Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information

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

▶ **To cite this version:**

Idowu Iseoluwa Ajayi, Yahia Medjahdi, Lina Mroueh, Fatima Zohra Kaddour. Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information. 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Oct 2021, Semarang, Indonesia. hal-03896129

HAL Id: hal-03896129
https://hal.science/hal-03896129v1

Submitted on 13 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Physical Layer Security by Interleaving and Diversity: Impact of Imperfect Channel State Information

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

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

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

***Abstract*—In recent years, physical layer security (PLS) has emerged as a promising concept to complement cryptography solutions. Many PLS schemes require perfect knowledge of the channel state information (CSI) at the transmitter. However, in practical cases, CSI is often imperfect due to channel estimation errors, noisy feedback channels and outdated CSI. In this paper, we study the impact of imperfect CSI on an adaptive PLS scheme that combines diversity with interleaving to provide security. Particularly, we derive the secrecy capacity expressions for the legitimate receiver and the eavesdropper's channels under imperfect CSI conditions. Numerical and theoretical simulations for secrecy capacity and bit error rate (BER) are carried out for the frequency-selective Rayleigh fading wiretap channel model. The results reveal the negative impact of imperfect CSI on the secrecy and BER performance of the single input single output (SISO) orthogonal frequency division multiplexing (OFDM) system. The analysis is done under both frequency division duplex (FDD) and time division duplex (TDD) modes.**

***Keywords*—Channel State Information, Estimation Error, OFDM, Diversity, Adaptive Interleaver, PLS, Frequency Division Duplex**

I. Introduction

Physical layer security (PLS) is an emerging paradigm used to enhance security in wireless communication systems. Its advantages over cryptography are lower computational complexity and resource requirement [1]. The idea behind PLS is to use wireless channel characteristics such as noise, fading, interference and dispersion to provide secure communication between a transmitter and a legitimate receiver in the presence of an eavesdropper. The authors in [2]–[4] enhanced PLS using artificial noise (AN) injection. Beamforming for PLS can be seen in [5]–[8]. The use of channel coding techniques for security is addressed in [9], [10] and optimal power allocation as a PLS technique was worked on in [11], [12]. The authors in [13]–[15] improved PLS through precoding.

Most PLS schemes require knowledge of the instantaneous channel state information (CSI). In practical systems, perfect CSI is usually not available due to factors such as channel estimation errors at the receiver, noisy feedback channel between the receiver and the transmitter, outdated CSI, etc. This means that the effectiveness of the security solution in PLS depends on the accuracy of the CSI available to the transmitting devices. Several works have been done on PLS under imperfect CSI conditions [16]–[20]. The authors in [18] studied secure communications in a multi-user massive multiple input multiple output (MIMO) 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 [19], the impact of imperfect CSI in a multi-user MIMO having selection transmission at the transmitter and maximum ratio combining (MRC) at the receivers was studied where PLS performance in terms of probability of non zero secrecy capacity and secrecy outage probability degrades with rise in imperfect CSI. In [20], the authors analysed the secrecy performance of a MIMO relay system under imperfect CSI. The conclusion was that among other factors, 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 the interesting security scheme proposed by the authors in [21] for orthogonal frequency division multiplexing (OFDM) system. The scheme uses instantaneous CSI to design an adaptive interleaver and combines this with signal space diversity (SSD) to ensure a better bit error rate (BER) performance at the legitimate receiver compared to the eavesdropper. SSD is a diversity approach in which the in-phase and quadrature signal components are sent on independent subcarriers to provide diversity gain. For simplicity sake, we have replaced SSD with a repetition scheme for diversity. It is worth mentioning that the diversity scheme provides reliability while the interleaving scheme improves the security of the

