Performance Analysis of Hash Encrypted DWT-OFDM and Hash Encrypted FFT-OFDM Systems

N.R.Raajan, Abinaya,E, Elavarasi,M
Department of Electronics and Communication Engineering
School of Electrical and Electronics Engineering
SASTRA University
Thanjavur, Tamilnadu, India
nrraajan@ece.sastra.edu,

Abstract— **Orthogonal Frequency Division Multiplexing (OFDM), in the recent past is being preferably used in wireless communication because of its high data rate and its unique property of the transmitted symbols being mathematically orthogonal. This mathematical orthogonality allows signals with different frequencies to propagate in the same subcarrier unlike traditional Frequency Division Multiplexing Technique (FDM) where each piece of information is propagated with a single carrier which saves the additional guard period there by giving robustness to the system from impairments due to frequency fading caused by multipath propagation and Inter Symbol Interference(ISI). Through this paper it was inferred that adding security and authenticity(encryption) followed cons though there were considerable amount of pros. Secured Hash Algorithm(SHA 1) conceals the data by furnishing an unrecognizable distinct hundred and sixty bits digest. This gave rise to reliable protection but eventuated increased Bit Error Rate(BER) . The 160 bits hash sequences contributes to larger bit error rate emanating from the fact that greater number of bits results in greater probability of BER.**

Keyword- OFDM, Hash encryption, SHA1, BER

I. INTRODUCTION

The Broad Band systems are predominantly dependant on data rate. The mathematical orthogonality of OFDM saves the requirement of guard intervals which increases robustness to noise, frequency selective fading, etc. In this technique there is a parallel modulation of each symbol with each subcarrier. So any external disturbance distorts the transmission of data through that particular subcarrier unlike the conventional Frequency Division Multiplexing (FDM) where a slight distortion affects the entire channel. Absence of orthogonality between the subcarriers in the FDM causes overlapping which calls guard intervals between the subcarriers. OFDM comparatively has an efficient utilization of the band width. From the figure 1 it is clear that about 25% bandwidth is saved by this technique.

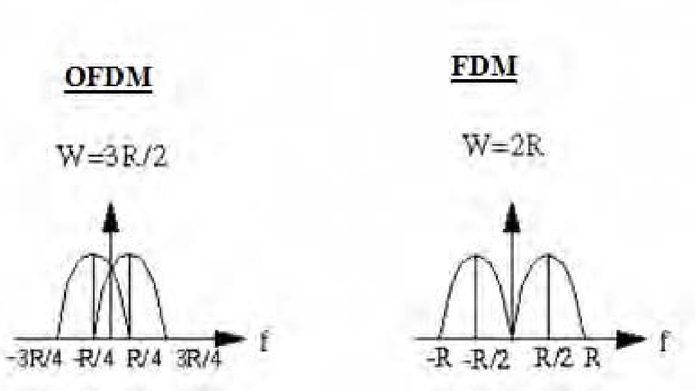


Fig 1. Comparision of OFDM and FDM

II. METHOD AND PROPOSAL

The process is initiated with serial to parallel conversion of high speed data stream into slow parallel data stream. The random integer generation helps in the formation of symbols. These symbols are encrypted by SHA 1 to yield unique 160 bits Hash digest of the symbols. These Hash sequences are fed into the QAM mapper to perform Quadrature Amplitude Modulation.

II.A.1 Encryption:

- A set of Hash keys are generated.
- The Hash keys are mapped on to the symbols.
- The symbols are synthesized depending on the Hash sequence

II.A.2 Modulation:

The complex base band representation of OFDM symbol is given by

$$s(t) = \mathrm{Re}\left\{ \sum_{i=-\frac{N_s}{2}}^{\frac{N_s}{2}-1} d_{i+N_s/2} \exp\left(j2\pi\left(f_c - \frac{i+0.5}{T} \right)(t-t_s) \right) \right\}, \; t_s \le t \le t_s + T$$

$$s(t) = 0, \; t < t_s \quad \wedge \quad t > t_s + T$$

where d_{i} - denotes the complex modulation symbol, Ns - denotes the number of subcarriers. T - denotes the duration of the symbol. Fc - denotes the frequency of the subcarrier.

