A Novel Encryption Technique for LTE-PHY Layer with OFDM Modulation using Wavelet Transform

Rakesh. S
PG Student
Department of ECE, M.Tech (DCN)
BTLITM, Bangalore, India

Prof. Prathima
Asst Professor
Department of ECE, M.Tech (DCN)
BTLITM, Bangalore, India

***Abstract*—Orthogonal Frequency Division Multiplexing (OFDM) and Multiple Input and Multiple Output (MIMO) are two main techniques employed in 4th Generation Long Term Evolution (LTE) with Conventional DFT for multicarrier data modulation and XOR encryption techniques performing bitwise XOR operation between one message bit and one key stream bit to generate one ciphertext bit. However, use of DFT is computationally complex and the use of XOR encryption results in large key size and hence higher frame size. Wavelet based OFDM provides good orthogonality and reduces the number of mathematical operations for multicarrier modulation, improving the Bit Error Rate (BER) and with the use of phase encryption on the modulated symbols the key length is reduced. The usage of wavelet based OFDM system does not require cyclic prefix which increases the spectral efficiency. Hence, we propose to use discrete wavelet transform(DWT) in place of Fast fourier transform(FFT) in the conventional OFDM system and with the inclusion of phase encryption, show that a wavelet based system with phase encryption provides a much better performance than a conventional OFDM system.**

Keywords—OFDM; Wavelet; BER; Encyrption.

I. INTRODUCTION

In the modern day wireless applications some of the major factors to consider are spectral efficiency and the efficient usage of available bandwidth. If we choose modulation using multiple carriers or multi carrier modulation, this divides the data into several streams which can be used to modulate the different carriers. Since the subcarriers in OFDM are always orthogonal to each other, bandwidth efficiency is obtained without the presence of any ICI (Inter Carrier Interference).

A wavelet is a small waveform that has effectively limited duration having an average value of zero. Wavelet analysis consists of breaking up a signal into scaled and shifted versions of the original signal. . Wavelets are a class of functions used to localize a given function in both space and scaling. ISI (Inter Symbol Interference) and ICI (Inter Carrier Interference) are generally caused by loss of orthogonality between the carriers in a Discrete Fourier Transform (DFT) based OFDM. . ISI is between successive symbols of same sub-carrier and ICI is among different signals at different subcarriers. But, the use of cyclic prefix causes power loss and bandwidth inefficiency in DFT based OFDM.

When we look at the implementation of an encryption system for the OFDM system, conventional encryption or the stream cipher encryption involves performing of XOR operation between one message bit and one key stream bit which generates a cipher text. The reason why XOR is chosen is due to its hardware efficiency. But when it comes to LTE which uses OFDM, phase encryption would be more suitable. It involves multiplying the real and imaginary components of time domain OFDM samples by two {1,−1} binary key streams at the PHY layer to provide data confidentiality.

In this paper we have compared the performance of wavelet based OFDM system with the performance of conventional OFDM system for different LTE modulation techniques with the application of XOR and PHASE encryption. For wavelet based system we have used daubechies2 and haar wavelets. Additive White Gaussian Noise (AWGN) channel is used for transmission.

II.CONVENTIONAL OFDM SYSTEM

Orthogonal frequency division multiplexing (OFDM) is a multi-carrier modulation technique in which the original is split into many independent signals, each of which is modulated at a different frequency. The basic block diagram is shown in figure-1.As all the subcarriers are orthogonal to each other, they can be transmitted simultaneously over the same bandwidth without any interference. Thus, the available spectrum is utilized efficiently. The disadvantage of FDM i.e., the insertion of guard bands between the sub-carriers which results in wastage of the bandwidth is overcome here.

