Research Journal of Applied Sciences 11 (5): 224-228, 2016
ISSN: 1815-932X

Improved Ofdm Based Speech Scrambler for next Generation Mobile Systems

G. Dhanya and J. Jayakumari
Noorul Islam University Nooral Islam University Kanyakumari, Tamil Nadu, India

Abstract: The speech scrambling is very important for providing security in communication systems. Many of the scrambling techniques show poor performance. In this study, a new time domain based scrambling using pseudo random sequences is proposed for OFDM based scramblers. In this technique pseudo random sequences are used to scramble the data at the transmitter side and at the receiver, descrambling of data is infeasible without the knowledge of a secrete key. The system is simulated and quality of the speech is measured using Perceptual Evaluation of Speech Quality (PESQ) and the intelligibility is measured using Speech Transmission Index (STI) and Common Intelligibility Scale (CIS). The simulation result shows that the proposed approach provides more security and gives better performance compared to conventional technique.

Key words: 4G, OFDM, speech scrambling, technique, system

INTRODUCTION

The security and privacy is highly essential in the field of mobile communication. The tremendous growth in data traffic, almost every corner the internet has been reached. According to recent statistics, numerous ways of encryption methods are used to protect the data traffic (Yang, *et al*., 2015; Zhou *et al*., 2015; Yang *et al*., 2015). In applications, the analog voice channel communication provides tactical level of security (Francisco and Ricardo 2012).

4G mobile communication provides enhanced services with higher data rate to address cellular user's ever-increasing demands for higher speed multimedia communication (Bhattacharjee *et al*., 2014; Duan *et al*., 2013. 4G is global network, it provides voice, data and multimedia to users on an "Anytime, Anywhere" basis (Khan *et al*., 2009). In 4th generation of mobile communication, the data rate is increased, it improves the quality of media communication and promises worldwide roaming at lower cost than 3G . 4G system provides quality service and stable system performance by supporting personalized and comprehensive services (Kim *et al*., 2004).

To satisfy multimedia requirements and support high data rate efficiently, OFDM has been considered for modulation in 4G systems (Kim *et al*., 2004). Orthogonal frequency division multiplexing is a multi carrier digital modulation technique, which is a global standard for 4th generation wireless communication. In the OFDM system, symbols are transmitted in parallel on several narrow-band sub-channels, which are overlapping and orthogonal (Cho and Park, 2006). OFDM is considered to be the best promising technique for 4G mobile networks and it is highly flexible for high data rate transmission over fading channels.

The attractive and efficient technology for mobile communication, OFDM which offers high spectral efficiency, multipath delay spread tolerance, immunity to the frequency selective fading channels and power efficiency (Hameed, 2014). OFDM does not have any security features. The additional security algorithms or encryption/scrambling algorithms should be providing to the required data security. Eavesdropping is security vulnerability and it is a great issue in wireless networks. It is the interception of an authorized person of a private communication. To prevent eavesdropping attacks computationally secured algorithms are used. Speech encryption does not sufficient for this if the scrambled speech contains residual intelligibility.

Analog scrambling is one of the best encryption methods in speech communication. The scrambler makes a speech signal unintelligible via permutation of speech segments in the time domain, frequency domain, and time-frequency domain. Also, there are many other scrambling techniques in the transform domain, such as FFT, DCT and wavelet transform, etc. (Tseng and Chiu, 2007). However, all of the above techniques are not efficient, due to signal with high residual intelligibility.