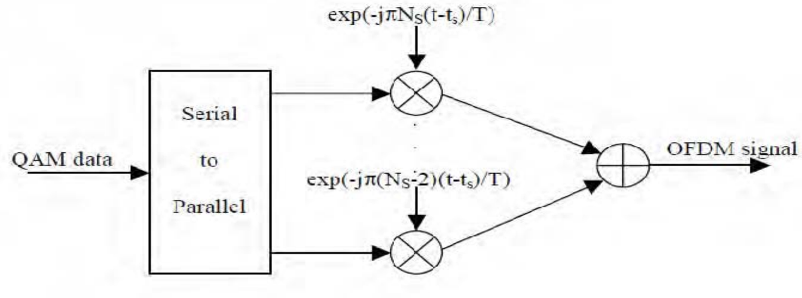
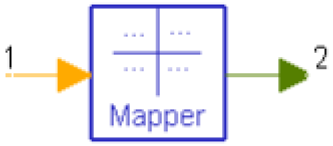


Fig 2. Modulation of OFDM using QAM

From the base band expression, the real part stands for the In-phase Component and the imaginary stands for the Quadrature-phase component. Product of the In-Phase and the Quadrature-phase component with cosine and sine gives the OFDM signal. OFDM is a combined digital and analogue modulation which is performed using the component, Mapper and creates a symbol distribution over the two dimensional scatter space which makes it easy for the receiver to decode the symbols.

II.A.3 FUNCTION OF A QAM MAPPER:



It is a component acting as a modulator for 16QAM, 32QAM, 128QAM and 256QAM. Inputs under a specific category of tokens yields outputs contained in another class of tokens.

Table 1 Pin Inputs:

Pin	Pin Name	Depiction	Data type
1	In	Input bit sequence	Integer

Table 2: Pin Outputs:

Pin	Name	Depiction	Signal Type
2	Out	Output symbol Sequence	Complex

Table 3: Modulation and scalars

Modulation Type	Number of Input scalars
16 QAM	4
32 QAM	5
64 QAM	6
128 QAM	7
256 QAM	8

Depending on the number of input scalars triggered, one OUT token is produced as explained in the table.

C. Constellation Diagram:

The distribution of the symbols in the two dimensional scatter space in the complex plane is accomplished by a tool called Constellation Diagram. Each symbol at different symbol instants are plotted in this Scatter Diagram. The transmitted symbols are represented as a complex number and the real and imaginary parts are separately modulated by a cosine and sine carrier respectively. They are defined as Quadrature subcarriers. This makes multiple symbols to be carried by the same subcarrier. The points plotted on the Constellation Diagram are called Constellation Points.

D. Interpretations from the Constellation Diagram:

At the receiver upon reception of the symbols corrupted by Additive White Gaussian Noise(AWGN), the actual symbol is discovered from the error symbol by making an estimate on the constellation map by considering the nearest possible Euclidean distance. This is called Maximum Likelihood Detection. The different type of flaws in the symbols imposes distinct discrepancies in the scatter plot as follows:

- The Constellation points become fuzzy when the symbols travel in AWGN channel
- The Constellation points become rotationally spread when phase noise is encountered.
- Interferences eventuate in non-coherent single frequencies which are depicted as circularly aligned constellation points.

