IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Secure Communication – Using Interleaved Subcarrier Selection Technique

Steffi Jose[1]

M.Tech Scholar, Department of ECE, Mount Zion college of Engineering, Kadammanitta, Kerala, India[1]

Abstract: In this paper, a sorted subcarrier interleaving technique is used for preventing eavesdropping in OFDM system. In each OFDM signal, subcarriers are interleaved according to the sorted order of channel impulse response. Random noise can be added before interleaves to get two tire secrecy rate. The frequently updated subcarrier interleaving pattern can only be shared between legitimate nodes based on channel reciprocity. Without a proper de-interleaving pattern, mismatched information recovery occurs at the eavesdropper, thus preventing eavesdropping. A subcarrier selection algorithm is investigated to realize a trade-off between the eavesdropping resilience and transmission reliability.

Keywords: Security, wireless communications, orthogonal frequency division multiplexing (OFDM), eavesdropping, subcarrier interleaving.

I. INTRODUCTION

Securing wireless communication is a critical challenge due to the inherent broadcast nature of radio signal propagation. Intruders can possibly intercept the data traffic as long as they lie within the radio transmission coverage areas. Orthogonal frequency-division multiplexing (OFDM) has been widely adopted in modern wireless communications networks, because of its high spectral efficiency and robustness against multipath fading. Unfortunately, a conventional OFDM signal is vulnerable to eavesdropping attacks due to its distinct time and frequency characteristics, such as the time- and frequency-domain correlations and second-order cyclostationarity. Taking advantage of these characteristics, eavesdroppers can blindly estimate the transmission parameters of OFDM systems and then infer the transmitted information.

A. Contributions of the proposed secure communication system.

An effective secure system is proposed in this paper. Relying on the dynamic channel state information (CSI) between legitimate users, a subset of subcarriers in each OFDM signal is selected and then interleaved according to the decreasing order of their channel gains. Based on channel reciprocity, the CSI-based subcarrier interleaving permutation can be shared between legitimate terminals without any signaling. Due to the independence between spatially separated wireless channels, legitimate and eavesdropping channels are uncorrelated. It is thus hard for eavesdroppers to deduce the dynamic interleaving pattern and then to recover the transmitted information. Contributions of the paper are summarized as follows:

- CSI-based sorted subcarrier interleaving method is used to overcome passive eavesdropping. Although subcarrier interleaving has been introduced into OFDM systems to improve the transmission reliability.
- The impact of imperfect reciprocity of channel estimates at the legitimate communicating pair, which is induced by noisy channel estimations, is addressed in the design. A subcarrier selection algorithm is investigated to achieve a trade-off between the resilience against eavesdropping and reliability of legitimate transmission.
- The symbol error rate (SER) of eavesdropping, information leakage at the eavesdropper and security against brute force attacks are analyzed to prove the security of the proposed approach.
- The performances of bit error rate (BER) Vs signal to noise ratio (SNR) are analyzed.

II. PROBLEM FORMULATION

A wireless communication system model considered in Fig 1.A source node communicates with a legitimate receiver in a richly scattered radio environment, in the presence of a passive and silent eavesdropper. OFDM is adopted for the transmission between legitimate users, and the eavesdropper also has the capability to de- modulate OFDM signals. Moreover, the eavesdropper can intercept all transmissions between legitimate users, but is not interested in disrupting the legitimate transmission. The forward and reverse channels between legitimate users occupy the same frequency band. A slow fading channel condition is considered, so that the forward and reverse channels remain constant over several time slots. In addition, the underlying noise and interference in both the main channel (between the transmitter and intended receiver) and eavesdropping channel (between the transmitter and eavesdropper) are modeled as additive white Gaussian noise (AWGN).

Generally, a third party, who is at a distance larger than half a wavelength from the intended receiver, experiences fading conditions that are uncorrelated to those between the original legitimate communicating terminals. For instance, in the 2.4 GHz frequency band, an eavesdropper which is roughly 6.25 cm away from the legitimate receiver would be affected by an eavesdropping channel independent of the main channel.

