Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9455-9460, 2017
ISSN: 1816-949X


# Efficient and Secure Key Extraction Approach for OFDM System with Adaptive Filtration

Preeti Pathania and Rajpreet Singh
Department of Electronics and Communication Engineering,
Chandigarh University, Gharaun, Punjab, India

**Abstract:** Key extraction is the propitious technique to create a protected key between the users over the OFDM subcarrier. This study present a new perspective for extraction of key securely and efficiently with adaptive filtration for OFDM system. The efficiency is accomplished by the totally exploiting randomness from frequency and time domain and cross correlation of channel measurements. The system can be classified in terms of Key Generation Rate (KGR), Key Disagreement Rate (KDR) and key randomness. RLS adaptive filter is introduced for better noise reduction in OFDM sub carriers and improves convergence speed.

**Key words:** OFDM, adaptive filter, RLS algorithm, LMS algorithm, BER, subcarrier

## INTRODUCTION

Wireless communication grant all the users to hear transmission within the spectrum, thus, making it endangered to different attacks (Attar *et al*., 2012; Zhang *et al*., 2016a, b; Yang *et al*., 2014), some of the attacks are jamming, traffic analysis, DoS (Denial of Service attack), spoofing, etc. In 5G network, there are various facilities have developed such as large scale mimo,full duplex communication, etc. (Xi *et al*., 2014). There are many ways to protect wireless transmission data from various unwanted and unusual attacks. Wireless network security thus attracted many research interests. Key generation is the promising technique to established a secure key between the users over the OFDM sub carriers (Shrivas, 2015). RLS algorithm is used to improve noise quality and convergence speed. In LMS, the convergence speed and noise in unsatisfactory. Adaptive filter is introduced to recover convergence speed and improve noise quality which is not upto the mark in LMS. RLS offer fast speed. Key extraction for OFDM system from RLS filtration is easy and effective for the improvement of echo signals, system identification, system prediction and noise cancellation. The system is asses in terms of key randomness, key generation rat system is assess in terms of key randomness, KGR (Key Generation Rate) and key disagreement rate (Zhang *et al*., 2016a, b). The key generation rate titrate or evaluate the total of several key bits developed in every second.KGR can be written as:

$$KGR = \frac{Nk}{Tk}$$

where, Nk and Tk are the number of key bits and time taken. Key sequence is very important in cryptography with a proper length. key disagreement rate is the disagreement rate of unprocessed bits. For better efficiency, disagreement rate of key should be small and generation rate of key should be high. Key disagreement rate could be better by correcting the signal cross correlation (Patwari *et al*., 2010). Key disagreement rate could be enhanced by CSI (Channel State Information) and exploiting randomness from spatial, frequency and temporal domain. A high and efficient KGR can be easily obtained by channel state information (Wilson *et al*., 2007). For extracting keys, various practical simulations have been proposed from various channel parameters. Some of the channel parameters are cannel phase in narrow band system, RSS, etc. (Liu *et al*., 2013; Mathur *et al*., 2008). In the proposed research, we have evaluated the key generation scenario to find channel state information from channel responses and evaluate the correlations and entropy of the system and shows that our proposed approach is less key disagreement rate which should be low for efficient reducing the overhead from the system and reveals limited data in the time of public conversation. Efficient key generation is having low key disagreement rate which are helpful in getting high channel (Wilson *et al*., 2007).

## OFDM

The orthogonal frequency division multiplexing is the statistics of signal modulation that converts the high data rate into smaller closely spaced OFDM sub carriers for better transmission of signals over the system orthogonal

**Corresoponding Author:** Preeti Pathania, Department of Electronics and Communication Engineering, Chandigarh University, Gharaun, Punjab, India

frequency division multiplexing is referred to as a multicarrier which is widely used for modulation and multicarrier technique OFDM transmission alleviates many of the problems confront with the single carrier transmission (Mathai and Sagayam, 2013). In OFDM system, the carriers are orthogonal to each other. Orthogonality in OFDM is the main aspect as it should be maintained between the carriers (Wallace and Sharma, 2010; Minn *et al*., 2003). In 4G and 5G wireless communication system, the orthogonal frequency division multiplexing is a very alluring technique for high bit transmission rate. The concept of parallel transmission of symbols has a great importance in wireless communication system. OFDM is one of the best multicarrier transmission technique for parallel transmission in wireless communication system. In OFDM, the FFT (Fast Fourier Transform) and IFFT (Inverse Fast Fourier Transform) methods are collectively used for modulation and demodulation of the sub carriers in ofdm system (Wallace *et al*., 2009).

