International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Smart Data Transfer: An Energy-Conscious Approach for Wireless Networks

[1]Alka Sawlikar, [2]Bireshwar Ganguly, [3]Devashri Kodgire

Submitted: 12/12/2023 **Revised:** 25/01/2024 **Accepted:** 04/02/2024

Abstract: Orthogonal Frequency Division Multiplexing (OFDM) is one of the most promising and widely adopted modulation techniques in both wireless and wired communication standards. It efficiently utilizes the available bandwidth by dividing it into multiple orthogonal subcarriers, thereby enhancing data transmission performance and spectral efficiency.This paper focuses on the efficient implementation of an OFDM system, encompassing both the transmitter and receiver, integrated with various encryption and compression algorithms to optimize energy consumption during data transmission. The study aims to identify the most effective combination of encryption and compression techniques that not only ensure data security and integrity but also contribute to energy-efficient communication.Through simulation and comparative analysis, the paper evaluates multiple algorithms to determine the optimal configuration for secure and energy-aware data transfer in OFDM-based communication systems.

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

I. INTRODUCTION

In many communication applications, it is desirable to transmit the same information-bearing signal over multiple channels. This multichannel transmission strategy is particularly effective in environments where individual channels may become unreliable or subject to interference intermittently. By transmitting redundant data across several channels, the system introduces signal diversity, which the receiver can exploit to recover the original information even when some channels are compromised.

One implementation of multichannel communication is multiple carrier transmission, wherein the available frequency band is divided into a number of sub-channels, each carrying a portion of the data. However, non-ideal linear filter channels often introduce inter-symbol interference (ISI), which can significantly degrade system performance compared to an ideal channel. The extent of this degradation largely depends on the channel's frequency response characteristics [1][2]. Moreover, as the ISI span increases, so does the complexity of the receiver, adding to both processing load and power consumption.

To address these issues, modern systems adopt multi-carrier modulation techniques, such as Orthogonal Frequency Division Multiplexing (OFDM), where information is transmitted simultaneously across multiple carriers within the allocated bandwidth. This technique effectively mitigates ISI and improves system robustness in dispersive environments.

At the same time, energy efficiency in wireless communication remains a critical concern—

Alka Sawlikar
Dept. of Electronics Engg, R.C.E.R.T, Chandrapur-India
alkaprasad.sawlikar@gmail.com

Bireshwar Ganguly
Dept. of Data Science. R.C.E.R.T, Chandrapur-India
bireshwar.ganguly@gmail.com

Devashri Kodgire
Dept. of Data Science, R.C.E.R.T, Chandrapur-India
devashriraich@gmail.com

especially in mobile devices like smartphones. Despite their ubiquitous role in daily life, users are often frustrated by their limited battery life. A significant portion of power consumption originates from the cellular interface, which supports mobile data connectivity.

In networks such as UMTS 3G and 4G (HSPA+ and LTE), multiple timers are used to manage radio resources. These timers often have long timeout values—exceeding 15 seconds in some cases—before releasing unused radio connections. This behavior leads to the so-called "long tail problem", where the cellular interface continues to draw power even in the absence of active data transmission.

Recent studies [3] have shown that in 3G networks, the energy wasted during the tail state can exceed the energy used for actual data transmission in many applications. This inefficiency becomes even more pronounced in 4G networks due to their higher tail power and extended tail duration [3]. As a result, any optimization technique—be it in the form of energy-aware scheduling, compression, encryption, or multichannel signaling—should take into account not only throughput and security but also energy minimization, especially in mobile environments.

Summary Points:

- Multichannel signaling introduces diversity and resilience against interference.
- Multiple carrier transmission (like OFDM) combats ISI and improves robustness.
- ISI degrades performance and increases receiver complexity.
- Mobile data interfaces (3G/4G) suffer from long tail power drain, wasting energy.
- Energy optimization in wireless systems is crucial for battery-powered devices.

