CHINESE OPTICS LETTERS
Vol. 19, No. 1 | January 2021

Physical layer data encryption using two-level constellation masking in 3D-CAP-PON

Shuaidong Chen (陈帅东)[1], Bo Liu (刘 博)[1*], Yaya Mao (毛雅亚)[1], Jianxin Ren (任建新)[2], Xiumin Song (宋秀敏)[2], Rahat Ullah[1], Delin Zhao (赵德林)[1], Lei Jiang (姜 蕾)[1], Shun Han (韩 顺)[1], Jianye Zhao (赵建业)[1], Jiajia Shen (沈佳佳)[1], and Xueyang Liu (刘雪阳)[3]

[1] Nanjing University of Information Science and Technology, Nanjing 210044, China
[2] Beijing University of Posts and Telecommunications, Beijing 100876, China
[3] University of Wollongong, NSW 2522, Australia

*Corresponding author: bo@nuist.edu.cn

Received July 20, 2020 | Accepted September 4, 2020 | Posted Online November 24, 2020

A novel physical layer data encryption scheme using two-level constellation masking in three-dimensional (3D) carrier-less amplitude and phase modulation (CAP) passive optical network (PON) is proposed in this Letter. The chaotic sequence generated by Chua's circuit model realizes two-level encryption of displacement masking and constellation rotation for 3D constellations. We successfully conduct an experiment demonstrating 8.7 Gb/s 3D-CAP-8 data transmission over 25 km standard single-mode fiber. With two-level constellation masking, a key space size of 2.1×10^{85} is achieved to bring about high security and good encryption performance, suggesting broad application prospects in future short-range secure communications.

Keywords: physical layer data encryption; constellation masking; carrier-less amplitude and phase modulation; passive optical network.
DOI: 10.3788/COL202119.010601

1. Introduction

Recently, due to the rapid development of information technologies such as 4K video, cloud computing, and virtual reality (VR) and due to the merging of optical and wireless communications, bandwidth demand by the end users is continuously increasing[1]. As far as the current access network is concerned, the passive optical network (PON) has proved to be a future-oriented network architecture due to its provision of high bandwidth, with low cost and high-speed data transmission rate across the long haul networks[2,3]. Further, various researches are proposed for introducing new and advanced modulation formats that are deployed in the PON system. A time division multiplexing (TDM) and wavelength division multiplexing (WDM)/TDM long reach 10 Gb/s PON architecture of 100 km reach with no infield amplification or dispersion compensation was achieved[4]. A colorless scheme supporting 40 Gb/s downlink and uplink transmissions-based differential phase shift keying (DPSK) and on–off keying (OOK), respectively, was produced[5]. Similarly, a symmetrical 50 Gb/s TDM-PON system for the O-band based on 25G optics was investigated[6]. A 100 Gb/s space-division multiplexing PON (SDM-PON) system using commercial 10G class directly modulated laser (DML) that is modulated with 25/28 Gb/s data signals was presented[7]. In addition, a traffic estimation based on a long short-term memory neural network for PON was proposed to improve the performance of the system[8]. Although the PON expands the scope of access, it usually sends downlink data in the form of a broadcast. All optical network units (ONUs) connected to the optical line terminal (OLT) can receive downlink data frames. Therefore, an illegal ONU can be disguised as a legal ONU to hijack the downlink data signal sent by the OLT, so it is extremely important to encrypt the information before its transmission via downlink of the PON system[9,10]. Among various current physical layer encryption schemes, chaotic-based secure communication technology has broad prospects in the field of secure communication due to its high initial sensitivity, large bandwidth, and noise-like characteristics. Encrypted communication schemes with chaotic systems have been widely studied and proved to have superior confidentiality and anti-deciphering capabilities. Therefore, applying chaotic systems to encrypt the communication at the physical layer is considered a promising encryption scheme[11–14].