**Advantages of OFDM:**

- It has low multipath distortion
- It is immune to selective fading
- It has a high spectral efficiency
- It is easily equalized
- Flexible

**Limitation of OFDM:**

- It exhibits high PAPR
- Intercarrier interference between the sub carriers

## ADAPTIVE FILTER

Adaptive filters are adaptive in nature and is very useful in increasing speed and improves noise quality and hence, improves complexity of the system. The real-time adaptive filtering algorithms are essential for future communication. Adaptive filters are used for both wired and wireless. Adaptive filter cancel out noise at input signal and is the important algorithm for system improvement. In this study, two adaptive filters are used, one is the LMS (Least Mean Square) and another is the RLS (Recursive Least Square).

**Various application of adaptive filter:**

- Noise cancellation
- System identification
- Echo cancellation
- Signal prediction

**System identification:** It designs an adaptive filter that provides approximation.

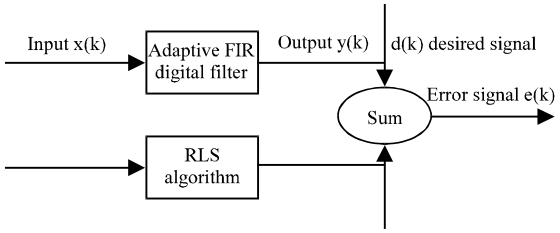


Fig. 1: Block diagram of adaptive filter algorithm

**Noise cancellation:** It reduces noise from received signal to improve SNR.

**Echo cancellation:** It break off unexplored interference from primary signal.

**Signal prediction:** It predicts the present value of random signal. In Fig. 1,where x(K) refers to input signal, y(K) refers to output signal, d(K) refers to desired signal and e(K) refers to error signal.

**LMS algorithm:** LMS algorithm are used to mimic desired signal and is a class of adaptive filter. LMS algorithm is also known as stochastic gradient algorithm. LMS is slightly inferior to RLS algorithm. LMS (Least Mean Square) algorithm are unsatisfactory in terms of noise cancellation. The major disadvantage of LMS algorithm is that it has slow rate of convergence and is sensitive to the eigen delay spread.

**RLS algorithm:** RLS algorithm is used to solve the least square error and is the well known least square method. In previous years, RLS can be regarded as a powerful tool for adaptive filtering, prediction and identifying. The aim of RLS is to minimize the difference between desired signal and the filtered output. RLS (Recursive Least Square) exhibit high rate of convergence as compared to LMS algorithm. The SNR in case of RLS is better than the LMS. RLS is considered as the best adaptive filter (Islam and Ajra, 2015). The proposed algorithm is given in Fig. 2.

**Proposed algorithm**

**Simulation results:** Figure 3 shows the temporal correlation coefficient which is a measure of variance or spatial variability as the signal is travelling in free space. Figure 4 shows the amplitude of the signal in the distorted channel which is having scattering or multipath effect with respect to the change in frequency.

Figure 5 shows the LMS filtered output with less mean square error rates with respect to the change in

