International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

A Novel Hybrid Security system for OFDM-PON using Highly Improved RC6 Algorithm and Scrambling

Rensu Elsa Chacko[1], Sruthi Maria Abraham[2], Hari s[3]

[1]PG Scholar, Dept. of ECE, Mount Zion College of Engineering, Kadammanitta
[2,3]Assistant Professor, Dept. of ECE, Mount Zion College of Engineering, Kadammanitta, Kerala, India

---

Abstract - *This paper proposes a scheme for security enhancement in the orthogonal frequency division multiplexing passive optical network (OFDM-PON) based on highly Improved RC6 algorithm and scrambling technique. Here the data stream is scrambled and then performs the highly improved RC6 algorithm to make the data encryption more secure. Scrambling using morlet wavelet method is efficient for altering the data in the spatial domain without losing the data. The highly improved RC6 algorithm is the modified version of the improved RC6 algorithm which is more beneficial and secure for the encryption process. By using scrambling along with the highly improved rc6 algorithm, encryption security standard will improve without any extra module with low complexity. Usage of MIMO-OFDM and SIC makes this system more attractive. We are also testing this system with the LTE communication system. After decryption, the signal loss is compensated by the signal enhancement at the receiver end.*

Key Words: **Orthogonal Frequency Division Multiplexing (OFDM), Highly Improved Rivest Cipher6 (hirc6) algorithm, Walsh Hadamard Transform**

1. INTRODUCTION

To meet the demands of next generation networks in optical communication systems, the orthogonal frequency division multiplexing passive optical network (OFDM-PON) [1] has introduced because of its spectral efficiency, flexibility and relatively high signal transmission capability [2]. Also communication security is becoming a great requirement in our society. Since the processes like encryption, decryption and authentication protocols are available, increasing security in transmission level is also a vital concern. Digital chaos algorithms [3] and analog chaos algorithms [4] are used at the physical layer to increase the security level of OFDM-PON systems. Noise like characteristics and sensitivity to initial parameters made the chaos algorithm more efficient for data transmission in a highly secure manner.

Pseudo random characteristics, huge parameter space [5], [6] and good compatibility with the digital signal processing technology make the digital chaos algorithm very suitable nowadays. Chaotic scrambling [7], [8], [9], chaotic constellation manipulation [10] and chaos IQ encryption techniques [11] are proposed and implemented in several papers. In chaotic coding, the QAM symbols are rotated in the constellation and its phases are changed, and at the same time the symbol to carrier or symbol to time mappings are not interrupted. In modern schemes, the iteration process is done by using floating point algorithm with high computational precision. The main disadvantage of the floating point algorithm includes its computational complexity and hence calculation speed is limited. So several OFDM frames uses same chaotic sequences, which reduces the security.

The RC6 algorithm [12] is a secure block cipher algorithm which was a final candidate project in the AES (Advanced Encryption Standard) project of the United States and NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project of Europe. The block cipher is classified into Feistel structure and SPN (Substitution Permutation Network) [13]-[14]. Fiestel structure uses the same algorithm between encryption and decryption whereas the SPN uses different algorithm between encryption and decryption. Therefore the SPN structure uses twice the area than Fiestel structure when implemented via hardware. The RC6 algorithm has a modified Fiestel structure and uses different algorithm between encryption and decryption. Thus it uses double space for implementation on hardware. So an improved version of RC6 is introduced which uses the same structure for encryption and decryption. The improved RC6 encryption algorithm is implemented by using a symmetric layer between encryption and decryption process. The symmetric layer is inserted by using simple rotation and XOR operations. Here the half of the whole algorithm performs encryption process and the rest performs decryption and in between these two the symmetric layer is introduced.