However, these chaotic encryption methods for the PON at the physical layer are based on the quadrature amplitude modulation (QAM) constellation to perform random position change, phase compensation, position exchange between different constellation points, and rotation of the constellation points for encryption. In fact, the high-dimensional constellation can further expand the Euclidean distance between the constellation points, which makes the position of the constellation points more flexible and the encryption method more diverse. It can also improve the system's bit error rate (BER) performance.

Compared to QAM, carrier-less amplitude and phase modulation (CAP) uses two fixed filters whose impulse responses are Hilbert transform pairs[15]. Two channels of signals are filtered and then superimposed and transmitted so that CAP does not need to use expensive mixer. At the receiver, QAM utilizes coherent reception with a complex structure, while CAP only needs to pass the received signal to the filter matched with the curing filter at the transmitting end that can restore the original signal. In Ref. [16], a novel constellation-shaping CAP modulation scheme was proposed to alleviate the systematic nonlinearity in visible light communication (VLC) systems. A CAP-PON downstream with enhanced bandwidth efficiency was proposed that can be translated into savings in cost and power consumption[17]. In Ref. [18], a high-security CAP-PON based on floating probability disturbance was presented, which combined probabilistic shaping (PS) and chaotic sequences to improve the security and performance of the CAP-PON. Designing more dimensional CAP filters can achieve more ONU access, and the expansion method is also very simple. It can be achieved by adding a few filters at both the transmitting and receiving ends. This multi-dimensional CAP meets the low cost and low energy consumption required by PON for capacity expansion. A security-enhanced three-dimensional (3D)-CAP-PON based on two-stage spherical constellation masking was proposed that used chaotic sequence to encrypt the signal to improve the security of CAP-PON[19]. It can be seen that 3D and even higher-dimensional CAP-PON will become a new research hotspot.

In this paper, to the best of our knowledge, we propose for the first time a physical layer data encryption scheme using two-level constellation masking in 3D-CAP-PON. Chua's circuit model is used to generate three sets of chaotic sequences, which are then applied to generate displacement and rotation vectors, respectively. The original constellation points are encrypted by these vectors. Through two-level encryption, the constellation points are distributed into a noise-like spherical structure, which effectively improves the security performance of 3D-CAP-PON. To further test the system performance, 25 km standard single-mode fiber (SSMF) data transmission employing the proposed encrypted 3D-CAP-8 signal is successfully demonstrated in the experiment.

2. Principle

The principle diagram of the proposed physical layer data encryption using two-level constellation masking in 3D-CAP-PON is shown in Fig. 1. The original data is transformed into

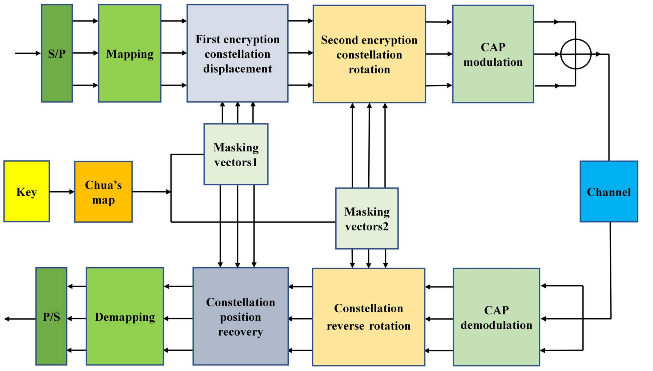
S/P
Mapping
First encryption constellation displacement
Second encryption constellation rotation
CAP modulation
Masking vectors1
Key
Chua's map
Masking vectors2
Channel
P/S
Demapping
Constellation position recovery
Constellation reverse rotation
CAP demodulation

Fig. 1. Schematic diagram of physical layer data encryption using two-level constellation masking in 3D-CAP-PON.