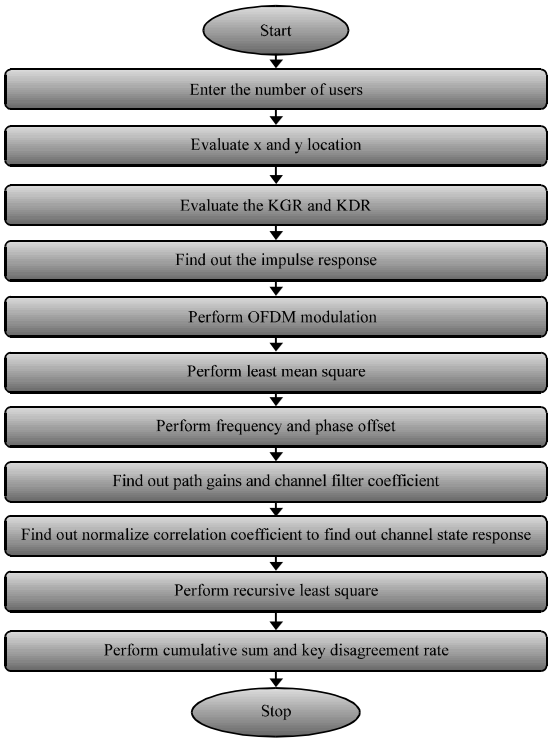


Fig. 2: Proposed algorithm

frequency and is showing that after apply least square approach the channel is having least error rates.

Figure 6 shows correlation coefficients and normalized correlations which shows the correlation between channel coefficients for the channel state information with respect to the time delay. Figure 7 shows the correlation coefficients with respect to the subcarrier location or index to evaluate channel state information and shows high peaks due to some high frequency components in the signal.

Figure 8 shows the bit error rate with respect to the signal to noise ratio. As it is showing that BER is decreases as SNR increases which shows that the loss of bits are less and having high signal strength.

As it is shown in the Fig. 9, the disagreement rate is coming less as the signal to noise ratio increases which shows the our proposed approach is having less KDR as compared to our base approach.

Figure 10 shows the cumulative sum between the base and proposed work and shows that the cumulative sum of the proposed work is high. Through cumulative sum we can estimate the outbreaks in the signal which will degrade the strength of the signal. Through cumulative sum we can also estimate the

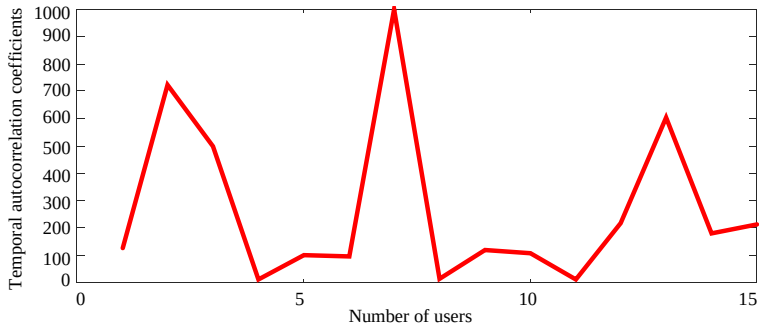


Fig. 3: Temporal correlation coefficient

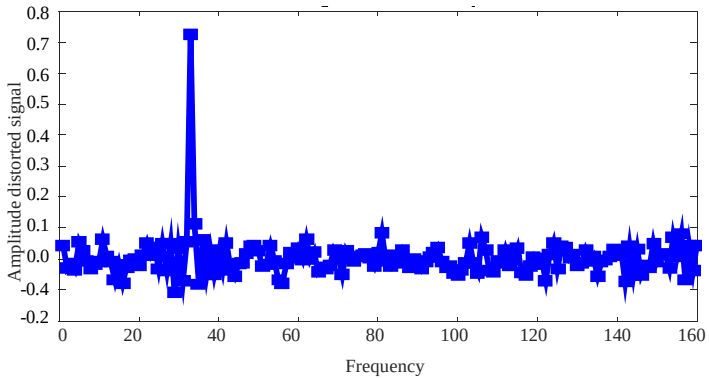


Fig. 4: Multipah effect (Transmitted signal with multipath effect)

