硬件加密的扩频通信方案*

萧宝瑾[1)] 仝海丽[1)] 张建忠[2)] 张朝霞[2)] 王云才[2)3)†]

1)(太原理工大学信息与通信工程系,太原 030024)

2)(太原理工大学物理与光电工程系,太原 030024)

3)(山西大学量子光学与光量子器件国家重点实验室,太原 030006)

(2010 年 9 月 30 日收到;2011 年 2 月 11 日收到修改稿)

提出了一个利用混沌激光源产生 1 Gbit/s 的随机序列作为扩频码的方案. 理论分析表明,该随机序列克服了伪随机序列的周期性,在扩大扩频码容量的同时实现了扩频码可变,提高了通信安全性. 利用 Simulink 软件对该扩频系统进行仿真. 结果表明,当信息速率一定时,扩频增益越大,误码率越低,与理论结果相符. 与传统的扩频系统相比,该方案在提高系统抗干扰能力的同时也增强了保密性.

关键词: 扩频通信, 随机序列, 混沌激光源

PACS: 05.45.Vx

1. 引 言

扩频通信(spread spectrum communication)与光纤通信、卫星通信一同被誉为进入信息时代的三大高技术通信方式. 扩频通信是将每个信源码用高速率的随机序列(码片)代替,从而提高通信系统的抗干扰能力. 扩频通信可分为直接序列扩频、跳频、跳时和线性调频等方式. 目前的扩频通信大部分是用伪随机序列作为扩频码,而伪随机序列是由一个 n 级的 m 序列移位寄存器产生的,周期最长为 $2^n - 1$. 理论上已经证明,伪随机序列是可破译的,只要知道 m 序列中任意 $2n$ 位即可确定整个 m 序列[1],因此安全性不高.

在直接扩频通信系统中,扩频码一旦产生就在通信过程中固定不变(固定码直扩),在码片间形成周期性,黑客利用这种码片间的周期平稳性来估计扩频通信中的码片周期和扩频码. 2009 年, Zhong 等[2]已经检测出长伪随机序列的周期. 为提高扩频系统的抗干扰性和安全性,降低通信信号被截获的概率,扩频码应该是变化的. 因此, Wang 等[3]采用混沌映射的方法生成混沌序列,并将其作为扩频码. 理论上,混沌序列的周期无限长,但实际应用时受微处理器字长的限制,混沌序列的周期必定有限,且 0 与 1 的比例不均衡[4]. 此外,采用自编码扩频方法虽然满足了扩频码可变和不可预测的要求,但存在错码传播现象,导致接收方无法正确解调. 若采用真随机数作为扩频码,则可克服以上缺点. 真随机数具有非周期性、不可预测性、不可重复性,是一种相对安全、不易被破解的随机数.

目前,有很多产生真随机数的物理熵源,如电路或电阻中的热噪声[5]、振荡器中的振荡频率[6]、量子力学基本量的随机性[7,8]、电路混沌[9]和生物无规则特性[10]等. 然而,用这些物理熵源产生的随机数,速率都比较低,通常仅为 10 Mbit/s[6,11]. 2007 年,本课题组[12]提出用光反馈半导体激光器产生的宽带混沌激光(CL)作为产生真随机数的物理熵源,构造快速真随机数发生器的方案. 2008 年,日本的 Uchida 等[13,14]基于光反馈半导体激光器,利用两路不相关的 CL 经模数转换、逻辑异或处理后首次实验产生了 1.7 Gbit/s 的真随机数. 2009 年,以色列的 Kanter 研究小组[15]基于光反馈半导体激光器,提出使用 8 位模数转换器对 CL 进行采样,并结合后续差分处理技术可产生出 12.5 Gbit/s 的真随机数. 最近,他们进一步提出利用后续多级差分处理技术理论上可获得码率达 300 Gbit/s 的真随机数[16]. 目前,真随机数的产生速率已超过了 Gbit/s 的量级,同步技术也取得了一定的进展,以色列的 Kanter

* 国家自然科学基金(批准号:60927007, 60872019)和量子光学与光量子器件国家重点实验室基金(批准号:200903)资助的课题.

† 通讯联系人. E-mail: wangyc@tyut.edu.cn

等[17]已经实现了真随机数的同步,因此可以考虑用真随机数作为扩频码.

本文提出了一个利用 CL 产生的随机序列用于扩频通信的方案,并用 Simulink 软件仿真验证了其可行性.

2. 用 CL 源产生随机序列

2.1. CL 随机序列的生成

利用 CL 产生随机序列的系统框图如图 1 所示. 两路 CL 源输出的光信号经过光电探测器后转换为电信号,用比较器将模拟信号转变为数字信号,通过触发器将数字信号变为二进制随机序列[18],用采样时钟来控制随机序列的码率,用异或门进行后续处理以改善随机序列的随机性.

