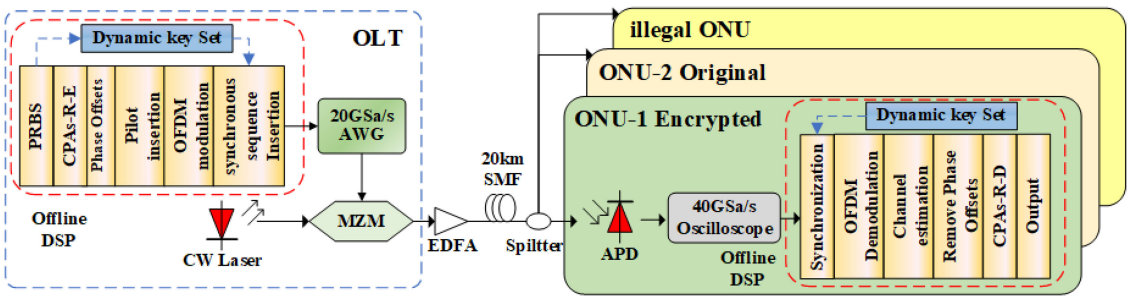
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Physical Layer Dynamic Key Encryption in OFDM-PON System Based on Cellular Neural Network

Volume 13, Number 2, April 2021

Yuxin Zhou
Meihua Bi
Xianhao Zhuo
Yunxin Lv
Xuelin Yang
Weisheng Hu



DOI: 10.1109/JPHOT.2021.3059369

Physical Layer Dynamic Key Encryption in OFDM-PON System Based on Cellular Neural Network

Yuxin Zhou,[1] Meihua Bi,[1,2] Xianhao Zhuo,[1] Yunxin Lv,[1] Xuelin Yang,[2] and Weisheng Hu[2]

[1]College of Communication Engineering, Hangzhou Dianzi University, Hangzhou, Zhe Jiang province 310018, China
[2]State Key Laboratory of Advanced Optical Communication System and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

DOI:10.1109/JPHOT.2021.3059369

Manuscript received January 11, 2021; revised February 3, 2021; accepted February 10, 2021. Date of publication February 15, 2021; date of current version March 3, 2021. This work was jointly supported by the Natural Science Foundation of Zhejiang Province under Grant LY20F050004, the Scientific research project of Zhejiang Provincial Department of Education under Grant Y202044258, and the National Natural Science Foundation of China under Grant 62001147. Corresponding author: Meihua Bi (e-mail: bmhua@hdu.edu.cn).

Abstract: In this paper, we propose a dynamic key technique based on Cellular Neural Network (CNN) for security improvement in the orthogonal frequency division multiplexing passive optical network (OFDM-PON). To enhance the encryption scheme security, a six-dimensional CNN hyperchaotic system is employed to encrypt the data. And, the keys are divided into the dynamic and static. The dynamic key is randomly extracted from a key set by incorporating the random feature of the input data. Then, the chaotic sequence generated by the dynamic key is served as the synchronous sequence for encryption. Moreover, the chaotic sequences generated by the static keys are used to resist the chosen-plaintext attacks (CPAs) and scramble the phase of QAM symbols on the frequency domain. With these processing techniques, the multi-fold data encryption can create a key space of $\sim 10^{315}$ to protect against the exhaustive trial. The transmission of 10-Gb/s encrypted 16-QAM-based OFDM signal is demonstrated over 20-km single mode fiber (SMF) by experiment. The results show that our proposed scheme can provide excellent confidentiality of data transmission against the CPAs and brute-force attack.

Index Terms: Orthogonal frequency-division multiplexing passive optical network (OFDM-PON), Chaotic encryption, Dynamic Key, Cellular Neural Network.

1. Introduction

Orthogonal frequency division multiplexing passive optical networks (OFDM-PON) are considered to be one of the best candidates for providing high-speed optical fiber transmission for next-generation access networks, which is due to its advantages of high spectrum efficiency, flexible resource allocation and strong anti-dispersion ability [1]–[4]. However, owing to the broadcast structure for the downstream transmission of PON, the transmitted data is vulnerable to eaves-dropping via an illegal optical network unit (ONU). Therefore, the security of PON has attracted wide attention [5], [6]. Typically, most research is focused on the upper layer for the security of the optical access network. However, the control data and the header information of upper layer

encryption are exposed in the physical-layer, which easily result in information leakage due to the malicious attacks. Even though several different types of security schemes have been proposed and studied at the physical layer, the security of the keys has not been adequately considered. Owing to the ciphertext is static, it is easy for the attacker to infer the key by choosing a plaintext attack [7]. Therefore, the security of the physical layer encryption key has attracted wide attention.

Numerous secure schemes have been proposed recently to enhance the security of OFDM-PON [8]–[22]. Among these proposed schemes, the chaos with its unique properties of the high sensitivity to the initial values, nonlinear and unpredictability is widely studied in the encryption. In [8], the chaotic sequence is used to randomly select different algorithms for encryption. This increases the complexity of the system. In [9], 4D-hyperchaotic mapping is used to generate four masking factors to achieve encryption in four different dimensions. Owing to the efficient parallel computing power of deoxyribonucleic acid (DNA), the transmission data is encrypted by DNA coding rules, which can achieve the fast encryption and decryption [10]. In [11], [12], the encryption method based on multi-scrolls system for physical-layer security is proposed. To achieve the Peak to Average Power Ratio (PAPR) reduction and encryption simultaneously, numerous secure schemes have been proposed and demonstrated, such as chaotic selected mapping [13], chaotic partial transmit sequences [14], chaotic Walsh-Hadamard Transform (WHT) processing matrix [15], chaotic discrete Hartley Transform (DHT) processing matrix [16], chaotic Discrete Fourier Transform (DFT) [17] and chaotic I/Q Walsh-Hadamard transform (WHT) scheme [18]. However, in the above schemes, there exists the problem that the key is static and can't resist the chosen-plaintext attacks (CPAs), which would seriously threaten the security of encrypted system. In [7], to resist the CPAs, the subcarrier phase of the OFDM symbol is disturbed by the dynamic phase rotation, which is jointly determined by the chaotic sequence and original input data. Furthermore, we have proposed the chaotic nonlinear encryption to resist the CPAs, in which the reduction of system performance is compensated by the CAZAC matrix [19]. Additionally, the security of the key is considered in these schemes, such as pilot-aided secure key agreement [20], secure key distribution based on the random bit generator [21] and time-variable keys from ONUs [22]. However, these methods are either limited by the finite accuracy of hardware or the security can't be guaranteed well. For the time-variable keys from ONUs scheme, since the dynamic of the key is introduced by the randomness of the upstream data of different ONUs, the upstream data is vulnerable to illegal theft. Based on the above the schemes, we can find that no any scheme yet been proposed to consider the key security and CPAs resistance simultaneously. Therefore, under the guarantee of the security of the key, our scheme also takes the CPAs resistance into account for further improve the system security without channel resource occupation.

