerns about the security of wireless communication led researchers develop new concepts to keep information secret from eavesdroppers. Among them, physical layer security relies on the features of the wireless channels. Most of the work in physical layer security does focus on data transmission. On the other hand the focus of this work is to use manipulation of pilot tones to enhance communication security and to reduce eavesdroppers' ability to estimate the wireless channel. Particularly, we are introducing two novel algorithms, which manipulate pilot tones according to legitimate channels' phase and amplitude characteristics. Both algorithms decrease the channel estimation quality of the eavesdropper considerably, while the amplitude based algorithm provides high quality reception at the legitimate receiver. We provide resulting pilot error rates due to proposed algorithms. In addition, we show the effect of threshold selection to channel estimation quality both at the legitimate receiver and eavesdropper.**

***Index Terms*—Physical Layer Security, channel estimation, eavesdropping, pilot manipulation, communication secrecy.**

I. Introduction

Wireless communications enable reaching multiple parties simultaneously. However, due to this property wireless networks are vulnerable to eavesdropping of unauthorized receivers. With our daily lives becoming more and more dependent on wireless communications to transfer critical data such as business deals, financial transactions or health information, security of the data during transmission becomes critical. Efforts to keep information secret from malicious eavesdroppers started long before radio communications. Many methods are developed such as encryption of the data using secret keys shared between users and stenography i.e. watermarking, which are used in wireless communications as well. On top of all of these protection schemes, system designers envision to use the properties of the wireless communications to enhance security. Such methods are termed as physical layer security.

The main proposition of physical layer security is enabling secure communication, without exclusively using encryption at higher layers. This can be achieved primarily in two ways: by developing secret keys from the very nature of the wireless communication medium or by designing transmission methods which limits the information at the eavesdropper [1]. Shannon laid foundations of the theory of secrecy with his 1949 paper entitled "Communication theory of secrecy systems" [2]. Shannon studied a secure communication system, which is based on secret-key encryption. According to the paper, secrecy capacity exists only if the entropy of the secret key is equal or larger than the entropy of the message itself without taking the computational resources of the malicious eavesdropper into account.

For the case of exploiting the random nature of wireless channels, Koorapaty *et al.* relied on the independence of the channels between transmitter/receiver and transmitter/eavesdropper to use the phase of the fading coefficients as a secret key [3]. In [4] key generation process is performed by benefiting from the unique level crossing rates of the fading processes at the legitimate terminals. Authors in [5] proposed a secret key generation by discretization of wireless multipath coefficients. In [6] and [7], authors use channel state information shared between transmitter and legitimate receivers as a secret key to interleave either the modulated symbols associated with a selected number of subcarriers or to interleave subcarriers themselves.

On the other hand, Wyner showed that secure communication is possible without sharing any secret keys but using intelligent transmission schemes [8]. As an example, one many inject artificial noise to degrade the channel condition of the eavesdropper [9]–[13].

The aforementioned techniques aim to guarantee secrecy in the data transmission phase. It is possible to discriminate the channel estimation performances at legitimate receivers and eavesdroppers. Authors in [14] proposed the insertion of artificial noise during transmission of pilot symbols to degrade the channel estimation performance at the eavesdropper.

Our novel contribution in this paper is to degrade eavesdroppers ability during channel estimation phase without introducing artificial noise. More specifically, by manipulating the pilot symbols based on the channel state information shared between legitimate parties, we propose power efficient algorithms by which intended receiver is able to estimate the channel correctly while eavesdropper estimates its own channel erroneously, thus guaranteeing performance discrimination between the legitimate receiver and the eavesdropper.

The rest of the paper is organized as follows: Section II introduces system model. In Section III we describe proposed algorithms. The simulation results are presented in Section IV, and Section V concludes the paper.

II. System Model

We consider an OFDM system that consists of a legitimate transmitter (Alice), a legitimate receiver (Bob), and a passive Eavesdropper (Eve) as shown in Fig. 1.

