Impact of Imperfect Channel State Information on Physical Layer Security by Precoding and Diversity

Idowu Iseoluwa Ajayi, Yahia Medjahdi, Lina Mroueh, Fatima Zohra Kaddour

Impact of Imperfect Channel State Information on Physical Layer Security by Precoding and Diversity

I. Ajayi
Institut Superieur d'Electronique de Paris
10 rue de vanves, 92170
Issy-les-Moulineaux, France
idowu.ajayi@isep.fr

Y. Medjahdi
IMT Nord Europe
Rue Guglielmo Marconi, 59650 Villeneuve-d'Ascq
Lille, France
yahia.medjahdi@imt-nord-europe.fr

F. Kaddour
ANFR - Agence Nationale des Frequences
78 Avenue du General de Gaulle, 94704
Maisons-Alfort, France
fatima.kaddour@anfr.fr

L. Mroueh
Institut Superieur d'Electronique de Paris
10 rue de vanves, 92170
Issy-les-Moulineaux, France
lina.mroueh@isep.fr

***Abstract*—Physical layer security (PLS) is an emerging paradigm that makes use of wireless channel characteristics to provide security. Many PLS schemes require knowledge of the channel state information (CSI). However, CSI is usually imperfect due to factors such as noisy feedback channels, channel estimation errors and outdated CSI. In this paper, we investigate the impact of imperfect CSI on the secrecy and error rate performances of a PLS scheme that combines adaptive matched-filter (MF) precoding and diversity in orthogonal frequency division multiplexing (OFDM). Particularly, we derive the secrecy capacity and error rate expressions for the legitimate and eavesdropper's channels under imperfect CSI assumption. The impact of the imperfect CSI is studied via theoretical as well as numerical techniques in frequency-selective Rayleigh fading wiretap channel. The analysis is done in both frequency division duplex (FDD) and time division duplex (TDD) modes.**

***Keywords*—Imperfect CSI, Adaptive Matched-Filter Precoding, Diversity, PLS, OFDM, FDD, TDD**

I. Introduction

Physical layer security (PLS) techniques take advantage of the characteristics of wireless channels such as noise, fading, interference, diversity, dispersion, etc to ensure an intended receiver successfully decodes a transmitted data while preventing an eavesdropper from doing so [1]. The use of artificial noise injection to enhance security by degrading the eavesdropper's channel can be seen in [2]–[4]. Beamforming, a technique that involves adjusting the signal amplitudes and phases to form a strong beam towards a direction of interest, has also been used for PLS [5]–[7]. The use of channel coding techniques for security is addressed in [8], [9]. Optimal power allocation as a PLS technique was worked on in [10], [11]. In wireless communications, diversity is used to mitigate the effects of multipath fading [12]–[14]. Some works in the literature address the use of diversity in providing PLS [15]–[17].

Precoding is an interesting way to enhance PLS and we take a look at some of the research works in this direction. In [18], the authors proposed the use of zero-forcing (ZF) and the minimum means squared error (MMSE) precoders for PLS in a wiretap system where there is spatial decorrelation between the main channel and the wiretap channel. The performance of the eavesdropper is completely degraded because it carries out blind equalization as there is no channel state information (CSI) leakage to it. A precoded orthogonal space-time block coding (POSTBC) in a multiple-input single-output (MISO) setup that minimizes the error rate only at the legitimate receiver was investigated in [19]. In the paper, the authors also proposed a new technique called "precoding along with partial pre-equalizing" (PCPPE) that further improves the security of the system. This is achieved by using a new precoder design that is composed of both the original precoder and a newly designed unitary matrix. In [20], a precoder that incorporates the CSI of the eavesdropper in a millimetre-wave (mmWave) unmanned aerial vehicles (UAV) system was proposed. Symbol-level precoding to counteract learning-assisted eavesdropping in downlink multiuser-MISO system was worked on in [21]. The authors in [22] studied the impact of imperfect CSI on the mean square error (MSE) performance of a downlink MISO orthogonal frequency division multiplexing (OFDM) systems using a matched-filter (MF) precoder. Some of the works in the literature that employ MF precoding in multi-antenna scenarios can be seen in [23]–[25]. These are in contrast to our work that considers a single antenna multi-carrier scenario.