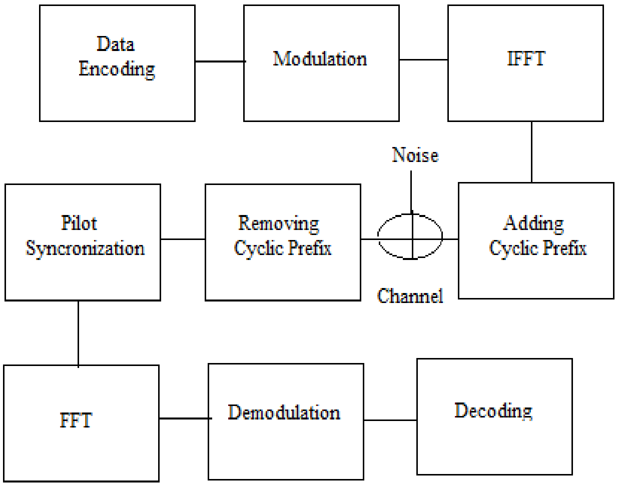

Figure-1: Conventional OFDM system

Practically, Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) are used for the implementation of the OFDM system because less number of computations required in FFT and IFFT. In order to protect the data from loss of symbols due to the synchronization problems a guard band or cyclic prefix is attached. Cyclic prefix is just the replica of a fraction of the signal. As long as the channel delay spread remains within the limit of the cyclic prefix there would not be any loss in orthogonality.

III.WAVELET BASED OFDM SYSTEM

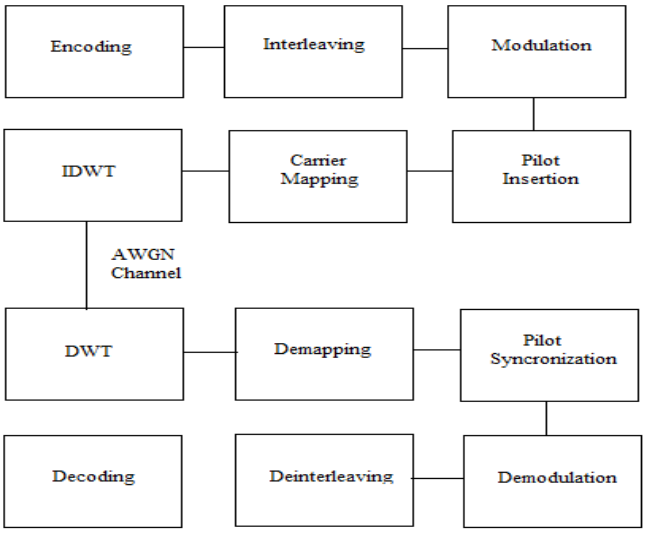

Figure-2: Wavelet Based OFDM system

Wavelet transform helps in the joint analysis of the data signal in both the time and frequency domain jointly. It is a multi resolution analysis mechanism where-in the input data is decomposed into different frequency components. Wavelet Transform compared to Fourier Transform possesses better orthogonality and hence are capable of reducing the power of the ISI and ICI, which results from loss of orthogonality. A conventional OFDM system uses cyclic prefixes to deal with ISI and ICI which makes it bandwidth in-efficient but wavelets do not need such a cyclic prefix to guard against ISI or ICI. With the use of wavelet transforms the complexity reduces from O[N log2 N] for Fourier transform to O[N] for wavelet transform. Discrete wavelet transform (DWT) initially passes the signal through a series of filters that decompose the original signal into low pass band and high pass bands through the filters. During decomposition the high pass filter will remove the frequencies below half of the highest frequency and low pass filter will remove frequencies that are above half of the highest frequency. The decomposition halves the time resolution because half of the samples are used to characterize

the signal similarly frequency resolution will be doubled and this decomposition process will be repeated again for obtaining the wavelet coefficients of required level.This process results in 2 types of co-efficients. First ones are called detailed co-efficients resulting from the high pass filters. The second ones are called coarse approximations resulting from low pass filters followed by the performing of decimation process. All these processes are performed until the required level is met.

This entire process of decomposition through the filters can be expressed using the equations:

$$res_{high}[k] = \sum_{n} x[n]\, HPF[2k-n]$$

$$res_{low}[k] = \sum_{n} x[n]\, LPF[2k-n]$$

x[n] is the original data signal, HPF[2k-n] is the impulse response of the high pass filter, LPF[2k-n] is the impulse response of the low pass filter, res[k] represents the resulting signals after filtering and decimation by a factor of 2.

In inverse Discrete Wavelet Transform (IDWT) the reverse process of decimation occurs i.e., up-sampling followed by the passage of the signal through the filters and the resulting data will be the reconstructed data. It needs to be noted that both decimation and reconstruction processes will both have the same number of levels.