In this paper, we propose a novel dynamic key encryption scheme for physical-layer security enhancement in OFDM-PON, to achieve the key protection, CPAs resistance and brute-force attack. In the proposed scheme, the 6-dimension (6-D) cellular neural network (CNN) hyperchaotic system is employed to generate the chaotic sequences, which are used for the signal synchronization, CPAs resistance and QAM symbol phase scrambling. First, the randomness of input data is used for the generation of dynamic key and further generate the chaotic synchronous sequence, thereby achieving the key protection and system encryption simultaneously. Then, the dynamic characteristic of input data is diffused to the whole ciphertexts for the CPAs resistance. Moreover, the chaotic sequence generated by the static key of CNN is employed to scramble the phase of QAM symbols, thereby constructing a noisy constellation with phase offsets. Via the three-step operation, a huge key space of 10^{315} can be created, which significantly enhances the security of OFDM-PON. To verify the feasibility of our encryption scheme, a 10-Gb/s encrypted 16-QAM OFDM signal transmission is experimentally demonstrated over 20-km standard single mode fiber (SSMF).

2. Principles

The block diagram of dynamic key encryption and decryption based on 6-D CNN in OFDM-PON is depicted in the Fig. 1. The pseudo random binary sequence (PRBS) is adopted as input data.

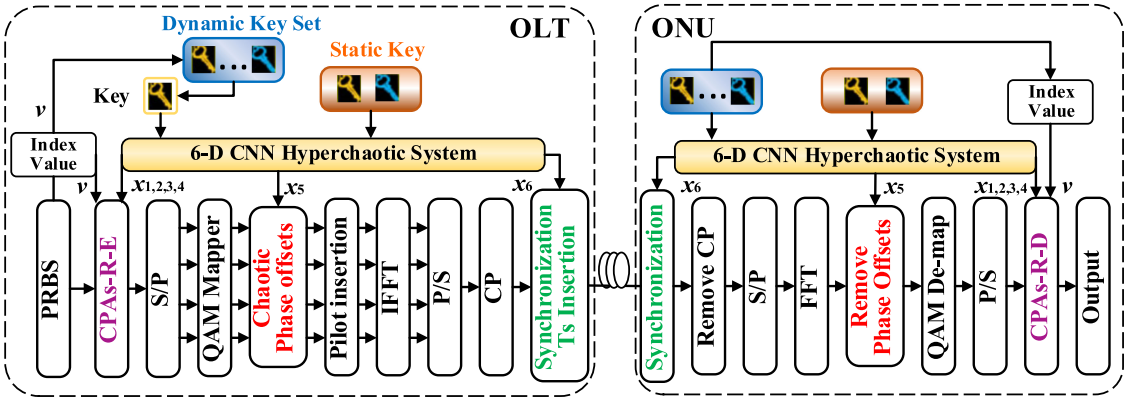


Fig. 1. Block diagram of our proposed dynamic key encryption and decryption based on CNN.

First, the index value generated by the PRBS is used to extract the key from the dynamic key set, which is composed of the initial value of 6-D CNN. Then, the chaotic sequence generated by the dynamic key is inserted as the synchronization training sequence (TS). Before the QAM mapping, the input bit stream is encrypted for CPAs resistance with the index value and the chaotic sequence generated by the static key. After the QAM mapping, the phase of QAM symbols is scrambled by the chaotic phase offsets. Hence, a 6-D CNN is employed to generated six independent chaotic sequences {*x1-x6*}, which are used to achieve the multi-fold encryption. Here, the CNN is an artificial neural network based on Hopfield neural network and cellular automaton, which is characterized by local interconnection between neurons and cells. It can be easily implemented by nonlinear circuits and with the ability to process signals in real time, high speed and parallel. In addition, the dimensions of CNN can be extended to multidimensional, which can present more complex dynamic behaviors than low dimensional chaotic systems, such as bifurcation, hyperchaotic behavior and periodic solutions within a certain parameter range [23]. And, the static equation of the 6-D CNN hyperchaotic system is given by

$$\begin{cases} x_1 = -x_3 - x_4 \\ x_2 = 2x_2 + x_3 \\ x_3 = 14x_1 - 14x_2 \\ x_4 = 100x_1 - 100x_4 + 200p_4 \\ x_5 = 18x_2 + x_1 - x_5 \\ x_6 = 4x_5 - 4x_6 + 100x_2 \end{cases} \tag{1}$$

Where $p_4 = 0.5(|x_4 + 1| - |x_4 - 1|)$. To prevent the decrease of sensitivity of 6-D CNN chaotic system, the Eq. (1) is solved via the Runge-Kutta method with a time step of h $= 0.005$ [24]. The projections of the chaotic attractor of CNN hyperchaotic system in the three-dimensional space are shown in the Fig. 2. We can see that attractors of CNN present complex folding and separation trajectories rather than a clear curve trace. Furthermore, the Lyapunov exponent is also introduced to evaluate the dynamical behavior of the 6-D CNN. By calculating the Lyapunov exponents of 6-D CNN, there exists two positive Lyapunov exponents $\lambda_1 = 2.7481$ and $\lambda_2 = 1.2411$, which further verified its hyperchaotic behavior [25]. Compared to the low dimensional chaotic systems with only a single positive Lyapunov exponent, the chaotic sequence generated by 6-D CNN has the higher security.

In order to further verify the randomness of the sequence generated by the 6-D CNN, the STS software package from the National Institute of Standards and Technology (NIST) is employed to measure the randomness. According to two criteria proposed by NIST for evaluating sequence randomness: P-value and passing rate. And, P-Value represents the uniform distribution of the sequence (P-Value $>$ 0.001, it indicates that the distribution of sequence is uniform). The passing

