# Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 218-225, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.218.225
© 2013 Academic Journals Inc.

# Hash Encrypted Synchronized OFDM

N.R. Raajan, A. Jenifer Philomina, M. Ramkumar, G.N. Jayabhavani and C. Nishanthini
School of Electrical and Electronics Engineering SASTRA University, India

*Corresponding Author: N.R. Raajan, School of Electrical and Electronics Engineering SASTRA University, India*

## ABSTRACT

High data rate and vulnerable are major challenges faced by present wireless communication systems since the demand for the internet and multimedia services are rapidly increasing and also the multimedia information are more secured in wired environment than in wireless environment. Orthogonal Frequency Division Multiplexing (OFDM) has been considered as a hopeful technique for to achieve high data rate transmission, it also has many advantages like spectral efficiency, robust to multipath fading effect, easy hardware implementation etc. Though OFDM has many advantages, it is highly sensitive to synchronization error. Since the error rate is increased and the system performance is degraded due to synchronization error, it seems to be a major problem in OFDM. An Inter-Symbol Pilot Aided Algorithm is used to overcome this problem which estimate and compensate the synchronization error. In this study, the data is secured using Hash Encryption Algorithm which introduces authentication and encryption in OFDM system, without impairing its spectral efficiency. In this study, an OFDM system is designed with improved security and synchronization which increases the overall efficiency of the system.

**Key words:** OFDM, Hash algorithm, synchronization error, inter-symbol pilot

## INTRODUCTION

OFDM is a multicarrier modulation technique that has increasing levels in present radio communication. Wi-Fi arena adopts OFDM, 802.11a IEEE standard uses OFDM to provide 54 Mbps data rate in 5 GHz ISM (Industrial, Scientific and Medical) band. OFDM is used in WiMAX and it is also the format of choice for the next generation Mobile communication system including LTE (Long Term Evolution). It is also proposed as the modulation technique for the future 4G cellular system.

In OFDM the allocated bandwidth is split into N narrow band sub-channels are mapped with symbol and then all the N channels are frequency multiplexed. In fading environment only a portion of the data is destroyed thus the receiver able to retrieve it using forward error correction coding technique. The sub-channels are made orthogonal to each other by having carrier spacing reciprocal to the symbol period. Due to its orthogonality property it allows overlapping of sub-channels which leads to good spectral efficiency.

However, OFDM has advantages like spectrally efficient and robustness to fading effect, the synchronization error decreases the overall system performance. The cause for this synchronization error is offsets such as Carrier Frequency Offset (CFO) or frequency offset and Sampling Clock Offset (SCO) which destroys the orthogonality. In OFDM Cyclic Prefix and Guard Band are used to protect the symbols from ICI (Inter Carrier Interference) and ISI (Inter Symbol Interference).

But the loss of orthogonality due to offset leads to ISI and ICI. For to improve the performance of the system both these CFO and SCO should be estimated for proper OFDM synchronization.

The multimedia information is not secured in the wireless environment, thus there is a need to encrypt the information before transmitting over wireless medium and the decryption is carried out in the receiver to recover the original information.

Generally hash algorithm is used for mapping keys (large data sets of variable length), to a smaller data sets of fixed length. Hash function is generally given as:

$$h:\{0, 1\}^{*}\rightarrow\{0, 1\}^{m}$$

As shown in the above equation a set of binary strings are mapped into a set of binary strings of a fixed size. In hash function two different inputs are unlikely mapped to the same value (Qin and Chen, 2012).

In this study, the information is hashed and given to OFDM process for data security and in the receiver side reverse process is carried for obtaining the original data (Fu *et al*., 2009). Custom-designed widely used Message Digest Algorithm-5 (MD5) hash algorithms is used for hashing the data.

The OFDM system is synchronization using Inter Symbol Pilot Aided Algorithm. In this algorithm the difference in phase is calculated between the pilots of same OFDM symbol, from which CFO and SCO can be estimated. The estimated values are compensated. Thus both security and synchronization can be achieved in OFDM system (Raajan *et al*., 2012a).