IV. XOR AND PHASE ENCRYPTION

XOR encryption involves performing of XOR operation between one bit of the message and one bit of the keystream thereby resulting in one bit of a ciphertext making this kind of an implementation very hardware efficient.

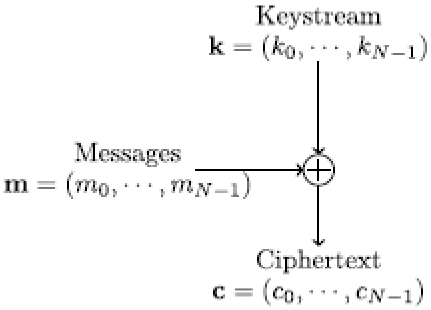
Keystream
$\mathbf{k} = (k_0, \cdots, k_{N-1})$
Messages
$\mathbf{m} = (m_0, \cdots, m_{N-1})$
Ciphertext
$\mathbf{c} = (c_0, \cdots, c_{N-1})$

Figure-3: XOR-Enc block.

Here m, k & c represent the message stream, keystream and the ciphertext respectively. The ciphertext c is a result of the XOR operation between the message bits m and the keystream k.

Phase-Enc on the other hand is performed on modulated symbols with each modulated symbol containing n = log2 M bits of message, where M is the constellation size. This means that phase enc depends upon the kind of modulation technique chosen.

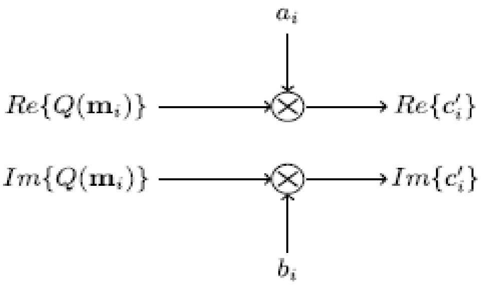

Figure-4: Phase-Encryption block.

In the figure, $Q(\mathbf{x})$ is a function that maps the message **x** to the modulated symbol. $Q(\mathbf{x})$ is generally complex valued and it is dependent on the type of the employed modulation. If $Q(\mathbf{m})$ is in general complex valued, we use two bits of key stream, one for the in-phase portion of the modulated symbol and one for the quadrature portion of the modulated symbol. If $Q(\mathbf{m})$ is real valued, then only one branch is needed. In this case, the key streams required are reduced by half. For decryption first the imaginary and real components of the received ciphertext is multiplied by the keystreams a and b followed by the necessary demodulation and decoding techniques to recover the original transmitted message.

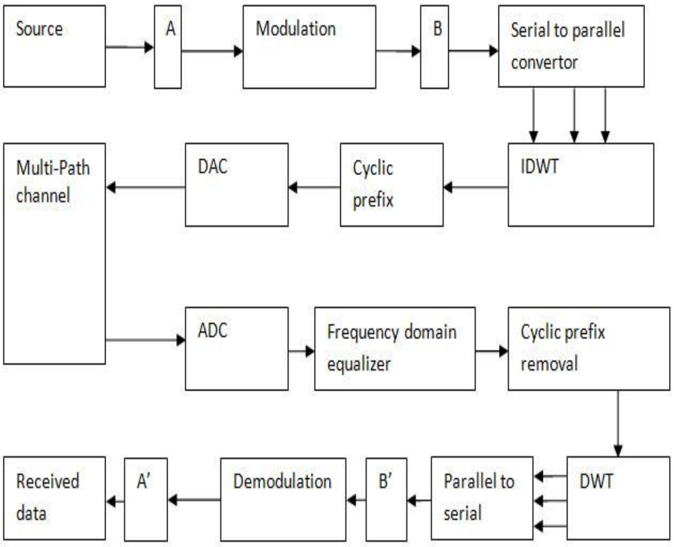

Figure-5: System Level XOR and Phase Encryption

In figure-5 blocks A and A' represent the positions of XOR Encryption and Decryption respectively in a communication system. Blocks B and B' represent Phase Encryption and decryption respectively.

