American-Eurasian Journal of Scientific Research 11 (1): 56-62, 2016
ISSN 1818-6785

DOI: 10.5829/idosi.aejsr.2016.11.1.22722

Secure Speech Communication Using Improved OFDM Scrambler for next Generation Mobile Communication Systems

G. Dhanya and J. Jayakumari

Noorul Islam University, Kanyakumari, India

Abstract: OFDM scrambling is one of the most popular techniques for secure communication. This paper proposes a new scrambling technique based on random permutation with the pseudo random binary generator to improve the performance of OFDM scrambler. To measure the intelligibility of speech, speech transmission index (STI) and common intelligibility scale (CIS) are used. The Bit Error Rate (BER) and Signal to interference plus noise ratio (SINR) are used to evaluate the performance of the speech. By the measurement of PESQ, the quality of the recovered speech was observed. The simulation result shows that the proposed OFDM scrambler is an efficient technique for achieving high data security in 4G broadband wireless communication.

Key words: Speech scrambling · 4G · OFDM · Speech transmission index · Common intelligibility scale

INTRODUCTION

Speech security is an important feature in the modern mobile communication system, the needs to secure communication increases every day [1], involving military and civil applications. Now a day's secure communication ensures maximum security at minimum cost and minimum complexity. The modern day encryption systems do not provide full flexibility in choosing the level of security [2]. These systems may require a considerable amount of power consumption due to their complexity. With the rapid development of electronic commerce applications, the technology-oriented consumer's should be accessing information on an anywhere anytime basis [3].

The 4th generation of mobile communication supports high data rate and high spectral efficiency due to the ever increasing demand of users [4]. In the commercial operation of 4G systems, to fulfill the sharp surge of data and video capabilities complex modulation schemes has been introduced [5]. The 4G systems can be exceedingly useful to manage traffic in emerging situations as well as normal situations [6]. By the optimization of spectral efficiency, the 4G wireless revolution is demanding a high- quality speech at higher channel capacity and lower cost per bit [7]. With the growing demand of mobile applications need to develop an OFDM based 4G networks to support data applications and to eradicate intra-cell interference due to orthogonality between subcarriers [8]. For mobile communication applications, OFDM is the widely used modulation scheme due to its excellent robustness and high spectral efficiency to fading channels [9]. FFT (Fast Fourier Transform) and IFFT (Inverse Fast Fourier Transform) are used for modulation and demodulation [10]. In OFDM, a cyclic prefix is added to eliminate the inter-symbol interference and inter-channel interference [11] Due to the adequate inter-symbol interference reduction, the OFDM has become a promising technique for high-speed data transmission over time dispersive or frequency selective channels [12].

The most significant model of communication is the speech or man's spoken word. A variety of encryption methods have been used to protect the speech communication [13]. The scrambling and descrambling plays a symbolic role in communication system. One of the popular encryption methods, analog scrambling plays a significant role in secure communication [14]. The scrambling is performed by permuting the speech elements either in a time domain or in a frequency domain or the combination of a time and frequency domain. Moreover, other scrambling techniques in the transform domain are wavelet transform, FFT (Fast Fourier Transform) and DCT (Discrete Cosine Transform).

Corresponding Author: G. Dhanya, Noorul Islam University, Kanyakumari, India.