**OFDM**

OFDM is a multicarrier modulation technique that has increasing levels in present radio communication. Wi-Fi arena adopts OFDM, 802.11a IEEE standard uses OFDM to provide 54 Mbps data rate in 5 GHz ISM (Industrial, Scientific and Medical) band. OFDM is used in WiMAX and it is also the format of choice for the next generation Mobile communication system including LTE (Long Term Evolution). It is also proposed as the modulation technique for the future 4G cellular system.

In OFDM the allocated bandwidth is split into N narrow band sub-channels are mapped with symbol and then all the N channels are frequency multiplexed. In fading environment only a portion of the data is destroyed thus the receiver able to retrieve it using forward error correction coding technique.

**Message digest algorithm-5:** In this a arbitrary length message is takes as input and a message digest is produced with 128-bit output (Rabah, 2005).

Let the input message be M of length b bits. Pad the input message M to a multiple of 512 bits and divided to blocks of 512 bits. Let each block $M_0, \ldots, M_{N-1}$ consists of 16 words (Tahir *et al*., 2010). Sixteen operations takes place in a single round, totally there will be 4 rounds for all the blocks.

The step by step process of MD5 algorithm is explained as follows:

- **Padding:** At the end of the message append a single bit '1'. Then append '0' bit till the produced message length is similar to 448 modulo 512. Thus the original message 'b' can be appended as a 64-bit representation. Thus finally a multiple of 512 bit message is obtained

- **Buffer initialization:** Initialize the buffer to the hex values (The least significant bit should be listed first)
- A 64 element table has been computed using the sine function based on the formula $k_t = \lfloor \underline{2^{32}}.\lfloor \sin(t+1) \rfloor \rfloor$ for t = 0,... , 63 where t in radiance
- **Auxiliary functions:** It has four auxiliary functions, each takes three words of 32-bit as input and a single 32-bit word is produced as output. They are defined as follows:

$$f_t(B,C,D) = (B \wedge C) \vee (\neg B \wedge D) \text{for}, t = 0,...,15$$

$$f_t(B,C,D) = (B \wedge D) \vee (C \wedge \neg D) \text{for}, t = 16,...,31$$

$$f_t(B,C,D) = (B \oplus C \oplus D) \text{for}, t = 32,...,47$$

$$f_t(B,C,D) = C \oplus (B \vee \neg D) \text{for}, t = 48,...,63$$

where, $\oplus$, $\vee$, ?, $\neg$ denotes the XOR and, OR and NOT operations, respectively.

- **Message process in 16-word blocks:** Message in each 16-word block is processed as follows, for i= 0, ., n-1

  - The input message is divided into words as shown, where 'Wo' is the left most word $M_i \rightarrow W_o,\ldots, W_{15}$
  - Then the initialized buffer are saved as $\bar{A} = A$, $\bar{B} = B$, $\bar{C} = C$, $\bar{D} = D$
  - The process done for t = 0, . . . , 63 is:

$$X = B + ((A + f_t(B,C,D)) + W_{jt} + k_t) <<< S_t$$

$$A = D, D = C, C = B, B = X$$

  - All the above steps are carried as a loop for all the 16 word blocks i.e., the loop on t ends
  - Finally the registers A, B, C and D are incremented by the same value which it had initially:

$$A = \bar{A} + A$$

$$B = \bar{B} + B$$

$$C = \bar{C} + C$$

$$C = \bar{D} + D$$

  - With this the loop on i ends
- The resultant values in A, B, C, D gives the final message digest output

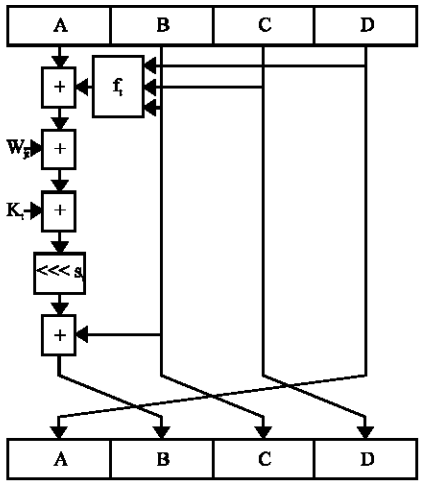


Fig. 1: One MD5 operation

MD5 algorithm uses 128-bit state for its operation and divided into 32-bit words. Initialized the four 32 bit to fixed constants. The algorithm operates on message block of 512-bit. Message block process has four similar stages and each has 16 similar stage of operations based on F (F indicates non-linear function (Tan and Sun, 2011).