Studies on the impact of imperfect CSI in different PLS schemes can be seen in [26]–[30]. The authors in [28] studied secure communications in a multiuser massive multiple input multiple output (MU-mMIMO) system with imperfect CSI due to outdated CSI and channel estimation errors. The obtained results showed a significant reduction in secrecy capacity due to imperfect CSI. In [29], the

impact of imperfect CSI in an MU-MIMO system that combines selection transmission at the transmitter and maximum ratio combining (MRC) at the receivers was studied. It was observed that PLS performance in terms of probability of non zero secrecy capacity and secrecy outage probability degrades with a rise in imperfect CSI. In [30], the authors analysed the secrecy performance of a MIMO relay system under imperfect CSI. They concluded that the saturated minimum secrecy outage probability and maximum secrecy capacity depends on the severity of the imperfect CSI.

In this paper, we study the impact of imperfect CSI on a PLS scheme that combines repetition scheme for diversity and adaptive MF precoding in OFDM. The study investigates the use of MF precoding in a single antenna frequency selective channel scenario. Precoding transfers most of the signal processing to the transmitter and the receiver only carries out symbol detection. This means that the accuracy of the CSI at the transmitter will have a greater impact on the system's performance compared to the accuracy of the CSI at the receiver. We assume that imperfect CSI with equal estimation error variance is available at the three nodes: sender (Alice), legitimate receiver (Bob) and eavesdropper (Eve). Repetition scheme is adopted to provide diversity gain to Bob but the MF precoder ensures that Eve loses the diversity gain. This leads to a security gap between Bob and Eve measured in terms of bit error rate (BER) and secrecy capacity. We summarize our major contributions as follows:

- We study the use of adaptive MF precoding in a single-antenna multi-carrier transmission mode, combined with repetition diversity.
- We derive the expressions for the received signals, conditional secrecy capacity and conditional QPSK BER for Bob and Eve under imperfect CSI conditions.
- These derivations are verified numerically and theoretically.
- We provide an analysis of this imperfect CSI on the security performance of the system.
- We consider frequency division duplex (FDD) and time division duplex (TDD) modes. In FDD mode, there is CSI feedback between Alice and Bob and this CSI leaks to Eve. In this mode, we assume that Eve is passive but fully aware of the CSI of the wiretap and main channels. This is the worst case for security. Channel reciprocity is adopted in TDD mode and Eve only carries out blind equalization.

This paper is organized as follows. In Section II, we describe the system model. Section III is dedicated to the impact of imperfect CSI. Performance evaluation is discussed in Section IV and conclusions drawn in Section V.

Notations: Vectors are denoted by bold letters, whereas individual vector elements are denoted by normal letters. Norm- 2 is defined by $\|.\|$. Conjugate and absolute value are symbolized by $(.)^*$ and $|.|$ respectively.

II. SYSTEM MODEL

Fig. 1 shows the block diagram for the OFDM communication system. Alice transmits information signals to Bob in the presence of Eve. At Alice, the instantaneous CSI is used to design an adaptive MF precoder unique to all subcarriers. After this, diversity encoding takes place on two uncorrelated subcarriers before OFDM modulation and transmission. An advantage of this scheme is a reduced receiver complexity compared to the legacy repetition scheme since channel equalization is done at Alice. The receiver simply adds the two received signals for every diversity pair and carries out symbol detection. It is important to note that other transmitter diversity approaches such as diagonal algebraic space-time (DAST) coding [14] and Alamouti scheme [13] can also be adopted with minimal modifications to match the specifics of the schemes.

