ISSN (e): **2250 – 3005** || *Volume, 07* || *Issue, 08*|| *August – 2017* ||
International Journal of Computational Engineering Research (IJCER)

Chaos Coding-Based QAM IQ-Encryption For Improved Security In OFDMA-PON

[1]SANKARSAN SAHU, [2]SOUMYA RANJAN PRADHAN
Gandhi Institute of Excellent Technocrats, Bhubaneswar
Kalam Institute of Technology,Berhampur, Ganjam, Odisha, India

ABSTRACT:
In this letter, we propose a quadrature amplitude modulation (QAM) encryption method based on chaos coding for security improvement in orthogonal frequency-division multiple access-based passive optical network (OFDMA-PON) systems. In the encrypted QAM symbols, the real (I) and imaginary (Q) parts are separately coded with key sequences, which are generated by a modified Logistic mapping. Iteration parameters of the mapping formula are set as the security keys, which are determined in each optical network unit (ONU) and then sent to optical line terminal (OLT). The key sequences for different ONUs are generated with their corresponding security keys. According to the subcarrier allocation information, downstream signal is encrypted in the OLT and then decrypted in each ONU with distinct key sequences. Encryption of 10-Gb/s 16QAM OFDM and 12.5-Gb/s 32QAM OFDM signals has been successfully implemented over 30-km standard single mode fiber in the security improved OFDMA-PON.
Index Terms—Passive optical network (PON), orthogonal frequency-division multiple access (OFDMA), quadrature amplitude modulation (QAM), chaos encryption.

I. INTRODUCTION

DRIVEN by the ever-increasing data traffic of diversified services nowadays, the bandwidth and capability requirements are rapidly growing in passive optical networks (PONs) [1], [2]. Orthogonal frequency-division multiple access (OFDMA) technology is a prominent candidate to meet these requirements in the future optical access networks, due to its inherent advantages such as high spectral efficiency, strong tolerance to fiber dispersion, flexible resource allocation and potentially low cost [3]. Therefore, OFDMA-PON has been widely investigated in recent years [2]–[4]. In a typical
OFDMA-PON, downstream signal coming from the optical line terminal (OLT) is broadcasted to all the optical network units (ONUs). As a result, malicious users can be disguised as legitimate ONUs to eavesdrop useful information from the downstream signal. Moreover, there are also other security threats such as jamming, physical infrastructure attacks, and interception [5]. In consequence, security is of great importance in an OFDMA-PON system.
So far, several technologies have been proposed to improve the security of an OFDM-PON. Conventional MAC-layer encryption method encrypts the cryptographic protocols at the high-layer, but lefts the control data or headers unprotected. This is a risky practice to build security on top of an insecure foundation [5], [6]. Physical layer encryption has also been proposed to secure the OFDM-PON, which can prevent the network against threats at the lowest layer. Recently, a few signal encryption and decryption methods in OFDM-PON systems have been studied, such as constellation masking, chaotic scrambling and chaotic permutation [7]–[9]. However, in these schemes, the interleaving of time domain and/or frequency domain information has a high implementation complexity.
In this letter, we propose a chaos coding based physical layer encryption scheme for the OFDMA-PON. In this scheme, a pair of key sequences is utilized to code the real (I) and imaginary (Q) parts of quadrature amplitude modulation (QAM) symbols, respectively. The key sequences are generated by a modified Logistic mapping. Owning to the properties of the chaotic map such as ergodicity, high sensitivity to initial conditions and control parameter, the generated key sequences have a good random feature while the complexity of this process is relatively low. In our work, a 10 Gb/s 16QAM OFDM signal and a 12.5 Gb/s 32QAM OFDM signal are successfully encrypted in an OFDMA-PON.