XOR-Enc and P-Enc in a communication system are illustrated in Figs below,

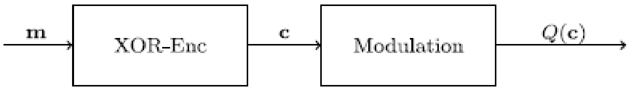

Figure-6: XOR encryption in a communication system

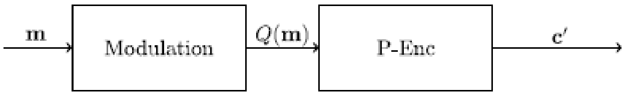

Figure-7: Phase-encryption in a communication system

In these two figures, **m** is the message, again $Q(\mathbf{x})$ is a function that maps the message **x** to the modulated symbol. **c** and **c**' are the resulting modulated cipher text symbols for XOR-Enc and P-Enc, respectively. we see the order of encryption and modulation is reversed between XOR-Enc and P-Enc. XOR-Enc takes place prior to the modulation. Consequently, XOR-Enc is independent of the modulation methods. On the other hand, P-Enc takes place after the modulation; the required key stream size depends on the underlying modulation scheme as well as the constellation size.

V. MATHEMATICAL FORMULATIONS OF XOR-ENC AND P-ENC WITH DIFFERENT TYPES OF MODULATION

1) *PSK Modulation:* Let fc be the carrier frequency, θ be the message symbol represented in phase, then the M-ary PSKmodulated passband signal s(t) has the form

$$s(t) = \cos(\, 2\pi f_c t + \theta \frac{2\pi}{M}), 0 \le t \le T$$

where $\theta = 0, 1, \dots, (M - 1)$.

Now, let QPSK (x_i) be a function that maps i th symbol x_i to one of the M phases, again k_i and k_i' denote key streams used for encrypting ith symbol in XOR-Enc and P-Enc, respectively, and $g(\, \mathrm{m_{i,}}\; k_i' \,)$ be the phase shift of ith symbol using P-Enc with key stream k_i' then we can model the ith modulated ciphertext symbol c_i and c_i' with XOR-Enc and P-Enc, respectively, by

$$c_i(t) = \cos\left(2\pi f_c t + Q_{psk}(m_i + k_i)\frac{2\pi}{M}\right) \text{-(1)}$$

$$c_i^{'}(t) = \cos\left(2\pi f_c t + Q_{psk}(m_i)\frac{2\pi}{M} + g\left(m_{i\,,}k_i^{'}\right)\right) \text{-(2)}$$

Comparing (1) and (2), we observe in XOR-Enc, similar to ASK modulation, ciphertext $m_i + k_i$ takes on the same space as message m_i. Therefore, the phase offset between the modulated message and ciphertext symbols is $2\pi lM$, where $l = 1, \dots, M - 1$. Recall that P-Enc is performed by multiplying each of real and quadrature components of the modulated symbol by a $\{-1,1\}$ valued key stream, then the modulated ciphertext symbol using P-Enc only takes on four phase values which lies in four different quadrants and it is determined by the four key streams. Without loss of generality, we denote the phase that lies in the first quadrant as $p0$, then the other three phase values are $\pi - p0$, $\pi + p0$ and $2\pi - p0$.

Remark: If the M-ary PSK signal constellation is not symmetrical along the x-axis and y-axis, as it is the case when M is odd, then there exists an attack. When M is odd, the signal constellation is symmetrical only along the x-axis. Therefore, only two out of all four phases of the modulated ciphertext symbol lie in the valid signal constellation, the adversary can identify and remove those that are not belong to the signal constellation. Therefore, the searching space is reduced by half. This attack only exists when M is odd. In practice, $n = log_2 M$, or $M = 2^n$. In this case, M is always even and all four phases of the modulated ciphertext lie in the valid signal constellation. Therefore, this attack is not applicable in practice. In general, n is an integer greater than or equal to 2. Thus, in terms of required key stream size, if message **m** contains k symbols, then the total required key stream size is nk for XOR-Enc. This number becomes $2k$ for

P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{n}{2}$, respectively. The required key streams for P-Enc would always be smaller than or equal to that of XOR-Enc. In general, the key stream size is reduced by a factor of $\frac{2}{n}$ using P-Enc compared to XOR-Enc in a PSK-modulated communication system.

