物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于动态混沌映射的三维加密正交频分复用无源光网络

林书庆 江宁 王超 胡少华 李桂兰 薛琛鹏 刘雨倩 邱昆

A three-dimensional encryption orthogonal frequency division multiplexing passive optical network based on dynamic chaos-iteration

Lin Shu-Qing Jiang Ning Wang Chao Hu Shao-Hua Li Gui-Lan Xue Chen-Peng Liu Yu-Qian Qiu Kun

引用信息 Citation: Acta Physica Sinica, **67**, 028401 (2018) DOI: 10.7498/aps.20171246
在线阅读 View online: http://dx.doi.org/10.7498/aps.20171246
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2018/V67/I2

基于动态混沌映射的三维加密正交频分复用无源光网络*

林书庆 江宁† 王超 胡少华 李桂兰 薛琛鹏 刘雨倩 邱昆

(电子科技大学通信与信息工程学院, 光纤传感与通信教育部重点实验室, 成都 611731)

(2017 年 5 月 31 日收到; 2017 年 10 月 12 日收到修改稿)

提出了一种基于混沌映射的三维加密正交频分复用无源光网络保密通信系统. 该系统通过相关性检测锁定收发端混沌系统参数, 实现收发双方混沌系统同步; 并利用同步混沌系统生成密钥, 实现符号扰动以及二重子载波加密. 该加密方案的密钥空间超过 10^{86}, 能够有效对抗穷举攻击. 实验实现了 13.3 Gb/s 基于 64 进制正交幅度调制的加密正交频分复用信号在 25 km 标准单模光纤中的传输, 并完成了信息的有效解密.

关键词: 正交频分复用, 无源光网络, 动态混沌同步, 混沌加密

PACS: 84.40.Ua, 42.81.Uv, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.67.20171246

1 引 言

随着通信网络的高速发展, 信息安全已经成为关系国计民生的重要问题, 已经上升至国家战略层面. 作为宽带接入网重要支撑技术的无源光网络 (passive optical network, PON) 技术由于其大吞吐量和高服务质量已经成为最有潜力的宽带光接入解决方案[1−5]. 在现有 PON 网络中, 基于正交频分复用的无源光网络 (orthogonal frequency division multiplexing passive optical network, OFDM-PON) 由于频谱利用率高、抗色散能力强、资源分配灵活等优势被认为是未来 PON 接入网的重要发展方向[1,4,5]. 然而 PON 网络的开放性使其容易遭受链路窃听、身份冒充等攻击[6,7], 因此从物理层提升 PON 网络数据传输安全性具有重要意义.

混沌系统因其高度的初始敏感性、类噪声、大带宽等特点, 在保密通信领域具有重要应用前景. 近二十年来, 基于激光混沌的物理层加密通信技术已成为保密通信领域的研究热点, 研究者们对单/双向耦合激光混沌系统的同步机理、同步条件、同步类型、混沌加密/解密技术、混沌通信性能等各方面进行了详细全面的研究[8−15]. 2005 年, Argyris 等[16] 在雅典的城市商用光纤网络上成功实现了速率为 1 Gbit/s, 传输距离为 120 km 的高速混沌保密通信; 该实验证明了高速混沌加密通信的可行性. 另一方面, 近年来在 OFDM 调制过程中利用混沌序列对数据进行加密实现高速保密通信成为一个新兴的热点研究课题. 目前, 国内外学者们已经提出了多种基于混沌的 OFDM-PON 物理层加密方案[17−24]. 文献 [17, 18] 利用混沌序列对信息进行频域扰动实现加密, 提升通信安全性. 文献 [19] 从时域和频域两个角度对信息进行加密, 达到提升安全性的目的. 文献 [20, 21] 提出了将分数阶傅里叶变换与混沌加密结合的多维加密方法, 并分析了该加密方法对系统峰均功率比 (peak to average power ratio, PAPR) 的影响. 文献 [22, 23] 分析了同时实现信息加密与降低系统 PAPR 的混沌加密方法, 对比了不同加密条件对 PAPR 下降的影响. 文献 [24] 将混沌序列用于控制相干通信中的正交幅度调制 (quadrature amplitude modulation,

* 国家自然科学基金 (批准号: 61671119, 61471087, 61301156) 资助的课题.

† 通信作者. E-mail: uestc_nj@uestc.edu.cn

QAM) 以及替换导频和训练序列, 从信息、导频和训练序列三个角度进行加密, 提升了安全性. 上述面向OFDM技术的混沌保密通信技术主要集中于混沌加密方案的研究, 而未对混沌密钥分发进行详细探讨. 针对此问题, 本文提出一种基于动态参数控制的混沌密钥分发方法, 并在此基础上提出一种基于动态混沌映射的二重子载波加密和符号扰动的三维加密OFDM-PON.

本文首先介绍了基于动态参数控制的混沌密钥分发方法以及基于动态混沌映射的二重子载波加密和符号扰动的三维加密OFDM-PON系统, 然后研究分析了该加密系统的性能及安全性, 最后进行基于64QAM调制的13.3 Gb/s@25 km单模光纤传输的OFDM-PON系统实验验证.

2 基于动态参数控制的密钥分发方法

混沌同步是实现密钥安全分发的前提, 收发端混沌系统动态同步过程如图1所示. 混沌系统的输出序列由系统参数决定, 系统参数包含静态参数和动态参数, 其中静态参数来自参数集U_0, U_0中仅包含一组静态参数; 动态参数来自于参数集U_1, U_1中包含多组动态参数, 每组动态参数由不同的系统初值和工作参数组成; U_0和U_1由收发双方按照约定方式产生.

