WIRELESS NETWORK DATA TRANSFER ENERGY OPTIMIZATION ALGORITHM

Alka P.Sawlikar[1], Dr.Z.J.Khan[2], Dr.S.G.Akojwar[3]

[1, 3] *Department Electronics Engineering, RCERT, Chandrapur, MS, (India)*

[2] *Department Electrical Engineering, RCERT, Chandrapur, MS, (India)*

ABSTRACT

Orthogonal Frequency Division Multiplexing (OFDM) is the most promising modulation technique. It has been adopted by most wireless and wired communication standards. The idea is to utilize a number of carriers, spread regularly over a frequency band, in such a way so that the available bandwidth is utilized to maximal efficiency. The objective of this paper is to carry out an efficient implementation of the OFDM system (i.e. transmitter and receiver) using different Encryption and compression algorithm for the energy optimization on data transmission. The best combination for the algorithm is finding for the encryption and compression of the data for the transmission and energy optimization.

Keywords*: *AES, Compression, Decompression, Decryption, ECC, Encryption, OFDM, RSA.

I. INTRODUCTION

In some applications, it is desirable to transmit the same information bearing signal over several channels. This mode of transmission is used primarily in situations where there is high probability that one or more of the channels will be unreliable from time to time. One form of this multichannel signaling is sometimes employed in wireless communications systems as means of overcoming the effects of interference of the transmitted signal.[1] By transmitting the same information over multiple-channels, provides signal diversity, which the receiver can exploit to recover the information. Another form of the multichannel communications in multiple carrier transmission, where the frequency band of the channel is subdivided into a number of sub-channels and information is transmitted on each of the sub channels. In non-ideal linear filter channels it is observed that such channels introduce ISI, which degrades performance compared with the idea channel. The degree of performance degradation depends on the frequency response characteristics [1][2]. Furthermore, the complexity of the receiver increases as the span of ISI increases. In this system, we consider the transmission of information on multiple carriers contained within the allocated channel bandwidth. The primary motivation for transmitting data on multiple carriers is to reduce ISI and thus, eliminate the performance degradation that is incurred in several methods to implement the system.

Smartphone's have become the essential components of our daily life; however, we are also frustrated with their short battery life. One major source of the power consumption comes from the cellular interface which is used for supporting mobile data[3]. In UMTS 3G network or 4G (HSPA+) network, multiple timers are used to control the cellular interface, and the timeout value for releasing the radio resource can be more than 15 seconds. Thus, it is possible that the cellular interface continues to consume a large amount of energy (also referred to as the *long tail problem*) before the timer expires, even when there is no network traffic. For

example, recent research showed that the energy wasted in the long tail in 3G networks could be more than that of the real data transmission in many applications, and this becomes worse in[3].A 4G network due to its higher tail power and longer tail time[3].

II. LITERATURE REVIEW

2.1 OFDM Transmitter and Receiver

Figure 1 shows the complete block diagram of OFDM transmitter and Receiver System.