Remark: If Binary PSK (BPSK) modulation is used, then $n = 1$ and the modulated symbol only contains only the inphase signal (real valued). This is identical to binary ASK. Thus, we only perform encryption on the real part of the modulated symbol. Consequently, the number of key streams required for XOR-Enc and P-Enc are still identical. In conclusion, P-Enc would always require smaller or equal amount of key streams for PSK-modulated systems. If the adversary performs random guessing on the received ciphertext symbols, excluding the BPSK case, then his successful probability for recovering message **m** with XOR-Enc $P_{suc,PSK-XOR}$ and P-Enc $P_{suc,PSK-P}$ are, respectively

$$P_{suc,PSK-XOR} = \frac{1}{2^{nk}}$$

$$P_{suc,PSK-P} = \frac{1}{2^{2k}}$$

If BPSK modulation is used, $P_{suc,BPSK-XOR}$ has the same form as ASK modulation, namely

$$P_{suc,BPSK-P} = \frac{1}{2^{k}}$$

2) *QAM Modulation:* Let fc be the carrier frequency, A_l be the symbol amplitude and θ_l be the phase, then the M-ary QAM
modulated passband signal s(t) has the form

$$s(t) = A_l \cos(2\pi f_c t + \theta_l), 0 \le t \le T$$

where $l = 1, 2, \ldots, M$.

Unlike ASK and PSK modulations where the modulation is performed either on the amplitude or the phase, QAM modulates message using both the amplitude and phase. Note that the values of amplitude *Al* and phase θ_l depend on the type of the employed QAM.

Now, let $QQAM(x_i)$ be a function that maps ith symbol x_i to one of the M symbols using QAM modulation which contains a amplitude of $|QQAM(x_i)|$ and a phase of $\angle QQAM(x_i)$, let k_i and k_i' represent key streams used for encrypting ith symbol in XOR-Enc and P-Enc, respectively, and $g(m_i, k_i')$ be the phase shift of ith symbol using P-Enc with key stream k_i' , then we can model the ith modulated ciphertext symbol c_i and c_i' with XOR-Enc and P-Enc, respectively, by

$$c_i(t) = |Q_{QAM}(m_i + k_i)| \cos\left(2\pi f_c t + \angle Q_{QAM}(m_i + k_i)\right) \text{ -(3)}$$

$$c_i'(t) = |Q_{QAM}(m_i)| \cos\left(2\pi f_c t + \angle Q_{QAM}(m_i) + g(m_i, k_i')\right) \text{ -(4)}$$

Comparing (3) and (4), we see for XOR-Enc, the modulated ciphertext symbol space is identical to the modulated message symbol space. Therefore, the modulated ciphertext symbol could be lie on any one of the valid signal constellations. However, encryption using P-Enc is achieved by only changing the phase of the modulated message symbol, the amplitude remains unchanged. For P-Enc in QAM modulation, modulated ciphertext symbol also takes on four phase values and these four phase values are identical to PSK modulation. Using the same notation as PSK modulation, these four phase values are $p0$, $\pi - p0$, $\pi + p0$ and $2\pi - p0$.

Remark: Note that for M-ary QAM, signal constellation is always symmetrical along the x-axis and y-axis. The modulated ciphertext symbols of all four phases are also a valid modulated message symbol. Therefore, the attack described previously for PSK modulation is not applicable here. In terms of required key stream size, if the message **m** contains k symbols, then for XOR-Enc, the total key stream size is nk. This number becomes $2k$ for P-Enc. Equivalently, the encryption efficiency for XOR-Enc and P-Enc are 1 and $\frac{n}{2}$, respectively. In general, the key stream size is reduced by a factor of $\frac{2}{n}$ using P-Enc compared to XOR-Enc in a QAM-modulated communication system. . If the adversary performs random guessing on the received ciphertext symbols, then his successful probability for recovering message **m** with XOR-Enc $P_{suc,QAM-XOR}$ and P-Enc $P_{suc,QAM-P}$ are identical to the PSK case, namely

$$P_{suc,QAM-XOR} = \frac{1}{2^{nk}}$$

$$P_{suc,QAM-P} = \frac{1}{2^{2k}}$$

VI. PROPOSED DWT BASED OFDM SYSTEM WITH PHASE ENCRYPTION

As shown in the figure in our proposed model we replace the blocks of DFT and IDFT in a conventional OFDM system with DWT and IDWT blocks. Also the conventional encryption technique or XOR encryption is replaced by Phase encryption. Thus, the original data will be modulated and then phase encryption is applied on it. Then the data after being converted to parallel form is subjected to inverse discrete wavelet transform followed by cyclic prefixing before being sent over the channel. At the receiver end, the parallel data after passing through a frequency domain equalizer and after removal of the guard band is subjected to discrete wavelet transform. This data will then be converted to serial form and demodulated to obtain the original data.