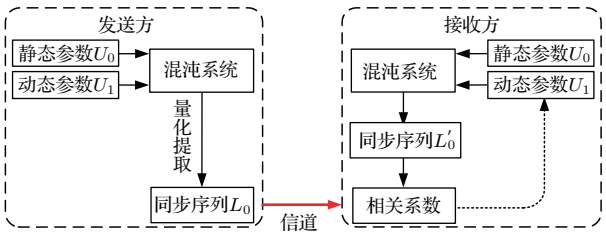

图1 混沌系统的动态同步原理

Fig. 1. Schematic of the dynamic synchronized chaotic system.

同步过程中, 发送方从动态参数集U_1中随机选取一组动态参数, 并结合静态参数共同控制混沌系统得到长度为l_0的二元同步序列L_0, 然后发送到接收方.

$$L_0 = \text{extract}(B, l_0), \tag{1}$$

式中B为二元序列, 由混沌序列量化产生, 运算"extract"表示从B中提取长度为l_0的序列L_0.

接收方保存接收到的二元同步序列L_0, 然后从本地动态参数集U_1中随机选取一组动态参数用于控制混沌系统产生长度为l_0的二元同步序列L_0', 并计算L_0和L_0'的相关系数. 由于混沌系统的高度初始敏感性, 不同的动态参数组将使混沌迭代的结果不相关, 二元同步序列L_0和L_0'之间相关系数将接近0. 接收方在已知动态参数集U_1的情况下, 经过多次尝试, 根据相关系数大小即可判定是否实现了与发送方混沌系统同步. 同步后的混沌系统输出序列一致, 收发双方利用该同步混沌系统产生混沌序列, 并经量化生成密钥, 实现数据加/解密. 整个密钥分发过程无需进行任何参数传递, 有效地提升了密钥的安全性.

3 基于动态混沌映射的三维加密OFDM-PON

以每个ONU连接4个用户为例, 对提出的基于动态混沌映射的三维加密OFDM-PON展开分析. 加密方案如图2所示. 收发双方首先进行混沌同步, 然后利用同步混沌系统生成密钥, 实现密钥的正确分发, 并用于控制信息加/解密. 发送端, 用户A, B, C, D分别产生一串比特序列, 并进行64QAM映射. 完成64QAM映射后, 发送方提取一定长度的混沌序列经量化生成矩阵$\boldsymbol{M}_1$用于控制子载波映射.

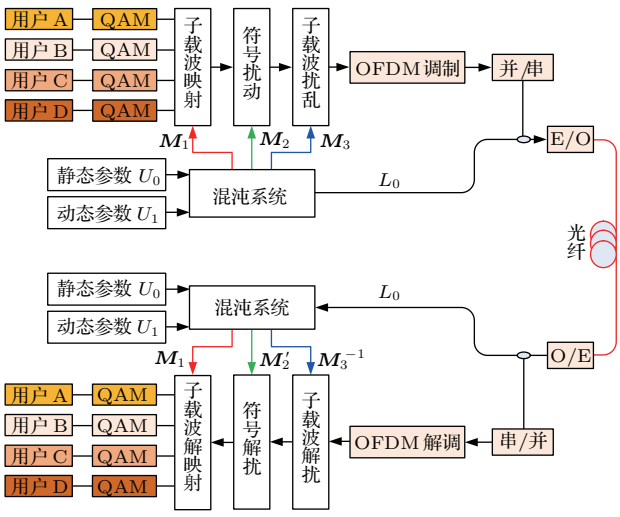

图2 基于动态混沌映射的三维加密OFDM-PON

Fig. 2. Schematic of the three-dimension encryption OFDM-PON based on dynamic chaos-iteration.

设 $f(f=1,2,\cdots,N)$ 表示子载波, N 表示子载波总数, 用户 A, B, C, D 根据 $\boldsymbol{M}_1$ 获取的子载波数分别为 $N_{\rm A}$, $N_{\rm B}$, $N_{\rm C}$, $N_{\rm D}$, 且满足

$$N=N_{\rm A}+N_{\rm B}+N_{\rm C}+N_{\rm D}. \tag{2}$$

设总的子载波集合为 $U_{\rm f}=\{1,2,\cdots,N\}$, 用户 A, B, C, D 根据 $\boldsymbol{M}_1$ 获取的子载波集合分别为 $U_{\rm A}$, $U_{\rm B}$, $U_{\rm C}$, $U_{\rm D}$, 则子载波集合满足如下关系:

$$U_{\rm A}=\{f_{A_i}, i=1,2,\cdots,N_{\rm A}\}, \tag{3}$$

$$U_{\rm B}=\{f_{B_i}, i=1,2,\cdots,N_{\rm B}\}, \tag{4}$$

$$U_{\rm C}=\{f_{C_i}, i=1,2,\cdots,N_{\rm C}\}, \tag{5}$$

$$U_{\rm D}=\{f_{D_i}, i=1,2,\cdots,N_{\rm D}\}, \tag{6}$$

$$U_{\rm f}=U_{\rm A}\cup U_{\rm B}\cup U_{\rm C}\cup U_{\rm D}, \tag{7}$$

$$U_i\cap U_j=\emptyset,\quad i,j\in\{{\rm A},{\rm B},{\rm C},{\rm D}\}且 i\neq j. \tag{8}$$

