Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

ICEENG

11th International Conference
on Electrical Engineering
ICEENG 2018

The Impact of Different Jamming Techniques on OFDM Communication Systems

Mohamed M. Wanis,*   Ehab M. Shaheen,* and M.Samir*

Abstract:

In this paper an investigation to the performance of a single input single output orthogonal frequency division multiplexing (OFDM) system in additive white Gaussian noise (AWGN) channel in the presence jamming is provided. The effect of different types of jamming techniques such as the traditional noise jamming schemes (presented by barrage band, partial band and pulsed jamming) and waveform jamming (matched jamming signal) is investigated on the performance of OFDM communication systems. Two novel jamming schemes are proposed (the first is a noise jamming technique and the second is a waveform jamming technique). The performance of the two proposed jamming schemes is compared with the previously mentioned jamming techniques. It will be shown that the two proposed jamming schemes outperforms the other traditional jamming techniques. Also, it will be shown that the proposed waveform jamming scheme is more efficient than the proposed noise jamming one. Yet, the latter outperforms in the issue of cost and complexity.

Keywords :

OFDM; Noise jamming; Waveform Jamming; IEEE802.11a.

───

* Egyptian Armed Forces

1- Introduction

The evolution of telecommunications industry from wired phones to wireless personal communication services results in an uprising demands on wireless systems and products. This is important to maintain an efficient performance and stability in spite of the complexity. In order to sustain an efficient performance which provides services such as Internet with high speed, multimedia messaging, video streaming and broadcasting; high data rates and capacities must be provided.

Nowadays; orthogonal frequency division multiplexing (OFDM) become one of the most considered wireless communication technique. This is due to its ability to provide high data rates and to maximize the bandwidth usage by orthogonal arrangement of frequency sub carriers [1]. OFDM has been adopted as the modulation/demodulation scheme in several digital communication standards. Mainly in wireless systems such as digital audio and terrestrial digital video broadcasting (DAV/DVB-T), local area networks (IEEE 802.11a/g/n) and metropolitan area networks (IEEE 802.16a), along with the fourth generation of mobile cellular communication and multiband OFDM ultra wideband systems [2].

Yet, the performance of OFDM system maybe deteriorated due to presence of intentional (jamming) or non-intentional (interference) signals. Jamming is defined as the deliberate use of radio noise or waveform signals in an attempt to disrupt communications. By other words it is the use of active signals to prevent a communication system from effectively exchanging information [3]. The issue of interference or jamming has been covered previously in many literatures. In [4] where the performance of OFDM system was investigated in presence of multi-tone jamming. In [5] the impact of multiple attacks against the OFDM preamble synchronization stage. It has been shown that these attacks can debilitate the OFDM receiver's performance. In [6] they applied swift attacks on the OFDM system frequency offset estimation mechanism also they proposed three different approaches to mitigate such an attack.

It was noted that from all these mentioned previous works the jamming signal was mainly adapted as a noise signal. To this end; the main contributions in this paper can be summarized as follows.

- A novel noise jamming signal (Pulsed Noise jamming (PPBJ)) is proposed and its impact on the performance of OFDM system is analytically investigated.
- A novel waveform jamming signal (Matched waveform jamming (PMJ)) is proposed and its impact on the OFDM system's performance is analytically evaluated.
- A comparison analysis among the proposed techniques and the traditional noise jamming techniques are presented.

This paper is organized as follows. Section II depicts the OFDM system model. The different jamming signal models (noise and waveform jamming signals) including the two

proposed jamming schemes are depicted and analytically evaluated in section III. Numerical and simulation results are presented in section IV. Finally, section V draws the conclusions.