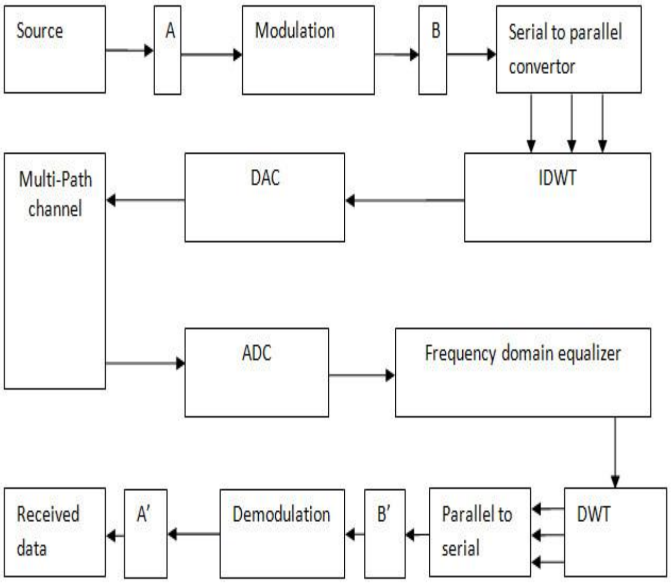

Figure-8: DWT based OFDM system with Phase-encryption.

VII. BER PERFORMANCE EVALUATION

In matlab for the different modulation techniques, we obtain the performance characteristics of both DFT based OFDM system and DWT based OFDM system. For the purpose of simulation, signal to noise ratio (SNR) of different values are introduced through AWGN channel. The modulation techniques chosen are PSK and QAM. From the SNR plots, we can see that the BER performance of the DWT based OFDM system with phase encryption is much better than the performance of the DFT based OFDM system with XOR encryption for constellation sizes of M = 2, 4 and 16.