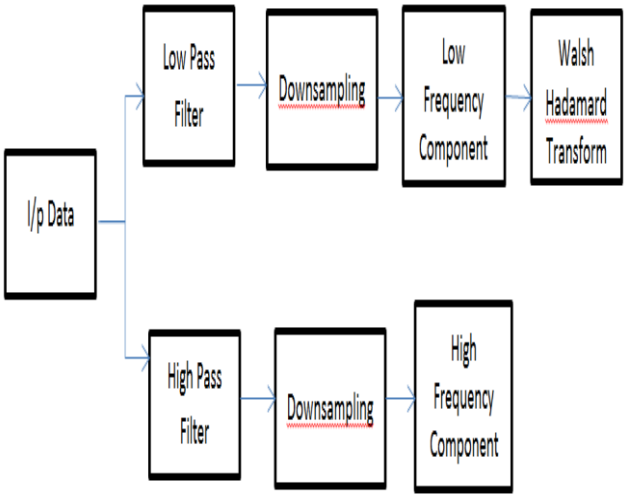
This paper introduces a highly improved RC6 (HIRC6) algorithm which increases the security of our system. Data integrity is the main concern in our modern world. Thus improving efficient RC6 algorithm makes our encryption standard security more efficient without using any extra module with low complexity. Here we are improving the algorithm by creating more security for two registers A and C and thus making it more efficient and secure. This paper also uses a technique called scrambling based on Morlet Wavelet transform for the secure transmission of data in OFDM-PON. The dynamical degradation problem is renovated by introducing the natural

impermanence of the data. Secure transmission of the encrypted OFDM signal is experimentally demonstrated. The low implementation complexity and high security performance necessities are considered here.

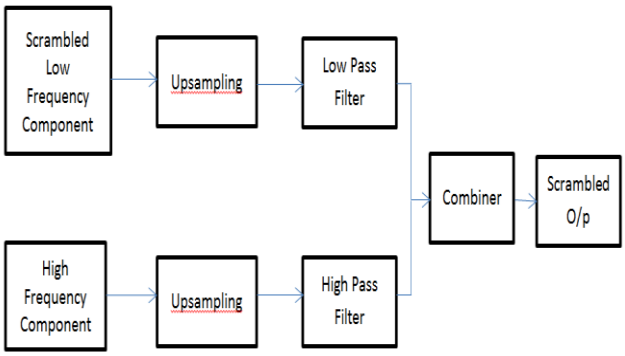
2. PRINCIPLE

The principle of this system is to first scramble the data using morlet wavelet and then do highly improved RC6 (HIRC6) encryption algorithm for high security. Implementing the two techniques together gives two tier security for our system. After scrambling operation the data is once encrypted and then doing encryption algorithm in this scrambled data makes our system double secure. Here, we are using an interleaver for increasing the random nature of our key which is used in the HIRC6 encryption technique. MIMO-OFDM and a Signal to Interference Canceller (SIC) is used which makes this system more efficient than the previous works.

The scrambling technique using morlet wavelet method is shown in the figure 1. The morlet wavelet splits the incoming data into two frequency domain as high frequency component and low frequency component by passing it through a high pass filter and a low pass filter. Then these are separately down sampled to reduce its size and then take the low frequency signals since it contains more number of information than high frequency. Then these low frequency signals are then shuffled using Walsh Hadamard transform. The walsh hadamard transform is a non sinusoidal, orthogonal transformation technique, which is used to scramble the data without any loss.Thus the data is encrypted once.



(a)



(b)

Figure: 1. (a) Scrambling based on morlet wavelet transform. (b) Reconstruction of the scrambled signal

The HIRC6 encryption and decryption algorithms are given below. Thus this scrambled data is again encrypted by using HIRC6 encryption technique. The scrambled data is stored in four registers named A, B, C and D and then performs the encryption. RC6 algorithm is symbolically presented as RC6-w/r/b in which w means the word size (32 bits), r denotes the number of rounds and b denotes the number of key (16 byte).

Six basic operations in RC6 are as follows:

1. a + b integer addition modulo 2^w
2. a - b integer subtraction modulo 2^w
3. a $\oplus$ b bitwise exclusive-or of w-bit words
4. a X b integer multiplication modulo 2^w
5. a<< >>b rotate the w-bit word a to the left by the amount given by the least significant lg w bits of b
6. a>><<b rotate the w-bit word a to the right by the amount given by the least significant lg w bits of b

HIRC6 Encryption Algorithm

B = B + S [0]

D = D + S [1]

for i = 1 to r do

t = (B X (2B + 1)) <<< lg w

u = (D X (2D + 1)) <<< lg w

A = ((A $\oplus$ t) <<< u) + S [2i]

A1 = ((A $\oplus$ t) <<< u) + S [2i]

A2= ((A $\oplus$ t) <<<u) + S [2i]

A=(A1+A2)/2

C = ((C $\oplus$ u) <<< t) + S [2i+ 1]

C1 = ((C ⊕ u) <<< t) + S [2i+ 1]

C 2= ((C ⊕ u) >>>t) + S [2i+ 1]