We adopt a scenario in which Bob and Eve are located at separate locations. Hence, their channels exhibit uncorrelated propagation in a rich scattering environment and the CSI of both channels are uncorrelated. To simplify the expressions and without loss of generality, the input-output relations are specified in frequency domains only. We model the imperfect CSI on the i_{th} subcarrier as given in [31]:

$$H_i = \sqrt{1-\varepsilon}\hat{H}_i + \sqrt{\varepsilon}\tilde{H}_i \tag{1}$$

where H is the actual channel gain without errors and $\hat{H}$ is the imperfect channel gain with errors. The estimation error $\tilde{H}$ is a zero-mean unit variance complex Gaussian random variable $C\mathcal{N}(0,1)$, and it is independent of H. The variance of the estimation error is denoted by $\varepsilon \in [0,1]$.

By employing the legacy repetition scheme for diversity, Alice transmits two precoded data symbols on two uncorrelated subcarriers in the same OFDM block. For every diversity pair (i,j), the received signals after OFDM demodulation are

$$r_i = H_i x_i + n_i, \quad r_j = H_j x_j + n_j \tag{2}$$

where x_i and x_j are the precoded data symbols while n_i and n_j are the complex additive white Gaussian noise (AWGN) terms for the subcarrier pair (H_i, H_j).

$$x_i = P_i s, \quad x_j = P_j s \tag{3}$$

and P is the adaptive MF precoder that is designed according to the instantaneous CSI of the legitimate receiver. It is expressed as

$$P_i = \frac{\sqrt{2}H_i^*}{\left\|H_{i,j}\right\|}, \quad P_j = \frac{\sqrt{2}H_j^*}{\left\|H_{i,j}\right\|} \tag{4}$$

where $H_{i,j}$ is the vector representing the subcarrier pair, (H_i,H_j), of the main channel under perfect CSI assumption. For a total of N available subcarriers, there are $N/2$ subcarrier pairs. By substituting (3) and (4) in (2) and simply summing the received signals on

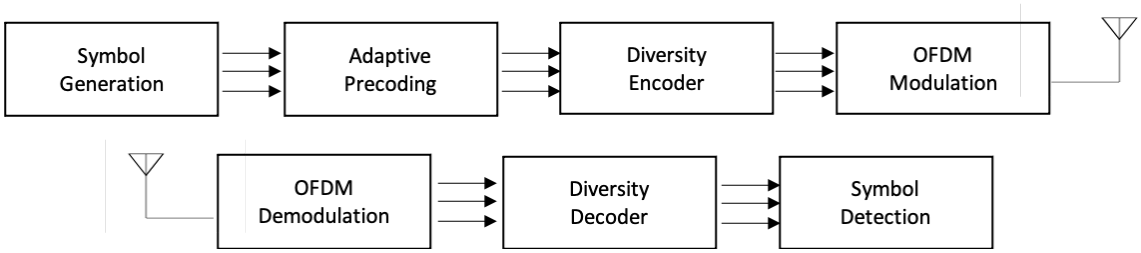

Figure 1: OFDM system model employing diversity and precoding for security

the two uncorrelated subcarriers, the received signal at Bob can be written as

$$\tilde{s}_{b1} = \sqrt{2}\left\|H_{i,j}\right\| s + n_i + n_j \tag{5}$$

From (5), the instantaneous signal to noise ratio (SNR) at Bob is given as

$$\gamma_{ib1} = \left\|H_{i,j}\right\|^2 \gamma_a \tag{6}$$

where γ_a is the average SNR at the receiver.

The calculation of the BER for QPSK constellation is readily available in the literature when the decision variables are Gaussian random variables [32]

$$\mathrm{BER(SNR)} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}}\right) \tag{7}$$

Therefore, by conditioning on the set of variables H_i and H_j, we can obtain the conditional QPSK error probability corresponding the subcarrier pair (i,j) at Bob

$$\mathrm{BER_{b1}(i,j)}\Big|_{\mathrm{H_i,H_j}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{b1}}}{2}}\right) \tag{8}$$

The final BER is obtained by averaging the conditional BER on the variables H_i H_j for all subcarrier pairs (i,j).

