Probabilistic Shaping Probability Distribution Scrambling based on Chaotic System for Security Enhancement in DFTs-OFDM

Shuang Wei, Yajie Li, Wang Wei, Kongni Zhu, Mingrui Zhang, Yuang Li, Yongli Zhao and Jie Zhang*

School of Electronics Engineering, Beijing University of Posts and Telecommunications, 100876, China, jie.zhang@bupt.edu.cn

Abstract *We propose a probabilistic shaping probability distribution scrambling based on chaotic systems for physical-layer security enhancement scheme in optical communication. Experimental results verify that the proposed scheme can resist brute force attacks with key space 10^{120}, with 0.6 dB OSNR degradation as cost. ©2023 The Author(s)*

Introduction

To satisfy the escalating need for high-capacity and long-distance data transmission, coherent optical communication has become a prominent field of research in core and metro network [1]. Probabilistic shaping (PS) is a technique for approaching Shannon's limit, which further improves capacity [2]. However, the transparent transmission nature of optical communication systems renders the payload data vulnerable to security attacks, necessitating the use of physical layer encryption techniques.

Recently, physical layer chaotic encryption schemes based on PS have been developed to improve both security and transmission performance. A method is proposed to change the mapping rule of constant composition distribution matching (CCDM) [3,4]. In addition, the shaping scheme based on the frequency of symbol occurrence in a period of time can also be used for security encryption [5,6]. It is also feasible to construct a false probability distribution of CCDM output symbols by inserting a few symbols into the symbols after shaping [7]. In shaped 16QAM symbols, the random number generated by chaotic sequence is used to slightly disturb the occurrence probability of each symbol point that has the same amplitude [8]. A non-uniformly distributed 4QAM is superimposed on a uniformly distributed 4QAM to construct the shaped 16QAM symbol, where redundant bits provide certain security and the bit error ratio (BER) of illegal parties is 0.15 [9]. Even though these schemes provide certain protection abilities, the probability distribution of shaping symbols is not well protected, and there are still security vulnerabilities. Therefore, it is necessary to fill the gap in physical secure encryption technology based on PS that effectively protects the probability distribution.

In this paper, we propose a probabilistic shaping probability distribution scrambling (PSPDS) based on chaotic systems. Firstly, the probability distributions of CCDM output symbols of I and Q channels are randomly selected. Then, an IQ mixer is adopted to exchange symbols between I and Q channels to preliminarily scramble probability. Lastly, all QAM symbols are scrambled to realize the scrambling of the probability distribution of each CCDM block output symbols. A 4D Chen chaotic system and a Logistic chaotic mapping are implemented to provide adequate key resisting brute force attack with key space 10^{120}. The Pearson correlation between probability distribution before and after scrambling reach 0.1195. The transmission performance penalty is 0.6 dB in term of OSNR.

Principle

- PSPDS principle

Fig.1 shows the basic principle of PSPDS scheme utilizing both a 4D Chen system and a 1D Logistic system. Firstly, in I or Q, bit stream is divided into two branches. The low branch bits are injected into CCDM, and output symbols are transformed into binary numbers in order to perform forward error correction (FEC) encoding with high branch bits [2]. The desired M/2-PAM symbol distribution determined by chaotic sequence $\{x\}$ and $\{y\}$ generated by 4D chaotic system. Then, an IQ mixer is adopted to preliminarily scramble probability distribution by exchanging symbols between I and Q according to the chaotic sequence $\{z\}$. After IQ mixing, two branches M/2-PAM symbols will be superimposed to constitute M-QAM symbols. Whereafter, sequence $\{w\}$ and $\{u\}$ together scramble all QAM symbols. To avoid affecting the gains of shaping, the overall probability distribution must be retained. Therefore, the

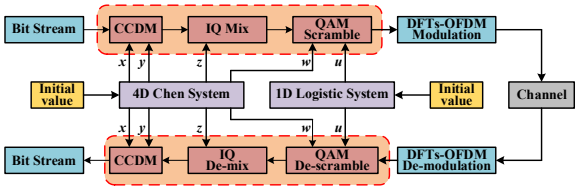

Fig. 1: the schematic diagram of PSPDS based on chaotic system in the DFTs-OFDM modulation.

symbol coordinates will be exchange instead of symbol amplitude. Lastly, the propose of scrambling probability distribution is achieved.

- Chaotic system

Herein, a 4D chaotic Chen system and 1D chaotic Logistic system are employed to supply chaotic random sequences. The 4D Chen system can be expressed [6], where a, b, c, d and r are the control parameters of Chen system. To ensure the system taking in a good hyper-chaotic state, the control parameters are set as $a = 35$, $b = 7$, $c = 12$, $d = 3$ and $r = 0.58$.