DOI 10.17148/IJARCCE.2016.5188

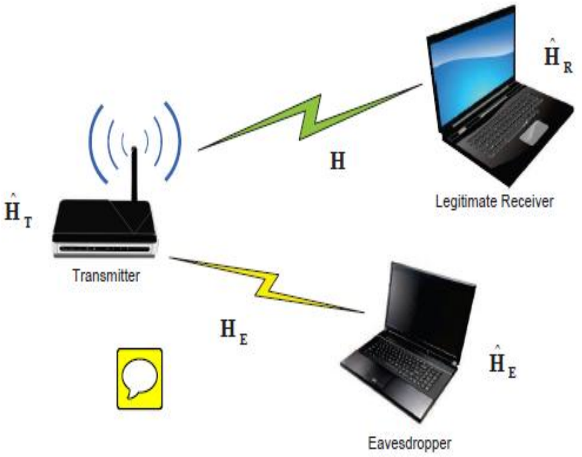

Fig 1: A wireless communication scenario consisting of two legitimate terminals and an eavesdropper.

In most practical scenarios, the eavesdropper has to be sufficiently separated from the legitimate terminals to avoid being detected, that is, with a distance of more than half a wavelength. Therefore, the distance between the legitimate receiver and eavesdropper is assumed to be larger than half a wavelength in this paper. The main channel and eavesdropping channel are thus modeled as independent channels.

III. PROPOSED SECURE OFDM SYSTEM WITH SORTED SUBCARRIER INTERLEAVING

The proposed eavesdropping-resilient OFDM system with sorted subcarrier interleaving is illustrated in Fig. 2. At the transmitter end, M out of the N subcarriers of each OFDM signal are selected and interleaved after the symbol modulation. Accordingly, subcarrier deinterleaving is carried out between the equalization and symbol demodulation processes at the receiver end. The selection of the M interleaved subcarriers and their interleaving permutation are determined by the real-time CSI between the transmitter and legitimate receiver. The other processing steps of the proposed system are identical to those of a conventional OFDM system. It is noteworthy that the transmitter and legitimate receiver would estimate the main channel and determine the subcarrier interleaving pattern individually based on channel reciprocity. No sharing of their CSI estimates is required and allowed.

A. Selection of Interleaved Subcarriers

Due to the presence of channel estimation errors, channel observations at the transmitter and legitimate receiver are not perfectly reciprocal. In order to mitigate the impairment caused by imperfect reciprocity, only a subset of M $\leq$ N subcarriers in each OFDM signal , which can provide an interleaving pattern robust against imperfectly reciprocal channel estimates under an instantaneous channel condition is selected for the dynamic interleaving sat the transmitter. A trade off between the resilience to eavesdropping and reliability of legitimate transmission is realized with a proposed subcarrier selection algorithm. Let M denote the subset of subcarriers involved in the dynamic subcarrier interleaving

$$\xi\,(k)= 1,\ k\ E\ M$$
$$0,\ k\ E\ \cancel{M},\quad k= 0,1,\ .....,\ N\text{-}1$$

Due to the channel reciprocity, the legitimate receiver is able to determine ξ However, a mismatched ξ may occur due to an asymmetric CSI observation, particularly in an extremely hostile communication environment. This would cause several transmission errors. As will be shown in Section IV, the eavesdropping prevention capability of the proposed system is dominated by the subcarrier interleaving permutation, rather than the side information ξ. Thus, ξ can alternatively be sent out by the transmitter to improve the reliability of legitimate transmission, though this operation faces a potential threat of leakage of the information ξ. Whether or not to share the subcarrier selection result ξ would depend on the transmission reliability requirements and channel conditions. In the presented system design, ξ is transmitted from the transmitter to the legitimate receiver along with the data traffic, in order to achieve a low error rate transmission. It must be emphasized that it is not necessary to share this side information.