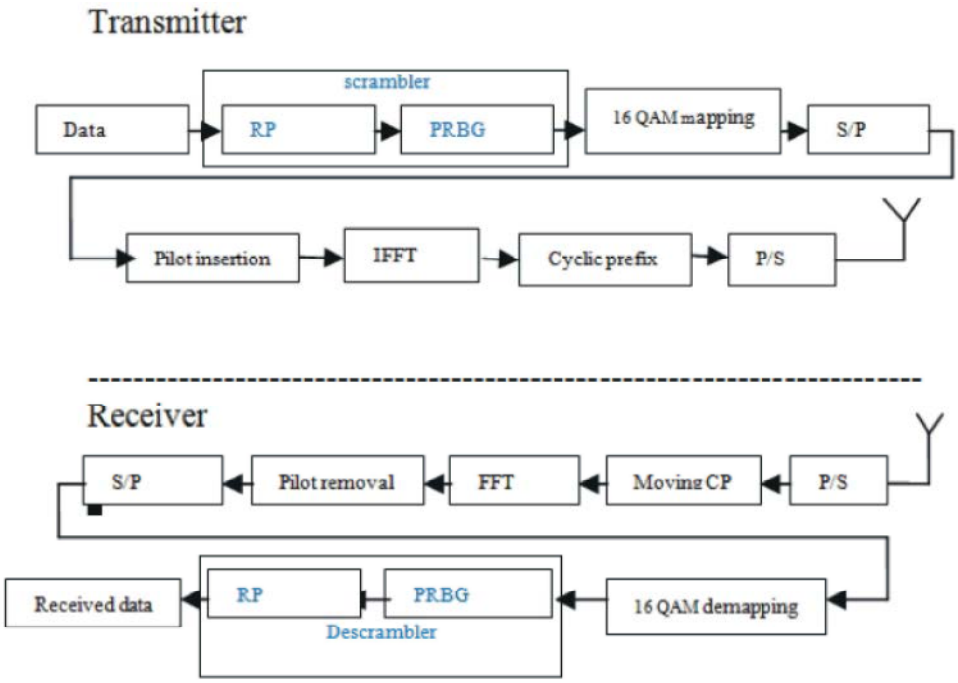

Fig. 1: Proposed OFDM based speech scrambler block diagram

Hao Li, Xianbin Wang and Weikun Hou in the "Secure Transmission in OFDM Systems by Using Time Domain Scrambling" have used random permutation based scrambling [15]. In this, speech signals are rearranged in time domain basis. Another system uses a scrambling key generator, which is controlled by a secret key and a seed. "An OFDM Speech Scrambler without Residual Intelligibility", D. C. Tseng and J. H. Chiu is explained it. [16]

Proposed OFDM Scrambler: The proposed OFDM-based speech scrambler block diagram is shown in Figure 1. The proposed scrambling system is the combination of two techniques, random permutation and Pseudo-random binary generator. The first scrambling is based on random permutation scrambling, which is performed by using a seed. It shuffles the speech signals in random order. The output of this scrambler produces a random data sequence and this output is XORed with the seed. Then this output is given to the next scrambler [17].

The second scrambler is Pseudo Random Binary Generator (PRBG). Here a key is used for scrambling. The output from the random permutation scrambling is XORed with the PRBS output. This is again XORed with a key, which is used for PRBS scrambling [17]. Here two types of permutations are performed. Therefore, the output of this scrambler is a scattered output and it does not have any similarity with the original signal, that is, it highly unintelligible to others. This data is transmitted through the channel. It is a highly secured algorithm against cryptanalytic attacks and it reduces residual intelligibility [17].

At the receiver side, the same key and seed is used for descrambling the data.

Let X be the input data be an array of 'n' elements, R be the Permuted data elements of an array, k denotes the position of an array element. R_k be the value of the k^{th} position element of permuted data array.

The mathematical analysis of the RP scrambler is:

$$R_k = \begin{cases} X_{k+1} \text{ if } 1 \le k \le n\text{-}1 \\ X_1 \text{ if } k=n \end{cases} \quad (1)$$

The output of the random permutation scrambler is XOR ed with the seed value 'S'. Then the equation becomes.

$$Y_k = R_k \text{ XOR } S \quad (2)$$

The output of the Random permutation scrambler is given to the next scrambler PRBG. In this scrambler XOR operation is done with a random key (K) and all the elements of the random permutated array. The output becomes.

$$Z_k = Y_k \text{ XOR } K \quad (3)$$

Z_k is the output of the scrambler, it is given as the input of the QAM mapping. The QAM mapped output is then converted to parallel form. After inserting pilots, data is given to the IFFT operation. The cyclic prefix is added to the output of IFFT and the data is converted back to serial form for transmission. Rayleigh and Rician channels are used for transmitting the data.

At the receiver side, inverse operations are performed.

$$Y_k = Z_k \text{ XNOR } K \quad (4)$$

$$R_k = Y_k \text{ XNOR } S \quad (5)$$

$$X_k = \begin{cases} R_{k+1} \text{ if } 2 \le k \le n\text{-}1 \\ R_n \text{ if } k=1 \end{cases} \quad (6)$$

Here we are using two types of keys. So it is more crypt analytically secured scrambling based on OFDM system.

