

安全性增强的双向长距离混沌保密通信

李琼, 邓涛, 吴正茂*, 徐攀, 夏光琼

西南大学物理科学与技术学院, 重庆 400715

摘要 基于混沌同步, 构建安全性增强的双向长距离混沌保密通信系统。结果表明: 在合适的双混沌光注入参数下, 驱动激光器(DL)可以产生低时延特征(TDS)、宽带宽的混沌信号; DL 输出的混沌信号注入到 2 个响应激光器(RLs)中, 通过优化注入参数, 2 个 RLs 可输出 TDS 更低、带宽更宽的混沌信号, 且 2 个混沌信号在实现高质量混沌同步的同时与 DL 输出混沌保持极低的相关系数(小于 0.1); 基于 2 个 RLs 之间高质量的混沌同步, 可实现安全性增强的双向远距离混沌保密通信。采用色散位移光纤作为传输信道, 20 Gbit/s 的信息在传输 120 km 后, 解调信息的 Q 因子大于 6; 而采用普通单模光纤作为传输信道, 1 Gbit/s 的信息在传输 140 km 后, 解调信息的 Q 因子大于 8。

关键词 光通信; 半导体激光器; 混沌保密通信; 混沌同步; 双向传输; 光纤

中图分类号 TN248.4

文献标识码 A

doi: 10.3788/CJL201845.0106001

Security-Enhanced Bidirectional Long-Distance Chaos Secure Communication

Li Qiong, Deng Tao, Wu Zhengmao, Xu Pan, Xia Guangqiong

School of Physical Science and Technology, Southwest University, Chongqing 400715, China

Abstract Based on the chaos synchronization, a security-enhanced bidirectional long-distance chaos secure communication system is proposed. The results show that, under suitable parameters of dual-path injection conditions, low time-delay signature (TDS) and broadband chaotic signals can be generated from driving laser (DL). The chaos signals from DL are injected into two response lasers (RLs). By optimization of injection strength and detuning frequency, the optimized chaos signals with lower TDS and wider bandwidth can be generated and high-quality chaos synchronization between two RLs can be obtained. Meanwhile, the maximal synchronization coefficient between DL and RLs is lower than 0.1. Based on the high-quality chaos synchronization between two RLs, a security-enhanced bidirectional long-distance chaos communication can be achieved. Q factor of 20 Gbit/s decoded messages is more than 6 after a propagation over 120 km under dispersion shifted fiber used as channel, and Q factor of 1 Gbit/s decoded messages is more than 8 after a propagation over 140 km under normal single-mode fiber used as channel.

Key words optical communications; semiconductor laser; chaos secure communication; chaos synchronization; bidirectional transmission; fiber

OCIS codes 060.4510; 140.5960; 140.1540

1 引 言

自 Pecora 和 Carroll 于 1990 年提出并验证混沌

同步方案以来^[1], 基于半导体激光器(SLs)的光混沌系统因具有复杂度高、带宽宽以及与现有光纤系统的兼容性良好等优势而成为混沌保密通信领域的研究

收稿日期: 2017-08-14; 收到修改稿日期: 2017-09-08

基金项目: 国家自然科学基金(61475127, 61575163, 61674123, 61775184)、重庆市自然科学基金(CSTC2016jcyjA0082)、中央高校专项业务费(XDJK2017B012)

作者简介: 李琼(1992—), 女, 硕士研究生, 主要从事光混沌保密通信方面的研究。E-mail: 1157000820@qq.com

导师简介: 夏光琼(1970—), 女, 博士, 教授, 主要从事激光非线性动力学及其应用方面的研究。

E-mail: gqxia@swu.edu.cn

* 通信联系人。E-mail: zmwu@swu.edu.cn

热点^[2-19]。2005年,Argyris等^[10]基于SLs所产生的混沌载波信号,在希腊雅典城域网中成功实现了1 Gbit/s的信息在120 km光纤信道的单向混沌保密传输,且其误码率仅为 10^{-7} 。随后基于光子集成激光器混沌光源,于2010年成功实现了2.5 Gbit/s信息在100 km光纤信道的保密通信,经过前向纠错处理后其误码率达 10^{-12} ^[11]。尽管上述研究已经证实了单向混沌保密通信的可行性,然而,双向甚至多向混沌保密通信始终是该领域发展的必然趋势。

近年来,基于SLs的双向混沌保密通信已经成为研究热点^[12-19]。目前研究的双向保密通信系统的结构主要包括两类。第1类是基于2个互耦SLs之间的混沌同步实现信息的双向传输^[12-15]。如Klein等^[12]实验和理论分析了2个互耦SLs之间的同步性能,并初步实现了2个激光器之间信息的双向传输;Zhang等^[13]利用极不对称的互耦合激光器结构理论上验证了信息双向传输的可能性。第2类是用1个公共的混沌光源(或者噪声)驱动2个响应激光器(RLs),从而使2个RLs之间达到混沌等时同步进而实现2个RLs之间信息的双向传输^[16-20]。本课题组于2013年在实验上成功实现了误码率低于 10^{-4} 的2个2.5 Gbit/s信息在10 km光纤的双向混沌保密传输^[16]。尽管上述成果已经大大推动了基于SLs的双向混沌保密通信的发展,但这些系统中使用的混沌信号通常还存在明显的由光反馈引入的时延特征(TDS)。已有研究报道,窃密者可通过自相关函数^[21-22]、互信息^[21-22]和排列熵^[23-25]等方法,利用混沌信号中的TDS重构系统,严重威胁通信系统的安全性^[26-27]。对于第2类结构,驱动激光器(DL)与RLs输出之间的关联性应该尽可能低,以防止窃密者通过对两者进行比较而将信息提取出来^[18-19]。因此,混沌载波信号TDS的抑制和DL与RLs输出之间较低的关联性均能有效增强第2类双向混沌保密通信系统的安全性。

本文利用一个带光反馈的注入激光器(IL)产生的混沌信号双路径注入到DL中以产生低TDS的宽带混沌信号,然后将该混沌信号注入到2个独立的RLs中以进一步抑制混沌信号的TDS和提高混沌信号的带宽,通过选择适合的参数,使2个RLs获得高质量混沌同步的同时,DL和RLs之间的关联性较小。构建了一种安全性增强的双向长距离混