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = bx - xz + cy \\ \dot{z} = yz - dw \\ \dot{w} = yz + rw \end{cases} \tag{1}$$

Moreover, Logistic chaotic mapping [10], which has a superior statistical property, is served as another random sequence provider. The equation of Logistic chaotic mapping is defined as (2), where η is the control parameter and $\eta \in [0,1]$.

$$u_{i+1} = 4\eta u_i (1 - u_i) \tag{2}$$

- Chaotic-based scrambling principle

Following above chaotic system, the sequences $\{x\}$, $\{y\}$, $\{z\}$, $\{w\}$ and $\{u\}$ can be iteratively updated, where the initial values are pre-shared secure key between legal parties. In order to encrypt plaintext, the chaotic sequence should be becomingly post-processed.

Firstly, the key sequence $K_{x,i}$ is obtained by chaotic sequence $\{x\}$, which is digitalized as

$$D_{x,i,1} = \mathrm{mod}(Extract(x_i, 14), 2) \tag{3}$$

$$D_{x,i,2} = \mathrm{mod}(Extract(x_i, 15), 2) \tag{4}$$

$$K_{x,i} = bi2de(D_{x,i,1} D_{x,i,2}) \tag{5}$$

where $Extract(x_i, m)$ represents that extracts an integer to mth digit in the decimal part of x_i; $mod(\alpha, \beta)$ is modular operation; $bi2de(n)$ is converted from binary to decimal. Using the operation rule, $K_{x,i}$ is in the range of {0, 1, 2, 3}. The key sequence $K_{y,i}$ is generated by $\{y\}$ in a similar way. $K_{x,i}$ and $K_{y,i}$ are served as probability selection parameters of CCDM, where the selectable probability set is {p1, p2, p3, p4}. The elements in the probability set represent the probability distribution of CCDM output symbols. For example, in the shaped 16QAM symbol, the elements of the probability set: p1 is [0.22, 0.28, 0.28, 0.22]; p2 is [0.19, 0.31, 0.31, 0.19]; p3 is [0.13, 0.37, 0.37, 0.13]; p4 is [0.1, 0.4, 0.4, 0.1].

Secondly, the IQ mixer is controlled by key sequence $K_{z,i}$, which is generated by (6).

$$K_{z,i} = \mathrm{mod}(Extract(z_i, 15), 2) \tag{6}$$

When $K_{z,i}$ is 1, the symbols in I and Q should be exchanged, whereas when $K_{z,i}$ is 0, symbol exchange is not performed.

Lastly, all QAM symbols are arranged as a $M \times N$ matrix $D_{M\times N}$, where M is sum of CCDM modules and N is block length in CCDM module. Note that each row in the matrix $D_{M\times N}$ is a block of CCDM. The key sequences $K_{w,i}$ and $K_{u,i}$ represent random index vector with the ascending order in chaotic sequence $\{w\}$ and $\{u\}$, which is defined as (7).

$$K_{w,i} = sort(w) \tag{7}$$

$$K_{u,i} = sort(u) \tag{8}$$

According to $K_{w,i}$ and $K_{u,i}$, the elementary matrixes $H_{M\times M}$ and $F_{N\times N}$ are obtained. Then, the scramble rule is shown in the following formula

$$C_{M\times N} = H_{M\times M} D_{M\times N} F_{N\times N} \tag{9}$$

The scrambled matrix is represented by $C_{M\times N}$. After taking the above operations, the purpose of scrambling the probability distribution of CCDM output symbols has been completed. The symbols whose probability distribution is scrambled are processed by discrete Fourier transform spread OFDM (DFTs-OFDM).

Experimental Setup and Results

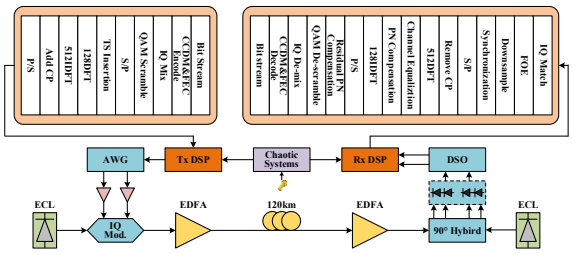

Fig. 2: Experiment setup and DSP flows.