three-way signals through serial-parallel (S/P) conversion, which are then mapped onto a 3D constellation diagram. The initial key is subjected to Chua's chaotic mapping to generate chaotic sequences. According to these chaotic sequences, the constellation displacement and rotation masking vectors are generated, respectively. After two-level encryptions, the positions of the constellation have all been disrupted. 3D-CAP processes the three signals and merges them into a symbol for transmission. At the receiver, after 3D-CAP demodulation, the original key is employed to rotate and restore the position of the constellation point. Lastly, the original data is obtained by demapping and parallel-serial (P/S) conversion. The 3D constellation diagram we use is shown in Fig. 2(a). This diagram of the constellation is a structure of two concentric tetrahedrons. The inner four constellation points are distributed on a regular tetrahedron, and the other four constellation points are distributed on the outer regular tetrahedron. The minimum Euclidean distance between adjacent constellation points is two.

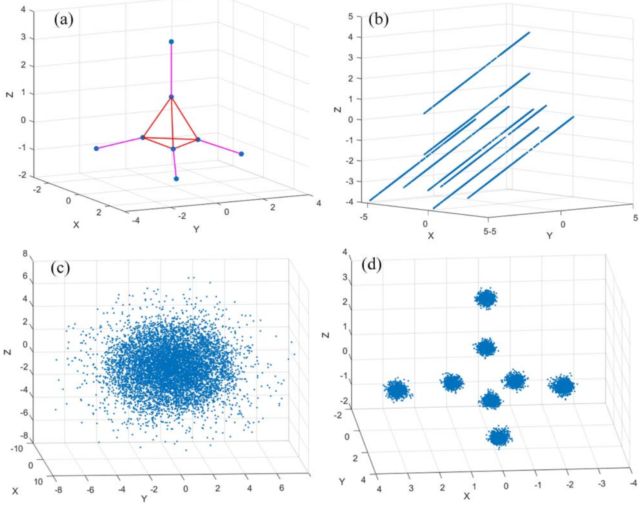

Fig. 2. Constellation diagram (a) before masking, (b) after constellation displacement masking, (c) after two-level constellation masking, and (d) with all of the correct keys.

Specifically, we utilize Chua's circuit model to encrypt constellation points, which can be expressed as[20]

$$\begin{aligned} \partial x_1/\partial t &= \alpha[y_1 - x_1 - f(x)], \\ \partial y_1/\partial t &= x_1 - y_1 + z_1, \\ \partial z_1/\partial t &= -\beta y_1, \\ f(x) &= bx_1 + 0.5(a-b)(|x_1+1| - |x_1-1|). \end{aligned} \quad (1)$$

Among them, α, β, a, b are constants, whose values are 8.8, 15, −1.3, −0.5. x_1, y_1, z_1, t are the variables. The initial value of (x_1, y_1, z_1) is set to (0.2, −0.15, 0.25). The ranges of the generated chaotic sequences are $x_1(-4,4), y_1 \in (-1,1), z_1 \in (-5,5)$, respectively. The phase diagram and bifurcation diagram of Chua's circuit model are shown in Fig. 3. It can be found from Fig. 3(a) that Chua's circuit model has a double scroll attractor and has complex chaotic characteristics. Figure 3(b) is a bifurcation diagram of Chua's circuit model. As can be seen from the figure, the distribution of the x_1 value varies greatly with different α. The generated sequence is very sensitive to the initial value, which is precisely required for secure communication. In our scheme, in order to further improve the randomness of chaotic sequences, we introduce a sampling factor $L = 5$, which means that the generated sequence would be sampled with a sampling factor of 5. The masking vector of displacement change can be expressed as

$$S = \mathrm{mod}[x_2, \mathrm{floor}\,(x_2 - 0.5)]. \quad (2)$$

Here, x_2 is the new sequence after sampling. Assuming that the coordinates of the original 3D constellation point are (x_m, y_m, z_m), then the coordinates of the constellation point after the displacement vector encryption can be expressed as

$$\begin{cases} x' = x_m + S \\ y' = y_m + S \\ z' = z_m + S \end{cases}, \quad (3)$$

where (x', y', z') is the constellation point coordinates after displacement masking. The encrypted constellation points are shown in Fig. 2(b). It can be found from the figure that the encrypted constellation presents eight bar structures. In our encryption process, the displacement vectors added in three dimensions are consistent, which causes the slopes of these eight lines to be the same.