Similarly, when the CSI is perfect, the received signal at Eve, the instantaneous SNR and conditional QPSK BER can be respectively written as

$$\tilde{s}_{e1} = \sqrt{2}\left(\frac{H_{ie}H_i^* + H_{je}H_j^*}{\left\|H_{i,j}\right\|}\right) s + n_{ie} + n_{je} \tag{9}$$

$$\gamma_{ie1} = \left(\frac{\alpha\alpha^*}{\left\|H_{i,j}\right\|^2}\right)\gamma_a \tag{10}$$

$$\mathrm{BER_{e1}(ie,je)}\Big|_{\mathrm{H_{ie},H_{je}}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{e1}}}{2}}\right) \tag{11}$$

where

$$\alpha = H_{ie}H_i^* + H_{je}H_j^* \tag{12}$$

$H_{ie,je}$ is a vector representing a wiretap channel subcarrier pair (H_{ie}, H_{je}) when the CSI is perfect. n_{ie} and n_{je} are the complex AWGN components for the subcarrier pair.

Secrecy capacity is the positive difference between the main channel capacity and eavesdropper's channel capacity [33]. A positive value means secrecy is achievable and a zero implies there is no secrecy guarantee. We measure secrecy capacity in bps/Hz (or bits/channel use). Similar to the error rate performance, the secrecy capacity also is obtained by averaging the conditional secrecy capacity on the channel gain variables H_i and H_j for all subcarrier pairs (i,j). The conditional channel capacities of Bob and Eve and the conditional secrecy capacity are respectively expressed as

$$\mathrm{C_{b1}(i,j)}\Big|_{\mathrm{H_i,H_j}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{b1}}) \tag{13}$$

$$\mathrm{C_{e1}(ie,je)}\Big|_{\mathrm{H_{ie},H_{je}}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{ie1}}) \tag{14}$$

$$\mathrm{C_{s1}}\Big|_{\mathrm{H_i,H_j,H_{ie},H_{je}}} = \begin{cases} \mathrm{C_{b1}} - \mathrm{C_{e1}}, & \text{if } \gamma_{ib1} > \gamma_{ie1} \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

The factor of half in (13) and (14) is because only half of the available bandwidth is used for the transmission. For N available subcarriers, N/2 unique symbols are transmitted.

III. IMPACT OF IMPERFECT CSI

To achieve secure communication in the presence of an eavesdropper, the adaptive MF precoder ensures that only Bob maintains the diversity gain provided by the repetition scheme. Since the eavesdropped signals are precoded using the legitimate user's CSI, Eve will lose the diversity gain and experience a higher error rate and lower channel capacity than Bob. This degradation of Eve compared to Bob guarantees secure communication in the presence of Eve as Bob can decode transmitted symbols at a higher SNR compared to Eve.

To investigate the impact of imperfect CSI on the system, we assume that imperfect CSI with equal estimation noise variance is available at Alice, Bob and Eve. The system will no longer be optimal for Bob because the precoded symbols do not maximize the SNR anymore as is expected in MF precoding. As this estimation error variance increases, the intersymbol interference increases and Bob loses the diversity gain and thus the security gap over Eve decreases.

The received signal at Bob under imperfect CSI is expressed as

$$\hat{r}_i = H_i\hat{x}_i + n_i, \quad \hat{r}_j = H_j\hat{x}_j + n_j \tag{16}$$

where

$$\hat{x}_i = \hat{P}_i s, \quad \hat{x}_j = \hat{P}_j s \tag{17}$$

and $\hat{P}$, the adaptive MF precoder that is designed according to the imperfect instantaneous CSI

$$\hat{P}_i = \frac{\sqrt{2}\hat{H}_i^*}{\left\|\hat{H}_{i,j}\right\|}, \quad \hat{P}_j = \frac{\sqrt{2}\hat{H}_j^*}{\left\|\hat{H}_{i,j}\right\|} \tag{18}$$

where $\hat{H}_{i,j}$ is the vector representing a particular subcarrier pair, ($\hat{H}_i$,$\hat{H}_j$), of the main channel under imperfect CSI assumption. By substituting (1), (17) and (18) in (16), the received signal at Bob is shown in (19) below