II. LITERATURE REVIEW

2.1 OFDM Transmitter and Receiver

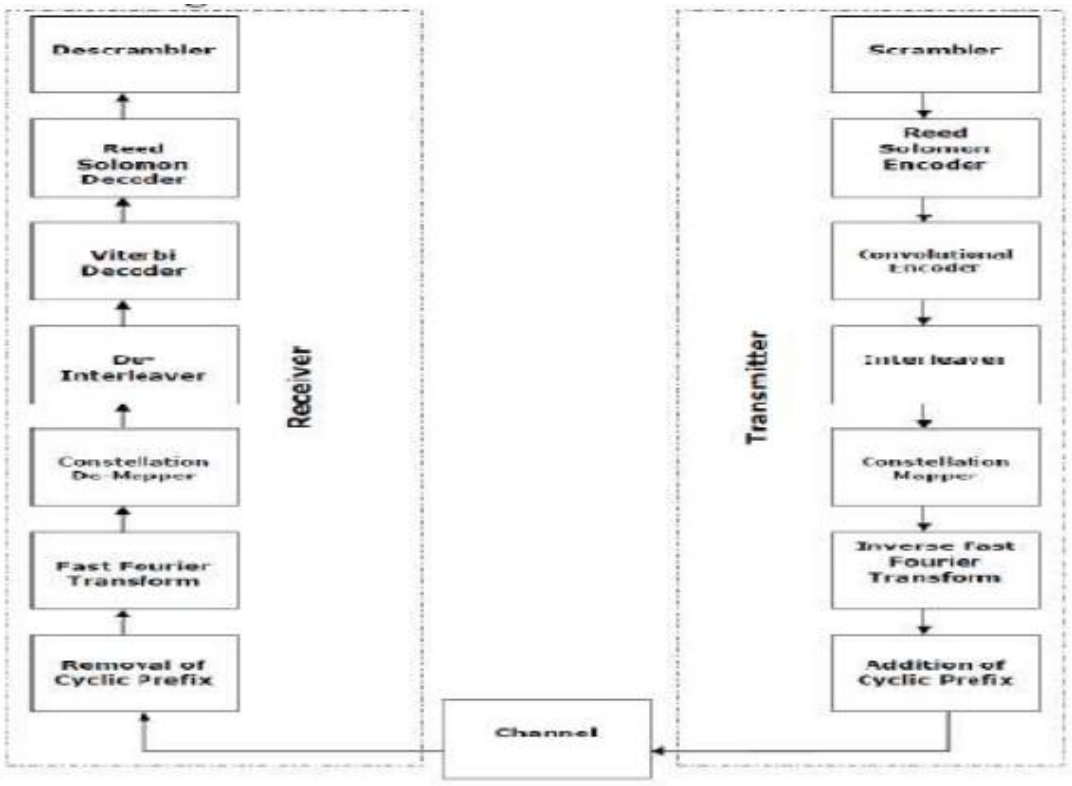

Figure 1 Complete OFDM System

2.2 Scramble/Descramble

In digital communication systems, the input data bits provided to the transmitter are first processed through a scrambler**.** The primary purpose of scrambling is to randomize the bit sequence, thereby reducing the likelihood of long runs of identical bits and making the signal more statistically uniform. This randomization ensures that the power spectrum of the transmitted signal becomes independent of the specific input data, effectively mitigating spectral peaks and improving transmission efficiency [4].Scrambling enhances signal properties such as timing recovery and reduces the probability of synchronization issues, especially in systems employing clock recovery mechanisms**.**At the receiver end, descrambling is applied as the final step in the data recovery process. The descrambler reverses the scrambling operation and reconstructs the original bit sequence from the received scrambled bits, ensuring data integrity.

2.3 Reed-Solomon Encoder/Decoder

Following the scrambling stage, the randomized bitstream is passed to the Reed-Solomon (RS) Encoder, which forms a core component of Forward Error Correction (FEC) mechanisms in communication systems. Reed-Solomon coding is a powerful block-based error correction technique designed to detect and correct multiple symbol errors caused by noise, interference, or fading in the transmission channel [4].

In RS encoding, the input data is over-sampled, and a series of parity symbols are computed and appended to the original data sequence. This introduces redundant information into the message, enhancing its resilience against data loss or corruption during transmission, particularly in harsh channel conditions.

A Reed-Solomon code is typically denoted as:

$n=2^m - 1$----------(a)

$k=2^m$-1-2t----------(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

After Reed-Solomon error correction, the coded bits undergo an additional level of protection using a Convolutional Encoder. This encoder introduces further redundancy by transforming each input data symbol into a longer output symbol, thereby increasing the robustness of the transmitted data against errors caused by noise and interference.In a convolutional coding scheme, each group of mmm input bits is transformed into nnn output bits, where the code rate is given by m/nm/nm/n. Unlike block codes, this transformation is memory-based—meaning that the output not only depends on the current input bits but also on the previous kkk input symbols. This memory span kkk is referred to as the constraint length of the convolutional code [4].At the receiver end, the received convolutionally encoded bits are decoded using the Viterbi algorithm, a maximum likelihood decoding technique. The Viterbi algorithm is well-suited for decoding convolutional codes, especially when the constraint length k≤10k \leq 10k≤10, balancing performance and computational complexity. It effectively traces the most likely path through a trellis diagram to recover the original transmitted bitstream.

