International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Threshold Based Subcarrier Interleaving for Spy Works Prevention in OFDM Systems

Faizy Fazal[1], Angel Mary Mathew[2]

[1]M.Tech Student, Department of Communication Engineering,
Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

Abstract: ***OFDM (orthogonal frequency division multiplexing) systems are widely employed in Wireless Communication. but unfortunately they are susceptible overhearing by SPY(intruder). In this paper an anti-spy OFDM system through threshold based on dynamic subcarrier co-ordinate interleaving (coordinate interleaving) is proposed. Here some of the OFDM subcarriers perform interleaving in an opportunistic manner at the transmitter. But the secret interleaving is determined by instantaneous channel state information (CSI) between transmitter and actual receiver. here a subcarrier symbol whose channel phase estimate is larger than a predefined threshold is co-ordinate interleaved. Consequently spy works are prevented due to mismatched de-interleaving in the spy(EAVESDROPPER).***

Keywords: OFDM, Eavesdropping Prevention, Dynamic Co-Ordinate Interleaving

1. Introduction

Communication security is a serious subject and is handled by well trained and experts. OFDM is a modulation format that finds increasing level of use in Today's radio communication scene. OFDM has been adopted In Wi-Fi, Where the 802.11a standard use it to provide data rates up to 5 Mbps in 5Ghz ISM (Industrial, Scientific, Medical) band.

In addition to this, it is used for WIMAX and it is also the format of choice for the next generation cellular radio communication system including 3G,LTE(LONG Term Evolution).OFDM is rather different format for modulation that used for more traditional format of transmission. It utilizes many carriers together to provide many advantages over simple modulation formats.

An OFDM signal consists of a number of closely spaced modulated carriers. When modulation of any forms voice, data etc are applied to a carrier. Then sidebands spreads out either side, it is necessary for a receiver to be able to successfully demodulate the data. As a result when signals are transmitted close to one another, they must be spaced so that receiver can separate them using a filter.

Unfortunately these OFDM systems are vulnerable to malicious Eavesdropping. In this paper sub carrier co-ordinate interleaving id done at the transmitter and the corresponding de-interleaving is done at the receiver and the proposed method reduces the information leakage to the eavesdropper (intruder or spy).

2. Motivation and Related Works

Information theoretic secrecy rate [1]considers that an achievable by an OFDM Transmitter/Receiver pair in the presence of an eavesdropper that might either use an OFDM structure or choose a more complex receive structure. The analysis is made possible by modeling a system as a particular instance of a high dimensional multiple-input multiple-output wiretap channel.

The secrecy loss[2]due to the OFDM structure constraint and the information gain for an eavesdropper that use a more complex receiver are considered. Providing physical-layer security for mobile users in future broad band wireless networks is of theoretical and practical importance.

The use of artificial noise for secure communication [5] is considered. Here propose the notion of practical secrecy as a new design criteria based on the behavior of the eavesdroppers error probability as the signal-to-noise ratio goes to infinity. Then show that the practical secrecy can be guaranteed by the randomly distributed artificial noise with specified power. The all previous studies only adopted the way to reduce the error rate not the eavesdropping prevention. So in this proposed scheme adopt a method to prevent the spy works by dynamic channel co-ordinate interleaving.

3. System Model

3.1 OFDM Concept

An OFDM signal consists of a number of closely spaced modulated carriers. When modulation of any form voice, data, etc. when side bands from each carrier overlap, they can still be received without the interference that might be expected because they are orthogonal to each other. this is achieved by having the carrier spacing equal to the reciprocal of the symbol period. to see how OFDM work it is necessary to look at the receiver.

The data to be transmitted on an OFDM signal is spread across the carriers taking part of the payload. This reduces the data rate taken by each carrier the lower data rate has the advantage that interference from reflections is much critical. This is achieved by adding a guard band time or guard interval into the system. This ensures that the data is only sampled when the signal is stable and no new delayed signals arrive that would alter the timing and phase of the signal.