Scrambling and Descrambling: To select the permutation for each sample, a permutation key is placed at the transmitting side. The inverse permutation key is put at the receiving side, to perform an inverse permutation for those components are permuted in the received sample. If "K" samples are permuted, the total numbers of possible permutations are K!. However, all these permutations cannot be used. Out of this K! permutations, a subset of permutations has to be selected for the use in the scrambling system [18]. For analyzing the system performance, the following parameters are used [17].

Performance Analysis: The intelligibility of speech and the quality of speech were evaluated by using Common Intelligibility Scale (CIS), Speech Transmission Index (STI) and Perceptual Evaluation of Speech Quality (PESQ). The performance of the noise is measured by using Bit Error Rate (BER) and Signal to Interference plus Noise Ratio (SINR).

Noise Performance: The SINR and BER performance of OFDM based PRBS scrambler compared with the OFDM based random permutation scrambler and the conventional OFDM scrambler under fading channels (Rayleigh and Rician). The Signal to Interference plus Noise Ratio is defined as the ratio between Signal power (Ps) and Interference power (PICI) plus noise power (N0) [17].

Table 1: Parameters of proposed OFDM based speech scrambler [17]

Parameter	Value
FFT size(IFFT)	64
Bandwidth of transmission channel	300-3400Hz
Bandwidth of the input speech channel	0-4000Hz
Number of subcarriers	52
Sampling frequency	8kHz
Subcarrier spacing	312.5 kHz
Data symbol duration Td	3.2microsec
Cyclic prefix duration Tcp	0.8 micro sec
Total symbol duration Ts(Td + Tcp)	4 micro sec
Mapping and demapping schemes	16 QAM

$$SINR = P_S / P_{ICI} + N_0 \quad (7)$$

The speech.wav was given as the input signal. For Rayleigh and Rician channel models, flat fading paths are employed and the K factor of 1 is used for rician channel. BER is calculated using the parameter Eb/N0. The random permutation with PRBS scrambling shows better performance and it has low bit error rate when compared with the others [17].

Perceptual Evaluation of Speech Quality (PESQ): PESQ is used to compare an original speech signal with received speech signal. The received speech signal is known as "degraded signal" and the original speech signal is known "reference signal" [19]. The Perceptual evaluation of speech quality (PESQ), it calculates the quality of a speech signal by a 5-point scale. The 5 corresponds to excellent speech quality, 4 for good, 3 for fair, 2 for poor and 1corresponds to bad or unsatisfactory speech quality [19].

The comparison table shows that the RP with PRBS scrambling gives better performance than two other methods.

Speech Intelligibility Measurement: Two parameters are used for measuring speech intelligibility.

Speech Transmission Index (STI)

Common Intelligibility Scale (CIS): The range of the speech transmission index lies between 0 and 1. The 0 indicates bad and the 1 indicates excellent. The weighted sum of Modulation transfer function (MTF) is used to measure speech transmission index (STI). Modulation transfer index (MTI) is derived from a modulation transfer function (MTF). Here STI is calculated for a band of frequencies. SNR ranges are limited from +15db to -15db [20]. Speech transmission index computes all the factors in the speech transmission path, affects intelligibility.

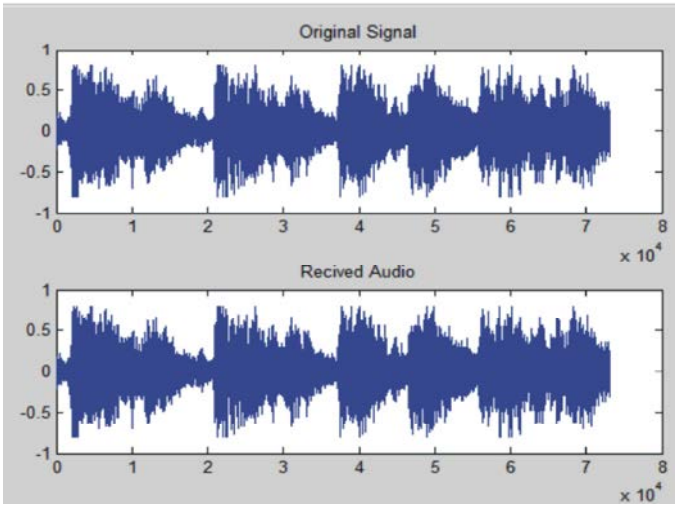

Fig. 2: Original and reconstructed speech waveform [17]