C=(C1+C2)/2

end

HIRC6 Decryption Algorithm

C = C – S [2r+3];

A = A – S [2r+2];

for i = r down to 1 do

{

(A, B, C, D) = (D, A, B, C)

u = (D* (2D + 1)) ⋘ lg w

t = (B *(2B + 1)) ⋘ lg w

C = ((C – S [2i+1]) ⋙ t) ⊕ u

A = ((A – S [2i]) ⋙ u) ⊕ t

}

D = D – S [1]

B = B - S[0]

3. BLOCK DIAGRAM

The below figure 2 shows the block diagram of the system. The key stream generation process is done by C program and the encryption and decryption process is done by offline MATLAB.

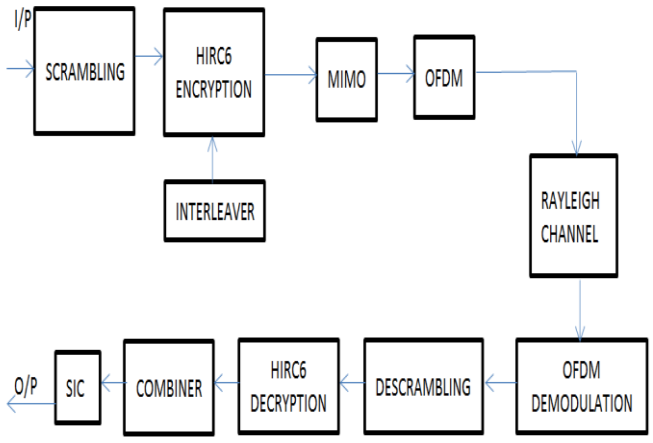


Figure 2: Block diagram of the system

In the block diagram, the input data is first scrambled using the morlet wavelet method. This includes walsh hadamard transform which is a non-sinusoidal, orthogonal transformation technique which makes the source data as a perturbed data for reducing the dynamical degradation problem. Then this scrambled data is encrypted by using the highly improved RC6 algorithm which makes the data secure. Encrypting data after scrambling process makes this system more resistant to eavesdroppers. Then it is transmitted using MIMO-OFDM, which has greatest spectral efficiency and thus delivers highest capacity and data throughput. It is transmitted through Rayleigh channel, which is a frequency varying channel that reduces channel noise and thus data can be decrypted easily. A combiner is used to combine data from the multiple antennas. Signal to interference canceller [SIC] is added for reducing interference at the receiver and can be used to reduce the effects of noises in the transmitted and received data.

4. RESULT

The experimental result is shown in figure 3. It shows the bit error rate (BER), symbol error rate (SER) and theory error rate. This result shows the performance of the system and here the BER and SER is small enough to show better performance of our system. Here, both the bit error rate and symbol error rate should be low when the signal to noise ratio increases. The black color line shows the theoretical value. The bit error rate is used to find the error between the received bits and original transmitted bits. The symbol error rate is used to find the error between received distorted symbol and original symbol. Thus the experimental result shows that the data encryption and decryption process are much secure and is well efficient.

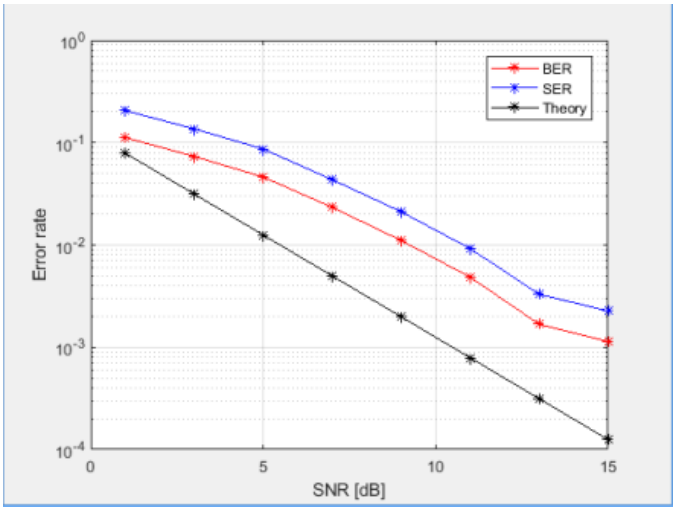


Figure 3: The experimental results showing bit error, symbol error and theory error rates curve with the improved performance of the system

5. CONCLUSIONS

Here we proposed a secure scheme for OFDM-PON based on highly improved RC6 encryption and scrambling with low computational precision. The dynamic generation of the key stream reduces the strength against attacks. Meanwhile, the dynamical degradation of the digital chaotic system is improved by introducing the endemic impermanence of the data source. The need for low implementation complexity and high security performance can be met together. This security upgraded OFDM-PON has potential applications in secure communications at the physical layer.

