# Controlled Inter-carrier Interference for Physical Layer Security in OFDM Systems

Marwan Yusuf* and Huseyin Arslan*†
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey 34810
†Department of Electrical Engineering, University of South Florida, Tampa, FL, USA 33620

***Abstract*—Performance of OFDM is known to be very sensitive to frequency synchronization errors. By exploiting this feature, a novel technique is proposed to provide secure communication against eavesdropping. The technique is based on introducing self inter-carrier interference to pre-compensate the carrier offset only for the legitimate user. This pre-compensation process depends on both the channel and the local carrier offset of the legitimate user, hence provides another degree of freedom for secrecy. Under the assumption that eavesdropper experiences an uncorrelated channel, his performance is expected to be degraded. Also our approach converts the simple one-tap frequency domain channel equalization to a very complex receiver operation for the eavesdropper. Moreover, the power aspects of this technique are discussed. By setting a threshold in the pre-compensation stage, we provide an acceptable trade-off between the transmitted power and the error performance.**

## I. Introduction

Wireless communications have become indispensable for providing seamless, mobile and broadband data transfer. However, the broadcast nature of radio waves results in a critical drawback in terms of transmission security and privacy, especially for vital applications such as military, public safety or health care. Confidential transmission has conventionally been achieved via cryptologic methods that are performed in the upper layers of the communication system. In order to make the signal meaningless for malicious nodes in the lowest layer possible, physical-layer security is emerging as a promising paradigm which exploits the physical characteristics of wireless channels [1], [2]. Besides their vulnerability, wireless links have explicit advantages that can be exploited for security such as the random multipath propagation environment, multiple degrees of input/output and flexible waveform design.

The physical layer security over wireless channels has been investigated from an information-theoretic perspective [3-5]. In addition to the demonstration of its feasibility, practical approaches have also been investigated. One of the most common techniques to conceal both information and the signal itself is to spread the signal in frequency [6], so that the malicious nodes cannot capture and decode the signal. This holds under the assumption of the malicious receiver not having any information regarding the spreading sequence. Artificial Noise (AN) was generated using multiple antennas in [7] or cooperative nodes in [8]. The noise was added to the nullspace of the legitimate user's channel to prevent eavesdropping. In [9], transmitter beamforming was proposed to facilitate the transmission confidentiality. With the collaboration of legitimate users in a cluster, an anti-eavesdropping space-time network coding scheme was proposed to prevent eavesdropping in [10]. Similarly, relay techniques were utilized to defend against eavesdroppers by increasing the secrecy rate at the cost of collaborative nodes [7]. However, the aforementioned security approaches have multiple requirements to be effective, such as additional transmitted power for AN emission, information of eavesdropping channel and location, multiple Tx and Rx antennas or cooperating nodes.

Another approach for providing secrecy is exploiting the characteristics of the transmitted signal. As an example, orthogonal frequency division multiplexing (OFDM) has been widely employed in modern wireless systems because of its high spectral efficiency and robustness against multipath fading. Unfortunately, a conventional OFDM signal is vulnerable to eavesdropping attacks due to its distinct time and frequency characteristics [11]. In the literature, various techniques were developed to achieve transmission level security and covertness in OFDM systems. In [12], cyclic prefix and pilot tones are removed to suppress OFDM features. The inter-symbol interference (ISI) is canceled using a decision feedback equalizer (DFE). This eliminates the advantage of OFDM in handling multipath fading channel by using cyclic prefix (CP), alongside with the possible error propagation between OFDM symbols due to the DFE. Alternatively, cyclic features are concealed by changing the CP selection region for each symbol [13] or by inserting random data between OFDM symbols [14] in a pseudo-random fashion. Also, CP length variation according to the maximum excess delay of the channel is offered as an extra precaution. However, these techniques require spectral redundancy either by using longer CP than needed or using irrelevant data.

