Optics Communications 398 (2017) 62–66

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Digital chaos-masked optical encryption scheme enhanced by two-dimensional key space

Ling Liu[a], Shilin Xiao[a,*], Lu Zhang[a], Meihua Bi[a,b], Yunhao Zhang[a], Jiafei Fang[a], Weisheng Hu[a]

[a] *Shanghai Jiao Tong University, State Key Laboratory of Advanced Optical Communication Systems and Networks, 800 Dongchuan Road, Shanghai 200240, China*

[b] *Hangzhou Dianzi University, College of Communication Engineering, Xiasha Gaojiaoyuan 2rd Street, Hangzhou 310018, China*

ARTICLE INFO

Keywords:
Optical encryption
Chaos
Two-dimensional key space
OFDM

ABSTRACT

A digital chaos-masked optical encryption scheme is proposed and demonstrated. The transmitted signal is completely masked by interference chaotic noise in both bandwidth and amplitude with analog method via dual-drive Mach-Zehnder modulator (DDMZM), making the encrypted signal analog, noise-like and unrecoverable by post-processing techniques. The decryption process requires precise matches of both the amplitude and phase between the cancellation and interference chaotic noises, which provide a large two-dimensional key space with the help of optical interference cancellation technology. For 10-Gb/s 16-quadrature amplitude modulation (QAM) orthogonal frequency division multiplexing (OFDM) signal over the maximum transmission distance of 80 km without dispersion compensation or inline amplifier, the tolerable mismatch ranges of amplitude and phase/delay at the forward error correction (FEC) threshold of 3.8×10^{-3} are 0.44 dB and 0.08 ns respectively.

1. Introduction

With the exponential growth of Internet traffic and bandwidth requirements, optical fiber network has become an important solution in modern high-speed transmission system [1]. Since the demands of privacy protection and information security for ordinary and military users increase rapidly, the security issues in optical transmission system have attracted massive attention [2,3]. Compared with encryption in higher layers such as the media access control (MAC) layer, encryption in physical layer is a better choice since it can provide overall protection for both data transmission and header information [4,5]. To enhance the confidentiality of physical layer, secure transmission based on chaos has been widely studied due to its advantages of broadband, noise-like, pseudo-periodicity and unpredictable [6]. For the encryption schemes based on optical chaos [7–9], a delayed-feedback loop is widely used to generate the optical chaotic carrier, however, the delay time as its most critical security key can be cracked with several methods [10]. For other encryption schemes based on digital chaos, there are two steps at the transmitter (TX), chaos generation and encryption. The conventional scheme [11–13] implements both steps with digital method. This type of encryption method is called chaotic coding whose encrypted signal is digital, an eavesdropper can easily record it and use post-processing technique to recover the original signal [14]. To cope with these issues, we propose a novel encryption scheme in which the chaos generation is implemented with digital method while the encryption uses analog method based on the mixture of signal and interference chaos at dual-drive Mach-Zehnder modulator (DDMZM). This type of encryption method is named digital chaos-masked whose encrypted signal is analog, consequently, the received encrypted signal cannot be digitized by the receiver without analog decryption. Its decryption process requires the accurate matches of both the amplitude and phase between the cancellation chaos and interference chaos before post-processing with the help of optical interference cancellation technology shown in our previous work [15], which form a large two-dimensional key space and hence enhance the key space significantly. The digital chaos-masked method combined with the optical interference cancellation technology can provide reliable encryption scheme that satisfies the requirement of high speed, noise-like encrypted signal and large key space in physical layer security.

In this paper, a novel digital chaos-masked optical encryption scheme enhanced by two-dimensional key space is proposed and demonstrated. The scheme is suitable for all kinds of signal with various modulation formats and supports massive application scenarios such as passive optical network (PON) and wavelength division multiplex (WDM) system. The 10-Gb/s 16-quadrature amplitude

[*] Corresponding author.
E-mail address: slxiao@sjtu.edu.cn (S. Xiao).

http://dx.doi.org/10.1016/j.optcom.2017.04.015
Received 3 March 2017; Received in revised form 27 March 2017; Accepted 6 April 2017