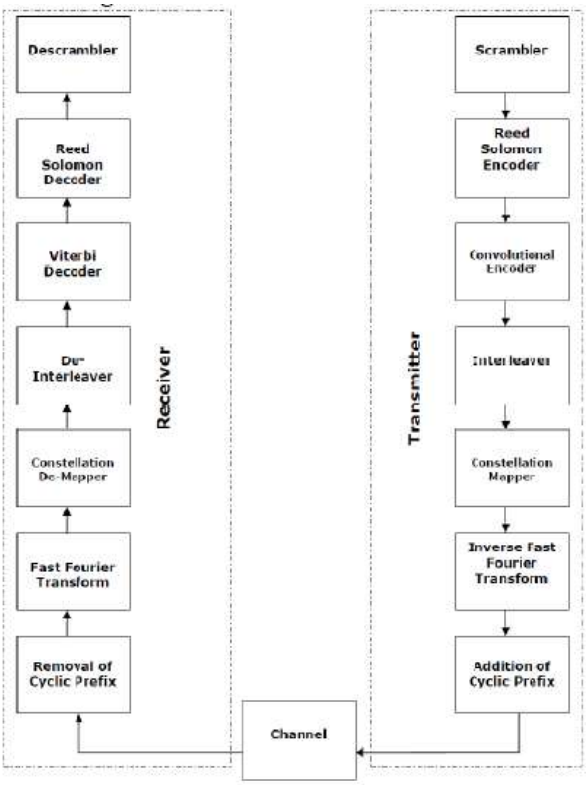

Figure 1 Complete OFDM System

2.2 Scramble/Descramble

Data bits are given to the transmitter as inputs. These bits pass through a scrambler that randomizes the bit sequence. This is done in order to make the input sequence more disperse so [4]that the dependence of input signal's power spectrum on the actual transmitted data can be eliminated. At the receiver end descrambling is the last step. Descrambler simply recovers original data bits from the scrambled bits.

2.3 Reed-Solomon Encoder/Decoder

The scrambled bits are then fed to the Reed Solomon Encoder which is a part of Forward Error Correction (FEC). Reed Solomon coding is an error-correction coding technique. Input data is over-sampled and parity symbols are calculated which are then appended with original data [4]. In this way redundant bits are added to the actual message which provides immunity against severe channel conditions. A Reed Solomon code is represented in the form RS (n, k), [4]where

$$n = 2^m - 1 \quad \text{(a)}$$

$$k = 2^m - 1 - 2t \quad \text{(b)}$$

Here m is the number of bits per symbol, k is the number of input data symbols (to be encoded), n is the total number of symbols (data + parity) in the RS codeword and t is the maximum number of data symbols that can be corrected. At the receiver Reed Solomon coded symbols are decoded by removing parity symbols.[4]

2.4 Convolution Encoder/Decoder

Reed Solomon error-coded bits are further coded by Convolutional encoder. This coder adds redundant bits as well. In this type of coding technique each m bit symbol is transformed into an n bit symbol; m/n is known as the code rate. This transformation of m bit symbol into n bit symbol depends upon the last k data symbols, therefore k is known as the constraint length of the Convolutional code[4]. Viterbi algorithm is used to decode convolutionaly encoded bits at the receiver side. Viterbi decoding algorithm is most suitable for Convolutional codes with k_10.

2.5 Interleaver/De-Interleaver

Interleaving is done to protect the data from burst errors during transmission. Conceptually, the in-coming bit stream is re-arranged so that adjacent bits are no more adjacent to each other. The data is broken into blocks and the bits within a block are rearranged[4]. Talking in terms of OFDM, the bits within an OFDM symbol are rearranged in such a fashion so that adjacent bits are placed on non-adjacent subcarriers. As far as De-Interleaving is concerned, [4]it again rearranges the bits into original form during reception.

2.6 Constellation Mapper/De-Mapper

The Constellation Mapper basically maps the incoming (interleaved) bits onto different sub-carriers. Different modulation techniques can be employed (such as QPSK, BPSK, QAM etc.) for different sub-carriers. The De-Mapper simply extracts bits from the modulated symbols at the receiver.[4]

2.7 Inverse Fast Fourier Transform/ Fast Fourier Transform

This is the most important block in the OFDM communication system. It is IFFT that basically gives OFDM its orthogonality.[4] The IFFT transform a spectrum (amplitude and phase of each component) into a time domain signal. It converts a number of complex data points into the same number of points in time domain[5]. Similarly, FFT at the receiver side performs the reverse task i.e. conversion from time domain back to frequency domain.

