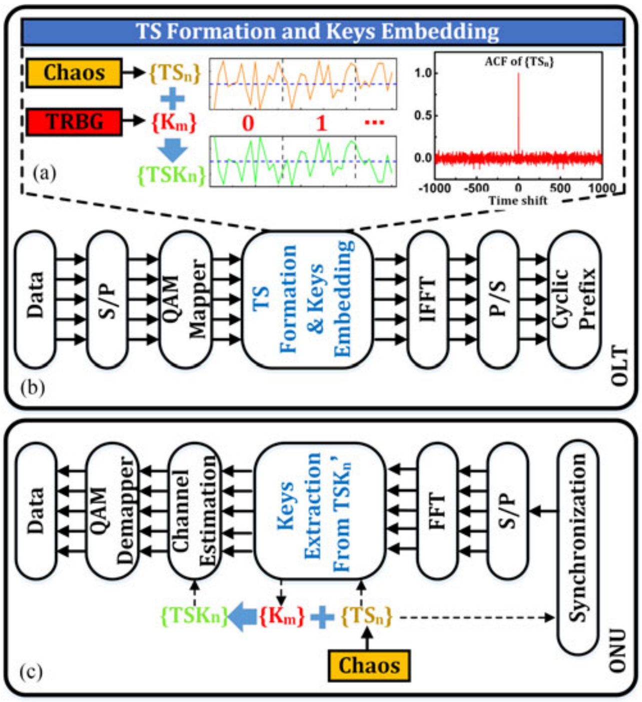
IEEE Photonics Journal
An IEEE Photonics Society Publication

Secure Key Distribution Strategy in OFDM-PON by Utilizing the Redundancy of Training Symbol and Digital Chaos Technique

Volume 10, Number 2, April 2018

Shanshan Li
Mengfan Cheng
Lei Deng
Songnian Fu
Minming Zhang
Ming Tang
Ping Shum, *Senior Member, IEEE*
Deming Liu



DOI: 10.1109/JPHOT.2018.2815001
1943-0655 © 2018 IEEE

Secure Key Distribution Strategy in OFDM-PON by Utilizing the Redundancy of Training Symbol and Digital Chaos Technique

Shanshan Li, Mengfan Cheng,[1] Lei Deng,[1] Songnian Fu,[1] Minming Zhang,[1] Ming Tang,[1] Ping Shum,[2] *Senior Member, IEEE*, and Deming Liu[1]

[1]Next Generation Internet Access National Engineering Lab (NGIA), School of Optoelectronic Science and Engineering, Huazhong University of Science & Technology (HUST), Wuhan 430074, China
[2]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 637553

DOI:10.1109/JPHOT.2018.2815001

Manuscript received December 1, 2017; revised March 6, 2018; accepted March 8, 2018. Date of publication March 12, 2018; date of current version March 30, 2018. This work was supported in part by the National Nature Science Foundation of China under Grant 61505061 and Grant 61675083, by the National “863” Program of China under Grant 2015AA016904, and in part by the Fundamental Research Funds for the Central Universities HUST under Grant 2017KFYXJJ034. Corresponding author: Mengfan Cheng (e-mail: chengmf@mail.hust.edu.cn).

Abstract: A secure key distribution scheme for orthogonal frequency division multiplexing (OFDM) passive optical network system is proposed and experimentally demonstrated. The training symbol (TS), which is used for time synchronization and channel estimation, is formed by adopting a noise-like chaotic sequence. The redundancy of the TS is utilized to embed secure keys. An experiment is performed, in which 7.64 Gb/s 16-quadrature-amplitude-modulation OFDM data and 28.4 Mb/s keys embedded in are successfully transmitted over 25 km standard single mode fiber. The results indicate a promising key distribution method for physical layer secure optical communication.

Index Terms: Orthogonal frequency division multiplexing (OFDM), passive optical network (PON), security key distribution, chaos, optical communication.