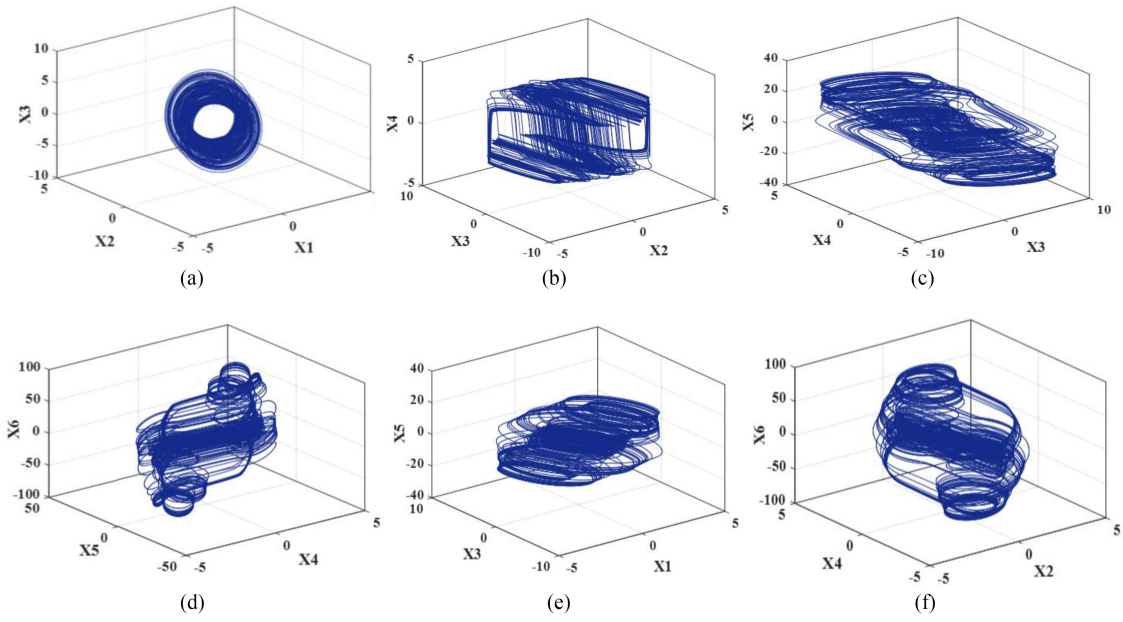


Fig. 2. The projections of the chaotic attractor of 6-D CNN hyperchaotic system in the three-dimensional space.

rate should be greater than 0.98577 according to the confidence interval of the test passing rate [26]. From the Table 1, we can see that 15 independent sequences all obtained relatively high P-value and the passing rate of 15 inspection test items are all greater than 0.98577, which proved that the chaotic sequences generated by 6-D CNN has good randomness.

The 6-D CNN is employed to generated six independent chaotic sequences, and then are used to realize data encryption, synchronization and dynamic key set generation. Different from the common dynamic key scheme based on initial value changes, the generated key set is not directly used to encrypt data. Instead, with the aid of input data stream randomness, the dynamic key index values are generated by summing and modulo operation on the plaintext. Subsequently, based on these indexes, the dynamic key is randomly extracted from the conducted dynamic key set. The index value v of dynamic key set can be obtained by the following processing

$$v = mod(sum(P), n) \tag{2}$$

Where n is numbers of keys in the dynamic key set, P is the input data stream, $sum(P)$ is the sum of all bits of the input data, and $mod(a, b)$ returns the reminder of a divided by b. v will change as long as the input data stream P change slightly. Therefore, to spread the randomness of the input data into the ciphertext, the index value v is used for the selection of the dynamic key and the CPAs resistance. The generation of dynamic key K can be described as

$$\mathrm{K} = \mathrm{Extract}(D\_K, v) \tag{3}$$

Where the function Extract(X, n) returns the n^{th} value in the set X and D_K denotes the dynamic key set. Subsequently, the dynamic key K generates the chaotic sequence through the 6-D CNN for the signal synchronization.

To ensure the security of the dynamic key, the dynamic key information is not sent from the OLT to the ONU. Here, the dynamic key set is pre-stored in advance in the OLT and ONUs. At the receiver, by utilizing autocorrelation property of chaotic sequence, the dynamic key information can be recovered. Based on the sliding window method, the chaotic sequence is extracted from the pre-stored dynamic key set in ONU, which has the same length as the synchronization sequence.

TABLE I
NIST Test Results of 6-D CNN Chaotic Sequence

Inspection Test Index	6-D CNN	
	P-value	Passing rate
ApproximateEntropy	0.40038	0.9922
BlockFrequency	0.36979	0.9922
CumulativeSums	0.05720	0.9981
FFT	0.52563	1
Frequency	0.04877	0.9961
LinearComplexity	0.46687	1
LongestRun	0.50634	1
NonOverlappingTemplate	0.34562	0.9922
OverlappingTemplate	0.51196	1
RandomExcursions	0.32938	0.9922
RandomExcursionsVariant	0.33750	1
Rank	0.50048	1
Runs	0.19098	0.9883
Serial	0.49424	0.9941
Universal	0.53394	1

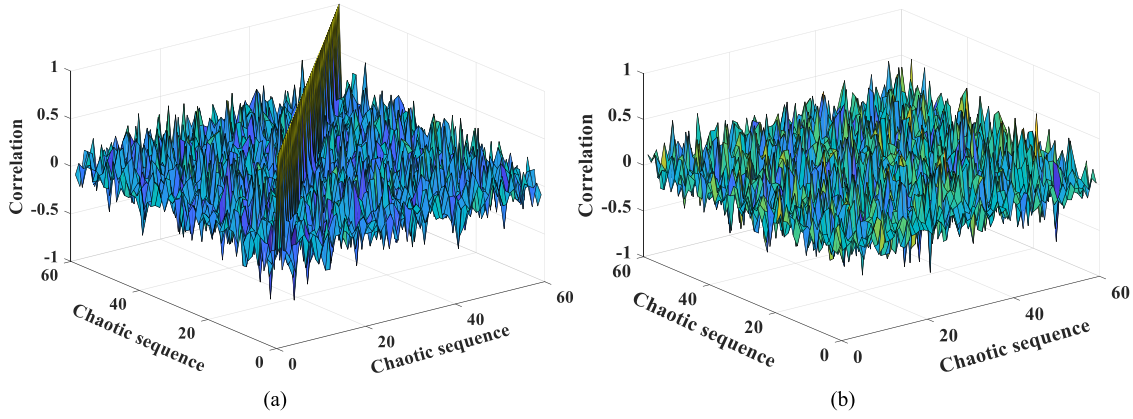


Fig. 3. (a) Correlation coefficient of the same chaotic sequence and (b) Correlation coefficient of different chaotic sequence.

Then, it is used to make correlation operation with the received data. As depicted in the Fig. 3, owing to its perfect autocorrelation, only the same chaotic sequence can get the correlation peak. Therefore, based on the correlation operation between the chaotic sequence and the received signal, the signal synchronization is realized and dynamic key information can be achieved thereby obtaining the index value v of the dynamic key in the key set.

In order to combine our encryption scheme, the chaotic sequence is converted into digital chaotic sequence by the following processing

$$D_i = mod\left(Ext\left(x_i, l, j, k\right), M\right) \tag{4}$$

The lower the decimal place of the chaotic value, the more sensitive it is to the initial value. So, the $Ext(x_i, l, j, k)$ returns the integer constructed by the l^{th}, j^{th}, k^{th} digits of the x_i decimal part ($l = 13$, $j = 14$, $k = 15$, owing to the chaotic value sensitivity 10^{-15}). M is the maximum value of the sequence, M varies according to different requirements in our scheme (for the chaotic sequences $\{x_1, x_2, x_3, x_4\}$, $M = 16$; $\{x_5\}$, $M = 360$; $\{x_6\}$, $M = 2$). By utilizing the operation (4), we can obtain the corresponding digital chaotic sequences $\{D_1, D_2, D_3, D_4, D_5, D_6\}$.