将用户 A 的信息记为 $\boldsymbol{S}_{\rm A}=A_1,A_2,\cdots,A_{N_{\rm A}}$; 用户 B 的信息记为 $\boldsymbol{S}_{\rm B}=B_1,B_2,\cdots,B_{N_{\rm B}}$; 用户 C 的信息记为 $\boldsymbol{S}_{\rm C}=C_1,C_2,\cdots,C_{N_{\rm C}}$; 用户 D 的信息记为 $\boldsymbol{S}_{\rm D}=D_1,D_2,\cdots,D_{N_{\rm D}}$; 用户 A, B, C, D 的信息按照先后顺序依次映射到各自的子载波上. 不同的 $\boldsymbol{M}_1$ 控制下, 各用户所获取的子载波数目和位置一般不相同, 相对应的各用户的信息 $\boldsymbol{S}_{\rm A}$, $\boldsymbol{S}_{\rm B}$, $\boldsymbol{S}_{\rm C}$, $\boldsymbol{S}_{\rm D}$ 的长度也是动态变化的. 定义映射运算符“map”表示子载波映射, 则子载波映射过程可表示为

$$\boldsymbol{S}_1={\rm map}[(\boldsymbol{S}_{\rm A},\boldsymbol{S}_{\rm B},\boldsymbol{S}_{\rm C},\boldsymbol{S}_{\rm D}),\boldsymbol{M}_1], \tag{9}$$

$\boldsymbol{S}_1$ 为随机子载波映射后的符号矩阵. 然后利用一定长度的混沌序列经量化生成符号扰动矩阵 $\boldsymbol{M}_2=[m_{k,l}]$ 实现符号扰动, 扰动矩阵 $\boldsymbol{M}_2$ 与符号矩阵 $\boldsymbol{S}_1$ 行列数一致且 $m_{k,l}={\rm e}^{{\rm j}B(i)}$, $B(i)$ 由混沌序列量化产生. 定义矩阵运算“F”表示矩阵对应位置的元素一一相乘, 则扰动过程可表示如下:

$$\boldsymbol{S}_2=F(\boldsymbol{S}_1,\boldsymbol{M}_2), \tag{10}$$

(10) 式中 $\boldsymbol{S}_2$ 为扰动完成后的符号矩阵. 最后利用混沌序列量化生成可逆矩阵 $\boldsymbol{M}_3$ 扰乱所有子载波顺序,

$$\boldsymbol{M}_3=\boldsymbol{I}\times\boldsymbol{E}_1\boldsymbol{E}_2\cdots\boldsymbol{E}_p, \tag{11}$$

$$\boldsymbol{S}_3=\boldsymbol{S}_2\times\boldsymbol{M}_3, \tag{12}$$

(11) 式中 $\boldsymbol{I}$ 为单位矩阵, $\boldsymbol{E}_i$ 为初等矩阵; (12) 式中 $\boldsymbol{S}_3$ 为扰乱后的符号矩阵. 加密完成后的 OFDM 时域信号可表示为

$$\begin{aligned}\boldsymbol{s}_{(t)}=&\sum_{k=1}^{N}(F(\boldsymbol{S}_1,\boldsymbol{M}_2)\times\boldsymbol{M}_3)_{(k)}\\&\times\exp\left[{\rm j}2\pi f_{(k)}\frac{(t-1)T}{N}\right]\\&t=1,2,\cdots,N,\end{aligned} \tag{13}$$

式中 N 表示快速傅里叶反变换 (inverse fast fourier transform, IFFT) 的长度, T 为符号周期, $f_{(k)}$ 表示第 k 个子载波频率.

加密完成后, 发送方利用 IFFT 实现 OFDM 调制, 然后进行并串转换, 并调制到光载波上. 接收方接收到数据后进行串并转换, 利用快速傅里叶变换 (fast Fourier transform, FFT) 完成 OFDM 解调, 然后进行信号恢复、解密和 QAM 解调. 定义运算符“demap”表示子载波解映射, 则解密过程可表示如下:

$$\begin{aligned}\boldsymbol{S}_i=&{\rm demap}[F(\boldsymbol{S}_3'\times\boldsymbol{M}_3^{-1},\boldsymbol{M}_2'),\boldsymbol{M}_1]\\&i={\rm A},{\rm B},{\rm C},{\rm D},\end{aligned} \tag{14}$$

式中 $\boldsymbol{S}_3'$ 为 OFDM 解调后的输出符号矩阵, $\boldsymbol{M}_2'=[m_{k,l}']$ 满足 $m_{k,l}\times m_{k,l}'=1$, $\boldsymbol{M}_3^{-1}$ 为 $\boldsymbol{M}_3$ 的逆矩阵. 数据安全性源于三维加密过程, 窃听者在没有密钥的情况下将无法准确获取信息.

