Physical−Layer Data Encryption using Chaotic Constellation Rotation in OFDM−PON

Amber Sultan, Xuelin Yang*, Syed B. Hussain, Weisheng Hu
Shanghai Institute for Advanced Communication and Data Science,
State Key Laboratory of Advanced Optical Communication Systems and Networks,
Shanghai Jiao Tong University, Shanghai, 200240, China
**x.yang@sjtu.edu.cn*

Abstract*—Physical-layer data encryption schemes are required to enhance the data security during transmission in passive optical networks (PONs). Encryption schemes using digital chaos provide a huge key space which results in high-level security for the user data. Here, a novel physical-layer encryption scheme using chaotic radial constellation rotation is proposed and experimentally demonstrated for orthogonal frequency division multiplexing PON (OFDM-PON). A one-dimensional (1D) chaos is employed to generate the digital chaotic sequences for data encryption. The proposed encryption scheme offers less computational complexity due to the use of 1D chaos. The initial values are pre-shared between the optical line terminal (OLT) and optical network unit (ONU), which provide a key space of 10^{15}. At the OLT, the original data is firstly encrypted by a chaotic XOR operation, and then further encrypted using the chaotic phase offsets. This multi-fold encryption generates an overall key space of 10^{30}. The proposed encryption scheme is verified by experiments, where a 9.4-Gb/s encrypted 16 quadrature amplitude modulation (16-QAM) optical OFDM signal transmission is successfully carried over 20 km standard single-mode fiber (SSMF). The bit error rate (BER) of the received encrypted signal was calculated for a legitimate ONU as well as an illegal ONU. The encrypted OFDM signal is also compared with the original OFDM signal for performance analysis. The transmission performance is improved for the proposed encryption scheme due to the reason that the introduction of chaotic radial rotation reduces the effect of phase noise in the encrypted OFDM signals.

Keywords— Digital Chaos, Data Encryption, Passive Optical Networks (PON), Orthogonal Frequency Division Multiplexing (OFDM), Bit Error Rate (BER).

I. INTRODUCTION

Passive Optical Network (PON) is regarded as energy-efficient solution for the rapid growing demand in broad-band services [1, 2]. Orthogonal Frequency Division Multiplexing-PON (OFDM) has been proved as a promising format in future PON due to its excellent properties of flexible allocation of subcarriers, high spectral efficiency etc. [3]. However, downstream data in PON is confronted with data security issues due to its architecture. Current data encryption in media access control (MAC) layer is unable to protect the header/address of the transmitted data. In order to prevent data from being eavesdropped by an illegal ONU, data encryption techniques are required within physical-layer [4].

Digital chaos is characterized by their high sensitive dependence on its initial condition and long period of ergodicity, which is ideal to serve as data encryption techniques [5, 6]. Recently, a few schemes have been proposed using digital chaos encryption in physical-layer [7-10], which improves the high-level security, however at the cost of high complexities [11]. This paper proposes for the first time a physical-layer encryption technique using chaotic constellation rotation, where a random phase offset is applied to encrypt the original data by rotating the 16-QAM constellation of OFDM signals.

II. PRINCIPLE

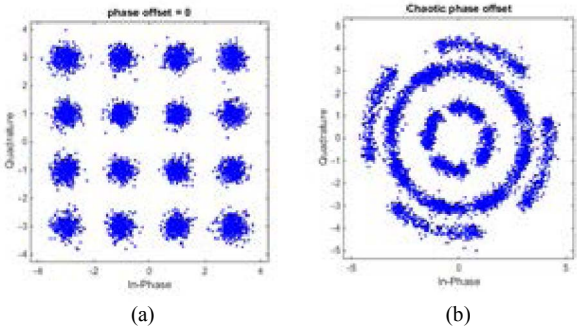
The data mapping comparison of the standard and the proposed chaotically rotated 16-QAM constellations is plotted in Fig. 1, where the phase offsets are chaotic and pre-determined for each data symbol. The chaotic phase offsets creates a radial constellation as shown in Fig. 1(b), thereby increasing the Euclidean distance between the constellation points, when compared with Fig. 1(a).

