AN EFFICIENT VOICE SCRAMBLING TECHNIQUE FOR NEXT GENERATION COMMUNICATION SYSTEMS

Dhanya G [#1], Dr. J. Jayakumari [*2]
[#] ECE Department, Research Scholar, Noorul Islam University, Kumaracoil
[1] dhanyagnr@gmail.com
[*] HOD, ECE Department, Noorul Islam University, Kumaracoil
[2] hellojayakumari@rediffmailcom

***Abstract*— The OFDM scrambler is most widely used for secure communication. In order to eliminate the intelligibility of speech, speech scrambling is used. Many of the scrambling techniques shows poor performance, to improve the efficiency of the scrambler an efficient speech scrambling technique, random permutation with pseudorandom- generator under multipath fading is proposed. The Common Intelligibility Scale (CIS) and Speech Transmission Index (STI) are used to predict the intelligibility of speech. Also to evaluate the performance of speech the BER (Bit Error Rate) and the SINR (Signal to Interference plus Noise Ratio) was used. By the measurement of PESQ (Perceptual Evaluation of Speech Quality) the recovered speech quality was observed. The simulations show that OFDM scrambler is a best technique for providing extremely high data security for 4G mobile communication when compared to a conventional technique.**

Keyword- Speech scrambling, 4G, OFDM, Pseudo- random generator, random permutation, speech transmission index, common intelligibility scale

I. INTRODUCTION

The security is now embracing the era of the mobile communication system, the needs to protect communication increases every day [1]. Present day, the increasing demand of secure communication deals with providing maximum security in many real applications such as civil and military applications at the cost of minimum complexity. With the growing electronic commercial applications [2], the technology oriented consumers expect the communication to be pervasive, i.e. to be able to communicate anywhere anytime using any platform or device [3].

The increasingly explosive growth of data communication the 4G provides much higher data rates to cellular users [4]. The commercial operation of 4G systems, complex modulation schemes has been introduced to fulfill the sharp surge of data and video capabilities [5]. The 4G systems can be exceedingly useful to manage traffic in normal situations as well as emerging situations such as flood, fire etc.[6]. By the optimization of spectral efficiency, the 4G wireless revolution is demanding increased channel capacity and higher data rate [7]. The emerging growth of mobile communication needs to develop an OFDM based 4G networks to support data applications at higher spectral efficiency and throughput [8]. The OFDM multicarrier modulation is expected to be the next enabling technology for 4G wireless system [9-10]. Due to effective intersymbol interference mitigation the OFDM has become a promising technique for high-speed data transmission over time dispersive or frequency selective channels [11-12].

The one of the multicarrier system, OFDM, which divides high speed data streams into low speed ones in parallel form and it transmits at the same time by several sub-carriers. FFT (Fast Fourier Transform) and IFFT (Inverse Fast Fourier Transform) are used for modulation and demodulation. Here the clock frequency is a very important factor, the difference in sampling frequencies between the user equipment and an access system will lead to performance degradation due to the orthogonality loss between the sub-carriers [13].The most fundamental form of communication is the speech or man's spoken word. To protect the speech communication, a variety of encryption techniques have been used [14]. The scrambling and descrambling plays a significant role in communication system [15].

Analog scrambling is one of the most popular encryption methods in speech communication [16]. The scrambling is performed by permuting the speech elements in the time domain, frequency domain and the combination of time and frequency domain. Moreover, other scrambling techniques in transform domain are wavelet transform, FFT (Fast Fourier Transform) and DCT (Discrete Cosine Transform) etc.

A. Conventional OFDM scrambler

The conventional OFDM scrambler uses a random permutation based scrambling; it rearranges the speech element in time domain basis. However, the other type of system uses a scrambling key generator, which is controlled by a secret key and a seed [17].

