High-speed Chaotic Secure Optical Communication Over 1000 km Based on Phase Scrambling

Shuai Tang
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, China
tangshuai@std.uestc.edu.cn

Ning Jiang*
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, China
uestc_nj@uestc.edu.cn

Gang Hu
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, China
hg@uestc.edu.cn

Yongsheng Cao
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, China
caoyongsheng@uestc.edu.cn

Qianwu Zhang
School of Communication and Information Engineering
Shanghai University
Shanghai, China
zhangqianwu@shu.edu.cn

Kun Qiu
School of Information and Communication Engineering
University of Electronic Science and Technology of China
Chengdu, China
kqiu@uestc.edu.com

***Abstract*—We propose a chaos-based optical communication scheme that supports high-speed and long-haul secure optical transmission, by encrypting the message signals in multiple dimensions, and numerically demonstrate a 40-Gbps secure QPSK transmission over 1000-km single-mode fiber.**

Keywords—chaotic optical communications, optical encryption, digital signal processing

I. Introduction

Chaotic secure optical communication is an effective physical layer security protection strategy to prevent information leakage [1]. It mainly uses optical devices and their parameters as encryption and decryption keys to enhance the security of the optical fiber communication system. With the growth of internet communication, to meet the high-capacity requirements of optical communication networks, chaotic secure optical communication is also developing towards higher speeds and longer distances [2-4]. In the past two decades, great research efforts have been focused on the enhancement of the data rate and transmission distance of chaotic communication systems [5-7], but there is still a big gap between the present conventional optical chaotic communication system and the commercial optical fiber communication systems, whose transmission capacity has been far larger than 100 Gbps × 1000 km [8].

The traditional chaotic encryption method is to modulate the message onto the chaotic carrier to achieve message hiding. This scheme has two main restrictions in realizing high-speed and long-haul communication. One is the strict requirement for chaotic hardware synchronization. In the traditional scheme, to achieve secure and reliable chaotic communication, the bandwidth of the chaotic signal must be larger than the bandwidth of the message. However, the bandwidth of the chaotic signal is limited by the relaxation oscillation frequency of the laser. Although some broadband chaotic generation schemes have been proposed, it is difficult to achieve broadband and long-haul chaotic synchronization. The other restriction is fiber transmission impairment over long distances. The chaotically encrypted signal will be affected by dispersion, nonlinearity, and accumulated noise over long-haul transmission [9], which will result in decreased compatibility between traditional chaotic communication and existing optical fiber communication systems. Therefore, it is necessary to compensate for all transmission impairments at the receiver to ensure reliable communication.

In this paper, we propose a chaotic optical communication scheme that encrypts messages in multiple dimensions and is suitable for high-speed and long-haul environments. Based on the phase modulator and dispersion element, this scheme can simultaneously encrypt the signal's amplitude and phase. Using the co-injection chaos generation and synchronization scheme, the transmitter injects a digital on-off keying (OOK) optical signal into the external cavity semiconductor laser (ECSL) to generate a chaotic optical signal. The OOK and encrypted signals are then transmitted over a common fiber. At the receiver side, chaos synchronization is achieved through signal shaping, optical signal injection, and phase modulation replicating the mechanism in the transmitter. The digital signal processing (DSP) algorithm is applied to compensate for the distortion after long-haul transmission. Based on the above description, the secure transmission of 40 Gbps quadrature phase-shift-keying (QPSK) signal over 1000 km fiber is finally achieved and the results are consistent with the expectations.

II. Principle

The setup shown in Fig.1 depicts the high-speed and long-haul secure optical communication system based on the chaotic phase scrambling. At the transmitter, a 40 Gbps QPSK signal is generated by a single-polarization Inphase and Quadrature (IQ) Mach-Zehnder modulator. The QPSK signal is then sent to the encryption module, which includes an electro-optical phase modulator (PM1) and a dispersion device (D1). The phase modulator scrambles the phase of the QPSK signal, and the dispersion element distorts the amplitude of the QPSK signal by the dispersion-induced phase modulation to intensity modulation (PM-to-IM) conversion [10]. The driving signal of the PM1 is the chaotic electrical signal, which is generated by the chaotic signal from the external cavity semiconductor laser SL1 through a photodetector (PD). The synchronous chaotic signal is generated by the structure of common external driving light and internal delayed feedback. The driving signal in the traditional synchronization channel is an analog signal which, will degrade the synchronization quality after long-haul transmission due to dispersion and nonlinearity. For digital signal, it is more robust to transmission distortions and these distortions can be eliminated by signal shaping. Therefore, in this scheme, we use a digital signal as the driving signal of the synchronization channel to achieve long-haul chaos synchronization. In the chaos generation module, the pseudo random binary sequence (PRBS) drives the Mach-Zehnder modulator (MZM) to modulate the optical carrier from CW2 to generate the OOK optical signal, and then it is split into two beams through a 50:50 fiber coupler (FC): one beam is injected to SL1, and the other beam is wavelength-multiplexed with the encrypted signal.