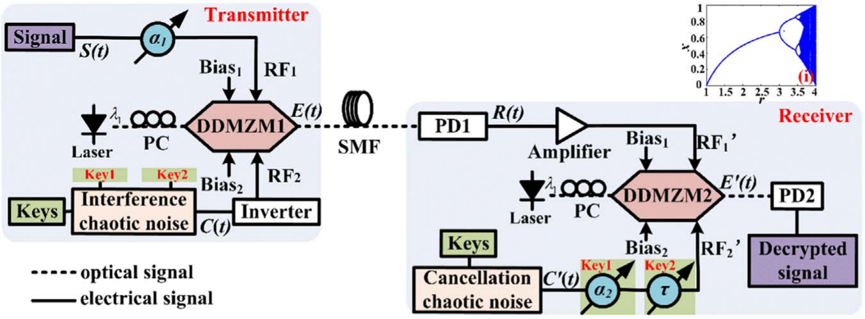

Fig. 1. Architecture of the proposed digital chaos-masked optical encryption system. PC: polarization controller; α: tunable attenuator; DDMZM: dual-drive Mach-Zehnder modulator; RF: radio frequency; SMF: single mode fiber; PD: photo-detector; τ: tunable time delay.

modulation (QAM) orthogonal frequency division multiplexing (OFDM) signal and single channel are chosen to verify the feasibility. Results show that, under the maximum transmission distance of 80 km, the tolerable mismatch ranges of amplitude and delay at the forward error correction (FEC) threshold of 3.8×10^{-3} [16] are 0.44 dB and 0.08 ns respectively. The reminder of this paper is organized as follows. Section 2 describes the principle theoretically. Section 3 first investigates the effect of signal's concealment depth on system confidentiality, and then the tolerable amplitude and phase/delay mismatch ranges at the FEC limit for legal receiver (RX) over various transmission distances are studied. Meanwhile, the anti-dawning ability against eavesdropping is tested as well. Conclusions are given in Section 4.

2. Principle

The architecture of the proposed digital chaos-masked optical encryption system is demonstrated in Fig. 1. At the TX, a simple one dimensional Logistic map with low complexity is adopted to generate the original interference chaotic noise C"(t), whose mapping equation is given by Eq. (1) [17],

$$x_{k+1} = rx_k(1 - x_k),\ 0 < x_k < 1 \tag{1}$$

where k denotes the k-th iteration, r is the bifurcation parameter and x_k is the k-th iterated value. Seen from the track of Logistic mapping presented in the insert (i) of Fig. 1, when r is within the range of (3.57, 4], it will exhibit chaotic behavior. It has also been proven that the logistic chaotic sequence will be quite different under a tiny discrepancy of the initial values [11]. We set the initial state r to 4 and x_0 to 0.1666, which are the keys of C"(t). By presetting the attenuation α_{pre} and delay τ_{pre} of C"(t), C"(t) turns into $\alpha_{\text{pre}}C$"(τ_{pre}) which is labeled as $C(t)$. Note that α_{pre} and τ_{pre} are key 1 and key 2 at the TX respectively as shown in Fig. 1. To protect the signal $S(t)$ from being decrypted, $C(t)$ needs to have strong amplitude and bandwidth overlap with $S(t)$. Therefore $S(t)$ is firstly attenuated by an attenuator α_1 and then delivered into the radio frequency (RF_1) port of DDMZM1. $C(t)$ is inverted first and then delivered into RF_2 port of the DDMZM1. The optical phase ϕ_1 and ϕ_2 of two arms in DDMZM1 are shown in Eqs. (2) and (3) respectively,

$$\phi_1 = \frac{\pi}{V_\pi}V_1 = \frac{\pi}{V_\pi}(V_{\text{bias1}} + RF_1) = \frac{\pi}{V_\pi}(V_0 + V_\pi + \alpha_1 S(t)) \tag{2}$$

$$\phi_2 = \frac{\pi}{V_\pi}V_2 = \frac{\pi}{V_\pi}(V_{\text{bias2}} + RF_2) = =\frac{\pi}{V_\pi}(V_0 - C(t)) \tag{3}$$

where V_1 and V_2 are the drive voltages of upper branch and bottom branch at DDMZM1 respectively. Drive voltage is the sum of bias voltage V_{bias} and RF voltage. V_0 represents a random voltage in the bias voltage range of DDMZM1, V_{bias1} is set as V_0+V_π and V_{bias2} is set as V_0. The optical field E_{out} and power P_{out} of output signal $E(t)$ at the DDMZM1 are presented in Eqs. (4) and (5) respectively, where E_{in} and P_{in} are the optical field and power of the carrier emitted by laser respectively. The bias voltage of DDMZM1 is set to quadrature point for linear modulation. Then the encrypted signal $E(t)$ transmits through standard single mode fiber (SMF) without dispersion compensation or inline amplifier.