The schematic diagram of the proposed encryption technique is shown in Fig. 2. User data is randomly distributed using chaotic XOR operation to realize the first part of the proposed multi-fold encryption. Then, after serial-to-parallel (S/P) conversion the data is sent to the 16-QAM mapper, which maps the data on to the constellation points with pre-defined chaotic phase offsets to complete the encryption process.

A one-dimensional (1D) chaos [12], is used to obtain the chaotic digital sequences for both of the XOR operation and phase offsets, can be expressed as

$$x_{n+1} = \mu x_n(1-x_n),\ \mu \in (3.57, 4],\ x_n \in (0, 1) \qquad (1)$$

where n stands for the n-th iteration and μ is the bifurcation parameter. The use of 1D chaos reduces the complexity in the proposed encryption technique.



(a) (b)

Figure 1: Constellation comparison (a). Standard 16-QAM (Un-encrypted) and (b). chaotically-rotated 16-QAM (Encrypted).

978-1-5386-3564-3/18/$31.00 ©2018 IEEE

It is proved that after a certain iteration steps (~1000), the

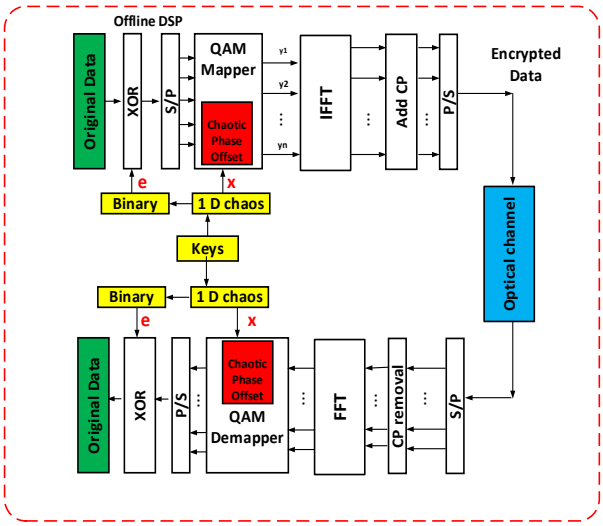


Figure 2: Block diagram of the encryption scheme.

1D chaos presents good pseudorandom chaotic behavior provided that μ is within the range (3.75, 4].

A binary chaotic sequence is required in the first part of encryption. This chaotic sequence is obtained by performing a binary digitalization process [13], which is presented as

$$e_i = \begin{cases} 0, & x_i \le 0.5 \\ 1, & x_i > 0.5 \end{cases} \quad (1 \le i \le n) \qquad (2)$$

The obtained binary integer, e_i, is XORed with the original binary data as

$$b_i = e_i \oplus d_i \qquad (3)$$

where $\oplus$ is the XOR operator and d_i is the i-th original data. From Eq. 3, the first part of data encryption is achieved.

To complete the encryption process, the chaotic sequences from Eq. 1 is used as the input of phase offsets in 16-QAM mapper. The phase offset results in the rotation of the corresponding constellation point by an angle determined by $\{x_n\}$. The introduction of the phase offset can be expressed as

$$y(i) = q(i)(\cos\varphi(i) + j\sin\varphi(i)) \qquad (4)$$

where $q(i)$ is the input signal and $\varphi(i)$ is the chaotic phase offset generated from Eq. 1.

Later, pilot data is inserted in order to estimate the channel at the receiver. Then, inverse Fast Fourier transform (IFFT), cyclic prefix (CP) insertion and parallel-to-serial (P/S) processing is done to modulate the encrypted OFDM signal on to the optical carrier. The receiver, having the pre-shared initial values will obtain the same chaotic sequence as that of the transmitter and will decrypt the received signal using the reverse of the encryption process, as shown in Fig. 2.