沌保密通信系统方案,并对该系统的高质量混沌信号的产生、同步性能、双向通信性能、安全性能以及光纤信道对信息传输的影响等进行了相关研究。

2 系统结构

安全性增强的双向长距离混沌保密通信系统的结构示意图如图1所示。与之前提出的系统^[19]有所不同,采用带光反馈的IL输出的混沌信号通过2条不同的延时路径单向注入到DL中以获得高质量混沌载波,这种简单的低成本技术能在更大的参数范围内获得复杂度增强的宽带混沌信号^[28],且其混沌信号的TDS也能在更大的参数范围内得到更好的抑制^[25]。从DL输出的混沌信号通过一个5:5的光纤耦合器(FC3)分成相等的2个部分,其中一部分通过偏振控制器(PC1)、光纤(F1)、光放大器(EDFA2)单向注入到RL1,另一部分经光纤分支F2后单向注入到RL2。当2个RLs的内部参数一致,且传输光纤的性能参数也一样时,RL1和RL2将受到完全一致的混沌信号驱动,从而使系统具有很好的对称性;在适当的驱动注入条件下,即使经过几十千米光纤链路的传输后,RL1和RL2之间也能达到高质量的等时混沌同步。基于该混沌同步,2个RLs之间能实现双向长距离混沌保密通信。如图1所示,从RL1输出的混沌信号经FC4分成2个部分,其中一个部分作为传输信息 m_1 的混沌载波,传输信息 m_1 经混沌调制方式与该混沌载波加载在一起经光纤链路F3、光环形器(OC2)、EDFA8后注入到光电探测器(PD3)中。从RL2输出的混沌信号同样经FC5后被分成2个部分,其中一部分经光纤延迟线(DF2)、EDFA9后注入到PD4中。因RL1和RL2输出的混沌信号能实现高质量的混沌同步,因而将PD3和PD4输出的信号进行一个“减”操作即可在RL2端恢复出RL1传输的信息 m_1 。同理,将PD1和PD2输出的信号作一个“减”操作也能在RL1端成功恢复出RL2传输的信息 m_2 。

3 理论模型

系统中4个激光器的动力学行为可以用如下包含光反馈或光注入的Long-Kobayashi(L-K)扩展模型来描述^[19,28]:

$$\frac{dE_1}{dt} = \frac{1}{2}(1 + j\alpha) \left(G_1 - \frac{1}{\tau_p} \right) E_1 + k_f E_1(t - \tau_f) \exp(-j\omega_1 \tau_f) + \sqrt{2\chi N_1} \xi_1(t), \quad (1)$$

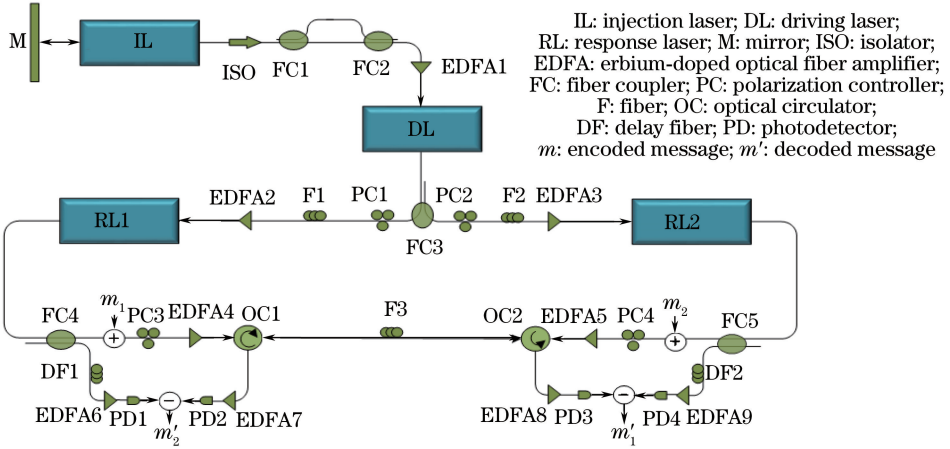


图 1 安全性增强的双向长距离混沌保密通信系统的结构示意图
Fig. 1 Schematic diagram for security-enhanced long-distance bidirectional chaos communication system

$$\frac{dE_D}{dt} = \frac{1}{2}(1 + j\alpha) \left(G_D - \frac{1}{\tau_p} \right) E_D + k_{in1} E_1(t - \tau_1) \exp(-j\omega_1 \tau_1) \exp(j\Delta\omega_{ID}t) + k_{in2} E_1(t - \tau_2) \exp(-j\omega_1 \tau_2) \exp(j\Delta\omega_{ID}t) + \sqrt{2\chi N_D} \xi_D(t), \quad (2)$$

$$\frac{dE_{R1,R2}}{dt} = \frac{1}{2}(1 + j\alpha) \left(G_{R1,R2} - \frac{1}{\tau_p} \right) E_{R1,R2} + k_{in} E_D(t - \tau) \exp(-j\omega_D \tau) \exp(j\Delta\omega_{DR}t) + \sqrt{2\chi N_{R1,R2}} \xi_{R1,R2}(t), \quad (3)$$

$$\frac{dN_{I,D,R1,R2}}{dt} = \frac{I_{I,D,R1,R2}}{q} - \frac{N_{I,D,R1,R2}}{\tau_e} - G_{I,D,R1,R2} |E_{I,D,R1,R2}(t)|^2, \quad (4)$$

式中下标 I、D、R1 和 R2 分别表示 IL、DL、RL1 和 RL2, E 为光信号的慢变场振幅, N 为载流子数, α 为线宽增强因子, I 为偏置电流, q 为单位电荷, τ_p 与 τ_e 分别为光子寿命和载流子寿命, ω 为激射角频率, $\Delta\omega_{ID} = \omega_1 - \omega_D$ 表示 IL 和 DL 之间的角频率失谐, $\Delta\omega_{DR} = \omega_D - \omega_{R1,R2}$ 表示 DL 与 2 个 RLs 之间的角频率失谐, τ_1 为 IL 的反馈延迟时间, k_f 为 IL 的反馈强度, τ_1 和 τ_2 分别为 IL 到 DL2 路径的注入延时, k_{in1} 和 k_{in2} 分别对应这 2 条路径的注入强度, τ 为 DL 到 RLs 的注入延时, k_{in} 为对应的注入强度。 $G = g(N - N_0)/(1 + \epsilon |E|^2)$, g 为微分增益系数, ϵ 为增益饱和因子, N_0 为透明载流子数, χ 为自发辐射率, ξ 为高斯白噪声。