The experimental setup and digital signal process (DSP) flows are shown in Fig. 2. A coherent optical transmission with 120 km fiber is constructed. An arbitrary waveform generator (AWG) with sampling rate 10 GSa/s generates electrical signal. An external cavity laser, whose linewidth is 100 kHz, provides a stable optical carrier with 1550 nm of wavelength and 10 dBm of power. The electrical signal is amplified by electrical amplifier (EA). Next, an IQ modulator (IQ Mod.) loads electrical signal into optical signal. The power of optical signal is amplified to 0dBm by an erbium-doped fibre amplifier (EDFA). After 120 km standard single mode fibre (SSMF) transmission, another EDFA is adopted to power compensation. A local optical signal with 10 dBm is used for coherent demodulation. A digital storage oscilloscope (DSO) with 20 GSa/s captures electrical signal.

Fig. 3(a) shows the probability of low-amplitude symbols at the output of the CCDM module, IQ mixing and QAM symbols scrambling. The statistical range is the symbol length of 100

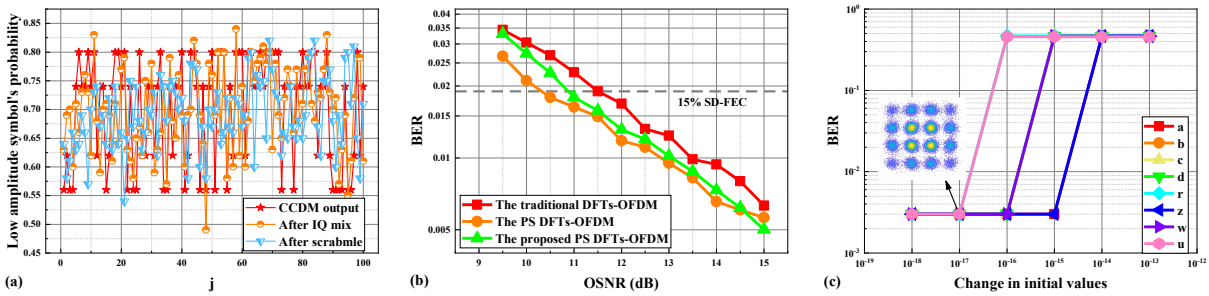

Fig. 3: (a) Low amplitude symbol's probability in 100 CCDM blocks, (b) BER curves of the traditional DFTs-OFDM, PS DFTs-OFDM and proposed PS DFTs-OFDM signals after 120km fiber and (c) BER performance of the proposed PS DFTs-OFDM signal with tiny changes of different initial values.

CCDM blocks, where j represents j th CCDM block. In this paper, we set the probability set of CCDM output symbols as: p1 is [0.22, 0.28, 0.28, 0.22]; p2 is [0.19, 0.31, 0.31, 0.19]; p3 is [0.13, 0.37, 0.37, 0.13]; p4 is [0.1, 0.4, 0.4, 0.1]. Since the four probability sets are selected randomly, the average entropy of the signal is 3.8 bit. We calculate the Pearson correlation coefficients between the probability distributions of low-amplitude symbols after probability scrambling and CCDM output, respectively. The Pearson correlation coefficient after IQ mixing is 0.5678, while the Pearson correlation coefficient is reduced to 0.1195 after QAM symbols scrambling. This proves that the probability of PS is successfully scrambled. It is difficult for Eve without key to effectively extract probability info.

We also measure the BER performance of proposed PS DFTs-OFDM signal over 120 km fiber transmission, as showed in Fig. 3(b). Meanwhile, the BER curves of the traditional DFTs-OFDM signal without any process and the PS DFTs-OFDM signal are recorded as the benchmark groups. Note that net data rates of three signals are maintained at the same by adjusting the AWG sampling rate. When the OSNR is 11.5 dB, the BER of the traditional DFTs-OFDM signal reaches the SD-FEC threshold of 15% overhead. In addition, we also notice, that the OSNR of the PS DFTs-OFDM signal and proposed PS DFTs-OFDM signal has been improved by about 1.2 dB and 0.6 dB respectively, compared with the traditional DFTs-OFDM signal. An OSNR difference of 0.6 dB exists between the proposed PS DFTs-OFDM signal and PS DFTs-OFDM signal, which is due to the BER performance penalty caused by our probability scrambling algorithm. It is worth noticed that the BER performance penalty will gradually decrease as OSNR increases. For illegal party without key, even if the constellation diagram is similar to the legal party, the BER performance is maintained at 0.47. This phenomenon proves that our scheme effectively prevents eavesdropping.