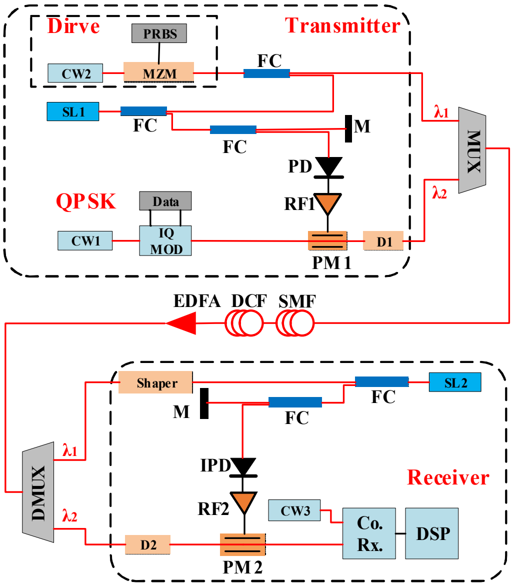

Fig. 1. High-speed and long-haul secure optical communication system based on the chaotic phase scrambling. CW, continuous wave laser; PRBS, pseudo random binary sequence; MZM, Mach-Zehnder Modulator; FC, fiber coupler; SL, semiconductor laser; (I)PD, (inverse) photodetector; RF, radio-frequency amplifier; IQ MOD, in-phase and quadrature modulator; PM, phase modulator; D, dispersion; MUX, wavelength division multiplexing; SMF, single-mode fiber; DCF, dispersion compensating fiber; EDFA, erbium-doped fiber amplifier; DMUX, wavelength division demultiplexing; DSP, digital signal processing.

Each span of the transmission link is 50 km long and features standard single-mode fiber (SSMF). An erbium-doped fiber amplifier (EDFA) and dispersion compensation fiber (DCF) are also included to compensate for the channel attenuation and dispersion. At the receiver side, a wavelength selective switch (WSS) is used to separate the OOK signal from the encrypted signal. The OOK signal is first converted to an electrical signal by a PD, then amplified and shaped by the electrical circuit, and finally re-modulated onto the optical source to regenerate the OOK signal. After that, the OOK light is injected into SL2 to generate the synchronous chaotic signal. The encrypted signal is sent to a dispersion element D2 and a phase modulator PM2 for decryption. Here the amplitude of the driving signal of PM2 is opposite to that of PM1. The coherent receiving module is composed of a coherent receiver and a DSP. The intensity and phase information of the decrypted QPSK signal can be obtained and used in the DSP. For unauthorized receivers, without well-matched parameters, the amplitude and phase parts of the chaotic carrier cannot be eliminated, and subsequent DSP will not work. Hence, security can be guaranteed. A detailed analysis will be given in the following simulation results.

To facilitate comparison, the adjustable parameters in the simulation are all selected to have the same or similar values. The center wavelength of the CW1 is set to 1550.6 nm and the center wavelength of the CW2 is set to 1549.8 nm. The dispersion element D1 is a section of dispersion fiber with a length of 2 km and a dispersion coefficient of 400 ps/nm/km. The half wave voltage of PM is 4 V. SMF's dispersion is 16 × 10^{-6} s/m^2, the dispersion slope is 80 s/m^3, the nonlinear coefficient is 1.3 W^{-1}km^{-1}, and its attenuation coefficient is 0.2 dB/km. The noise figure of EDFA is 5 dB. The transmission impairments caused by the phase noise, nonlinearity, and so on are taken into consideration in the system. To improve communication quality, digital signal processing (DSP) algorithms are introduced at the receiver, such as the digital backpropagation algorithm (DBP) [11] and the constant modulus algorithm (CMA) [12].