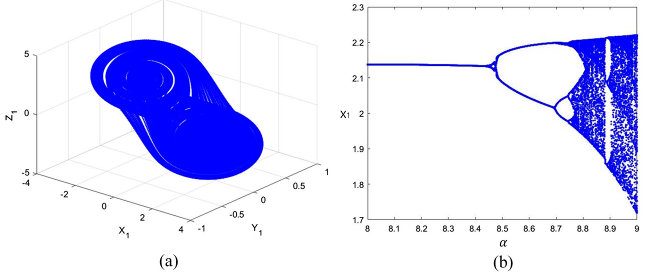

Fig. 3. (a) Phase diagram and (b) bifurcation diagram of the Chua's chaotic model.

As can be seen from Fig. 2(b), the distribution of the constellation points after the displacement transformation is regular, and it is easy to be eavesdropped on by the illegal receiver. It is necessary to perform secondary encryption on the constellation points. Therefore, we utilize the transformation relationship between the Euler angle and quaternion to realize the rotation encryption of constellation points. In 3D graphics, the most commonly used rotation representation methods are quaternion and Euler angle, which has the advantages of saving storage space and easy interpolation compared to the matrix. Chua's circuit model is also used to generate chaotic sequences in the rotation masking and deal with the produced chaotic sequence. Assuming that the original chaotic sequence is (x_c, y_c, z_c) in order to rotate the Euler angle of 0–360 deg, the chaotic sequence is amplified in equal proportions, and the remainder is generated to produce a rotation angle of 0–360:

$$\begin{cases} x_r = \mathrm{floor}[\mathrm{mod}(x_c \times 10^3, 360)] \\ y_r = \mathrm{floor}[\mathrm{mod}(y_c \times 10^3, 360)] \\ z_r = \mathrm{floor}[\mathrm{mod}(z_c \times 10^3, 360)] \end{cases}, \quad (4)$$

where (x_r, y_r, z_r) represents the angle of Euler angle transformation. These generated rotation sequences are used to encrypt the constellation points after the displacement masking:

$$\mathrm{quaternion} = \mathrm{angle2quat}(z_r, y_r, x_r), \quad (5)$$

$$(x, y, z) = \mathrm{quatrotate}[\mathrm{quaternion},(x', y', z')]. \quad (6)$$

Equation (5) turns the 3D Euler angle into a quaternion, and Eq. (6) rotates the constellation point after the displacement masking, where (x', y', z') is the coordinates of the constellation point after the masking of displacement, and (x, y, z) is the coordinates of the constellation point after two-level encryptions. The encrypted constellation is shown in Fig. 2(c). After two-level encryptions, the 3D constellation has been completely disrupted, and its distribution is similar to noise so that illegal receivers cannot correctly eavesdrop and steal the transmitted information, which greatly improves the security of the system and transmission performance of the system. If you have all of the keys, you can accurately restore the constellation diagram, as shown in Fig. 2(d).