2- System   Model

The frequency domain representation of the OFDM signal is shown in figure (1). The fast Fourier transform (FFT) and inverse fast Fourier transform (IFFT) are used to achieve the orthogonality among the subcarriers. In the OFDM transmission system, N-point IFFT is taken for the transmitted symbols.
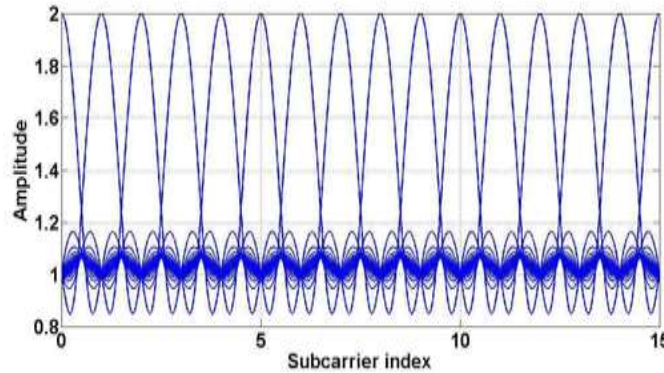

Fig. 1. *OFDM Signal in frequency domain*

The corresponding discrete-time OFDM symbol at the transmitter can be expressed as [1]

$$x_l[n] = IFFT\{X_l[k]\} = \sum_{k=0}^{N-1} X_l[k]e^{\frac{j2\pi kn}{N}}, \tag{1}$$

Where N is the number of subcarriers.

It is assumed that the channel is the AWGN channel. Let $x_l[n]$ be the transmitted signal and $y_l[n]$ be the received signal respectively, In presence of jamming signal, the received signal can be written as

$$y_l[n] = h_l[n] * x_l[n] + g_l[n] * J_l[n] + w_l[n], \tag{2}$$

Equation (2) depicts the transmitter-receiver pair under jamming attack where $h_l[n]$ and $g_l[n]$ are the channel impulse responses of the transmitted signal and the jamming signal respectively, and $w_l[n]$ is the independent and identically distributed AWGN signal samples with distribution N $(0,\sigma_n^2)$ [7].

Noted that the jamming signal $J_l[n]$ can be expressed as

$$J_l[n] = \frac{1}{N} \sum_{k=0}^{N-1} j_l[k]e^{\frac{j2\pi nk}{N}} \tag{3}$$

where $j_l[k]$ is the jamming signal representation in frequency domain with power equals $\frac{\|j_l[k]\|^2}{2}$ [8] .

$$Y_l[k] = FFT\{y_l[k]\} = \sum_{k=0}^{N-1} y_l[n]e^{\frac{-j2\pi kn}{N}} \qquad (4)$$

The main two classifications are the noise jamming and waveform jamming. In this paper, the considered types of noise jamming signals are barrage band jamming, pulsed jamming and partial band jamming along with the proposed noise jamming technique. Whereas, the second considered jamming signal form is the waveform jamming technique which include the matched jamming (MJ) signal along with the proposed waveform jamming technique.

3- JAMMING SIGNAL MODELS

A. Noise Jamming

1) Barrage Band Jamming

Barrage jamming (BJ) is one of the earliest forms of jamming attacks, where the whole spectrum of the target signal is being jammed. This is achieved by injecting to the system a band-limited noise with bandwidth greater than the useful signal's bandwidth. It has the same effect of AWGN, except it results in a significant increase in the noise variance σ_N^2 which in turn resulting in an overall increase in the noise floor. Thus, one can expect degradation in the signal to noise ratio (SNR) on the entire bandwidth.

$$PSD_{BJ} = N_0 + N_J \qquad (5)$$

Where N_0 is the AWGN PSD and NJ is the PSD of the barrage jamming signal [9].Figure (2) depicts the scenario of BJ. Usually this kind of jamming attack used as a reference in evaluating other jamming strategies. The BER for QPSK modulated OFDM system under BJ attack can be expressed as [9] and [10]
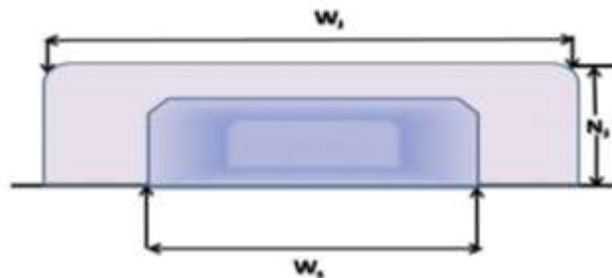

Fig. 2. Barrage Jamming

Usually this kind of jamming attack used as a reference in evaluating other jamming strategies. The BER for QPSK modulated OFDM system under BJ attack can be expressed as [9] and [10]