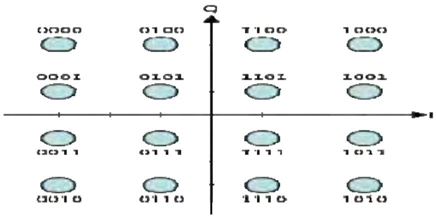
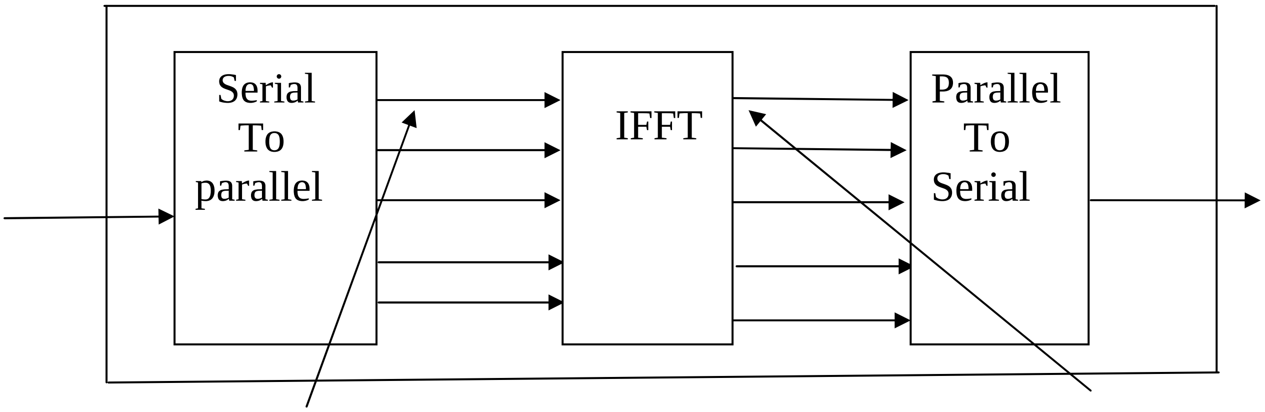


Fig 4. Constellation graph for the 16 QAM.

QAM has more robustness to signal deterioration due to noise unlike other digital shift keying techniques and can bear higher information density accompanied by more susception to interference.

III. Inverse Fast Fourier Transform



Parallel symbols in complex form

IFFT output samples

Fig 5. Receiver part of OFDM

IFFT possesses the dual property of conversion of symbols from frequency domain to time slots and acts as the multiplexer for the 'n' encrypted modulated inputs . The property of orthogonality can be verified through the outcome of IFFT. The dot products of IFFT samples yield zero when they are orthogonal to each other.

III. Channel Equalization by Cyclic Prefix**:**

It is an important feature of OFDM which combats ISI and ICI. It is the process of prefixing the last bits of the symbols by continous replication. It exhibits dual functions by acting as a guard interval between the subcarriers.Transforming linear convolution into circular convolution. The sinusoidal signal will have infinite time duration and is an eigen function of linear and time invariant channel. But in real time these sinusoids have finite time period. So conversion to circular convolution puts down this constraint.

A. At the receiver:

Cyclic Prefix is removed on reception to convert circular into linear convolution. The receiver exploits the property of Maximum Likelihood Detection using which obtaining the symbol from the constellation is highly propable. If the symbol is corrupted by noise, the receiver estimates the uncorrrupted symbol from the constellation map by the nearest Euclidean distance. The received symbols are decoded by taking Fast Fourier Transform. The converted frequency domain symbols are demodulated by Quadrature Orthogonal Demodulators.

B. In phase Quadrature Phase Demodulation:

The symbols have to travel three stages to yield intended data. Mixing of RF symbols with sines and cosines to retrieve back the original real(In Phase) and imaginary(Quadrature phase).

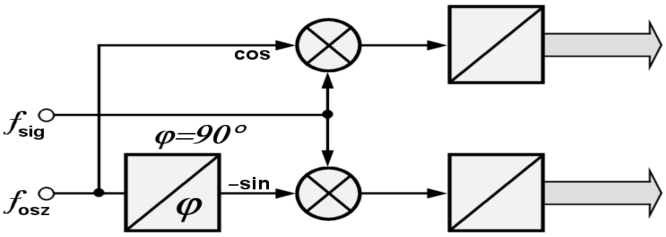


Fig 6. I and Q mapper

C. Low pass filtering

A low pass filter(LPF) with a rectangular response is chosen to impose filtering action on the individual real and imaginary parts of the complex symbols. Frequencies outside the desired bandwidth and noise are filtered by this LPF. For instance if 2MHZ is our intended bandwidth then the LPF with the response as shown in the fig 7 below is chosen.