II. PRINCIPLE OF THE PROPOSED SCHEME

Fig 1(a) illustrates the principle of security key transmission and key sequence generation. Iteration parameters of the modified Logistic mapping are used as security keys. They are determined and stored in each ONU, then sent to the OLT within the encrypted upstream signal. In the OLT, the received parameters are used to generate key sequences. The principle of encryption in the OLT and decryption in the ONUs is shown in Fig. 1(b). We assume that there are L ONUs and M subcarriers in the system. These subcarriers are separated into L groups and each group, which is used by a corresponding ONU, can have different number of subcarriers. The data

ZHANG et al.: CHAOS CODING-BASED QAM IQ-ENCRYPTION 1965

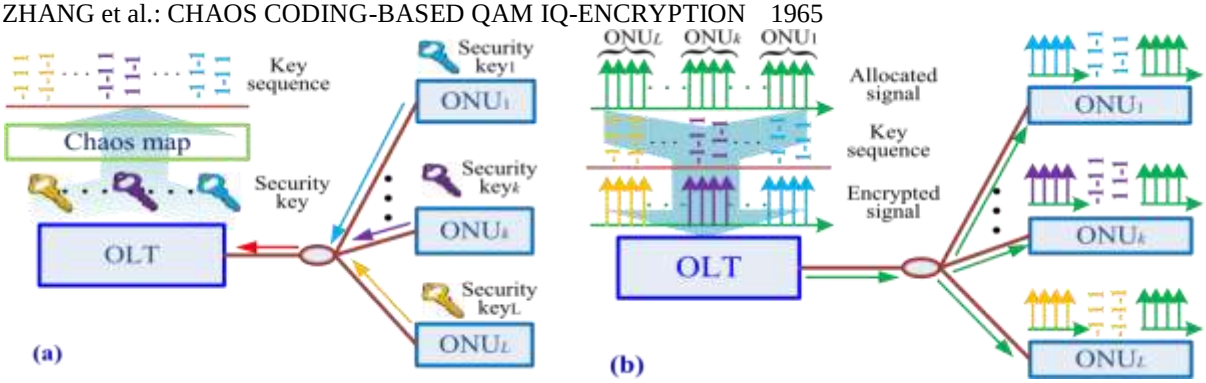

Fig. 1. (a) Principle of security key transmission and key sequence generation. (b) Diagram of encryption in the OLT and decryption in the ONUs.

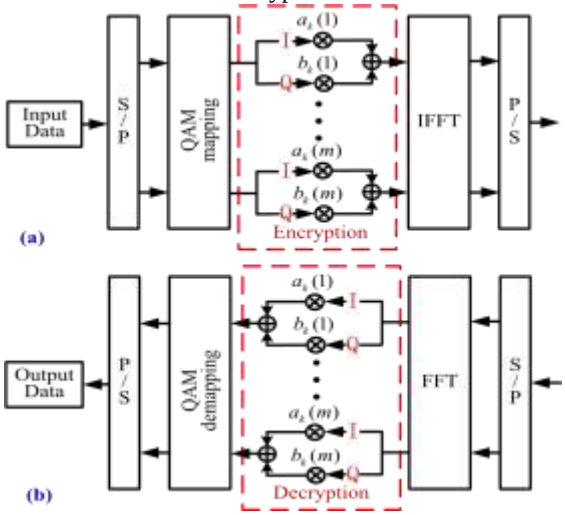

Fig. 2.(a) Encryption principle for ONUkin the OLT, (b) decryption principle in the ONUk.

for each ONU are embedded in the corresponding subset of subcarriers and then encrypted by using its own key sequences. At the ONU side, after receiving the downstream signal, each ONU extracts its own allocated subcarriers according to the subcarrier allocation information, and then decrypts the downstream signal by using the key sequences generated with the stored security key. One ONU cannot decrypt the other ONU's signal due to the lack of correct key sequences. Therefore, the communication security of an OFDMA-PON can be guaranteed by using this scheme.