II. PROPOSED OFDM SCRAMBLER

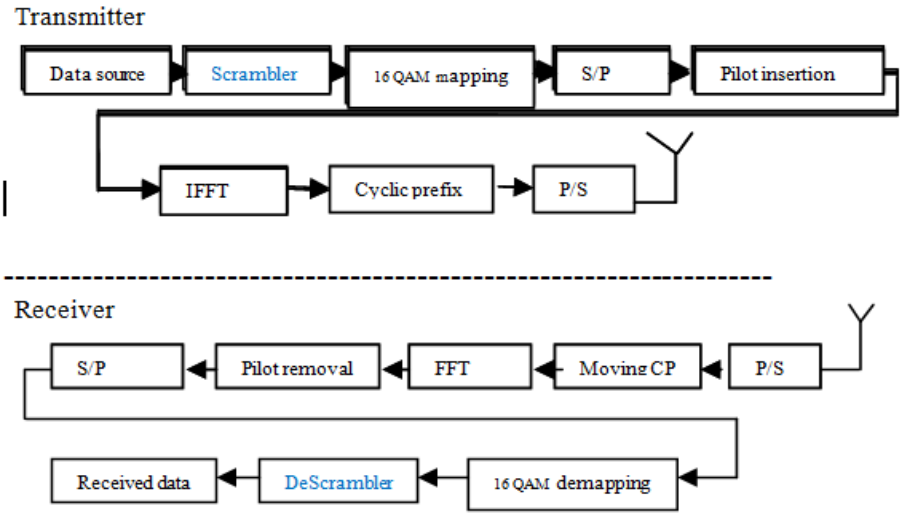

Fig. 1: Proposed OFDM based speech scrambler block diagram [17]

The proposed OFDM-based speech scrambler block diagram is shown in figure (1). The proposed OFDM scrambler is the combination of two techniques, random permutation and Pseudo-random number binary generator. The first scrambling is 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 given to the next scrambler [17].

The second scrambler is Pseudo Random Binary Generator (PRBS). Here a key is used for scrambling. This scrambler is a Linear Feedback Shift Register (LFSR), which produces a random data. The output from the LFSR first XORed with the random permutation scrambler output [17].The output of this scrambler is a scattered output and it has not any similarity with the original signal, that is, it highly unintelligible to others. Then this data is transmitted through the channel. It is a highly secured algorithm against cryptanalytic attacks and it produces zero residual intelligibility [17].

On the reception, the same key and seed is used for descrambling the data.

A. *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]

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

III. 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).

A. *Noise Performance*

The SINR and BER performance of OFDM based PRBS scrambler is 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 (P_{ICI}) plus noise power (N_0) [17].

$$SINR = P_S / P_{ICI} + N_0 \quad \textbf{(1)}$$

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 [17]. 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]

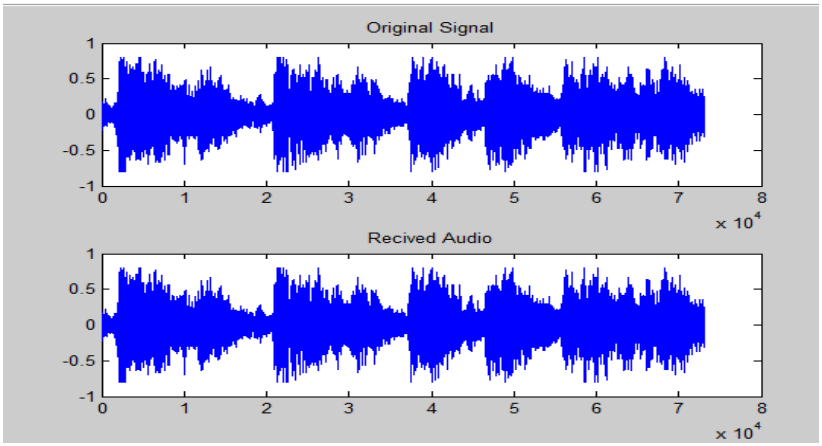

Fig.2. Original and reconstructed speech waveform [17]

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	8	0.4909	0.4209
OFDM with RP	8	0.4838	0.3462
OFDM with and RP & PRBS	8	0.4783	0.2818

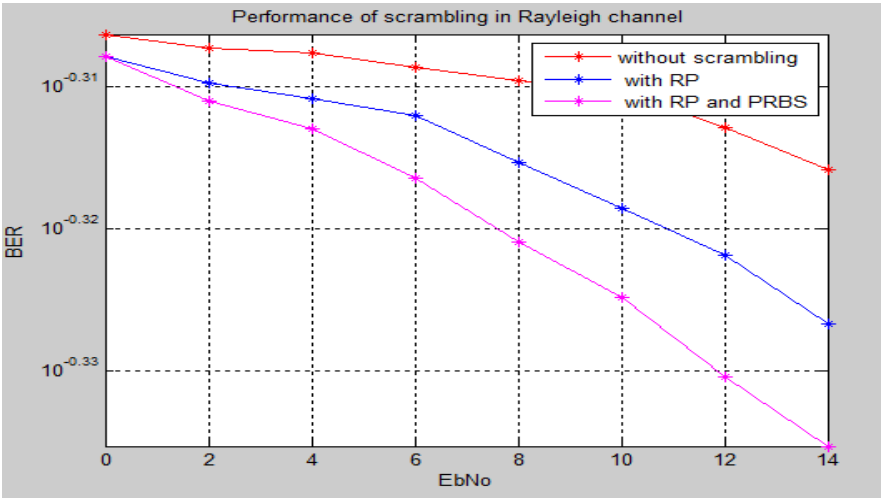

Fig. 3(a)