混沌光信号在光纤中传输可以用以下非线性薛定谔方程来描述^[29]:

$$j \frac{\partial E}{\partial z} = -\frac{j}{2} l_F E + \frac{1}{2} \beta_2 \frac{\partial^2 E}{\partial T^2} - \gamma_F |E|^2 E, \quad (5)$$

式中 l_F 为光纤损耗常数, β_2 为光纤的二阶色散系数, γ_F 为光纤的非线性系数, z 为传输距离, T 表示以信号脉冲群速度 v_g 运动的参考系中的时间变量 ($T = t - z/v_g$)。

2 个混沌信号之间的关联程度可以用关联函数 C 来描述, 其表达式为

$$C_{i,j} = \frac{\langle [E_i^2(t) - \langle E_i^2(t) \rangle][E_j^2(t + \Delta t) - \langle E_j^2(t) \rangle] \rangle}{\{ \langle [E_i^2(t) - \langle E_i^2(t) \rangle]^2 \rangle \langle [E_j^2(t + \Delta t) - \langle E_j^2(t) \rangle]^2 \rangle \}^{1/2}}, \quad (6)$$

式中下标 i, j 分别表示 2 个混沌信号 (如果 $i = j$, 那么 C 表示自相关函数, 在本文中被用来分析混沌时间序列的 TDS; 如果 $i \neq j$, 那么 C 代表互相关函数, 它被用来评估 2 个混沌信号之间的同步性能); $|E|^2$ 为激光器的输出场强度, Δt 为时间漂移, $\langle \cdot \rangle$ 为时间平均值。 $|C|$ 的取值范围为 $[0, 1]$, $|C|$ 值越大表示 2 个信号间的同步性能越好, 当 $|C| = 1$ 时, 2 个混沌信号达到完全同步。

系统的通信质量可以用 Q 因子来评估, 其定义如下:

$$Q = \frac{\langle P_1 \rangle - \langle P_0 \rangle}{\sigma_1 + \sigma_0}, \quad (7)$$

式中 $\langle P_1 \rangle$ 和 $\langle P_0 \rangle$ 分别表示比特“1”和比特“0”的平均功率, 而 σ_1 和 σ_0 分别表示比特“1”和比特“0”的标准差。 Q 因子越高表示通信质量越好。

4 结果讨论

基于上述系统架构和理论模型,利用四阶龙格-库塔法对该系统的性能进行相关数值仿真。计算过程中除特别说明外,假定各激光器除频率外的其他内部参数相同,具体取值如下^[19,25]: $\alpha = 3, \epsilon = 1 \times 10^{-7}, g = 1.5 \times 10^4 \text{ s}^{-1}, \tau_p = 2 \text{ ps}, \tau_n = 2 \text{ ns}, \tau_{in} = 1 \text{ ps}, q = 1.602 \times 10^{-19} \text{ C}, N_0 = 1.5 \times 10^8, \chi = 1.1 \times 10^3 \text{ s}^{-1}, \tau_f = 3 \text{ ns}, k_f = 11 \text{ ns}^{-1}, \tau_1 = 3 \text{ ns}, \tau_2 = 4 \text{ ns}, I_1 = 22 \text{ mA}, I_{D,R} = 29 \text{ mA}, \omega_D = 1.219 \times 10^{15} \text{ rad/s}$ (对应的激光器中心波长为 1550 nm)。

4.1 低 TDS 的宽带混沌信号产生

低 TDS 的宽带混沌载波信号是实现基于外腔 SLs 的高速混沌保密通信系统的前提。下面用 σ 来表示 TDS 抑制的效果,考虑到反馈延时 τ_f 为 3 ns,因此 σ 用自相关函数在 $\Delta t \in [2.5 \text{ ns}, 3.5 \text{ ns}]$ 内的最大值来表示, σ 越小代表 TDS 抑制得越好;

混沌信号带宽 W 用功率谱范围内总能量的 80% 所对应的频率范围来表示^[30-31]。图 2(a)和(b)给出了 DL 输出混沌信号的 σ_D 和 W_D 在注入强度 k_{in1} 和频率失谐 $\Delta f_{ID} = \Delta\omega_{ID}/2\pi$ 构成的参数空间中的演化,其中 2 条路径的光注入强度一致。图 2(a)中白色虚线代表 $\sigma_D = 0.1$ 的情况。从图中可以看出,一个 $\sigma_D < 0.1$ 的区域在 $\Delta f_{ID} = 0 \text{ GHz}$ 周围近似呈现一个类“V”形分布,代表这个区域的 TDS 抑制得较好。图 2(b)中白色虚线代表 $W_D = 25 \text{ GHz}$ 的情况。从图中可以看出,系统的非对称注入锁定导致 DL 的混沌信号带宽在 k_{in1} 和 Δf_{ID} 参数空间中呈现出非对称的分布,在一定的失谐频率和注入强度下 DL 可获得带宽大于 25 GHz 的宽带混沌信号,且正频率失谐整体上更有利于混沌信号带宽的增强。由此可见,双路径混沌光注入下 DL 可在适当的参数条件下获得低 TDS 的宽带混沌信号。

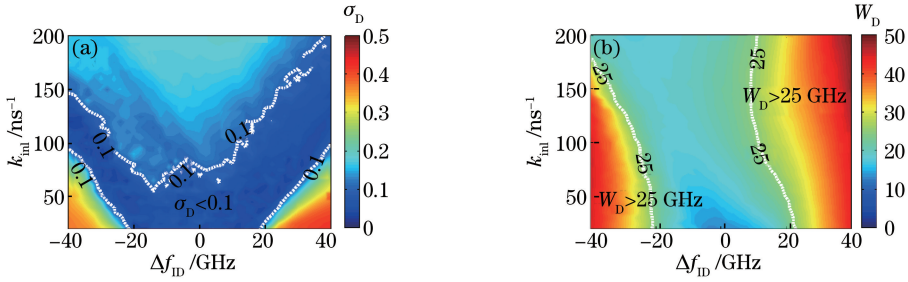


图 2 DL 输出混沌的 (a) σ_D 和 (b) W_D 在频率失谐 Δf_{ID} 和注入强度 k_{in1} 构成的参数空间中的演化图

Fig. 2 Evolution maps of (a) σ_D and (b) W_D of the chaos outputs from DL in the parameter space of frequency detuning Δf_{ID} and injection strength k_{in1}