In this paper we exploit one of the known drawbacks of OFDM for security purposes. The performance of OFDM is very sensitive to frequency synchronization errors. The existence of carrier frequency offset (CFO) between the transmitter and the receiver is mainly due to oscillator instabilities or Doppler shifts. The resulting inter-carrier interference (ICI) degrades the system performance [15] since the transmitted information cannot be retrieved error-free even in the absence of noise. Also, CFO may cause the loss of orthogonality among subcarriers. There have been several papers on the subject of synchronization in recent years especially in the crucial uplink case in OFDMA systems. One of the most robust synchronization methods can be found in [16]. Two main approaches, namely feedback method and compensation method, can be used to mitigate the frequency offset in the uplink of OFDMA systems. In the former, the estimated frequency offset values at the base station are fed back to the users on a control channel so that they can adjust their transmission parameters [17]. The obvious disadvantage of this approach is the need

978-1-5090-1701-0/16/$31.00 ©2016 IEEE

for the control channel. In the compensation method [18], [19], users do not change their transmission parameters, instead the base station compensates for the frequency offsets of all users by employing signal processing techniques without the need for a control channel.

In our work, we consider a Time-Division Duplexing system where we can exploit the reciprocity of the channel. In this system, the legitimate user (Bob) sends his signal with an induced CFO that the transmitter (Alice) can estimate and compensate using the second method mentioned earlier. With the channel state information (CSI) known to Alice, she will transmit her data with the carrier offset pre-compensated in such a way that, when it passes through Bob's channel, it is received without ICI. This is different from just having a CFO at Alice because the pre-compensation process depends also on the channel between Alice and Bob. Even if the eavesdropper (Eve) manages to blindly estimate the offset, she will still suffer from degradation due to the uncorrelation between her channel and Bob's channel. In other words, the pre-compensation acts as a pre-equalizer, not to the channel but to the ICI with respect to Bob's channel. To further increase the security of communication, Bob can change the offset continuously, hence both CFO and CSI need to be tracked by Alice. This makes the estimation and tracking done by Eve a difficult task, even if she uses a very complex algorithm to compensate what is done at Alice. Also the simple structure of the proposed scheme shown in Fig. 1, with only a carrier offset at the receiver and shifting the complexity to transmitter, allows it to be suitable for future low power demands of green radios.

The rest of the paper is organized as follows. The system model is investigated in Section II. Section III presents the effect of carrier frequency offset and the proposed algorithm followed by the simulation results in Section IV. Also in this section we check the power aspects of the technique and propose a solution to limit the consumption. Finally, conclusions are given in Section V.

## II. System Model

In OFDM the bit stream is mapped to symbols that modulate a series of subcarriers, each separated by a spacing of $1/T$ in frequency domain, where $T$ is the symbol duration. Even though the modulated symbols spectrally overlap, they are orthogonal to each other. This modulation process can be computed efficiently by applying the $N$-point Inverse Fast Fourier Transform (IFFT) to each OFDM block to obtain the time domain signal. The transmitted modulated signal sampled in time domain is given by

$$x_l(n) = \sum_{k=0}^{N-1} X_l(k) e^{j2\pi kn/N} \tag{1}$$

where $X_l(k)$ denotes the symbol at the $k^{th}$ subcarrier in the $l^{th}$ OFDM symbol and $N$ is the number of subcarriers. To overcome the multipath fading channel, a guard interval is appended at the front of each OFDM symbol. This guard interval is usually inserted by extending the OFDM symbol with a CP that allows for both the removal of ISI and maintaining subcarriers orthogonality. Hence, after the removal of this extension at the receiver, the signal is ISI-free and

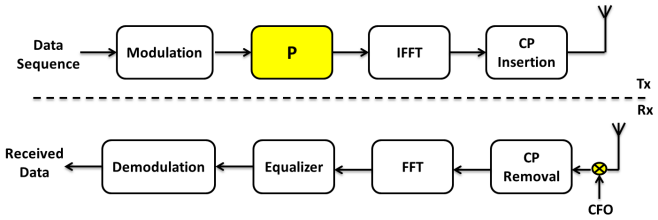


Fig. 1. Block Diagram of proposed OFDM system

each subcarrier channel response is considered as a flat fading channel. Let $y(n)$ be the received signal

$$y(n) = \sum_{m=0}^{M-1} h(m)x(n-m) + z(n) \tag{2}$$

where $h(m)$ is the channel response with $M$ taps and $z(n)$ is the sampled Additive White Gaussian Noise (AWGN) in time domain. This can be represented in a matrix form as