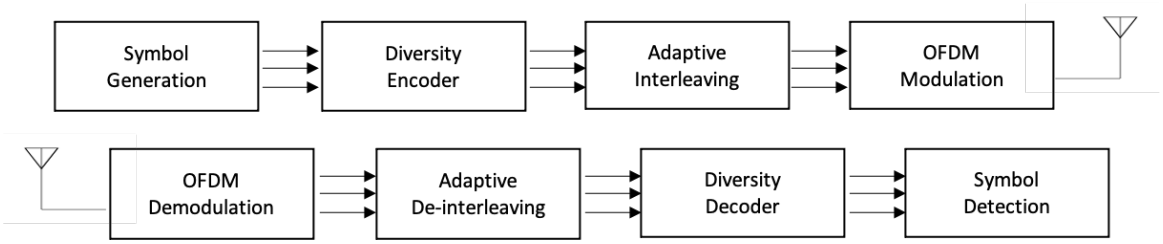

Figure 1: OFDM system model employing diversity and interleaving for security

system by ensuring more diversity gain is provided to the legitimate receiver than the eavesdropper. Other diversity schemes such as Alamouti Scheme [22] and diagonal space-time block (DAST) coding [23] can also be used. We derive the expressions of signal to noise ratio (SNR), secrecy capacity and BER of the system under imperfect CSI conditions. Two cases of imperfect CSI are considered: at the transmitter only and at both the transmitter and receivers. This study is done in both frequency division duplex (FDD) and time division duplex (TDD) modes. In FDD mode, there is CSI feedback between the transmitter (Alice) and the legitimate receiver (Bob) and this CSI leaks to the eavesdropper (Eve). Eve is assumed to be passive but fully aware of the CSI of the wiretap channel, the CSI of the main channel and the interleaving pattern. This is the worst case for security. In TDD mode, there is no CSI leakage and channel reciprocity assumption can be exploited.

The outline of this paper is organized as follows. Section II is devoted to describing the system model of interleaved secure OFDM transmission. We derive expressions of SINR, BER and secrecy capacity in presence of erroneous CSI in Section III. Simulation results are presented and discussed in Section IV. Section V concludes the paper.

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 respectively symbolized by $(.)^*$ and $|.|$.

II. SYSTEM MODEL

Fig. 1 shows the block diagram for the OFDM communication system. At the transmitter, diversity codeword is first formed and then the adaptive interleaving operation takes place, both in the frequency domain. This interleaving is designed according to the estimated instantaneous CSI feedback received from the receiver. The reverse takes place at the receiver, where the de-interleaving operation in the frequency domain is followed by the receiver decoding operation. We assume a wiretap channel model in which Alice is sending information signals to Bob in the presence of Eve. All signals propagate through different multipath channels using a similar propagation model.

To simplify the presentation and without loss of generality, imperfect CSI on the i_{th} subcarrier is modelled in the frequency domain as [24]:

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

where H is the actual channel gain without error and $\hat{H}$ stands for the imperfect channel gain with error. 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 $\varepsilon \in [0,1]$.

Using the legacy repetition scheme, each data symbol, s, is transmitted on two uncorrelated subcarriers in the same OFDM block. For every diversity pair (i,j), the received signals after OFDM demodulation are

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

where n_i and n_j are the complex additive white Gaussian noise (AWGN) components for the subcarrier pair (H_i, H_j).

III. IMPACT OF IMPERFECT CSI

To achieve secure communication between Alice and Bob in the presence of Eve, the authors in [21] made use of the instantaneous CSI of the main channel to design an adaptive interleaver that ensures a higher diversity gain for Bob compared to Eve. The interleaver is designed such that deep faded subcarriers are paired with high gain subcarriers. This means if a signal experiences deep fade in one subcarrier, the diversity component will be one experiencing high gain. To achieve this, the subcarriers are first sorted in decreasing order of magnitude and then paired from both edges progressively. The interleaver pairing is no longer random but ordered. This is better than when the diversity pairs are random and there is a possibility of two subcarriers in a diversity pair experiencing deep fading. The result is that Bob will experience a diversity gain much higher than Eve.

Due to the spatial decorrelation between the channels of Bob and Eve and the rich scattering environment, this adaptive interleaver that is specially designed for Bob will appear as a random interleaver to Eve. The diversity gain experienced at Eve will remain the same irrespective of the interleaver design. This improvement of Bob over Eve guarantees secure communication in the presence of Eve as Bob can decode transmitted symbols at a higher SNR compared to Eve.