用于产生密钥的混沌系统由二维耦合 Logistic 映射 [23,25] 构成, 数学模型如下:

$$\begin{cases}X_{i+1}=\mu_1X_i(1-X_i)+\gamma_1Y_i^2,\\Y_{i+1}=\mu_2Y_i(1-Y_i)+\gamma_2(X_i^2+X_iY_i),\end{cases} \tag{15}$$

其中参数取值范围满足 $\mu_1\in(2.75,3.4)$, $\mu_2\in(2.75,3.45)$, $\gamma_1\in(0.15,0.21)$, $\gamma_2\in(0.13,0.15)$, 混沌序列 $X_i,Y_i\in(0,1)$. 方案中, 规定混沌系统的初值 (X_0,Y_0) 为动态参数, 由动态参数集合 U_1 确定, 任意一组动态参数的取值属于区间 $(0,1)$; 混沌系统参数 $\mu_1,\mu_2,\gamma_1,\gamma_2$ 为静态参数, 由静态参数集合 U_0 确定, 分别属于区间 $(2.75,3.4)$, $(2.75,3.45)$, $(0.15,0.21)$, $(0.13,0.15)$, 静态参数与动态参数的取值均满足二维耦合 Logistic 系统能进入混沌状态. 混沌序列 (X_i,Y_i) 为混沌系统输出序列. 为了增强统计特性, 将序列 (X_i,Y_i) 进行如下量化操作后, 再用于生成密钥, 控制加解密处理过程.

$$\begin{aligned}X_i&=10^6X_i-{\rm floor}(10^6X_i),\\Y_i&=10^6Y_i-{\rm floor}(10^6Y_i);\end{aligned} \tag{16}$$

$$B_{2i-1}=\begin{cases}0, & X_i<0.5,\\ 1, & X_i\geqslant 0.5,\end{cases}$$
$$B_{2i}=\begin{cases}0, & Y_i<0.5,\\ 1, & Y_i\geqslant 0.5,\end{cases} \tag{17}$$

(16)式中运算“floor”表示向下取整.

由于加密处理产生的密钥空间大于混沌系统的密钥空间, 因此加密方案的安全性主要依赖于混沌系统密钥空间及其输出序列B的安全性. 图3(a)—(d)分别给出了混沌系统的初值敏感性、混沌序列X_i、二元序列B、同步序列L_0的自相关系数曲线. 自相关系数定义如下[26−28]:

$$R_{XX}(\tau)=\frac{\langle[X(i-\tau)-\langle X(i-\tau)\rangle]\times[X(i)-\langle X(i)\rangle]\rangle}{\sqrt{\langle[X(i-\tau)-\langle X(i-\tau)\rangle]^2\rangle\times\langle[X(i)-\langle X(i)\rangle]^2\rangle}}, \tag{18}$$

其中X表示进行相关性测试的实数序列, i和τ为整数, 运算“$\langle\cdot\rangle$”表示求算数平均值, R_{XX}为X的自相关系数. 图3(a)验证了混沌系统的高度初值敏感性(10^{-15}); 图3(b)—(d)则分别表明混沌序列X_i、二元序列B、同步序列L_0均具有良好的自相关特性.

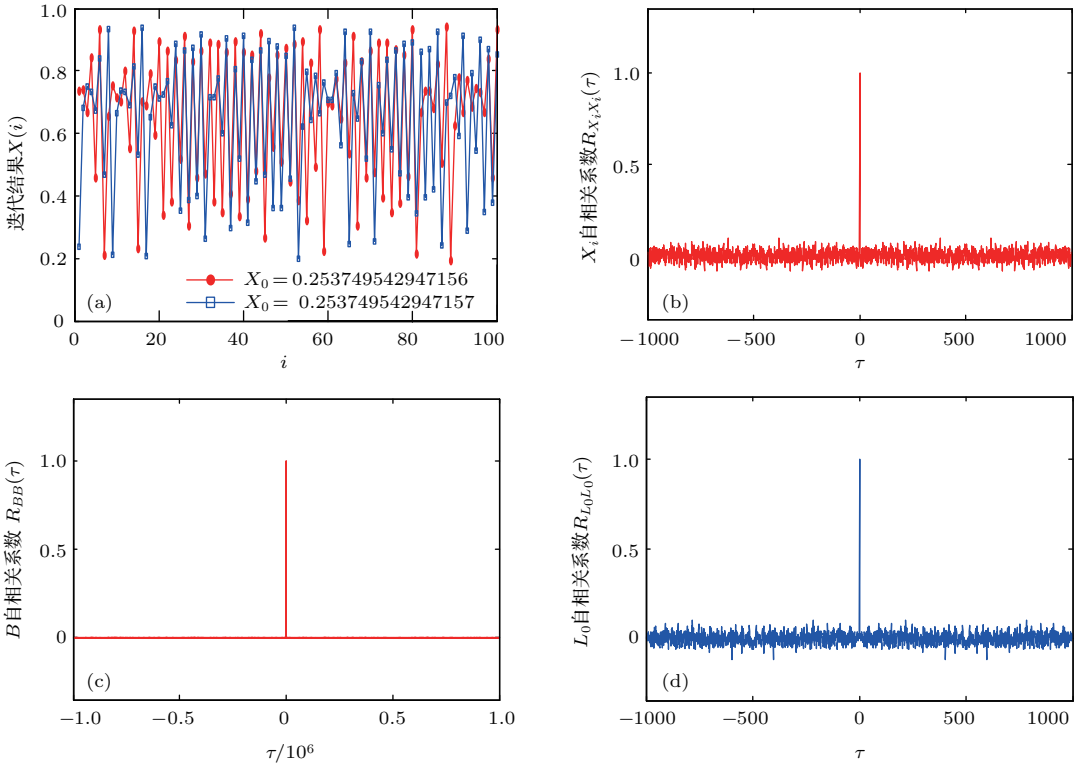

图3 (a) 二维耦合Logistic混沌系统初值敏感性; (b) 混沌序列X_i的自相关系数; (c) 二元序列B的自相关系数; (d) 同步序列L_0的自相关系数

Fig. 3. (a) Sensibility to the initial value X_0; (b) self-correlation curves of chaotic sequence X_i; (c) self-correlation curves of binary sequence B; (d) self-correlation curves of synchronization sequence L_0.