3. Experimental Setup and Results

The experimental setup of the proposed physical layer data encryption using two-level constellation masking 3D-CAP-8 is demonstrated in Fig. 4. At the transmitter side, the original data is mapped onto 3D constellation points. Then, the Chua's model is utilized to generate masking vectors to change the position and rotation of constellation points. The masked symbol will be up-sampled with a factor of 7. Three orthogonal filters of CAP process the corresponding parts of the signal, respectively, and add the output of three orthogonal filters as a 3D-CAP-8 signal. The encrypted signals are loaded to an

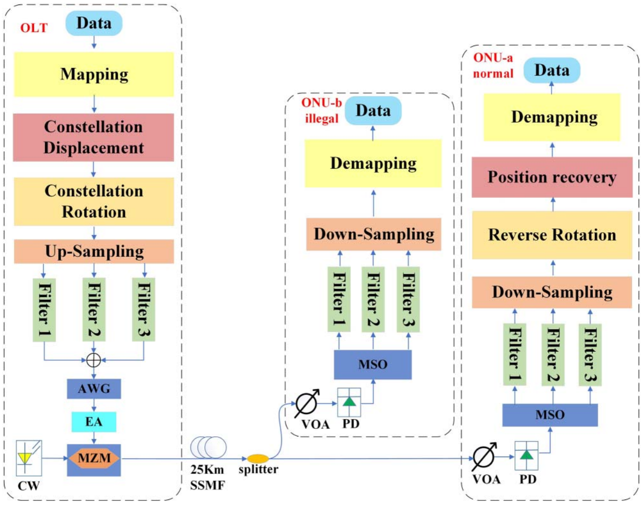

Fig. 4. Experimental setup (CW, continuous wave laser; MZM, Mach–Zehnder modulator; EA, electric amplifier; AWG, arbitrary waveform generator; SSMF, standard single-mode fiber; VOA, variable optical attenuator; PD, photodetector; MSO, mixed signal oscilloscope).

arbitrary waveform generator (AWG, TekAWG70002A) to produce the corresponding electrical waveform, which is amplified by an electric amplifier (EA). Onward, a Mach–Zehnder modulator (MZM) is utilized for riding over the encrypted information signal over the carrier, where a continuous wave (CW) laser source emits a light beam with a wavelength of 1550 nm. The modulated 3D-CAP-8 signal is transmitted with a 25 km SSMF. At the receiver side, a variable optical attenuator (VOA) is used for testing the BER behavior at different optical receiving powers. The signal is then detected by a photodetector (PD), and a mixed signal oscilloscope (MSO, TekMSO73304DX) is applied to record the data. The digital signal processing (DSP) unit at the receiver side performs the reverse process done at the transmitter side, including matched filters, down-sampling, constellation demasking, demapping, and, lastly, to restore the original data.

Figure 5 depicts the BER curve of the legal ONU and illegal reception before and after the transmission of 25 km. The legal ONU has the correct key including the control parameters, initial values, and step size of the chaotic model, while the illegal ONU does not know the key. For the encrypted 3D-CAP-8 signal, compared to back-to-back (b2b) configuration, the power penalty after 25 km SSMF transmission is about 0.45 dB at a BER of 1×10^{-3}. At the same time, as the received optical power increases, the BER of the legal ONU gradually decreases, and the BER of the illegal ONU has been maintained at about 0.5. Obviously, the illegal ONU cannot obtain any information like the legal ONU without having the information about the correct key. Figure 5 also inserts the reception constellation diagrams of the legal ONU and the illegal ONU when the received optical power is −11 dBm. The legal ONU obtains a clear 3D constellation diagram, and the constellation diagram obtained by the illegal ONU is meaningless, dense, and disorderly in a spherical shape.

In order to further explore the encryption security level of the proposed scheme, we have explored the sensitivity of the initial value. The experiment tests the BER curve when the received optical power is set to −10 dBm after a small initial value change, after 25 km SSMF transmission. The initial values (x_0, y_0, z_0) of Chua's circuit model are set to (0.2, −0.15, 0.25), respectively. For the three initial values, we test their impact on the BER curve under different small changes. It can be seen from Fig. 6 that when the initial value changes to 10^{-17}, there is no obvious change in the BER compared to the original correct parameter value. However, once the initial value changes to 10^{-16}, the BER of the system has been dramatically increased, and the value of the BER is close to 0.48. When the change of the initial value is 10^{-15} or larger, the system's BER has no significant change. This shows that our encryption method is very sensitive to the initial value. Therefore, for our system, a total of seven key parameters $(\alpha, \beta, a, b, x_0, y_0, z_0)$ can at least achieve a key space of