基于前面的分析,将 $k_{in1} = k_{in2} = 60 \text{ ns}^{-1}$ 、 $\Delta f_{ID} = 20 \text{ GHz}$ 时 DL 输出的混沌信号注入到 2 个相距 20 km 且相互独立的 RLs,并讨论了注入强度 k_{in} 和频率失谐 $\Delta f_{DR} = \Delta\omega_{DR}/2\pi$ 对 RLs 输出混沌特性的影响。考虑到 2 个 RLs 相对 DL 是对称的

结构,因此只需讨论 RL1 混沌信号输出的特性。同时,仅考虑光纤链路 F1 和 F2 均为色散位移光纤的情况,其参数取值为^[6]: $\beta_2 = 1 \text{ ps}^2/\text{km}, \gamma_F = 1.5 \text{ W}^{-1}/\text{km}$ 。图 3(a)和(b)给出了光纤链路 F1 和 F2 均为 10 km 时 RL1 混沌输出的 σ_{R1} 和 W_{R1} 在

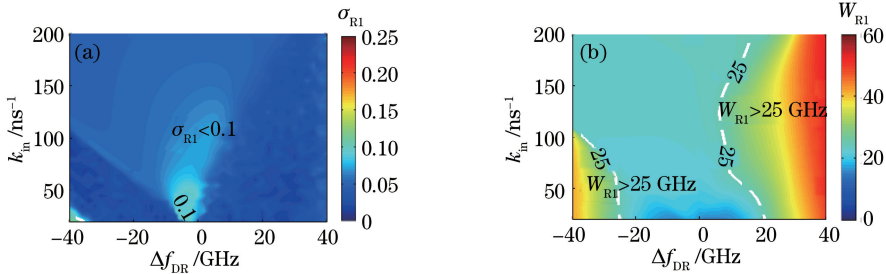


图 3 光纤链路 F1 和 F2 为 10 km 时,RL1 输出混沌信号的 (a) σ_{R1} 和 (b) W_{R1} 在频率失谐 Δf_{DR} 和注入强度 k_{in} 构成的参数空间中的演化图

Fig. 3 Evolution maps of (a) σ_{R1} and (b) W_{R1} of the chaos outputs from RL1 in the parameter space of frequency detuning Δf_{DR} and injection strength k_{in} , where the lengths of fiber links F1 and F2 are also 10 km

k_{in} 和 Δf_{DR} 构成的参数空间中的演化,其中,图 3 (a)中白色虚线代表 TDS 峰值为 0.1 的情况,图 3 (b)中白色虚线代表混沌信号带宽为 25 GHz 的情况。从图 3 可以看出,与 DL 产生的混沌信号相比,RL1 输出混沌信号的 TDS 被进一步抑制,且其带宽被进一步提高,激光器在更大的参数范围内获得了低 TDS 的宽带混沌信号。

4.2 混沌同步

图 4 给出了 RL1 和 RL2 之间相距 20 km,光纤链路 F1 和 F2 均为 10 km 时,RL1 和 RL2 输出混沌信号之间最大的互相关系数 $C_{max_R1,R2}$ 和 DL 与 RL1 输出混沌信号之间最大互相关系数 $C_{max_D,R1}$ 在参数空间 Δf_{DR} 和 k_{in} 中的演化图。其中,光纤链路 F1 和 F2 的光纤参数与图 3 一致,图 4(a)中白色虚线代表 RL1 和 RL2 同步系数为 0.9 的情况,图 4

(b)中白色虚线和红色虚线分别代表 DL 和 RL1 互相关系数为 0.5 和 0.1 的情况。可以看出,在正频率失谐的较大范围内,2 个 RLs 之间可以达到高质量的混沌同步,且 DL 与 RLs 之间的互相关系数在 0.5 以下,甚至在部分区域可达到 0.1 以下,DL 与 RLs 之间如此低的关联性能可在很大程度上提高系统通信的安全性^[18-19]。为了进一步探索传输距离对系统同步性能的影响,图 5 给出了当 F1 和 F2 的长度均为 50 km 时,RL1 和 RL2 混沌信号输出之间最大的互相关系数 $C_{max_R1,R2}$ 和 DL 与 RL1 混沌信号输出之间最大互相关系数 $C_{max_D,R1}$ 在参数空间 Δf_{DR} 和 k_{in} 中的演化图。综合比较图 4 和图 5 可以看出,随着传输距离的增加, $C_{max_R1,R2} < 0.9$ 的区域明显增大,且 $C_{max_D,R1} < 0.5$ 的区域也有进一步扩大的趋势。

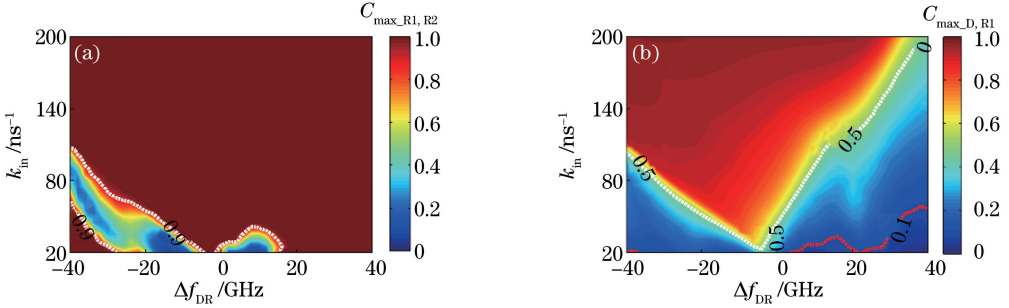


图 4 光纤链路 F1 和 F2 为 10 km 时,(a) RL1 与 RL2 和(b) DL 与 RL1 混沌输出之间最大互相关系数在频率失谐 Δf_{DR} 和注入强度 k_{in} 构成的参数空间中的演化图