978-1-4673-6782-0/15/$31.00 ©2015 IEEE

The forward and reverse channels between legitimate users are assumed to occupy the same frequency band and remain constant over several time slots. Hence, Alice and Bob would experience and observe identical channels based on the reciprocity property of wireless channels [15]. We assume that Eve does not posses any information about the legitimate channel because the channel response is unique to the location of the transmitter and receiver as well as the environment. More specifically, a rich scattering environment is assumed and the condition of Eve being at least a couple of wavelengths farther from Bob is also fulfilled.

Assuming the frequency domain OFDM symbol $\mathbf{x} \in \mathbb{C}^{N\times 1}$ is transmitted from Alice, the signals received by Bob and Eve are denoted by $\mathbf{y_B} \in \mathbb{C}^{N\times 1}$ and $\mathbf{y_E} \in \mathbb{C}^{N\times 1}$, respectively, where N indicates the number of subcarriers. In the received vectors, the kth element $(k = 0, 1, \cdots, N-1)$ corresponds to the kth subcarrier. The received signal vectors are given by

$$\begin{aligned} \mathbf{y_B} &= \mathbf{H_B x} + \mathbf{w_B} \\ \mathbf{y_E} &= \mathbf{H_E x} + \mathbf{w_E} \end{aligned} \tag{1}$$

where $\mathbf{H_B} \in \mathbb{C}^{N\times N}$ and $\mathbf{H_E} \in \mathbb{C}^{N\times N}$ denote corresponding channels, $\mathbf{w_B} \in \mathbb{C}^{N\times 1}$ and $\mathbf{w_E} \in \mathbb{C}^{N\times 1}$ denote circularly symmetric complex Gaussian noise vectors with zero mean and variances σ_B^2 and σ_E^2 at Bob and Eve. Assuming that the cyclic prefix (CP) is longer than the delay spread, channel matrices $\mathbf{H_B}$ and $\mathbf{H_E}$ become diagonal with diagonal entries being $\{H_B(0), H_B(1), \cdots, H_B(N-1)\}$ and $\{H_E(0), H_E(1), \cdots, H_E(N-1)\}$.

We assume that communication starts with an OFDM symbol containing pilot subcarriers followed by data OFDM symbols. The channel estimation results derived from the first OFDM symbol is used to detect data symbols. We assume that both Bob and Eve are relying on pilot symbols for channel estimation. As a result blind channel estimation or data directed channel estimation are out of the scope of this paper. Among channel estimation methods which rely on pilot symbols, we consider the performances of Least Squares (LS) and Minimum Mean Square Error (MMSE) channel estimation methods. The estimation of pilot signals based on LS method is given by

$$\begin{aligned} \widetilde{H}_B(k,k) &= \frac{Y_B(k)}{X(k)} = H_B(k) + \frac{W_B(k)}{X(k)} \\ \widetilde{H}_E(k,k) &= \frac{Y_E(k)}{X(k)} = H_E(k) + \frac{W_E(k)}{X(k)} \end{aligned} \tag{2}$$

where $\widetilde{H}_B(k,k)$ and $\widetilde{H}_E(k,k)$ are the diagonal entries of channel matrices, $Y_B(k)$ and $Y_E(k)$ are the received pilot symbol at the kth subcarrier, $W_B(k)$ and $W_E(k)$ denote the additive noise in frequency domain and the pilot symbols are assumed to be $X(k) = 1$ for all k.

Let $\widetilde{\mathbf{H}}_\mathbf{B}$ and $\widetilde{\mathbf{H}}_\mathbf{E}$ denote the diagonal matrices containing estimated channel coefficients obtained in (2). The estimated channel coefficients obtained via MMSE channel estimation at Bob and Eve are equal to:

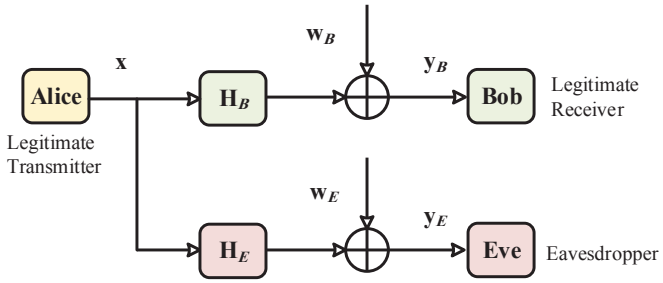

Fig. 1: System model consisting of legitimate transmitter (Alice) and receiver (Bob), and eavesdropper (Eve) with multipath fading channels.