Moreover, the index value v is utilized to select one of the digital chaotic sequences $\{D_1, D_2, D_3, D_4\}$ for CPAs resistance encryption (CPAs-R-E). The process of the selection can be expressed as

$$index = \mathrm{mod}(v, 4)+1 \tag{5}$$

Where index is the sort position of chaotic sequences $\{D_1, D_2, D_3, D_4\}$. To resist the CPAs, the dynamic cyphertext is necessary. Here, the index value v and chaotic sequence $\{D_{index}$, ($index = 12, 34$)$\}$ are introduced to encrypt the data, which can express as

$$\begin{aligned} S(1) &= \mathrm{mod}(P(1) + v^2 + D_{index}(1), 16) \\ S(i) &= \mathrm{mod}(P(i) + S(i-1) + D_{index}(i), 16)(i = 2, \ldots, N) \end{aligned} \tag{6}$$

Where P is the input plaintext, S is the output ciphertext, $\{D_{\mathrm{index}}\}$ is one of the chaotic sequences $\{D_1, D_2, D_3, D_4\}$ generated by the static key set, and N is the length of data sequence. In our scheme, since OFDM adopts the 16-QAM modulation, the input digital signals are converted into decimal number every four digits for encryption. From the Eq. 6, the ciphertext $S(i)$ is associated with the current plaintext $P(i)$, the previous ciphertext $S(i-1)$ and the chaotic value $D_{index}(i)$. Moreover, the index value v of plaintext is used for the generation of the first ciphertext, which can spread the variation in the plaintext throughout the entire ciphertext. In this way, each ciphertext is related to each other, which all ciphertext will change accordingly as long as one plaintext vary. Correspondingly, the inverse processing is given by

$$\begin{aligned} P(i) &= \mathrm{mod}(S(i) - S(i-1) - D_{index}(i), 16)\ (i = N, \ldots, 2) \\ P(1) &= \mathrm{mod}(S(1) - v^2 - D_{index}(1), 16) \end{aligned} \tag{7}$$

According to Eq. 5, the chaotic sequence $\{D_{index}\}$ is determined by the index value v. Then, the CPAs resistance decryption (CPAs-R-D) starts from the end of the ciphertext, the plaintext $P(i)$ can be recovered by the current ciphertext $S(i)$, the previous ciphertext $S(i-1)$ and chaotic value $D_{index}(i)$. Finally, the first plaintext can be recovered by the ciphertext $S(1)$, the index value v and chaotic value $D_{index}(1)$.

Subsequently, to further enhance the security of signals on the frequency domain, the phase of 16-QAM symbols is scrambled by the chaotic sequence $\{D_5\}$. First, the phase of 16-QAM symbols is separated to achieve the phase scrambling. Furthermore, to evenly distribute the 16-QAM symbols in all directions on the constellation, the phase of 16-QAM symbols is converted to the phase angle for encryption. Then, the phase angle of 16-QAM symbols is scrambled with chaotic sequence $\{D_5\}$, which can be expressed as

$$\theta(i) = \mathrm{mod}(\theta(i) + D_5(i), 360)\ (i = 1, \ldots, N) \tag{8}$$

Where θ is the phase angle of 16-QAM symbols. As shown in the Fig. 4, we can see that the new constellation changes into three rings of different sizes via encryption, which constructs a chaotic constellation. For each 16-QAM symbol, the mapping is spread randomly over in all direction of original constellation radius, which guarantee the data security on the frequency domain.

Furthermore, as mentioned above, the key step for recovering data in ONU is getting synchronization information. This operation can be realized by correlation operation between received

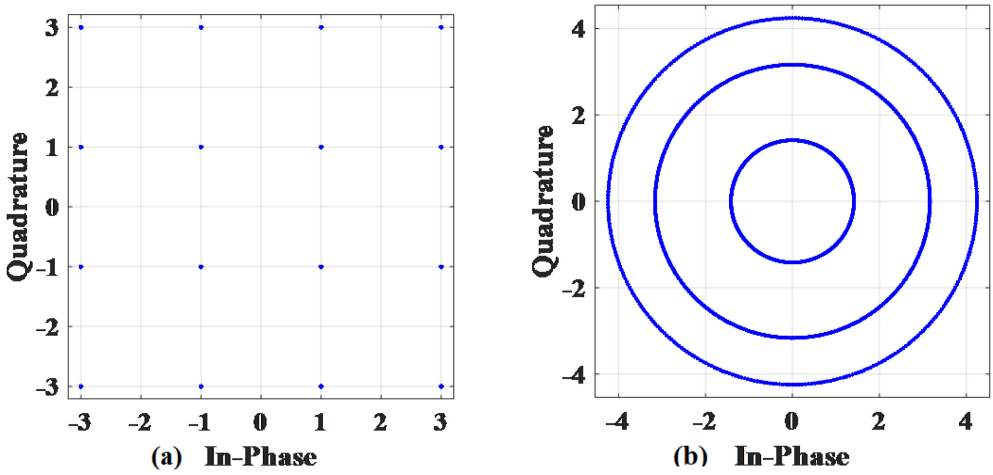


Fig. 4. 16-QAM constellation, (a) Original QAM. (b) Encrypted QAM.

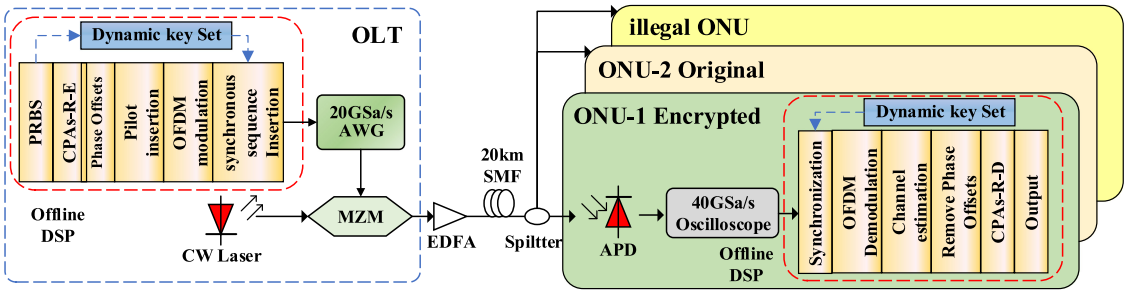


Fig. 5. The experiment setup of the proposed dynamic key encryption based on the 6D-CNN in OFDM-PON.

data and chaotic sequence of pre-stored key set. Once synchronization information is found, the corresponding index value v can be achieved which is used to recover of the resistance to CPAs encryption. Besides, as shown in Fig. 1, after the synchronization operation, the data can be implemented the reverse processing of transmitter in OLT. And, it is noted that, as for the phase scrambling of 16-QAM symbols, it can be recovered by appointment information between ONU and OLT.