Moreover, we further discuss the security of proposed scheme and plot the results in Fig. 3(c). The BER performance curves are measured when OSNR is 15 dB. For the sensitive characteristics of the initial value of the chaotic system, we change the initial value by adding or subtracting a small value (e.g. 1×10^{-17}) to measure change of BER. The chaotic system initial values are set as $x_0 = 3$, $y_0 = -4$, $z_0 = 5$, $w_0 = -6$ and $u_0 = 0.8$. We change the 8 parameters of a, b, c, d, r, z, w and u respectively, and then measure the corresponding BER performance. Note that x and y are only used to select the probability set for CCDM. Because the frequency of symbols in a period of time can be counted to infer the probability distribution, so x and y have no contribution to the improvement of security. It can be seen from Fig. 3(c) that the BER performance will sharply deteriorated to about 0.47 when a and z changed by 1×10^{-14}, b, c, d and w changed by 1×10^{-15}, r and u changed by 1×10^{-16}. Therefore, the total key space of our scheme is $(10^{14})^2(10^{15})^4(10^{16})^2 = 10^{120}$. The huge key space can provide sufficient security against brute force attacks from illegal parties.

Conclusions

In this paper, we propose and experimentally demonstrate a probabilistic shaping probability distribution scrambling scheme based on chaotic systems. The proposed scheme is based on IQ mixing and QAM symbols scrambling to scramble CCDM output's probability distribution. With the implementation of a 4D Chen system and a Logistic system, the key space reaches 10^{120} resisting interception by illegal parties. The experimental results indicate that the proposed scheme has a 0.6 dB OSNR penalty compared with PS without encryption.

Acknowledgements

This work is supported in part by NSFC (61831003, 62021005, 62101063), Beijing Natural Science Foundation (4232011).

References

[1] K. Kikuchi, "Fundamentals of Coherent Optical Fiber Communications," *Journal of Lightwave Technology*, vol. 34, no. 1, pp. 157-179, 1 Jan.1, 2016, DOI: 10.1109/JLT.2015.2463719

[2] J. Cho and P. Winzer, "Probabilistic Constellation Shaping for Optical Fiber Communications," *Journal of Lightwave Technology*, vol. 37, no. 6, pp. 1590-1607, 2019.
DOI: 10.1109/JLT.2019.2898855 .

[3] P. Schulte and G. Böcherer, "Constant Composition Distribution Matching," in *IEEE Transactions on Information Theory*, vol. 62, no. 1, pp. 430-434, Jan. 2016, DOI: 10.1109/TIT.2015.2499181

[4] J. Ren, B. Liu, D. Zhao, S. Han, S. Chen, Y. Mao, Y. Wu, X. Song, J. Zhao, X. Liu, and X. Xin, "Chaotic constant composition distribution matching for physical layer security in a PS-OFDM-PON," *Optics Express*, vol. 28, no. 26, pp. 39266-39276, 2020, DOI: 10.1364/OE.413024

[5] Y. Luo, C. Zhang, X. Liang, J. Peng, B. Liu, and K. Qiu, "Secure OFDM-PON using three-dimensional selective probabilistic shaping and chaos," *Optics Express*, vol. 30, no. 14, pp. 25339-25355, 2022, DOI: 10.1364/OE.461196

[6] Z. Zhang, Y. Luo, C. Zhang, X. Liang, M. Cui and K. Qiu, "Constellation Shaping Chaotic Encryption Scheme With Controllable Statistical Distribution for OFDM-PON," in *Journal of Lightwave Technology*, vol. 40, no. 1, pp. 14-23, Jan.1, 2022, DOI: 10.1109/JLT.2021.3119013

[7] Y. Chen, J. Chen, M. Zhang, W. Li, D. Liu, and Ming Tang, "High-security constellation shaped self-homodyne coherent system with 4-D joint encryption," *Optica Express*, vol. 31, no. 2, pp. 3153-3167 (2023) DOI: 10.1364/OE.477149

[8] R. Tang, B. Liu, Y. Mao, R. Ullah, J. Ren, X. Xu, J. Zhao, M. Li, S. Chen and Y. Han, "High security OFDM-PON based on an iterative cascading chaotic model and 4-D joint encryption", *Optics Communications*, vol. 495, 2021, DOI: 10.1016/j.optcom.2021.127055

[9] Y. Gu, F. Tian, T. Wu, J. Wang, Q. Zhang, Q. Tian, Y. Wang, R. Ullah and X. Xin, "Experimental Demonstration of Superimposed Probabilistic 16CAP With the Joint Chaotic Model in a Multi-Core Transmission System," in *IEEE Photonics Journal*, vol. 14, no. 3, pp. 1-6, June 2022, DOI: 10.1109/JPHOT.2022.3174221

[10] X. Tang, Z. Xu, F. Li, Z. Li, L. Liu, C. Yang, H. Huang, L. Chen, and X. Zhang, "A Physical Layer Security-Enhanced Scheme in CO-OFDM System Based on CIJS Encryption and 3D-LSCM Chaos," *Journal of Lightwave Technology*, vol. 40, no. 12, pp. 3567-3575, 2022.
DOI: 10.1109/JLT.2022.3153967