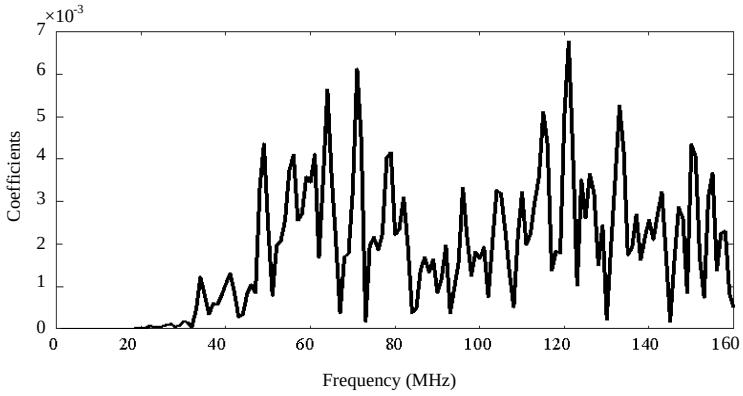


Fig. 5: MS filtered output

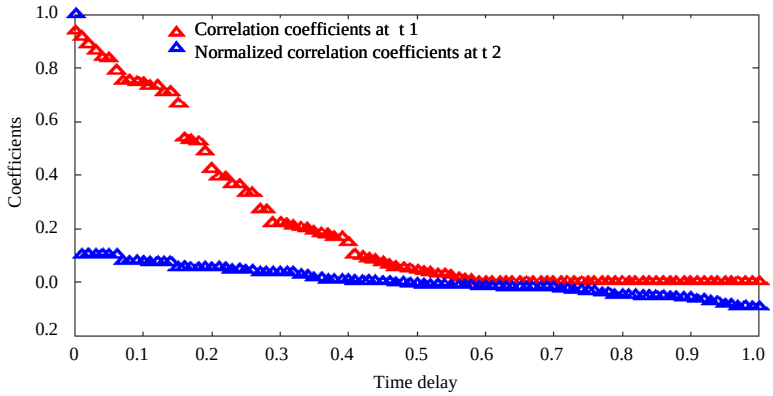


Fig. 6: Corelation and normalized correlation coefficient

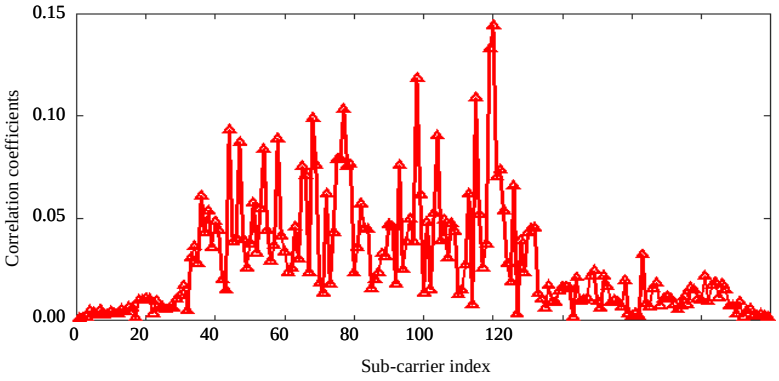


Fig. 7: Correlation coefficient with respect to sub-carrier index

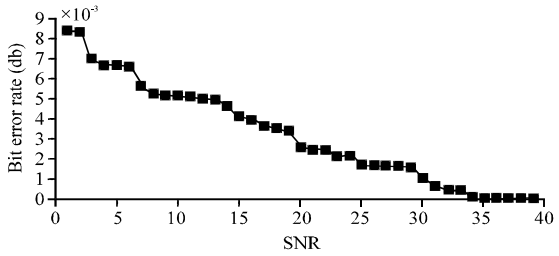


Fig. 8: Bit error rate performance

Table 1: Key disagreement rate

| Frequency (Hz) | Base | Proposed |
|---|---|---|
| 20 | 0.120 | 0.00020 |
| 50 | 0.110 | 0.00018 |
| 100 | 0.110 | 0.00015 |
| 200 | 0.005 | 0.00012 |
| 500 | 0.002 | 0.00009 |
| 1000 | 0.001 | 0.00008 |

variance of the signals and detects the multiple changes as applied through input signal (Table 1 and 2).