The DBP algorithm is a universal and efficient technique for dispersion and nonlinear effects compensation. It is based on the split-step Fourier method (SSFM) to solve an inverse nonlinear Schrodinger equation (NLSE). In a very small step, it is assumed that the effects of dispersion and nonlinearity are independent of each other, so we can define linear operator and nonlinear operator. The DBP algorithm updates the signal in each step using these operators so that the effect of dispersion and nonlinearity can be effectively compensated. The CMA is a blind equalization algorithm, that adjusts the tap coefficients of the equalizer to reduce the inter-symbol interference (ISI) of the received signal. The CMA algorithm takes advantage of the constant amplitude characteristic of the QPSK signal to minimize the error power between the output signal and the constant amplitude signal. By combining the DBP and CMA algorithms, the transmission quality of the optical communication system can be improved, ensuring the accuracy and reliability of the transmitted information.

III. Results And Analyses

First, we present the encryption and decryption performances of the proposed high-speed and long-haul secure optical communication system. Fig. 2(a) depicts the constellation obtained by the receiver after 400 km transmission without an encryption module. It can be seen that eavesdroppers can easily obtain information from the transmitter. Fig. 2(b) demonstrates the decrypted QPSK signal in the legal receiver, and the BER is calculated to be 1.6 × 10^{-6}. Due to the influence of Gaussian white noise, nonlinear effect, fiber dispersion, amplified spontaneous emission (ASE) and other factors in the link, there are still residual noises even after compensation using DSP algorithms. The eavesdroppers using direct current light as the local oscillator (LO) can get a constellation as shown in Fig. 2(c). It shows that the QPSK signal is scrambled by the chaos. The subsequent DSP cannot work normally without chaos decryption and the BER is calculated to be 0.13.

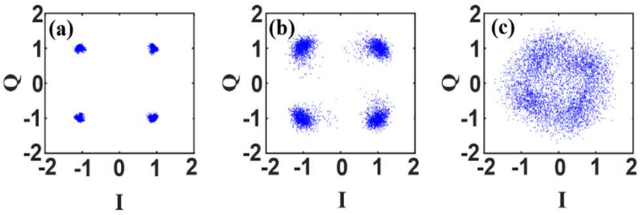

Fig. 2. (a) QPSK signal without encryption module. (b) decrypted QPSK signal after 400 km transmission. (c) coherent detected signal without chaos synchronization.

Fig. 3 illustrates the chaos synchronization performance after 1000 km transmission. Fig. 3(a) and Fig. 3(c) depict the temporal waveform of intensity chaos of SL1 and SL2. In this scheme, the 10 Gbps digital OOK signal is used as the driving signal of the synchronization channel to realize the long-haul chaotic synchronization and secure communication. The correlation plots in Fig. 3(b) clearly show that the chaotic signal in transmitter and receiver are well synchronized. The CC coefficient in Fig. 3(d) is calculated to be 0.9628.

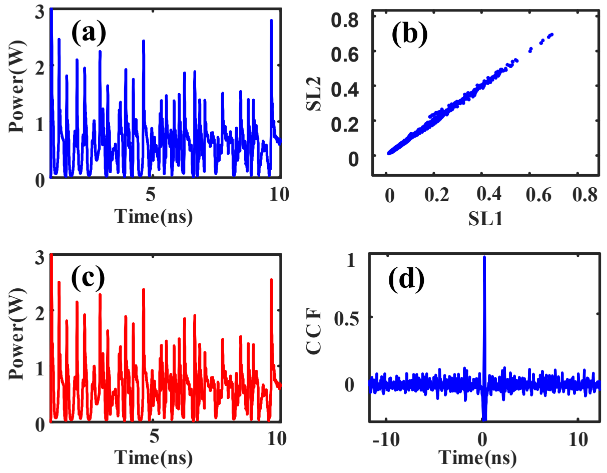

Fig. 3. (a) Time series of chaos of emitter. (b) Chaotic synchronization plot of the emitter and receiver time series. (c) Time series of chaos of receiver. (d) CCF coefficient of the emitter and receiver chaotic time series.

In the proposed system, we use a digital signal as the driving signal for chaotic synchronization channel, and use the digital signal co-injection chaotic synchronization structure for long-haul chaotic synchronization The system utilizes an injection laser for the nonlinear digital-to-analog conversion. The binary digital signal is converted into a noise-like analog signal by the nonlinear effect of the laser diode (LD). Additionally, the public OOK injection light is combined with the encrypted signal and transmitted over the same link, so no additional optical fiber links are required to transmit the public injection light. Furthermore, we can add encryption and decryption devices directly to the existing optical communication systems without replacing hardware, indicating that the proposed encryption scheme is fully compatible with modern fiber-optic communication systems.