1. Introduction

The orthogonal frequency division multiplexing passive optical network (OFDM-PON) has become one of the outstanding candidates to meet requirements of the next generation optical network due to its high spectral efficiency, robustness to fiber dispersion, and flexibility of resource allocation [1]. Meanwhile, the broadcast structure has also brought several secure challenges to the reliable data transmission in PONs. The security of OFDM-PON systems has become one of the research hot spots in recent years [2], [3]. Chaos based techniques are widely investigated to build multiplexing secure communication systems [4], [5] or incorporated in OFDM-PONs [6]–[10] to provide the security for data transmission. The security of these schemes mainly relies on the difficulty of cracking and obtaining the keys, which are used to encrypt and decrypt data. However, the key

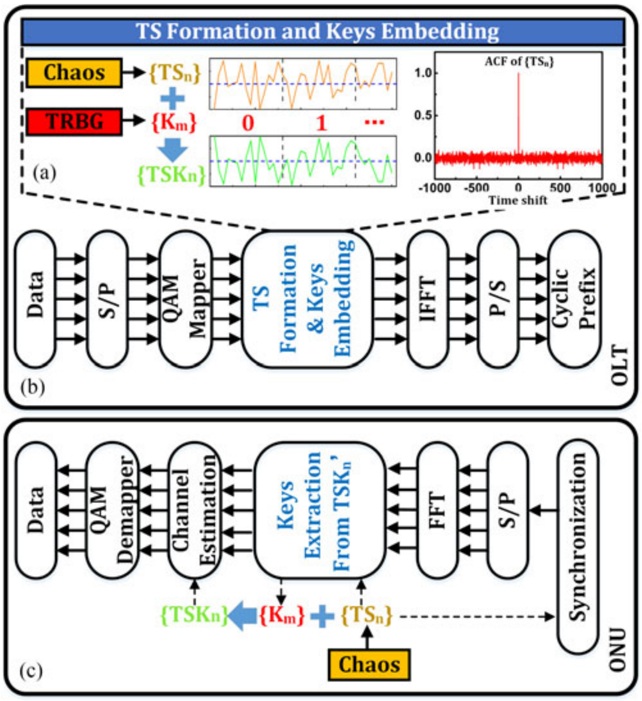


Fig. 1. The principle of the key distribution scheme for OFDM-PON. (OLT, the optical line terminal; ONU, the optical network unit)

has a service life [2], [11], and needs to be renewed periodically. The probability of key exposure gradually increases with the increase of key updating period. Unfortunately, most of the existing schemes only focus on the security level of encryption process, while the keys are assumed to be unchanged, which will certainly cause a performance degradation in the whole security hierarchy. Therefore, finding a suitable way to distribute and update the keys are of great significance.

There have been many existing methods to distribute keys between two parties in physical layer, such as the private key exchange using delay-coupled semiconductor lasers [12], key distribution based on synchronized chaotic lasers [13]–[15], key distribution scheme using synchronized cascades of semiconductor lasers driven by a common random source [16], and the quantum key distribution schemes [17], [18]. However, these methods have not been investigated under the point-to-multi-point topological structure. Certain modifications are essential if these schemes are adopted in the OFDM-PON scenario. Another concern is that the key distribution process in PONs should neither occupy too much channel resources nor increase system overhead significantly. If the key distribution scheme can be achieved along with the inherent DSP algorithm in OFDM implementation, it will be a lower cost and convenient way.

In this paper, we propose a dynamic key distribution scheme based on the redundancy of the training symbol (TS) which is used for time synchronization and channel estimation in OFDM-PON technique. By embedding the keys into the TS which is formed by a digital chaos sequence, the keys can be delivered to the receiver surreptitiously and extracted without occupying additional channel resources or interrupting the normal data transmission.

2. Principle

The principle of the proposed scheme is illustrated in Fig. 1. At the OLT, the downstream data is mapped onto quadrature amplitude modulation (QAM) sub-carriers after serial to parallel converting (S/P) in the traditional way. A true random bit generator (TRBG) is adopted to produce the secure keys. These keys are then embedded into a chaotic sequence which is used as the TS before being inserted in the OFDM frame. Due to the fact that the key distribution process is independent of most of the data encryption schemes (subcarrier scrambling [19], constellation mask [20], etc.), the data encryption process is not shown directly in this figure.