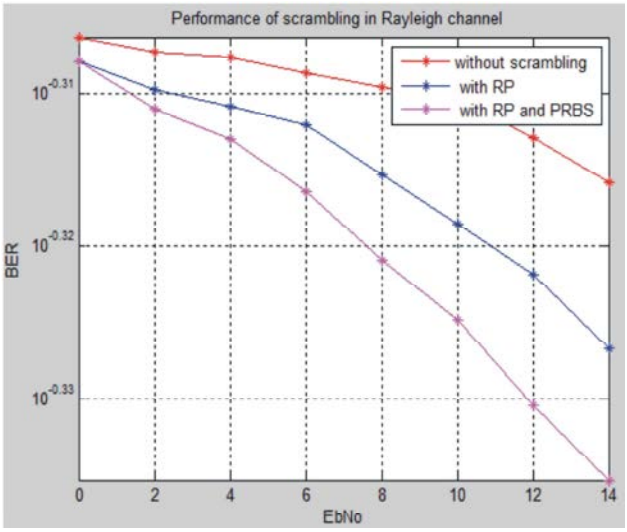

Fig. 3(a)

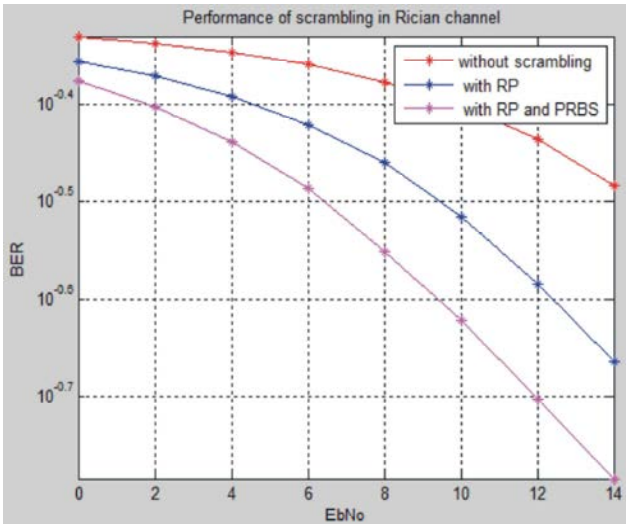

Fig. 3(b)

Fig. 3: BER performance of OFDM based speech scrambler (a)Rayleigh and (b)Rician channel [17]

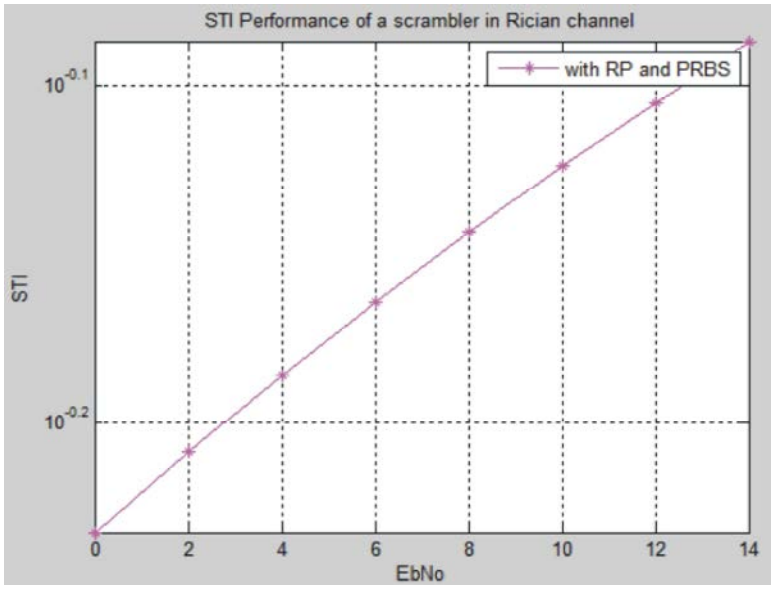

Fig. 4(a)