For a specific ONU_k, we assume that a subset of m subcarriers is allocated to it. The encryption principle for ONU_kin the OLT and the corresponding decryption principle in the $ONU_k$are shown in Figs. 2(a) and (b), respectively. After serial-to-parallel conversion (S/P), the input data are mapped to the QAM symbols. Then, the obtained QAM symbols are divided into I and Q parts. The encryption is performed by multiplying I and Q parts of the QAM symbols by a pair of key sequences separately, which can be represented as

$$C_k(i) = \mathrm{Re}(W_k(i)) \cdot a_k(i) + j\mathrm{Im}(W_k(i)) \cdot b_k(i) \quad (1)$$

where $W_k(i)$ is the input QAM symbol on the i-th subcarrier in $ONU_k$with i = 1,2,..., m. $a_k(i)$, $b_k(i) \in \{1, -1\}$are the elements of two different key sequences, which are generated by a chaotic map. This encryption process can avoid complex multiplications and thus can be easily implemented. Here, we adopt a modified Logistic mapping [10] as the chaos model, which has the following iterative formula $x_n+1 = f(x_n) = 1 - \mu x_n^2, \mu \in [1.40015,2], x_n \in (-1,1)$

(2) $s_n = \mathrm{sgn}(x_n)$ (3)

where$\mathrm{sgn}(\cdot)$ denotes the sign function and $s_n$is the n-th element of the generated chaotic sequence. $x_n$is the n-th state value of (2), x_0 is an arbitrary value between -1 and 1, and μ is the bifurcation parameter. Normally, it has been proved that the system evolution will fall into chaos when $\mu \in [1.40015, 2]$. As in practical applications, some initial iterated values $\{x_n, n = 1,2,..., N\}$ are abandoned, where
N is iteration step. In this scheme, the initial value x_0, the bifurcation parameter μ and iteration step N are used as the security keys. After iteration with a certain step N, the formula falls into the fully chaotic domain and the sequence $a_k$can be obtained by (3). Then, the sequence is split into m columns as $(a_k(1),..., a_k(m))'$ and m is equal to the number of subcarriers. $(b_k(1),..., b_k(m))'$ is also generated in this way but with different iteration parameters. After that, these two sequences are utilized to code the QAM symbols by (1). To encrypt the next OFDM symbol, the iteration step is updated to N + m to generate another pair of sequences. For $ONU_k$with a subset of m subcarriers, assume that the i-th subcarrier in this subset is $f_{l(i)}$, where l(i) is the subcarrier index in the system, thus the encrypted OFDM symbol can be expressed as

$$S_k(t) = C_k(i) \cdot \exp\left(j\frac{2\pi(l(i)-1)(t-1)}{M}\right), \quad 1 \le t \le M$$

$$\sum_{i=1}^{m}$$

(4) where $C_k(i)$ is the encrypted QAM symbol and t is the discrete time index. At the ONU side, the decryption principle is analogous to the encryption process

$$W_k(i) = \mathrm{Re}\, C_k(i) \cdot a_k(i) + j\mathrm{Im}C_k(i) \cdot b_k(i) \qquad (5)$$

where$C_k(i)$ is the output of the fast Fourier transform (FFT) corresponding to the i-th subcarrier in ONU_k. The length m of $C_k$is detected and then $a_k$and $b_k$with the same length are generated using the stored security keys by (2) and (3). After that, the iteration step is updated to N+mand the next OFDM symbol can also be decrypted. With the synchronization of OFDM symbols, synchronous encryption and decryption operations in the

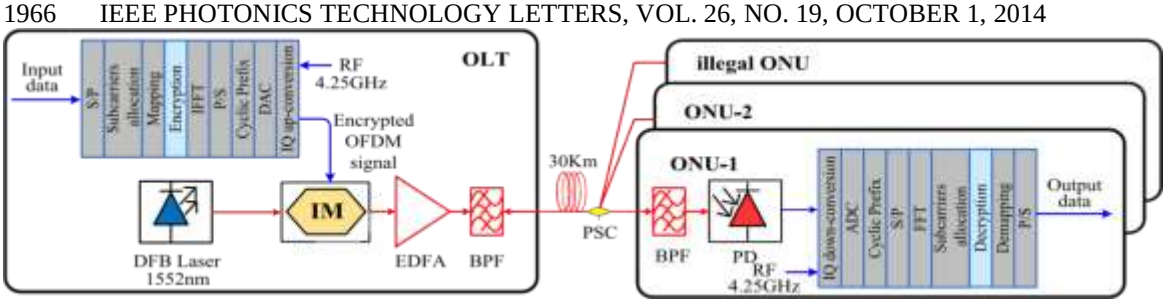

Fig. 3. The setup of the proposed secure OFDMA-PON (IM: intensity modulator; PSC: power splitter/coupler; PD: photodiode; RF: radio frequency).