This interesting security scheme proposed in [21] depends on the accuracy of the instantaneous CSI, a

constraint in most practical systems. There is therefore a need to study the impact of imperfect CSI on the security solution. For this study, two cases are examined:

1) Imperfect CSI-T and Perfect CSI-R: We assume here perfect channel estimation at Bob but noisy channel feedback between Bob and Alice. This leads to an imperfect CSI at Alice impacting thus the interleaver design. For a total of N subcarriers, Alice sorts the imperfect channel gains in descending order of magnitude as

$$|\hat{H}_1| \geq |\hat{H}_2| \geq ... \geq |\hat{H}_{N-1}| \geq |\hat{H}_N| \tag{3}$$

After sorting, the interleaving scheme will pair the subcarriers for diversity as follows

$$(\hat{H}_1, \hat{H}_N), (\hat{H}_2, \hat{H}_{N-1}), ..., (\hat{H}_{N/2}, \hat{H}_{N/2+1}) \tag{4}$$

This interleaving scheme will no longer be optimal for Bob. Note that the equalization at the receiver is not impacted. Bob therefore equalizes as follows

$$\tilde{s}_{b1} = H_i^* r_i + H_j^* r_j \tag{5}$$

By substituting (2) in (5), the received signal at Bob is

$$\tilde{s}_{b1} = \left\|H_{i,j}\right\|^2 s + H_i^* n_i + H_j^* n_j \tag{6}$$

where $H_{i,j}$ is the vector representing a particular subcarrier pair, (H_i,H_j) of the main channel. For a total of N available subcarriers, there are $N/2$ subcarrier pairs. From (6), the instantaneous SNR at Bob can be written as

$$\gamma_{ib1} = \left\|H_{i,j}\right\|^2 \gamma_a \tag{7}$$

where γ_a is the average SNR.

In the following derivation, we analyze the QPSK constellation case, the extension to another MQAM constellation is straightforward. The calculation of the bit error rate of this constellation is readily available in the literature when the decision variables are Gaussian random variables [25]

$$\mathrm{BER(SNR)} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}}\right) \tag{8}$$

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,

$$\mathrm{BER_{b1}(i,j)}\Big|_{\mathrm{H_i,H_j}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\left\|H_{i,j}\right\|^2 \frac{\gamma_\mathrm{a}}{2}}\right) \tag{9}$$

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

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

$$\tilde{s}_{e1} = \left\|H_{ie,je}\right\|^2 s + H_{ie}^* n_{ie} + H_{je}^* n_{je} \tag{10}$$

$$\gamma_{ie1} = \left\|H_{ie,je}\right\|^2 \gamma_a \tag{11}$$

$$\mathrm{BER_{e1}(i,j)}\Big|_{\mathrm{H_{ie},H_{je}}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\left\|H_{ie,je}\right\|^2 \frac{\gamma_\mathrm{a}}{2}}\right) \tag{12}$$

where $H_{ie,je}$ is the vector representing a particular wiretap channel subcarrier pair (H_{ie},H_{je}).

Secrecy capacity is the maximum transmission rate at which the eavesdropper is unable to decode any information [26]. It is equal to the positive difference between the capacity of the main channel and the capacity of the wiretap channel. 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

$$\mathrm{C_{b1}(i,j)}\Big|_{\mathrm{H_i,H_j}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{ib1}}) \tag{13}$$

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

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

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.

2) Imperfect CSI-T and Imperfect CSI-R: In this case, we assume that imperfect CSI with equal estimation noise variance is available at the three nodes: Alice, Bob and Eve. This means that Alice and Bob have the same imperfect CSI. Both the interleaving design and the receiver equalization will be impacted by the noisy CSI leading thus to intersymbol interference [27] that significantly degrades the performance. In this study, the interleaving pattern is assumed to be known at Bob and Eve.