Fig. 4 Evolution maps of maximal cross-correlation coefficients between two lasers for (a) RL1 and RL2 and (b) DL and RL1 in the parameter space of frequency detuning Δf_{DR} and injection strength k_{in} , where the lengths of fiber links F1 and F2 are also 10 km

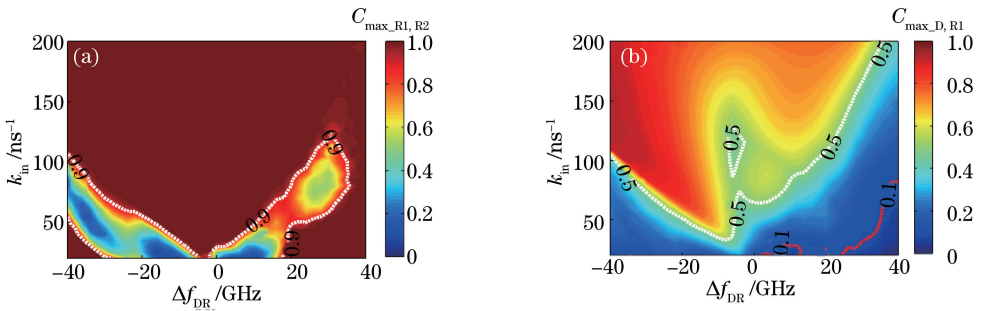


图 5 光纤链路 F1 和 F2 为 50 km 时,(a) RL1 与 RL2 和(b) DL 与 RL1 混沌输出之间最大互相关系数在频率失谐 Δf_{DR} 和注入强度 k_{in} 构成的参数空间中的演化图

Fig. 5 Evolution maps of maximal cross-correlation coefficient between two lasers for (a) RL1 and RL2 and (b) DL and RL1 in the parameter space of frequency detuning Δf_{DR} and injection strength k_{in} , where the lengths of fiber links F1 and F2 are also 50 km

结合图 3 和图 4,在下面的系统同步性能及通信性能分析中选定 $k_{in} = 30 \text{ ns}^{-1}$ 、 $\Delta f_{DR} = 30 \text{ GHz}$ 。为了更加直观地观察在选定注入条件下各激光器输

出混沌的关联性,图 6 给出了 DL、RL1 和 RL2 在上述条件下任意 2 个激光器输出的(a)时间序列、(b)功率谱及(c)对应的互相关函数。从图 6 中可以看

出,RLs 的输出功率谱较 DL 的输出功率谱更加平坦,其带宽约为 37.8 GHz,这为该系统实现高速混沌通信提供了可能。同时,RL1 和 RL2 的同步系数

非常接近 1,而 DL 与 RL1 之间的同步系数仅仅为 0.08 左右,这为系统通信安全性的增强提供有利的保障。

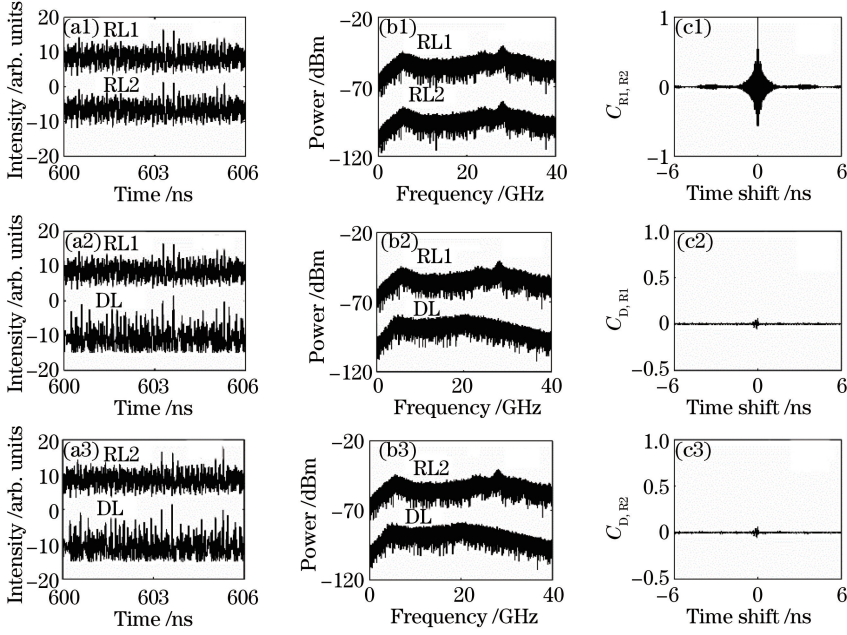


图 6 光纤链路 F1 和 F2 均为 10 km 时,DL、RL1 和 RL2 3 个激光器中任意 2 个激光器输出混沌信号的时间序列 (a1)-(a3)、功率谱 (b1)-(b3) 和对应的互相关函数 (c1)-(c3)

Fig. 6 (a1)-(a3) Time series, (b1)-(b3) power spectra and (c1)-(c3) corresponding cross-correlation coefficients for arbitrary two chaotic outputs from DL, RL1 and RL2, where the lengths of fiber links F1 and F2 are also 10 km

考虑到实际应用中很难获得参数完全一致的激光器和光纤信道,因此,有必要研究 2 个 RLs 之间的内部参数失配及光纤链路 F1 和 F2 之间参数失配对系统同步性能的影响。为了方便,仅改变 RL1 的 3 个典型内部参数 (g 、 α 、 ϵ) 及光纤 F1 的 3 个参数 (β_2 、 γ_F 和光纤长度 L)。相关的参数失配定义为

$$\Delta\epsilon = (\epsilon_{R1} - \epsilon_{R2}) / \epsilon_{R2}, \Delta\alpha = (\alpha_{R1} - \alpha_{R2}) / \alpha_{R2}, \Delta g = (g_R - g_{R2}) / g_{R2}, \Delta\beta_2 = (\beta_{2,F2} - \beta_{2,F1}) / \beta_{2,F1}, \Delta\gamma_F = (\gamma_{F2} - \gamma_{F1}) / \gamma_{F1}, \Delta L = (L_{F2} - L_{F1}) / L_{F1}, \quad (8)$$