$$\begin{aligned} \widehat{\mathbf{H}}_\mathbf{B} &= \mathbf{R}_{\mathbf{B}\widetilde{\mathbf{B}}}(\mathbf{R_{BB}} + \frac{\sigma_\mathbf{B}^2}{\sigma_\mathbf{x}^2}\mathbf{I_N})^{-1}\widetilde{\mathbf{H}}_\mathbf{B} \\ \widehat{\mathbf{H}}_\mathbf{E} &= \mathbf{R}_{\mathbf{E}\widetilde{\mathbf{E}}}(\mathbf{R_{EE}} + \frac{\sigma_\mathbf{E}^2}{\sigma_\mathbf{x}^2}\mathbf{I_N})^{-1}\widetilde{\mathbf{H}}_\mathbf{E} \end{aligned} \tag{3}$$

where $\sigma_\mathbf{x}^2$ denotes the variance of the pilot symbols, $\mathbf{R_{BB}}$, $\mathbf{R_{EE}}$ are auto-covariance matrices and $\mathbf{R}_{\mathbf{B}\widetilde{\mathbf{B}}}$, $\mathbf{R}_{\mathbf{E}\widetilde{\mathbf{E}}}$ are cross-covariance matrices between the estimated and perfect channel state information at Bob and Eve respectively.

III. Pilot Manipulation Algorithms

We are proposing two algorithms to enhance communication secrecy. In both algorithms, pilots are manipulated according to the previous subcarrier's instantaneous channel information that are observed at the side of Alice. To enable these algorithms, first Bob broadcasts a signal which includes OFDM pilot symbol to Alice.

The received pilots inside the OFDM symbol denoted by $X[k]$ are used to estimate the channel. The LS estimation at Alice $\widehat{\mathbf{H}}_{\mathbf{A,LS}}$ is equal to

$$\begin{aligned} H_A(k,k) &= \frac{Y_A(k)}{X(k)} \\ \widetilde{\mathbf{H}}_{\mathbf{A,LS}} &= diag\{H_A(k,k)\} \end{aligned} \tag{4}$$

and MMSE estimation $\widehat{\mathbf{H}}_{\mathbf{A,LMMSE}}$ is equal to

$$\widehat{\mathbf{H}}_{\mathbf{A,MMSE}} = \mathbf{R}_{\mathbf{A}\widetilde{\mathbf{A}}}(\mathbf{R_{AA}} + \tfrac{\sigma_\mathbf{A}^2}{\sigma_\mathbf{x}^2}\mathbf{I_N})^{-1}\widetilde{\mathbf{H}}_\mathbf{A} \tag{5}$$

First algorithm is based on the phase of the pilot tones whereas the second one is based on the amplitude of the pilot tones. We provide detailed descriptions in following subsections.

A. Phase-Based Pilot Manipulation

For phase-based pilot manipulation, the instantaneous channel phase of each subcarrier is compared with a properly selected thresholds Λ. In order to maximize the unpredictability during eavesdropping, pilots from Alice should have equal chance of being manipulated or not. As channel estimates $\widehat{\mathbf{H}}_{\mathbf{A,LS}}$ and $\widehat{\mathbf{H}}_{\mathbf{A,MMSE}}$ in (4),(5) follows a zero-mean com-

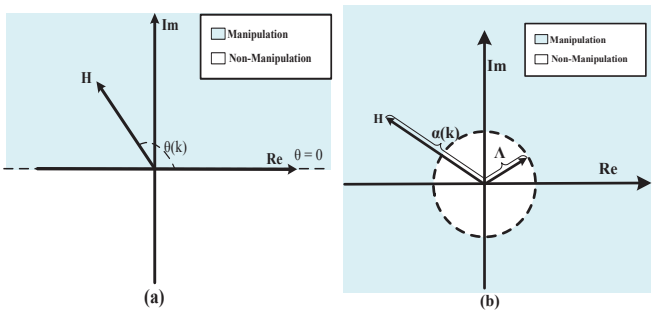

Fig. 2: Pilot manipulation decision regions.