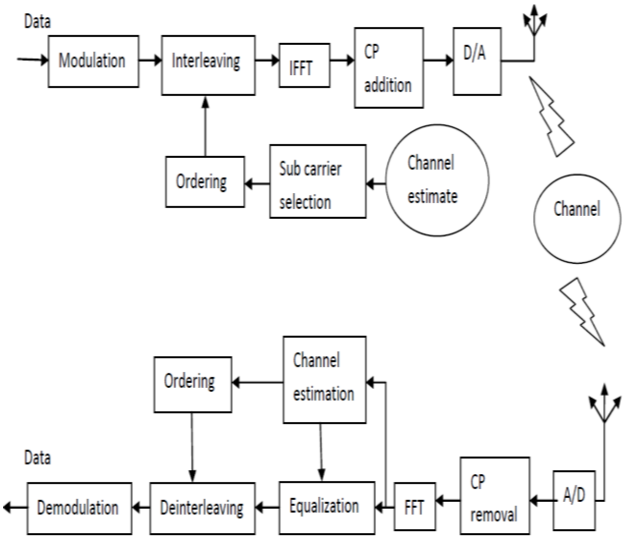

Fig. 2: Block diagram of Secure OFDM system

IV. INTERLEAVED SUBCARRIER SELECTION ALGORITHM

It can be concluded from the performance evaluation that the selection of the interleaved subcarrier subset M impacts both the eavesdropping resilience and transmission reliability of the proposed OFDM system. In the proposed eavesdropping-resilient OFDM system, interleaved subcarriers are selected with constraints Ω and Λ. Ω determines the minimum number of interleaved subcarriers, while Λ determines which subcarriers are going to be inter- leaved. It is noteworthy that when we select the subcarriers according to the constraint Λ, the size of the set of qualified subcarriers, M, may be smaller than Mmin under certain channel condition.

The procedure of the proposed subcarrier selection algorithm can be summarized as follows:

DOI 10.17148/IJARCCE.2016.5188

- All N subcarriers of an OFDM signal are arranged in descending order according to their channel gains.
- The subcarrier with largest channel gain is selected first.
- With the channel gain of the previously selected subcarrier, the estimated noise power and the constraint Λ, the required channel gain difference between the previously selected subcarrier and next subcarrier D
- The subcarrier, which has a channel gain at least smaller by a value of D than that of the previously selected subcarrier while it is closest to the previously selected subcarrier among all the qualified subcarrier is selected.
- Repeat until reaching the end of the order of the N subcarriers.

V. SIMULATION RESULTS

OFDM signals are generated using 64-point IFFT with a cyclic prefix (CP) of length 16. The modulation scheme quadrature phase shift keying is adopted for all subcarriers. Rayleigh fading channels with both uniform and exponential power delay profiles (PDP) are considered in the simulations. The channels are set to be time invariant over several data blocks, so that the transmitter and legitimate receiver are able to have channel estimates of identical channels. In order to make fair comparisons, we assume that the main channel and eavesdropping channel follow an identical statistical model, and that the noise levels at all nodes are the same. The least- square channel estimation technique is employed at all nodes in the network. Meanwhile, perfect synchronization is assumed at both the legitimate receiver and eavesdropper ends.

A. Interleaving permutation mismatch probability

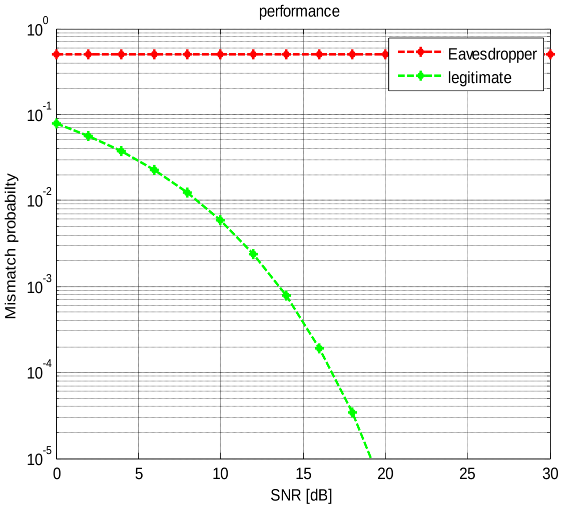

Fig.3: Interleaving permutation mismatch probabilities at the legitimate receiver and eavesdropper ends.