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

A new technique, OFDM based speech scrambler is used to avoid residual intelligibility. The OFDM scrambler can remove residual intelligibility of the scrambled speech and to obtain secured speech. It requires less key streams compared with other approaches. This study proposes a security enhancement for the OFDM system by using random permutation and PRBS (Pseudo Random Binary Sequence) scrambling. The computer simulations show that the proposed speech scrambler can attain a low level of residual intelligibility and a high level of security while retaining the quality of the recovered speech (Tseng and Chiu 2007; Li *et al*., 2013)

Conventional OFDM system: OFDM is an efficient communication technique to provide proper communication through frequency selective fading channels. The OFDM can be defined as a form of Multicarrier Modulation (MCM). Multicarrier modulation is used for transmitting a serial high data rate stream by splitting it into a set of parallel low-rate sub streams. The each of the data streams then modulating with individual subcarriers by applying N point Inverse Fast Fourier Transform (IFFT) to obtain time domain signal x(n). To make each subcarrier orthogonal to other subcarriers, the carrier spacing is carefully selected (Strohmer and Beaver, 2003):

$$x(n) = \sum_{k=0}^{k=n} X(k) e^{j2pkn} / N \quad (1)$$

Where, N = 0, 1, 2……N-1. X(k) denotes the kth discrete sample of N samples in the Frequency domain. The cyclic prefix addition is performed at the output of the inverse FFT. After the cyclic prefix addition, the signals are then converted back to serial stream by the parallel to a serial unit (P/S) before they are transmitted through the communication channel.

At the receiver side the data is recovered by performing an FFT on the received signal. (Hao Li *et al*., 2013):

$$Y(k) = FFT[x(n)] = \sum_{k=0}^{k=n} x(k) e^{-j2pkn} / N \quad (2)$$

Where, k = 0, 1, 2, ..., N-1. Where the sequence x (n) contains N samples in the time domain.

OFDM scrambler: The conventional OFDM scrambler uses a scrambling key generator which is controlled by a seed and a secret key. This system uses a single level of scrambling (Tseng and Chiu, 2007). The other OFDM scrambler uses random permutation scrambling, It rearrange the speech segments in time domain basis (Li *et al*., 2013). The proposed system combines these two techniques and uses double level of encryption using random permutation and pseudo random generator. This improves the security and reduces the residual intelligibility.

MATERIALS AND METHODS

Proposed system: The block diagram of proposed system is shown in Fig. 1 (Dhanya and Jayakumari, 2014).

Scrambling and descrambling: The proposed system uses double level of scrambling by one after another. The first scrambling is based on random permutation with a seed. By using this seed, the signals are reordered. The output of the scrambler generates a random data sequence and this sequence is given to the next scrambler.

The second scrambler is PRBS generator. The second type of scrambling is called pseudo random code based scrambling. Here, a key is used for scrambling; this scrambler is a linear feedback shift register which produces a random data. The output of the LFSR first XORed with the random permutation scrambler output (Dhanya, Jayakumari, 2014). The output will becomes a scattered output and it will unintelligible to others. This data is transmitted through the channel. It produces zero residual intelligibility and high security to cryptanalytic attacks.

On the receiver side, the same key and seed is used for descrambling the data. For analyzing the system, the following parameters are considered (Table 1)

Table 1: Parameters of proposed OFDM based speech scrambler (Dhanya and Jayakumari, 2014)

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	16 QAM

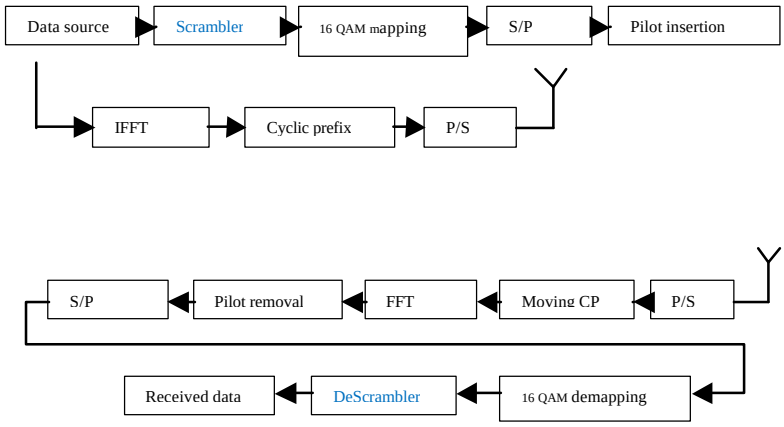

Fig. 1: Block diagram of proposed OFDM based speech scrambler

RESULTS AND DISCUSSION

Performance evaluation

Noise measurement: The performance of the system is evaluated by means of Signal to Interference plus Noise Ratio (SINR) and BER under AWGN channel. The SINR and the BER performance of PRBS with the random permutation (PRBS scrambling) are compared with conventional OFDM and OFDM with random permutation scrambling (Fig. 2).