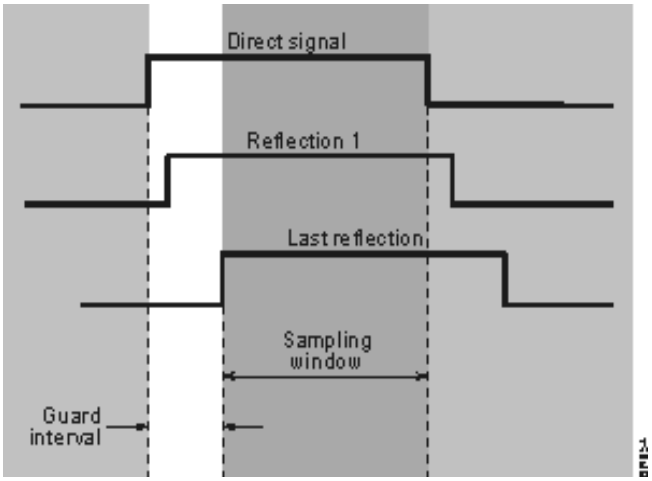

Figure 1: Guard Interval

3.2 Proposed Frame Work

We are considering here a OFDM system with three nodes that a transmitter communicates with actual receiver in the presence of a passive eavesdropper. The eavesdropper know the security protocol of the transmission and they can demodulate OFDM signals but they cannot wiretap information like channel phase estimation in users forward and reverse channel carrying same frequency in several time slots. So based on channel reciprocity transmitter and the corresponding receiver has identical main channel. But here assumed that the eavesdropper channel and the main channel are spatially located at a difference more than half a wavelength. It means that main channel and eaves dropper channel are independent of each other.

3.3 Multi Path Channels in OFDM

Assume that OFDM signals with N subcarriers are transmitted by the transmitter. At the corresponding receiver, the frequency domain received signal after removing cyclic prefix is

$$R = diag\{H\}^N S + W \quad (1)$$

H is a diagonal N by N matrix, identifies the complex frequency domain and channel response of the main channel. S is an N by 1 vector denote modulated symbols transmitted by N subcarriers which are mapped into a two dimensional constellation and vector W size N by 1 vector indicates the Gaussian noise, Throughout the analysis we approximate N subcarrier channel as independent and identically distributed variable. in the eavesdropper channel same modeling and approximation can be applied.

3.4 Channel Estimates In The Network

Estimation error generally occurs in the channel estimators due to the presence of noise, interference and hardware limitations. As a result only noisy channel estimators can be obtained by all nodes in the network. The observation of main channel at between the transmitter and the receiver is

$$\left|\hat{H}_{T/R}(k)\right| e^{j\hat{\theta}_{T/R}(k)} = \left|H(k)\right| e^{j\theta(k)} + \left|\Delta H_{T/R}(k)\right| e^{j\Delta\theta_{T/R}(k} \quad (2)$$

Where the subscripts T and R are for transmitter and receiver, second term is the actual phase and the third term is the phase estimate.

4. OFDM with Co-ordinate Interleaving

In the proposed OFDM system a subcarrier set M with M out of N subcarriers in each OFDM signal is involved in the dynamic subcarrier co-ordinate interleaving, where the symbol co-ordinate at a subcarrier is determined by instantaneous subcarrier channel state information. In this paper a channel phase interleaving pattern generation scheme is adopted as an example to demonstrate how the dynamic co-ordinate interleaving well prevent eavesdropping.

4.1 Transmitter End

At the transmitter end the instantaneous channel phase of each subcarrier belonging to set M in an OFDM signal compared with a properly selected threshold. if the channel phase of a subcarrier is greater than the predefined threshold the real and imaginary components of the symbol at the subcarrier is interleaved. Otherwise the modulated symbol at the subcarrier is transmitted in the original format.the other processing of transmitter is same as that of conventional OFDM transmitter. Mathematically the channel phase based co-ordinate interleaving can be written as

$$\begin{cases} \hat{\theta}_T(k) > \Lambda T, \text{int}\, erleaving \\ \hat{\theta}_T(k) \le \Lambda T, un - \text{int}\, erleaving \end{cases}, K \in \text{M} \quad (3)$$

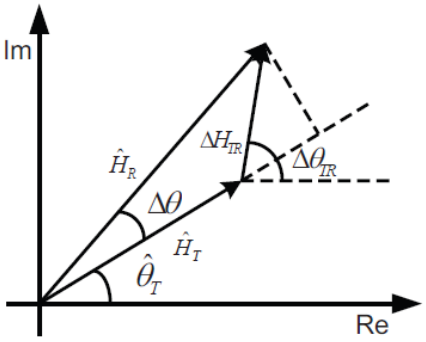

Figure 2: Channel phase estimate derivation

4.2 Receiver End

Receiver End in the proposed OFDM system as compared with a conventional receiver the only difference in this system is that co-ordinate de-interleaving is carried out at the subcarriers in set M after the symbol demodulation. The receiver would locally determine the interleaving pattern by comparing with a predefined threshold.