The interleaving permutation mismatch probabilities at both the eavesdropper and legitimate receiver, which essentially deter- mine the security and reliability of the proposed system, are evaluated in Fig. 3. A Rayleigh fading channel with uniform PDP of a delay spread as long as the CP length, i.e. 800 ns in the 802.11g system, is used in the simulations. As shown in the figure, the interleaving permutation mismatch probability at the eavesdropper is always close to 1. In contrast, the interleaving permutation mismatch probability at the legitimate user is lower than $10^{-3}$when SNR is larger than 15 dB. Since the interleaving per- mutation mismatch between legitimate users is mainly caused by channel estimation errors, a channel estimation technique inducing smaller estimation errors can further improve the reliability of the legitimate transmission.

B. Comparison with the CSI based secret key generation scheme.

Similar to the proposed subcarrier interleaving scheme, CSI-based secret key generation schemes also exploit the randomness of wireless channels to protect the transmission. To some extent, the subcarrier interleaving permutation can be treated as a secret key. Therefore, it is interesting to compare the security and reliability achieved by the interleaving permutation and CSI-based secret keys.

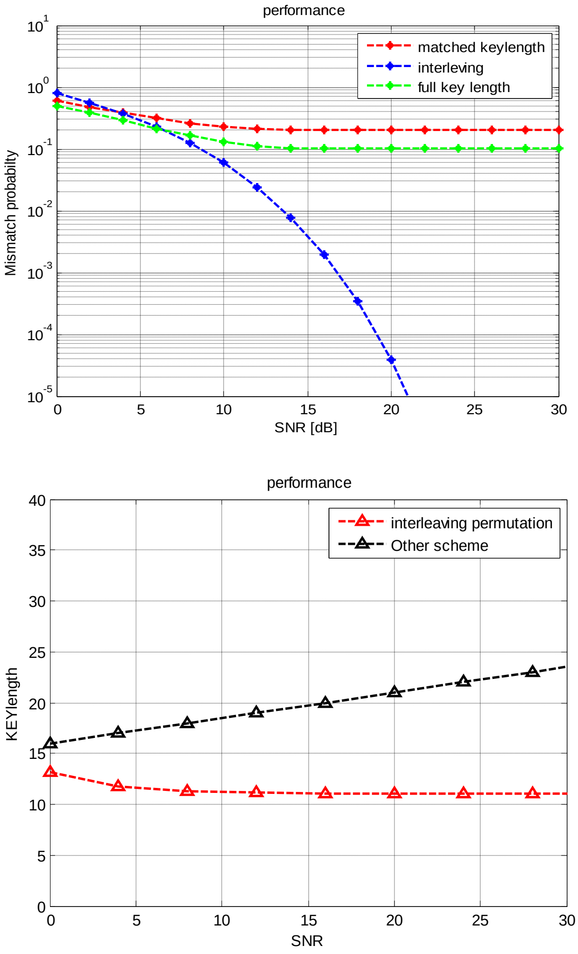

Fig 4: Security and reliability comparison between the proposed interleaving permutation and the key generated [28].

Considering that the interleaving pattern in the proposed system is determined by subcarrier channel gains, typical received signal strength (RSS) based secret key generation

DOI 10.17148/IJARCCE.2016.5188

protocol [28] is adopted for this comparison. In [28], the RSS was compared with two reference thresholds q+ and q−. If RSS is larger than q+, bit 1 is generated; if RSS is smaller than q−, bit 0 is generated. Moreover, a key reconciliation technique was also introduced to mitigate its probability of key mismatch. Please refer to [28] for the detailed design the security of these two schemes is compared in terms of the length of generated “keys”. With M involved subcarriers, the scheme in [28] can generate M bits of secret key, while the proposed subcarrier interleaving permutation can provide a “key” with a length of log2 (M!) bits.

C. Performance of the proposed secure OFDM system.
In the simulations, the performance of the proposed secure OFDM system is evaluated from SERs experienced by the legitimate receiver and eavesdropper. The SER of the conventional OFDM system is provided as a bench-mark reference to assess the transmission reliability of the proposed system. Figure 5 shows the SERs of the proposed and conventional OFDM systems under a Rayleigh fading channel with uniform PDP of 800 ns delay spread. It can be observed from this figure that an eavesdropper always has a SER close to 1 when it utilizes its local channel estimates to intercept signals transmitted from the proposed OFDM system. In contrast, the performance of the legitimate transmission can be almost the same as that of the conventional OFDM system.

