Experimental Demonstration of Chaotic Secure Transmission with Mutual Injection of Semiconductor Lasers over 130-km Multi-Core Fiber

Lei Shen[1+], Zhongyang Wang[2+], Min Yang[2], Ziyi Tang[2], Lei Zhang[1], Changkun Yan[1], Liubo Yang[1], Ruichun Wang[1], Jun Chu[1], Jian Wang[2*]

[1]State Key Laboratory of Optical Fiber and Cable Manufacture Technology, YOFC, Optics Valley Laboratory, Wuhan, China.
[2]Wuhan National Laboratory for Optoelectronics and School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China.
*+These authors contributed equally to this work. *Corresponding author: jwang@hust.edu.cn*

Abstract: We propose and demonstrate chaotic synchronization and communication based on the mutual injection of semiconductor lasers over long-distance multi-core fiber (MCF). It achieves chaotic secure transmission with successful encryption and decryption through 130-km seven-core fiber in the experiment. © 2023 The Author(s)

1. Introduction

Chaotic transmission has drawn significant attention for its high-level security. There are several ways of pushing a semiconductor laser into a chaotic state, for instance, optical feedback [1], mutual injection [2], and optoelectronic feedback [3]. In addition to the chaos model derived from the nonlinearity of the semiconductor laser itself, the Mach-Zehnder modulator (MZM) and phase modulator (PM) have been also experimentally proved to be chaotic sources as a result of their optoelectronic nonlinearity. While they reduce the complexity of synchronization and transmission, the modulator-based schemes are limited by electrical bandwidth and high cost. Furthermore, dual optical injection [4] and active optical feedback [5] have been proposed, with their bandwidth reaching even 38.9-GHz. Whereas, among these schemes, there is still a trade-off between capacity and distance for fiber-based chaotic transmission. In this scenario, a laudable goal would be to expand capacity in long-distance transmission through a single fiber.

Recently, multiplexing schemes have been proposed to expand the communication capacity of optical chaos communication in fiber, such as wavelength-division multiplexing (WDM) and space-division multiplexing (SDM). For instance, a WDM-based scheme through a 40-km single-mode fiber (SMF) has been proposed [6], where two wavelength channels are deployed with one channel as a common noise for synchronization and the other as the chaotic signal assisted by optical injection. The wavelength channels are not fully utilized for chaotic signals. An SDM-based scheme through a 10-km multi-core fiber (MCF) has also been reported [7], where the chaotic carrier is transmitted in the center core and the message is transmitted in an outer core. Not all cores of the MCF are fully utilized for chaotic signals. Meanwhile, since coherent detection is applied at the receiver without decryption. It may suffer the risks of information leakage when the eavesdropper receives the chaotic carrier. So far, it is quite a challenge to take full advantage of all multiplexing channels for chaotic secure transmission with scaled capacity over 100 km fiber.

In this paper, we propose and experimentally demonstrate a chaotic communication scheme of aggregate 70 Gbps on-off key (OOK) signal through a 130-km seven-core fiber. The encrypted messages are transmitted in all seven core channels with each channel transmitting a 10 Gbps chaotic signal. The optical chaos is generated by the mutual injection of semiconductor lasers and synchronized with high quality.

2. Experimental setup

Fig. 1(a) illustrates the experimental setup of chaotic secure transmission with mutual injection of semiconductor lasers through MCF. In this diagram, the 130-km seven-core fiber is introduced to provide parallel transmission. The cross-sectional view of MCF is depicted in Fig. 1(b). At the transmitter side, a chaos laser generated by mutual injection of double semiconductor lasers, namely SL1 and SL2, and connected by a 90:10 coupler, is deployed and serves as chaotic noise source. Particularly, the wavelength and wavelength difference between SL1 and SL2 are well-tuned, which are set to be 1548.49 and 1548.85 nm with a wavelength difference of 45 GHz, marked as red and blue curves respectively in Fig. 1(c). Additionally, a polarization controller (PC) and a variable optical attenuator (VOA) are deployed to tune SL1 to a chaotic state. The chaotic laser is divided by a 1x8 coupler for encryption. The light from a tunable laser is modulated by the RF signals generated by an arbitrary waveform generator (AWG, Tektronix AWG70002). Then the signals are masked by a chaotic laser via a 50:50 coupler. Since the wavelength of