2.5 Interleaver / De-Interleaver

Interleaving is employed to mitigate the impact of burst errors during data transmission. Conceptually, the incoming bitstream is rearranged so that adjacent bits are no longer placed sequentially. In OFDM systems, this means that bits within an OFDM symbol are distributed across non-adjacent subcarriers, thereby spreading out the errors. This significantly improves error resilience, especially in noisy or fading environments.At the receiver, the De-Interleaver reorders the received bits back into their original sequence, enabling accurate decoding and error correction.

2.6 Constellation Mapper / De-Mapper

The Constellation Mapper converts interleaved bits into modulation symbols, which are mapped onto subcarriers using schemes such as BPSK, QPSK, or QAM. Each modulation technique defines a specific constellation diagram that determines how bits are grouped and represented in the complex plane.The De-Mapper, at the receiver, reverses this process—extracting the original bits from the received constellation points using demodulation.

2.7 Inverse Fast Fourier Transform (IFFT) / Fast Fourier Transform (FFT)

This is the core of the OFDM system. The IFFT converts frequency-domain data (amplitude and phase of each subcarrier) into a time-domain signal, thus enabling simultaneous transmission of multiple subcarriers with preserved orthogonality.At the receiver, the FFT performs the reverse transformation—converting the received time-domain signal back into the frequency domain for further demodulation and decoding [5].

2.9 Addition / Removal of Cyclic Prefix

To preserve subcarrier orthogonality and to combat intersymbol interference (ISI) caused by multipath propagation, a Cyclic Prefix (CP) is added. The CP is a copy of the last portion of an OFDM symbol appended to its beginning.This transforms linear convolution (caused by the channel) into circular convolution, allowing simple frequency-domain equalization. At the receiver, the CP is removed before the signal is processed by the FFT module.

2.10 AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric block cipher standardized by NIST in 2001, based on the Rijndael algorithm. AES operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits. It uses multiple rounds of substitution, permutation, mixing, and key addition operations to achieve high levels of security, performance, and flexibility [6].In this implementation, AES provides robust encryption for securing data during wireless transmission.

2.11 RSA Algorithm

Developed by Rivest, Shamir, and Adleman in 1978, the RSA algorithm is one of the first and most widely used public-key cryptographic systems. RSA is based on the computational difficulty of prime factorization, making it suitable for secure data exchange and digital signatures.Unlike AES, which is symmetric, RSA uses two keys: a public key for encryption and a private key for decryption [7][8].

2.12 ECC Algorithm

Elliptic Curve Cryptography (ECC) is a public-key encryption technique based on the algebraic **Flow Diagram Overview** structure of elliptic curves over finite fields. ECC provides the same level of security as RSA but with smaller key sizes, resulting in faster computation and lower power consumption—critical for mobile and wireless applications.

ECC was independently proposed by Victor Miller and Neal Koblitz in 1985 and is now widely used in applications requiring secure yet efficient cryptographic operations [10][11][12][13].

2.13 Hill Cipher Algorithm

The Hill Cipher, introduced by Lester S. Hill in 1929, is a classical symmetric key cipher based on linear algebra. It treats blocks of plaintext letters as vectors and encrypts them by matrix multiplication modulo 26.Each letter is mapped to a number (A=0, ..., Z=25), and blocks of nnn characters are multiplied by an invertible n×nn \times nn×n key matrix. The decryption process involves multiplying the ciphertext blocks by the inverse of the key matrix, again modulo 26 [14].

III. PROPOSED METHOD

In this paper, we propose an enhanced method for energy-efficient wireless data transmission using a combination of compression and encryption algorithms integrated into an OFDM-based communication system. The primary objective is to identify the most effective combination of encryption and compression techniques that minimizes energy consumption while maintaining data integrity, security, and transmission efficiency.