The TS plays an important role in OFDM-PON. Digital chaos sequence is an outstanding candidate owing to some properties in common, such as pseudo-randomness and rapid decay of the autocorrelation. In our scheme, a time-delayed chaotic system model [21] is utilized to generate the TS. The mathematical model can be expressed as

$$\dot{x}\left(t\right)=-cx(t)+a\sin\left(x\left(t-\tau\right)\right). \tag{1}$$

Here parameters $c = 1.0$, $a = 5.0$, $\tau = 2$, and the system behaves a chaos characteristic. Chaotic sequences $\{x1_n\}$ and $\{x2_n\}$ are generated with different initial conditions. The delayed differential equation in (1) is solved by 4th-order Runge-Kutta method and the time step size is chosen as 0.001. Then the TS is formed by (2)

$$TS_n = 0.5\times\left(T_{x1_n}+iT_{x2_n}\right). \tag{2}$$

where

$$\begin{aligned} T_{x1_n} &= mod\left(Extract\left(x1_n, 12, 13, 14\right), 256\right)/256-0.5\\ T_{x2_n} &= mod\left(Extract\left(x2_n, 12, 13, 14\right), 256\right)/256-0.5\ . \end{aligned} \tag{3}$$

Equation (3) denotes the post process of the raw chaos sequences, the function $Extract\left(\alpha, p, q, r\right)$ returns an integer which include the pth, qth and rth digits in the decimal part of α. Here, we choose the 12th, 13th, 14th digits, since the digits in low positions have better randomness than those in high positions and the fact [22] that the entropy rates for sequences of least significant bits more closely approach the metric entropy of a chaotic system. After this transform, statistical analyses show that the sequences $\{T_{x1_n}\}$ and $\{T_{x2_n}\}$ can pass the random tests of NIST SP800-22 standard [23]. The auto-correlation function of $\{TS_n\}$ becomes δ-like, as shown in Fig. 1(a).

At the OLT, a true random bit generator is used to produce binary key sequence $\{K_m\}$, which is then embedded into $\{TS_n\}$. Other procedures are identical with those of the traditional OFDM. The keys embedding process can be represented as

$$\begin{aligned} &TSK_n = TS_n\times(-1)^{(K_m+1)}\\ &(m-1)\times(N/M) < n \le m\times(N/M)\\ &N = kM,\ \ k = 1, 2, 3\ldots. \end{aligned} \tag{4}$$

where $n = 1, 2, \ldots, N$ and $m = 1, 2, \ldots, M$. The key embedding process described in (4) can be further demonstrated by Fig. 1(a). The sequence $\{\mathrm{TS_n}\}$ is divided into M segments, and each segment is controlled by the one-bit key K_m. If $K_m = 0$, the waveform of the segment is vertically flipped, while $K_m = 1$, the waveform remains unchanged. As a result, M-bit keys are embedded into the sequence $\{TS_n\}$ of length N.

At the ONUs, an identical sequence $\{TS_n\}$ is generated by using the same chaotic system as described in (1) and the same initial conditions (including the initial value and the parameters). It is firstly used to perform the time synchronization for each frame. Under the assumption that the synchronization can be established accurately, the keys $\{K_m\}$ can be extracted by comparing the local chaotic sequence $\{TS_n\}$ and the received $\{TSK'_n\}$, where $\{TSK'_n\}$ denotes $\{TSK_n\}$ after transmitted by the channel, as shown in Fig. 1(c). The key extraction is performed by correlation algorithm, which can be expressed by (5)

$$\begin{aligned} &\begin{cases} K'_m = 0 & corrcoef\left(\left\{TSK'_n\right\}, \{TS_n\}\right) \le 0\\ K'_m = 1 & corrcoef\left(\left\{TSK'_n\right\}, \{TS_n\}\right) > 0 \end{cases}\\ &(m-1)\times(N/M) < n \le m\times(N/M). \end{aligned} \tag{5}$$