Consequently, the received signal at Bob after equalization can be written as,

$$\tilde{s}_{b2} = \hat{H}_i^* r_i + \hat{H}_j^* r_j \tag{16}$$

By substituting (1) and (2) in (16), we have

$$\tilde{s}_{b2} = \sqrt{1-\varepsilon}\left\|\hat{H}_{i,j}\right\|^2 s + \sqrt{\varepsilon}(\hat{H}_i^* \tilde{H}_i + \hat{H}_j^* \tilde{H}_j)s + \hat{H}_i^* n_i + \hat{H}_j^* n_j \tag{17}$$

From (17), the Instantaneous Signal to Interference plus Noise Ratio (SINR) ,γ_{ib2}, at Bob is derived below (similar to [27])

$$\gamma_{ib2} = \frac{(1-\varepsilon)\left\|\hat{H}_{i,j}\right\|^2 \gamma_a}{\varepsilon\gamma_a + 1} \tag{18}$$

To simplify the BER expressions , we express the corresponding average SNR due the imperfect CSI as, γ',

$$\gamma' = \frac{(1-\varepsilon)\gamma_a}{\varepsilon\gamma_a + 1} \tag{19}$$

In this case, the conditional QPSK BER at Bob is expressed as

$$\mathrm{BER_{b2}(i,j)}\Big|_{\hat{\mathrm{H}}_\mathrm{i},\hat{\mathrm{H}}_\mathrm{j}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\left\|\hat{H}_{i,j}\right\|^2 \frac{\gamma'}{2}}\right) \tag{20}$$

Similar to the derivations for Bob, the received signal, instantaneous SINR and conditional QPSK BER for Eve are

$$\tilde{s}_{e2} = \sqrt{1-\varepsilon}\left\|\hat{H}_{ie,je}\right\|^2 s + \sqrt{\varepsilon}(\hat{H}^*_{ie}\tilde{H}_{ie} + \hat{H}^*_{je}\tilde{H}_{je})s + \hat{H}^*_{ie}n_{ie} + \hat{H}^*_{je}n_{je} \tag{21}$$

$$\gamma_{ie2} = \frac{(1-\varepsilon)\left\|\hat{H}_{ie,je}\right\|^2 \gamma_a}{\varepsilon\gamma_a + 1} \tag{22}$$

$$\mathrm{BER_{e2}(i,j)}\Big|_{\hat{\mathrm{H}}_\mathrm{ie},\hat{\mathrm{H}}_\mathrm{je}} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\left\|\hat{H}_{ie,je}\right\|^2 \frac{\gamma'}{2}}\right) \tag{23}$$

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

$$\mathrm{C_{b2}(i,j)}\Big|_{\hat{\mathrm{H}}_\mathrm{i},\hat{\mathrm{H}}_\mathrm{j}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{b2}}) \tag{24}$$

$$\mathrm{C_{e2}(ie,je)}\Big|_{\hat{\mathrm{H}}_\mathrm{ie},\hat{\mathrm{H}}_\mathrm{je}} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{ie2}}) \tag{25}$$

$$\mathrm{C_{s2}}\Big|_{\hat{\mathrm{H}}_\mathrm{i},\hat{\mathrm{H}}_\mathrm{j},\hat{\mathrm{H}}_\mathrm{ie},\hat{\mathrm{H}}_\mathrm{je}} = \begin{cases} \mathrm{C_{b2}} - \mathrm{C_{e2}}, & \text{if } \gamma_{ib2} > \gamma_{ie2} \\ 0, & \text{otherwise.} \end{cases} \tag{26}$$

IV. PERFORMANCE EVALUATION

In this section, we present the numerical and theoretical results. We consider a system with N=128 subcarriers. The data are QPSK modulated. Three error variances are considered: perfect (ε = 0) and noisy (ε = 0.02 and 0.1). We compare the performances of Bob and Eve under the assumptions of uncorrelated channels but the same average SNR.