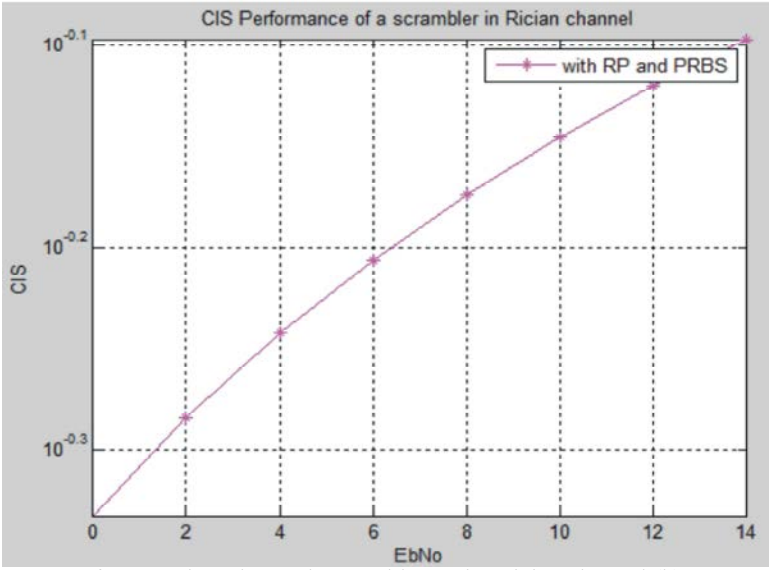

Fig. 4(b)

Fig. 4: (a) STI performance of OFDM based speech scrambler under Rician channel (b) CIS performance of OFDM based speech scrambler under Rician channel

Table 2: Comparison of different types of OFDM speech scramblers based on BER under Rayleigh and Rician channels [17]

Type of OFDM	Eb/N0	Rayleigh	Rician
Without scrambling	10	0.4818	0.4105
OFDM with RP	10	0.4727	0.3250
OFDM with RP & PRBS	10	0.4663	0.2714

Table 3: Comparison on different types of OFDM speech scramblers based on PESQ [17]

Type of OFDM	PESQ (Rayleigh)	PESQ (Ricin)
Without scrambling	1.69	2.016
OFDM with RP	2.17	2.019
OFDM with RP & PRBS	2.28	2.089

Table 4: Relation between STI and speech intelligibility [19]

STI	.00-.30	.30-.45	.45-.60	.60-.75	.75-1.00
Speech intelligibility	Bad	Poor	fair	Good	Excellent

Table 5: Evaluating random permutation with PRBS scrambling using different parameters

Type of OFDM	Eb/N0	BER	SINR	STI	CIS
OFDM with RP&PRBS (rician)	12	0.3129	0.1515	.7853	.7583
OFDM with RP&PRBS (Rayleigh)	12	0.4064	0.1351	0.7853	0.7999

The simulation results show that, the quality of the speech and the intelligibility of the speech are excellent, also the noise performance is low in this scrambler. So, the proposed scrambler RP with PRBS is the best scrambling technique in future communication.

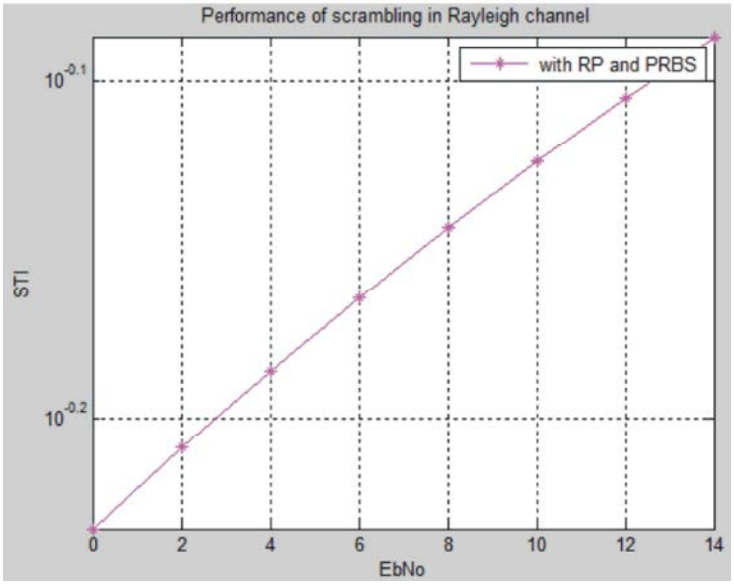

Fig. 5(a)