Figure 1 shows the one operation of MD5. A single MD5 process contains 64 operations, each having four rounds, each round of 16 operations. And the function F, is used in each round. The message input block of 32-bit are denotes as Mi. The 32-bit constant is denoted by Ki and it is unlike for every operation. The left bit rotation is denotes by <<< s and varies for each and every operation.

## INTER-SYMBOL PILOT AIDED SYNCHRONIZATION

Time and frequency has to be synchronized for a better OFDM system performance. Here the joint estimation of CFO and SCO is done by using Inter-Symbol Pilot Aided Synchronization Algorithm. The phase difference can be calculated for two successive OFDM symbols but channel noise is increased in this case which increases the error rate (Salari *et al.*, 2008). The below equation gives the phase difference among two successive OFDM signals:

$$\theta_j = <(d_i, \alpha_j, d_{i-1}, \alpha_j)$$

where, $\theta_j$ is the difference in phase and $d_j$ is the demodulated OFDM samples.

To increase the performance and to reduce the error the difference in phase is calculated for the pilots of same OFDM symbol from which CFO and SCO can be estimated:

$$\theta_j <(d_i, \alpha_j, \alpha^*_j)$$

where, $\theta_j$ gives the difference in phase for the OFDM pilots of the same symbol for better performance. After the phase estimated the phase offset is derived as:

$$\theta_j = 2\pi \frac{N + N_g}{N}\left(E_{\alpha j} + f_c T_s\right)\delta + e_j$$

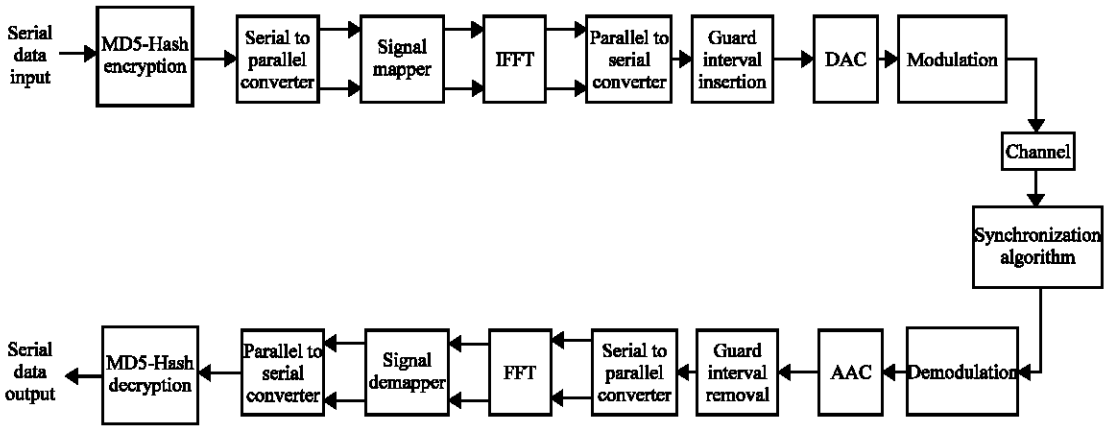


Fig. 2: Block diagram of Hash encrypted synchronized OFDM transceiver

The estimated CFO and SCO using inter symbol pilot aided algorithm is given as follows:

$$\hat{\delta} = \frac{\sum_{j=0}^{J-1} W_j \theta_j (E\alpha_j + f_c T)}{(2\pi \frac{N + N_g}{N}) \sum_{j=0}^{J-1} W_j (E\alpha_j + f_c T)}$$

The advantage of estimating phase difference is, the phase shift due to carrier frequency offset is identical for all the subcarriers if the ICI is ignored. In case of timing offset the phase shift due to SCO is proportional to the symbol index. Thus by estimating the phase difference both SCO and CFO can be estimated. The estimated values are compensated using interpolation and Inverse Carrier Frequency Offset (Raajan *et al*., 2012b).