$$\begin{aligned} E_{out} &= \frac{E_{in}}{2}(e^{j\phi_1} + e^{j\phi_2}) = E_{in}\cos\frac{\phi_1 - \phi_2}{2}e^{j\frac{\phi_1+\phi_2}{2}} \\ &= E_{in}\cos(\frac{\pi}{2} + \frac{\pi}{2V_\pi}(C(t) + \alpha_1 S(t)))e^{j\frac{\phi_1+\phi_2}{2}} \end{aligned} \tag{4}$$

$$P_{out} = P_{in}\cos^2(\frac{\pi}{2} + \frac{\pi}{2V_\pi}(C(t) + \alpha_1 S(t))) \tag{5}$$

After detected by photo-detector (PD1) at the RX, the encrypted signal $R(t)$ shown in Eq. (6) is received. Then, the decryption process is performed. DDMZM2 is biased at quadrature point which is similar to DDMZM1. The optical phase $\phi_1{}^{'}$ and $\phi_2{}^{'}$ of its upper branch and bottom branch are shown in Eqs. (7) and (8) respectively, where α_{link} and τ_{link} are the attenuation and delay brought by the fiber channel and devices, V_1' and V_2' are the drive voltage of the upper branch and bottom branch respectively. For the bottom branch of DDMZM2, by precisely adjusting the attenuator α_2 and delay τ, the cancellation chaotic noise C'(t) turns into $\alpha_{\text{link}}C(\tau_{\text{link}})$. That is, time and amplitude of the RF_2' and the noise component in RF_1' are aligned to recover the desired signal. As shown by the optical field E_{out}' of the output signal E'(t) at DDMZM2 in Eq. (9), $\alpha_{\text{link}}C(\tau_{\text{link}})$ is subtracted and $\alpha_{\text{link}}\alpha_1 S(\tau_{\text{link}})$ is remained, where E_{in}' is the optical field of the carrier emitted by laser at RX. The output optical power P_{out}' of DDMZM2 is given in Eq. (10) where P_{in}' is the optical power of the laser. At last, after E'(t) is detected by PD2, the decrypted signal is received.

$$R(t) = \alpha_{\text{link}}(C(\tau_{\text{link}}) + \alpha_1 S(\tau_{\text{link}})) \tag{6}$$

$$\phi_1' = \frac{\pi}{V_\pi}V_1' = \frac{\pi}{V_\pi}(V_{\text{bias1}} + RF_1') = \frac{\pi}{V_\pi}(V_0 + V_\pi + \alpha_{\text{link}}(C(\tau_{\text{link}}) + \alpha_1 S(\tau_{\text{link}}))) \tag{7}$$

$$\phi_2' = \frac{\pi}{V_\pi}V_2' = \frac{\pi}{V_\pi}(V_{\text{bias2}} + RF_2') = =\frac{\pi}{V_\pi}(V_0 + C'(t)) \tag{8}$$

$$E_{out}' = \frac{E_{in}'}{2}(e^{j\phi_1'} + e^{j\phi_2'}) = E_{in}'\cos(\frac{\pi}{2} + \frac{\pi}{2V_\pi}(\alpha_{\text{link}}\alpha_1 S(\tau_{\text{link}}))e^{j\frac{\phi_1'+\phi_2'}{2}} \tag{9}$$

$$P_{out}' = P_{in}'\cos^2(\frac{\pi}{2} + \frac{\pi}{2V_\pi}\alpha_{\text{link}}\alpha_1 S(\tau_{\text{link}})) \tag{10}$$

In summary, the secure keys in this optical encryption system are: the keys of interference chaotic noise $C(t)$ at TX which is needed to generate cancellation chaotic noise C'(t) at RX, the delay and amplitude matching values between RF_2' and the noise component in RF_1' at DDMZM2 which are orthogonal to each other and consequent form a two-dimensional key space.