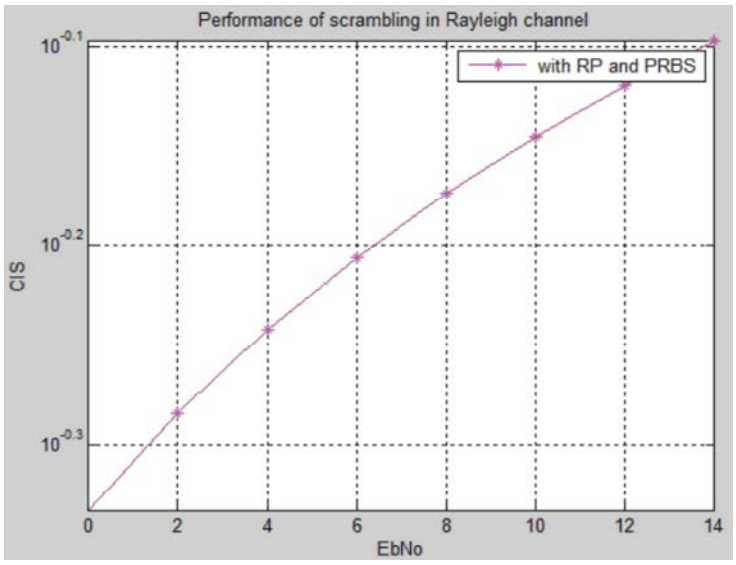

Fig. 5(b)

Fig. 5: (a) STI performance of OFDM based speech scrambler under Rayleigh channel (b) CIS performance of OFDM based speech scrambler under Rayleigh channel.

CONCLUSION

This paper proposes a new improved OFDM scrambler, which incorporates scrambling with random permutation and PRBS scrambling, it makes low residual intelligibility and high speech quality. The two parameters Speech Transmission Index and Common Intelligibility scale are used to evaluate the intelligibility of speech. For evaluating the noise performance, BER and Signal to Interference plus noise ratio are considered. To measure the quality of speech, perceptual evaluation of speech quality is used. This proposed OFDM scrambler is suitable for frequency selective highly dispersive fading channels and it is the best technique for providing high security in the next generation mobile communication systems. The simulation results show that the proposed system, provides low residual intelligibility and high quality. It is crypt analytically secured algorithm and it can be used in the transmitter as well as receiver ends without any modifications. It is an encouraging technique for high data rate transmission in 4G communication and also it is an excellent technique for proving a high security in next generation mobile communication system.