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_{0+}N_J}}\right) \tag{6}$$

2) Partial Band Noise Jamming

In partial band jamming (PBJ), only a certain portion of the entire system bandwidth is jammed. If the jamming power is constant, then the performance of the PBJ depends on the fraction between jamming bandwidth and signal bandwidth. The jammer to signal power ratio (JSR),δ, can be described by

$$\delta = \frac{W_J}{W_s} \tag{7}$$

In PSD of the PBJ technique is depicted in figure (3). If the average PSD of PBJ is N_J, then the effective PSD of PBJ in the jammed bands becomes $\frac{N_J}{\delta}$.
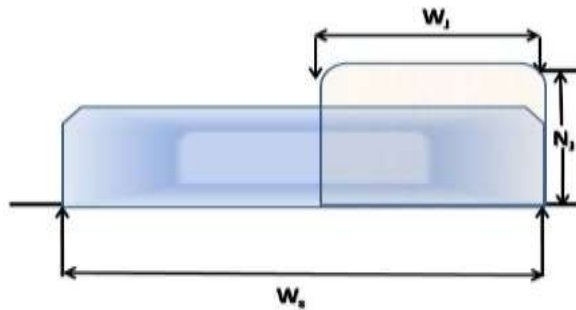

Fig. 3. *PBJ Technique.*

The BER for QPSK modulated OFDM system under PBJ can be written as [9] and [10]

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_{0+}\frac{N_J}{\delta}}}\right) \tag{8}$$

3) Pulsed Jamming Technique

Pulse jamming is similar in concept to PBJ. Yet, the duty cycle of the pulsed jamming, which is the ratio of the pulse duration to the repetition period determines the relationship between the average power and peak power. The jamming effect depends on the peak power

and how often that signal returns to the receiver. In pulsed jamming; the jammer transmits broadband noise but for only a fraction of time with large power.

Considering the case where the jammer pulse duration is greater than the transmitted signal bit duration. Then, a particular transmitted data bit either encounters a channel with jammer on with probability ρ or jammer off with probability (1-ρ).

$$\grave{N}_j = \frac{J}{W_J} = \frac{N_J}{\rho} \tag{9}$$

The BER for QPSK modulated OFDM system under pulsed jamming can be written as [9] and [10]

$$P_b = \rho.Q\left(\sqrt{\frac{2E_b}{N_{0+}\frac{N_J}{\rho}}}\right) + (1-\rho).Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{10}$$

4) Proposed Noise Jamming Technique

In order to maximize the impact of the jamming signal a combination between two noise jamming techniques is proposed. These jamming techniques are the BPJ and the pulsed jamming. The proposed jamming technique can be called partial-pulsed band jamming (PPBJ). Noted that in the proposed PPBJ jamming scheme, the jammer is assumed to transmit the partial band noise for a fraction of time instead of transmitting a broadband noise as considered in most of the previous literatures [3].

The proposed PPBJ noise technique in this case can be easily derived as

$$P_b = \rho.Q\left(\sqrt{\frac{2E_b}{N_{0+}\frac{N_J}{\delta\rho}}}\right) + (1-\rho).Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{11}$$

B.　Waveform Jamming (Matched Jamming vs. Proposed Jamming Technique)

While BJ can be considered the effective jamming technique when the jammer lacks the target information. However, wideband systems such as OFDM requires a lot of energy to be jammed on. This is due to its large bandwidth. Researchers attempted to invent various partial band jamming techniques that require much less power than BJ. Conventional noise jamming techniques are not effective against OFDM waveform because it only can successfully jam individual subcarriers resulting in ineffective jamming performance. In this paper, a waveform jamming signal that capable of doing more harm to the victim signal is proposed.

The first considered waveform jamming signal is a signal matched or similar to the OFDM transmitted victim signal. This signal is called MJ signal. As, the OFDM receiver performs FFT operation to convert time domain signal to frequency domain signal. Forward FFT takes a signal, multiplies it successively by complex exponential over a range of frequencies, sums each product and plots results as a coefficient of that frequency. However, if the input signal is not perfectly periodic in the sample window or have offset at sampling frequencies, then the energy gets smeared from the true frequency into adjacent frequency bins that eventually creates Inter Carrier Interference (ICI) of the OFDM waveforms at the receiver [10]. Besides the tail or side-lobes of a signal are not aligned with the orthogonal OFDM subcarriers due to presence of frequency offset which can be a source of ICI.