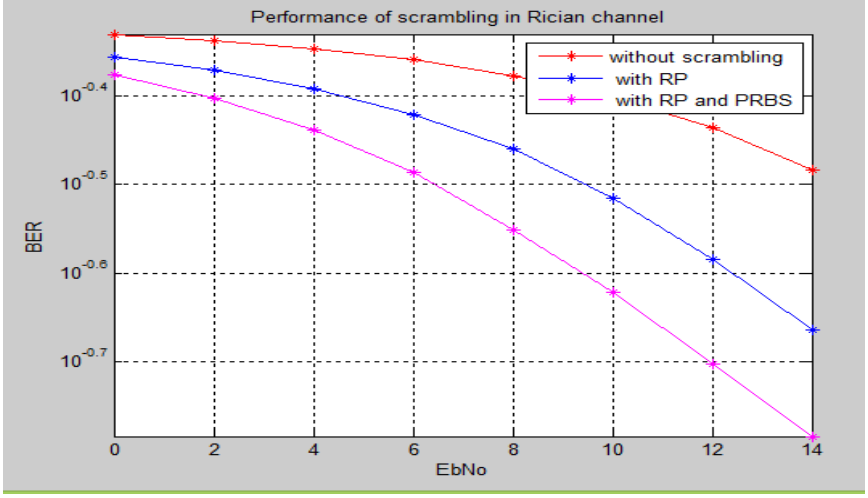

Fig. 3(b)

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

B. *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].

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

Type of OFDM	PESQ (Rayleigh)	PESQ (Rician)
Without scrambling	1.66	2.006
OFDM with RP	2.12	2.008
OFDM with RP & PRBS	2.23	2.059

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

C. *Speech Intelligibility Measurement*

Two methods are used for measuring speech intelligibility

1. *Speech Transmission Index(STI)*
2. *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.

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

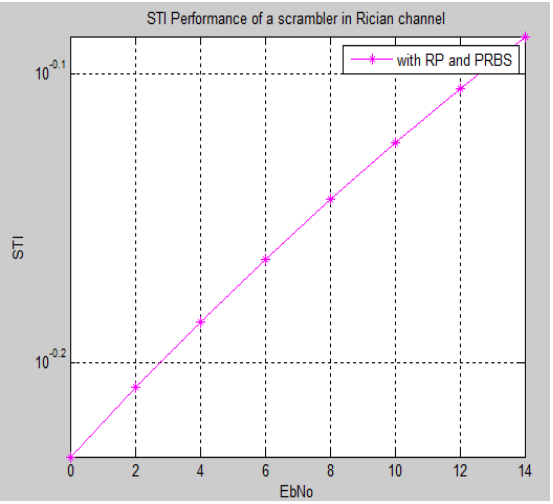

Fig. 4(a)

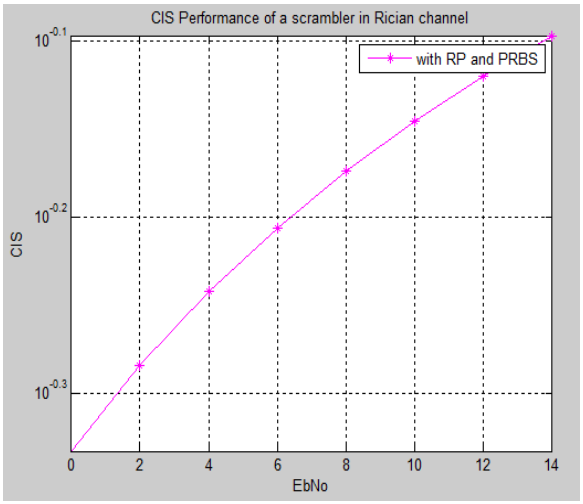

Fig. 4(b)

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 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