OFDMA-PON can be successfully performed. Furthermore, different ONUs can only decrypt their own encrypted data by using their own key sequences, which are generated with the same security keys as at the OLT side. Since an illegal ONU cannot obtain any information about the security keys and the key sequences of other ONUs, the physical layer security of an OFDMA-PON can be greatly enhanced. According to the principle of encryption and decryption, only a two-bit key sequence and two additional multiplications are needed to code the I and Q parts of a QAM symbol, no matter what level the QAM symbol is. Compared with the traditional methods, this method needs less key sequence bits and less multiplication operations. Therefore, the encryption efficiency of our proposed scheme is high while the implementation complexity is relatively low.

III. SYSTEM SETUP

The setup of the proposed physical layer encrypted OFDMA-PON is shown in Fig. 3. We perform the simulation using VPI transmission-Maker Version 8.3. The OFDM modulation and the I-Q encryption are executed by Matlab program offline. The number of OFDM subcarriers is 128 and the DC subcarrier f_0 is not used for data transmission. For simplicity, two subsets of subcarriers f_1- f_{63} and f_{64}- f_{127} are allocated for ONU_1 and ONU_2, respectively. The bandwidth of OFDM signal is 3 GHz. Thus each ONU has a bit rate of about 5 Gb/s when employing 16QAM mapping and about 6.25 Gb/s for 32QAM mapping. Cyclic Prefix (CP) is set to 1/16 of the length of an OFDM symbol. The baseband OFDM signal is firstly up-converted to 4.25 GHz and then intensity modulation with direct detection (IM/DD) is realized in the optical domain. A 1552 nm distributed feedback (DFB) laser and a Mach-Zehnder modulator (MZM) are used to produce the double side-band (DSB) optical OFDM signal. After an Erbium-doped optical fiber amplifier (EDFA) and a band-pass filter (BPF), a single side-band (SSB) optical OFDM signal with about -9.7 dBm transmitted optical power is generated and then launched into a 30 km standard single mode fiber (SSMF). After a BPF and a photodiode (PD) in each

ONU, the obtained optical OFDM signal is converted to an electrical signal and then the obtained 4.25 GHz OFDM signal is down-converted to the baseband. According to the subcarrier allocation information, the corresponding subset of

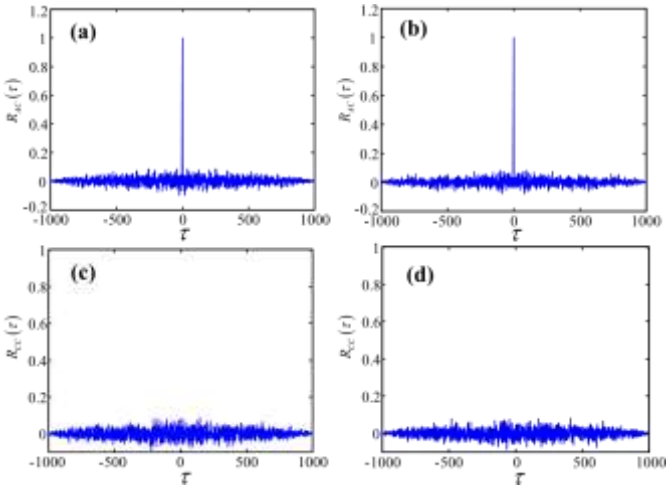

Fig. 4. Auto-correlation and cross-correlation of the chaos sequences, (a) auto-correlation for x0 = 0.655007, N = 1000; (b) auto-correlation for x01000= 0.6550080.655008,,NN == 1000; (2000; (d) cross-correlation for xc) cross-correlation for x00 == 0.6550080.655007, and x0 = and N = 2000.

