Proceedings of Engineering and Technology Innovation, vol. 3, 2016, pp. 04 - 06

Security Enhancement on Reconfiguring Coded Wavelength with Tunable Wavelength Filter Array Triggered Chaotic Sequences

Yao-Tang Chang[1,*], Jen-Fa Huang[2], Yen-Chung Huang[2] and Yan-Tai Liou[1]

[1]Department of Information Technology, Kao Yuan University, Kaohsiung, Taiwan.

[2]Department of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan.

Received 02 February 2016; received in revised form 17 March 2016; accepted 02 April 2016

Abstract

In current study, the reconfigurable optical code-division multiple-access (OCDMA) scheme is implemented that the chaos sequence is created non-linear time-variant sequence as secret key and then trigger tunable wavelength filter array as random wavelength allocation. In the encryption, the distribution of light carrier is designed and implemented by using tunable wavelength filter array triggered chaotic sequence. In addition, the arrayed waveguide grating (AWG) router is rewritten with maximal length code (M-sequence) to act as encoder. In the decryption, symmetric scheme and balanced photo-detector is presented and reconfigurable mechanism is followed the encryption synchronously either public or private channel. Hence, the multiple access interference (MAI) is cancelled completely while chaotic sequence is varied synchronously in transmitter and receiver. Compared to previous reconfigurable scheme by triggered register and switches after AWG router, the simulation results show that the secret key number of proposed cryptography is significantly increased to avoid eavesdropping attack in physical layer.

Keywords: reconfigurable coded wavelength, tunable wavelength filter array, chaotic sequence, Optical Code-Division Multiple-Access (OCDMA)

1. Introduction

The optical code-division multiple-access (OCDMA) technique has attracted considerable attention for the application in local-area networks because it provides a burst and asynchronous multiple-access environment in both the time and the spectral domains [1-6].

The reconfigurable scheme was presented with triggering register and switches configured behind AWG router in previous work [7]. However, the triggering varies of register was limited by M-sequence code pattern resulting in few reconfigurable state. The proposed cryptography is significantly increased while the tunable wavelength filter array is configured in front of coded AWG router.

The proposed encryption/decryption is presented with tunable wavelength filter array triggered chaotic sequence in section 2. Section 3 evaluates the secret key number of proposed cryptography to avoid eavesdropper's attacking in physical layer. Finally, we provide some concluding remarks and future works.

2. The Proposed Cryptography Configured with Random Wavelength Distribution

As shown in Fig. 1, the reconfigurable OCDMA-based encryption is designed that the chaos sequence is created non-linear time-variant sequence as secret key and then trigger tunable wavelength filter array as random wavelength allocation of broadband light source. The FBG is generally used to play wavelength filter role. In current study, the tunable wavelength filter array is triggered with chaotic sequence. Broadband light source is designed to depend on many varies of tunable wavelength filter array.

* Corresponding author. Email: t10066@cc.kyu.edu.tw

In the decryption end shown in Fig. 2, symmetric scheme and balanced photo-detector is presented and reconfigurable mechanism is followed the encryption synchronously either public or private channel. Hence, the multiple access interference (MAI) is cancelled completely while the tunable wavelength filter array is trigged by the same random parameter and initial value of chaotic sequence chaotic sequence synchronously in receiver end.

