Optical Fiber Technology 36 (2017) 370–373

Contents lists available at ScienceDirect

Optical Fiber Technology

www.elsevier.com/locate/yofte

Regular Articles

An approach for physical layer security enhancement and PAPR reduction in OFDM-PON

Junxin Chen [a], Zhi-liang Zhu [b,*]

[a] Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China

ARTICLE INFO

Article history:
Received 3 March 2017
Revised 21 May 2017
Accepted 23 May 2017

Keywords:
Cat map
Peak-to-average power ratio
Orthogonal frequency division multiplexing
Passive optical network

ABSTRACT

This work develops a solution for simultaneous physical layer security enhancement and peak-to-average power ratio (PAPR) reduction for orthogonal frequency division multiplexing passive optical network (OFDM-PON) systems. The encryption is carried out within the subcarriers with the help of three-dimensional (3-D) chaotic cat map. Experimental results demonstrate that the OFDM-PON system under the protection of the proposed technique is high sensitive to the secret key, invalid optical network units cannot obtain any useful information from the ciphertext. Besides, the PAPR of the OFDM symbols has also been significantly reduced, and hence the system is more robust against various nonlinear disturbances.

1. Introduction

Owing to the satisfactory tolerance to fiber dispersion, significant system flexibility and potentially low-cost for the access network beyond 10G, orthogonal frequency division multiplexing passive optical network (OFDM-PON) has emerged as the most attractive candidate for future ultra-high-speed optical access [1–3]. The booming attractiveness has increased the demand for better security in PON access. Currently, most of the related security achievements focus on the cryptographic and authentication protocol at medium access control (MAC) layer or higher layers [4]. Moreover, only data frames are encrypted whereas the control frames and headers are exposed in the MAC layer. It is well-known that, each optical network unit (ONU) will receive all the data, including the data transmitted to other ONUs, from the optical line terminal (OLT) in PON systems. Once the management information of the MAC layer is exposed to opponents, the data frame can be easily eavesdropped. This leaves the information security threats of the systems. Besides, the physical layer of OFDM-PON system is more vulnerable against various attacks as the physical layer that can be regarded as a transparent pipe for data communication is with high-risk to eavesdrop. Regarding the convenient digital processing of OFDM signal, it is feasible to realize data encryption at physical layer without any modification of the optical networks [5].

In recent years, some effective approaches have been proposed to enhance the security of OFDM-PON at physical layer, with the majority are implemented using various chaotic systems. The prevalence of the chaotic maps in cryptographic systems originates from the intrinsic features such as ergodicity, unpredictability, sensitivity to control parameters and initial states, which can be employed in both permutation and diffusion processes with satisfied efficiency and security [6]. In [5,7], chaos-based scrambling approaches are developed to enhance the security level of OFDM-PON at physical level. The encryption is carried out by shuffling the symbols among subcarriers with the help of a scrambling matrix that is generated by chaotic logistic map. Such scrambling technique in frequency domain has been investigated in [8], with a novel resetting time scheme for the generation of scrambling matrix. A two-dimensional permutation approach is investigated in [9], so as to scramble the data in not only frequency domain but also the time domain, and is further extended to three-dimensional in [10]. On the other hand, chaos-based constellation masking techniques are also developed for promoting the physical security of OFDM-PON [11–14]. For example, constellation masking both on each subcarrier and among different subcarriers are proposed in [11,12], while a hybrid system of digital chaos with analog chaos is developed in [13]. Besides, Zhang et al. proposes illuminating quadrature amplitude modulation (QAM) encryption methods in very recent years [15–19]. Specially speaking, the real (I) and imaginary (Q) parts are proposed to be separately coded with key sequences generated by a modified logistic mapping [15], and then a novel method that the IQ parts are independently

* Corresponding author.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.yofte.2017.05.013
1068-5200/

permutated is investigated in [16] so that the transmitted QAM symbols as well as symbol-to-subcarrier mapping can be simultaneously changed and disrupted. In [17], discrete Baker map and Henon map are introduced for encrypting the data before and after IFFT module, and hence more protection can be provided. A security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement is developed in [18], where an advanced cat map is employed to facilitate and secure the key management between the sender and receiver. In [20], a hybrid symbol substitution and interleaving technique based on Brownian motion is proposed, where the parameters of the Brownian motion are generated by using the chaotic maps. Besides the security level, another important issue of OFDM-PON on physical layer is the peak-to-average power ratio (PAPR) [14]. The OFDM frames are always with high PAPR, which will enter into the nonlinear area of the subsequent high power amplifier (HPA), such as the traveling wave tube amplifier (TWTA) or solid state power amplifier (SSPA) [21]. In these scenarios, severe inter-symbol-interference emerges, and the transmission performance of the system downgrades accordingly. A solution for simultaneous physical security enhancement and PAPR reduction for OFDM-PON is presented in [19], where the IQ parts of QAM symbols are independently encrypted multiple times and the frame with minimum PAPR is selected for transmission. Experimental results demonstrate that the PAPR at a CCDF of 10^{-4} can be reduced more than 2.8 dB compared with the original OFDM signal. In the above chaos-based security enhancements for OFDM-PON, the initial values or/and control parameters of the employed chaotic systems serve as the secret key, and should be privately shared between the transmitter and receiver. Such that, only legal ONU who owns valid secret key is able to recover the received data correctly, the eavesdropping from illegal ONUs can be therefore prevented and hence promote the security level of OFDM-PON in physical layer.