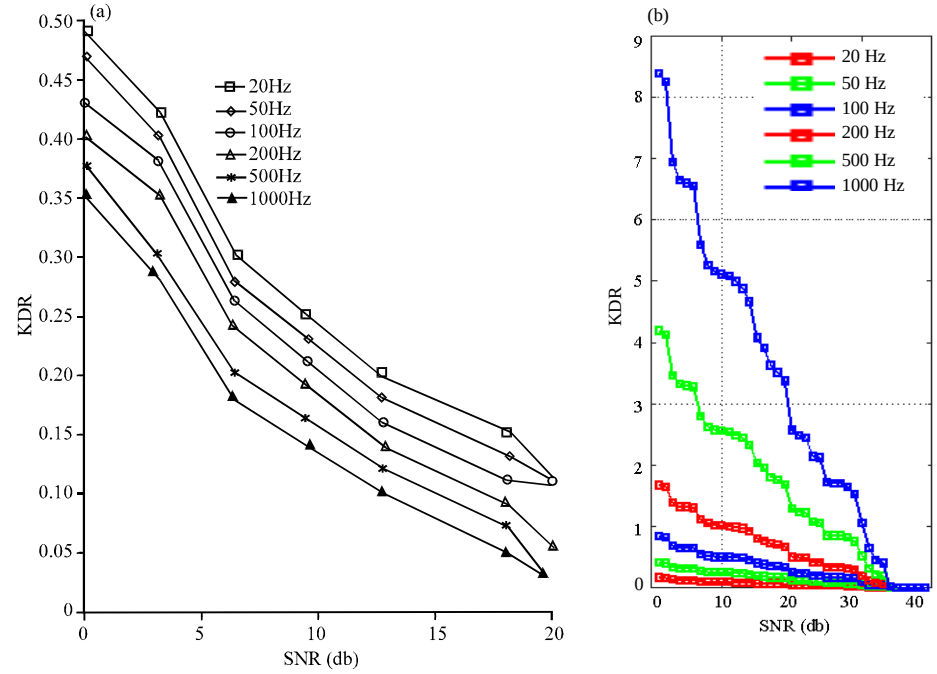


Fig. 9: The key disagreement rate with respect to number of frequencies; a) Key disagrrement rate (base results) and b) Key disagrrement rate

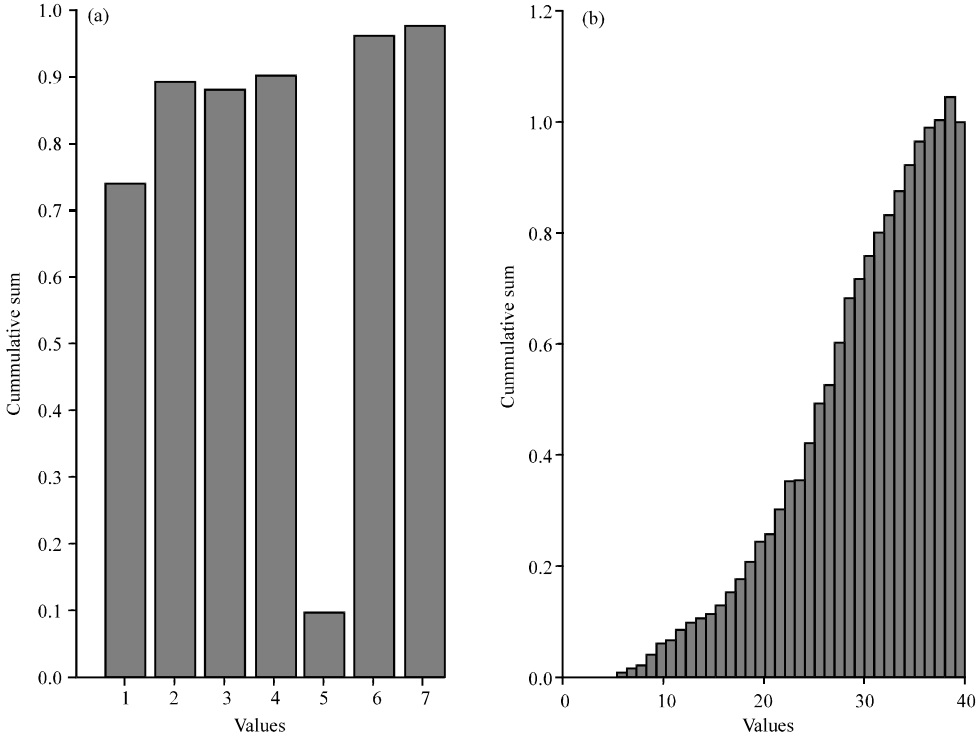


Fig. 10: The cumulative sum; a) Base and b) Proposed

Table 2: Cumulative sum

| Base | Proposed |
|---|---|
| 0.75 | 0.20 |
| 0.90 | 0.60 |
| 0.89 | 0.85 |
| 0.90 | 0.92 |
| 0.92 | 0.98 |
| 0.97 | 1.00 |