3. Experiment Setup

The experiment setup of the proposed dynamic key encryption based on the 6-D CNN in OFDM-PON is depicted in the Fig. 5. Here, we adopt two regular ONUs and one illegal ONU to simulate the case of encrypted data, original data and illegal user. At the OLT and ONUs, the digital signal processing is executed offline by the MATLAB. At the OLT, the PRBS is randomly generated by the MATLAB program. Then, the random feature of input data is utilized to generate the dynamic key, thereby obtaining the synchronous sequence. After input data encrypted by the CPAs-R-E and serial to parallel (S/P) conversion, the encrypted data is mapped onto the subcarrier. Owing to the transmission system adopts intensity modulation and direct detection (IM/DD), the Hermitian symmetry is employed to get the real value output. The downstream is mapped on the 129 subcarriers, of which 64 subcarriers carried with 16-QAM symbols, one is unfilled direct current

(DC) subcarrier and the other 64 subcarriers are filled with the complex conjugate data. Then, the 16-QAM symbols are scrambled on the frequency domain. In addition, the pilots are inserted in block form for channel estimation. After the parallel to serial (P/S), a cyclic prefix (CP) of 1/8 OFDM length is inserted before each OFDM symbol to avoid the inter symbol interference induced dispersion. Subsequently, the chaotic synchronous sequence is added before signal to achieve the timing synchronization at the receiver. After that, the encrypted OFDM signals are uploaded to the arbitrary waveform generator (AWG, Tektronix, 7122C) with a sample rate of 20GSa/s. The data rate is 10-Gb/s with the electrical bandwidth of 2.5 GHz (20GS/s$\times$64/2/256). The optical source adopts the continuous laser with a central wavelength of 1550 nm. Finally, the generated electrical OFDM signals are modulated optical subcarrier by the Mach-Zehnder modulator (MZM), which is working at its linear region. Then, the optical signals are launched into 20-km SSMF after the optical power is boosted to -10dBm by the erbium-doped fiber amplifier (EDFA).

At the ONUs, to maintain a constant received optical power, the variable optical attenuator (VOA) is employed to adjust the optical power. The optical signal is captured by the avalanche photodiodes (APD) with 10GHz bandwidth. Subsequently, the encrypted data is recorded with a 40GSa/s real-time oscilloscope (LeCroy SDA 830Zi-A) for offline processing. The original signal will be recovered by specific processing, which includes timing synchronization, channel estimation, OFDM demodulation and decryption, *et al*.

4. Experiment Results and Discussion

Correct time synchronization is the necessary condition for the data demodulation and key extraction. Such synchronization is conducted as the correlation operation between the received signals and chaotic sequences, which are generated by the local dynamic key set. In general, the dynamic key set for different ONUs is the same and public. If one ONU has the higher security requirement, it can pre-shared private dynamic key set with the OLT or increase the number of keys in the key set. However, this will simultaneously increase implementation complexity and memory overhead. In our scheme, there is a trade-off between complexity and security, and the amount of key in the dynamic key set is set as 16. In the 20-km optical fiber transmission experiment, the chaotic sequences generated by the dynamic key set stored in advance are used to make correlation operation with the received signals, which can be expressed as [5]

$$\mathrm{R}(\beta,\gamma)=\frac{\sum_{i=1}^{N}\left(\beta_i-E(\beta)\right)\left(\gamma_i-E(\gamma)\right)}{\sqrt{\sum_{i=1}^{N}\left(\beta_i-E(\beta)\right)^2}\sqrt{\sum_{i=1}^{N}\left(\gamma_i-E(\gamma)\right)^2}} \tag{9}$$

where β and γ are two different time sequences, which represent the received signals and chaotic sequences. N is the length of the sequence, $E(\beta)$ and $E(\gamma)$ are the average values of the β and γ vector, respectively. By the above calculation, the cross-correlation coefficient between received signals and chaotic synchronization sequences are shown below.

In the Fig. 6, compared to the other key, the key with an index value 13 in the dynamic key set can obtain the maximum correlation coefficient, which have been verified the key is the same as the sender. So, the key randomly extracted each time in the proposed scheme, we can all realize accurate timing synchronization with the correct dynamic key set.

In addition, as a non-negligible part in the orthogonal frequency division multiplexing system, the PAPR is evaluated, as presented in Fig. 7. It gives the PAPR and complementary cumulative distribution function (CCDF) curves of the OFDM signals. It is easily got that, our scheme has almost the same PAPR performance as the original signals without encryption. In other words, our encrypted scheme does not bring any PAPR deterioration compared to the original signals. Therefore, this proves our method can retain the PAPR performance of the common OFDM system.

The transmission performance of our proposed encryption scheme is evaluated by the bit error ratio (BER) in the Fig. 8. The BER is measured at the back-to-back (B2B) and 20-km fiber transmission respectively. From the results, we can see that our encrypted scheme in the receiver sensitivity is approximately 1 dB poor than the unencrypted case. The main reason for

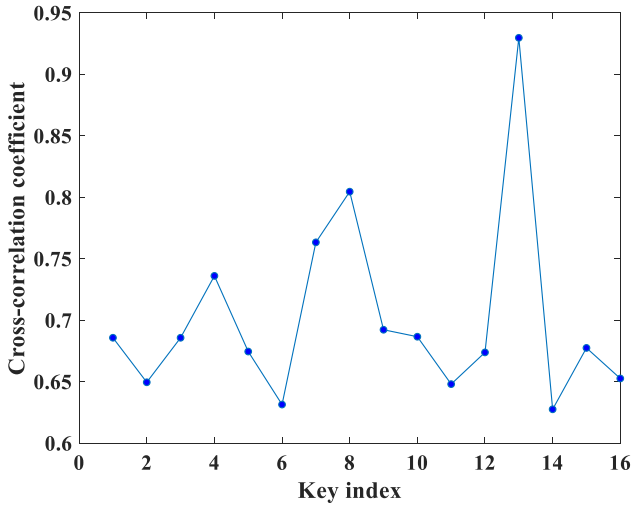


Fig. 6. The cross-correlation coefficient between received signals and chaotic sequences with the different key index.