$$\mathbf{y} = \mathbf{FTH_tGF^{-1}x} + \mathbf{z} \tag{3}$$

where $\mathbf{y}$ is the received symbols vector, $\mathbf{T}$ is the truncating matrix for CP removal, $\mathbf{H_t}$ is the matrix with channel impulse responses, $\mathbf{G}$ is the matrix for CP inserting, $\mathbf{F}$ and $\mathbf{F^{-1}}$ are the FFT and IFFT matrices, $\mathbf{x}$ is the vector of transmitted symbols and $\mathbf{z}$ is the noise vector. Assuming the CP length is greater than maximum delay spread, $\mathbf{TH_tG}$ is a circular square matrix and can be modeled as

$$\mathbf{TH_tG} = \mathbf{F^{-1}H_fF} \tag{4}$$

where $\mathbf{H_f}$ is the diagonal matrix of the channel frequency response. Then the received signal can be simplified into

$$\mathbf{y} = \mathbf{H_f x} + \mathbf{z} \tag{5}$$

## III. Securing Communication via Carrier Offset Pre-compensation

Let us consider the case where we have a carrier offset between Alice and Bob. This CFO is induced by Bob so that it can be estimated and compensated by Alice, then pre-compensated for securing the transmission. Assuming perfect time synchronization, the received symbols at Alice after FFT can be written as

$$Y_l(k) = \sum_{n=0}^{N-1} y_l(n) e^{-j2\pi(k+\epsilon)n/N} \tag{6}$$

$$= \sum_{k'=0}^{N-1} X_l(k')H(k')I(k,k',\epsilon) \tag{7}$$

where $\epsilon = \Delta f T$ is the CFO, which represents the frequency offset $\Delta f$ normalized to the carrier spacing $1/T$ and $H(k')$ is the flat channel response at the $k'^{th}$ subcarrier. The spectral leakage $I$ among subcarriers is defined as

$$I(k,k',\epsilon) = e^{j\pi(k-k'+\epsilon)\frac{N-1}{N}} \frac{\sin(\pi(k-k'+\epsilon))}{N\sin(\frac{\pi(k-k'+\epsilon)}{N})} \tag{8}$$

$I(k,k',\epsilon)$ can be interpreted as the normalized interference on the $k'^{th}$ subcarrier from the $k^{th}$ subcarrier. For a large number

of subcarriers $N$, the normalized interference power can be approximated by

$$|I(k,k',\epsilon)|^2 = \left|\frac{\sin(\pi(k-k'+\epsilon))}{\pi(k-k'+\epsilon)}\right|^2 \quad (9)$$

Note that the orthogonality among subcarriers is destroyed when $\epsilon$ is not an integer. In other words, to have ICI, the induced carrier offset should be a fractional multiple of the carrier spacing. Fig. 2 shows the increase of interference power among subcarriers as the fractional frequency offset (FFO) increases. As shown in (6) the effect of carrier offset on the time domain signal is a phase shift that is proportional to the FFO $\epsilon$ and time index $n$, so it can be written as

$$\mathbf{y} = \mathbf{F}\mathbf{E}\mathbf{F}^{-1}(\mathbf{H_f x} + \mathbf{z}) = \mathbf{E_c H_f x} + \mathbf{z}' \quad (10)$$

where $\mathbf{E}$ is a diagonal matrix given by diag[1 $e^{j2\pi\epsilon/N}$... $e^{j2\pi\epsilon(N-1)/N}$] and $\mathbf{E_c} = \mathbf{F}\mathbf{E}\mathbf{F}^{-1}$ is the interference matrix that models the same effect as a circular convolution in the frequency domain [20]. $\mathbf{E_c}$ is basically the effect of the ICI shown in (8).

For the proposed scheme, the transmitted symbols from Alice are first passed through a pre-compensation stage before IFFT as shown in Fig. 1. This pre-compensation matrix P is generated such that the effect of ICI is eliminated at Bob. This is done by setting the received signal as following, disregarding the noise

$$\mathbf{y_B} = \mathbf{E_c H_f P x} = \mathbf{H_f x} \quad (11)$$

$$\mathbf{P} = \mathbf{H_f^{-1} E_c^{-1} H_f} \quad (12)$$

where $\mathbf{E_c^{-1}} = \mathbf{F^{-1}E^{-1}F}$. Hence, $\mathbf{P}$ can be generated from the channel frequency response and the carrier offset both estimated at Alice. This process, which we may call as interference zero-forcing, is not computationally complex, since both matrices $\mathbf{E^{-1}}$ and $\mathbf{H_f^{-1}}$ are diagonal ones. For the case of Eve, the received signal will be