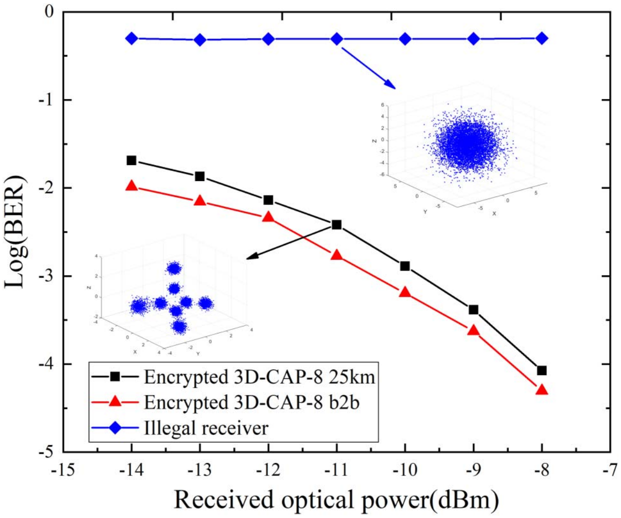

Fig. 5. BER curves of illegal receiver, 3D-CAP-8 for back-to-back (b2b) and 25 km transmission.

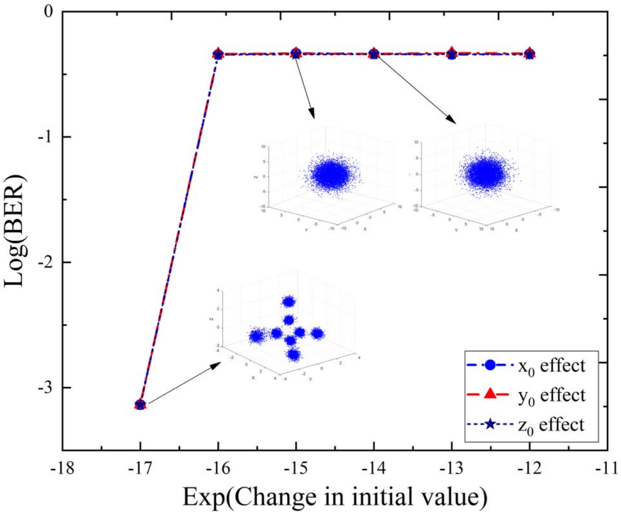

Fig. 6. BER measurements with a tiny change in initial value.

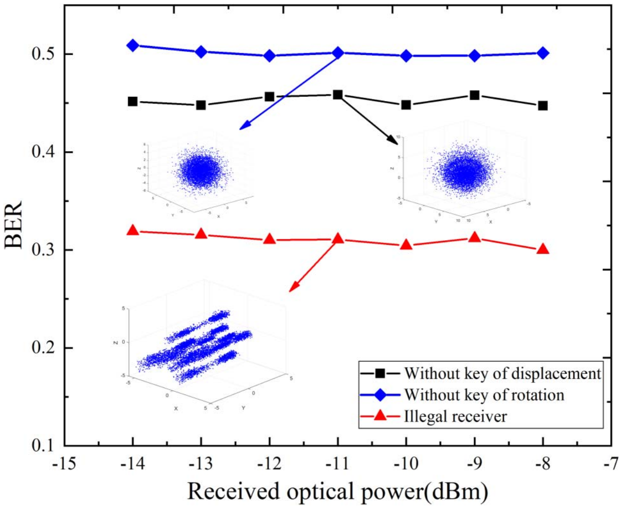

Fig. 7. Measured BER curves at the illegal receiver with different keys.