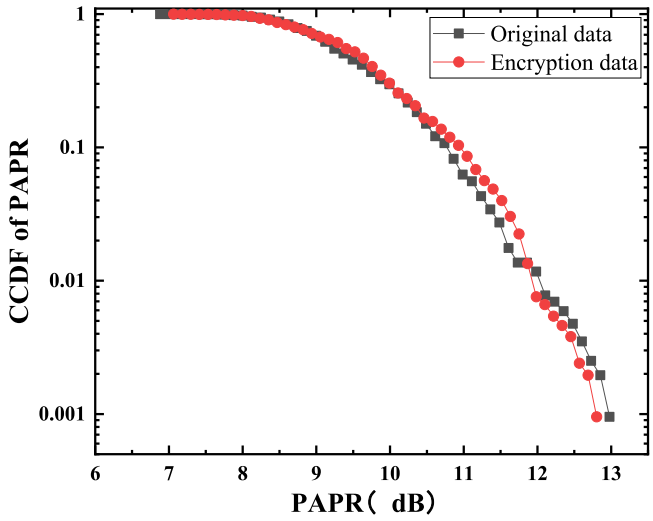


Fig. 7. CCDF of PAPR for the original and encrypted signal.

the performance degradation is attributed to the noise accumulation and superposition, which is caused by the error diffusion of CPAs resistance. As demonstrated in [27], due to the correlation property of CPAs generation, the encrypted signals are correlated with each other. In this way, the distortion of the first transmitted signal will affect the subsequent data transmission, and the received data with certain errors are repeatedly used to process the fully dynamic ciphertext, thereby bring system performance degradation. To guarantee the security of data transmission, the receiver sensitivity penalty of 1dB is acceptable. If the system has the higher performance requirement, our scheme can be utilized jointly our previous proposed modified DFT method [17] to compensate for the performance losses.

To evaluate the capability against CPAs of the proposed encryption scheme, we observe the variations of ciphertext with respect to a tiny change in the plaintext. The experimental result is shown in the Fig. 9 In the Fig. 9(a), one bit is changed in the input bit stream. Then, the difference of each subcarrier after IFFT between the original and encrypted signal is recorded and shown

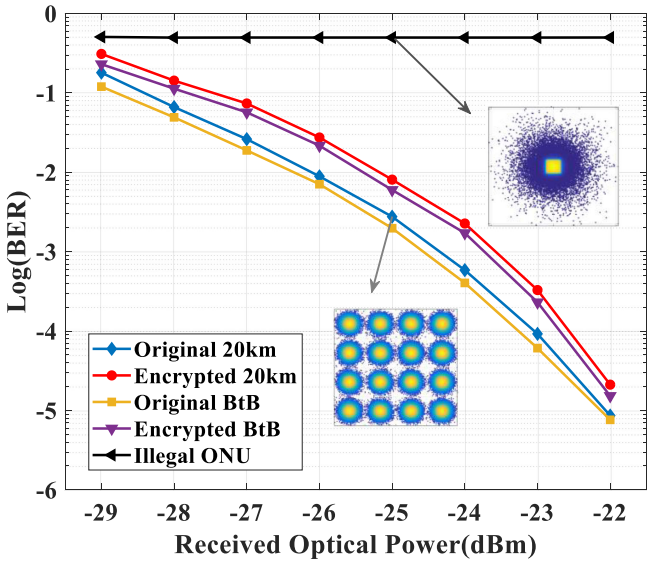


Fig. 8. BER curves of the OFDM signal in the conventional scheme and our proposed encryption scheme.

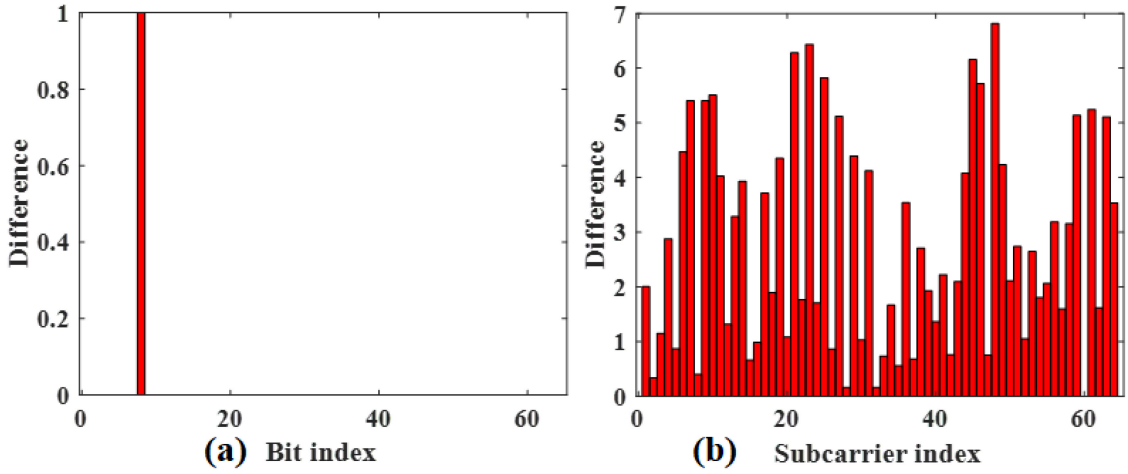


Fig. 9. The variation of ciphertext with the input bit stream. (a) Change one bit in the input bit stream. (b) The variation of all subcarriers of one OFDM symbol.

in the Fig. 9(b). We can see that the variation of these difference values is distributed among all subcarriers of the OFDM symbol in the ciphertext, in which the difference values change randomly as long as a bit variation. The dynamic ciphertext is generated iteratively by the Eq.(6), in which the ciphertext is associated with the plaintext, previous ciphertext and the chaotic value. Moreover, the first ciphertext is determined by the index values of input data, which is generated by sum of all input data. As distinguished from the proposed CPAs resistance encryption [9], this processing can further improve the ciphertext dynamic, which can solve the problem that the ciphertext variation cannot spread globally.

To verify the effect of noise interference on the encryption system. the key-mismatch rate (KMR) curves for dynamic key encryption and phase scrambling encryption are measured as shown in Fig. 10. as description in [28], [29], the KMR is a ratio consisting of two parts, the number of bits that are mismatch between the transmitting and receiving nodes, and the whole number of

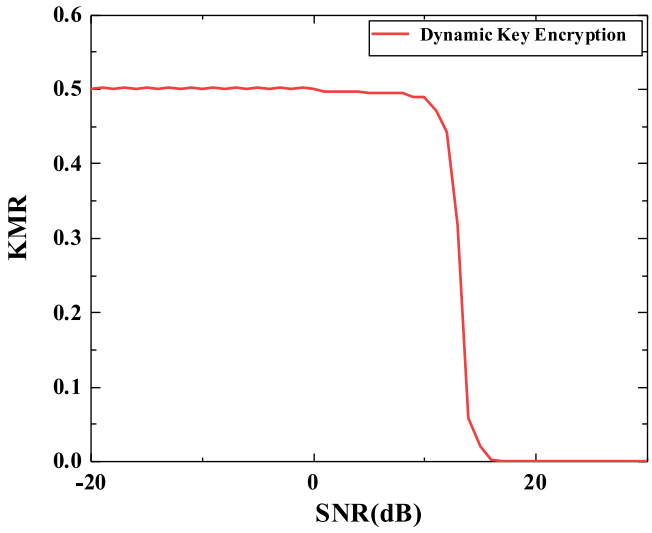


Fig. 10. The KMR curves for dynamic key encryption.