plex Gaussian distribution, the estimated channel phase vector, $\{\hat{\theta}_A(0), \hat{\theta}_A(1), \cdots, \hat{\theta}_A(N-1)\}$, are i.i.d uniformly distributed variables over $[-\pi, \pi]$. Therefore, the threshold can be selected as: $\Lambda = 0$. After estimating the channel, Alice manipulates the pilots according to the following equation

$$\hat{X}[k] = \begin{cases} X[k] & k = 0 \\ jX[k] & \hat{\theta}_A[k-1] > 0, k \neq 0, \\ X[k] & \hat{\theta}_A[k-1] < 0, k \neq 0 \end{cases} \tag{6}$$

where vector $\hat{\mathbf{x}} = [\hat{X}(0), \hat{X}(1), \cdots, \hat{X}(N-1)]$ includes manipulated pilots, $\hat{\theta}$ is the channel phase vector of the estimated channel and $k = 0, 1, \cdots, N-1$. Decision regions for phase-based pilot manipulation are shown in Fig. 2(a).

The received OFDM signals containing manipulated pilots at Bob and Eve are equal to:

$$\begin{aligned} \hat{\mathbf{y}}_\mathbf{B} &= \mathbf{H}_\mathbf{B}\hat{\mathbf{x}} + \mathbf{w}_\mathbf{B} \\ \hat{\mathbf{y}}_\mathbf{E} &= \mathbf{H}_\mathbf{E}\hat{\mathbf{x}} + \mathbf{w}_\mathbf{E} \end{aligned} \tag{7}$$

Since the first pilot is not manipulated as indicated in (6), Bob estimates the channel coefficient of the first pilot using (2) and compares the phase of the estimate with the threshold for demanipulation of the the following pilot. General equation for pilot demanipulation is shown below:

$$\hat{\hat{X}}[k] = \begin{cases} \hat{X}[k] & k = 0 \\ -j\hat{X}[k] & \hat{\theta}_B[k-1] > 0, k \neq 0 \\ \hat{X}[k] & \hat{\theta}_B[k-1] < 0, k \neq 0 \end{cases} \tag{8}$$

After demanipulation of the pilots, if necessary the MMSE channel estimation methods shown in (5) is used.

The probability that Bob and Alice disagree on whether a pilot is manipulated or not, $p_{Er,\theta}(k)$, can be given as

$$\begin{aligned} p_{Er,\theta}(k) = &\frac{1}{2}P(\hat{\theta}_A(k) > 0, \hat{\theta}_B(k) \leq 0) \\ &+ \frac{1}{2}P(\hat{\theta}_A(k) \leq 0, \hat{\theta}_B(k) > 0) \end{aligned} \tag{9}$$

where $k = 1, 2, \cdots, N-1$.

In the next subsection we explain amplitude-based manipulation.

B. Amplitude-Based Pilot Manipulation

The algorithm for amplitude-based manipulation is as follows:

$$\hat{X}[k] = \begin{cases} X[k] & k = 0 \\ jX[k] & \hat{\alpha}_A[k-1] > \Lambda, k \neq 0 \\ X[k] & \hat{\alpha}_A[k-1] < \Lambda, k \neq 0 \end{cases} \tag{10}$$

where $\hat{\alpha}_A$ is the estimated channel amplitude vector and Λ is the threshold for manipulation decision as shown in Fig. 2(b).

Similar to the phase-based algorithm the demanipulation algorithm performed by Bob is equal to:

$$\hat{\hat{X}}[k] = \begin{cases} \hat{X}[k] & k = 0 \\ -j\hat{X}[k] & \hat{\alpha}_B[k-1] > \Lambda, k \neq 0 \\ \hat{X}[k] & \hat{\alpha}_B[k-1] < \Lambda, k \neq 0 \end{cases} \tag{11}$$

The pilot error rate for this case can be calculated by the probability of the following event:

$$\begin{aligned} p_{Er,\alpha}(k) = &\frac{1}{2}P(\hat{\alpha}_A(k) > \Lambda, \hat{\alpha}_B(k) \leq \Lambda) \\ &+ \frac{1}{2}P(\hat{\alpha}_A(k) \leq \Lambda, \hat{\alpha}_B(k) > \Lambda) \end{aligned} \tag{12}$$

where $k = 1, 2, \cdots, N-1$.