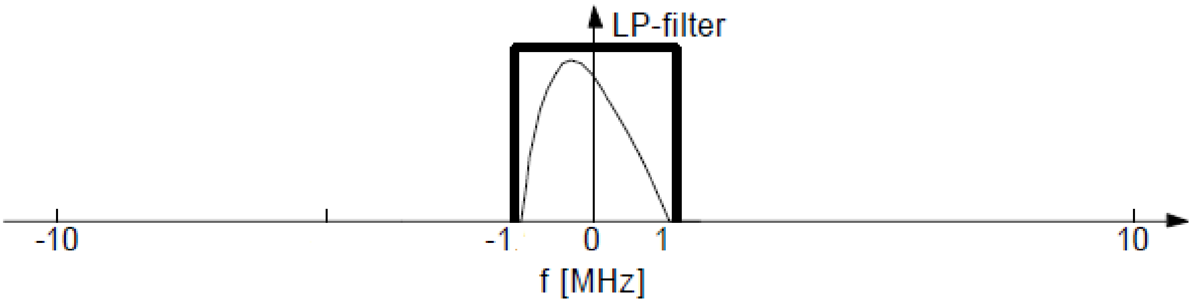


Fig 7. LPF filter design

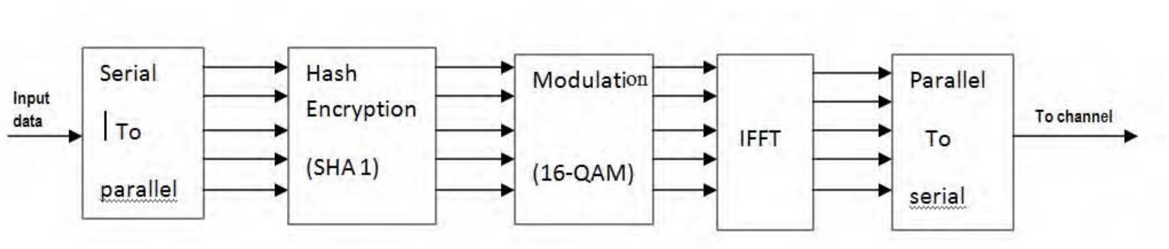
IV. Decimation to scale down the sampling instants.

As a consequence of removal of unwanted frequencies by the LPF, comparatively lesser number of frequency samples resulted. So the Decimation operation is performed to scale down the sampling frequencies. For example if 20MHz is the frequency of the signal in use, the sampling rate can be scaled down to 3.333MHz . The decimation cannot be performed when the scaled down sampling frequency is not greater than twice the cut off frequency of LPF(Nyquist Criterion). The output of demodulation gives the encrypted demodulated symbols which are deprived of the complex form. Though by employing Cyclic

Prefix it is possible to obtain the transmitted data at the receiver, the data obtained is concealed by SHA 1. The reverse process of decryption by SHA 1 is not feasible. The data received is always in the Hash digested form. The fact of non decodeability of Hash digest brings a trade off between security and decryption. In this paper, there is a comparison between transmitted and received Encrypted OFDM symbols. Any undesirable tapping of data causes change in the 160 bits Hash value and on comparison at the receiver shows negative result. The original data can be retrieved only when the receiver gets a positive result on comparison between the transmitted and received encrypted QAM symbols.

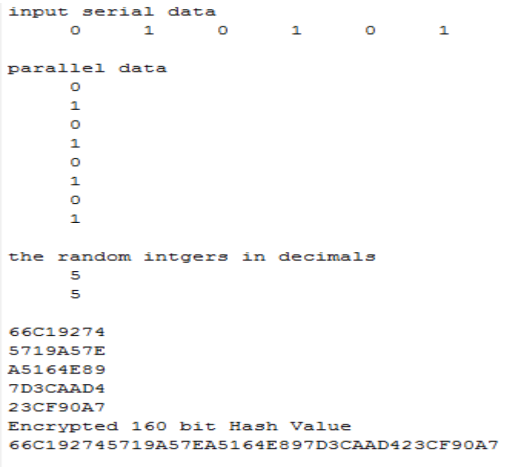
V.IMPLEMENTATION AND RESULTS

A. At theTransmitter:



Serial stream of random integers are transformed to parallel stream of symbols for encryption. On encryption, a 160 bits hash value is formed for each symbol. Making it computationally difficult in Matlab, this large value is converted to a truncated decimal value for easy manupulation.