$2^{31} \times 2^{31} \times 2^{31} \times 2^{31} \times 10^{16} \times 10^{16} \times 10^{16} = 2.1 \times 10^{85}$, which can effectively resist illegal attacks.

To investigate the performance of an illegal receiver with different keys, we did further experiments without key of displacement and without key of rotation. The measured BER curves are illustrated in Fig. 7. When all of the security keys are wrong, the BER of the illegal receiver is around 0.5. The received constellation is shown in Fig. 7, which is completely non-understandable. When the keys of displacement are obtained, the BER would be around 0.46. The constellation diagram is similar to the illegal receiver, which is also like the spherical structure.

However, compared with the illegal receiver, this constellation has a larger range of constellation distribution due to the displacement masking. When keys of rotation are known by the illegal receiver, the BER would be about 0.31. The constellation diagram is also shown in Fig. 7. Because of the rotating masking key, the entire constellation diagram is equivalent to only the displacement masking, and the constellation diagram is consistent with Fig. 2(b). With only the displacement masking, the constellation distribution is regular, and its BER is relatively low, which is the reason for second-level encryption. After two-level encryption, the constellation has a spherical distribution similar to noise whose key space reaches 2.1×10^{85}, which can ensure high security in short-distance communication.

4. Conclusion

We have proposed a physical layer data encryption using two-level constellation masking in 3D-CAP-PON. Chua's model is applied to generate chaotic sequences to produce the masking vector of two-level encryption. The use of 3D constellation points for encryption can increase the minimum Euclidean distance, thereby obtaining a larger constellation space and a more flexible and variable encryption scheme. With two encryption methods to encrypt the constellation twice, the 3D constellation points turn into a noise-like spherical structure, which can effectively improve the security of the system. The encryption scheme we propose has a key space of 2.1×10^{85}, which can effectively resist attacks from illegal receiving ends. An experimental demonstration of encrypted 3D-CAP-8 signal transmission over 25 km SSMF is successfully conducted. The experimental results show that the proposed encryption system has very strong anti-attack performance and has good application prospects in future 3D-CAP-PON.

Acknowledgement

The project was supported by the National Key Research and Development Program of China (No. 2018YFB1801302), National Natural Science Foundation of China (Nos. 61835005, 61822507, 61522501, 61475024, 61675004, 61705107, 61727817, 61775098, 61720106015, and 61875248), Beijing Young Talent (No. 2016000026833ZK15), Open Fund of IPOC (BUPT) (No. IPOC2019A011), Jiangsu Talent of Innovation and Entrepreneurship, Jiangsu Team of Innovation and Entrepreneurship, and Postgraduate Research & Practice Innovation Program of Jiangsu Province (No. KYCX20_0963).