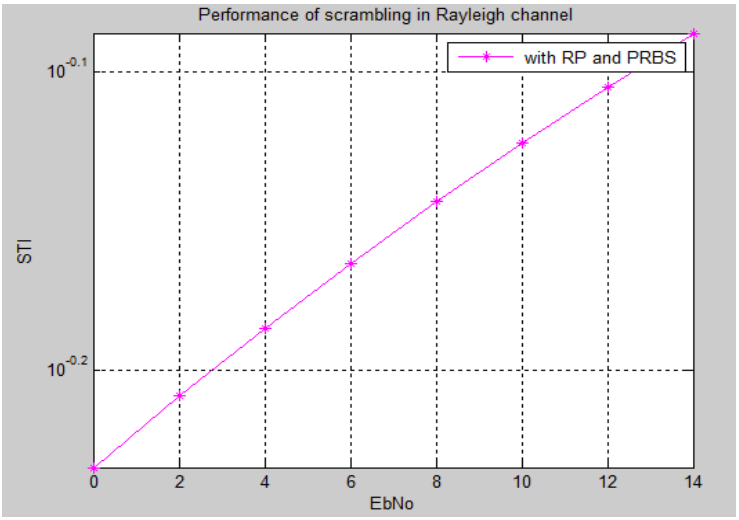

Fig. 5(a)

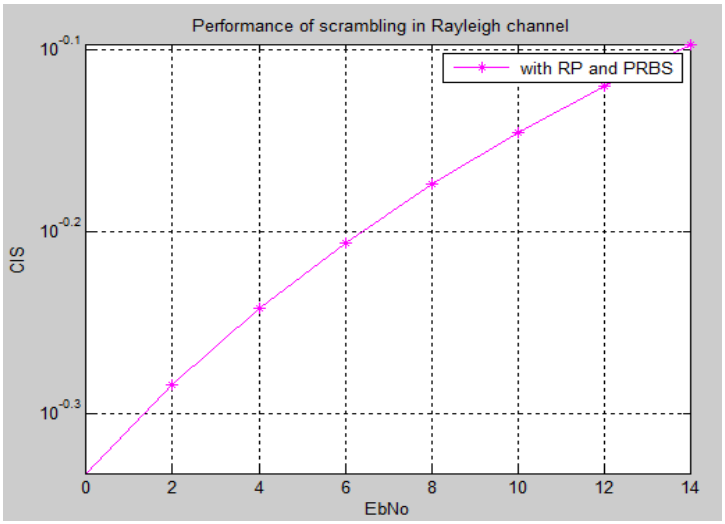

Fig. 5(b)

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

The simulation results shows 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.

IV. CONCLUSION

In this paper, a new OFDM scrambler, the OFDM scrambler with random permutation and PRBS scrambling is proposed. The results and simulations show that the original speech signal could be scrambled into unintelligible signal and it is also be confirmed that the scrambled signal could be recovered into the original speech signal. Also, the residual intelligibility of the scrambled speech is very low, since the intelligibility of the speech is excellent and the recovered speech files are identical to the original ones. The OFDM scrambler is suitable for frequency selective fading channels and it is a best technique for providing high security in the next generation mobile communication systems.

REFERENCES

[1] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo “Safeguarding 5G Wireless Communication Networks Using Physical Layer Security”, IEEE Communications Magazine, April 2015, Vol. 53, No. 4,pages:20-27

[2] Jiankun Hu;Ziping Xi;Jennings, A.;Lee, .Y.J.;Wahyudi, D, “DSP application in e-commerce security”, IEEE International Conference on Acoustics, Speech and Signal Processing, 2001. Proceedings. (ICASSP '01). , Volume: 2, DOI: 10.1109/ICASSP.2001.941087, Publication Year: 2001, Page(s): 1005 - 1008 vol.2

[3] Almasalha, F. ; Khokhar, A. ; Baqai, S. , “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 , Page(s): 1850 – 1853

[4] Lingjie Duan ; Jianwei Huang ; Walrand, J, “Economic analysis of 4G network upgrade” INFOCOM, 2013 proceedings IEEE DOI: 10.1109/INFCOM.2013.6566897 Publication Year: 2013 , Page(s): 1070 – 1078

[5] Zhancang Wang, “Demystifying Envelope Tracking” IEEE microwave magazine, DOI: 0.109/MMM.2014.2385351Date of publication: 6 March 2015

[6] Allsopp, S. ; Allsopp Helikites Ltd, Fordingbridge, “Emergency airborne 4G comms to aid disaster traffic management” Road Transport Information and Control Conference 2014 (RTIC 2014), IET, Page(s): 1 – 7

[7] Zayani, R. ; Sup"Com, Tunis, Tunisia ; Bouallegue, R. ; Roviras, D., “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, Page(s): 966 – 970

[8] Boudreau, G. ; Nortel, Toronto, ON ; Panicker, J. ; Ning Guo ; Rui Chang , “Interference coordination and cancellation for 4G networks”, Communications Magazine, IEEE , Volume:47 Issue:4

[9] Jaya kumari.J and Sakuntala.S.Pillai, “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.