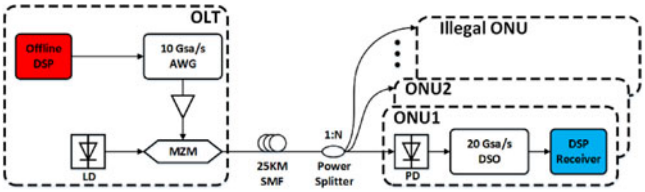


Fig. 2. Experimental setup for the secure key distribution in OFDM-PON.

where $corrcoef(\beta,\ \gamma)$ means the cross-correlation coefficient of sequences β and γ. K'_m is the recovered keys in each segment. The cross-correlation coefficient is defined by

$$corrcoef\,(\beta, \gamma) = \frac{(\beta_n - \beta_n)\,(\gamma_n - \gamma_n)}{\sqrt{(\beta_n - \beta_n)^2(\gamma_n - \gamma_n)^2}}\,. \tag{6}$$

Where $\langle\cdot\rangle$ stands for the time average, β and γ represent two different time sequences.

Note that the transmitted signal at the OLT is $\{TSK_n\}$ instead of $\{TS_n\}$, the channel estimation should be conducted by using $\{TSK'_n\}$ and $\{TSK_n\}$. After correctly extracting the keys, $\{TSK_n\}$ can be reproduced by using $\{TS_n\}$ and $\{K'_m\}$ in the same way as described in (4). Then the transmitted data signal can be decrypted and demodulated in the traditional manners.

3. Experiment Setup

The experimental setup of our scheme is shown in Fig. 2. At the OLT, the downstream data with a PRBS length of 214 is mapped onto 257 sub-carriers, of which 128 sub-carriers carry real 16-QAM data and one is unfilled DC sub-carrier. The remaining 128 sub-carriers are the complex conjugate of the aforementioned 128 sub-carriers. The Hermitian symmetry is utilized for 512-point IFFT in order to perform direct intensity modulation. The cyclic prefix is 51 points, which is 1/10 of the IFFT length, the OFDM symbol size is 563. The TS with M-bit keys embedded in is inserted at the beginning of each frame that contains 10 symbols. Meanwhile the data is encrypted through chaos and fractional Fourier transform techniques reported in [24]. Incorporated with the key distribution scheme, the keys can be renewed periodically, thus the overall security level of the OFDM-PON system is improved.

An arbitrary waveform generator (AWG) with a sample rate of 10 GSa/s is used to generate the OFDM signal with a raw data rate of 8.18 Gbps (10 GSa/s $\times$ 4 $\times$ 128/563 $\times$ 9/10). The net data rate is 7.64 Gb/s since 7% FEC overhead needs to be considered. The corresponding transmission rate of the keys is determined by M (10 GSa/s $\times$ M/563 $\times$ 1/10). A 100 kHz linewidth continuous-wave (CW) external cavity laser is utilized as optical source. The OFDM signal is modulated onto the optical carrier by a Mach-Zehnder modulator (MZM) which is working in the linear region. After 25 km standard single mode fiber (SSMF) transmission, the signal is captured by a 16 GHz photodiode (PD) and a 20 GSa/s digital sampling oscilloscope (DSO). Offline keys extraction, data decryption, demodulation and BER testing are then performed by the DSP, and 16384 bits are calculated for data BER testing in our experiment.

4. Experiment Results and Discussions

Correct time synchronization is a necessary condition for the keys extraction as well as data demodulation. Such synchronization is conducted using the correlation between the transmitted signal and the local TS. However, the redundancy of the TS allows us to sacrifice certain degree of synchronization performance. Fig. 3(a) shows the cross-correlation coefficient at the correlation peak between the received signal and the local TS within one frame under different M. Here we consider the ideal situation, which is noise free. With the increasing number of the embedded keys,

