Optics and Photonics Journal, **2013, 3, 183-186**
doi:10.4236/opj.2013.32B044 Published Online June 2013 (http://www.scirp.org/journal/opj)

Experimental Investigation of Improving the Performance of the Chaotic Optical Communication with Chaos-Masking through Wavelength Mismatch*

Wei Chang, Xiaolei Chen, Qingchun Zhao, Hongxi Yin, Nan Zhao
Lab of Optical Communications and Photonic Technology, School of Information and Communication Engineering, Dalian University of Technology, Dalian, China
Email: hxyin@dlut.edu.cn

Received 2013

ABSTRACT

In this paper, the wavelength mismatch between the message and the chaotic carrier in the chaotic optical communication with chaos-masking has been experimentally investigated. The results show that the decryption performance of the receiver can be improved when the message wavelength is greater than that of the chaotic carrier. When the wavelength offset is set to 0.12 nm, high-speed secure optical communication with a message of 2.5 Gbits/s is achieved.

Keywords: Chaos Masking; Chaotic Synchronization; Chaotic Communication; Wavelength Mismatch

1. Introduction

As a hardware-based encryption technique at the physical layer, the chaotic optical communication has attracted extensive interests from the community of secure and optical communications during the past decade [1,2]. At the receiver, the message can be filtered out by the receiver laser, and the chaotic carrier that synchronizes with the carrier generated by the transmitter can be obtained. Then, the message can be decrypted by subtracting the output of the receiver laser from the encrypted signal [3,4]. With the in-depth exploring the secure chaotic optical communication, the issues for secure chaotic optical communication mainly focus on bandwidth enhancement [5], generation of novel chaotic carriers [6], chaotic photonic integrated circuits (PICs) [7], and bidirectional communications [8]. It is important to solve these issues for which can improve the performance of the system and promote the practical applications. However, the encryption schemes as well as the relationship between the message and the chaotic carrier is the most important factor, which constraints the performance of the secure chaotic optical communication system directly.

At present, three encryption schemes have been proposed for the secure chaotic optical communications, namely, chaos modulation (CM), chaos masking (CMS), and chaos shift-keying (CSK) [9]. For simple physical processes and convenient achievement, CMS is the most common encryption scheme. Argyris et al. experimentally investigated the performance of the three encryption schemes with a message of 1.5 Gbits/s [10]. However, it is still a problem being worthy further investigating how to improve the performance of different encryption schemes and to promote the data-rate of message.

In this paper, the mismatch of the wavelength between the message and the chaotic carrier in the secure chaos-masking optical communication has been experimentally investigated. The relationship between the mismatch of the wavelength and the performance of the system has been quantitatively analyzed. When the wavelength offset is set to 0.12 nm, high-speed secure communication with a message of 2.5 Gbits/s has been achieved experimentally.

2. Experimental Setup

Figure 1 shows the experimental setup of the secure optical communication system with chaos-masking. The chaotic carrier is generated by optical feedback. The circulator, optical coupler (OC), and the variable optical attenuator (VOA) constitute the fiber-loop. The chaotic carrier is then split into two paths by a 50:50 OC after amplified by an Erbium-doped fiber amplifier (EDFA). The upper path is used for encrypting the secure message by CMS, and the lower path is transmitted as a secure

*This work is supported in part by the National Natural Science Foundation of China (NSFC) under Grants 61071123, 61172059, and 61201224, the Funds for Ph. D. Student Academic New Investigator of Ministry of Education of China, and the Natural Science Foundation of Changzhou City under CJ20120015.

key. At the receiver, the two optical signals are detected by two photodetectors (Discovery Semiconductor, DSC-R401HG-39). Then, the message can be decrypted by subtracting the secure key from the encrypted message. The radio-frequency filter here is used to filter the extra high-frequency noise. The digital storage oscilloscope (Agilent DSO90404A) at the receiver-end is used for real-time record of the synchronization between the two chaotic signals and the decrypted message.