## HASH ENCRYPTED SYNCHRONIZED OFDM

Figure 2 shows the block diagram for hash encrypted synchronized OFDM. The following algorithm gives the step by step process for obtaining the secured and synchronized OFDM.

**Algorithm:**

| | | |
|---|---|---|
| **Step 1** | : | Generate random data |
| **Step 2** | : | Spread the data using MD5 Hash encryption algorithm |
| **Step 3** | : | Convert the serial data stream into parallel data stream |
| **Step 4** | : | Select the orthogonal subcarriers. |
| **Step 5** | : | The symbol time waveform is found using IFFT |
| **Step 6** | : | Then all the symbol time waveforms are added by a Guard Interval (GI) |
| **Step 7** | : | The signal is transmitted through AWGN channel |
| **Step 8** | : | The timing and frequency offsets are estimated using inter symbol pilot aided algorithm |
| **Step 9** | : | The offsets are compensated. |
| **Step 10** | : | From the received OFDM signal the GI removed |
| **Step 11** | : | The carriers are extracted using FFT |
| **Step 12** | : | Convert parallel data stream into serial data stream |
| **Step 13** | : | The data is decrypted using Hash decrypted algorithm |
| **Step 14** | : | Thus the original data is obtained |

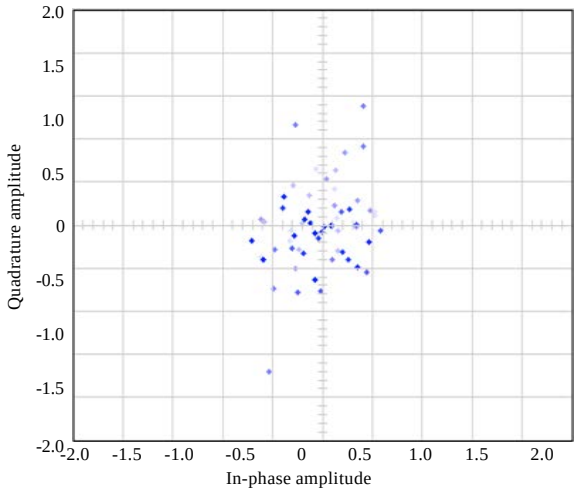


Fig. 3: Unsynchronized OFDM demodulated output

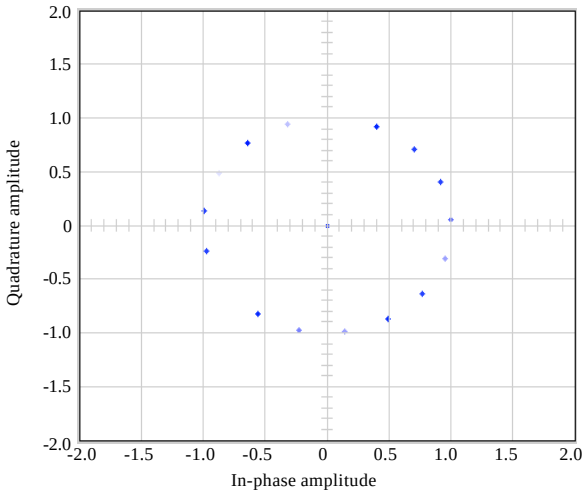


Fig. 4: Synchronized OFDM demodulated output using inter-symbol pilot aided synchronization

11-K bit embedding of D2 and D1 derived from PVD is done in both GREEN and BLUE channels simultaneously.

## RESULTS

Using MATLAB simulation work, the following results are obtained for Hash encrypted synchronized OFDM. Figure 3 gives unsynchronized OFDM demodulated output. Figure 4 shows the synchronized OFDM demodulated output using inter-symbol pilot aided synchronization the scatter plot shows the offset reduced using this algorithm. The unsecured OFDM transmitter spectrum is shown in Fig. 5 and 6 shows the MD5 Hash encrypted OFDM spectrum.

