A Novel Hybrid Security system for OFDM-PON Using Digital Chaos and Scrambling with Fixed-Point Implementation

Rensu Elsa Chacko[1], Sruthi Maria Abhraham[2], Hari S[3]
[1,2,3] Mount Zion College of Engineering, Kadammanitta

Abstract- *This paper proposes a scheme for security improvement in the orthogonal frequency division multiplexing passive optical network (OFDM-PON) and LTE based on fixed-point digital chaos algorithm with low computational precision. In this paper aperiodic key streams are generated from a fixed-point chaos with its trajectory disturbed by the upstream data, and then used to encrypt the downstream data. Then in order to improve the security we have added scrambling to get two tire security and we have testing with the LTE communication system. After the decryption the loss is compensated by the signal enhancement at the receiver end.*

Keywords- Orthogonal Frequency Division Multiplexing (OFDM), Fixed point digital chaos algorithm.

I. 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 this scheme, 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.

Hence the fixed point algorithm is used to improve these disadvantages. But the dynamical degradation problem is not completely removed by using the fixed point algorithm only. Thus using the data source as the perturbation source is the main secret of this method to reduce the degradation problem. Otherwise the dynamical degradation problem may become a serious issue if the digital chaotic system based on a low precision fixed point algorithm is used.

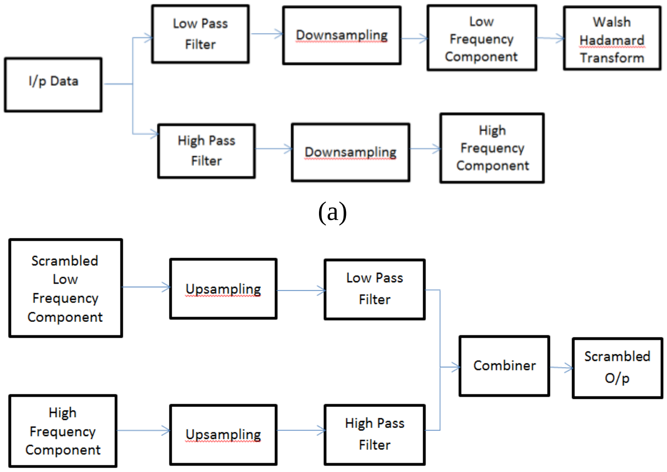
This paper introduces a digital chaotic system based on a fixed point algorithm with low calculation precision and a scrambling based on Morlet Wavelet transform for the secure transmission of data in OFDM-PON. The dynamical degradation problem is renovated by introducing the natural impermanence of the data. Secure transmission of the encrypted OFDM signal is experimentally demonstrated. The low implementation complexity and high security performance necessities are considered here.

II.PRINCIPLE

For hardware exertion, fixed point digital chaos algorithm is very helpful, although its performance gets reduced by the dynamical degradation. By introducing the permanence of the source data we can improve the dynamical degradation of the fixed-point chaos algorithm. The idea of using the upstream data as a key stream was first proposed by Cao et al. in [12]. The impermanence of the source data is used to generate different keys for encrypting the downstream data in separate OFDM frames. Yet definite security problems exist. The local statistical properties of the plaintext may not guarantee it to use as a direct encryption key. So many post processes can be performed on the plain text to make it as a good encrypted key stream. Hence by using the chaotic transformation, its nonlinearity behavior will help the plain text to be a good key stream and removes the local statistical problems. Most dynamical properties of the chaotic system may be removed in a quantized finite field phase space [13]. So the discretization of state space may remove chaos in digital systems. The chaotic dynamics may exist and is different from original chaotic system.

The principle of this system is to first scramble the data using morlet wavelet and then do chaos operation. After scrambling operation the data is once encrypted and then doing chaos 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 chaos operation, 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. Thus the data is encrypted once.



(a)

(b)

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

Figure 2 shows the chaotic operation done on the scrambled data. Then this scrambled data is again encrypted by using chaotic operation. The chaotic operation is done in two stages. First the data is splitted as upstream and downstream data. The upstream data is used to generate the original key by doing chaotic operation with the key generated by the interleaver. Then this original key is used to encrypt the downstream data by applying bit wise XOR operation. The decryption of this method is done by using the pre-stored upstream data in the receiver.

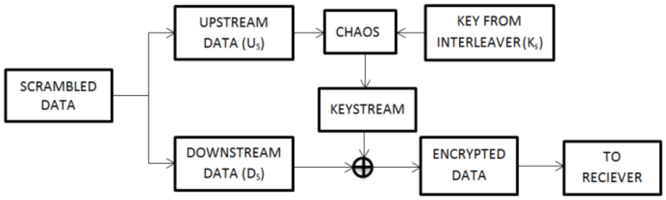


Figure: 2.Chaotic operation on scrambled data for increasing security.

III. BLOCK DIAGRAM

The block diagram of the system is given in the figure 3. The key stream generation process is done by C program and the encryption and decryption process is done by offline MATLAB.

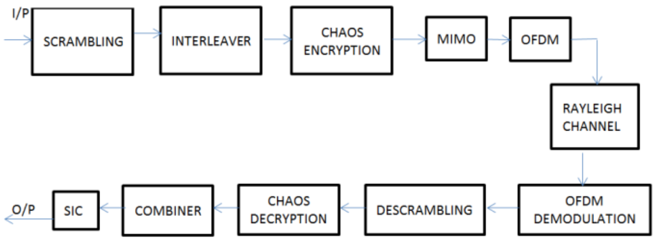


Figure 3: Block diagram of the system

The main advantages of this work includes the PON is cost effective have low energy consumption and has high transmission capacity. The OFDM-PON has high spectral efficiency, long reach access, vulnerable to various attacks and the secure problem should be taken into serious consideration. Here, the fixed point based implementation is used because it contains only integer value for chaos transformation. So output is in integer form and not in floating point. By using the module operation the encryption capacity is high and also the response time and computation is low because of fixed point algorithm.

The scrambling technique along with chaos algorithm makes this system more secure. MIMO-OFDM makes the signal transmission and reception capacity more efficient. 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.

IV. RESULTS

The experimental result is shown in figure 4. 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.

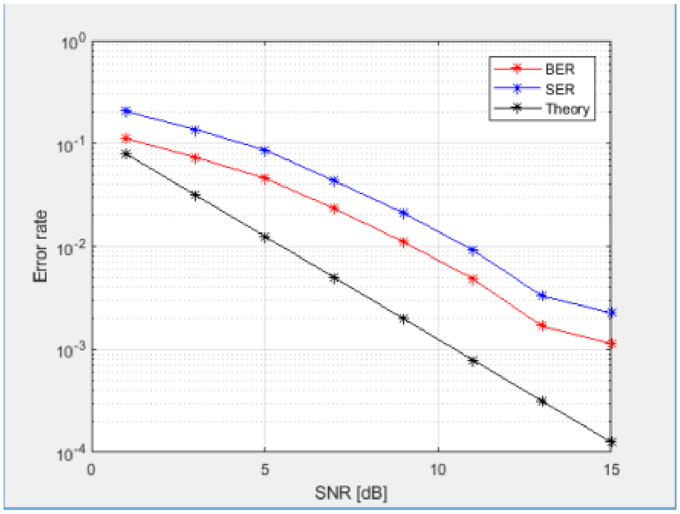


Figure 4: The experimental results showing bit error, symbol error and theory error rates curve with the improved performance of the system

V. CONCLUSION

Here we proposed a secure scheme for OFDM-PON based on random key stream encryption and a fixed-point digital chaos algorithm 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 chaos encryption 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.