[10] Şahin, M.E. ; 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, Page(s): 666 – 670

[11] Jaya kumari.J and Sakuntala.S.Pillai, “Orthogonal Frequency Division Multiplexing” Proc. 17th Kerala Science Congress, KFRI, Peechi, pp.139-142, 29-31 Jan 200

[12] 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, (Volume:8 , Issue: 10), DOI:10.1109/TWC.2009.090263 , Page(s): 5328 – 5337

[13] Dae Soon Cho ; 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.2006.1682802, Page(s): 192 – 195

[14] Hana'a M. A. Salman, "A Transform Based 3D- Speech Scrambling Using Multi-Wavelet: Design and Evaluation", The International Arab Conference on Information Technology (ACIT'2013)
[15] B. Jayaramakrishnan, Rajesh Vijayaraghavan2 and V. Ravichandran3, "On Counting Certain Permutations Used For Speech Scrambling", Journal of Physical Science, Vol. 17(2), 131–139, 2006
[16] Qiu-Hua Lin ; Sch. of Electron. & Inf. Eng., Dalian Univ. of Technol. ; Fu-Liang Yin ; Tie-Min Mei ; Hualou Liang, "A blind source separation based method for speech encryption" ,IEEE Transactions on Circuits and Systems I: Regular Papers, (Volume:53 , Issue: 6), DOI:10.1109/TCSI.2006.875164, Page(s): 1320 – 1328
[17] Dhanya G, Dr. J Jayakumari, "Optimal speech scrambling technique for OFDM based system", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 9, Number 24 (2014) pp. 28871-28878
[18] Thomas Strohmer and Scott Beaver, "Optimal OFDM design for high frequency dispersive cahnnels", IEEE transactions on communications,Vol.51,No.7,July2003,DOI:10.1109/TCOMM.2003.814200, Publication Year: 2003, Page(s):1111-1122.
[19] Tiago H. Falk1 and Wai-Yip Chan2, "Performance Study of Objective Speech Quality Measurement for Modern Wireless-VoIP Communications", EURASIP Journal on Audio, Speech, and Music Processing, Volume 2009, Article ID 104382, 11 pages.
[20] Jianfen Ma, Yi Hu and Philipos C. Loizou, "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions", Acoustical Society of America, May 2009

BIOGRAPHY

Dhanya. G received her A.M.I.E (Associate Membership of Institution of Engineers) in Electronics and Communication Engineering from Institution of Engineers (India), Kolkata in 2007 and M. E degree in Communication systems from Anna University Coimbatore in 2009. Since 2009 she has been working as an Assistant Professor with KMEA Engineering College, Ernakulum District, and Kerala. In addition, she has been pursuing her Ph.D. degree in Electronics and communication engineering at Noorul Islam University. She is a member of Institution of Engineers (India) and Institution of Electronics and Telecommunication Engineers (IETE)

Jayakumari. J is presently working as Dean, Faculty of Technology, Professor and Head, Department of Electronics & Communication Engineering, Noorul Islam University, Kanyakumari District, Tamil Nadu. She received her B.E. degree in Electronics & Communication Engineering from M.S. University, Tirunelveli in 1994 and M. Tech degree in Applied Electronics and Instrumentation from University of Kerala in 1998 and Ph.D. degree in Electronics and communication engineering from University of Kerala in 2009. Have teaching experience of 19 years, research experience of 13 years and administrative experience of 15 years. Was Head of Dept. of Electronics & Communication, C.S.I. Institute of Technology, Thovalai, Kanyakumari district (2000-2009). Have published several papers in International Journals and has chaired many technical sessions in International Conferences. Her research interest includes MIMO, OFDM, Signal processing, Detection & Estimation Theory Spread Spectrum Systems and Error Correcting Codes. She is a Fellow member of the Council of Engineering and Technology (India), senior member of Institution of Electrical and Electronics Engineers (IEEE) and life member of Institution of Electronics and Telecommunication Engineers (IETE), Indian Society for Technical Education (ISTE) and Institution of Engineers (India).