In this paper, an approach for physical layer security enhancement and PAPR reduction is presented. A chaotic system, named 3-D cat map [22] is employed to generate three-dimensional (3-D) chaotic sequences. The digital-modulated symbols in each subcarrier will be shuffled with the first chaotic sequence, and then the symbols are phase-modulated by the other two quantized masks, respectively. Consequently, two secure OFDM symbols that represent the same plain information are generated, and the one with lower PAPR will be selected for transmission. Results well reveal the security and PAPR reduction effect of the proposed algorithm. The proposed scheme will be given out in Section 2, while the experimental result is presented in Section 3. Finally, conclusions will be drawn in the last section.

2. Systems and principles

The proposed secure OFDM-PON system is illustrated in Fig. 1. The key stream elements are generated from a 3-D cat map [22], as described by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod 1, \tag{1}$$

where

$$A = \begin{bmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}, \tag{2}$$

$mod(x, y)$ divides x by y and returns the remainder of the division. The chaotic map is invertible and area-preserving as $\det|A| = 1$. As a special case $a_x = b_x = a_y = b_y = a_z = b_z = 1$, the three eigenvalues of A can be easily obtained: $\sigma_1 = 7.1842$, $\sigma_2 = 0.2430$ and $\sigma_3 = 0.5728$. Note that the leading Lyapunov characteristic exponent is strictly larger than 1, meaning that the 3-D map is in a stronger sense chaotic and therefore can perform better data mixing.

The encryption is performed within each OFDM symbol, in other words, among the subcarriers. Without loss of generality, we suppose that the OFDM system has N subcarriers, and the data in each subcarrier is $S = [s(1), s(2), \cdots, s(N)]$. For each symbol, the chaotic map will be iterated N times, and then we can get three chaotic series, described as $X = [x(1), x(2), \cdots, x(N)]$, $Y = [y(1), y(2), \cdots, y(N)]$, and $Z = [z(1), z(2), \cdots, z(N)]$. Then these values will be quantized to the required key stream sequences, denoted as $K^{(X)} = \left[k^{(X)}(1), k^{(X)}(2), \cdots, k^{(X)}(N)\right]$, $K^{(Y)} = \left[k^{(Y)}(1), k^{(Y)}(2), \cdots, k^{(Y)}(N)\right]$, and $K^{(Z)} = \left[k^{(Z)}(1), k^{(Z)}(2), \cdots, k^{(Z)}(N)\right]$, respectively. The transformation is performed according to Eqs. (3)–(5), respectively, where $n \in (1, 2, \cdots, N)$.

$$k^{(X)}(n) = mod\left[x(n) \times 10^{15}, N - n + 1\right] + n \tag{3}$$

$$k^{(Y)}(n) = \begin{cases} -1, & if \quad y(n) \leqslant 0.5 \\ 1, & if \quad y(n) > 0.5 \end{cases} \tag{4}$$

$$z^{(Y)}(n) = \begin{cases} -1, & if \quad z(n) \leqslant 0.5 \\ 1, & if \quad z(n) > 0.5 \end{cases} \tag{5}$$

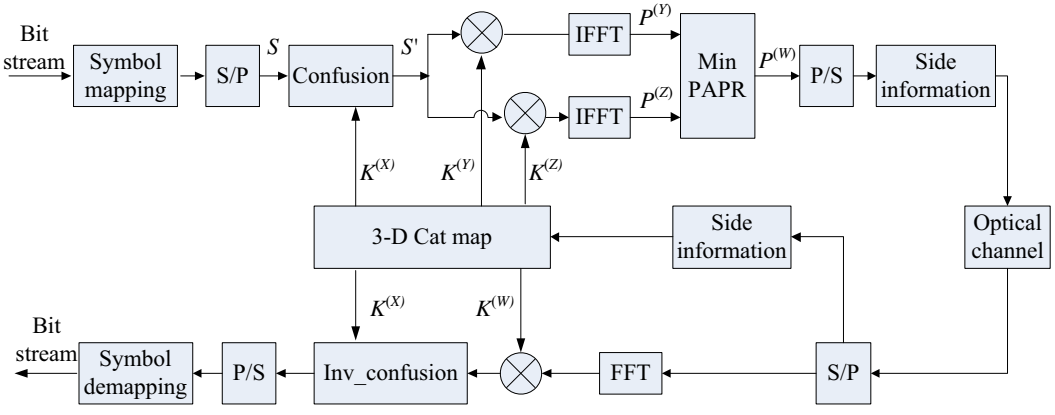

Fig. 1. The block diagram of the secure OFDM-PON system.