$$\mathbf{y_E} = \mathbf{E_E H_E H_f^{-1} E_c^{-1} H_f x} \quad (13)$$

where a different frequency offset gives the ICI matrix $\mathbf{E_E}$ and $\mathbf{H_E}$ is Eve's frequency channel response. Because the channels of Bob and Eve are uncorrelated, it is hard to eliminate the effect of the ICI induced by the pre-compensation stage. Even if Eve manages to get the right offset, the channel to be estimated is no longer flat as shown in (13). The estimation of the diagonal and off diagonal elements becomes a tedious process for Eve. By rapidly varying the offset value at Bob, this estimation process will even be more difficult, if not impossible. It will be shown in the simulation results that, with the same offset value as Bob, Eve still suffers from performance degradation since the channel estimation assumes flat fading for each subcarrier.

## IV. Secrecy Evaluation

To measure the secrecy performance of the proposed scheme, we refer to the information-theoretic metrics usually used for characterizing the security level of a communication link, in our case a fading wire-tap channel [20]. We define the achievable secrecy rate as

$$R_s = R_B - R_E \quad (14)$$

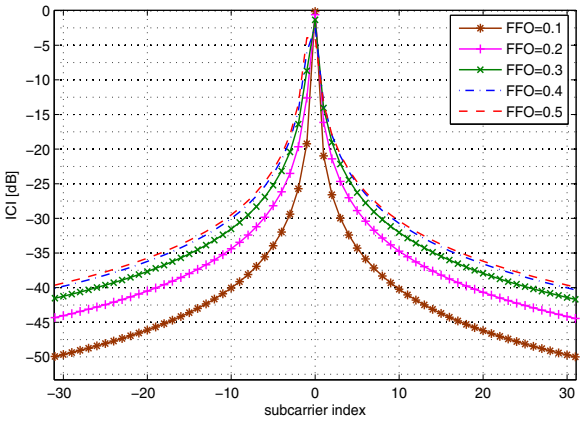


Fig. 2. The interference power at each carrier index for various fractional offset values

where $R_B$ and $R_E$ are the achievable rates of Bob and Eve respectively. For an OFDM system with $N$ subcarriers, the rate is given by the summation of the rates of each individual subchannel

$$R = \sum_{k=1}^{N} \log_2(1 + \mathrm{SINR}(k)) \quad (15)$$

where $\mathrm{SINR}(n)$ is the signal to interference plus noise ratio of the $k^{th}$ subchannel. Hence, for Bob's channel

$$\mathrm{SINR}_B(k) = \frac{|H(k)|^2}{N_B} P_t \quad (16)$$

where $N_B$ is Bob's noise power and $P_t$ is the transmitted signal power. Note that there is no interference component, since the carrier offset is pre-compensated for Bob's channel according to (11). On the other hand, for Eve's case

$$\mathrm{SINR}_E(k) = \frac{|q_k(k)|^2 P_t}{\sum_{k' \neq k}^{N} |q_{k'}(k)|^2 + N_E} \quad (17)$$

where $[q_1(k)\ q_2(k)..\ q_N(k)]$ is the $k^{th}$ row of Eve's interference matrix given from (13) by $\mathbf{Q} = \mathbf{E_E H_E P}$. Hence, the secrecy rate can be rewritten as

$$R_s = \sum_{k=1}^{N} \log_2 \left( \frac{1 + P_t |H(k)|^2 / N_B}{1 + P_t |q_k(k)|^2 / \left( \sum_{k' \neq k}^{N} |q_{k'}(k)|^2 + N_E \right)} \right) \quad (18)$$

## V. Simulation Scenario and Results

To verify the performance of the proposed transceiver structure with carrier offset pre-compensation, we simulate an OFDM system of 64 subcarriers and QPSK modulation with a multi-tap channel model of Rayleigh fading distribution. The power delay profile is a normalized 8-tap exponentially decaying profile with a delay spread smaller than the CP. First, we assume perfect channel and offset estimation, then we show in our figures that the effect of the estimation error will just introduce some noise floor to the receiver. Also we assume a conventional receiver for Eve, that is, a receiver that tries to compensate the frequency offset and estimate the one-tap channel based on the received signal.