Signal to Interference Plus Noise Ratio (SINR) analysis: For SINR performance analysis considering that all the terms are zero mean and statistically independent random variables (Amutha and Manikandan 2012). The received power is expressed by (Nguyen and Nguyen, 2012):

$$P_r = P_S + P_{ICI} + N_0 \quad (3)$$

The value of Signal to Interference plus noise ratio (SINR) is expressed as the ratio between Signal power (P_S) and Interference power (P_{IC}) plus noise power (N_0):

$$SINR = P_S / P_{ICI} + N_0 \quad (4)$$

The speech.wav file was given as input signal, shown in Fig. 3 and 4 Table 2. The BER is calculated using the parameter Eb/No. The random permutation with PRBS shows better performance and it has low-bit error rate when comparing with the others (Dhanya and Jayakumari 2014).

Perceptual Evaluation of Speech Quality (PESQ): PESQ implements an algorithm for comparing an original speech signal with received speech signal. The original speech signal is known as "reference signal" and received signal is known as "degraded signal" (Falk and Chan, 2009).

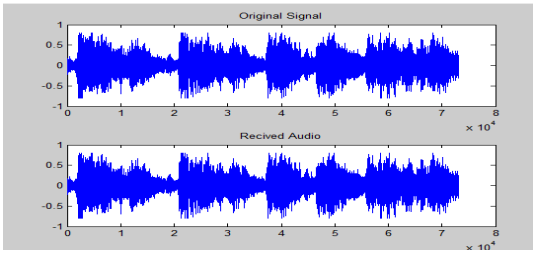

Fig. 2: Original and reconstructed speech waveform

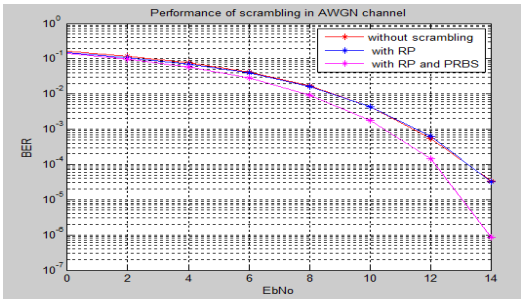

Fig. 3: BER performance of OFDM based speech scrambler under AWGN channel

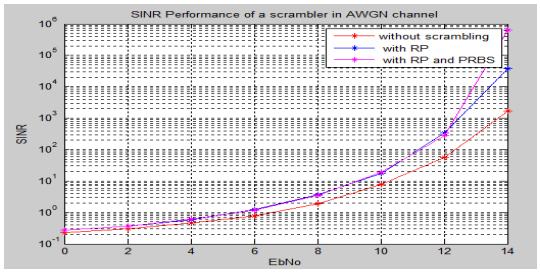

Fig. 4: BER performance of OFDM based speech scrambler under AWGN channel

Table. 2: Comparison of different types of OFDM speech scramblers based on SINR in AWGN channel

Type of OFDM	Eb/N0	BER	SINR
Without scrambling	10	0.0043	0.0080
OFDM with RP	10	0.0045	0.0077
OFDM with and RP and PRBS	10	0.0017	0.0018

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

Type of OFDM	PESQ (AWGN)
Without scrambling	4.13
OFDM with Random permutation(RP)	4.18
OFDM with RP and PRBS	4.40

The Perceptual Evaluation of Speech Quality (PESQ), it calculates the quality of a speech signal by a 5 point scale. The 1 corresponds to bad or unsatisfactory speech quality 2 for poor, 3 for fair 4 for good and 5 indicates excellent speech quality (Falk and Chan, 2009).

From the above comparison reveals that the RP with PRBS scrambling shows good performance than two the other methods (Table 3).