From (19), the instantaneous SNR at Bob can be written as

$$\gamma_{ib2} = \frac{(1-\varepsilon)\left\|\hat{H}_{i,j}\right\|^2 \gamma_a}{\varepsilon\gamma_a + 1} \tag{20}$$

Similar to earlier derivations, the conditional QPSK BER at Bob is given as

$$\mathrm{BER_{b2}(i,j)}\Big|_{\mathrm{H_i,H_j}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{ib2}}}{2}}\right) \tag{21}$$

Following the same convention, the received signal (shown in (22) below), instantaneous SNR and conditional QPSK BER at Eve are respectively expressed as

$$\gamma_{ie2} = \frac{(1-\varepsilon)(\beta\beta^*)\gamma_a}{(\varepsilon\gamma_a + 1)\left\|\hat{H}_{i,j}\right\|^2} \tag{23}$$

$$\mathrm{BER_{e2}(ie,je)}\Big|_{\mathrm{H_{ie},H_{je}}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\gamma_{\mathrm{ie2}}}{2}}\right) \tag{24}$$

where

$$\beta = \hat{H}_{ie}\hat{H}_i^* + \hat{H}_{je}\hat{H}_j^* \tag{25}$$

$\hat{H}_{ie}$ and $\hat{H}_{je}$ are the channel frequency response for the wiretap channel (channel between Alice and Eve) when the CSI is imperfect.

In this case, the conditional channel capacities for Bob and Eve and the conditional secrecy capacity can be respectively expressed as

$$\mathrm{C_{b2}(i,j)}\Big|_{\hat{\mathrm{H}}_\mathrm{i},\hat{\mathrm{H}}_\mathrm{j}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{ib2}}) \tag{26}$$

$$\mathrm{C_{e2}(ie,je)}\Big|_{\hat{\mathrm{H}}_\mathrm{ie},\hat{\mathrm{H}}_\mathrm{je}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{ie2}}) \tag{27}$$

$$\mathrm{C_{s2}}\Big|_{\hat{\mathrm{H}}_\mathrm{i},\hat{\mathrm{H}}_\mathrm{j},\hat{\mathrm{H}}_\mathrm{ie},\hat{\mathrm{H}}_\mathrm{je}} = \begin{cases} \mathrm{C_{b2}} - \mathrm{C_{e2}}, & \text{if } \gamma_{ib2} > \gamma_{ie2} \\ 0, & \text{otherwise.} \end{cases} \tag{28}$$

Table I: Simulation Parameters

Parameter	Values
Modulation Scheme	QPSK
Error Variance(ε)	0, 0.02, 0.1
Number of subcarriers	128

IV. PERFORMANCE EVALUATION

Table I is the summary of the parameters and their values for the simulations carried out. We adopt an OFDM system with a total of N = 128 subcarriers. The symbols are QPSK modulated. Firstly, we assume a perfect CSI ($\varepsilon = 0$), then imperfect CSI is assumed with error variances of ε = 0.02 and 0.10 respectively.

For a fair comparison, we compare the error rate and secrecy performances of Bob and Eve under the assumptions of the same average SNR and estimation error variances at both of them. Due to spatial decorrelation and rich scattering, the main channel and wiretap channel are uncorrelated.

A. Bit Error Rate (BER)

BER is a Quality of Service (QoS) related metric that can also be used to analyse the security of a system. The channel with higher BER is less secure and more degraded compared to the channel with lower BER under similar conditions and the same information signal. The difference in the BER is a measure of the security gap in the system [1]. Fig. 2 shows the BER performance of the system. We present the numerical and theoretical results.