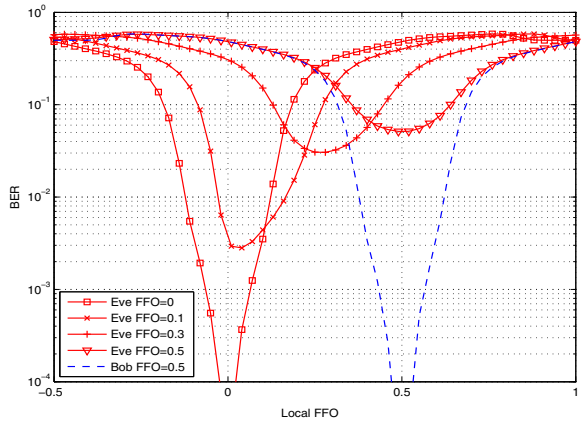


Fig. 3. BER vs. local carrier offset FFO for Bob (blue) and Eve (red) at different pre-compensated FFO values

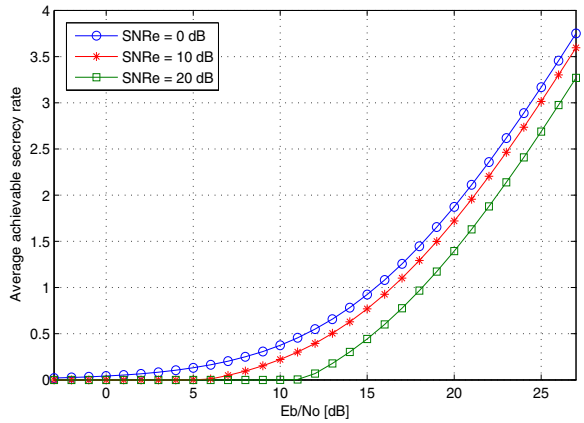


Fig. 4. The change of the average achievable secrecy rate per subchannel with respect to Eb/No of Bob's channel at FFO=0.5

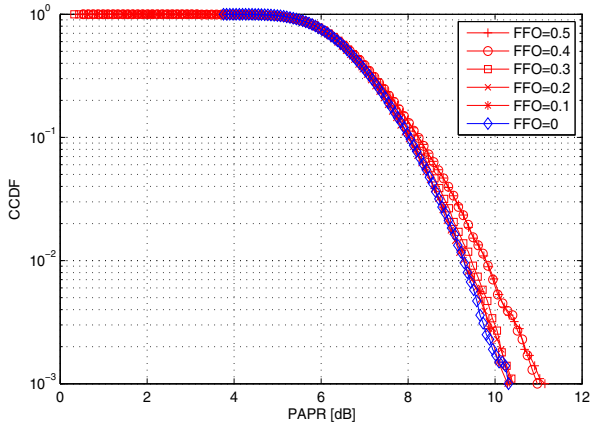


Fig. 5. PAPR distribution at different pre-compensated FFO values

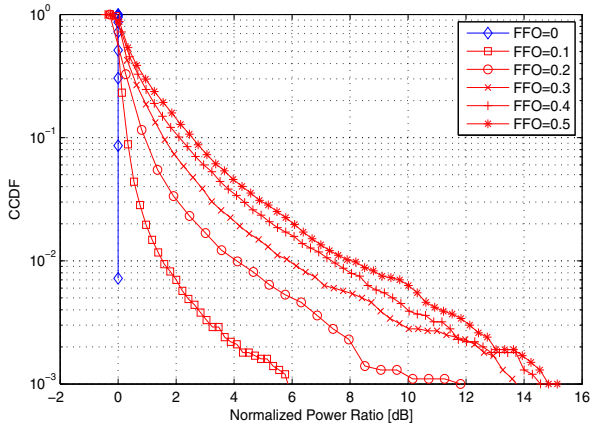


Fig. 6. Power distribution normalized to zero-offset average power at different pre-compensated FFO values

First, we test for the fading channel without any noise. Fig. 3 shows the Bit Error Rate (BER) vs. the local carrier offset at different pre-compensated FFO values. It shows the degradation of Eve's performance as the offset value increases. On the other hand, Bob receives the data error-free when the local offset is the same as the pre-compensated value, that is, there is no mismatch in the offset estimation between transmitter and receiver. In case of an estimation error, some BER will start to appear as shown by the V-shaped performance of FFO = 0.5 for Bob. Note that Eve has the same V-shaped performance at FFO = 0. Since this security scheme depends on the self-ICI induced, the best case is for FFO = 0.5 which gives the largest spectral leakages among subcarriers. It is clear that, with the same FFO value as Bob, Eve still suffers from performance degradation.