## CONCLUSION

In the proposed research, we have evaluated the key generation scenario to find channel state information from channel responses and evaluate the correlations and entropy of the system and shows that our proposed approach is less key disagreement rate which should be low for efficient reducing the overhead from the system and reveals less information during public discussion. In this study, an adaptive filtration is used for OFDM system to extract efficient and secure key. The proposed adaptive filter is based on RLS algorithm. The proposed RLS algorithm exhibit better noise cancellation in OFDM signal when it compared to LMS algorithm. The simulation result obtained by RLS guarantees the superior performance in terms of speed, BER.

## RECOMMENDATION

In future research, RLS based proposed noise canceller can be tested on different scheme in OFDM system.

## REFERENCES


Attar, A., H. Tang, A.V. Vasilakos, F.R. Yu and V.C. Leung, 2012. A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proc. IEEE., 100: 3172-3186.

Islam, M.S. and H. Ajra, 2015. Comparative study of adaptive filter algorithm of a QO-STBC encoded MIMO CDMA system. Intl. J. Comput. Networks Appl., 2: 254-260.

Liu, H., Y. Wang, J. Yang and Y. Chen, 2013. Fast and practical secret key extraction by exploiting channel response. Proceedings of the 2013 IEEE International Conference on INFOCOM, April 14-19, 2013, IEEE, Turin, Italy, ISBN:978-1-4673-5944-3, pp: 3048-3056.

Mathai, V. and K.M. Sagayam, 2013. Comparison and analysis of channel estimation algorithms in OFDM systems. Intl. J. Sci. Technol. Res., 2: 76-80.

Mathur, S., W. Trappe, N. Mandayam, C. Ye and A. Reznik, 2008. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, September 14-19, 2008, ACM, San Francisco, California, USA., ISBN:978-1-60558-096-8, pp: 128-139.

Minn, H., V.K. Bhargava and K.B. Letaif, 2003. A robot timing and frequency synchronization for OFDM system. IEEE. Trans. Wireless Commun., 2: 822-839.

Patwari, N., J. Croft, S. Jana and S.K. Kasera, 2010. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE. Trans. Mobile Comput., 9: 17-30.

Shrivas, A.K., 2015. A comparative analysis of LS and MMSE channel estimation techniques for MIMO-OFDM system. Intl. J. Sci. Res. Dev., 1: 44-48.

Wallace, J.W. and R.K. Sharma, 2010. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis. IEEE. Trans. Inf. Forensics Secur., 5: 381-392.

Wallace, J.W., C. Chen and M.A. Jensen, 2009. Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits. Proceedings of the 3rd European Conference on Antennas and Propagation EuCAP, March 23-27, 2009, IEEE, Berlin, Germany, ISBN:978-1-4244-4753-4, pp: 1499- 1503.

Wilson, R., D. Tse and R.A. Scholtz, 2007. Channel identification: Secret sharing using reciprocity in ultra-wideband channels. IEEE. Trans. Inf. Forensics Secur., 2: 364-375.

Xi, W., X.Y. Li, C. Qian, J. Han and S. Tang *et al*., 2014. KEEP: Fast secret key extraction protocol for D2D communication. Proceedings of the 2014 IEEE 22nd International Symposium on Quality of Service (IWQoS), May 26-27, 2014, IEEE, Hong Kong, China, ISBN:978-1-4799-4852-9, pp: 350-359.

Yang, H., Y. Zhang, Y. Zhou, X. Fu and H. Liu *et al*., 2014. Provably secure three-party authenticated key agreement protocol using smart cards. Comput. Networks, 58: 29-38.

Zhang, J., T.Q. Duong, A. Marshall and R. Woods, 2016a. Key generation from wireless channels: A review. IEEE. Access, 4: 614-626.

Zhang, J., A. Marshall, R. Woods and T.Q. Duong, 2016b. Efficient key generation by exploiting randomness from channel responses of individual OFDM sub carriers. IEEE. Trans. Commun., 64: 2578-2588.