Multiple encryption algorithms, such as AES, RSA, ECC, and Hill Cipher, are evaluated in combination with standard compression algorithms to determine the optimal pair. This integrated model ensures data security and reduced transmission overhead, which results in energy optimization—a critical requirement for battery-powered and mobile devices.

The proposed system architecture consists of both transmitter and receiver components that incorporate the following operations:

Transmitter Side:

1. Input Data
   ↓
2. Scrambling
   ↓
3. Compression Algorithm
   ↓
4. Encryption Algorithm (AES/RSA/ECC/etc.)
   ↓
5. Reed-Solomon Encoding
   ↓
6. Convolutional Encoding
   ↓
7. Interleaving
   ↓
8. Constellation Mapping (e.g., QAM)
   ↓
9. IFFT (Inverse Fast Fourier Transform)
   ↓
10. Cyclic Prefix Addition
    ↓
11. OFDM Transmission over Wireless Channel

Receiver Side:

1. Received Signal from Wireless Channel
   ↓
2. Cyclic Prefix Removal
   ↓
3. FFT (Fast Fourier Transform)
   ↓
4. Constellation De-Mapping
   ↓
5. De-Interleaving
   ↓
6. Convolutional Decoding (Viterbi Algorithm)
   ↓
7. Reed-Solomon Decoding
   ↓
8. Decryption Algorithm
   ↓
9. Decompression Algorithm
   ↓
10. Descrambling
    ↓
11. Output Reconstructed Data

This architecture ensures that the transmitted data is compressed to reduce payload size, encrypted to ensure confidentiality, and error-protected using FEC techniques such as Reed-Solomon and

Convolutional codes. The use of OFDM as the modulation scheme further enhances the system's resilience to multipath fading and inter-symbol interference (ISI), while ensuring optimal use of bandwidth.

IV. FIGURES AND TABLES

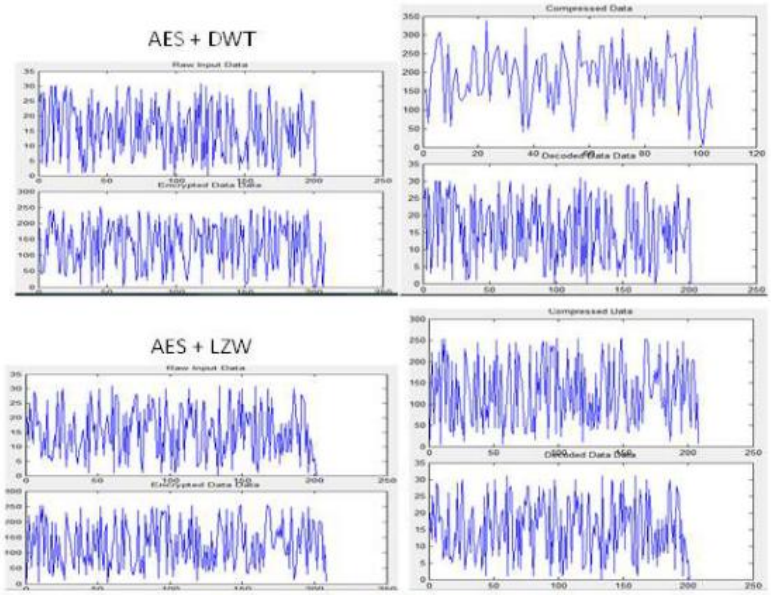

Fig.3. Result of Different Combination for the Encryption and Compression

	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	3.53sec	208	208	0.00%
	LZ	2.56sec	208	190	8.65%
HILL	RLE	3.10sec	1219	208	82.54%
	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	2.26sec	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 presented in this paper demonstrates an effective and efficient approach to energy optimization in wireless data transmission. By integrating multiple encryption and compression algorithms within an OFDM-based communication system, the framework successfully addresses the dual challenges of data security and energy efficiency.The experimental results validate that combining appropriate algorithms significantly improves transmission performance. In particular, the evaluation of various encryption and compression techniques revealed that the RSA algorithm for encryption, when used in conjunction with the Run-Length Encoding (RLE) compression method, offers the best results. This combination achieves a high compression ratio and minimal processing time for both transmitter-side (compression and encryption) and receiver-side (decompression and decryption) operations.Thus, the proposed system not only ensures secure data transmission but also contributes to energy-saving communication, which is especially valuable for power-constrained mobile and IoT devices. Future work can focus on expanding this study to include dynamic algorithm selection based on real-time network and energy parameters for even greater efficiency.

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