为了验证本方案采用的混沌系统产生的二元序列的随机性, 表1给出了随机选择1000组初始值产生的二元序列B的随机性测试结果. 这里采用国际标准NIST SP800-22对随机性进行测试, 每个样本包含1 Mb的二进制序列, 显著水平设为0.01[29]. 结果表明, 序列B能通过标准NIST SP800-22的所有15项随机性测试. 结合(15)式, 系统输出序列由参数$(X_0,Y_0,\mu_1,\mu_2,\gamma_1,\gamma_2)$决定, 因此加密方案的密钥空间为$5.46\times10^{86}(1\times1\times0.65\times0.7\times0.06\times0.02\times10^{15\times6})$[23]. 若用穷举法破解该混沌加密系统, 以每秒3.38×10^{17}的运算速度, 需要1.61×10^{69} a, 这表明该加密方案能够有效对抗穷举攻击. 动态参数控制下, 任意时刻混沌系统输出均随着初始条件的变化而改变, 窃密者在破解混沌

表 1 NIST SP800-22 随机性测试结果[29]

Table 1. Result of NIST SPECIAL PUBLICATION 800-22 TEST[29].

统计测试指标	P 值	百分比	结果
单比特频数测试	0.681789	0.991	通过
分块频数测试	0.196392	0.996	通过
累加和测试	0.806491/ 0.565663	0.992/ 0.993	通过
游程测试	0.563615	0.992	通过
块内长游程测试	0.857181	0.993	通过
二进制矩阵秩测试	0.734904	0.987	通过
离散傅里叶变换测试	0.799073	0.988	通过
非周期性测试	0.310795	0.991	通过
重叠块匹配测试	0.288958	0.984	通过
Maurer 的通用测试	0.204985	0.989	通过
近似熵检测	0.984178	0.996	通过
随机游动测试	0.118924	0.990	通过
随机游动状态频数测试	0.784127	0.992	通过
串行测试	0.586241	0.999	通过
线性复杂度测试	0.009103	0.988	通过

系统时, 需要同时考虑系统初始敏感性和动态参数的变化, 直接跟踪并破解混沌系统更加复杂. 同时, 动态参数还有助于系统获取更丰富的序列 B, 增大窃听者破译信息的难度, 提升数据传输安全性.

4 实验分析

图 4 为基于二重载波加密与符号扰动的三维加密 OFDM-PON 实验系统. 该系统包含一个光线路终端 (optical line terminal, OLT), 两个合法光网络节点 (optical network unit, ONU) 以及一个窃听 ONU. 在 OLT 端, 下行数据进行 64QAM 调制和加密映射到子载波上. 为保证 OFDM 调制信号全为实值, 本文利用了 Hermitian 对称结构[22], 即在 512 个子载波中, 仅 255 个子载波传输 64QAM 数据, 1 个子载波作为直流分量, IFFT 的长度为 512. OFDM 调制完成后, 进行并串转换, 然后插入 1/8 符号长度的循环前缀. 以上过程均通过线下处理实现. 加密 OFDM 信号被加载到符号率为 5 Gs/s 的任意波形发生器 (AWG7102) 产生 OFDM 电信号, 并通过 MZ 调制器调制到波长为 1550 nm 光载波上. 加密 OFDM 信号时域波形以及频谱如图 5 所示, 信号带宽为 2.5 GHz, 信息速率为 13.3 Gb/s ($5\ \text{Gs/s} \times \log_2 64 \times 8/9 \times 255/512$). 在 ONU 端, 接收信号经过带宽为 10 GHz 的光电探测器 (photodiode, PD) 后, 利用数字示波器 (采样率 25 Gs/s) 保存, 然后通过线下处理依次进行 OFDM 解调、信号恢复、解密和 QAM 解调.

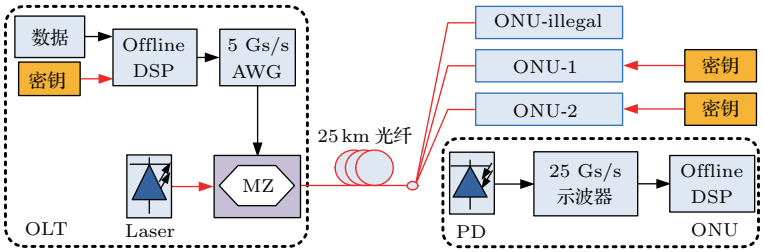

图 4 三维加密 OFDM-PON 的实验系统设置

Fig. 4. Experimental setup of the proposed three-dimension encryption OFDM-PON.

进行数据解密前, 接收方首先需要实现与发送方的混沌同步. 通过计算机仿真模拟该过程, 得到如图 6 所示的仿真结果. 静态参数 $\mu_1, \mu_2, \gamma_1, \gamma_2$ 的取值分别为 3.20, 3.05, 0.17, 0.14, 动态参数集 U_1 包含 100 组动态参数, 且任意一组动态参数 $(X_0, Y_0)_i$ 的取值属于区间 $(0, 1)$, 静态参数与动态参数均满足系统能进入混沌状态, 同步序列 L_0 的长度为 1000. 根据图 6 中的结果, 当且仅当 $i = 50$ 收发双方动态参数一致, 同步序列 L_0 与 L_0' 相关系数为 1, 即接收方实现了与发送方的混沌同步, 而其余动态参数控制下, 相关系数均小于 0.1, 接收方未实现与发送方混沌同步.