N =

subcarriers is selected by each ONU after the FFT. Finally, the obtained encrypted signal is decrypted and demodulated.

IV. RESULTS AND DISCUSSIONS

The random characteristic of key sequences is very import to ensure the security of the proposed encryption method. The auto-correlation and cross-correlation functions of the chaotic key generation with different initial value x_0 and different iteration step N are studied to verify this random characteristic. Here, for the generated chaos sequences $b_h$and $b_j$with length D, which is set to 1000, the normalized auto-correlation and cross-correlation functions of them are defined by

$$\text{D 1} = \frac{1}{D}\sum^{-} \quad R_{ac}(\tau)b_j(n)b_j(n+\tau), -(D-1) \le \tau \le D-1$$

n=0

(6)

$$\text{D 1} = \frac{1}{D}\sum^{-} \quad R_{cc}(\tau)b_h(n)b_j(n+\tau), -(D-1) \le \tau \le D-1$$

n=0

(7)

In this letter, the bifurcation parameter μ is set to 2. Figs. 4(a) and (b) show the auto-correlation functions of the chaos sequences for N = 1000, x_0 = 0.655007 and

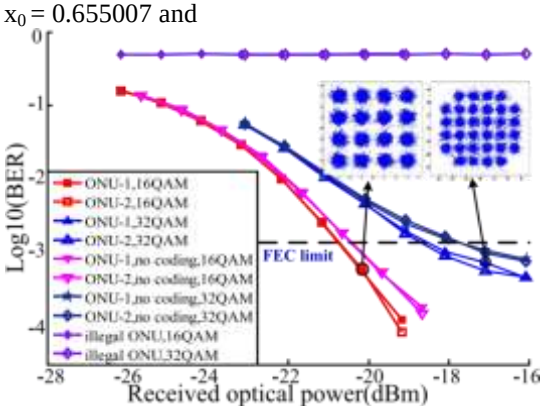

Fig. 5. BER performance and the corresponding constellations of 16-QAM and 32-QAM OFDM signals.

N = 2000, x_0 = 0.655008, which are utilized as the security keys for ONU_1 and ONU_2, respectively. It can be seen that when $\tau = 0$, the value of the auto-correlation functions of the key sequences are very small (around zero). The cross-correlation functions of the chaos sequences for N = 1000, x_0 = 0.655007 and x_0 = 0.655008 as well as

N = 1000 and N = 2000, x_0 = 0.655008 are represented in Figs. 4(c) and (d). Here N = 1000 and x_0 = 0.655008 are set as the security keys utilized to eavesdrop the information from ONU_1 by an illegal ONU. The values of cross-correlation functions are also around zero for all values of τ. As a result, the generated sequences have a quite good random feature which is fundamentally important to cryptosystems. If the adversary knows the modulated symbols M_k, both $a_k$and $b_k$can be recovered from (1). However, the adversary only knows a subset of the messages and only some segments of the sequences can be recovered. Moreover, the random characteristic and timeslot-varying security keys can guarantee that the recovered key sequences in one time slot cannot be used to decrypt the encrypted signal in another time slot. In this case, this encryption method is expected to be more resistant against the known plaintext and cipher-text attack. Then, the exhaustive search for brute-force attack from an illegal ONU is also considered. In this letter, for key sequences $a_k$and b_k, the security keys can be expressed as $\{x_0^a, \mu^a, N^a, x_0^b, \mu^b, N^b\}$. $x_0$and μ can be arbitrary values in (-1, 1) and [1.40015, 2], respectively. It has been shown in Fig (4) that $R_{ac}$and $R_{cc}$are sensitive to 10^{-6} difference for x_0. Therefore, the key space size will be above 4×10^{34}, which is much larger than 2^{100} and thus can provide a sufficient security against brute-force attacks [11]. In addition, the security keys are timeslot-varying, which will introduce an exponential growth of the exhaustive trial for the illegal receiver. Consequently, this scheme reveals significant potential to efficiently resist the brute-force attack.