III. Experimental Setup

The experimental setup shown in Fig. 3 was used to verify the proposed encryption scheme for OFDM-PON. Experimental data was analyzed for two ONUs (legal and illegal). Encrypted OFDM signals were generated at OLT by offline MATLAB programs. A 512 point IFFT was used, of which 128 subcarriers were used to carry 16-QAM data and

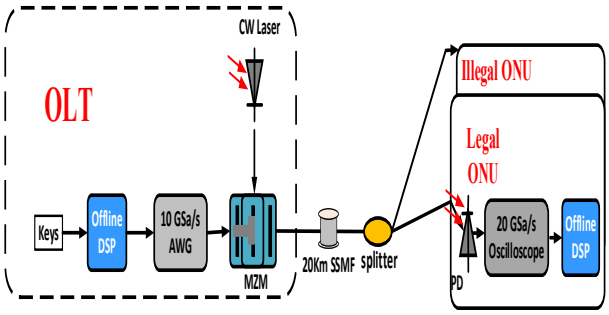


Figure 3: Experimental setup of the encryption scheme.

other 128 carried complex conjugate of the 16-QAM data to fulfill Hermitian symmetry. Cyclic prefix was set to 1/16 of the length of OFDM symbol to prevent inter symbol interference (ISI), and was loaded into the arbitrary waveform generator (AWG) with a 10-GHz sampling rate to generate the electric OFDM signals. The electric signals were then converted into optical signals through a continuous-wave laser operating at 1550 nm and an optical Mach-Zehnder modulator (MZM). These optical signals were then transmitted on 20 km standard single-mode fiber (SSMF). The signals were distributed to all of ONUs using a passive optical splitter. These optical OFDM signals were received via a 10 GHz photodiode (PD) and then sampled using a 20 Gs/s real-time oscilloscope. Offline processing in MATLAB was done to decrypt the received OFDM signals. The two initial values in 1D chaos, which served as the secret key, were set at x_o= 0.61854656454 and μ= 3.9955454875. These chaotic initial keys were pre-shared between the OLT and legal ONU only.

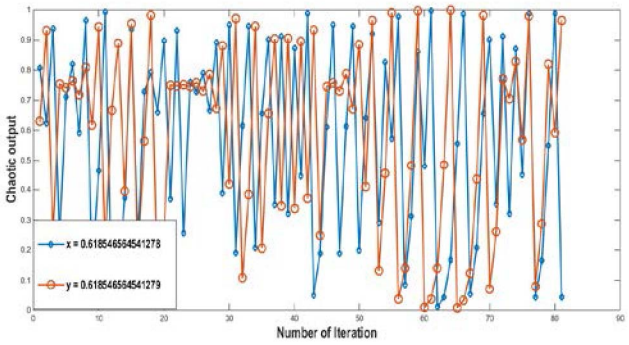


Figure 4: Chaotic sequences under a tiny change in the initial value.

IV. Results

The pseudorandom characteristics of the 1D chaos ensure the high-level security in the proposed scheme. The key sensitivity of the 1D chaos used is shown in Fig. 4. It can be seen that, a tiny discrepancy (~10^{-15}) in the initial value, $\{x_n\}$, creates an entire different chaotic output sequence. Thus, an illegal ONU will not be able to correctly extract the original data from the received signal.

To further evaluate the feasibility of the proposed scheme, the bit error rate (BER) performances for both back-to-back (b2b) and after 20 km SSMF transmission are depicted in Fig. 5, for the original and encrypted OFDM signals. The BER curves and the corresponding received 16-QAM constellations

for an illegal ONU and legal ONU are also shown in Fig. 5. The encrypted signals were correctly recovered at -7 dBm (BER@10^{-3}) by the decryption process. However, for an illegal ONU the BER remained >0.5 for all received optical powers. Therefore, an illegal ONU will not get any useful information from the received OFDM signals. Furthermore, from Fig. 5 it can be seen that, the BERs of the encrypted signal is improved if compared to the original OFDM signal. This improvement is due to the increased Euclidean distance between the constellation points. This increase in distance reduces the effect of phase noise. The chaotic system generates a random-like phase offset for each data symbol, based on the pre-shared initial values, while only the legal ONU knows the precise phase offsets for each of the incoming OFDM symbols, and therefore can recover the original information embedded in the complex radial constellation.