3. Simulation setup and result analysis

Following the system configuration in Fig. 1, simulation is con-

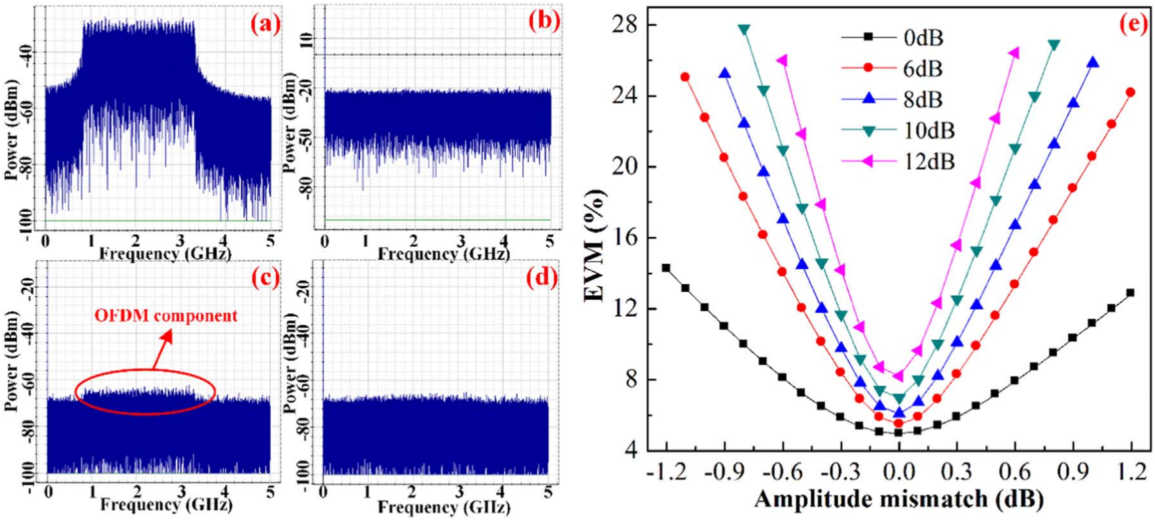

Fig. 2. RF spectra of (a) the OFDM signal $S(t)$, (b) the chaotic noise $C(t)$, (c) the encrypted signal $R(t)$ when α_1 attenuates 0 dB and (d) encrypted signal $R(t)$ when α_1 attenuates 6 dB. (e) Under different attenuation value of α_1, EVM performance of legal RX versus different amplitude mismatches of attenuator α_2 when the optimum matching value of delay τ is known in BtB transmission.

ducted on the commercial simulation software OptiSystem 7.0 combined with MATLAB. At both TX and RX, laser with 10-dBm output power, 0.1-MHz linewidth and 1550-nm wavelength is used as optical carrier. The 10-Gb/s 16-QAM OFDM signal is used as signal, which is generated offline by MATLAB following the procedures illustrated in our previous work [18]. The parameter settings are as follows. The FFT size is 128 points of which 32 subcarriers are used to carry 16-QAM mapped data and another 32 subcarriers are chosen for Hermitian symmetry operation to generate real value RF OFDM signal $S(t)$, occupying the frequency from 859 MHz to 3.28 GHz. The total number of the measured symbol is 1500. The chaotic noise is generated offline by MATLAB, the invert of $C(t)$ at the bottom branch of DDMZM1 is easy to implement offline in MATLAB as well. RF spectra of the OFDM signal $S(t)$ and interference chaotic noise $C(t)$ are presented by Fig. 2(a) and (b) respectively, clearly showing that $C(t)$ has a strong bandwidth overlap with $S(t)$. As mentioned in Section 2, $C(t)$ also needs to have a strong amplitude overlap with $S(t)$, so the attenuator α_1 needs adjusting to lower the amplitude of $S(t)$. When $S(t)$ is not attenuated, the spectrum of the encrypted signal $R(t)$ is shown in Fig. 2(c) where the OFDM component can be identified; while when $S(t)$ is attenuated by 6 dB and more, the OFDM component cannot be distinguished from $R(t)$ as depicted in Fig. 2(d).