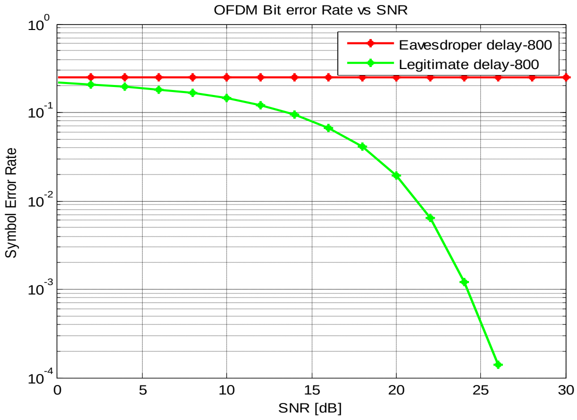

Fig 5: SER Vs SNR under a Rayleigh fading channel with uniform PDP of 800 ns delay spread.

The SER vs. SNR performance of the proposed secure OFDM system under a different channel condition is depicted in Fig. 6, where a Rayleigh fading channel with exponen- tial PDP of 50 ns root-mean-square (RMS) delay spread is considered. This represents a multipath channel with much less scattering in comparison with the one used before. As illustrated in this figure, the eavesdropper still suffers from a very high SER though the SER is slightly less than that observed in Fig. 5. The SER of eavesdropping on the proposed system can be up to 506 times larger than that of eaves- dropping on the conventional OFDM system in this simulated channel condition.
Figure 7 shows that the performance of the BER Vs SNR

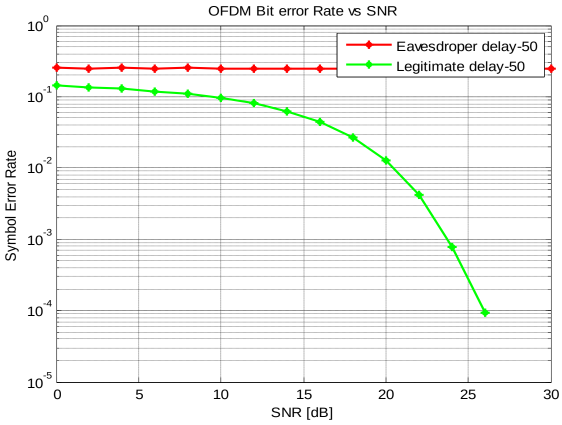

Fig 6: SER Vs SNR under a Rayleigh fading channel with exponential PDP of 50 ns delay spread.

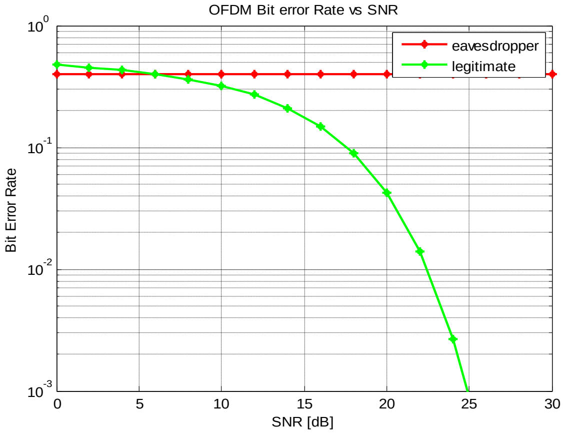

Fig 7: BER Vs SNR

D. Impact of side information ξ on eavesdropping prevention

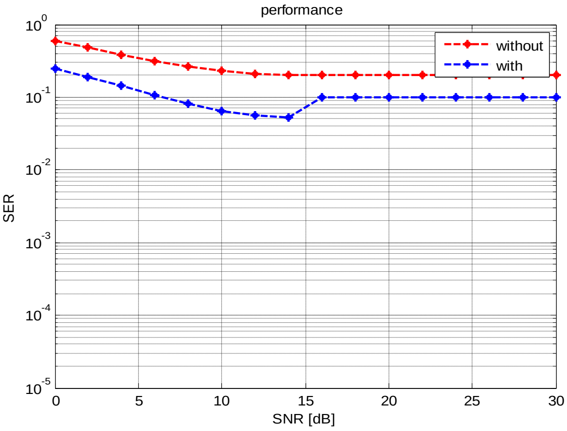

Fig 8: SER comparison for eavesdroppers with and without side information.

