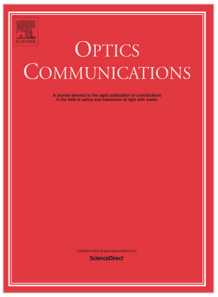
Accepted Manuscript



Multi-Gbit/s real-time modems for chaotic optical OFDM data encryption and decryption

Ying Wang, Wenlong Zhang, Guojie Chen, Xuelin Yang, Weisheng Hu

PII: S0030-4018(18)30829-0
DOI: https://doi.org/10.1016/j.optcom.2018.09.048
Reference: OPTICS 23487

To appear in: *Optics Communications*

Received date : 31 July 2018
Revised date : 16 September 2018
Accepted date : 19 September 2018

Please cite this article as:, Multi-Gbit/s real-time modems for chaotic optical OFDM data encryption and decryption, *Optics Communications* (2018), https://doi.org/10.1016/j.optcom.2018.09.048

Multi-Gbit/s Real-Time Modems for Chaotic Optical OFDM Data Encryption and Decryption

Ying Wang, Wenlong Zhang, Guojie Chen, Xuelin Yang*,Weisheng Hu

Shanghai Institute for Advanced Communication and Data Science,
State Key Laboratory of Advanced Optical Communication Systems and Networks,
Shanghai Jiao Tong University, Shanghai, 200240, China
** x.yang@sjtu.edu.cn*

Abstract

Real-time high-speed modems are proposed and demonstrated for physical-layer secure encryption and decryption of optical orthogonal frequency division multiplexing (OFDM) signals using field programmable gate array (FPGA). In the modems, the multi-fold data encryption is applied, including chaotic XOR, chaotic permutation and chaotic dynamic mapping, to enhance the physical-layer security for optical OFDM data during transmission. Real-time modems for encrypted 16-QAM OFDM signals at 4.8 Gbit/s are successfully demonstrated, using parallel multiple channels design on FPGA. The security performances of the real-time encrypted OFDM signals are evaluated, while a huge key space of ~10^{168} is created to resist the exhaustive attacks.

Keywords: Optical communication; signal processing; orthogonal frequency-division multiplexing (OFDM); field programmable gate array (FPGA); digital chaos; data security.

1. Introduction

With the exponential growth in demand for user bandwidth in the internet services, passive optical networks (PONs) have proved as a suitable candidate for addressing the bandwidth requirements, due to their excellent performances, such as high capacity, low cost, and energy efficiently [1]. Besides, orthogonal frequency division multiplexing (OFDM) becomes an attractive and popular modulation format in PONs, because of its advantages such as: tolerance to fiber dispersion, high spectrum efficiency and cost-effectiveness [2,3]. However, as a result of the broadcast characteristics of downstream traffic in PONs, it is obvious that the transmitted data becomes more vulnerable to be eavesdropped or intercepted by an illegal optical network unit (ONU) [4]. Consequently, the secure transmission in PONs has become one of the hot topics in current research.

For data security enhancement, the data encryption schemes have been proposed using chaos communication [5], optical code division multiple access (OCDMA) [6], or quantum encryption [7]. Among these approaches, chaos-based schemes have acquired much attention due to the unique properties such as: high sensitivity to the chaotic initial values, the pseudo randomness and the ergodicity [8, 9]. In particular, chaos theory is extensively deployed in image encryption [10] and OFDM data encryption in PONs [11-12]. However, the demonstrated chaotic schemes in OFDM transmission so far were offline digital signal processing (DSP), while real-time implementation has not been explored. To verify the feasibility of the practical chaotic approaches, the real-time implementation with high data rate processing has to be considered.

Field programmable gate array (FPGA) has been widely applied in telecommunications [13], image and signal processing [14], because it offers a hardware platform that can provide high speed, flexibility, efficiency and reliability [15]. Real-time optical OFDM transmission has been realized using FPGA [16-19]. However, the real-time implementation was focused on the traditional OFDM transmission, while no real-time modem has been reported for secure OFDM transmission.

In this paper, we propose and demonstrate for the first time, a novel FPGA-based real-time, high-speed OFDM data encryption/decryption modem, to enhance the physical-layer security during data transmission, where the multi-fold data encryption is introduced to ensure the high-level data security. Consequently, the noise-like constellation will be generated after the multi-fold data encryption, such as: chaotic XOR, chaotic permutation and chaotic scrambling using chaotic sequences provided by a hyper digital chaos. Since the noisy constellation of the encrypted QAM signals is predetermined by the hyper digital chaos,