To investigate the effect of signal's concealment depth on system confidentiality, under different attenuation values of α_1, Fig. 2(e) presents the error vector magnitude (EVM) performances of legal RX versus different amplitude mismatches of attenuator α_2 in back-to-back (BtB) transmission case when the optimum matching value of delay τ is known. Legal RX is defined as the RX with pre-known information about the keys of $C(t)$. It can be seen that as the attenuation value of α_1 increases, the tolerable amplitude mismatch range decreases for a fixed EVM and the gradient of measured curves increases, leading to an increase in system confidentiality. Specifically, the amplitude mismatch ranges that lead to EVM lower than 12.5% are 2.0856 dB, 1.0619 dB, 0.8468 dB, 0.6665 dB and 0.5094 dB when α_1 attenuates 0 dB, 6 dB, 8 dB, 10 dB and 12 dB respectively. No doubt that the method of masking signal by chaos can effectively enhance the anti-dawning ability. In the following content, the attenuation values of α_1 is set to 6 dB.

Since one of the keys is amplitude matching value, the impact of amplitude mismatch on system performance is studied. Fig. 3(a) and (b) demonstrate the bit error rate (BER) and EVM performances versus different amplitude mismatches of attenuator α_2 over different transmission distances when the optimum matching value of delay τ is known. For legal RX, the maximum reachable transmission distance is 80 km since the optimum BER is beyond the FEC threshold of 3.8×10^{-3} when the transmission distance is larger than 80 km. Results show that BER increases exponentially when the amplitude is not matched at DDMZM2. Meanwhile, the tolerable amplitude mismatch range decreases with the increasing transmission distance for a fixed BER value, specifically, the amplitude mismatch ranges that lead to BER lower than 3.8×10^{-3} are 1.57 dB, 1.42 dB, 1.11 dB, 0.59 dB and 0.44 dB when the transmission distances are 0 km, 25 km, 50 km, 75 km and 80 km respectively. It indicates that difficulty of eavesdropping increases with the transmission distance. Inserts (i) and (iii) of Fig. 3(b) depict the constellation diagrams of the received OFDM signal with the optimum amplitude match under BtB and 80 km transmission respectively, which are convergent; while the constellation diagrams presented in inserts (ii) and (iv) of Fig. 3(b) which depict the case with a tiny amplitude mismatch are indistinct. That is, without pre-known information about the amplitude, an eavesdropper even with knowing the keys of $C(t)$ has to find the accurate 0.44 dB range of amplitude in order to decrypt the data after 80-km transmission, indicating a good resistance to eavesdropping. For illegal RX which is defined as the RX without knowing the keys of $C(t)$ or the matching values of amplitude and phase, the keys of $C'(t)$ are set to r=4 and x_0 =0.1667, which are slightly different from the keys of $C(t)$. As shown in Fig. 3, even with knowing the amplitude matching value, the BER and EVM of illegal RX are as high as 0.5 and > 210% respectively, owing to the fact that chaos are highly sensitive to the initial conditions and hard to predict. It can be concluded that a tiny discrepancy of chaotic keys will lead to the failure of decryption. The constellation diagrams of illegal RX under BtB and 80 km transmission are shown in inserts (i) and (ii) of Fig. 3(a) respectively where the 16 points can't even be distinguished. Moreover, the relationship of EVM (BER) to amplitude mismatch for illegal RX is quite different from that for legal RX, so an eavesdropper cannot obtain the amplitude matching range by testing different chaos.

Since another key in this scheme is phase/delay matching value, the impact of delay mismatch on system performance is investigated. Fig. 4 demonstrates the EVM performance versus different delay mismatches of delay τ over different transmission distances when the matching value of attenuator α_2 is known. For legal RX, the tolerable delay mismatch range is 0.08 ns, when beyond this range, EVM will increase significantly. The reason is that OFDM must obtain strict orthogonality among subcarriers [18] which means it is extremely sensitive to time delay, a small mismatch in time will cause dramatic performance degradation. Without pre-known information about the delay, an