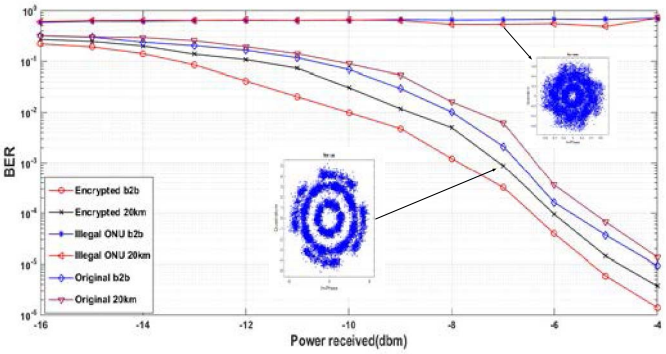


Figure 5: BER comparisons of encrypted and original OFDM signal.

V. Conclusion

A novel physical-layer encryption scheme using chaotic constellation rotation is proposed and experimentally demonstrated. The use of 1D chaos makes this encryption scheme less complex as compared to previous schemes using hyper chaos. An overall key space of 10^{30} is created using 1D chaos. A successful experiment to transmit 9.4 Gb/s, 16-QAM encrypted OFDM signals over 20 km SSMF proves the feasibility and the computational efficiency of the proposed encryption scheme, which could be an excellent candidate for next-generation secure OFDM- PON.

Acknowledgment

This work was supported in part by International S&T Cooperation Program of China, 2016YFE0104500, National Natural Science Foundation of China under Grants 61571291, 61431009 and 61221001.

References

[1] Kani, Jun-ichi, et al. "Next-generation PON-part I: Technology roadmap and general requirements." IEEE Communications Magazine 47.11 (2009).

[2] Chen, Chen, et al. "Tunable optical frequency comb enabled scalable and cost-effective multiuser orthogonal frequency-division multiple access passive optical network with source-free optical network units." Optics letters37.19 (2012): 3954-3956.

[3] Cvijetic, Neda. "OFDM for next-generation optical access networks." Journal of lightwave technology 30.4 (2012): 384-398.

[4] Fok, Mable P., et al. "Optical layer security in fiber-optic networks." IEEE Transactions on Information Forensics and Security 6.3 (2011): 725-736.

[5] Argyris, Apostolos, et al. "Chaos-on-a-chip secures data transmission in optical fiber links." Optics express 18.5 (2010): 5188-5198.

[6] van Turnhout, Maarten, and Florian Bociort. "Chaotic behavior in an algorithm to escape from poor local minima in lens design." Optics express 17.8 (2009): 6436-6450.

[7] Liu, Bo, et al. "Piecewise chaotic permutation method for physical-layer security in OFDM-PON." IEEE Photonics Technology Letters 28.21 (2016): 2359-2362.

[8] Zhang, Lijia, Bo Liu, and Xiangjun Xin. "Secure coherent optical multi-carrier system with four-dimensional modulation space and Stokes vector scrambling." Optics letters 40.12 (2015): 2858-2861.

[9] Cheng, M., et al. "Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation." IEEE Photonics Journal 6.6 (2014): 1-9.

[10] Deng, Lei, et al. "Secure OFDM-PON system based on chaos and fractional Fourier transform techniques." Journal of Lightwave Technology 32.15 (2014): 2629-2635.

[11] Zhang, Wei, et al. "Hybrid Chaotic Confusion and Diffusion for Physical-layer Security in OFDM-PON." IEEE Photonics Journal 9.2 (2017): 1-10.

[12] Liu, Lingfeng, et al. "Pseudorandom bit generator based on non-stationary logistic maps." IET Information Security 10.2 (2016): 87-94.

[13] Bi, Meihua, et al. "A Key Space Enhanced Chaotic Encryption Scheme for Physical-layer Security in OFDM-PON." IEEE Photonics Journal 9.1 (2017): 1-10.