In fig 8, eavesdropper without information on ξ does experience higher SERs, compared with the one who knows exactly the interleaved subcarrier selection. Eavesdropping to the proposed system is always difficult. The reason of this phenomenon is that the eavesdropping prevention capability of the proposed system is dominated by the interleaving permutation itself instead of the side information ξ

DOI 10.17148/IJARCCE.2016.5188

E. Capacity of the system.

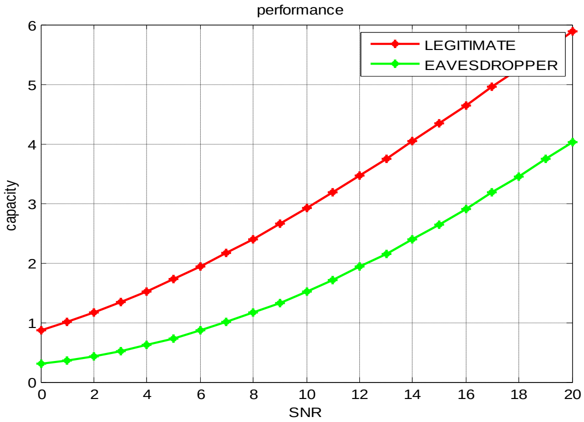

Fig9. Capacity Vs SNR

VI. CONCLUSION

In this paper, propose an interleaved subcarrier selection techniques for avoiding eavesdropping in OFDM system.. Exploiting the CSI between the transmitter and legitimate receiver, some subcarriers of each OFDM signal are selected and then interleaved according to the sorted order of their channel impulse response. Since wireless channels associated with each pair of users at separate locations exhibit independent fading processes, the frequently updated subcarrier interleaving pattern can only be shared between legitimate nodes based on channel reciprocity. Without a proper de-interleaving pattern, mismatched information recovery occurs at the eavesdropper, thus preventing eavesdropping. In order to mitigate the impairments from imperfectly reciprocal channel estimates at legitimate parties, interleaved subcarriers are selected according to a specially developed procedure to achieve a trade-off between the eaves- dropping resilience and transmission reliability. Theoretical analysis and Monte Carlo simulation results have been pro- vided to validate the proposed system. It can be observed from the simulation results that eavesdropping on the proposed system suffers from SER values close to 100% while the legitimate transmission has a SER performance about the same as that of conventional OFDM systems.

REFERENCES

[1] F. Renna, N. Laurenti, and H. V. Poor, “Physical-Layer Secrecy for OFDM Transmissions over Fading Channels,” IEEE Trans. Inf. Forens. Security, vol. 7, no. 4, pp. 1354-1367, Aug. 2012.

[2] K. Ren, H. Su, and Q. Wang, “Secret Key Generation Exploiting Channel Characteristics in Wireless Communications,” IEEE Wireless Commun. vol. 18, no. 4, pp. 6-12, Aug. 2011.

[3] A. D. Wyner, “The Wiretap Channel,” Bell Syst. Tech. Journal, vol. 54, pp. 1355-1387, 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian Wiretap Channel,” IEEE Trans. Inform. Theory, vol. 24, no. 4, pp. 451-456, Jul. 1978.

[5] M. Bloch, et al., “Wireless Information-Theoretic Security,” IEEE Trans. Inform. Theory, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[6] P. Gopala, L. Lai, and H. E. Gamal, “On the Secrecy Capacity of Fading Channels,” IEEE Trans. Inform. Theory, vol. 54, no. 10, pp. 4687-5698, Oct. 2008.

[7] R. Zhang, L. Song, Z. Han, and B. Jiao, “Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers,” IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3693-3704, Oct. 2012

[8] S. Goel and R. Negi, “Guaranteeing Secrecy Using Artificial Noise,” IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[9] H. M. Wang, Q. Yin, and X. G. Xia, “Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks,” IEEE Trans. Signal Process., vol. 60, no. 7, pp. 3532-3545, Jul. 2012.