Measurement of speech intelligibility: Speech intelligibility is a number defined as the how much of speech units are recognize correctly in acertain situation. Otherwise we can say that it is the degree to which we can understand the spoken language. It may be a single number value (Ma *et al*., 2009). Two methods are frequently used for measuring speech intelligibility.

Speech Transmission Index (STI)

Common Intelligibility Scale(CIS): The most important and comprehensive speech intelligibility parameter is speech transmission index. The speech transmission index is in the range between 0 and 1. The one indicates excellent. The weighted sum of Modulation Transfer Function (MTF) (Fig. 5-7, Table 4) 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. The SNR ranges are limited from +15db-15db (Ma *et al*., 2009). Speech transmission index computes all the factors in the speech transmission path, affects intelligibility.

The results shows that the RP with PRBS scrambling shows better performance since the speech transmission index, common intelligibility scale and perceptual evaluation of speech quality are better in this scrambling. Also, shows the low SINR and the BER performance (Table 5).

Table 4: Relation between STI and speech intelligibility [21]

STI	0.00-.30	0.30-.45	0.45-.60	0.60-.75	0.75-1.00
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 and PRBS	10	0.0017	0.0018	0.7520	0.7150

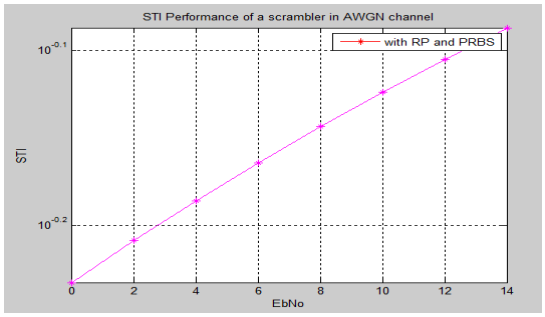

Fig. 5: STI performance for intelligibility measurement in OFDM based speech scrambler under AWGN channel

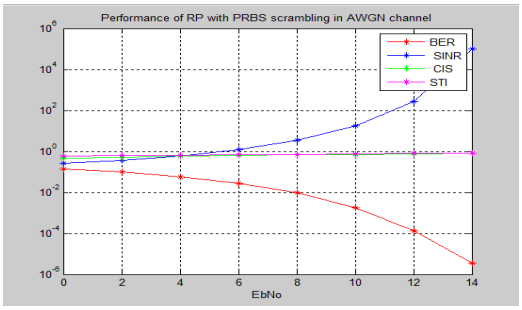

Fig 6: CIS performance for intelligibility measurement in OFDM based speech scrambler under AWGN channel

CONCLUSION

This study evaluated the two different parameters Speech Transmission Index and Common Intelligibility Scale for predicting the intelligibility of speech, used two other parameters Signal to Interference plus Noise Ratio and Bit Error Rate for evaluating the noise performance. The Perceptual Evaluation of Speech Quality was used to measure the quality of speech. From the simulation results, the value of BER (0.0017) and SINR (0.0018) is very low, the value of STI (0.7520) and CIS (0.7150) is excellent with respect to the value of Eb/N0 is 10.The PESQ (4.40) is also excellent. These results show that the

new speech scrambling algorithm, random permutation with pseudo random number sequence, makes low residual intelligibility and high speech quality. It is crypt analytically secured algorithm and this algorithm can be used for transmitter as well as receiver ends without any modifications. In 4G mobile communication, it is a promising technique for high data rate transmission and it is to be best for providing high security in next generation mobile communication systems.

REFERENCES

Amutha, N.P. and V. Manikandan, 2012. Optimum medium access technique for next generation wireless systems. J. Theor. Appl. Inf. Technol., 36: 279-283.

Bhattacharjee, P.K., S. Roy and R.K. Pal, 2014. Advance artificial intelligence based mutual authentication technique with four entities in 4-G mobile communications. Proceedings of the 2014 International Conference on Soft Computing and Machine Intelligence (ISCMI), September 26-27, 2014, IEEE, New Delhi, India, pp: 139-145.