图 7(a) 和 (b) 给出了 RL1 和 RL2 之间最大互相关系数以及 DL 与 RL1 之间最大互相关系数随以上 6 个参数失配的变化曲线。从图 7(a) 可以看出,对系统内部参数而言,系统对参数 ϵ 失配有较高的容忍度,在参数失配 $\pm 10\%$ 的范围内, $C_{\max,RL1,RL2}$ 均大于 0.9。而参数 g 、 α 对系统同步性能的影响相对更大,但在一定的参数范围内 2 个 RLs 的同步

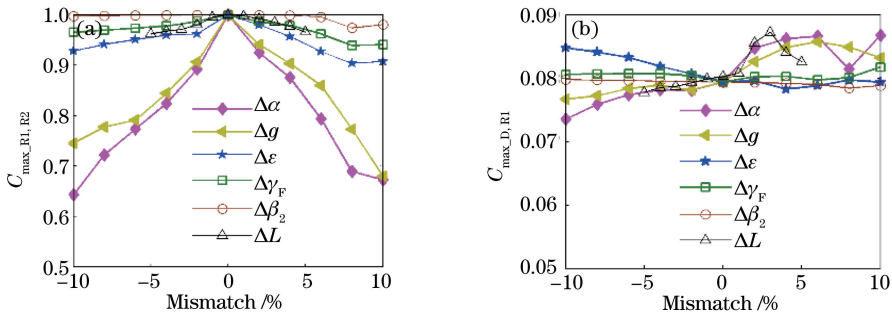


图 7 RL1 与 RL2 之间的最大互相关系数 $C_{\max,RL1,RL2}$ 和 DL 与 RL1 之间的最大互相关系数 $C_{\max,D,RL1}$ 随激光器内部参数及链路 F1 和 F2 光纤参数失配的变化

Fig. 7 Maximal cross-correlation coefficients $C_{\max,RL1,RL2}$ between RL1 and RL2, $C_{\max,D,RL1}$ between DL and RL1 versus internal parameters of lasers and parameter mismatches between F1 and F2

系数仍能保持在 0.8 以上,说明系统对内部参数失配具有一定的容忍性。由图 7(b)可知,在整个 $\pm 10\%$ 的参数失配范围内,DL 与 RLs 之间的最大互相关系数始终保持在 0.1 以下,这对系统通信的安全性非常有利^[18]。对于光纤参数而言, β_2 对系统同步性能的影响较小,在 $\pm 10\%$ 的参数失配范围内, $C_{\max_R1,R2}$ 始终保持大于 0.97;相对于 β_2 , γ_F 失配对系统同步性能的影响更大,但在 $\pm 10\%$ 的参数失配范围内 $C_{\max_R1,R2}$ 也能一直保持在 0.94 以上。上述结果说明在较短距离的传输中,光纤参数失配对系统的同步性能影响极小。当然,随着传输距离的增加,光纤参数失配对系统同步性能的影响将会逐步增大。而对于光纤长度,其失配在 $\pm 5\%$ 的范围内(对应光纤长度差为 ± 500 m), $C_{\max_R1,R2}$ 总是保持在 0.96 以上,说明本系统对光

纤长度失配具有较强的容忍性。

4.3 双向长距离保密通信

图 8 给出 2 个 20 Gbit/s 的信息在色散位移光纤中经不同传输距离后的解码信息及对应的眼图。这里用振幅调制的方式将信息 $m(t)$ 加载到混沌载波中,加载了信息的混沌载波为 $|E^{\text{mod}}(t)| = |E(t)|[1 + \eta m(t)]$,其中 $\eta = 5\%$ 为调制深度。从图 8 中可以看出,随着传输距离的增加,两个相反传输方向的信息解码后的 Q 因子整体呈现逐渐减小的趋势,即系统通信质量随传输距离的增加逐渐降低。然而,在经过 120 km 的光纤传输后,2 个相反方向解码信息的 Q 因子仍然保持在 6 以上(对应的误码率估计小于 10^{-9}),表明加载的信息能得到很好地解调,信息在该系统中可以实现双向长距离通信。

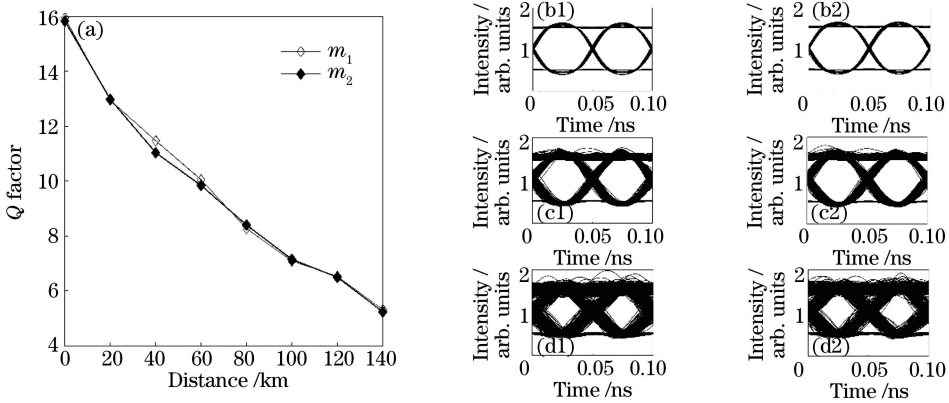


图 8 20 Gbit/s 的信息在不同距离色散位移光纤中双向传输的解码效果。(a)解码信息的 Q 因子随传输距离变化的曲线; (b)-(d)传输距离分别为 20,80,120 km 时 2 个相反方向解码信息的眼图

Fig. 8 Q factors of 20 Gbit/s decoded messages for different bidirectional transmission distances in dispersion-shifted fibers. (a) Q factors of decoded messages versus the transmission distance;

(b)-(d) eye diagrams of decoded messages for transmission distances of 20, 80, 120 km along 2 opposite directions