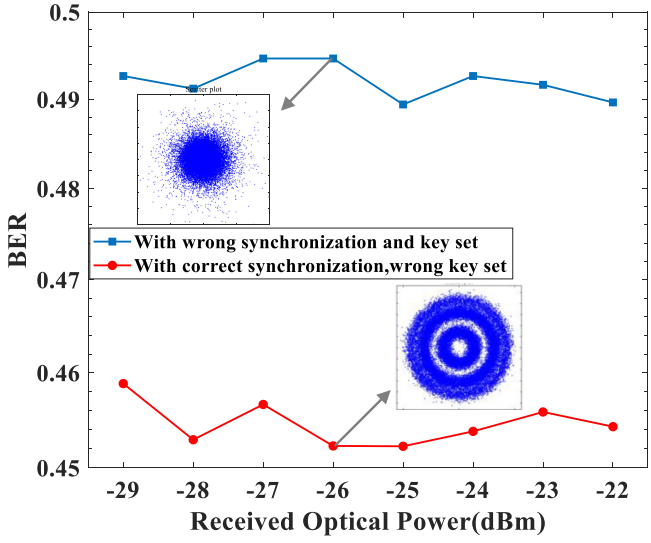


Fig. 11. Measured BER curves versus the received optical power for Illegal ONU.

generated keys bits. Obviously, when SNR is below a specific value (10 dB in the case of dynamic key encryption), the KMR of the keys between the transmitting and receiving nodes became higher than zero, in which the BER suddenly increased to approximately 0.5. In other words, the original would be not correctly recovered. This result can be used to analyze the degradation of our scheme than unencrypted case. This can be also attributed that, the error diffusion property of encryption data with strong correlation brought by the CPAs. And, this problem would be further studied in our future work.

Furthermore, in our scheme, the key information can be delivered to the receiver surreptitiously through the synchronization sequence without occupying the additional channel resource and interrupting the normal data transmission. Fig. 11 shows the measured BER performance of the illegal ONU. If the adversary uses wrong synchronization sequence decrypt the received signals, the BER is about 0.49. Even the adversary achieves the timing synchronization in illegal means,

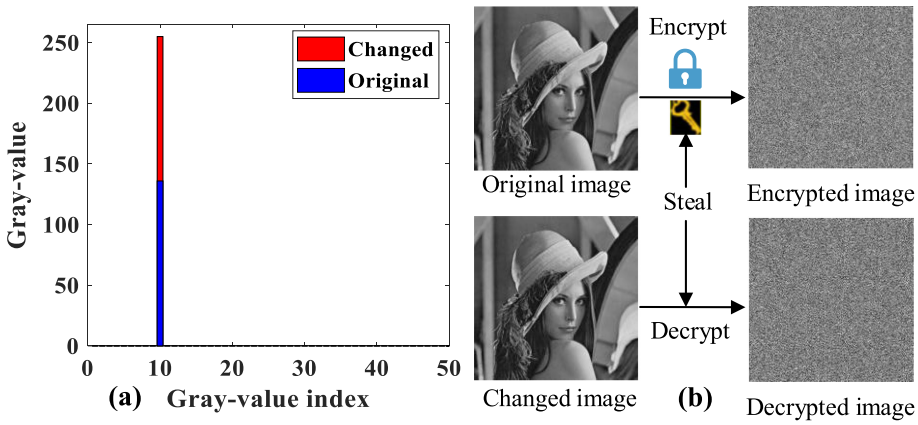


Fig. 12. Key dynamic security test. (a) one gray value change in the original image (b) The illegal user obtains the dynamic key for decryption.

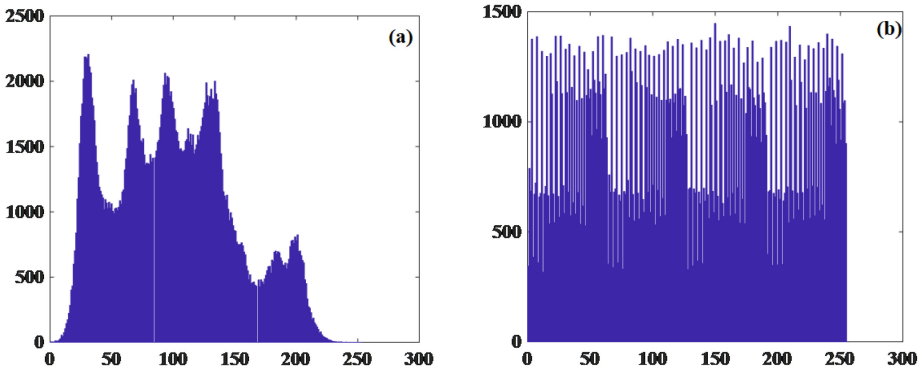


Fig. 13. The histogram of Lena images, (a) the original image (b) the encrypted image.

the BER is still as high as 0.45 without the correct key set. The constellation diagram at illegal ONU also has presented in the Fig. 11, where the correct information is difficult to recover effectively. These results further verified that dynamic key encryption scheme can guarantee the secure data transmission for OFDM-PON system.

Moreover, the dynamic key security is also verified by a classic gray image, as shown in the Fig. 12. First, the two similar Lena images are served as the sender information, which are encrypted and transmitted to the receiver to verify the encryption performance. And, the changed image is distinguished from the original image with one gray value change, which are shown in Fig. 12(a). Then, the original image is encrypted by our scheme and sent to the fiber transmission. Supposing the adversary obtain the security key of the original image by some illegal means. After that, the security key is used to decrypt the changed image of one gray difference, the corresponding result is shown in the Fig. 12(b). Even if the two pieces of information at the sending end are similar, the intruder still cannot crack the other piece of encrypted ciphertext after obtaining the key of one piece of information, which further verifies the high sensitivity of the dynamic key to input data in our scheme. Moreover, the size of dynamic key set in our scheme can be adjusted according to the security requirements, which provides high flexibility.

Moreover, the histogram of the original and encrypted Lena images is shown in the Fig. 13. The histogram revels the distribution of image pixels. The histogram of the original image presents the multi-peak distribution with obvious statistical characteristics. However, the histogram of encrypted

image is completely different from that of original image, and the encrypted image histogram is evenly distributed. What's more, the statistical characteristics of the original image are completely broken, thereby hiding the information of the original image.