signals are related to the quality of synchronization and decryption, blocking eavesdroppers from extracting the wavelength of signals by filtering, the wavelength of signals is set to be 1548.62 nm. Then the encrypted messages are coupled into MCF channels by a fan-in device after an erbium-doped fiber amplifier (EDFA1) for the compensation of link losses. An EDFA2 at the receiver side is needed followed by an optical bandwidth-variable tunable filter to reduce amplified spontaneous emission (ASE) noise.

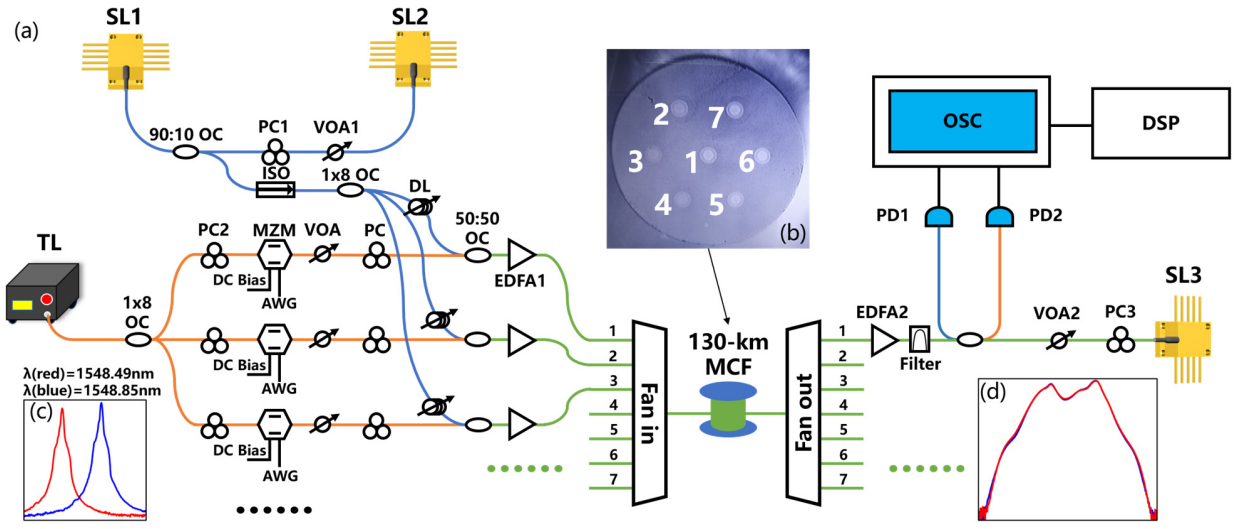

Fig. 1. (a) Experimental setup of chaotic secure transmission with the mutual injection of semiconductor lasers through multi-core fiber. (b) Cross-sectional view of MCF. (c) The optical spectrum of SL1 (red) and SL2 (black). (d) The optical spectrum of chaotic laser (red) and synchronized laser (blue). SL, semiconductor laser; OC, optical coupler; PC, polarization controller; ISO, isolator; DL, delay line; TL, tunable laser; MZM, Mach-Zehnder modulator; VOA, variable optical attenuator; EDFA, erbium-dropped fiber amplifier; MCF, multi-core fiber; PD, photodetector; OSC, oscilloscope; DSP, digital signal processing.