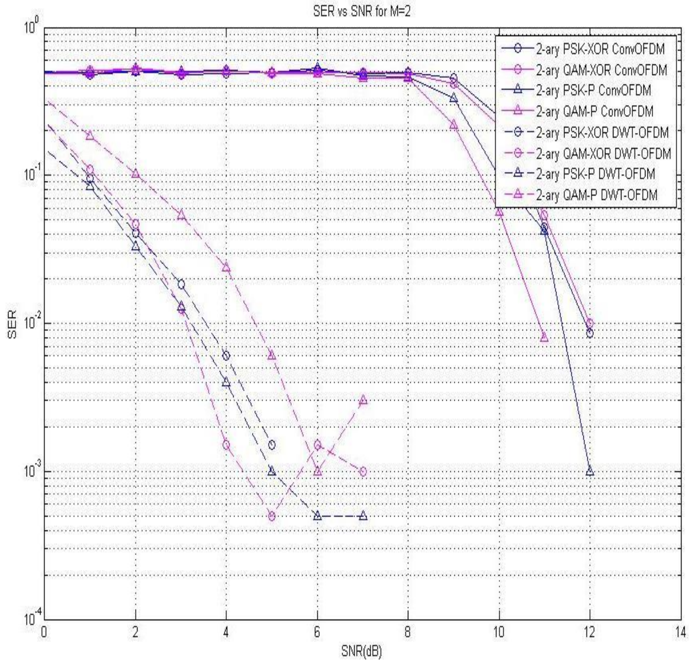

Figure-9: SER versus SNR for M = 2

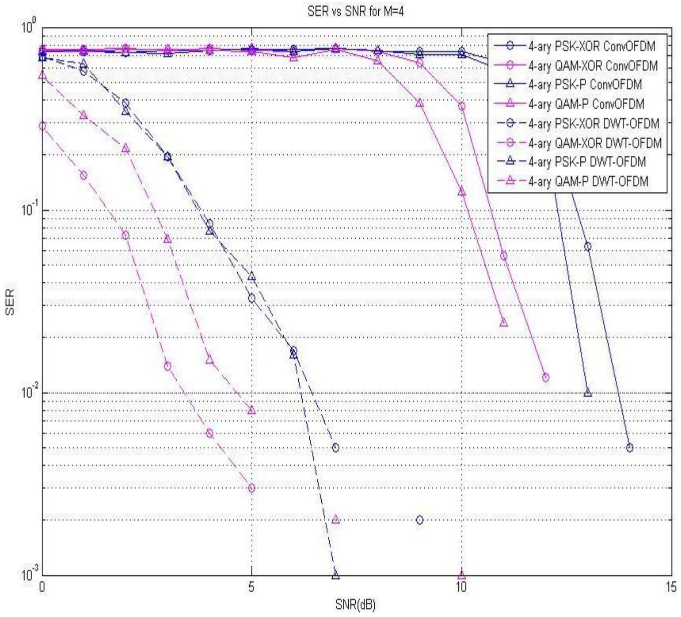

Figure-10: SER versus SNR for M = 4

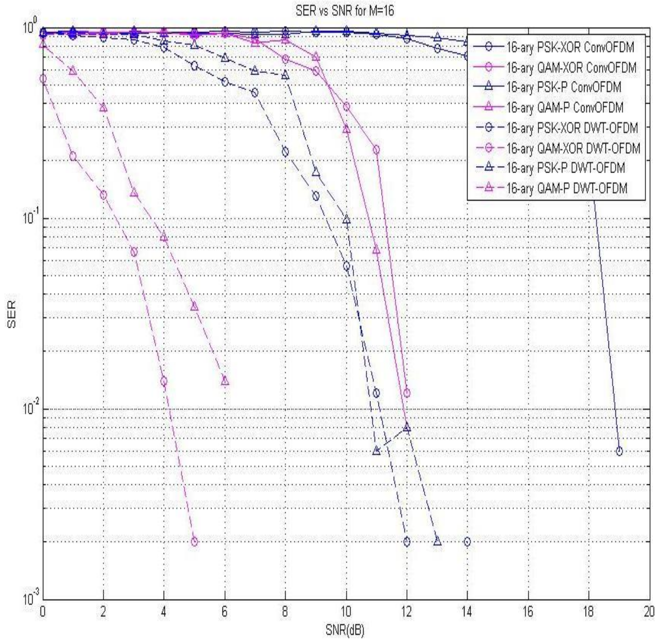

Figure-11: SER versus SNR for M = 16

VIII. CONCLUSION

In this paper we first compared the XOR and Phase Encryption techniques. Using mathematical formulations we compared the security and encryption efficiency of these two encryption methods. Through this we showed that phase encryption requires a much smaller keystream size than that needed by XOR encryption. We then compared the performances of the wavelet based OFDM system with phase encryption with the performances of DFT based OFDM system with XOR encryption for both PSK and QAM modulation techniques for different constellation sizes. Observing the performance curves we can say that the BER performance of the wavelet based OFDM system is clearly better than the DFT based OFDM system.

IX. REFERENCE

[1] K. Volkan, K. Oguz, "Alamouti coded wavelet based OFDM for multipath fading channels", IEEE Wireless telecommunications symposium, pp.1-5, April 2009.

[2] Fei Huo, Guang Gong, "XOR Encryption Versus Phase Encryption, an In-Depth Analysis" in IEEE transactions on electromagnetic compatibility, vol 57, no 4, pp. 903-911, 30 January 2015.

[3] Anuradha, Naresh Kumar, "BER analysis of conventional and wavelet based OFDM in LTE using different modulation techniques" in engineering and computational sciences., pp. 1-4, March - 2014

[4] *Evolved Universal Terrestrial Radio Access (E-UTRA): Security Architecture*, 3GPP TS 33.401 v11.7.0, 2013.

[5] *Evolved Universal Terrestrial Radio Access (E-UTRA): PhysicalChannels and Modulation*, 3GPP TS 36.211 v11.4.0, 2013.

[6] L. D. Callimahos, "Introduction to traffic analysis," Declassified by NSA, 2008.