For Evaluating the secrecy performance, we calculate the average achievable secrecy rate per subchannel for different Eb/No values of Bob's channel. Fig. 4 shows the change of the achievable secrecy rate with the change of SNR of Eve's channel for the largest pre-compensated FFO of 0.5. Since we want to measure the performance of our scheme, we added the noise to Eve's channel based on the signal power without the interference component. That is why we plot the rate at different SNR, not SINR for Eve. It is clear that we can achieve a positive secrecy rate even when the SNR at Bob is lower than that at Eve.

We now take a look at the power aspects of this technique. The transmitted power is expected to increase as a function of the FFO until we reach 0.5, due to the pre-compensation stage. Also the Peak to Average Power Ratio (PAPR) is a crucial factor affecting signal linearity and front-end design. Figures 5 and 6 show the distributions of the PAPR and the average power of the transmitted signal, for different offset values. While higher powers become more probable with increasing the offset value, this technique doesn't change PAPR much as shown.

A major contributor to the power increase is the inverse channel response $\mathbf{H_f^{-1}}$ in the pre-compensation stage. In a practical system, a threshold $\tau$ can be introduced as a design parameter. For subcarriers with estimated frequency response of magnitude $|H(k)| < \tau$, magnitude of the corresponding coefficients used in the pre-compensation stage are forced to this threshold value. This will reduce the power increase at the transmitter at the expense of a residual interference at the

receiver. Moreover, it will create an error floor that depends on the value of the threshold. The same effect is introduced by channel estimation errors or imperfect channel reciprocity case. Shown in Fig. 7 is the effect of different threshold values on the signal power in case of a 0.5 offset. While the PAPR is not affected by the threshold, transmitted power decreases as expected. Fig. 8 shows the respective increase of the error floor. Hence, depending on the SNR range of operation, the threshold value is chosen to provide an acceptable BER performance.

## VI. Conclusion

In this paper, one of the critical drawbacks of OFDM systems is exploited for secrecy. The inter-carrier interference caused by carrier frequency offset is controlled to degrade the eavesdropper performance without affecting the performance of the legitimate user. This is feasible via the knowledge of the channel state information and the carrier offset value of the legitimate user. The simple structure of the proposed scheme shifts all the computational complexity from the mobile receiver to the base station, which makes it convenient for future low-consumption green radios. Also the power consumption of the scheme is treated. The choice of a threshold parameter provides acceptable performance depending on the SNR range of operation at the receiver. Moreover, we provide some secrecy rate results, leaving the investigation of the secrecy capacity of such scheme as a future work, along with the effect of the channel selectivity.

## Acknowledgment

This work was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under project number 114E244.