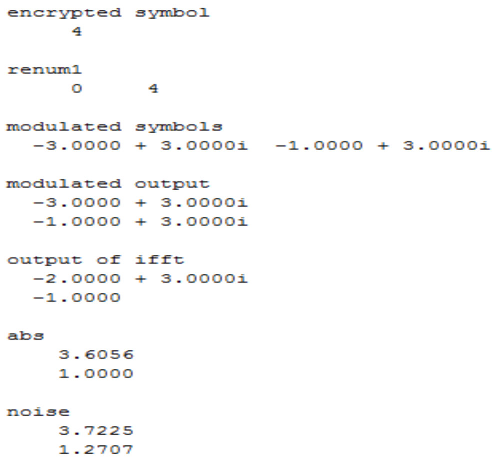
Output in command window:



```
input serial data
     0     1     0     1     0     1     0     1

parallel data
     0
     1
     0
     1
     0
     1
     0
     1

the random intgers in decimals
     5
     5

66C19274
5719A57E
A5164E89
7D3CAAD4
23CF90A7
Encrypted 160 bit Hash Value
66C192745719A57EA5164E897D3CAAD423CF90A7
```

Complex numbers are generated by QAM mapper for each encrypted symbol mapping.

Out put in command window:



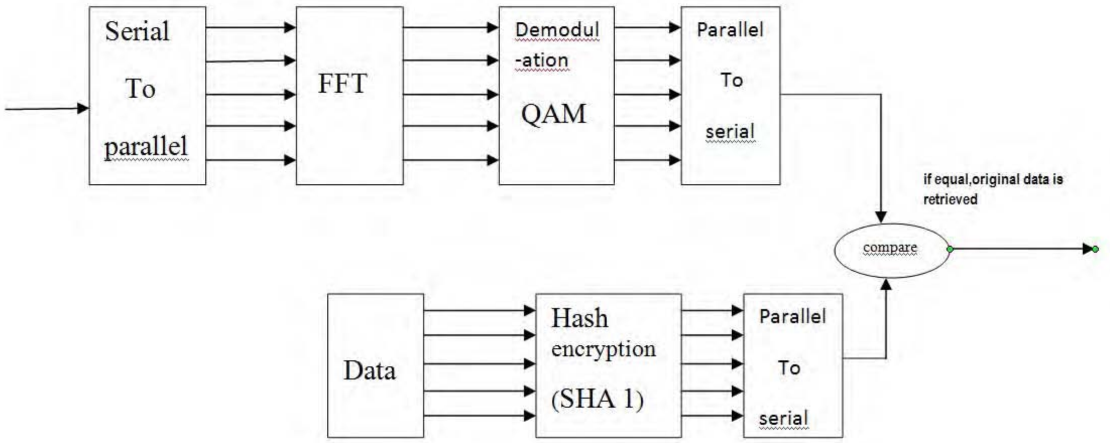
```
encrypted symbol
     4

renum1
     0     4

modulated symbols
  -3.0000 + 3.0000i  -1.0000 + 3.0000i

modulated output
  -3.0000 + 3.0000i
  -1.0000 + 3.0000i

output of ifft
  -2.0000 + 3.0000i
  -1.0000

abs
    3.6056
    1.0000

noise
    3.7225
    1.2707
```

renum1 indicates the encrypted decimal value.