Cho, D.S. and H.J. Park, 2006. Implementation of an improved clock frequency offset compensator for 4G OFDM system at ETRI. Proceedings of the 2006 IEEE 63rd Conference on Vehicular Technology, May 7-10, 2006, IEEE, Melbourne, Victoria, Australia, ISBN: 0-7803-9391-0, pp: 192-195.

Dhanya, G. and J. Jayakumari, 2014. Optimal speech scrambling technique for OFDM based system. Int. J. Appl. Eng. Res., 9: 28871-28878.

Duan, L., J. Huang and J. Walrand, 2013. Economic analysis of 4G network upgrade. Proceedings of the 2013 IEEE Conference on INFOCOM, April 14-19, 2013, IEEE, Turin, Italy, ISBN: 978-1-4673-5944-3, pp: 1070-1078.

Falk, T. and W.Y. Chan, 2009. Performance study of objective speech quality measurement for modern wireless-VoIP communications. EURASIP. J. Audio Speech Music Process., Vol, 10.1155/2009/104382

Francisco A.D.O.N. and G.T. Ricardo, 2012. Frequency speech scrambler based on the hartley transform and the insertion of random frequency components. Int. J. Forensic Comput. Sci., 1: 8-15.

Hameed, L.S., 2014. A combined weighting and PTS technique for PAPR reduction in OFDM signals. Proceedings of the 2014 2nd International Conference on Current Trends in Engineering and Technology (ICCTET), July 8, 2014, IEEE, Coimbatore, India, ISBN: 978-1-4799-7986-8, pp: 228-232.

Khan, A.H., M.A. Qadeer, J.A. Ansari and S. Waheed, 2009. 4G as a next generation wireless network. Proceedings of the. International Conference on Future Computer and Communication ICFCC, April 3-5, 2009, IEEE, Kuala Lumpar, Malaysia, ISBN: 978-0-7695-3591-3, pp: 334-338.

Kim, N., H. Choi and H. Yoon, 2004. Seamless handoff scheme for 4G mobile systems based on IP and OFDM. Proceedings of the 2004 IEEE 60th Conference on Vehicular Technology VTC2004-Fall, September 26-29, 2004, IEEE, Daejeon, South Korea, ISBN: 0-7803-8521-7, pp: 3315-3318.

Li, H., X. Wang and W. Hou, 2013. Secure transmission in OFDM systems by using time domain scrambling. Proceedings of the 2013 IEEE 77th Conference on Vehicular Technology (VTC Spring), June 2-5, 2013, IEEE, Dresden, Germany, pp: 1-5.

Ma, J., Y. Hu and O. Loizou, 2009. Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions. J. Acoust. Soc. Am., 125: 3387-3405.

Nguyen, V.D.N. and H.L.C.T.T. Nguyen, 2012. Interference analysis for OFDM transmissions in the presence of time-varying channel impairment REV. J. Electron. Commun., Vol. 2,

Strohmer, T. and S. Beaver, 2003. Optimal OFDM design for time-frequency dispersive channels. IEEE. Trans. Commun., 51: 1111-1122.

Tseng, D.C. and J.H. Chiu, 2007. An OFDM speech scrambler without residual intelligibility. Proceedings of the 2007 IEEE Region 10 Conference on TENCON, October 30-November 2, 2007, IEEE, Taipei, Taiwan, ISBN: 978-1-4244-1271-6, pp: 1-4.

Yang, M., J. Luo, Z. Ling, X. Fu and W. Yu, 2015. De-anonymizing and countermeasures in anonymous communication networks. IEEE. Commun. Mag., 53: 60-66.

Yang, N., L. Wang, G. Geraci, M. Elkashlan and J. Yuan, *et al*., 2015. Safeguarding 5G wireless communication networks using physical layer security. IEEE. Commun. Mag., 53: 20-27.

Zhou, H., C. Wu, M. Jiang, B. Zhou and W. Gao *et al*., 2015. Evolving defense mechanism for future network security. IEEE. Commun. Mag., 53: 45-51.