4.3 Symbol Error Rate Of Eavesdropping

Since the eavesdropper at the third location feels a multipath channel independent of the main channel, the subcarrier channel phase estimate at the eavesdropper is uncorrelated with that of transmitter. So eavesdropper can make only random guess of the time varying co-ordinate interleaving pattern initiated by the transmitter. When M subcarriers that are involved in opportunistic interleaving, the probability that the eavesdropper obtain mismatched interleaving is calculated as

$$P_E = 1 - \frac{1}{2^M} \quad (4)$$

The ser of eavesdropper in the proposed system as

$$P_{S,E} = 1 - (1 - P_E)(1 - P_S) \quad (5)$$

4.4 Information Leakage at the Eavesdropper

In the proposed system the bit error rate (BER) of eavesdropping at each subcarrier as

$$p_k = \begin{cases} \frac{1 - 1/2(1 - P_s)}{\alpha}, k \in M \\ \frac{P_s}{\alpha}, k \notin M \end{cases} \quad (6)$$

Where alpha denotes the number of bits per symbol at the subcarrier. Assuming that each transmitted bit has equal probability of being 0 and 1.then information leakage in terms of mutual information can be derived as

$$L_{OFDM} = \frac{1}{N} \sum_{k-0}^{N-1} I_k (Y_E ; X) \quad (7)$$

5. Simulation Results

In order to make a fair comparison, the statistical model of the main channel and eavesdropping channel, as well as the noise power levels at all nodes are set to be the same. The SER of the proposed anti-eavesdropping OFDM system is shown in Fig.3.the proposed anti eavesdropping can prevent eavesdropping at the same time provide a reliable correct transmission. As the performance loss of the correct transmission is mainly caused by channel estimation errors, more reliable channel estimates can further improve the transmission reliability.

The information leakage at the eavesdropper is shown in Fig.4.the proposed system can significantly decrease the information leakage at the eavesdropper. Especially when more subcarriers in an OFDM signal are involved in dynamic co-ordinate interleaving. Please note that the information leakage of the proposed system mainly comes from subcarriers that are not involved in co-ordinate interleaving. More specifically, the transmitter performs co-ordinate interleaving at subcarriers with channel phase larger than a predefined threshold. Since wireless channels associated with each pair of users at separate location exhibit independent propagation characteristics. The frequently updated co-ordinate interleaving pattern is only shared between actual users based on channel reciprocity. Without a matched co-ordinate interleaving pattern erroneous information recovery is carried out at the eavesdropper so that eavesdropping is prevented. Theoretical analysis and simulation results have been provided to validate the proposed system.

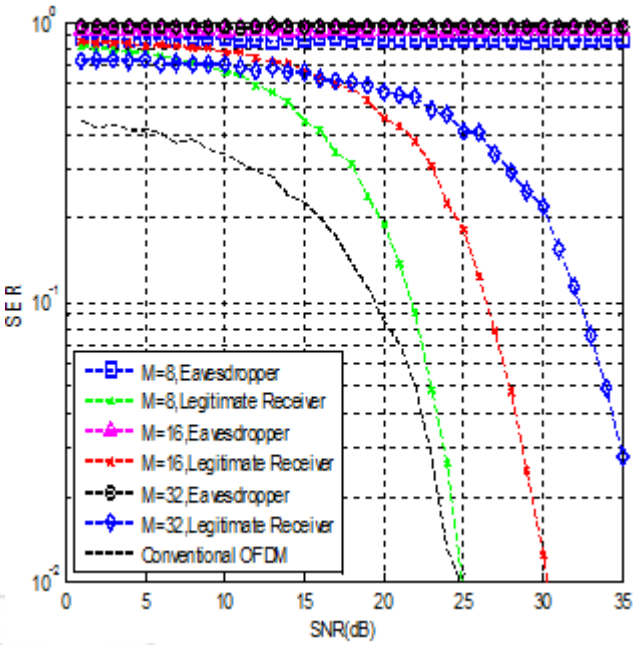

Figure 3: SER comparison between the proposed anti eavesdropping and conventional OFDM

This simulation is done using MATLAB. To find the comparison between the conventional OFDM and proposed OFDM QAM modulation with choices that M=8, M=16 and M=32 for correct receiver and the eavesdropper is plotted. From the Fig 3 we could analyze that, Anti eavesdropping method that we proposed has high SNR and low SER.As the value of M increases the symbol error rate decreases and the signal-to-noise ratio increase

In the Fig.4 the amount of information that is overheard by the spy is calculated using (7) and it is plotted for different values of M. this is referred to as information leakage at the eavesdropper or spy or intruder. Information leakage for conventional OFDM and proposed anti-eavesdropping is plotted. By analyzing we could found that information leakage in proposed system is low compared to the conventional system.