We investigate effects of different threshold values on Bob and Eve's reception performance in the next section, which includes simulation results.

IV. Simulation Scenarios and Results

In our simulations, we assume a 10-tap quasistatic Rayleigh fading channel. The modulation scheme is chosen to be QPSK.

The first results are acquired for the phase-based pilot manipulation algorithm and are shown in Fig. 3. Both LSE and MMSE channel estimation methods are utilized at Bob and Eve. Although not shown, the performance at Eve is the same for both methods and error floor at a BER of 0.2 is observed.

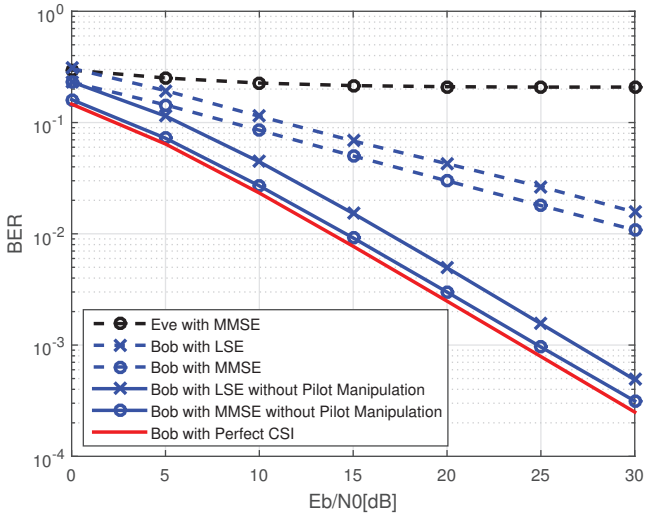

Fig. 3: Bit Error Rate performance of different channel estimation with phase-based pilot manipulation.

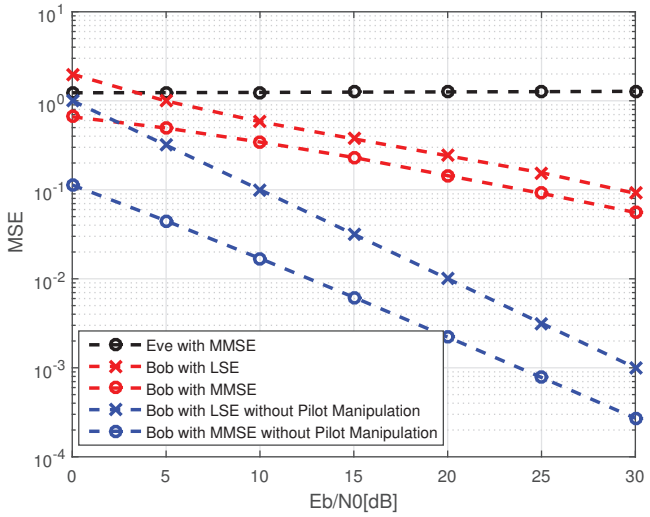

Fig. 4: Average Mean Square Error of different channel estimation with phase-based pilot manipulation.

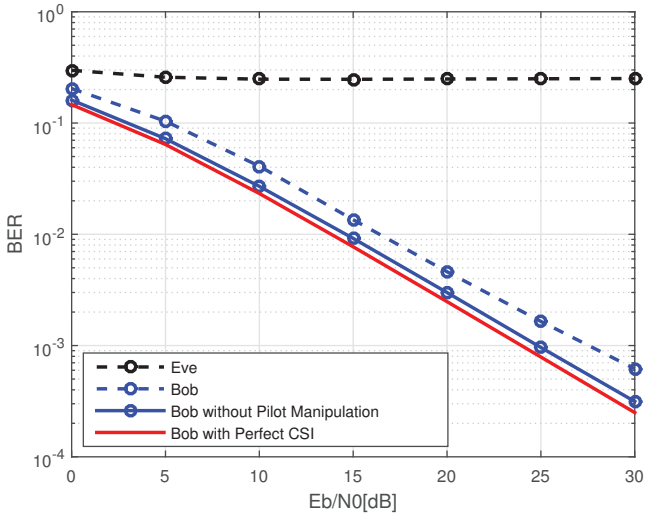

Fig. 6: Bit error rate performance with amplitude-based pilot manipulation with MMSE channel estimation.