2.8 Addition/Removal of Cyclic Prefix

In order to preserve the sub-carrier orthogonality and the independence of subsequent OFDM symbols, a cyclic guard interval is introduced. The guard period is specified in terms of the fraction of the number of samples that make up an OFDM symbol. The cyclic prefix contains a copy of the end of the forthcoming symbol. Addition of cyclic prefix results in circular convolution between the transmitted signal and the channel impulse response. Frequency domain equivalent of circular convolution is simply the multiplication of transmitted signal's frequency response and channel frequency response, therefore received signal is only a scaled version of transmitted signal (in frequency domain),[4] hence distortions due to severe channel conditions are eliminated. Removal of cyclic prefix is then done at the receiver end and the cyclic prefix–free signal is passed through the various blocks of the receiver.

2.9 AES Algorithm

The algorithm originates from the initiative of the National Institute of Standards and Technology (NIST) in 1997 to select a new symmetric key encryption algorithm. From the initial candidates [4]. Rijndael algorithm was selected as the Advanced Encryption Standard (AES) [5] due to the combination of security, performance, efficiency, ease of implementation and flexibility[6]. Rijndael is a symmetric byte-oriented iterated (each iteration is called a round) block cipher that can process data blocks of 128 bits (4 words), using keys with length of 128, 192 and 256 bits. Rijndael is capable of processing additional block sizes (160, 192 and 244 bits) and key lengths (160 and 244 bits), however they are not adopted in AES. Our implementation refers to AES algorithm.

2.10 RSA Algorithm

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm, which was essentially to replace the less secure National Bureau of Standards (NBS) algorithm[7]. Most importantly, RSA implements a public-key cryptosystem, as well as digital signatures[8]. RSA is motivated by the published works of Die and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it [8][9].

2.11 ECC Algorithm

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems, independently by Victor
Miller of IBM and Neal Koblitz At that time, elliptic curves were already being used in various cryptographic contexts, such as integer factorization and primality proving. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985[10][11][12][13].

2.12 Hill Algorithm

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once. The following discussion assumes an elementary knowledge of matrices.
Each letter is represented by a number modulo 26. (Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.) To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible $n \times n$ matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption[14].

III. PROPOSED METHOD

In this paper we proposed the method for transfer the data from the network by using the encryption and compression method. We used the several combination of the encryption and compression algorithm to obtain the best combination for the energy optimization. For transmission and Receiver of the data in the network we used OFDM.

Block Diagram shows the overall implementation of the proposed methodology.