When the CSI is perfect ($\varepsilon = 0$), it can be observed that Bob outperforms Eve. Bob maintains a diversity gain of 2 but Eve loses the diversity gain in FDD mode and is fully degraded in TDD mode. In FDD mode, Eve is aware of the main channel instantaneous CSI and is able to use this instantaneous CSI for equalization. However, since the eavesdropped symbols have been precoded with an uncorrelated CSI, it leads to loss of diversity gain compared to Bob. The higher BER for Eve compared to Bob is an indication of the security gap in the system. In TDD mode, the main channel CSI is not available to Eve, Eve carries out blind equalization and is completely degraded.

Next, we look at the impact of imperfect CSI on the BER performance. When ε = 0.02, we observe in Fig. 2 a slight increase in the error rates of Bob and Eve. However, the system is still secure as the gap between Bob and Eve remains significant. As the error variance increases to ε = 0.1, the error rate significantly increases at both Bob and Eve. Bob completely loses the diversity gain. They both begin to exhibit an error floor around an average SNR of 20dB. The system is highly sensitive to channel estimation errors.

B. Secrecy Capacity

In Fig. 3, we plot the secrecy capacity of the system against the average SNR. As expected, we

$$\tilde{s}_{b2} = \sqrt{2(1-\varepsilon)}\left(\left\|\hat{H}_{i,j}\right\|\right)s + \frac{\sqrt{2\varepsilon}(\tilde{H}_i\hat{H}_i^* + \tilde{H}_j\hat{H}_j^*)}{\left\|\hat{H}_{i,j}\right\|}s + n_i + n_j \tag{19}$$

$$\tilde{s}_{e2} = \frac{\sqrt{1-\varepsilon}(\hat{H}_{ie}\hat{H}_i^* + \hat{H}_{je}\hat{H}_j^*) + \sqrt{\varepsilon}(\tilde{H}_{ie}\hat{H}_i^* + \tilde{H}_{je}\hat{H}_j^*)}{\left\|\hat{H}_{i,j}\right\|/\sqrt{2}}s + n_{ie} + n_{je} \tag{22}$$

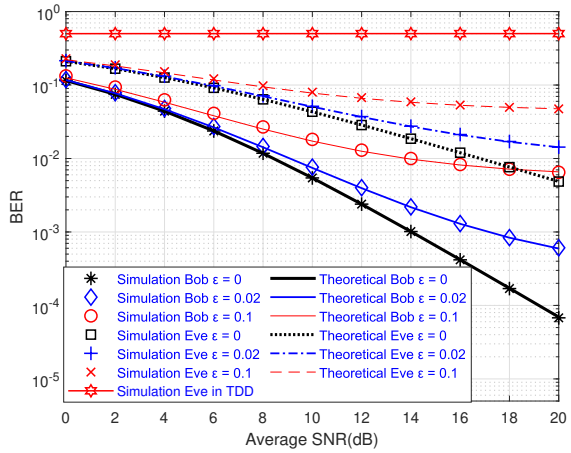

Figure 2: Bob and Eve error rate performances with imperfect CSI at Alice, Bob and Eve, ε = 0, 0.02, 0.1

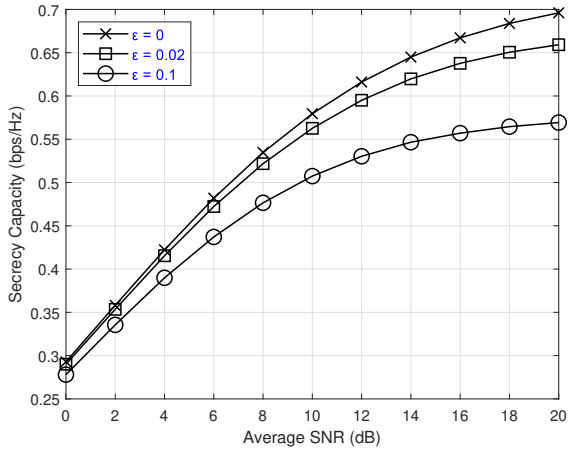

Figure 3: Secrecy capacity performances under perfect and imperfect CSI conditions, ε = 0, 0.02, 0.1

see that the secrecy capacity is highest when there is no estimation error (ε = 0), an ideal assumption. However, when the CSI is imperfect, the secrecy capacity reduces as the variance of the estimation error increases. The higher the magnitude of the estimation error variance, the lower the overall secrecy capacity in the system. This is in agreement with the BER performance. At all estimation error variances studied, the secrecy capacity remains positive. This means that although the imperfect CSI causes performance degradation at Bob and Eve, the channel capacity of Bob remains higher than the channel capacity of Eve.