References

1. Y. J. Guo, O. Alkhazragi, C. H. Kang, C. Shen, Y. Mao, X. B. Sun, T. K. Ng, and B. S. Ooi, "A tutorial on laser-based lighting and visible light communications: device and technology," Chin. Opt. Lett. **17**, 040601 (2019).
2. K. Ohara, A. Tagami, H. Tanaka, M. Suzuki, T. Miyaoka, T. Kodate, T. Aoki, K. Tanaka, H. Uchinao, S. Aruga, H. Ohnishi, H. Akita, Y. Taniguchi, and K. Arai, "Traffic analysis of Ethernet-PON in FTTH trial service," in *Optical Fiber Communications Conference* (2003), paper ThAA2.
3. Y. Luo, X. Zhou, F. Effenberger, X. Yan, G. Peng, Y. Qian, and Y. Ma, "Time- and wavelength-division multiplexed passive optical network (TWDM-PON) for next-generation PON stage 2 (NG-PON2)," J. Lightwave Technol. **31**, 587 (2013).
4. J. D. Downie, A. Boh Ruffin, and J. Hurley, "Ultra-low-loss optical fiber enabling purely passive 10 Gb/s PON systems with 100 km length," Opt. Express **17**, 2392 (2009).
5. C. W. Chow and C. H. Yeh, "40-Gb/s downstream DPSK and 40-Gb/s upstream OOK signal remodulation PON using reduced modulation index," Opt. Express **18**, 26046 (2010).
6. C. C. Li, J. Chen, Z. X. Li, Y. X. Song, Y. C. Li, and Q. W. Zhang, "Demonstration of symmetrical 50-Gb/s TDM-PON in O-band supporting over 33-dB link budget with OLT-side amplification," Opt. Express **27**, 18343 (2019).
7. F. D. Bao, Y. H. Ding, M. Nooruzzaman, Y. Amma, Y. Sasaki, L. K. Oxenløwe, H. Hu, and T. Morioka, "DSP-free single-wavelength 100 Gbps SDM-PON with increased splitting ratio using 10G-class DML," Opt. Express. **27**, 33915 (2019).
8. M. Zhang, B. Xu, X. Y. Li, Y. Cai, B. J. Wu, and K. Qiu, "Traffic estimation based on long short-term memory neural network for mobile front-haul with XG-PON," Chin. Opt. Lett. **17**, 070603 (2019).
9. B. B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express **14**, 3738 (2006).
10. L. J. Zhang, X. J. Xin, B. Liu, and J. J. Yu, "Physical-enhanced secure strategy in an OFDM-PON," Opt. Express. **20**, 2255 (2012).
11. A. Sultan, X. Yang, A. A. Hajomer, and W. Hu, "Chaotic constellation mapping for physical-layer data encryption in OFDM-PON," IEEE Photon. Technol. Lett. **30**, 339 (2018).
12. A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, "Dynamic QAM mapping for physical-layer security using digital chaos," IEEE Access **6**, 47199 (2018).

13. C. F. Zhang, W. Zhang, C. Chen, X. J. He, and K. Qiu, “Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding,” J. Lightwave Technol. **36**, 1706 (2018).
14. L. J. Zhang, B. Liu, X. J. Xin, and D. M. Liu, “A novel 3D constellation-masked method for physical security in hierarchical OFDMA system,” Opt. Express **21**, 15627 (2013).
15. T. K. Zhong, X. Zhou, J. Huo, C. Yu, C. Lu, and A. P. T. Lau, “Digital signal processing for short-reach optical communications: a review of current technologies and future trends,” J. Lightwave Technol. **36**, 377 (2018).
16. Z. X. Wang, M. J. Zhang, S. Y. Chen, and N. Chi, “Carrier-less amplitude and phase modulated visible light communication system based on a constellation-shaping scheme,” Chin. Opt. Lett. **15**, 030602 (2017).
17. Z. Dong, J. Yu, and J. Lu, “Bandwidth-efficient WDM-CAP-PON using digital Hilbert single-sideband modulation,” IEEE Photon. J. **7**, 7903907 (2015).
18. J. Y. Zhao, B. Liu, Y. Y. Mao, J. X. Ren, X. Xu, X. Y. Wu, L. Jiang, S. Han, and J. Y. Zhang, “High-security physical layer in CAP-PON system based on floating probability disturbance,” IEEE Photon. Technol. Lett. **32**, 367 (2020).
19. J. X. Ren, B. Liu, X. Y. Wu, X. Xu, Y. Y. Mao, Y. F. Wu, X. M. Song, L. Jiang, J. Y. Zhang, Y. Zhang, and X. J. Xin, “Security-enhanced 3D-CAP-PON based on two-stage spherical constellation masking,” IEEE Access **8**, 111966 (2020).
20. M. J. Ogorzalek, Z. Galias, A. M. Dabrowski, and W. R. Dabrowski, “Chaotic waves and spatio-temporal patterns in large arrays of doubly-coupled Chua's circuits,” IEEE Trans. Circuits Syst. I: Fundam. Theory Appl. **42**, 706 (1995).