The main work in this paper includes, a technique scrambling using morlet wavelet is used with highly improved RC6 encryption algorithm for increasing security. Thus a two tier security is provided. Here MIMO-OFDM is used which increases the efficiency of the system. Using an interleaver instead of a pseudo random binary sequence [PRBS] generator increases the randomness of the data and makes it more secure transmission. Frequency varying channel for transmission is used which reduces the channel noise and thus the data can decrypted easily. Signal to interference canceller [SIC] is added for reducing interference at the receiver and can be used to reduce the effects of noises in the transmitted and received data.

REFERENCES

[1]. Shanshan Li, Mengfan Cheng, Lei Deng, Songnian Fu, Minming Zhang, Ming Tang, Ping Shum, and Deming Liu, “Secure Strategy for OFDM-PON Using Digital Chaos Algorithm with Fixed-Point Implementation”, IEEE Lightwave Technol. Vol. 36 , Issue. 20 , Oct.15, 2018.

[2]. N. Cvijetic, "OFDM for Next-Generation Optical Access Networks", J. Light wave Technol., vol. 30, no. 4, pp. 384-398, Feb. 2012.

[3]. B. Liu, L. Zhang, X. Xin and N. Liu, "Piecewise Chaotic Permutation Method for Physical Layer Security in OFDM-PON", IEEE Photonics Technol. Lett., vol. 28, no. 21, pp. 2359-2362, Nov. 1, 2016.

[4]. N. Jiang, D. Liu, C. Zhang and K. Qiu, "Modeling and Simulation of Chaos-Based Security-Enhanced WDM-PON", IEEE Photonics Technol. Lett., vol. 25, no. 19, pp. 1912-1915, Oct. 1, 2013.

[5] M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. Fu, P. Shum and D. Liu, "Enhanced Secure Strategy for OFDM-PON System by Using Hyperchaotic System and Fractional Fourier Transformation ", IEEE Photonics J., vol. 6, no. 6, Dec. 2014, Art. no. 7903409.

[6]. Z. Shen, X. Yang, H. He and W. Hu, "Secure Transmission of Optical DFT-S-OFDM Data Encrypted by Digital Chaos", IEEE Photonics J., vol. 8, no. 3, Jun. 2016, Art. no. 7904609.

[7] W. Zhang, C. Zhang, C. Chen, H. Zhang and K. Qiu, "Brownian Motion Encryption for Physical-Layer Security Improvement in CO-OFDM-PON", IEEE Photonics Technol. Lett., vol. 29, no. 12, pp. 1023-1026, Jun. 15, 2017.

[8] L. Zhang, X. Xin, B. Liu and X. Yin, "Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling", Opt. Exp., vol. 20, no. 26, pp. B32-B37, Nov. 2012.

[9] C. Zhang, W. Zhang, C. Chen, X. He and K. Qiu, "Physical-enhanced Secure Strategy for OFDMA-PON Using Chaos and Deoxyribonucleic Acid Encoding." J. Lightw. Technol., vol. 36, no. 9, pp. 1707-1712, May 1, 2018.

[10] J. Zhong, X. Yang and W. Hu, "Performance-Improved Secure OFDM Transmission Using Chaotic Active Constellation Extension", IEEE Photonics Technol. Lett., vol. 29, no. 12, pp. 991-994, Jun. 15, 2017.

[11]. W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin and K. Qiu, "Hybrid Chaotic Confusion and Diffusion for Physical Layer Security in OFDM-PON", IEEE Photonics J., vol. 9, no. 2, Apr. 2017, Art. no. 7201010.

[12]. Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, “An improved RC6 algorithm with the same structure of encryption and decryption”, Feb. 15-18, 2009 ICACT 2009.

[13]. H. Feistel, “Cryptography and Computer Privacy,” Scientific American, Vol.228, No.5, pp. 15-23, 1973.

[14]. C. E. Shannon, “Communication theory of secrecy system,” *Bell System Technical Journal,* Vol.28, No.4, pp. 656-715, 1949.