3. Chaotic Synchronization

The waveforms of the two chaotic signals without message at the receiver are shown in **Figure 2(a)** and **(b)**. It can be seen that the synchronization of the system is well achieved. The correlation coefficient of the two chaotic signals is 0.9485, which provides a guarantee for the realization of the secure chaotic optical communication.

4. Effect of Wavelength Mismatch on the Decryption Performance

In the experiment of secure chaos-masking optical communication, the continuous wave (CW) emitted by a tunable laser (Thorlabs, TL1550-B) is modulated by a Mach-Zehnder modulator (MZM). Then a 1.25-Gbits/s optical message is generated. The message is hidden into a chaotic carrier by an OC, and launched into the fiber for secure transmission. At the receiver, the message can be decrypted by subtracting the secure key from the encrypted message. The wavelength of the message can be changed by adjusting the wavelength of the tunable laser, and $\Delta\lambda$ is defined as the wavelength offset between the wavelength of the message and that of the chaotic carrier

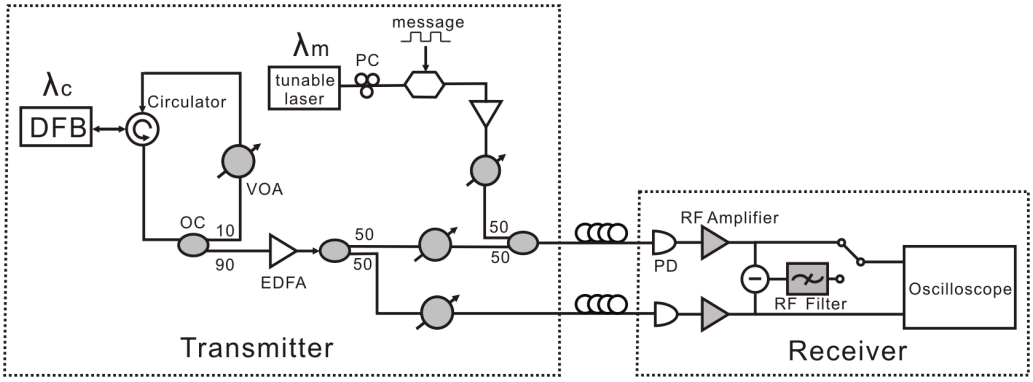

Figure 1. Experimental setup of the secure optical communication system with chaos-masking. DFB: distributed feedback laser diode, OC: optical coupler, VOA: variable optical attenuator, EDFA: Erbium-doped fiber amplifier, PC: polarization controller, MZM: Mach-Zehnder modulator, PD: photodetector.

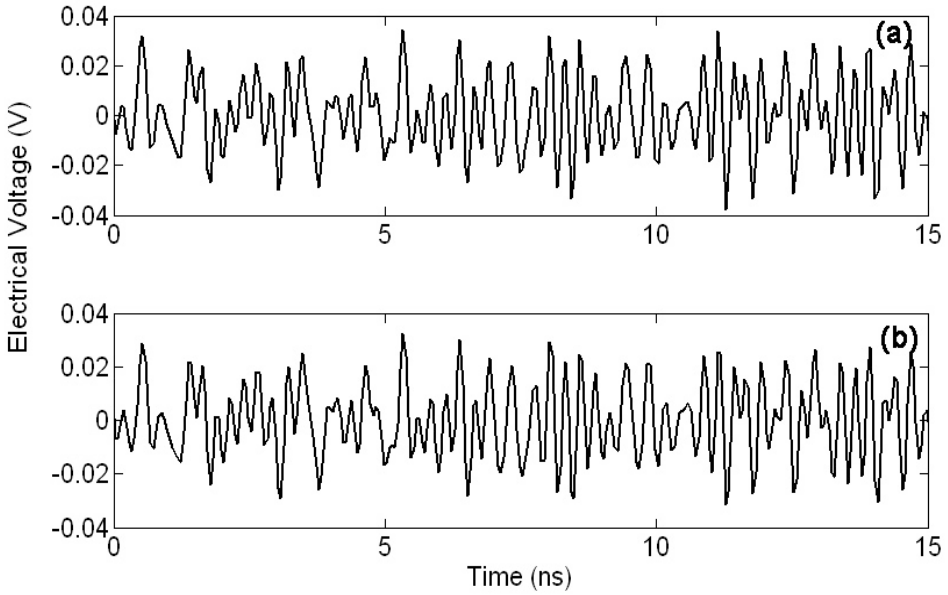

Figure 2. Time domain waveforms of the two chaotic signals without message at the receiver-end. (a) chaotic carrier without message, (b) secure key.