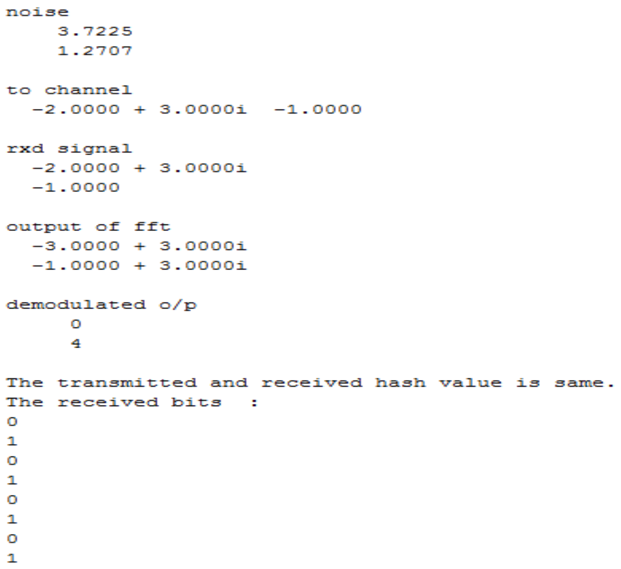
These QAM symbols are converted to time domain and transmitted to the receiver.

abs is the absolute modulus value of the modulated symbols for plotting the BER graph.

noise represents the symbols in Additive White Guassian Noise (AWGN) channel.
B. At the receiver:

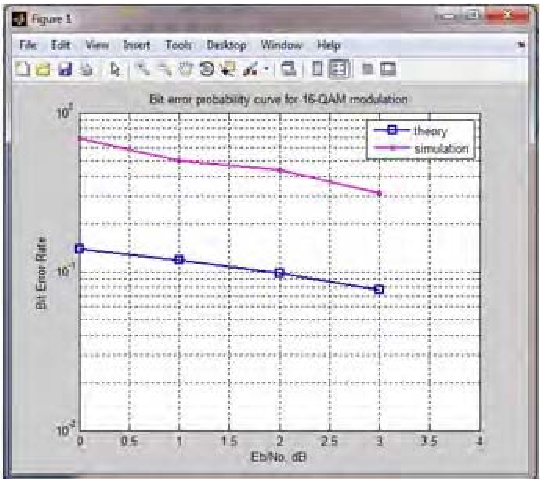


Fast Fourier Transform transfers the symbols received at different time slots into parallel flow of symbols in frequency domain after Serial to Parallel conversion.
IQ demodulator gives the demodulated encrypted symbols after checking whether the hash values of transmitter and receiver are equal.
Output in command window:

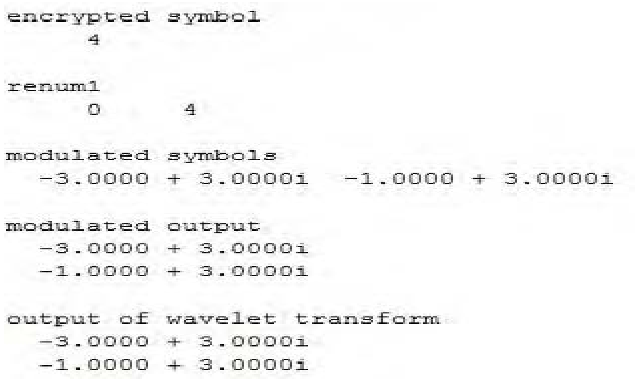


```
noise
    3.7225
    1.2707

to channel
  -2.0000 + 3.0000i  -1.0000

rxd signal
  -2.0000 + 3.0000i
  -1.0000

output of fft
  -3.0000 + 3.0000i
  -1.0000 + 3.0000i

demodulated o/p
     0
     4

The transmitted and received hash value is same.
The received bits  :
0
1
0
1
0
1
0
1
```

C. Bit Error Rate Graph:
Bit Error Rate is the ratio of the number of error bits in the symbol travelling in the channel to the total number of bits in the symbol. Here the BER graph is plotted for four symbols in the AWGN channel as follows



D. Implementation using Discrete Wavelet Transform:
Out put in the command window:



```
encrypted symbol
     4

renum1
     0     4

modulated symbols
  -3.0000 + 3.0000i  -1.0000 + 3.0000i

modulated output
  -3.0000 + 3.0000i
  -1.0000 + 3.0000i

output of wavelet transform
  -3.0000 + 3.0000i
  -1.0000 + 3.0000i
```

VI. REFERENCES

[1] N.R.Raajan, Y.Venkatramani, T.R.Sivaramakrishnan, "*Rearranging architecture for WCDMA over GSM*", Sensors and transducers journal, Vol.106, issue 7, July 2009, PP 114 – 122. 2012.