Noted that carrier frequency offset (CFO) adds an extra phase factor that can harm the received signal affecting OFDM System overall performance. Secondly, the idea of the proposed waveform jamming technique was based on creating an intentional CFO on a matched OFDM jamming signal.

The proposed matched jamming (PMJ) signal can be expressed as

$$J_{PMJ}[\mathrm{n}] = \frac{1}{N} \sum_{k=0}^{N-1} j_{Matched}[k] e^{\frac{j2\pi(k+\varepsilon)n}{N}}$$

(12)

where $j_{Matched}[k]$ is the jamming signal in the frequency domain with power equals to $\frac{\|j_{Matched}[k]\|^2}{2}$, and ε is the normalized CFO [9], If the target subcarrier spacing is, Δf_{SC}, and jamming CFO from target's center frequency is, f_{offset}, then the normalized CFO, ε, can be written as [1]

$$\varepsilon = \frac{f_{offset}}{\Delta f_{SC}}$$

(13)

One can expect a change in the signal's phase offset in time domain. This change is proportional to a frequency shift in the frequency domain. Generally, the normalized CFO, ε, can be written as [1]

$$\varepsilon = \varepsilon_i + \varepsilon_f$$

(14)

where ε_i denotes the integer (IFO) part and ε_f denotes the fractional frequency offset (FFO) part of the normalized CFO (ε), respectively.

Noted that IFO doesn't introduce any ICI among the sub-carriers spacing. Yet, it introduces a cyclic shift of data sub-carriers and a phase change proportional to the OFDM symbol number. This has no effect on the OFDM sub-carriers orthogonality. On the other hand, the FFO Causes a rotation and introduces ICI among the OFDM sub-carriers. This leads to a destruction of the OFDM sub-carriers orthogonality resulting in a degradation of the overall system BER.

The received signal $\widetilde{Y}[k]$ can be expressed as

$$\tilde{Y}[k] = \frac{1}{\widehat{H}[k]}(FFT\{y_l[n]\}) = \frac{1}{\widehat{H}[k]}\left(\sum_{n=0}^{N-1} y_l[n]e^{\frac{-j2\pi kn}{N}}\right) \tag{15}$$

Where $\widehat{H}[k]$ denotes the channel impulse response value on the path between transmit antenna and receive antenna at time k.

Expanding equation (15), it can be rewritten as

$$\tilde{Y}[k] = \frac{1}{\widehat{H}[k]}\left(\sum_{n=0}^{N-1}\frac{1}{N}\sum_{m=0}^{N-1}H[m]e^{\frac{j2\pi mn}{N}}X_l[m]e^{\frac{-j2\pi kn}{N}} + \sum_{n=0}^{N-1}\frac{1}{N}\sum_{m=0}^{N-1}G[m]e^{\frac{j2\pi mn}{N}}J_{Matched}[m]e^{\frac{-j2\pi kn}{N}}\right) + \sum_{n=0}^{N-1}w_l[n]e^{\frac{-j2\pi kn}{N}} \tag{16}$$

$$\tilde{Y}[k] = \frac{1}{\widehat{H}[k]}\left(H[k]X_l[k] + \frac{1}{N}\sum_{m=0,m\neq k}^{N-1}G[m]\ J_{Matched}[m]\frac{1-e^{j2\pi(m-k+\varepsilon)}}{1-e^{\frac{j2\pi(m-k+\varepsilon)}{N}}} + W_l[k]\right)$$