[10] Z. Gao, Y. H. Yang, and K. J. R. Liu, “Anti-Eavesdropping Space-Time Network Coding for Cooperative Communications,” IEEE Trans. Wireless Commun., vol. 10, no. 11, pp. 3898-3908, Nov. 2011.

[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[12] Y. Zou, X. Wang, and W. Shen, “Optimal Relay Selection for Physical- Layer Security in Cooperative Wireless Networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[13] D. W. K. Ng, E. S. Lo, and R. Schober, “Energy-Efficient Resource Allocation for Secure OFDMA Systems,” IEEE Trans. Veh. Technol., vol. 61, no. 6, pp. 2572-2585, Jul. 2012.

[14] H. Qin, et al., “Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2717-2729, Jun. 2013.

[15] A. Chorti and H. V. Poor, “Faster than Nyquist Inference Assisted Secret Communication for OFDM Systems,” in Proc. IEEE Asilomar Conf. Signals, Systems and Comput., 2011, pp. 183-187.

[16] W.-J. Lin and J.-C. Yen, “An Integrating Channel Coding and Cryptography Design for OFDM based WLANs,” in Proc. IEEE Int. Symp. Consum. Electron., 2009, pp. 657-660.

[17] R. Ma, L. Dai, Z. Wang, and J. Wang, “Secure Communication in TDS- OFDM System Using Constellation Rotation and Noise Insertion,” IEEE Trans. Consum. Electron. vol. 56, no. 3, pp. 1328-1332, Aug. 2010.

[18] H. Li, X. Wang, and Y. Zou, “Dynamic Subcarrier Coordinate Interleav- ing for Eavesdropping Prevention in OFDM Systems,” IEEE Commun. Lett., vol. 18, no. 6, pp. 1059-1062, Jun. 2014.

[19] W. Y. Zou and Y. Wu, “COFDM: An Overview,” IEEE Trans. Broad- cast, vol. 41, no. 1, pp. 1-8, Mar. 1995.

[20] S.-W. Lei and V. K. N. Lau, “Performance Analysis of Adaptive Interleaving for OFDM Systems,” IEEE Trans. Vel. Technol., vol. 51, no. 3, pp. 435-444, May 2002.

[21] A. Filippi and E. Costa, “Low-Complexity Interleaved Subcarrier Allo- cation in Multicarrier Multiple-Access Systems,” IEEE Trans Commun., vol. 55, no. 1, pp. 35- 39, Jan. 2007.

[22] S. Mathur et al., “Exploiting the Physical Layer for Enhanced Security,” IEEE Wireless Commun. vol. 17, no. 5, pp. 63-70, Oct. 2010.

[23] M. K. Ozdemir and H. Arslan, “Channel Estimation for Wireless OFDM Systems,” IEEE Commun. Surv. Tut. vol. 9, no. 2, pp.18-48, 2007.

[24] United States Computer Emergency Readiness Team (2012, Jan. 06). Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack [Online].

[25] Available: http://www.us-cert.gov/ncas/alerts/TA12-006A [25] H. A. David, “Order Statistics,” New York: Wiley, 1981.

[26] [26] M. K. Simon and M.-S. Alouini, “On the Difference of Two Chi- Square Variates with Application to Outage Probability Computation,” IEEE Trans. Commun., vol. 49, no. 11, pp. 1946-1954, Nov. 2001.

[27] [27] IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE standard 802.11, 2012.

[28] [28] S. Mathur, et al., “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel,” in Proc. ACM Int. Conf. Mobile Computing and Networking, Sept. 2008, pp. 12139.

BIOGRAPHY

Miss Steffi Jose is a student of M.Tech (second year) communication engineering, Department of Electronics & Communication Engineering at Mount Zion College of Engineering and Technology Kadammanitta Kerala. She completed BE in Mar Ephraem College of Engineering and technology Tamilnadu. This is her second paper published here .Her area of interest is Secure communication.

DOI 10.17148/IJARCCE.2016.5188