[2] N.R. Raajan, B. Monisha, K. Vinoth, R. Niranjan, D. Diwakar Padmanabhan, CORDIC Based Modified OFDM for Pipelined Data Process, Procedia Engineering, Volume 38, 2012, Pages 3300-3307, ISSN 1877-7058, 10.1016/j.proeng.2012.06.382.

[3] N.R. Raajan, A. Jenifer Philomina, S. Suganya, B. Monisha, M.V. Priya, D. Parthiban, M. Ramkumar, Performance Evaluation of MIMO-OFDM Modeling for UMTS-Long Term Evolution Downlink System, Procedia Engineering, Volume 38, 2012, Pages 607-612, ISSN 1877-7058, 10.1016/j.proeng.2012.06.075.

[4] N.R. Raajan, B. Monisha, Niranjana Rangarajan, R. Vishnupriya, Secured OHWDM Using Fractals, Procedia Engineering, Volume 38, 2012, Pages 724-729, ISSN1877-7058, 10.1016/j.proeng.2012.06.091.

[5] N.R. Raajan, A. Jenifer Philomina, K. Avudaiappan, V. Avinash, Synchronized OFDM System Using Inter-Symbol Pilots, Procedia Engineering, Volume 38, 2012, Pages 1291-1296, ISSN 1877-7058, 10.1016/j.proeng.2012.06.159.

[6] Philomina, A.J.; Parthiban, D.; Monisha, B.; Priya, M.V.; Suganya, S.; Kumar, M.R.; Raajan, N.R., "Channel estimation of WCDMA with synchronized OFDM system for MIMO communication,"*Computer Communication and Informatics (ICCCI), 2012 International Conferenceon*volnopp.1,610-12Jan2012 doi:
10.1109/ICCCI.2012.6158852URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6158852&isnumber=6158648

[7] Raajan, N.R.; Monisha, B.; Kumar, M.R.; Philomina, A.J.; Priya, M.V.; Parthiban, D.; Suganya, S., "Design and implementation of orthogonal wavelet division multiplexing (OHWDM) with minimum bit error rate," *Trendz in Information Sciences and Computing (TISC)20113rdInternationalConferenceon* volnopp.122,1278-9 Dec2011 doi:
10.1109/TISC.2011.6169097URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6169097&isnumber=6169071

[8] Monisha, B.; Ramkumar, M.; Priya, M.V.; Philomina, A.J.; Parthiban, D.; Suganya, S.; Raajan, N.R., "Design and implementation of orthogonal based haar wavelet division multiplexing for 3GPP networks,"*Computer Communication and Informatics (ICCCI)", 2012 InternationalConferenceon* ,vol.,no.,pp.1,6,10-12Jan.2012 doi:
10.1109/ICCCI.2012.6158851 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6158851&isnumber=6158648

[9] Raajan, N.R.; Philomina, A.J.; Priya, M.V.; Monisha, B.; Suganya, S.; Kumar, M.R.; Parthiban, D., "Improved OFDM system using inter symbol pilot aided synchronization in asynchronous mode of transmission," *Advances in Engineering, Science and Management (ICAESM),2012InternationalConferenceon* ,vol.,no.,pp.652,656,30-31 March
2012 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6216077&isnumber=6215562

[10] Parthiban, D.; Philomina, A.J.; Raajan, N.R.; Monisha, B.; Priya, M.V.; Suganya, S., "Wavelet-based multiple access technique for mobile communications," *Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on* , vol.,no.,pp.121,124,21-23 March2012 doi:
10.1109/ICPRIME.2012.6208298 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6208298&isnumber=6208277