Finally, the received signal in presence of the proposed jamming can be written as

$$\tilde{Y}[k] = \frac{H[k]}{\widehat{H}[k]}X_l[k] + e^{\frac{j\pi\varepsilon(N-1)}{N}}\left[\frac{\sin(\pi\varepsilon)}{N\sin\left(\frac{\pi\varepsilon}{N}\right)}\right]\frac{G[k]}{\widehat{H}[k]}\ J_{Matched}[k] +$$

$$e^{\frac{j\pi\varepsilon(N-1)}{N}}\sum_{m=0,m\neq k}^{N-1}\frac{\sin(\pi(m-k+\varepsilon))}{N\sin\left(\frac{\pi(m-k+\varepsilon)}{N}\right)}\frac{G[m]\ J_{Matched}[m]}{\widehat{H}[m]}e^{\frac{j\pi(m-k)(N-1)}{N}} + \tag{17}$$

$$\frac{W_l[k]}{\widehat{H}[k]}$$

It can be seen that the jammer has two fold effects in equation (17). The first term represents the desired useful signal component. Whereas, the second term represents the amplitude and phase change of the jamming signal frequency component that results a scaling to the jamming signal. The third term represents the impact of the proposed jamming signal components on the victim signal results in orthogonality lost among the subcarriers of the victim signal

4- Analytical and Simulation Results

In this section the analytical formulas will be validated by the aid of extensive simulation experiments. It was assumed that the victim OFDM communication system is modeled as the standard OFDM based IEEE802.11a wireless local area network ((MJ)). Simulation results were adapted by using 105 Monte-Carlo iterations with variable SNR and signal to jamming ratio (SJR) values.

The scenario of noise jamming signals along with the proposed noise jamming signal is investigated first.

Figure (5) depicts a comparison among the four noise jamming techniques (BJ, PPJ, pulsed jamming and the proposed PPBJ) at different SJR values and at SNR = 5dB. It can be seen that the proposed PPBJ jamming technique outperforms the other four jamming techniques. In order to achieve a BER = 10^{-1}, an increase in the SJR about 2dB if the proposed PPBJ is used when compared with the BJ technique. Also, an increase in the SJR about 7dB when compared with PBJ technique (which occupies 50% of the victim signal bandwidth).

Figure (6) depicts a comparison between the BJ technique and the proposed PPBJ noise jamming technique at SNR = 5dB, and at different values (δ). As expected it can be seen that the performance of the OFDM system deteriorated as the value of δ decreases in the proposed PPBJ technique

Figure (7) investigates depicts the optimal value of ε that produces the maximum error magnitude in waveform jamming scenario. It can be seen that the simulation and analytical results are in a good match, the simulated results are slightly better than theoretical results because the simulated results are computed using average error for all subcarriers. From this figure one can see that the optimal value for ε is found to be equal to 0.5.
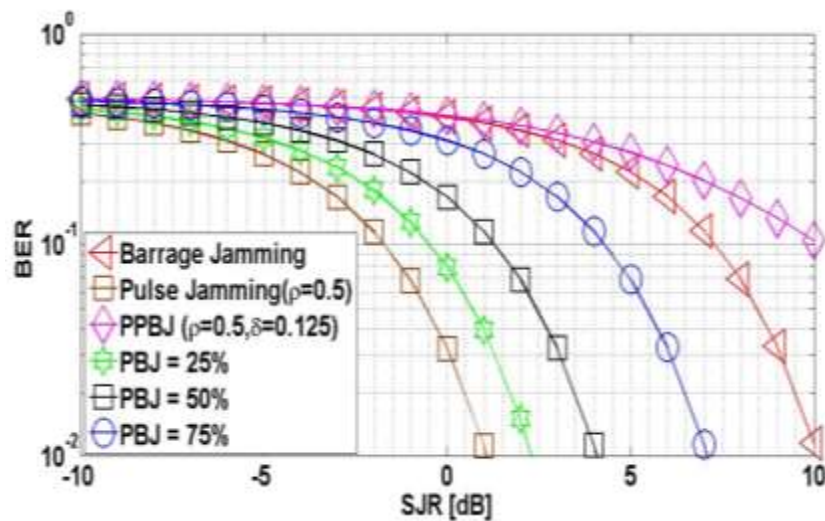