IV. FIGURES AND TABLES

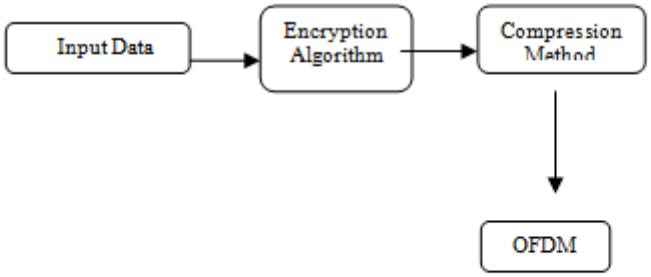

Figure 2.a. Block Diagram of proposed method on Transmitter Side

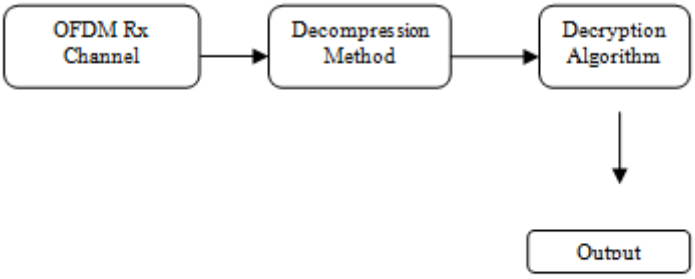

Figure 2.b. Block Diagram of proposed method on Receiver Side

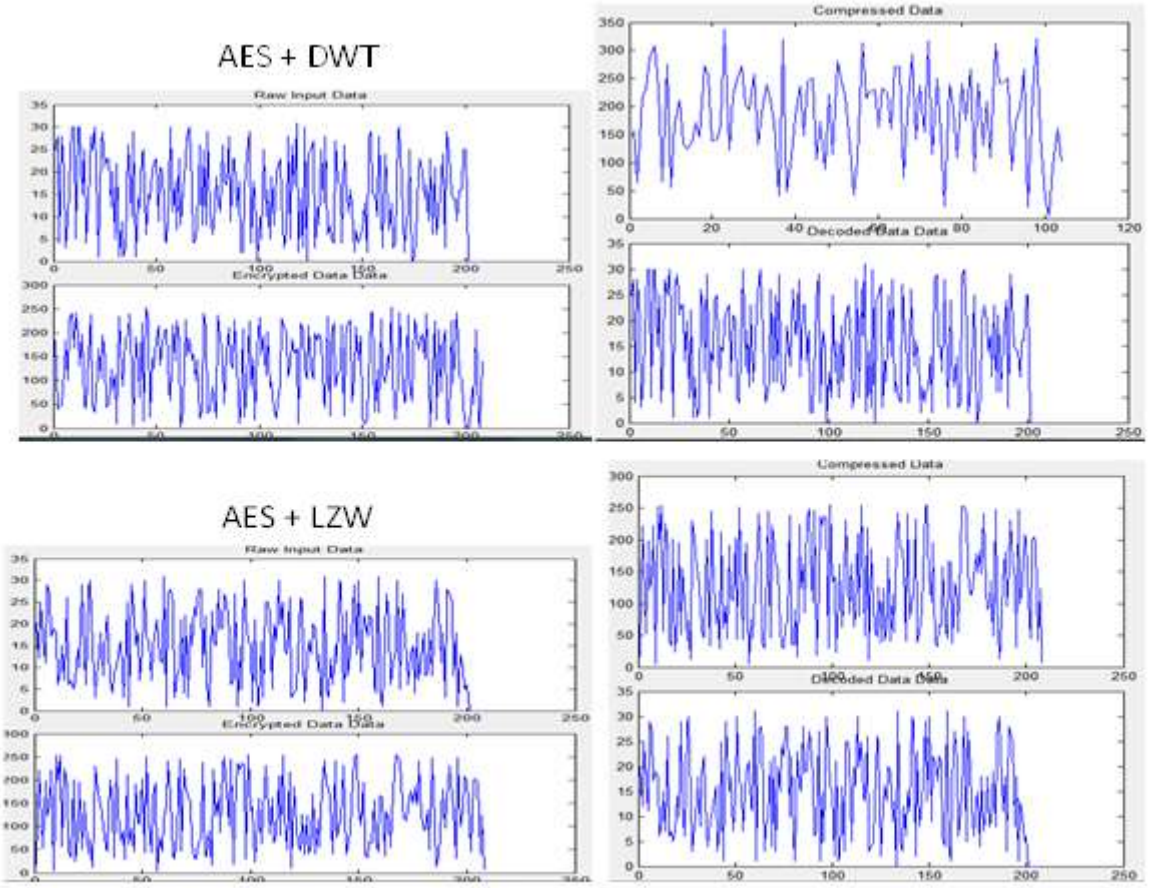

Fig.3. Result of Different Combination for the Encryption and Compression

	Input Bits==200				
ENCRYPTION TECH	COMPRESSION TECH	TIME	Normal Data Size	Compressed Data Size	COMPRESSION RATIO
AES	RLE	6.85sec	1719	208	87.905
	DWT	8.9556sec	208	104	50.00%
	DCT	7.85sec	208	208	0.00%
	HUFFMAN	5.77sec	208	208	0.00%
	LZ	5.51sec	208	208	0.00%
INTERLEAVING	RLE	4.82sec	1299	208	83.99%
	DWT	2.55sec	208	104	50.00%
	DCT	3.28sec	208	208	0.00%
	HUFFMAN	3.52sec	208	208	0.00%
	LZ	2.56sec	208	190	8.65%
HILL	RLE	3.10sec	1219	208	82.94%
	DWT	2.61sec	208	104	50.00%
	DCT	2.05sec	208	208	0.00%
	HUFFMAN	3.38sec	208	208	0.00%
	LZ	2.991sec	208	187	10.10%
RSA	RLE	2.11sec	1191	208	82.54%
	DWT	2.34sec	208	104	50.00%
	DCT	2.15sec	208	208	0.00%
	HUFFMAN	2.20sec	208	208	0.00%
	LZ	3.60sec	208	191	8.17%
ECC	RLE	2.97sec	1283	208	83.79%
	DWT	2.51sec	208	104	50.00%
	DCT	2.44sec	208	208	0.00%
	HUFFMAN	2.03sec	208	208	0.00%
	LZ	2.73sec	208	187	10.10%

