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
Available online 18 April 2017

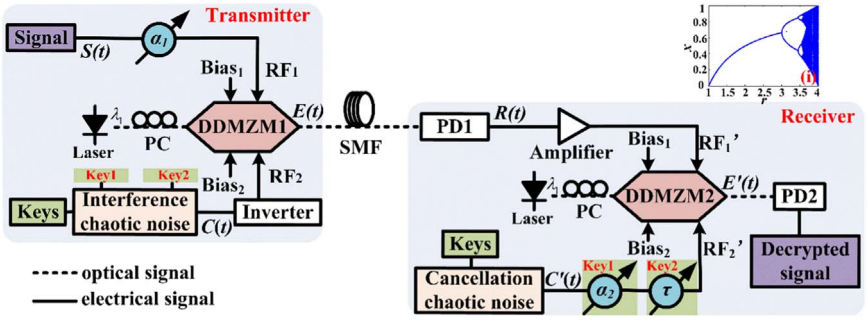

Fig. 1. Architecture of the proposed digital chaos-masked optical encryption system. PC: polarization controller; α: tunable attenuator; DDMZM: dual-drive Mach-Zehnder modulator; RF: radio frequency; SMF: single mode fiber; PD: photo-detector; τ: tunable time delay.

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 $\alpha_{\mathrm{pre}}C$"(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,

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

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

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.

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

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

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 ϕ_1' and ϕ_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 $\alpha_{\mathrm{link}}C(\tau_{\mathrm{link}})$. 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), $\alpha_{\mathrm{link}}C(\tau_{\mathrm{link}})$ is subtracted and $\alpha_{\mathrm{link}}\alpha_1 S(\tau_{\mathrm{link}})$ 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.

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

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

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

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

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

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-