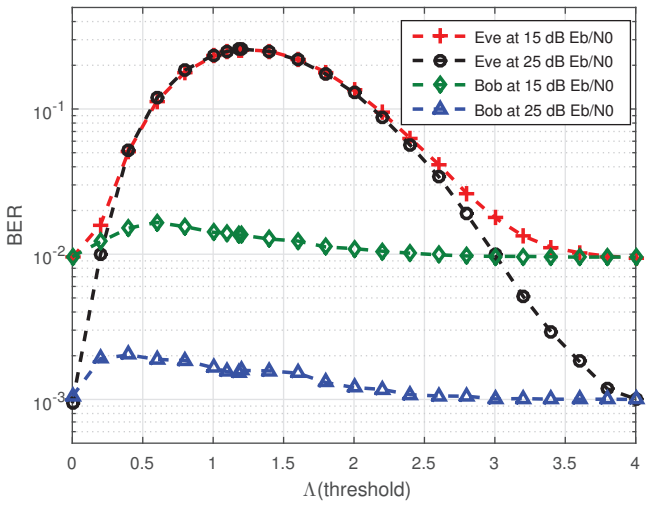

Fig. 5: Bit Error Rate Performance versus different threshold values at 15 and 25 dB E_b/N_0.

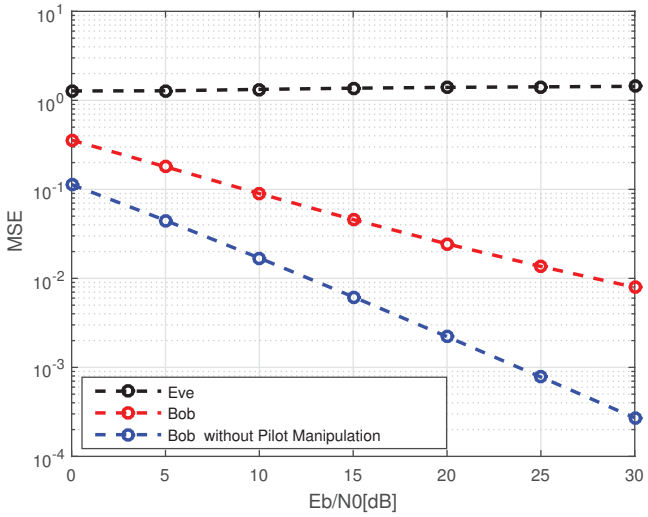

Fig. 7: Average Mean Square Error with amplitude-based pilot manipulation and MMSE channel estimation.

The algorithm is successful to decrease the BER performance at Eve. For Bob, MMSE channel estimation performs better than LSE channel estimation, however its performance is still unacceptable, when compared to BER performance without using the pilot manipulation algorithm.

Fig. 4 depicts the mean square error at the receivers of Bob and Eve. As expected Eve's performance is the worst. The mean square error performance at Bob's receiver follows the BER performances shown in the Fig. 3. The use of the phase-based algorithm increases BER and MSE in such a level that it would be illogical to be used at the legitimate receiver.

The second set of simulations are obtained for amplitude-based pilot manipulation algorithm. Unlike the phase-based, for which selecting the threshold value was straightforward, for the amplitude-based algorithm determining the right threshold is essential. For this purpose, we obtained BER performance at 15 and 25 dB $Eb/N0$ for Bob and Eve with different threshold values for normalized amplitude values. Since Rayleigh Fading channel is simulated, normalization results in Gaussian distributed in-phase and quadrature components with variances equal to 0.5. With the results shown in Fig. 5, we have found that when the threshold is chosen to be median value ($\sqrt{ln(4)} \approx 1.18$) of the Rayleigh distribution, the performance of Eve is minimized for the reason that the ambiguity at the Eve's receiver is maximized. On the other hand there is small amount of performance difference for Bob at different threshold values. As a result system designers may choose the optimum threshold value according to their needs. Next we provide BER and MSE performances of Bob and Eve