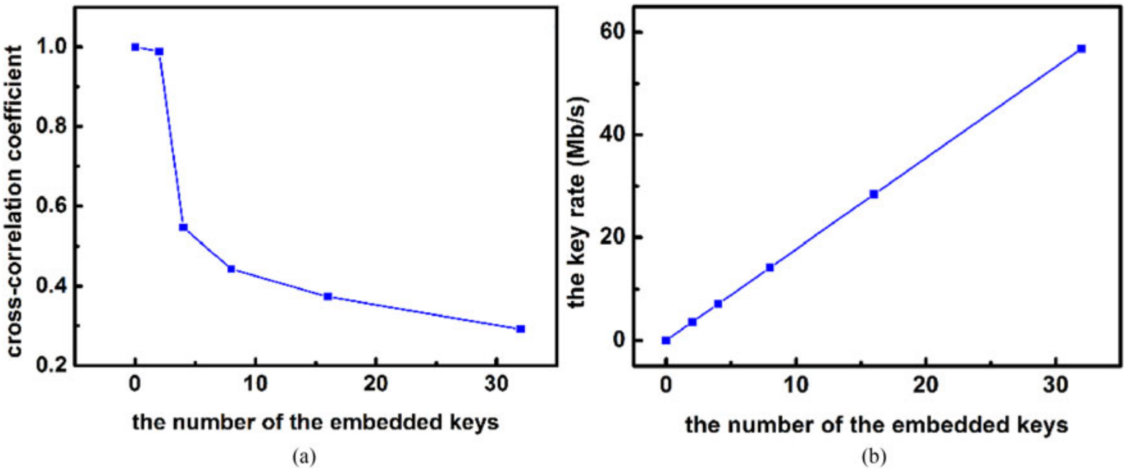


Fig. 3. (a) The cross-correlation coefficient between $\{TS_n\}$ and $\{TSK'_n\}$ with the increasing number of the embedded key bits during the time synchronization. (b) Theoretical key transmission rate with the increasing number of the embedded key bits.

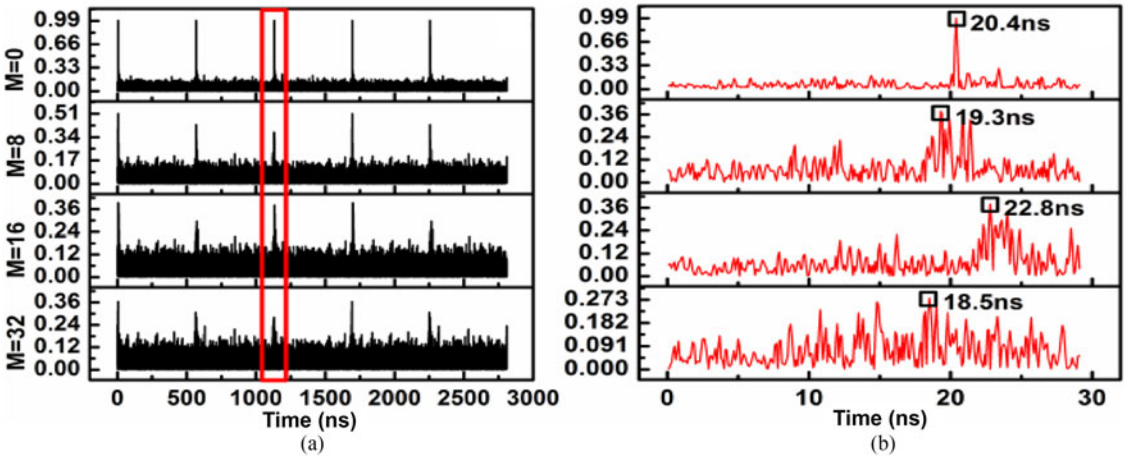


Fig. 4. (a) The time synchronization performance of 5 OFDM-frames. (b) The detail of local peaks in a short time scale.

the correlation coefficient decreases. Meanwhile the theoretical key rate increases, as shown in Fig. 3(b).

Since the TS does not carry any data information in the traditional OFDM scheme, the increasing number of embedded keys will not cause data-rate loss. Fig. 4 shows the synchronization performance under the situations of $M = 0$ (no key is embedded in), $M = 8$, $M = 16$ and $M = 32$. When $M = 0$, the timing of synchronization (the position of the correlation peaks) is certainly correct and accurate. When $M = 8$, 16, and 32, the timing is still roughly correct although certain time shift can be observed.