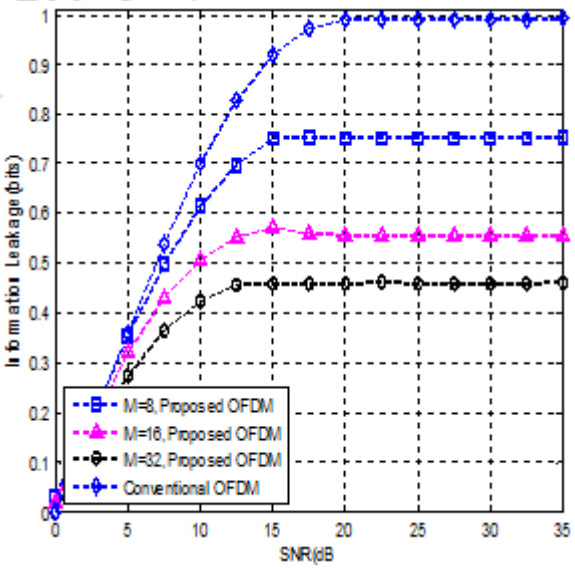

Figure 4: Information leakage at the eavesdropper

6. Conclusion

This method explained in the paper proposed an anti eavesdropping strategy in OFDM systems through dynamic subcarrier co-ordinate interleaving. Symbol co-ordinates subcarriers in an opportunistic manner depending on CSI between transmitter and receiver. more specifically, the transmitter performs co-ordinate interleaving if its channel phase estimate is greater than predefined threshold. Since wireless channels associated with each pair of users at the separate location exhibit independent propagation characteristics, the frequently updated co-ordinate interleaving pattern is only shared between actual users based on channel reciprocity. Without a matched co-ordinate de-interleaving pattern, erroneous information recovery is carried out at the eavesdropper so that eavesdropping is prevented, this paper can be extended to find the SNR and SER in different leakage region.

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] Chorti and H. V. Poor, "Faster than Nyquist Interference Assisted Secret Communication for OFDM Systems," in Proc. IEEE Asilomar Conf. Signals, Systems and Comput., 2011, pp. 183-187. ed. Englewood Cliffs, NJ, USA: Prentice Hall, 2005.
[3] X. Wang, et al., "Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks considering the rate capacity," IEEE Trans. Inf. Forens. Security, vol. 6, no. 3, pp. 693-702, Sept. 2011.
[4] 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.
[5] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008
[6] Z. Ding, et al., "On the Application of Cooperative Transmission to Secrecy Communications," IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359-368, Feb. 2012
[7] J. Boutros and E. Viterbo, "Signal Space Diversity: A Power and Bandwidth-Efficient Diversity Technique for Rayleigh Fading Channel," IEEE Trans. Inform. Theory, vol. 44, no. 4, pp. 1453-1467, Jul. 1998
[8] C. Yoon, H. Lee, and J. Kang, "Performance Evaluation of Space- Time Block Codes from Coordinate Interleaved Orthogonal Designs in Shadowed Fading Channels," IEEE Trans. Veh. Technol., vol. 60, no. 3, pp. 1289-1295, Mar. 2011
[9] J. Harshan and B. S. Rajan, "Co-ordinate Interleaved Distributed Space- Time Coding for Two-Antenna-Relays Networks," IEEE Trans. Wireless Commun.,. vol. 8, no. 4, pp. 1783-1791, Apr. 2009
[10] Y. E. H. Shehadeh, O. Alfandi, and D. Hogrefe,. Towards Robust Key Extraction from Multipath Wireless Channels," IEEE J. Commun. Netw., vol. 14, no. 4, pp. 385-394, Aug. 2012.

Author Profile

Faizy Fazal: received the B.Tech degrees in Electronics and Communication Engineering from M.G University, Kerala at Musaliar College of Engineering in 2013. And now she is pursuing her M.Tech degree in Communication Engineering under the same university in Mount Zion College of Engineering.

Angel Mary Mathew: received the B.Tech degrees in Electronics and Communication Engineering from kerala University, Kerala at Baselios Mathwes College of Engineering in 2012. And now she is pursuing her M.Tech degree in Communication Engineering under M.G University in Mount Zion College of Engineering.