长距离色散位移光纤信道的使用无疑会极大地增加系统成本,几个 Gbit/s 的通信速率已能满足目前的保密通信的要求。因此,将上述系统中的色散光纤替换成普通的单模光纤(参数为^[19]: $\beta_2 = -20 \text{ ps}^2/\text{km}$, $\gamma_F = 1.5 \text{ W}^{-1}/\text{km}$),对 1 Gbit/s 的信息在系统中双向通信性能进行分析,所得的结果如图 9 所示。从图 9(a)可以看出,随着传输距离的增加,解调信息的 Q 因子整体上依然呈现逐渐减小的趋势。当传输距离小于 80 km 时,Q 因子随传输距离的变化相对缓慢;当传输距离大于 80 km 后,Q 因子随着传输距离的增大迅速减小。传输距离达到 140 km 时,Q 因子也能保持在 8 以上。说明该基于普通单模光纤的双向混沌通信系统具有较好的通信性能,对于 1 Gbit/s 信息可实现远距离的双向混沌

保密通信。

最后,从该系统可能受到的几种攻击方式来分析系统通信的安全性。由于系统采用双路径混沌光注入方式使 2 个 RLs 获得了低 TDS 的高复杂度混沌信号,窃密者很难通过直接窃取光纤链路中混沌信号利用相空间重构方法窃取通信系统中传输的信息,在一定程度上增强了系统通信的安全性。就具体的窃听攻击方式而言,分为 3 类。1) 假如窃听者试图利用从光纤链路 F3 和光纤链路 F1 或 F2 窃取信号来恢复信息。由于本系统采用的参数可使 RL1 和 RL2 之间获得高质量的混沌同步,而 DL 与 RL1 或 RL2 之间的相关系数甚至可以降到 0.1 以下,如图 4 和图 7 所示,因此这种窃听方式实际上是无效的。2) 假如窃听者试图窃取在光纤链路 F3 中

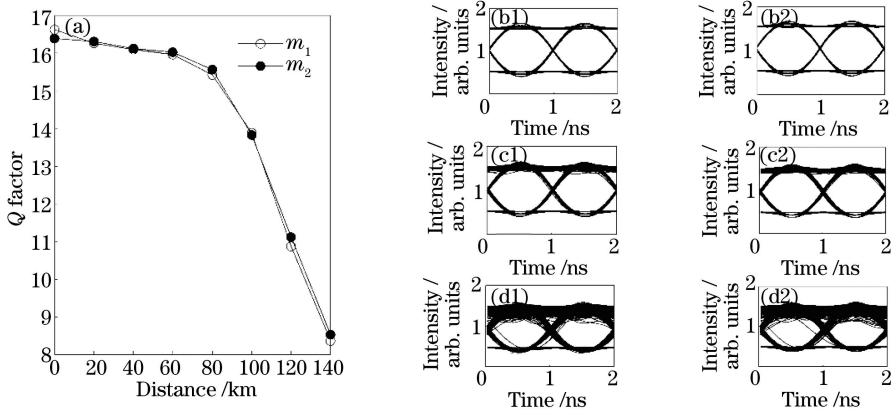


图 9 Gbit/s 的信息在不同距离普通单模光纤中双向传输的解码效果。(a)解码信息的 Q 因子随传输距离变化的曲线；(b)-(d)传输距离分别为 20,80,120 km 时 2 个相反方向解码信息的眼图

Fig. 9 Q factors of 1 Gbit/s decoded messages for different bidirectional transmission distances in dispersion-shifted fiber. (a) Q factors of decoded messages versus the transmission distance,

(b)-(d) eye diagrams of decoded message for transmission distances of 20 , 80 , 120 km along 2 opposite directions

双向传输的信息,通过“减”操作来窃取通信双方传输的信息。这种方式仅仅能获得通信双方传输信息的差值,在不知道通信双方加载的原始信息的情况下,窃听者并不能最终恢复真正传输的信息。3) 假如窃听者试图通过直接窃取光纤链路 F3 中某一方向的信号来获取信息。由于传输的信息幅值很小,能很好地隐藏在混沌载波中,因此窃听者只能先放大信号然后再通过驱动-响应同步方式来恢复信息。然而,放大过程中必然会引入更多噪声的干扰,从而导致这种窃听方式很难实现。此外,窃听者在窃听过程中一旦改变了系统的注入参数,将导致系统同步系数的变化,因此也可以通过监控系统同步系数的变化来确保系统通信的安全性。一旦通信过程中发现系统的同步系数发生抖动,可以立即停止通信来防止信息被窃取。基于此,提出的双向长距离混沌保密通信方案能在很大程度上确保系统通信的安全性。

5 结 论

提出一种安全性增强的双向长距离混沌保密通信系统,研究了该系统的低 TDS 宽带混沌信号的产生、同步性能、通信性能及系统的安全性等方面的性能。结果表明:利用光反馈 IL 产生的混沌信号通过双路径注入到 DL 可获得低 TDS 的宽带混沌信号。将 DL 输出的混沌信号注入到 RLs 中,在选择适当的注入强度和频率失谐后,RLs 产生的混沌信号的 TDS 可被进一步抑制,其带宽也可被进一步提高,且 2 个 RLs 能实现高质量的等时混沌同步,而 DL 与 RLs 的相关性较低。基于该混沌同步,2 个 RLs

之间能实现信息的双向远距离保密传输。采用色散位移光纤作为信道,20 Gbit/s 的信息在传输 120 km 后,解码信息的 Q 因子可保持在 6 以上;而采用普通单模光纤作为信道,1 Gbit/s 的信息在传输 140 km 后,解码信息的 Q 因子可保持在 8 以上。该研究结果可为基于 SLs 的混沌保密通信的实际应用提供一定的借鉴和参考。

参 考 文 献

- [1] Pecora L M, Carroll T L. Synchronization in chaotic systems[J]. Physical Review Letters, 1996, 64(8): 142-145.
- [2] Yan S L. Theoretical studies on chaotic semiconductor laser dual-directional secure communication system [J]. Chinese Journal of Lasers, 2005, 32(11): 1503-1509.
颜森林. 半导体激光器混沌双向保密通信系统理论研究[J]. 中国激光, 2005, 32(11): 1503-1509.
- [3] Xue P P, Zhang J Z, Yang L Z, et al. Chaotic synchronization and optimization of semiconductor ring lasers [J]. Acta Optica Sinica, 2015, 35(4): 0414002.
薛萍萍, 张建忠, 杨玲珍, 等. 半导体环形激光器的混沌同步及优化[J]. 光学学报, 2015, 35(4): 0414002.
- [4] Liu J M, Chen H F, Tang S. Synchronized chaotic optical communications at high bit rates [J]. IEEE Journal of Quantum Electronics, 2002, 38(9): 1184-1196.
- [5] Pan X M, Wu Z M, Tang X, et al. Chaos synchronization and communication in mesh network based on mutually coupled semiconductor lasers [J].