Fig. 5. *BER Performance of the IEEE802.11a OFDM based WLAN system under different noise jamming techniques, SNR = 5dB.*
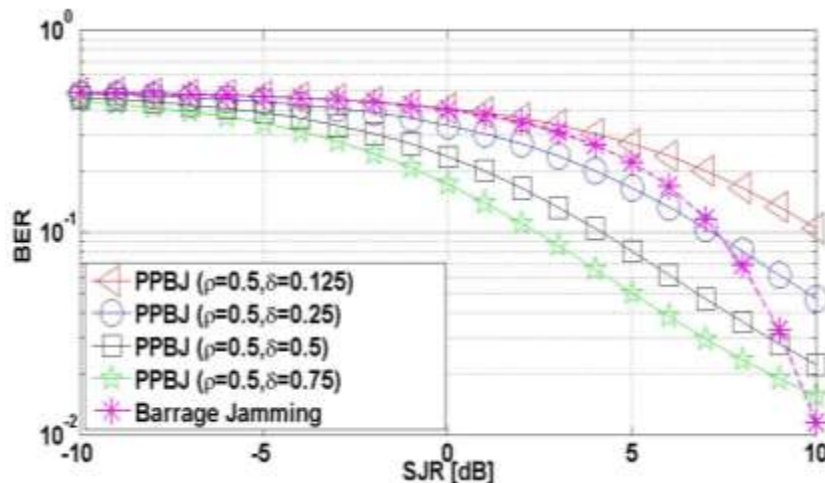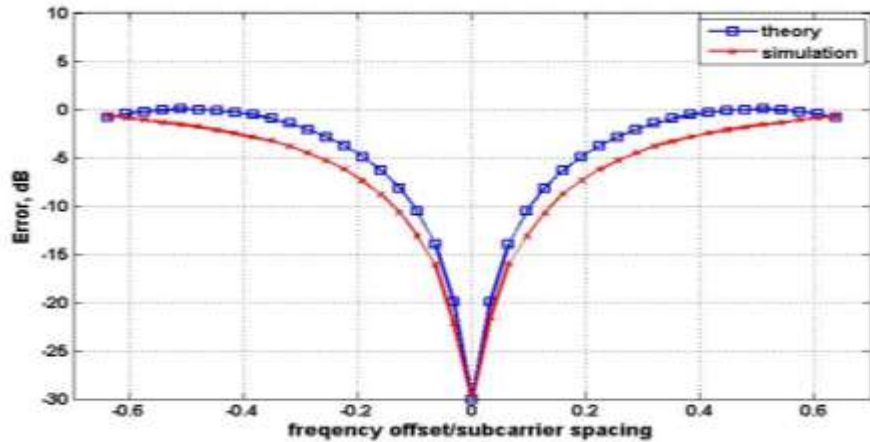

9

Fig. 7. *Error magnitude against different values of CFO*

Figure (8) depicts the impact of changing the CFO value on the BER performance of OFDM system at SNR = 0dB and 10dB. It can be seen that as evaluated in Figure (8), the maximum error occurred at $\varepsilon = 0.5$.
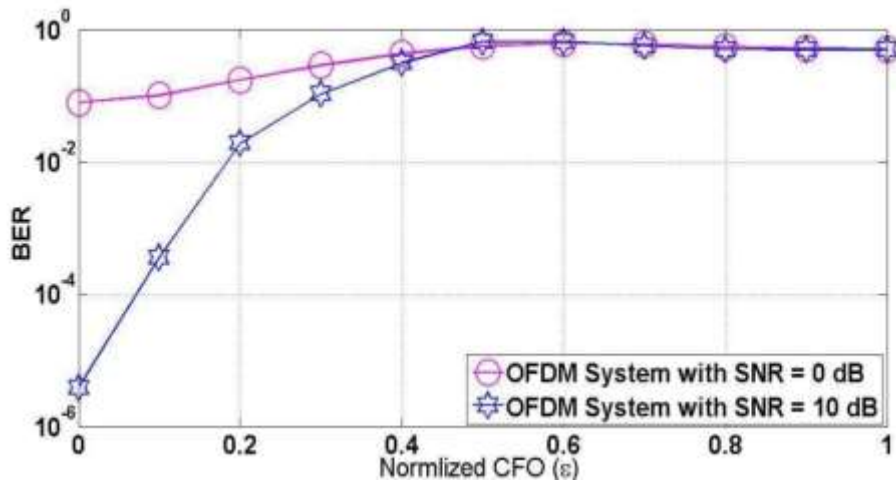