The bit-error-rate (BER) performance of both regular and illegal ONUs is depicted in Fig. 5. It is observed that two legal ONUs, ONU_1 and ONU_2, they have nearly the same performance for both 16QAM and 32QAM cases. The original data have been well recovered after decryption and demodulation. However, for the illegal ONU, a BER of above 0.5 has been observed which indicates that it cannot extract any useful information from downstream signal. Moreover, compared with the case that no chaos coding is performed, there are power gains of about 0.3 dB and 0.5 dB for 16QAM and 32QAM OFDM signals, respectively. It is believed that the observed power gains are mainly contributed by the coding gain of chaos encoding. The received constellation diagrams of 16QAM and 32QAM OFDM signals in ONU_1 are also shown as inset in Fig. 5.

V. CONCLUSION

We have proposed and verified a novel QAM IQ-encryption method to effectively improve the physical layer security of an OFDMA-PON. The modified Logistic map is adopted as the key sequence generator. A 10 Gb/s 16QAM OFDM signal and a 12.5 Gb/s 32QAM OFDM signal using the proposed encryption method have been successfully implemented for two legal ONUs and one illegal ONU, to verify the feasibility of our proposal. The obtained results prove that the generated key sequences have a good random characteristic and the proposed encryption method can effectively prevent eavesdropping from any illegal ONUs. Furthermore, this encryption method has high encryption efficiency and low implementation complexity. Hence, the proposed encryption method is quite promising for the security improvement in future OFDMA-PON systems.

REFERENCES

[1] J.-I. Kaniet al., "Next-generation PON—Part I: Technology roadmap and general requirements," IEEE Commun. Mag., vol. 47, no. 11, pp. 43–49, Nov. 2009.

[2] C. Chen, C. Zhang, D. Liu, K. Qiu, and S. Liu, "Tunable optical frequency comb enabled scalable and cost-effective multiuser orthogonal frequency-division multiple access passive optical network with sourcefree optical network units," Opt. Lett., vol. 37, no. 19, pp. 3954–3956, Oct. 2012.

[3] N. Cvijetic, "OFDM for next-generation optical access networks," J. Lightw. Technol., vol. 30, no. 4, pp. 384–398, Feb. 15, 2012.

[4] C. Chen, C. Zhang, Y. Feng, and K. Qiu, "Bidirectional radio frequency up-converted orthogonal frequency-division multiple access passive optical network with novel source-free optical network units using four-wave mixing in semiconductor optical amplifier," IEEE Photon. Technol. Lett., vol. 24, no. 24, pp. 2206–2209, Dec. 15, 2012.

[5] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[6] A. Harris, D. R. Jones, K. H. Horbatuck, and A. Sierra, "A novel wavelength hopping passive optical network (WH-PON) for provision of enhanced physical security," J. Opt. Commun. Netw., vol. 4, no. 3, pp. 289–295, Mar. 2012.

[7] B. Liu, L. Zhang, X. Xin, and Y. Wang, "Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation," IEEE Photon. Technol. Lett., vol. 26, no. 2, pp. 127–130, Jan. 15, 2014.

[8] L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure OFDM-PON based on chaos scrambling," IEEE Photon. Technol. Lett., vol. 23, no. 14, pp. 998–1000, Jan. 15, 2011.

[9] L. Zhang, B. Liu, X. Xin, Q. Zhang, J. Yu, and Y. Wang, "Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation," J. Lightw. Technol., vol. 31, no. 1, pp. 74–80, Jan. 1, 2013.

[10] G. Heidari-Bateni and C. D. McGillem, "Chaotic sequences for spread spectrum: An alternative to PN-sequences," in Proc. IEEE ICSTWC, Jun. 1992, pp. 437–440.
[11] G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," Int. J. Bifurcation Chaos, vol. 16, no. 8, pp. 2129–2151, Mar. 2006.