Table.1. Result of different combination for the Encryption and Compression

V. CONCLUSION

The proposed method brought forward by means of this paper work effectively and efficiently energy optimization for the transfer in the wireless network. Various efficient algorithms are used in the work, thus giving fruitful results. The best combination is obtained from the result of the experiment. The best combination is find from the maximum compression ratio and minimum time required for the compression and encryption in transmitter side and decompression and decryption in the receiver side. From the table we can see that the RSA algorithm for encryption and RLE algorithm for compression gives the most satisfactory result in terms of time and compression ratio.

REFERENCES

[1] Tirumala Rao Pechetty, Mohith Vemulapalli, "An Implementation of OFDM Transmitter and Receiver on Reconfigurable Platforms", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , Vol. 2, Issue 11, November 2013

[2] Kehinde Obidairo, Greg. O. Onwodi , "A Book Of National Open University Of Nigeria School Of Science And Technology", Course Code: Cit654; Course Title: Digital Communications; Course Writer :Greg. O. Onwodi.

[3] Wenjie Hu and Guohong Cao, "Energy Optimization Through Traffic Aggregation in Wireless Networks",Department of Computer Science and Engineering,The Pennsylvania State University

[4] Nasreen Mev, Brig. R.M. Khaire, "Implementation of OFDM Transmitter and Receiver Using FPGA", International Journal of Soft Computing and Engineering (IJSCE),ISSN: 2231-2307, Volume-3, Issue-3, July 2013

[5] R. Housley, " Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax", INTERNET DRAFT S/MIME Working Group,Vigil Security, January 2007

[6] Nithya, Dr.E.George ,Dharma Prakash Raj, " Survey on asymmetric key cryptography algorithms", Journal of advanced computing and communication technologies,vol no. 2,issue no,1,ISSN-2347-2804.

[7] Evgeny Milanov ,"A Report on:The RSA Algorithm".,3 June 2009.

[8] Pabitra Kumar Das, Crocmaster ,"A research paper on RSA Encryption part I" , Hackshark , Aug 27, 2012

[9] Daniel J. Bernstein and Chitchanok Chuengsatiansup and Tanja Lange , "A Report on :New ECC Curve Bumps Speed/Security Baseline", July 10 2014.

[10] Kristin Lauter, "The Advantages Of Elliptic Curve Cryptography For Wireless Security",IEEE Wireless Communications , February 2004,1536-1284

[11] International journal of advanced scientific and technical research Issue 3 volume 3, May-June 2013

[12] An article on Hill cipher , Wikipedia *February 2012*

[13] B. Zhao, Q. Zheng, G. Cao, and S. Addepalli, "Energy-Aware Web Browsing in 3G Based Smartphones," in *IEEE ICDCS, 2013*.

[14] Hero Modares, Amirhossein Moravejosharieh, Rosli Salleh, "Wireless Network Security Using Elliptic Curve Cryptography", 2011First International Conference on Informatics and Computational Intelligence.

[15] Nguyen Toan Van, "Hardware Implementation Of OFDM TransmitterAnd Receiver Using FPGA"

[16] C.K.P.Clarke," Reed Solomon Error Correction", Research & Development British Broadcasting corporation July 2002