The aforementioned simulation results indicate that the key embedding is feasible and will not affect the synchronization performance significantly under ideal circumstances. Then we consider the realistic condition, under which the channel noise and the non-ideal performance of devices cannot be ignored. The key embedding and extraction process for $M = 8$ under experimental configurations is demonstrated in detail. The waveform of $\{TS_n\}$ is shown in Fig. 5(a). After 8-bit binary key $\{K_m\} = [0, 1, 0, 0, 1, 0, 0, 1]$ is embedded in, the resulted $\{TSK_n\}$ is shown in Fig. 5(b). The

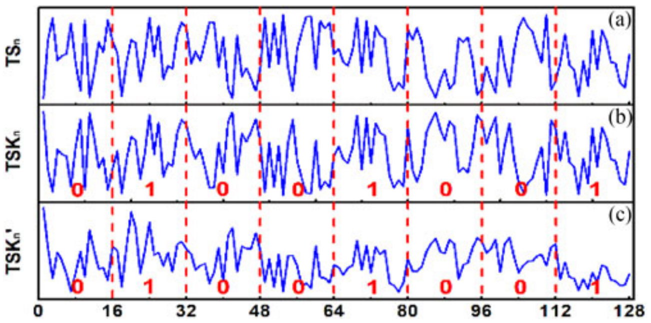


Fig. 5. (a) The chaotic sequence $\{TS_n\}$ before the embedding keys. (b) The TS $\{TSK_n\}$ with the embedded keys and (c) the received $\{TSK'_n\}$ after transmitted in the fiber channel.

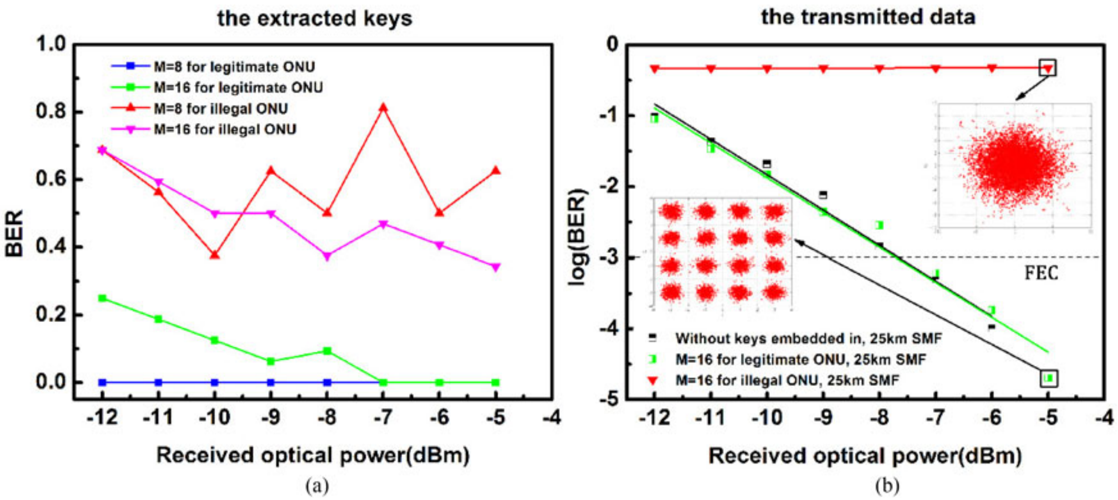


Fig. 6. (a) BER curves of the extracted keys when 8-bit and 16-bit keys are embedded in each frame. (b) Measured BER curves of the transmitted data with and without keys embedded in.

waveform of the received $\{TSK'_n\}$ is shown in Fig. 5(c) after the time synchronization. Compared with $\{TSK_n\}$, certain distortion can be observed in $\{TSK'_n\}$. However, the relationship between these waveforms is still distinguishable, and the keys can be recovered with error free by using (5).