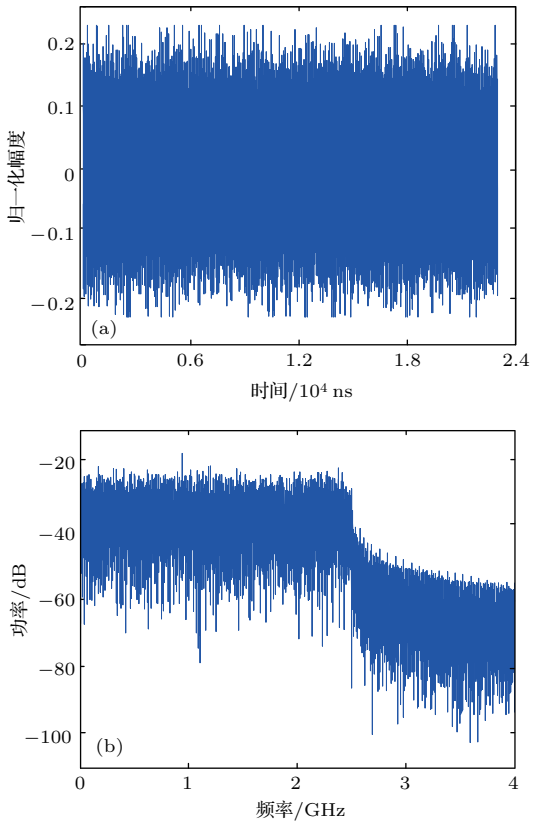

图 5 (a) 加密 OFDM 信号时域波形; (b) 加密 OFDM 信号频谱

Fig. 5. (a) Temporal waveforms and (b) spectrum of the encrypted OFDM signal.

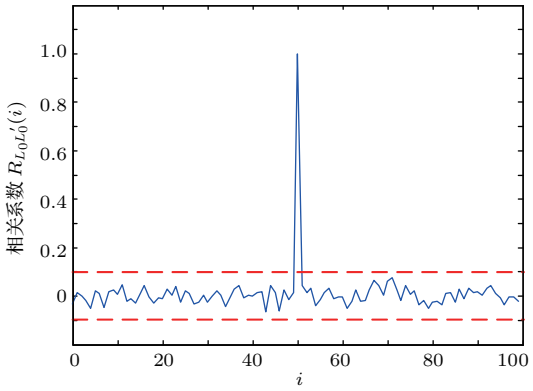

图 6 同步序列 L_0 与 L_0' 的相关系数

Fig. 6. Correlation curves of synchronization sequences L_0 and L_0'.

图 7 给出了合法用户和非法窃听者解密信息的误比特率随接收光功率的变化曲线, 以及接收光功率为 −7 dBm 时加密信号经 25 km 标准单模光纤传输后的合法用户与窃听者的星座图. 实验结果表明: 对于背靠背传输和经 25 km 标准单模光纤传输的加密 OFDM 信号, 当接收光功率分别大于 −11 和 −8 dBm 时, 合法用户的误比特率下降到 FEC (forward error correction, FEC) 限以下, 即合法用户能够正确获取有效信息; 对于窃听者, 由于无法获取密钥进行解密, 其星座图处于混乱状态,

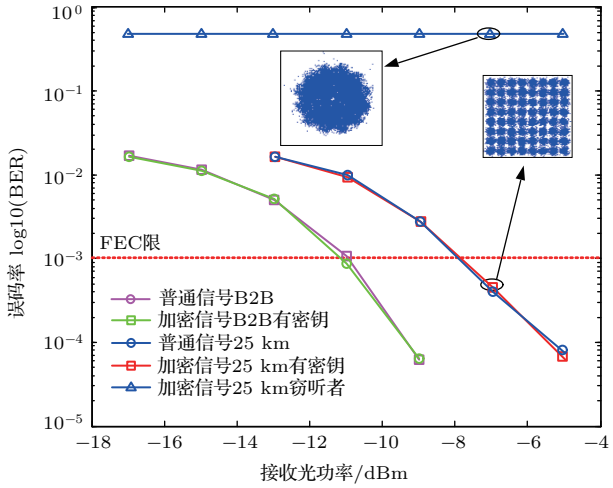

图 7 合法接收和非法接收误比特率随接收光功率的变化

Fig. 7. BER curves for legal decryption and illegal decryption versus the received optical power.