A. Bit Error Rate (BER)

BER is a popular metric that is used to study the error performance of a system. In terms of security, difference in BER is an indication of security gap [1]. We see in Fig. 2 the BER performance for the first case of our study when there is an imperfect CSI at Alice but a perfect CSI at Bob and Eve. When the CSI is perfect (ε = 0), it can be observed that Bob outperforms Eve with a diversity gain significantly higher than 2. This is due to the adaptive interleaving pattern that is specifically designed for Bob's channel [21]. There is no additional diversity gain for Eve due to the uncorrelation between the channels of Bob and Eve. When ε = 0.02, we observe a slight degradation

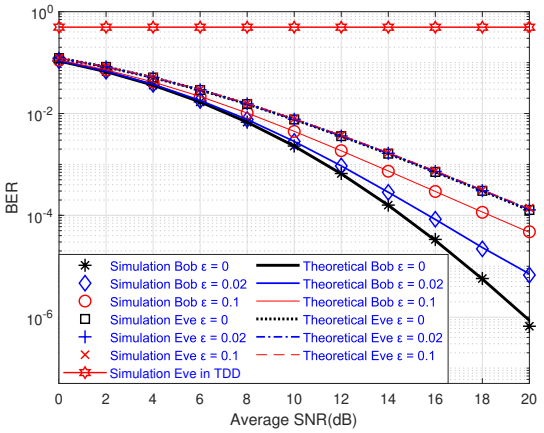

Figure 2: Bob and Eve error rate performances with imperfect CSI at Alice only, ε = 0, 0.02, 0.1

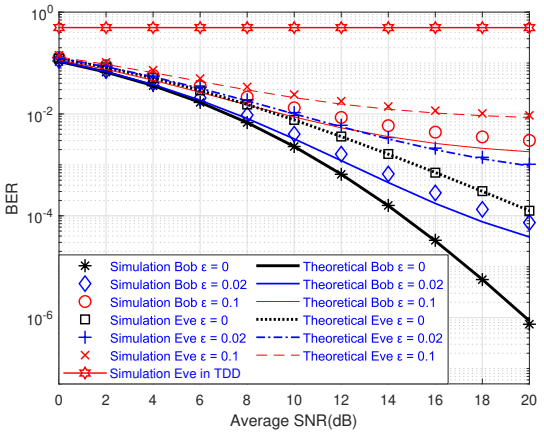

Figure 3: Bob and Eve error rate performances with imperfect CSI at Alice, Bob and Eve, ε = 0, 0.02, 0.1

in the BER performance of Bob but the diversity gain of Eve remains the same. Bob's BER degradation is severe and increases when the CSI error variance is larger (ε = 0.1). In contrast to Bob, the performance of Eve is insensitive to the quality of CSI available at Alice. Indeed, the interleaving scheme is totally affected and becomes random to both Bob and Eve when ε is high. At that point, the system will offer zero security. In TDD mode where the main channel CSI is not available to Eve, we see that the BER performance of Eve is totally degraded and secrecy is guaranteed.

Fig. 3 shows the BER performance for the second case of our study when imperfect CSI is available at all three nodes. As before, the imperfect CSI at Alice results in less optimal interleaver design. The difference here is that the receivers now use this imperfect CSI for equalization leading to a significant degradation in the BER performance of Bob and Eve. Bob and Eve are more sensitive to estimation error variance and diversity gain can be completely lost by both. At ε = 0.1, they exhibit an error floor around an average SNR of 20dB onward due to the intersymbol interference caused by the imperfect CSI. The degradation is more for Bob but it still slightly outperforms Eve at the error variances considered.

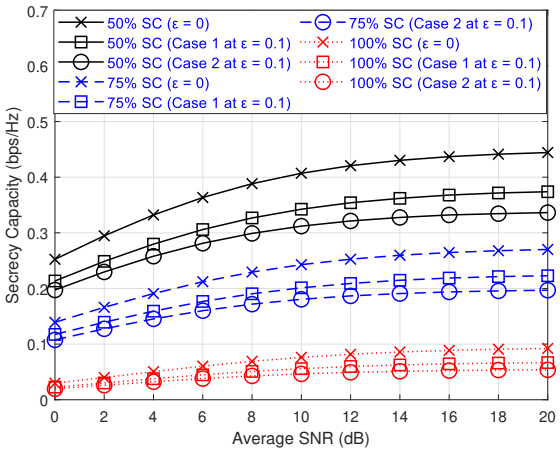

Figure 4: Secrecy capacity performances under perfect and imperfect CSI conditions, ε = 0, 0.1, subcarrier usage = 50%, 75%, 100%

Similarly, the BER performance of Eve in TDD mode is totally degraded since there is no CSI feedback leakage to Eve and Eve is only able to carry out blind equalization.