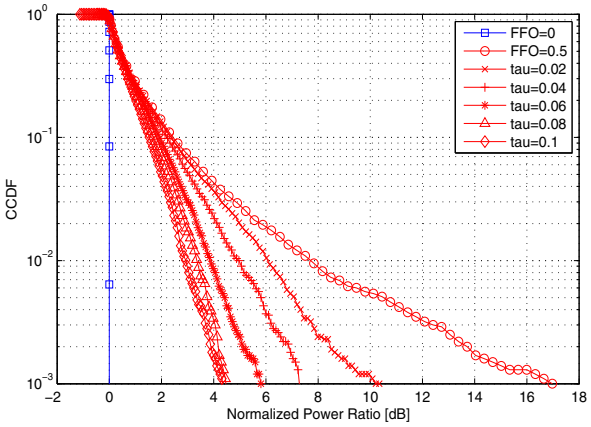


Fig. 7. Power reduction for 0.5 FFO at different threshold values

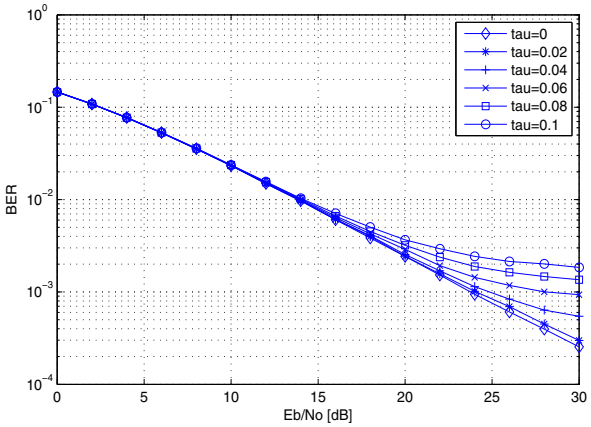


Fig. 8. BER performance for 0.5 FFO at different threshold values

## References

[1] A. D. Wyner, "The Wiretap Channel," Bell Syst. Tech. Journal, vol. 54, pp. 1355-1387, 1975.

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wiretap Channel," IEEE Trans. Inform. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.

[3] M. Bloch, J. Barros, M. Rodrigues and S. McLaughlin, "Wireless Information-Theoretic Security," IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[4] K. Ren, H. Su, and Q. Wang, "Secret Key Generation Exploiting Channel Characteristics in Wireless Communications," IEEE Wireless Commun., vol. 18, no. 4, pp. 6-12, Aug. 2011.

[5] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 13541367, Aug. 2012.

[6] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," IEEE Trans. Signal Processing, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 21802189, 2008.

[8] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical Layer Security forTwo-Way Untrusted Relaying With Friendly Jammers," IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[9] H. Koorapaty, A. Hassan and S. Chen., "Secure information transmission for mobile radio," IEEE Commun. Lett., vol. 4, pp. 52-55, Feb. 2000.

[10] A. O. Hero, "Secure space-time communication," IEEE Trans. Inform. Theory, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[11] T. Yucek and H. Arslan, "OFDM signal identification and transmission parameter estimation for cognitive radio applications," Proc. IEEE Global Telecomm. Conf. (Globecom), Washington, D.C., USA, Nov. 2007.

[12] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," IEEE J. Select. Areas Commun., vol. 23, no. 5, pp. 963-972, May 2005.

[13] Z. E. Ankaral, M. Karabacak and H. Arslan, " Cyclic Feature Concealing CP Selection for Physical Layer Security," IEEE Military Commun. Conf. (MILCOM), 2014.

[14] T. Yucek, and H. Arslan. "Feature suppression for physical-layer security in OFDM systems," IEEE Military Commun. Conf. (MILCOM), 2007.

[15] T. Pollet, M. Van Bladel, and M. Moeneclaey, "BER sensitivity of OFDM systems to carrier frequency offset and Weiner phase noise," IEEE Trans. Commun., vol. 43, pt. 1, pp. 191193, Feb.-Apr. 1995.

[16] Schmidl, M. Timothy, and C. Cox. Donald "Robust frequency and timing synchronization for OFDM," IEEE Trans. Commun., vol. 45, no. 12, pp. 1613-1621, 1997.

[17] J.-J. van de Beek, P. O. Borjesson, M.-L. Boucheret, D. Landstrom, J. M. Arenas, P. Odling, C. Ostberg, M. Wahlqvist, and S. K. Wilson, "A time and frequency synchronization scheme for multiuser OFDM," IEEE J. Sel. Areas Commun., vol. 17, no. 11, pp. 1900-1914, Nov. 1999.

[18] Z. Cao, U. Tureli, Y.-D. Yao, and P. Honan, "Frequency synchronization for generalized OFDMA uplink," Proc. IEEE Global Telecomm. Conf. (Globecom), vol. 2, Nov. 2004, pp. 1071-1075.

[19] J. Choi, C. Lee, H. W. Jung, and Y. H. Lee, "Carrier frequency offset compensation for uplink of OFDM-FDMA systems," IEEE Commun. Lett., vol. 4, no. 12, pp. 414-416, Dec. 2000.

[20] Barros, Joao, and Miguel RD Rodrigues, "Secrecy capacity of wireless channels," IEEE Inter. Symp. Inform. Theory, pp. 356-360, 2006.