[7] L. Chen and G. Gong, *Communication System Security*. Boca Raton, FL, USA: CRC Press, 2012

[8] A. P. Duffy, A. J. M. Martin, A. Orlandi, G. Antonini, T. M. Benson, and M. S.Woolfson, "Feature selective validation (FSV) for validation of computational electromagnetics (CEM). Part I—The FSV method," *IEEE Trans. Electromagn. Compat.*, vol. 48, no. 3, pp. 449–459, Aug. 2006.

[9] M. Fresia, F. Perez-Cruz, H. V. Poor, and S. Verdu, "Joint source and channel coding," *IEEE Signal Process. Mag.*, vol. 27, no. 6, pp. 1053–5888, Nov. 2010.

[10] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 1024–1032.

[11] F. Huo and G. Gong, "Physical layer phase encryption for combating the traffic analysis attack," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2014, pp. 604–608.

[12] A. Ian F., G. David M., R. Elias Chavarria, "The evolution to 4G cellular systems: LTE-advanced", Physical communication, Elsevier, vol. 3, no. 4, pp. 217-244, Dec. 2010

[13] B. John A. C., "Multicarrier modulation for data transmission: an idea whose time has come", IEEE Communications magazine, vol. 28, no.5, pp. 5-14, May 1990.

[14] L. Jun, T. Tjeng Thiang, F. Adachi, H. Cheng Li, "BER performance of OFDM-MDPSK system in frequency selective rician fading and diversity reception" IEEE Transactions on Vehicular Technology, vol. 49, no. 4, pp. 1216-1225, July 2000.

[15] K. Abbas Hasan, M. Waleed A., N. Saad, "The performance of multiwavelets based OFDM system under different channel conditions", Digital signal processing, Elsevier, vol. 20, no. 2, pp. 472-482, March 2010.

[16] K. Volkan, K. Oguz, "Alamouti coded wavelet based OFDM for multipath fading channels", IEEE Wireless telecommunications symposium, pp.1-5, April 2009.

[17] G. Mahesh Kumar, S. Tiwari, "Performance evaluation of conventional and wavelet based OFDM system", International journal of electronics and communications, Elsevier, vol. 67, no. 4, pp. 348-354, April 2013.

[18] J. Antony, M. Petri, "Wavelet packet modulation for wireless communication", Wireless communication & mobile computing journal, vol. 5, no. 2, pp. 1-18, March 2005.

[19] L. Madan Kumar, N. Homayoun, "A review of wavelets for digital wireless communication", Wireless personal communications, Kluwer academic publishers- Plenum publishers, vol. 37, no. 3-4, pp. 387-420,May 2006.

[20] L. Alan, "Wavelet packet modulation for orthogonally multiplexed communication", IEEE transaction on signal processing, vol. 45, no. 5, pp. 1336-1339, May 1997.

[21] K. Werner, P. Gotz, U. Jorn, Z Georg, "A comparison of various MCM schemes", 5th International OFDM-workshop, Hamburg, Germany, pp. 20-1 – 20-5, July 2000.

[22] IEEE std., IEEE proposal for 802.16.3, RM wavelet based (WOFDM), PHY proposal for 802.16.3, Rainmaker technologies, 2001.

[23] O. Eiji, I Yasunori, I Tetsushi, "Multimode transmission using wavelet packet modulation and OFDM", IEEE vehicular technology conference, vol. 3, pp. 1458-1462, Oct. 2003.

[24] L. Louis, P. Michael, "The principle of OFDM" RF signal processing, http://www.rfdesign.com, pp. 30-48, Jan 2001.

[25] "LTE in a nutshell: The physical layer", white paper, 2010, http://www.tsiwireless.com.

[26] R. Mika, T. Olav, "LTE, the radio technology path toward 4G", Computer communications, Elsevier, vol. 33, no. 16, pp. 1894-1906, Oct. 2010.

[27] Broughton SA, Bryan K. Discrete Fourier analysis and wavelets. New Jersey, John Wiley, 2009.

[28] C. See Jung, L. Moon Ho, P. Ju Yong, "A high speed VLSI architecture of discrete wavelet transform for MPEG-4", IEEE transaction consumer electron, vol. 43, no. 3, pp. 623-627, June 1997.