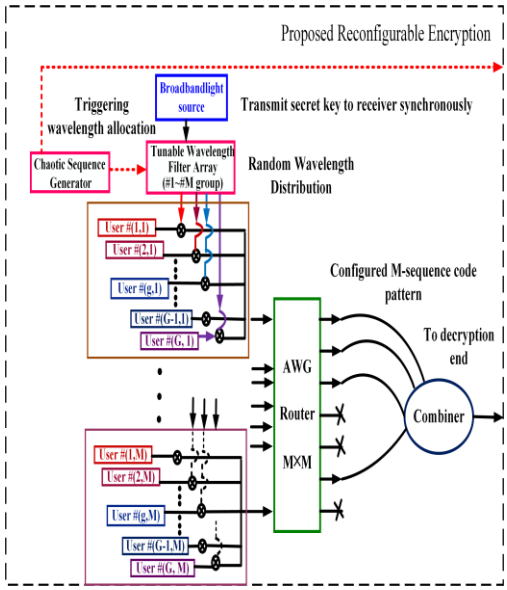

Fig. 1 The proposed encryption with tunable wavelength filter array

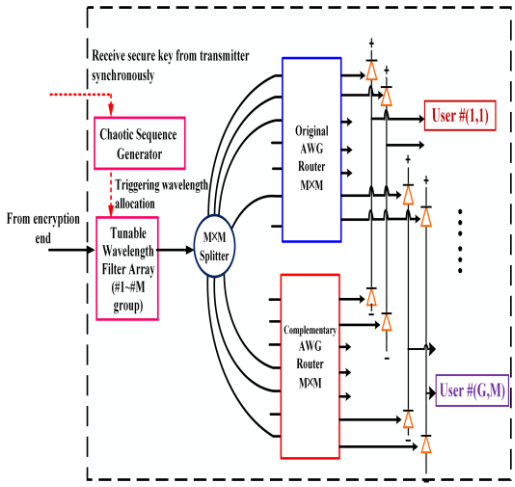

Fig. 2 The proposed decryption with tunable wavelength filter array

3. The Secret Key Evaluation of Proposed Cryptography

By selecting random parameter and initial value of chaotic sequence as the secret key to trigger tunable wavelength filter array, many of random wavelength allocations is obtained resulting from tunable wavelength filter distribution and then the proposed cryptography is implemented and characterized with the reconfigurable and flexible wavelength hopping to avoid the tracking easily by eavesdropping.

Here, the distributed pattern L of broadband light source can be possibly assigned and obtained by probability function of statistics in Eq. (1).

$$L = \binom{N}{M}\binom{N-M}{M}\binom{N-2M}{M}\cdots\binom{M}{M} = \frac{N!}{M!^{N/M}} \quad (1)$$

where M donates the code length of M-sequence code and provide the usage of M authorized users. N denotes the maximum chipped wavelength number of broadband light source.

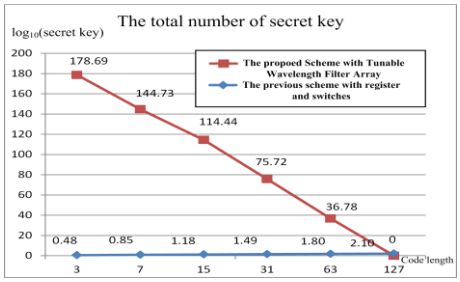

Fig. 3 The number of secret key for different code length

Compared to previous reconfigurable scheme by triggered register and switches behind AWG router, the simulation results show that the secret key number of proposed cryptography is significantly increased shown in Fig. 3. For 63 authorized users' consideration, the increasing performance of proposed scheme is more 10E+36 times than previous scheme [7].

Fig. 3 The evaluation and comparison of the total number of secret key with the proposed wavelength filter array and previous scheme [7].

4. Conclusions

Since the OCDMA scheme is characterized with higher bandwidth and confidentiality, this have much attractive for many researches to enhance the security by increasing the secret key (i.e., code family) of authorized users.

The reconfigurable cryptography applied the chaos sequence to create non-linear time-variant sequence as secret key and trigger tunable wavelength filter array as random wavelength allocation. In addition, the AWG router is re-written with maximal length code (M-sequence) to act as encoder. Hence, the more random wavelength allocations is obtained resulting from tunable wavelength filter distribution and implement the reconfigurable and flexible wavelength hopping to avoid the tracking easily by eavesdropping.

Compared to previous reconfigurable scheme by triggered register and switches behind AWG router, the simulation results show that the secret key number of proposed cryptography is significantly increased to avoid eavesdropper's attacking in physical layer. For 63 authorized users' consideration, the increasing performance of proposed scheme is more 10E+36 times than previous scheme [7]. Hence, the degree of confidentiality for proposed cryptography will be evaluated and verified secure enhancement of the OCDMA scheme in future works.

References

[1] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks—part I: fundamental principles," IEEE Trans. Commun., vol. 37, no. 8, pp. 824-833, August 1989.

[2] Y. T. Chang, J. F. Huang, C. C. Wang, C. T. Yen, H. C. Cheng, and L. W. Chou, "Adaptive modified time-spreading and wavelength-group-hopping embedded M-sequence code for improved confidentiality over synchronous networks," Optical Engineering, vol. 50, no. 5, pp. 055001, May 2011.

[3] M. Kavehrad and D. Zaccarin, "Optical code-division-multiplexed systems based on spectral encoding of noncoherent sources," J. Lightw. Technol., vol. 13, no. 3, pp. 534-545, March 1995.

[4] H. Takahashi, K. Oda, H. Toda, and Y. Inoue, "Transmission characteristics of arrayed waveguide N × N wavelength multiplexer," J. Lightw. Technol., vol. 13, no. 3, pp. 447-455, March 1995.

[5] Z. Wang, J. Chang, and P. R. Prucnal, "Theoretical analysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system," IEEE J. Lightwave Technol., vol. 28, no. 12, pp. 1761-1769, June 2010.

[6] Y. T. Chang and Y. C. Lin, "Dynamic reconfigurable encryption and decryption with chaos/M-sequence mapping algorithm for secure H.264/AVC video streaming over OCDMA passive optical network," Multimedia Tools and Application, vol. 74, no. 15, pp. 1931-1948, July 2015.

[7] Y. T. Chang, C. C. Sue, and J. F. Huang, "Robust design for reconfigurable coder/decoders to protect against eavesdropping in spectral amplitude coding optical CDMA networks," J. Lightw. Technol, vol. 25, no. 8, pp. 1931-1948, August 2007.