Fig. 4(a) shows the decryption performance of the chaotic secure optical communication system under different transmission distances for the legal receiver. When the transmission distance is less than 1000 km, the BER of the legal receiver increases with the communication distance but remains below 3.8 × 10^{-3}, which is the hard decision forward error correction (HD-FEC) threshold. This indicates that the transmitter and the receiver can communicate correctly.

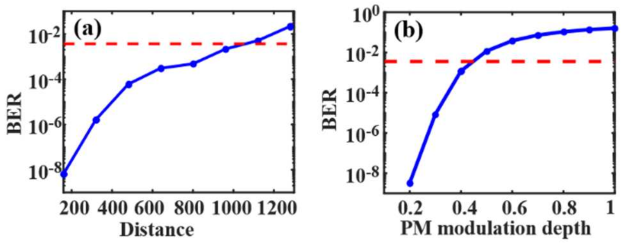

Fig. 4. (a) BER performance under different transmission distances. (b) the encryption performance of the system under different PM modulation depths.

The encryption performance is closely related to the modulation depth of PM1. As shown in Fig. 4(b), as the PM modulation depth increases, the BER of the encrypted signal increases rapidly until it reaches a stable level (0.5). This indicates that the larger the PM modulation depth, the better the encryption performance. When the modulation depth is less than 0.4, the BER is less than 3.8 × 10^{-3}. Therefore, the PM modulation depth should be large enough (at least 0.4) to ensure sufficient encryption efficiency. In the simulation, the modulation depth of PM1 is set to 1, which is large enough to well encrypt the transmission QPSK signal.

IV. Conclusion

A high-speed and long-haul secure optical communication system based on chaotic phase scrambling is demonstrated. With coherent detection and DSP algorithms, a 40 Gbps QPSK signal encrypted by chaotic phase scrambling transmission over 1000 km is numerically demonstrated, and the BER is 1.3 × 10^{-3}. This work enables to break through the transmission limitations in the traditional direct detection-based chaotic optical communication systems.

References

[1] A. Argyris et al., “Chaos-based communications at high bit rates using commercial fibre-optic links,” Nature, vol. 438, pp. 343–346, Nov. 2005.

[2] N. Jiang, A. Zhao, Y. Wang, S. Liu, J. Tang, and K. Qiu, “Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion,” OSA Continuum, vol. 2, pp. 3422, Dec. 2019.

[3] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, “Physical secure optical communication based on private chaotic spectral phase encryption/decryption,” Opt. Lett., vol. 44, pp. 1536, Apr. 2019.

[4] Y. Wu et al., “Capacity expansion of chaotic secure transmission system based on coherent optical detection and space division multiplexing over multi-core fiber,” Opt. Lett., vol. 47, pp. 726, Feb. 2022.

[5] Z. Yang, L. Yi, J. Ke, Q. Zhuge, Y. Yang, and W. Hu, “Chaotic optical communication over 1000 km transmission by coherent detection,” J. Lightw. Technol., vol. 38, pp. 4648–4655, Sep. 2020.

[6] Y. Fu et al., “Analog-digital hybrid chaos-based long-haul coherent optical secure communication,” Opt. Lett., vol. 46, pp. 1506, Apr. 2021.

[7] Y. Wu et al., “60 Gb/s coherent optical secure communication over 100 km with hybrid chaotic encryption using one dual-polarization IQ modulator,” Opt. Lett., vol. 47, pp. 5285, Oct. 2022.

[8] K. Roberts, Q. Zhuge, I. Monga, S. Gareau, and C. Laperle, “Beyond 100 Gb/s: capacity, flexibility, and network optimization,” J. Opt. Commun. Netw., vol. 9, pp. C12–C24, Apr. 2017.

[9] J.-G. Wu, Z.-M. Wu, Y.-R. Liu, L. Fan, X. Tang, and G.-Q. Xia, “Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system,” J. Lightw. Technol., vol. 31, pp. 461–467, Feb. 2013.

[10] H. Chi, X. Zou, and J. Yao, “Analytical models for phase-modulation-based microwave photonic systems with phase modulation to intensity modulation conversion using a dispersive device,” J. Lightw. Technol., vol. 27, pp. 511–521, Apr. 2009.

[11] V. Sinkin, R. Holzlohner and J. Zweck, and C. R. Menyuk, “Optimization of the split-step Fourier method in modeling optical-fiber communications systems,” J. Lightw. Technol., vol. 21, pp. 61–68, Jan. 2003.

[12] J. H. Zhou and Y. W. Zhang, “Blind time domain nonlinear compensator embedded in the constant modulus algorithm,” Opt. Express, vol. 27, pp. 22794–22807, Jul. 2019.