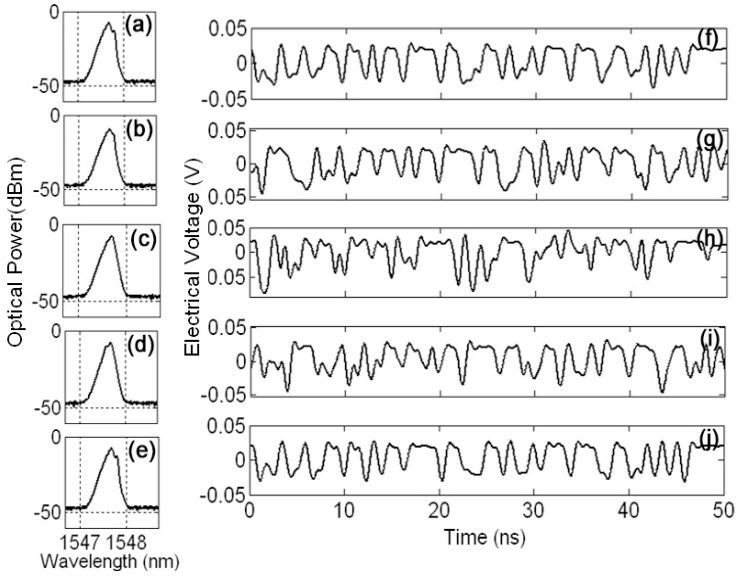

Figure 3. Recovered messages with different $\Delta\lambda$. (a) - (e) are the optical spectra of the encrypted messages, and the $\Delta\lambda$ is set to -0.15nm, -0.08nm, 0nm, 0.08nm, 0.15nm, respectively. (f) - (j) are the recovered messages correspond to different $\Delta\lambda$.

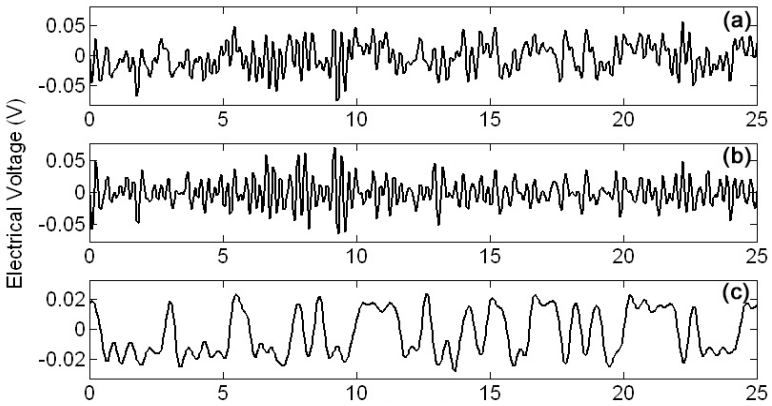

Figure 4. Experimental results of the secure chaotic optical communication with a 2.5-Gbits/s message when the $\Delta\lambda$ is set to 0.12 nm. (a) chaotic carrier with a 2.5-Gbits/s message, (b) the recovered message at the receiver.

$$\Delta\lambda = \lambda_m - \lambda_c,$$

where λ_m and λ_c denote the wavelengths of the message and that of the chaotic carrier, respectively. $\Delta\lambda > 0$ means the wavelength of the message is grater than that of the chaotic carrier and vice versa. In the experiment, the wavelength of the message is changed to get different $\Delta\lambda$, and then the decryption results are recorded

The experimental results are shown in **Figure 3**. It can be seen that when $\Delta\lambda = 0$, which means the wavelength of the message matches with that of the chaotic carrier, the message recovered at the receiver is of bad quality. When $\Delta\lambda$ is less than zero, the quality of the recovered message is improved. And a lager $|\Delta\lambda|$ means a better result. When $\Delta\lambda$ is greater than zero, the decryption performance can also be improved. Comparing different wavelength offset, it is found that the decryption performance is better when $\Delta\lambda$ is greater than zero.