V. CONCLUSION

We studied the impact of imperfect CSI on a system that combines the popular MF precoding and repetition scheme to provide PLS. The adaptive MF precoder is designed based on the instantaneous CSI of the main channel and ensures that only the legitimate receiver experiences the diversity gain from the repetition scheme. The precoder deteriorates the error rate and secrecy performance of the eavesdropper. Since this scheme depends on CSI estimation, imperfect CSI has a significant impact on the secrecy and error rate performance of the system. We derived the expressions for the received signals, secrecy capacity and BER for the legitimate receiver and the eavesdropper under perfect and imperfect CSI conditions. Using numerical and theoretical simulations, we observe that as the CSI estimation error variance increases, the secrecy capacity reduces and BER significantly increases leading to system degradation. To mitigate the effect of imperfect CSI and improve the security in the system, a future work on this paper will be the proposal of low resource consuming real time CSI prediction algorithms. Alice will then use the predicted CSI for adaptive precoding. When the CSI prediction is highly accurate, Bob's performance will be optimal and near the perfect CSI performance while the effects of Imperfect CSI will remain at Eve.

ACKNOWLEDGMENT

This work has been supported by ISEP and ANFR.

REFERENCES

[1] J. M. Hamamreh, H. M. Furqan, H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys Tutorials*, pp. 1–57, 2018.

[2] S. Hong, C. Pan, H. Ren , K. Wang, A. Nallanathan, "Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[3] Y. Feng, S. Yan, Z. Yang, "Secure Transmission to the Strong User in Non-Orthogonal Multiple Access," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2623–2626, 2018.

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

[5] S. Liang, Z. Fang, G. Sun, J. Zhang, "A Physical Layer Security Approach Based on Optical Beamforming for Indoor Visible Light Communication," *IEEE Communications Letters*, vol. 24, no. 10, pp. 2109–2113, 2020.

[6] Chan Dai Truyen Thai, "Beamforming and jamming for physical-layer security with different trust degrees," *AEU - International Journal of Electronics and Communications*, vol. 128, 2021.

[7] J. Song, B. Lee, J. Park, M. Lee, J. Lee, "Beamformer Design for Physical Layer Security in Dual-Polarized Millimeter Wave Channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 306–12 311, 2020.

[8] A. Nooraiepour and T. M. Duman, "Randomized serially concatenated ldgm codes for the gaussian wiretap channel," *IEEE Communications Letters*, vol. 22, no. 4, pp. 680–683, 2018.

[9] Y. Masuda, E. Okamoto, T. Yamamoto, "Low Complexity Decoding of Downlink Chaos NOMA Scheme with Physical Layer Security," *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, 2020.

[10] X. Chen, H. Qin, L. Xiao, M. Zhao, and J. Wang, "Power-efficient joint resource allocation for multiuser wiretap OFDM channels," *IEEE International Conference*, p. 2862â2867, 2015.

[11] S. Karachontzitis and S. Timotheou, "Security-aware maxmin resource allocation in multiuser OFDMA downlink," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, p. 529â542, 2015.

[12] Seyed Alireza Ghasempour Shirazi, "Impact of a Time-Varying Rician Fading Channel on the Performance of Alamouti Transmit Diversity Technique," *The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)*, pp. 1– 4, 2007.

[13] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE Journal on Select Areas of Communication*, vol. 16, no. 8, pp. 1451–1458, 1998.

[14] M. O. Damen, K. Abed-Meraim, J. C. Belfiore, "Diagonal Algebraic Space Time Block Codes," *IEEE Trans. on Information Theory*, vol. 48, no. 3, pp. 628–636, 2002.