Finally, the security level of the system can be evaluated by the key space. Owing to the chaotic system is highly sensitive to the initial value, chaotic trajectory will change dramatically if only the initial value varies $\sim 10^{-15}$. So, the chaotic initial value is served as the key. In our proposed encryption scheme, the keys are divided into two parts, one is the dynamic key and the others are the static keys. The static keys are the fixed initial value of 6-D CNN, which are shared with the sender and receiver. The five initial values can create the key space $\sim 10^{75}$ ($10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15}$). The dynamic key is randomly extracted from the dynamic key set by incorporating the random feature of the input data. The size of dynamic key set determined the security level. However, for received signals to synchronize correctly, the chaotic synchronization sequence should be generated by traversing all the values in the dynamic key set. The computational complexity increased exponentially with the size of the dynamic key set. So, the security and the computational complexity should be trade off to achieve efficient and secure data transmission. Here, we employed 16 initial values of CNN to construct the dynamic key set, which can create the key space of $\sim 10^{240}$. In total, our proposed encryption scheme can create the key space of $\sim 10^{315}$, which can efficiently prevent the brute-force attack. Moreover, owing to the noise-like and the randomness of chaotic sequence, the correlation of encrypted input data stream is greatly reduced, which can prevent the statistical attack.

5. Conclusion

In this paper, a novel dynamic key encryption based 6-D CNN is proposed and demonstrated for improving physical-layer security in OFDM-PON. For the key security problem of current proposed encryption scheme, our proposed encryption scheme utilizes the random feature of input data to randomly select the key in the dynamic key set for the key protection. Moreover, the random of input data is applied for CPAs resistance, which can completely diffuse the dynamic characteristic of input data into entire ciphertext. Furthermore, to guarantee the security of data in the frequency domain, the phase of the QAM symbol is scrambled by the chaotic phase offsets. By these processing, a large key space of $\sim 10^{315}$ can be achieved to resist the brute-force attack. A 10-Gb/s encrypted OFDM signals are successfully transmitted through 20-km SSMF to verify the feasibility of proposed encryption scheme. The experimental results show that the encrypted OFDM signal is poor 1dB than the original signal in the receiver sensitivity. Owing to the accumulation of noise generated by resisting the most threatening CPAs, the performance penalty is within the reasonable limits. Therefore, the dynamic key encryption scheme based on 6-D CNN can be a promising candidate for future physical-layer security in OFDM-PON.

References

[1] S. Li *et al.*, "Enhancing the physical layer security of OFDM-PONs with hardware fingerprint authentication: A machine learning approach," *J. Lightw. Technol.*, vol. 38, no. 12, pp. 3238–3245, 2020.
[2] T. Wu, C. Zhang, H. Huang, Z. Zhang, H. Wei, H. Wen and K. Qiu, "Security improvement for OFDM-PON via DNA extension code and chaotic systems," *IEEE Access*, vol. 8, pp. 75119–75126, 2020.
[3] T. Wu, C. Zhang, H. Wei and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Exp.*, vol. 27, no. 20, pp. 27946–27961, 2019.
[4] Y. Xiao, Y. Chen, C. Long, J. Shi, J. Ma and J. He, "A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON," *IEEE Photon. J*, vol. 12, no. 3, Jun. 2020, Art. no. 7201215.
[5] X. Zhuo, M. Bi, Z. Hu, H. Li, X. Wang and X. Yang, "Secure scheme for OFDM-PON system using TR based on modified henon chaos," *Opt. Commun.*, vol. 462, 2020, Art. no. 125304.
[6] M. Li *et al.*, "5D data iteration in a multi-wavelength OFDM-PON using the hyperchaotic system," *Opt. Lett.*, vol. 45, no. 17, 2020, Art. no. 125304.
[7] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Chaos-based physical-layer encryption for OFDM-based VLC schemes with robustness against known/chosen plaintext attacks," *IET Optoelectron.*, vol. 13, no. 3, pp. 124–133, 2019.

[8] H. Wei, C. Zhang, T. Wu, H. Huang and K. Qiu, "Chaotic multilevel separated encryption for security enhancement of OFDM-PON," *IEEE Access*, vol. 7, pp. 124452–124460, 2019.
[9] J. Zhao *et al.*, "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," *Opt. Exp.*, vol. 28, no. 14, 2020, Art. no. 21236.
[10] C. F. 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. 1706–1171, 2018.
[11] Y. Xiao *et al.*, "Two-level encryption for physical-layer security in OFDM-PON based on multi-scrolls system," *Opt. Commun.*, vol. 440, pp. 126–131, 2019.
[12] Y. Chen *et al.*, "Multi scrolls chaotic encryption scheme for CO-OFDM-PON," *Opt. Exp.*, vol. 28, 2020, Art. no. 19808.
[13] X. Hu, X. Yang, and W. Hu, "Chaos-based selected mapping scheme for physical layer security in OFDM-PON," *Electron. Lett.*, vol. 51, no. 18, pp. 1429–1431, 2015.
[14] 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.
[15] 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.
[16] A. A. E. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete hartley transform," *IEEE Photon. J.*, vol. 20, no. 2, 2018, Art. no. 7901209.
[17] X. Fu *et al.*, "A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON," *Opt. Fiber. Technol.*, vol. 42, pp. 126–131, 2018.
[18] Z. Hu and C. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure Fast-OFDM-PON," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3373–3381, 2018.
[19] M. H. Bi, X. S. Fu, X. F. Zhou, X. L. Yang, S. L. Xiao, and W. S. Hu, "Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 24, pp. 2147–2150, Dec. 2017.
[20] 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, 2017.
[21] S. S. Li *et al.*, "Secure key distribution strategy in OFDM-PON by utilizing the redundancy of training symbol and digital chaos technique," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201108.
[22] S. Li *et al.*, "Secure strategy for OFDM-PON using digital chaos algorithm with fixed-point implementation," *J. Lightw. Technol.*, vol. 36, no. 20, pp. 4826–4833, 2018.
[23] X. Y. Wang, B. Xu, and H. G. Zhang, "A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 1, pp. 124–133, 2010.
[24] N. Razali, R. R. Ahmad, M. Darus, and A. S. Rambely, "Fifth-order mean Runge-Kutta methods applied to the Lorenz system," in *Proc. 13th Wseas Int. Conf. Appl. Math.*, 2008, pp. 333–338.
[25] X. Huang, Z. Zhao, Z. Wang, and Y. Li, "Chaos and hyper chaos in fractional-order cellular neural networks," *Neurocomputing*, vol. 94, no. 3, pp. 13–21, 2012.
[26] M. S. Malik *et al.*, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-Boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.
[27] M. Bi, X. Fu, X. Zhou, X. Yang, S. Xiao and W. Hu, "Chaotic nonlinear encryption scheme for CPAs resistance and PAPR reduction in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 24, pp. 2147–2150, Dec. 2017.
[28] Y. M. Al-Moliki, M. T. Alresheedi and Y. Al-Harthi, "Improving availability and confidentiality via hyperchaotic baseband frequency hopping based on optical OFDM in VLC networks," *IEEE Access*, vol. 8, pp. 125013–125028, 2020.
[29] Y. Al-Moliki, M. Alresheedi, and Y. Al-Harthi, "Design of physical layer key generation encryption method using ACO-OFDM in VLC networks," *IEICE Trans. Commun.*, vol. E103-B, no. 9, pp. 1–10, 2020.