Fig. 8. *BER of OFDM System at different values of Normalized CFO ε*

Figure (9) depicts the BER performance of the OFDM system in absence and presence of MJ waveform technique (no CFO, $\varepsilon = 0$) at different SJR = 5dB, 8dB and 10dB respectively. There is a difference between the simulation and theoretical results due to the effect of

removal of cyclic prefix. It can be seen that the performance of the IEEE802.11a OFDM system can be severely degraded in the presence of high power MJ signal.
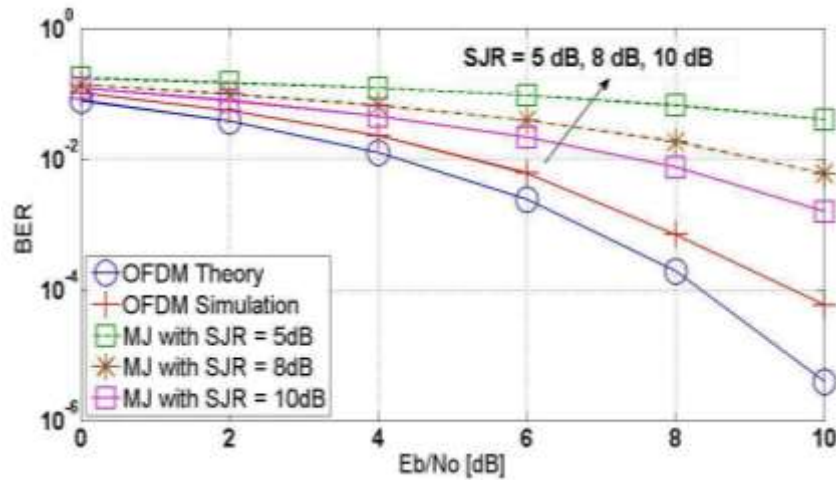

Fig.9. *OFDM BER Performance for MJ technique (ε = 0) with different SJR values*

Figure (10) depicts the BER performance of the OFDM system under the PMJ waveform technique (ε = 0.5 and SJR = 10dB). It can be seen that the performance of the OFDM system completely degraded in presence of such jamming technique. Finally, Figure (11) depicts a comparison between the MJ technique (ε = 0) and the PMJ waveform technique (ε = 0.5) at SJR = 5dB. It can be that the PMJ waveform technique outperforms the MJ technique.
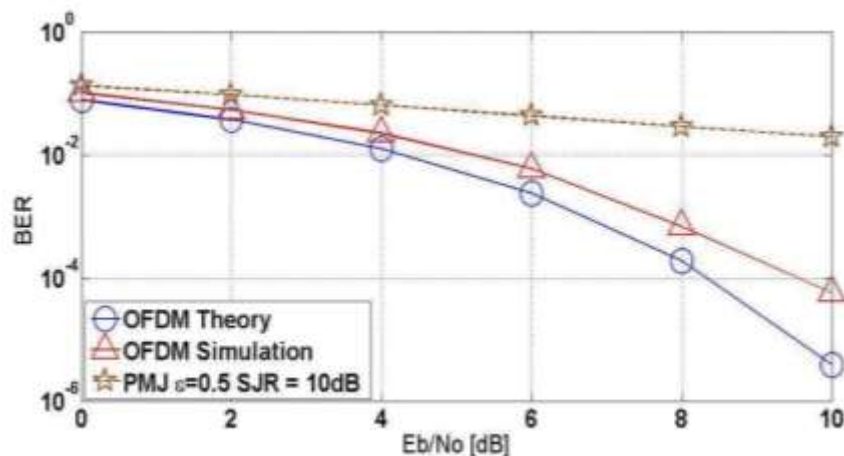
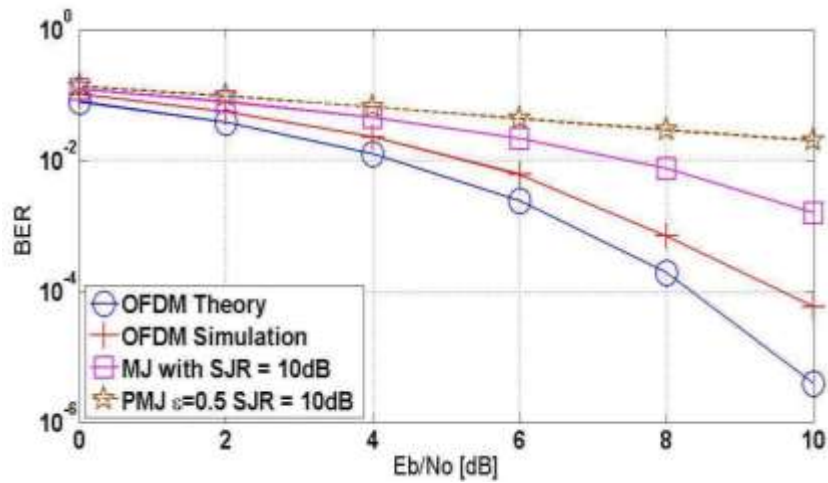**Fig.10**. *OFDM BER Performance for PMJ technique (ε = 0.5) with SJR = 10 dB*