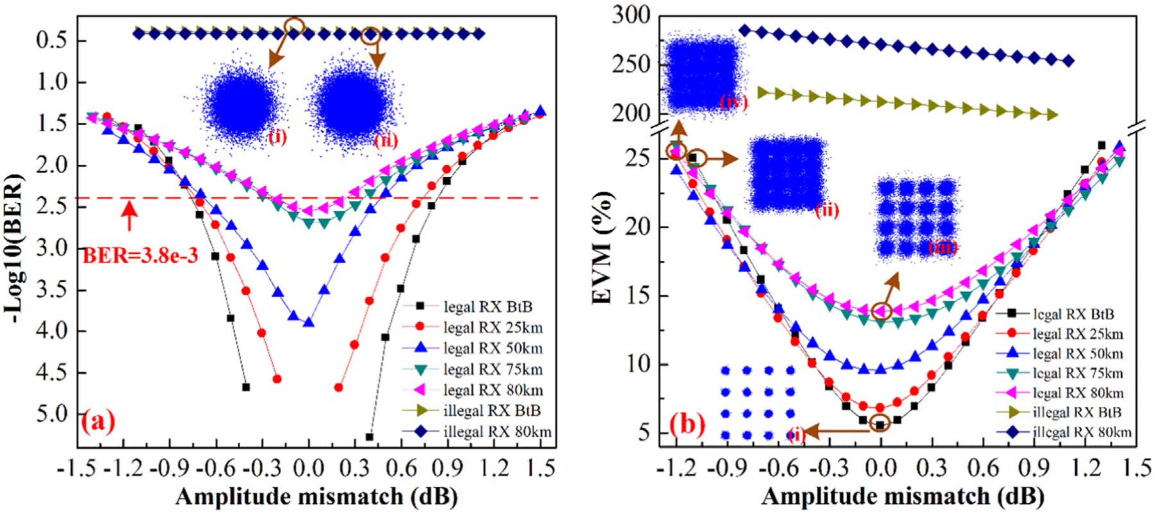

Fig. 3. (a) BER and (b) EVM versus different amplitude mismatches of attenuator α_2 over different transmission distances when the optimum matching value of delay τ is known.

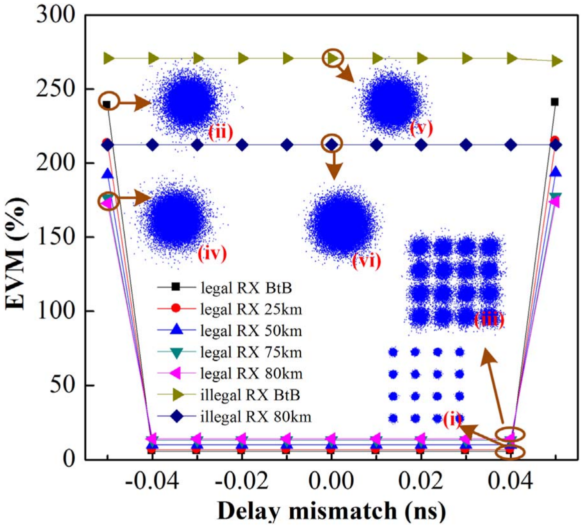

Fig. 4. EVM versus different delay mismatches of time delay τ under different transmission distances when the optimal matching value of attenuator α_2 is known.

eavesdropper has to find the accurate 0.08 ns range to decrypt the data. Inserts (i) and (iii) of Fig. 4 depict the constellation diagrams in legal RX within the tolerable delay mismatch range under BtB and 80 km transmission respectively, which are convergent; while inserts (ii) and (iv) of Fig. 4 show the case beyond tolerable delay mismatch range, which are too worse to recover. For illegal RX even with pre-known information about the optimal amplitude matching value, EVM is as high as >210% with any time delay. The constellation diagrams of illegally received signal under BtB and 80 km transmissions are given in inserts (v) and (vi) of Fig. 4 respectively, revealing the high security. In addition, similar to amplitude mismatch, the relationship between delay mismatch and EVM in illegal RX is quite different from that in legal RX, so an eavesdropper can't obtain the correct delay/phase matching value for the scheme by testing different chaos as well. Given the above, an eavesdropper without knowing either the keys of $C(t)$ or the delay/amplitude matching values at DDMZM2 cannot recover $S(t)$, and has to receive the noise-like time domain signal and indistinct constellation diagram.