5. High-speed Secure Chaotic Optical Communication

In the secure chaos-masking optical communication system, the larger the wavelength difference is, the better the decryption performance is. However, a larger wavelength difference will lead to less security of the message. Therefore, it is necessary to consider both the security of the message and the decryption performance of the receiver. A suitable wavelength offset will facilitate the achievement of the high-speed secure communication.

When $\Delta\lambda$ is set to 0.12 nm, the experimental results of the secure chaotic optical communication with a 2.5-Gbits/s message is shown in **Figure 4**. It can be seen that the message is safely hidden in the chaotic carrier and well recovered at the receiver, which means the high-speed secure communication is realized successfully.

6. Conclusions

In this paper, the mismatch of the wavelength between the message and the chaotic carrier in the chaotic optical communication with chaos-masking has been experimentally investigated. The results show that the decryption performance of the receiver can be improved when the wavelength of the message is greater than that of the chaotic carrier. When the wavelength offset is set to 0.12 nm, high-speed secure communication with a message of 2.5 Gbits/s can be achieved. The results presented here may provide some useful suggestions for the practical applications of secure chaotic optical communications.

REFERENCES

[1] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, et al., "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, Vol. 438, No. 7066, 2005, pp. 343-346. doi:10.1038/nature04275

[2] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, M. Norgia, and B. Provinzano, "Optical chaos masking of video signals," *IEEE Photonics Technology Letters*, Vol. 17, No. 9, 2005, pp. 1995-1997. doi:10.1109/LPT.2005.853267

[3] Q. Zhao and H. Yin, "Performance analysis of dense wavelength division multiplexing secure communications with multiple chaotic optical channels," *Optics Communication*, Vol. 285, No. 5, 2012, pp. 693-698. doi:10.1016/j.optcom.2011.10.085

[4] Q. Zhao, H. Yin, and X. Chen, "Long-haul dense wavelength division multiplexing between a chaotic optical secure channel and a conventional fiber-optic channel," *Applied Optics*, Vol. 51, No. 22, 2012, pp. 5585-5590. doi:10.1364/AO.51.005585

[5] A. Wang, Y. Wang, and H. He, "Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback," *IEEE Photonics Technology Letters*, Vol. 20, No. 19, 2008, pp. 1633-1635. doi:10.1109/LPT.2008.2002739

[6] M. Nourine, Y. K. Chembo, and L. Larger, "Wideband chaos generation using a delayed oscillator and a two-dimensional nonlinearity induced by a quadrature phase-shift-keying electro-optic modulator," *Optics Letters*, Vol. 36, No. 15, 2011, pp. 2833-2835. doi:10.1364/OL.36.002833

[7] A. Argyris, M. Hamacher, K. Chlouverakis, A. Bogris, and D. Syvridis, "Photonic integrated device for chaos applications in communications," *Physical Review Letters*, Vol. 100, No. 19, 2008, p. 194101. doi:10.1103/PhysRevLett.100.194101

[8] R. Vicente, C. R. Mirasso, and I. Fischer, "Simultaneous bidirectional message transmission in a chaos-based communication scheme," *Optics Letters*, Vol. 32, No. 4, 2007, pp. 403-405. doi:10.1364/OL.32.000403

[9] J. M. Liu, H. F. Chen, and S. Tang, "Synchronized chaotic optical communications at high bit rates," *IEEE Journal of Quantum Electronics*, Vol. 38, No. 9, 2002, pp. 1184-1196. doi:10.1109/JQE.2002.802045

[10] A. Argyris, D. Kanakidis, A. Bogris, and D. Syvridis, "Experimental evaluation of an open-loop all-optical chaotic communication system," *IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 10, No. 5, 2004, pp. 927-935. doi:10.1109/JSTQE.2004.837224