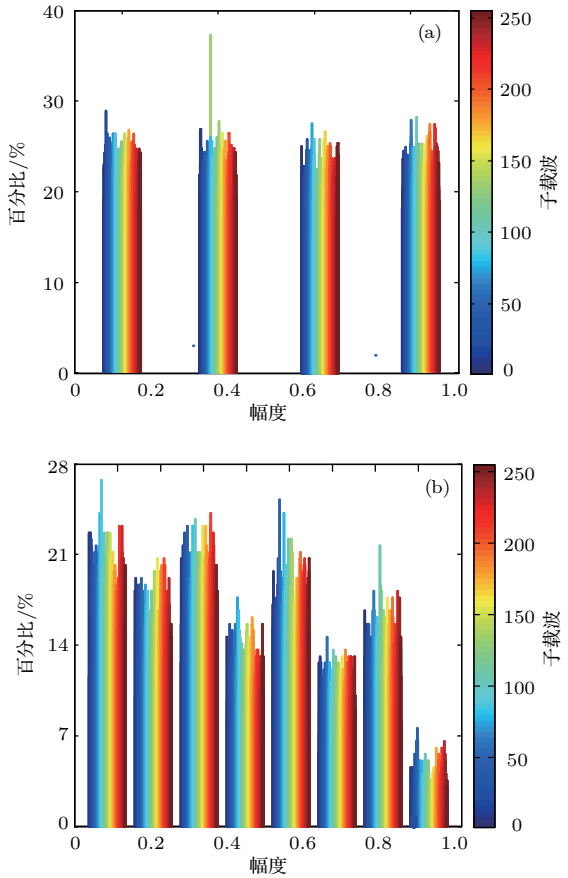

图 8 子载波 QAM 符号归一化幅值统计百分比 (a) 加密处理前; (b) 加密处理后

Fig. 8. Statistical histograms with subcarriers of 255: (a) Before QAM symbol scrambling; (b) after QAM symbol scrambling.

误码率始终在0.46附近, 无法获取有效信息. 值得注意的是, 相较于普通OFDM信号传输, 本文提出的三维加密OFDM信号的传输不会造成系统额外的光功率代价. 加密前后各子载波上的QAM符号归一化幅值统计如图8所示. 统计结果表明, 加密处理使得QAM符号的归一化幅值分布更加丰富, 有效地掩盖了原始的QAM符号统计分布特性, 有利于抵抗统计分析攻击, 提升安全性.

5 结 论

利用混沌系统的初始敏感性和相关性检测方法, 提出了一种基于动态同步的密钥分发方法. 该方法可以增加密钥系统的复杂度, 增大破解混沌系统的难度, 并有助于获取更丰富的密钥序列, 增加破译信息的难度; 此外, 该方法也无需传递任何系统参数, 可以有效提升密钥安全性; 通过分析密钥生成系统的初始值敏感性和混沌序列的相关性以及基于混沌的二元序列的随机性表明, 该密钥分配系统密钥空间可达10^{86}以上, 能有效抵抗穷举攻击. 在此基础上, 通过对OFDM信号进行二重混沌子载波加密和符号扰动, 建立了一种三维加密OFDM-PON系统. 实验结果表明, 合法解密可以正确恢复信息, 而非法窃密者的误码率始终在0.46附近. 本文提出的基于动态混沌映射的三维加密OFDM-PON能够有效提高信息传输安全性.

参考文献

[1] Zhang J, Qiu K, Bao W B, Deng M L, Li Y G, Zhang H B 2009 *China Commun.* **2009** 103

[2] Cvijetic N, Qian D Y, Hu J Q 2010 *IEEE Commun. Mag.* **48** 70

[3] Qian D Y, Cvijetic N, Hu J Q, Wang T 2010 *J. Lightwave Technol.* **28** 484

[4] Qiu K, Yi X W, Zhang J, Zhang H B, Deng M L, Zhang C F 2011 *Proc. SPIE* **8309** 1

[5] Zhang L J, Xin X J, Liu B, Yu J J, Zhang Q 2010 *Opt. Express* **18** 18347

[6] Ren J Y 2009 *Netinf. Security* **2009** 61 (in Chinese) [任建勇 2009 信息网络安全 **2009** 61]

[7] Peng D Q, Gu Y, Wan L Y, Chen Y 2015 *Video Engineer.* **39** 50 (in Chinese) [彭大芹, 谷勇, 万里燕, 陈勇 2015 电视技术 **39** 50]

[8] Wu L C 2006 *China Water Transport* **6** 125 (in Chinese) [吴立春 2006 中国水运 (学术版) **6** 125]

[9] Liu L Z, Zhang J Q, Xu G X, Liang L S, Wang M S 2014 *Acta Phys. Sin.* **63** 010501 (in Chinese) [刘乐柱, 张季谦, 许贵霞, 梁立嗣, 汪茂盛 2014 物理学报 **63** 010501]

[10] Li X F, Pan W, Ma D, Luo B, Zhang W L, Xiong Y 2006 *Acta Phys. Sin.* **55** 5094 (in Chinese) [李孝峰, 潘炜, 马冬, 罗斌, 张伟利, 熊悦 2006 物理学报 **55** 5094]

[11] Cao L P, Xia G Q, Deng T, Lin X D, Wu Z M 2010 *Acta Phys. Sin.* **59** 5541 (in Chinese) [操良平, 夏光琼, 邓涛, 林晓东, 吴正茂 2010 物理学报 **59** 5541]

[12] Zhao Q C, Wang Y C 2010 *Laser Optoelectron. Prog.* **47** 030602 (in Chinese) [赵清春, 王云才 2010 激光与光电子学进展 **47** 030602]

[13] Zhao Y M, Xia G Q, Wu J G, Wu Z M 2013 *Acta Phys. Sin.* **62** 214206 (in Chinese) [赵艳梅, 夏光琼, 吴加贵, 吴正茂 2013 物理学报 **62** 214206]

[14] Xiang S Y, Wen A J, Pan W, Lin L, Zhang H X, Zhang H, Guo X X, Li J F 2016 *J. Lightwave Technol.* **34** 4221

[15] Xue C P, Jiang N, Lü Y X, Wang C, Li G L, Lin S Q, Qiu K 2016 *Opt. Lett.* **41** 3690

[16] Argyris A, Syvridis D, Larger L, Annovazze-Lodi V, Colet P, Fischer I, Garcia-Ojalvo J, Mirasso R C, Pesquera L, Shore K A 2005 *Nature* **438** 343