- Chinese Journal of Lasers, 2013, 40(12): 1202005.
潘兴茂, 吴正茂, 唐曦, 等. 基于互耦半导体激光器的混沌网状网络的同步与通信[J]. 中国激光, 2013, 40(12): 1202005.
- [6] Bogris A, Kanakidis D, Argyris A, *et al.* Performance characterization of a closed-loop chaotic communication system including fiber transmission in dispersion shifted fibers [J]. IEEE Journal of Quantum Electronics, 2004, 40(9): 1326-1336.
- [7] Xue C P, Jiang N, Lü Y X, *et al.* Security-enhanced chaos communication with time-delay signature suppression and phase encryption[J]. Optics Letters, 2016, 41(16): 3690-3693.
- [8] Hu H P, Chen X F, Su W, *et al.* Multi-coupled chaos synchronization and communication based on optoelectronic feedback delay[J]. Acta Optica Sinica, 2014, 34(4): 0406006.
胡汉平, 陈笑风, 苏威, 等. 基于光电反馈延迟的多点耦合混沌同步和通信[J]. 光学学报, 2014, 34(4): 0406006.
- [9] Sciamanna M, Shore K A. Physics and applications of laser diode chaos[J]. Nature Photonics, 2015, 9(3): 151-162.
- [10] Argyris A, Syvridis D, Larger L, *et al.* Chaos-based communications at high bit rates using commercial fibre-optic links[J]. Nature, 2005, 438(7066): 343-346.
- [11] Argyris A, Grivas E, Hamacher M, *et al.* Chaos-on-a-chip secures data transmission in optical fiber links [J]. Optics Express, 2010, 18(5): 5188-5198.
- [12] Klein E, Gross N, Kopelowitz E, *et al.* Public-channel cryptography based on mutual chaos pass filters[J]. Physical Review E, 2006, 74(4): 046201.
- [13] Zhang W L, Pan W, Luo B, *et al.* Chaos synchronization communication using extremely unsymmetrical bidirectional injections [J]. Optics Letters, 2008, 33(3): 237-239.
- [14] Vicente R, Mirasso C R, Fischer I. Simultaneous bidirectional message transmission in a chaos-based communication scheme[J]. Optics Letters, 2007, 32(4): 403-405.
- [15] Deng T, Xia G Q, Cao L P, *et al.* Bidirectional chaos synchronization and communication in semiconductor lasers with optoelectronic feedback [J]. Optics Communications, 2009, 282(11): 2243-2249.
- [16] Wu J G, Wu Z M, Tang X, *et al.* Experimental demonstration of LD-based bidirectional fiber-optic chaos communication [J]. IEEE Photonics Technology Letters, 2013, 25(6): 587-590.
- [17] Jiang N, Xue C P, Lü Y X, *et al.* Physically enhanced secure wavelength division multiplexing chaos communication using multimode semiconductor lasers[J]. Nonlinear Dynamics, 2016, 86(3): 1937-1949.
- [18] Li P, Wu J G, Wu Z M, *et al.* Bidirectional chaos communication between two outer semiconductor lasers coupled mutually with a central semiconductor laser[J]. Optics Express, 2011, 19(24): 23921-23931.
- [19] Wu J G, Wu Z M, Liu Y R, *et al.* Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system [J]. Journal Lightwave Technology, 2013, 31(3): 461-467.
- [20] Yamamoto T, Oowada I, Yip H, *et al.* Common-chaotic-signal induced synchronization in semiconductor lasers[J]. Optics Express, 2007, 15(7): 3974-3980.
- [21] Rontani D, Locquet A, Sciamanna M, *et al.* Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback[J]. Optics Letters, 2007, 32(20): 2960-2962.
- [22] Nguimdo R M, Soriano M C, Colet P. Role of the phase in the identification of delay time in semiconductor lasers with optical feedback [J]. Optics Letters, 2011, 36(22): 4332-4334.
- [23] Bandt C, Pompe B. Permutation entropy: A natural complexity measure for time series [J]. Physical Review Letters, 2002, 88(17): 174102.
- [24] Zhong Z Q, Wu Z M, Wu J G, *et al.* Time-delay signature suppression of polarization-resolved chaos outputs from two mutually coupled VCSELs [J]. IEEE Photonics Journal, 2013, 5(2): 1500409.
- [25] Xiang S Y, Pan W, Wen A J, *et al.* Conceal time delay signature of chaos in semiconductor lasers with dual-path injection [J]. IEEE Photonics Technology Letters, 2013, 25(14): 1398-1401.
- [26] Voss H, Kurths J. Reconstruction of nonlinear time-delayed feedback models from optical data[J]. Chaos Solitons & Fractals, 1999, 10(4): 805-809.
- [27] Rontani D, Locquet A, Sciamanna M, *et al.* Time-delay identification in a chaotic semiconductor laser with optical feedback: a dynamical point of view[J]. IEEE Journal of Quantum Electronics, 2009, 45(7): 879-1891.
- [28] Xiang S Y, Pan W, Li N Q, *et al.* Randomness-enhanced chaotic source with dual-path injection from a single master laser[J]. IEEE Photonics Technology Letters, 2012, 24(19): 1753-1756.
- [29] Agrawal G P. Nonlinear fiber optics[M]. San Diego, CA: Academic, 2012.

- [30] Lin F Y, Liu J M. Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback [J]. Optics Communications, 2003, 221(1/2/3): 173-180.
- [31] Wang A B, Wang Y C, He H C. Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback [J]. IEEE Photonics Technology Letters, 2008, 20(19): 1633-1635.