At the receiver side, there are synchronization and decryption to recover chaotic laser from the encrypted signals and decrypt signals by subtracting optical chaotic noise from encrypted messages. Since the signals transmitted in seven channels are encrypted by the same optical chaos source but different delay parameters, seven photodetectors (PDs) and one synchronization device composed by SL3 which is identical to SL1 and SL2 are required for decryption in digital signal processor (DSP). This setup takes part of the core-1 channel for synchronization. The laser after 130-km MCF transmission of core-1 is divided into two parts by a 2x2 coupler. One part, whose power and state of polarization are adjusted by VOA2 and PC3, is unidirectionally injected into SL3 for synchronization, and the other part is detected by PD1 directly. The optical spectrum of SL3 is in accord with the optical spectrum of chaotic laser from the transmitter side, shown as blue and red curves separately in Fig. 1(d). The synchronization device recovers the chaos waveform from signals encrypted by chaotic noise. The detected waveforms by PDs are sampled by a high-speed oscilloscope (OSC, Keysight DSA-Z 204A) and the decryption is conducted by offline DSP. In receiver DSP, a conventional method is carried on to extract the signals. A subtraction between encrypted signals and recovered chaos waveform is conducted, followed by calibration, linear equalization, and calculation of BER.

3. Experimental results and discussions

Indeed, the synchronization of chaos lasers is vitally concerned for most chaotic communication systems. The quality of synchronization is evaluated by correlation coefficients (CC), which can be described as $CC = \langle [x(t)-\langle x(t)\rangle][y(t)-\langle y(t)\rangle]\rangle \Big/ \sqrt{\langle [x(t)-\langle x(t)\rangle]^2\rangle \langle [y(t)-\langle y(t)\rangle]^2\rangle}$, where the $x(t)$ is the time series of chaos laser waveform and $y(t)$ is the time series of synchronization laser. The quality of synchronization is studied when only chaos laser is transmitted over 130-km MCF. For core-1, the time series of chaotic laser waveform from transmitter side is illustrated in the upper one of Fig. 2(a) and time series of synchronization laser waveform at receiver side is shown in the lower one of Fig. 2(a), where the waveforms are synchronized well. In addition, the chaos waveform

versus synchronization is illustrated in Fig. 2(b), which is almost a line representing a better synchronization between transmitter and receiver, and the CC reaches 0.942. The time series waveform in core-2 is illustrated in Fig. 2(c). The chaos waveform versus synchronization in core-2 and the CC reaches 0.940, as illustrated in Fig. 2(d). The measured bit-error rate (BER) performance in the case of chaotic transmission with increasing mask coefficients over 130-km MCF is also investigated, as shown in Fig. 2(e). The mask coefficient is around 0.8 at BER of 2e-2 (20% soft-decision forward-error correction (SD-FEC) threshold), which means 10 Gbps OOK signals are encrypted and decrypted successfully and the aggregate transmission capacity reaches 70 Gbps. The signals are effectively encrypted with the BER of above 0.2, which is far from 20% SD-FEC at the BER of 0.02 for eavesdroppers. As for authorized users, the BER of decrypted signals reaches a minimum value of 0.0013 at a mask coefficient of around 1.6. Moreover, similar performance is achieved in the other channels.