B. Secrecy Capacity

In Fig. 4, the secrecy capacity performance for the scheme under perfect CSI condition (ε = 0) and under an imperfect CSI condition (ε = 0.1) is plotted against the average SNR. We have shown the secrecy capacity performance for the two cases studied. Case 1 is when there is an imperfect CSI at Alice but a perfect CSI at the receivers. The secrecy capacity expression for this case is seen in (15). Case 2 is when we have an imperfect CSI at both the transmitter and the receivers, the secrecy capacity expression for this case is seen in (26). We have also run simulations for the special instances where not all available N subcarriers are used for data transmission. For each instance, the secrecy capacity is highest with a perfect CSI ($\varepsilon = 0$) and reduces with a higher error variance ($\varepsilon = 0.1$). At the same error variance, case 1 shows a higher secrecy capacity than case 2. The reason for this is that in case 1, the imperfect CSI only affects the interleaving scheme used by Alice. It will no longer be optimal for Bob but the receivers are still able to perfectly equalize the received signals. The additional diversity gain offered to Bob is gradually lost as the error variance increases. The channel capacity of Eve remains the same but the channel capacity of Bob reduces as the error variance increases. However, in case 2, the interleaver is not optimal and there is also an equalization error at the receivers. This leads to intersymbol interference and a more degraded system. The channel capacities of both Bob and Eve significantly reduces. The results also show that at 50% subcarrier usage, the secrecy capacity is higher than at 75% subcarrier usage, which is in turn higher than at 100% subcarrier usage. This is because when we use fewer subcarriers, we can select only the subcarriers with the highest gains and avoid deep faded subcarriers. There is however a trade-off between the number of available subcarriers used for data transmission, the secrecy capacity and the system throughput. As the number of subcarriers used for data transmission out of all available subcarriers reduces, the secrecy capacity increases but in turn, the overall system throughput decreases. Hence in a practical system, there needs to be an optimal choice based on user requirements in terms of the secrecy and throughput targets.

V. CONCLUSION

In this paper, we have investigated the impact of CSI errors on interleaved OFDM secure transmission. The adaptive interleaving scheme is designed based on the instantaneous CSI of the main channel to provide more diversity gain to Bob than Eve [21]. A global evaluation has been performed considering two cases of imperfect CSI: at the transmitter only and at all nodes. We derived the expressions for the received signals, secrecy capacity and BER for Bob and Eve in both cases. We observed that as the variance of the CSI estimation error increases, secrecy capacity reduces and BER increases. Through this evaluation, we have shown that the security solution is slightly more robust in the first case compared to the second one. This is because the system only suffers from less optimal interleaver design in case 1 but is faced with both the challenges of less optimal interleaver design and incorrect receiver equalization leading to intersymbol interference in case 2.

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*, vol. 21, pp. 1773–1828, 2019.

[2] W. Liu, M. Li,X. Tian, Z. Wang, Q. Liu, " Transmit Filter and Artificial Noise Design for Secure MIMO-OFDM Systems," *arXiv*, 2017.

[3] 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.

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

[5] E. Yaacoub, M. Al-Husseini, " Achieving physical layer security with massive MIMO beamforming," *11th European Conference Antennas Propagation*, p. 1753â1757, 2017.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

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

[27] K.Vanganuru and A. Annamalai, "Analysis of Transmit Diversity Schemes: Impact of Fade Distribution, Spatial Correlation and Channel Estimation Errors," *IEEE Wireless Communications and Networking*, pp. 247–251, 2003.