At the legitimate ONUs, $\{TSK_n\}$ is reconstructed after correctly extracting the keys. Then the channel estimation can be performed by comparing $\{TSK'_n\}$ and $\{TSK_n\}$. Here we consider the influences of the key distribution scheme to the normal data transmission process. For the sake of system integrity, the data is encrypted using the scheme described in [23]. The measured BER curves of the extracted keys and the data under different circumstances are shown in Fig. 6(a) and (b), respectively.

As shown in Fig. 6(a), with the increase of received optical power, the BER of keys reduced in the legitimate ONU, and the keys can be extracted error free when the received optical power is higher than −8 dBm. The maximum value of M is 16, and the corresponding key rate is 28.4 Mbps under the current system configuration. if the received optical power is lower than −8 dBm, the keys cannot be extracted error free. Although the BER of the extracted keys at the illegal ONUs are unstable due to the limited experimental data length, the fact that the illegal ONUs are not able to extract the correct key (BER is non-zero) still can be obtained from Fig. 6(a). However, according to Fig. 6(b), the BER of the data is beyond the FEC limit for all the cases, including the case without keys embedded in. This fact means when the keys cannot be extracted correctly, the channel is in a

TABLE 1
The Permutation Entropy of Chaos Systems.

Logistic	Henon	Lorenz	Chen	system (1)
0.62	0.55	0.12	0.13	0.95

bad condition that cannot be acceptable even in conventional scheme. If we consider a conservative strategy, which is M = 8, the keys can be extracted error free when received power is −12 dBm, and in this situation the BER for the data in conventional OFDM scheme is far beyond FEC limit, as shown in Fig. 6(b). Fig. 6(b) also shows that the BER curves for both cases (16 bit keys embedded in and the conventional one) are almost coincident. This result indicates that the keys embedding scheme is robust to channel noise and has little influence to the demodulation process.

The discussions above confirm the fact that the keys embedding process will not affect the performance of the data transmission for legitimate ONUs. While the illegal ONUs cannot correctly demodulate data due to the failure of time synchronization.

The security of the scheme is manifested in three aspects:

1) The key extraction as well as the time synchronization are hard to perform for an eavesdropper. Firstly, the training sequence $\{TS_n\}$ is generated by a digital chaos system, an eavesdropper cannot generate the same TS without knowing the correct initial values and parameters. As a result, the time synchronization is hard to perform. Secondly, assume that the time synchronization can be established for the eavesdropper by certain means, and $\{TSK_n\}$ (TS with random keys embedded in) can also be obtained by the eavesdropper, the keys $\{K_m\}$ are still hard to extract. Since $\{TS_n\}$ is a noise-like sequence, with the true random keys $\{K_m\}$ embedded in, $\{TSK_n\}$ is still a random noise-like sequence and the randomness is even improved by the key. It is hard to separate these two random sequences without the knowledge of any one of them for an eavesdropper.
2) The keys are embedded into the noise-like chaotic sequence in an obscure way. It's hard to judge whether there is meaningful information in the TS without any priori- knowledge.
3) The security performance can be improved by the use of a chaos source with higher dynamical complexity. As listed in Table 1, the permutation entropy [25] of system (1) is much higher than that of the other commonly used chaotic systems. Nevertheless, the computational complexity is also relatively high due to the time-delay differential equation model and the Runge-Kutta calculation. Consider the fact that the transmission rate of TS is low because time synchronization is performed only once in each OFDM frame. The scheme is feasible in DSP without occupying a large amount of computing resources.

5. Conclusions

A secure key distribution scheme for OFDM-PON is achieved by utilizing the digital chaos technique and the redundancy of the TS. The random keys can be delivered from the OLT to the ONUs under standard OFDM-PON structure without occupying additional channel resources, and this process will not affect the normal data transmitting. For a legitimate receiver, the extracted random keys can be used to update the initial values and parameters of the chaotic system as well as the keys of data encryption algorithm. The keys for the different ONUs can be embedded in arbitrary frames by predefining a protocol. From the viewpoint of an eavesdropper, neither the time synchronization nor the key extraction process is able to conduct without the knowledge of the correct chaos sequence. The random keys and the chaotic system are interlocked together, thus the overall security can be maintained. The proposed method is proved to be effective and robust to channel noise. This scheme is also compatible with most of the data encryption schemes in secure OFDM-PON.