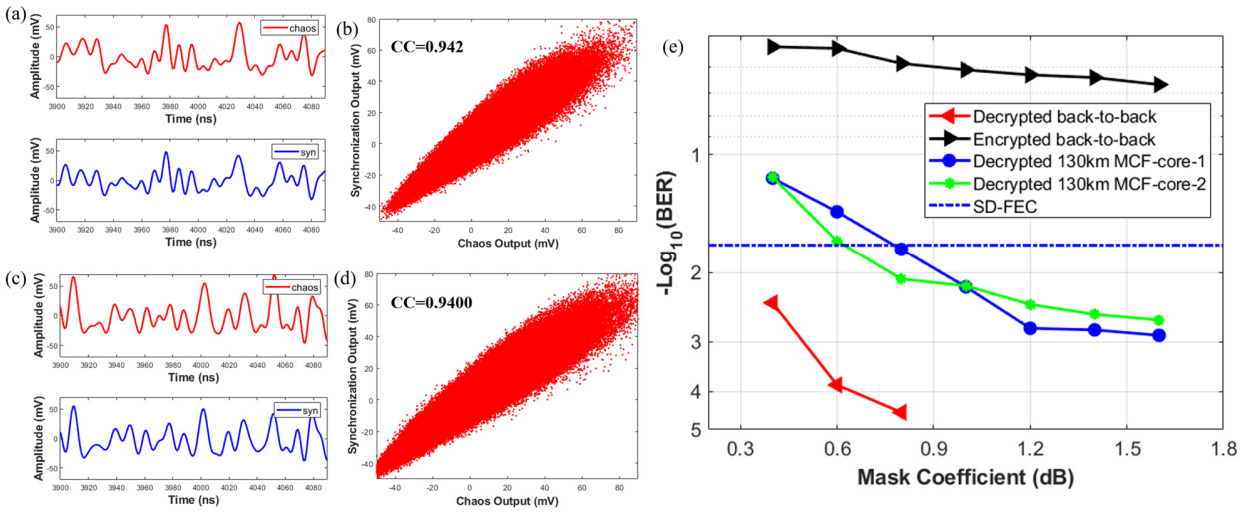

Fig. 2. The performance of chaotic secure transmission with mutual injection of semiconductor lasers through multi-core fiber. (a) Time series of chaos waveform and synchronization waveform in core-1. (b) The chaos waveform versus synchronization in core-1. (c) Time series of chaos waveform and synchronization waveform in core-1. (d) The chaos waveform versus synchronization in core-2. (e) The measured BER performance with increasing mask coefficients.

4. Conclusion

In summary, we experimentally demonstrate the chaotic synchronization and communication of aggregate 70 Gbps OOK based on the mutual injection of semiconductor lasers over 130-km MCF. The signals are effectively encrypted for eavesdroppers. The obtained results indicate that the MCF holds the potential to effectively increase the capacity of long-distance chaotic secure transmission.

5. Acknowledgements

This work was supported by the National Key R&D Program of China (2018YFB2200204), the National Natural Science Foundation of China (NSFC) (62125503), the Key R&D Program of Guangdong Province (2018B030325002), the Key R&D Program of Hubei Province of China (2020BAB001, 2021BAA024), and the Science and Technology Innovation Commission of Shenzhen (JCYJ20200109114018750).

6. References

[1] Mork, Jesper, Bjarne Tromborg, and Jannik Mark. "Chaos in semiconductor lasers with optical feedback: theory and experiment." IEEE Journal of quantum electronics 28.1 (1992): 93-108.
[2] Xiang, Shunkai, Min Yang, and Jian Wang. "Chaotic optical communications of 12.5-Gbaud OOK and 10-Gbaud QPSK signals based on mutual injection of semiconductor lasers." Optics Letters 47.11 (2022): 2818-2821.
[3] Sciamanna, Marc, and K. Alan Shore. "Physics and applications of laser diode chaos." Nature photonics 9.3 (2015): 151-162.
[4] Xiang, Shui Ying, et al. "Wideband unpredictability-enhanced chaotic semiconductor lasers with dual-chaotic optical injections." IEEE Journal of Quantum Electronics 48.8 (2012): 1069-1076.
[5] Yang, Qiang, et al. "Generation of a broadband chaotic laser by active optical feedback loop combined with a high nonlinear fiber." Optics Letters 45.7 (2020): 1750-1753.
[6] Gao, Zhensen, et al. "Photonic-layer secure 56 Gb/s PAM4 optical communication based on common noise driven synchronous private temporal phase en/decryption." Optics Letters 47.19 (2022): 5232-5235.
[7] Wu, Yuqing, et al. "Capacity expansion of chaotic secure transmission system based on coherent optical detection and space division multiplexing over multi-core fiber." Optics Letters 47.3 (2022): 726-729.