4. Conclusions

A novel universal optical encryption scheme based on digital chaos-masked and the optical interference cancellation technology is proposed and demonstrated. The principle is deduced theoretically and the 10-Gb/s 16-QAM OFDM signal is used to verify the feasibility by simulation. By the analog encryption process based on DDMZM, the signal transmitted is completely masked by interference chaotic noise in both bandwidth and amplitude, making the encrypted signal analog, noise-like and unrecoverable by post-processing techniques. The decryption process requires the precise matches of both the amplitude and phase between the cancellation and the interference chaotic noises, which provide a large two-dimensional key space. For the maximum reachable transmission distance of 80 km without dispersion compensation or inline amplifier, the tolerable amplitude and delay mismatch ranges at the FEC limit are 0.44 dB and 0.08 ns respectively.

Funding

The work was jointly supported by the National Natural Science Foundation of China (Nos. 61501157, 61433009) and Natural Science Foundation of Zhejiang Province, China (Grant No. LQ16F050004).

References

[1] G. Keiser, Optical Fiber Communications, John Wiley & Sons Inc, 2003.

[2] X. Gao, X., F. Xie, H. Hu, Enhancing the security of electro-optic delayed chaotic system with intermittent time-delay modulation and digital chaos, Opt. Commun. 352 (2015) 77–83.

[3] L. Yi, T. Zhang, Z. Li, J. Ke, Y. Dong, W. Hu, Secure optical communication using stimulated Brillouin scattering in optical fiber, Opt. Commun. 290 (2013) 146–151.

[4] M.P. Fok, Z. Wang, Y. Deng, P.R. Prucnal, Optical layer security in fiber-optic networks, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 725–736.

[5] L. Zhang, X. Xin, B. Liu, Y. Wang, Secure OFDM-PON based on chaos scrambling, IEEE Photonics Technol. Lett. 23 (14) (2011) 998–1000.

[6] L.M. Pecora, T.L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (1990) 821–823.

[7] T. Wu, W. Sun, X. Zhang, S. Zhang, Concealment of time delay signature of chaotic output in a slave semiconductor laser with chaos laser injection, Opt. Commun. 381 (2016) 174–179.

[8] I.V. Ermakov, S.T. Kingni, V.Z. Tronciu, J. Danckaert, Chaotic semiconductor ring lasers subject to optical feedback: applications to chaos-based communications, Opt. Commun. 286 (2013) 265–272.

[9] R.M. Nguimdo, M.C. Soriano, P. Colet, Role of the phase in the identification of delay time in semiconductor lasers with optical feedback, Opt. Lett. 36 (22) (2011) 4332–4334.

[10] T.T. Hou, L. Yi, J. Ke, Y. Hu, W. Hu, Time delay signature concealment in chaotic systems for enhanced security, in: Proceedings of Asia Communications and Photonics Conference, OSA, AF2A. 97, 2016.

[11] Z. Shen, X. Yang, H. He, W. Hu, Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos, IEEE Photonics J. 8 (3) (2016) 1–9.

[12] B. Liu, L. Zhang, X. Xin, J. Yu, Physical layer security in CO-OFDM transmission system using chaotic scrambling, Opt. Commun. 291 (2013) 79–86.

[13] W. Zhang, C. Zhang, C. Chen, W. Jin, K. Qiu, Joint PAPR reduction and physical layer security enhancement in OFDMA-PON, IEEE Photonics Technol. Lett. 28 (9) (2016) 998–1001.

[14] B. Wu, M.P. Chang, B.J. Shastri, Z. Wang, P.R. Prucnal, Analog noise protected optical encryption with two-dimensional key space, Opt. Express 22 (12) (2014) 14568–14574.

[15] Y. Zhang, S. Xiao, Y. Yu, C. Chen, M. Bi, L. Liu, L. Zhang, W. Hu, Experimental study of wideband in-band full-duplex communication based on optical self-interference cancellation, Opt. Express 24 (26) (2016) 30139–30148.

[16] ITU -T Recommendation G.975.1, Appendix I.9 (2004).

[17] R.M. May, Simple mathematical models with very complicated dynamics, Nature 261 (5560) (1976) 459–467.

[18] M. Bi, S. Xiao, H. He, J. Li, L. Liu, W. Hu, Power budget improved symmetric 40-Gb/s long reach stacked WDM-OFDM-PON system based on single tunable optical filter, IEEE Photonics J. 6 (2) (2014) 1–8.