Fig.11. *OFDM BER Performance for MJ (ε = 0) technique versus PMJ technique (ε = 0.5) with SJR = 10 dB*

V- CONCLUSION

In this paper, the BER performance of the OFDM system is investigated jamming. Two novel jamming techniques were analytically proposed. One is a noise jamming technique and the other is a waveform jamming technique. It was proven analytically that the proposed noise jamming technique outperforms the others traditional noise jamming techniques (such as BJ, PPJ and pulsed jamming). Also, it was shown analytically that the proposed waveform jamming technique completely deteriorate the BER performance of the OFDM system. One can choose between these two jamming techniques with respect to the issue of complexity and cost. The proposed noise jamming technique is much simpler than the proposed waveform jamming one. Yet, the latter is proven to be much efficient.

References:

[1] Y. Cho, J. Kim, W. Yang, and C. Kang, MIMO-OFDM Wireless Communications with MATLAB. John Wiley & Sons, 2010. [2] D. Tao, X. Li, X. Wu and S. Maybank, Human Carrying Status in Visual Surveillance, IEEE Conference Computer Vision and Pattern Recognition, Vol. 2, P. 1670-1677, 2006.

[2] E. M. Shaheen and M. El-Tanany, "The impact of narrowband interference on the performance of UWB systems in the IEEE802.15.3a channel models," CCECE 2010, Calgary, AB, 2010, pp. 1-6. doi: 10.1109/CCECE.2010.5575235R.

[3] Poisel, Modern Communication Jamming Princples and Techniques, Artech House, 2011. [5] D. Tan, K. Huang, S. Yu, and T. Tan, Orthogonal Diagonal Projection for Gait Recognition, International Conference on Image Processing (ICIP'07), Vol. 1, P. 337-340, 2007.

[4] W. Ping, and Sun Guozhong, "Performance of OFDM in Presence of Multitone Jamming," IEEE Symposium on Robotics and Applications (ISRA 2012).

[5] M. J. La Pan, T. C. Clancy, and R. W. McGwier, "Jamming Attacks Against OFDM Timing Synchronization and Signal Acquisition," IEEE Military Communications Conference, 2012.

[6] H. Rahbari, M. Krunz, and L. Lazos, "Swift Jamming Attack on Frequency Offset Estimation: The Achilles' Heel of OFDM Systems," IEEE Transactions on Mobile Computing, Vol. 15, Issue: 5, 2016 .

[7] T. S. Rappaport, Wireless communications Principles and Practices, 2nd Edition, 2001.

[8] S. Amuru and R. M. Buehrer, "Optimal Jamming Strategies in Digital Communications – Impact of Modulation," pp. 1619 – 1624, IEEE Global Communications Conference, 2014.".

[9]   C. Shahriar, S. Sodagari, R. McGwier, and T. C. Clancy, "Performance Impact of Asynchronous Off-tone Jamming Attacks against OFDM," IEEE International Conference on Communications, ICC2013, June 2013.

[10] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," IEEE Communications Magazine, pp. 54-61, vol. 54, Issue 4, 2016.