[15] T. Allen, N. Al-Dhahir, "Secure Space-Time Block Coding without Transmitter CSI," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 573–576, 2014.

[16] P. O. Akuon, H. Xu, "Secure Signal and Space Alamouti Scheme," *SAIEE*, vol. 107, no. 4, pp. 237–244, 2016.

[17] M. Yusuf, H. Arslan, "Enhancing Physical-Layer Security In Wireless Communications Using Signal Space Diversity," *Military Communications Conference*, 2016.

[18] P. Cruz, R. Suyama and M. B. Loiola, "Wireless Physical-layer Security Using Precoding and an Active Eavesdropper," *Brazilian Telecommunication Symposium and Signal Processing*, 2017.

[19] J. M. Hamamreh, E. Guvenkaya, T. Baykas, H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," *IEEE Wireless Conference and Networking Conference*, 2016.

[20] S. J. Maeng, Y. Yapici, I. Guvenc, H. Dai, A. Bihuyan, "Precoder Design for mmWave UAV Communications with Physical Layer Security," *IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications*, 2020.

[21] A. Mayouche, D.Spano, C.G. Tsinos, S.Chatzinotas , B.Ottersten, "Learning-Assisted Eavesdropping and Symbol-Level Precoding Countermeasures for Downlink MU-MISO Systems," *IEEE ComSoc*, vol. 1, pp. 535–549, 2020.

[22] T. H. Nguyen, J. Louveaux, P. D. Doncker, F. Horlin, "Performance Analysis of Matched-Filter Precoded MISO-OFDM Systems in the Presence of Imperfect CSI," *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020.

[23] Azzam Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *The Institution of Engineering and Technology Communications*, vol. 10, pp. 50–56, 2016.

[24] J. Zhu, V. K. Bhargava, "Secure Transmission in Multi-Cell Massive MIMO Systems," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 4766–4781, 2014.

[25] N. P. Nguyen, H. Q. Ngo, T. Q. Duong, H. D. Tuan, K. Tourki, "Secure Massive MIMO With the Artificial Noise-Aided Downlink Training," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 36, no. 4, pp. 802–816, 2018.

[26] T. Yang, R. Zhang; X. Cheng, L.Yang, "Secure Massive MIMO Under Imperfect CSI: Performance Analysis and Channel Prediction," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 1610– 1623, 2018.

[27] Zhao, H., Tan, Yy., Pan, Gf. et al., "Ergodic secrecy capacity of MRC/SC in single-input multiple-output wiretap systems with imperfect channel state information," *Frontiers Inf Technol Electronic Eng 18*, pp. 578 – 590, 2017.

[28] T. Yang, R. Zhang, X. Cheng,L. Yang, "Performance Analysis of Secure Communication in Massive MIMO with Imperfect Channel State Information," *IEEE International Conference on Communications (ICC)*, 2018.

[29] R. Kumar, S. S. Chauhan, "Physical layer security for multiuser multi-eavesdroppermulti-input multi-output (MIMO) system in the presence ofimperfect feedback," *International Journal of Communication Systems*, 2020.

[30] C. T. Dung, L. X. Hung, T. M. Hoang, H. V. Toan, L. T. Dung, "Secrecy Performance Analysis for MIMO Relay System with Transmit/Receive Antenna Selection under Imperfect CSI," *International Conference on Advanced Technologies for Communications*, pp. 106 – 110, 2020.

[31] A. Hyadi, Z. Rezki, M. Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems With CSIT Uncertainty," *The Bell System Technical Journal*, vol. 4, pp. 6121– 6132, 2016.

[32] K. Cho, D. Yoon, "On the general BER expression of one and two dimensional amplitude modulation," *IEEE Trans. Commun.*, vol. 50, no. 7, pp. 1074– 1080, 2002.

[33] J. Barros, M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *IEEE International Symposium on Information Theory*, pp. 356 – 360, 2006.