References

[1] H. Abbas and M. Gregory, "The next generation of passive optical networks: A review," *J. Netw. Comput. Appl.*, vol. 67, pp. 53–74, May 2016.

[2] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, Feb. 2017.

[3] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 2016.

[4] D. Rontani *et al.*, "Generation of orthogonal codes with chaotic optical systems," *Opt. Lett.*, vol. 36, no. 12, pp. 2287–2289, Jun. 2011.

[5] D. Rontani *et al.*, "Multiplexed encryption using chaotic systems with multiple stochastic-delayed feedbacks," *Phys. Rev. E*, vol. 80, no. 6, Dec. 2009, Art. no. 066209.

[6] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic Walsh–Hadamard transform for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 6, pp. 527–530, Mar. 2017.

[7] M. Bi *et al.*, "A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON," *IEEE Photon. J.*, vol. 9, no. 1, pp. 1–10, Feb. 2017.

[8] B. Liu, L. Zhang, X. Xin, and N. Liu, "Piecewise chaotic permutation method for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 28, no. 21, pp. 2359–2362, Nov. 2016.

[9] Z. Shen, X. Yang, H. He, and W. Hu, "Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos," *IEEE Photon. J.*, vol. 8, no. 3, Jun. 2016, Art. no. 7904609.

[10] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, "Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 2015.

[11] D. Forsberg, "LTE key management analysis with session keys context," *Comput. Commun.*, vol. 33, no. 16, pp. 1907–1915, Oct. 2010.

[12] X. Porte *et al.*, "Bidirectional private key exchange using delay-coupled semiconductor lasers," *Opt. Lett.*, vol. 41, no. 12, pp. 2871–2874, Jun. 2016.

[13] I. Kanter *et al.*, "Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography," *Opt. Exp.*, vol. 18, no. 17, pp. 18292–18302, Aug. 2010.

[14] C. Xue *et al.*, "Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing," *Opt. Exp.*, vol. 23, no. 11, pp. 14510–14519, May 2015.

[15] B. Wu *et al.*, "Long range secure key distribution over multiple amplified fiber spans based on environmental instabilities," in *Proc. Conf. Lasers Electro-Opt.*, Jun. 2016, pp. 1–2.

[16] H. Koizumi *et al.*, "Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers," *Opt. Exp.*, vol. 21, no. 15, pp. 17869–17893, Jul. 2013.

[17] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, Aug. 2015.

[18] K. Inoue, "Differential phase-shift quantum key distribution systems," *IEEE J. Sel. Topics. Quantum Electron.*, vol. 21, no. 3, pp. 109–115, May 2015.

[19] X. Yang *et al.*, "Chaotic signal scrambling for physical layer security in OFDM-PON," in *Proc. 17th Int. Conf. Transp. Opt. Netw.*, Jul. 2015, pp. 1–4.

[20] L. Zhang *et al.*, "A novel 3D constellation-masked method for physical security in hierarchical OFDMA system," *Opt. Exp.*, vol. 21, no. 13, pp. 15627–15633, Jun. 2013.

[21] D. D. Lee and H. S. Seung, "Algorithms for non-negative matrix factorization," in *Proc. Adv. Neural Inf. Process. Syst.*, 2001, pp. 556–562.

[22] N. J. Corron *et al.*, "Entropy rates of low-significance bits sampled from chaotic physical systems," *Phys. D*, vol. 332, pp. 34–40, Oct. 2016.

[23] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Rep. 800-22, May 2001.

[24] M. Cheng *et al.*, "Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation," *IEEE Photon. J.*, vol. 6, no. 6, pp. 1–9, Dec. 2014.

[25] C. Bandt and B. Pompe, "Permutation entropy: A natural complexity measure for time series," *Phys. Rev. Lett.*, vol. 88, no. 17, Apr. 2002, Art. no. 174102.