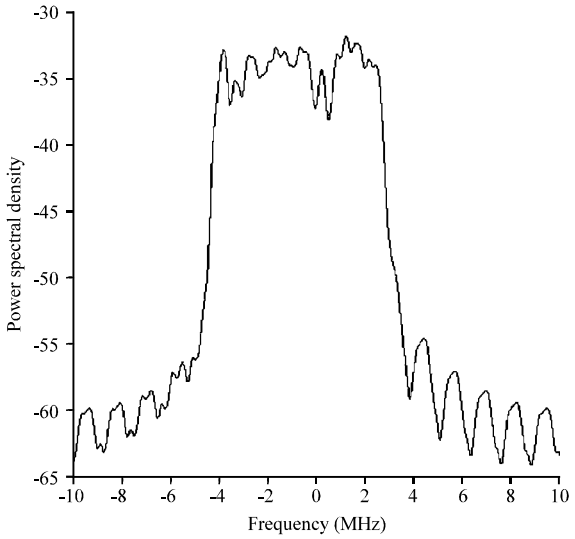


Fig. 5: OFDM transmitter spectrum before Hash encryption

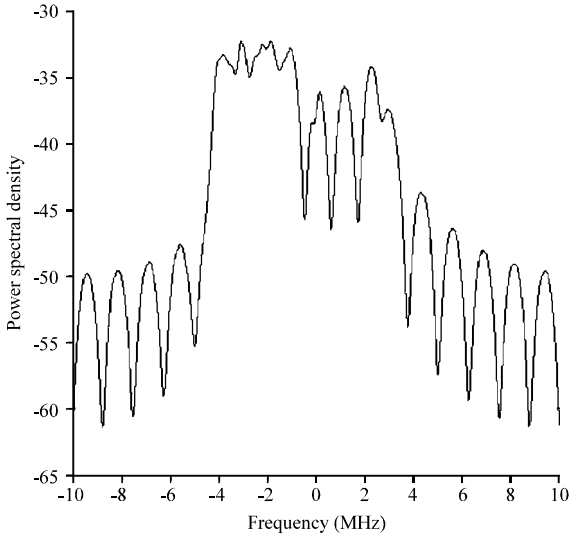


Fig. 6: MD5-Hash encrypted OFDM transmitter spectrum

## CONCLUSION

The obtained results show that the OFDM spectrum is encrypted. Thus by using MD5 Hash Encryption, the data is encrypted which increase the security of the OFDM system. In the receiver section the data is decrypted and the original signal is obtained. Using Inter Symbol Pilot aided algorithm the offset values are close approximately estimated and compensated this results in synchronized OFDM with reduced BER. Thus a secured and synchronized OFDM system is obtained which increases the overall efficiency of the system.

## REFERENCES

Fu, Y., X. Wang and S. Li, 2009. Distributed index based on geographic hashing table for mobile Ad hoc networks. Inform. Technol. J., 8: 1197-1204.

Qin, T. and H. Chen, 2012. An enhanced scheme against node capture attack using hash-chain for wireless sensor networks. Inform. Technol. J., 11: 102-109.

Raajan, N.R., A.J. Philomina, M.V. Priya, B. Monisha and S. Suganya *et al*., 2012a. Improved OFDM system using inter symbol pilot aided synchronization in asynchronous mode of transmission. Proceedings of the 2nd International Conference on Advances in Engineering Science and Management, March 30-31, 2012, Nagapattinam, Tamil Nadu, India, pp: 658-662.

Raajan, N.R., B. Monisha, N. Rangarajan and R. Vishnupriya, 2012b. Secured OHWDM using Fractals. Proceedings of the International Conference on Modeling Optimization and Computing-(ICMOC-2012), April 10-11, 2012, TamilNadu, India, Article in Press.

Rabah, K., 2005. Secure implementation of message digest, authentication and digital signature. Inform. Technol. J., 4: 204-221.

Salari, S., M. Ardebilipour and M. Ahmadian, 2008. Channel and frequency offset estimation for MIMO-OFDM systems. J. Applied Sci., 8: 809-815.

Tahir, M., S.P.W. Jarot and M.U. Siddiqi, 2010. Wireless physical layer security using Encryption and channel precompensation. Proceedings of the International Conference on Computer Applications and Industrial Electronics (ICCAIE), December 8-10, 2010, Kuala Lumpur, Malaysia, pp: 304-pp: 304.

Tan, L. and X. Sun, 2011. Robust text hashing for content-based document authentication. Inform. Technol. J., 10: 1608-1613.