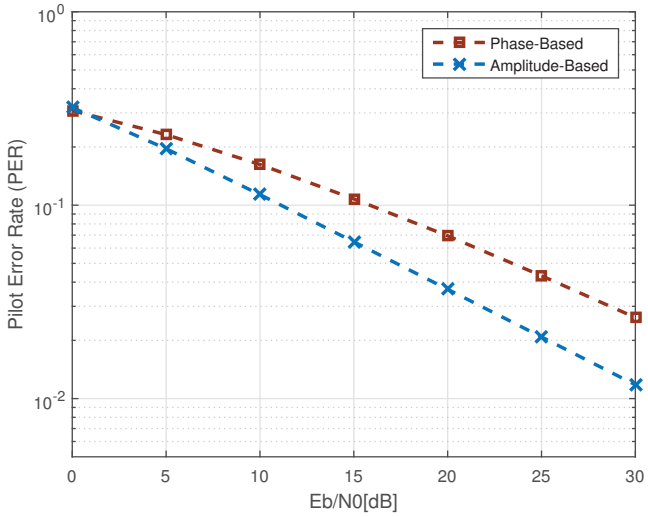

Fig. 8: Pilot Error Rate performance with MMSE channel estimation for phase-based and amplitude-based pilot manipulation.

with the optimum protection threshold.

Figures 6, 7 provide the BER and MSE performances with MMSE channel estimation. Since the LSE has poorer performance, we did not provide simulation results. Similar to phase-based pilot manipulation, we observe in Fig. 6 the algorithm provides enough protection against eavesdropping. On top of that, the performance at Bob is only 3 dB inferior than a receiver which does not utilize the algorithm. If we examine the MSE results shown in Fig. 7, the MSE performance at Eve is similar compared to performance shown in Fig. 4 whereas considerable improvement is observed at the performance of Bob.

The last figure of this section compares the pilot error rates of different manipulation schemes. The superiority of the amplitude-based pilot manipulation compared to phase-based one is observed one more time in Fig. 8. Due to the nature of the Rayleigh fading channel, phase-based pilot manipulation results in higher pilot error rate since manipulation at Alice and demanipulation at Bob may mismatch at faded subcarriers. For amplitude-based approach, the algorithm does not manipulate the pilots if fading is observed, thus reduces the pilot error rate.

V. Conclusion

In this work, we introduced two novel algorithms to improve the security of wireless communications via decreasing the ability of the eavesdropper's channel estimation. Both algorithms are based on manipulating the pilot symbols according to the channel observed between the legitimate transmitter and receiver. The first algorithm uses the phase of the channel coefficients to decide the manipulation whereas the second one relies on the channel coefficient amplitudes. According to simulation results both algorithms reduce the reception performance at the eavesdropper to a level, in which pilot based channel estimation is useless. We showed the amplitude based algorithm has a lower pilot error rate and provides satisfactory performance at the legitimate receiver. We investigated the effect of the manipulation threshold and found that there is an optimum threshold for the security of the channel and the performance at the legitimate receiver. Our future work will focus on improving the algorithms for better performance while continuing the protection from eavesdropping.

Acknowledgment

This work is supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under grant no. 114E244 and Istanbul Development Agency ISTKA under grant no. TR10/14AFK/0001.

References

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

[2] C. E. Shannon, "Communication theory of secrecy systems," *j-BELL-SYST-TECH-J*, vol. 28, no. 4, pp. 656–715, 1949.

[3] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," in *Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on*, Aug 1998, pp. 381–.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, June 2010.

[5] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of itu channels," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, Sept 2007, pp. 2030–2034.

[6] H. Li, X. Wang, and Y. Zou, "Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1059–1062, 2014.

[7] H. Li, X. Wang, and J. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 2, pp. 1155–1165, 2015.

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

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[10] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, 2012.

[11] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, 2010.

[12] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Communications Workshops (ICC), 2014 IEEE International Conference on*, June 2014, pp. 813–818.

[13] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 6, pp. 2717–2729, June 2013.

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

[15] J. Ran and L. Li, "An adaptive method utilizing channel reciprocity in TDD-LTE system," in *Communication Technology and Application (ICCTA 2011), IET International Conference on*, Oct 2011, pp. 896–900.