REFERENCES

1. Jiankun Hu, Ziping Xi, A. Jennings, Y.J. Lee and D. Wahyudi, 2001. "DSP application in e-commerce security", IEEE International Conference on Acoustics, Speech and Signal Processing, 2001. Proceedings. (ICASSP '01)., DOI: 10.1109/ ICASSP. 2001.941087, Publication Year: 2001, 2: 1005-1008.
2. Laskar, R.H., F.A. Talukdar, B. Bora and K.S.P. Fernando, 2009. "Complexity reduced multi-tier perceptual based partial encryption for secure speech communication" TENCON 2009 - 2009 IEEE Region 10 Conference, 23-26 Jan. 2009, 10.1109/TENCON. 2009.5396217, pp: 1-6.
3. Almasalha, F., A. Khokhar and S. Baqai, 2010. "Selective encryption based data security for Ogg streams", IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), 2010, DOI: 10.1109/ICASSP.2010.5495374 Publication Year: 2010, pp: 1850-1853.
4. Dongwook Kim, Seunghak Lee, Hanjin Lee and Hyunsoo Yoon, 2005. "An Effective Hotspot Cell Management Scheme Using Adaptive Handover Time in *4*G Mobile Networks" TENCON 2005 2005 IEEE Region 10, Date of Conference:21-24 Nov. 2005, DOI:10.1109/ TENCON.2005.300850, pp: 1-6.
5. Zhancang Wang, 2015. "Demystifying Envelope Tracking" *IEEE microwave magazine*, DOI: 0.109/ MMM.2014. 2385351 Date of Publication, pp: 6.
6. Allsopp, S., 2014. Allsopp Helikites Ltd, Fordingbridge, "Emergency airborne 4G comms to aid disaster traffic management" Road Transport Information and Control Conference 2014 (RTIC 2014), IET, pp: 1-7.
7. Zayani, R., Sup"Com, Tunis, Tunisia, R. Bouallegue and D. Roviras, 2010. "Crossover Neural Network Predistorter for the compensation of Crosstalk and nonlinearity in MIMO OFDM systems" , IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), 2010, DOI:10.1109/PIMRC.2010.5671770, pp: 966-970.
8. Jaya, Kumari J. and Sakuntala S. Pillai, 2005. "Performance of multicarrier OFDM systems" Proc. 36th IETE Mid Term Symposium on Emerging and Futuristic Communication Systems (EFCoS-05), pp: 347-352, 30 Apr-01 May 2005.
9. Sahin, M.E., 2007. Univ. of South Florida, Tampa ; Arslan, H. ; Singh, D., "Reception and Measurement of MIMO-OFDM Signals with a Single Receiver", IEEE 66th Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007, DOI:10.1109/VETECF.2007.149, pp: 666670.
10. Jaya Kumari, J. and Sakuntala S. Pillai, 2005. "Orthogonal Frequency Division Multiplexing" Proc. 17th Kerala Science Congress, KFRI, Peechi, pp: 139-142, 29-31 Jan 2005
11. Wang, M.M., Qualcomm Res. Center, Qualcomm Inc., San Diego, CA, USA ; Lei Xiao ; Brown, T. ; Min Dong, "Optimal symbol timing for OFDM wireless communications" *IEEE Transactions on Wireless Communications,* DOI:10.1109/TWC.2009.090263, 8(10): 5328-5337.
12. La Pan, M.J., T.C. Clancy and R.W. McGwier, 2014. "An Assessment of OFDM Carrier Frequency Offset Synchronization Security for 4G Systems" Published in: Military Communications Conference (MILCOM), 2014 IEEE, Date of Conference:6-8 Oct. 2014, DOI:10.1109/ MILCOM.2014.86, pp: 473-478.
13. Dae Soon Cho, 2006. Mobile Telecommun. Res. Lab., Electron. & Telecommun. Res. Inst., Daejeon ; Hyeong-Jun Park, "Implementation of an improved clock frequency offset compensator for 4G OFDM System at ETRI", IEEE 63rd Vehicular Technology Conference, 2006. VTC 2006-Spring. (Volume:1), DOI:10.1109/VETECS.2006.682802, pp: 192-195.
14. Hana'a M.A. Salman, 2013. "A Transform Based 3D-Speech Scrambling Using Multi-Wavelet: Design and Evaluation", The International Arab Conference on Information Technology (ACIT'2013).
15. Hao Li, Xianbin Wang and Weikun Hou, 2013. "Secure Transmission in OFDM Systems by Using Time Domain scrambling" IEEE Transactions.
16. Tseng, D.C. and J.H. Chiu, 2007. "An OFDM Speech Scrambler without Residual Intelligibility" IEEE Proceedings 2007
17. Dhanya, G. and J. Jayakumari, 2014. "Optimal speech scrambling technique for OFDM based system", International Journal of Applied Engineering Research, ISSN 0973-4562, 9(24): 28871-28878.
18. Thomas Strohmer and Scott Beaver, "Optimal OFDM design for high frequency dispersive cahnnels", IEEE transactions on communications, 51(7) July2003, DOI:10.1109/TCOMM.2003.814200,PublicationYeare: 2003, pp: 1111-1122.
19. Tiago H. Falk1 and Wai-Yip Chan, 2009. "Performance Study of Objective Speech QualityMeasurement for ModernWireless-VoIP Communications", EURASIP Journal on Audio, Speech and Music Processing,Volume 2009, Article ID 104382, pp: 11.
20. Jianfen Ma, Yi Hu and Philipos C. Loizou, 2009. "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions", Acoustical Society of America, May 2009.