[17] Zhang L J, Xin X J, Liu B, Yu J J 2012 *Opt. Express* **20** 2255

[18] Liu B, Zhang L J, Xin X J, Liu N 2016 *IEEE Photon. Technol. Lett.* **28** 2359

[19] Zhang L J, Liu B, Xin X J, Zhang Q, Yu J J, Wang Y J 2013 *J. Lightwave Technol.* **31** 74

[20] Deng L, Cheng M F, Wang X L, Li H, Tang M, Fu S N, Shum P, Liu D M 2014 *J. Lightwave Technol.* **32** 2629

[21] Cheng M, Deng L, Wang X, Li H, Tang M, Ke C, Shum P, Liu D 2014 *IEEE Photon. J.* **6** 1

[22] Hu X L, Yang X L, Shen Z W, He H, Hu W S, Bai C L 2015 *IEEE Photon. Technol. Lett.* **27** 2429

[23] Zhang W, Zhang C F, Chen C, Jin W, Qiu K 2016 *IEEE Photon. Technol. Lett.* **28** 998

[24] Jin W, Zhang C F, Yuan W C 2016 *Opt. Engineer.* **55** 026103

[25] Wang X Y, Shi Q J 2005 *Chin. J. Appl. Mech.* **22** 501

[26] Zhang J Z, Wang A B, Wang J F, Wang Y C 2009 *Opt. Express* **17** 6357

[27] Jiang N, Pan W, Yan L S, Luo B, Zhang W L, Xiang S Y, Yang L, Zheng D 2010 *J. Lightwave Technol.* **28** 1978

[28] Wu J G, Wu Z M, Liu Y R, Fan L, Tang X, Xia G Q 2013 *J. Lightwave Technol.* **31** 461

[29] Zhang L M, Pan B W, Chen G C, Guo L, Lu D, Zhao L J, Wang W 2017 *Sci. Rep.* **8** 45900

A three-dimensional encryption orthogonal frequency division multiplexing passive optical network based on dynamic chaos-iteration*

Lin Shu-Qing Jiang Ning† Wang Chao Hu Shao-Hua Li Gui-Lan Xue Chen-Peng Liu Yu-Qian Qiu Kun

(*Key Laboratory of Optical Fiber Sensing and Communications (Education Ministry of China), School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*)

(Received 31 May 2017; revised manuscript received 12 October 2017)

Abstract

Orthogonal frequency-division multiple passive optical network (OFDM-PON) has emerged as one of the most promising solutions to meet the requirements for the next-generation wide-band optical access network with high capacity, strong fiber dispersion tolerance, and flexible resource allocation. However, like other optical access network in which the downstream signal is broadcasted to all the optical network units (ONUs), OFDM-PON is vulnerable to being eavesdropped. Thus the security of OFDM-PON should be taken seriously into consideration.

Recently, some chaos based encryption methods, including chaotic scrambling and permutation, hyper-chaotic system and fractional Fourier transformation, chaos based IQ encryption method and chaos based two-dimensional scrambling, have been proposed to enhance the physical layer security of OFDM-PON system. Owing to the special chaos-related characteristics, such as ergodicity, pseudo randomness, and high sensitivity to the initial values, etc., these encryption methods are of high physical layer security. However, in most of these schemes, key distribution is not considered.

In this paper, we propose a three-dimensional encryption OFDM-PON based on dynamic chaos-iteration. The key distribution is implemented through the dynamic chaos synchronization between the transmitter and receiver. The receiver tries to synchronize his chaos system with the transmitters' by calculating the correlation index of the synchronization sequence, which comes from the transmitter and is controlled by dynamic parameters in the parameter sets. The calculation is not very complex because the transmitter and receiver are acquainted with the parameter sets. The synchronized chaos system is used to generate keys for both encryption and decryption.

In the proposed encryption scheme, one ONU is connected with four users, and the message is irrelevant to the users. Quadrature amplitude modulation (QAM) symbols from the users are mapped randomly onto the subcarriers in a flame based on the chaotic matrix $\boldsymbol{M}_1$. For the $\boldsymbol{M}_1$ is changeable, the number and position of subcarriers for different users are dynamically varying. Then the matrix $\boldsymbol{M}_2$ generated from chaos system is utilized to mask all QAM symbols. Finally the QAM symbol matrix is multiplied by an invertible chaotic matrix $\boldsymbol{M}_3$ to realize subcarrier perturbation. These three key matrixes are generated from the two-dimension logistic iteration chaos system, to which the initial sensitivity increases up to 10^{-15}. The output sequence of the chaos system after quantification process is of good self-correlation and cross-correlation characteristic and can pass all NIST SP800-22 randomness tests. The key space of the encryption scheme is over 10^{86}, which would be against exhaustive attack effectively.

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61671119, 61471087, 61301156).

† Corresponding author. E-mail: uestc_nj@uestc.edu.cn

Specifically, a proof-of-principle experiment is conducted to demonstrate the aforementioned proposed scheme. In the experiment, a 13.3 Gb/s encrypted 64QAM OFDM signal transmits over 25 km standard single mode fiber in an OFDM-PON and successfully decrypts at the legal receiver. For an eavesdropper lacking correct keys, the received QAM constellation is totally in disorder and the bit error rate increases up to 0.46, which indicates that not any useful message is eavesdropped. The proposed scheme provides a promising candidate for the next-generation secure optical access networks.

Keywords: orthogonal frequency-division multiple, passive optical network, dynamic chaos synchronization, chaos-based encryption

PACS: 84.40.Ua, 42.81.Uv, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.67.20171246