利用无光隔离器的分布反馈(DFB)半导体激光器产生 CL[19]的实验装置如图 2 所示. 实验中采用 WTD 公司生产的 LDM5S752 型半导体激光器(中心波长为 1550 nm,阈值电流 I_{th} 为 22.5 mA). 该激光器输出的光通过光纤反射镜反馈回谐振腔中,反馈光的强度和偏振态分别通过可调谐衰减器和偏振控制器来调节,并用光功率计监控反馈光强度. 当激光器的工作电流为 1.6 I_{th},反馈光的强度为 10% 时,DFB 半导体激光器通过耦合比为 40∶60 (40% 反馈,60% 输出)的耦合器输出的 CL 信号功率为 0.5 mW,通过 2 GHz 的光电探测器将光信号转化为电信号,信号幅值为 45 mV 左右. 再利用 Tektronix 公司生产的 TDS3052 型实时示波器(带宽为 500 MHz,采样率为 5×10^9 s^{-1})对信号进行采样和存储. 为了使生成的 CL 随机序列的随机性更好[15,16],可以采用一系列离线处理手段,如两路异或,一路差分等. 在实验过程中采用的是两路异或的方式,产生了速率为 1 Gbit/s 的随机数,并最终通过了美国国家标准技术研究院公布的 800-22 随机数检测标准.

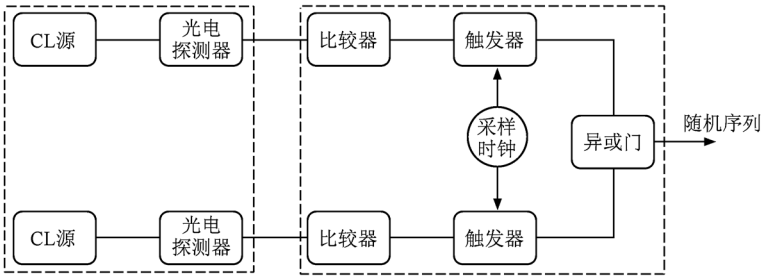

图 1 基于 CL 源产生随机序列的系统框图

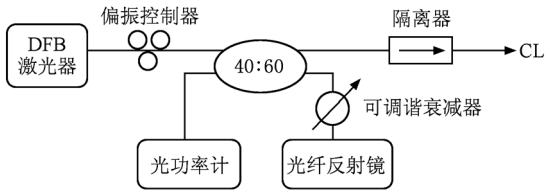

图 2 利用 DFB 激光器产生 CL 信号的装置示意图

2.2. CL 随机序列的特性

自相关函数 $R_{ac}(m)$ 及互相关函数 $R_{cc}(m)$ 反映的是一随机序列自身的相关性以及它与另一随机序列之间的相关性,表达式分别为

$$R_{ac}(m)=\frac{1}{N}\sum_{i=0}^{N-1}x_i x_{i+m}, \qquad (1)$$

$$R_{cc}(m)=\begin{cases}\dfrac{1}{N}\displaystyle\sum_{i=0}^{N-1}x_{1i}x_{2(i+m)} & (m>0),\\ \dfrac{1}{N}\displaystyle\sum_{i=0}^{N-1}x_{1i}x_{2i} & (m=0),\\ \dfrac{1}{N}\displaystyle\sum_{i=0}^{N-1}x_{1(i-m)}x_{2i} & (m<0),\end{cases} \qquad (2)$$

其中 x_1 和 x_2 为两个不同的随机序列, N 为序列长度, m 为延迟位数[4].

自相关系数和互相关系数为自相关函数和互相关函数的归一化表示. 理想情况下,真随机序列的自相关函数应为 δ 函数,互相关函数应为零. m 序列在其自相关图上反映出周期性,如图 3(a)所示;CL 随机序列的自相关函数类似于 δ 函数,如图 3(b)所示. 从图 3(a)可以看出,周期为 15 的 m 序列自相关后每隔 15 位就有一个尖脉冲,呈现出周期

性;从图 3(b)可以看出,随机序列不论多长,它的自相关函数都近似于 δ 函数. 同时,在互相关特性图上,伪随机序列(m 序列)有尖锐的脉冲尖峰,而随机序列的互相关特性相对较好.

在传统的直接扩频码分多址通信系统中,系统容量取决于可用的扩频码数目. 如扩频因子 $N = 1023$ 时,可用的 m 序列只有 60 个,限制了系统的容量. 若利用 CL 源产生的随机序列作为扩频码,可以使系统容量有很大的提高,并且线性复杂度高,保证了通信系统的抗侦破和抗干扰能力.

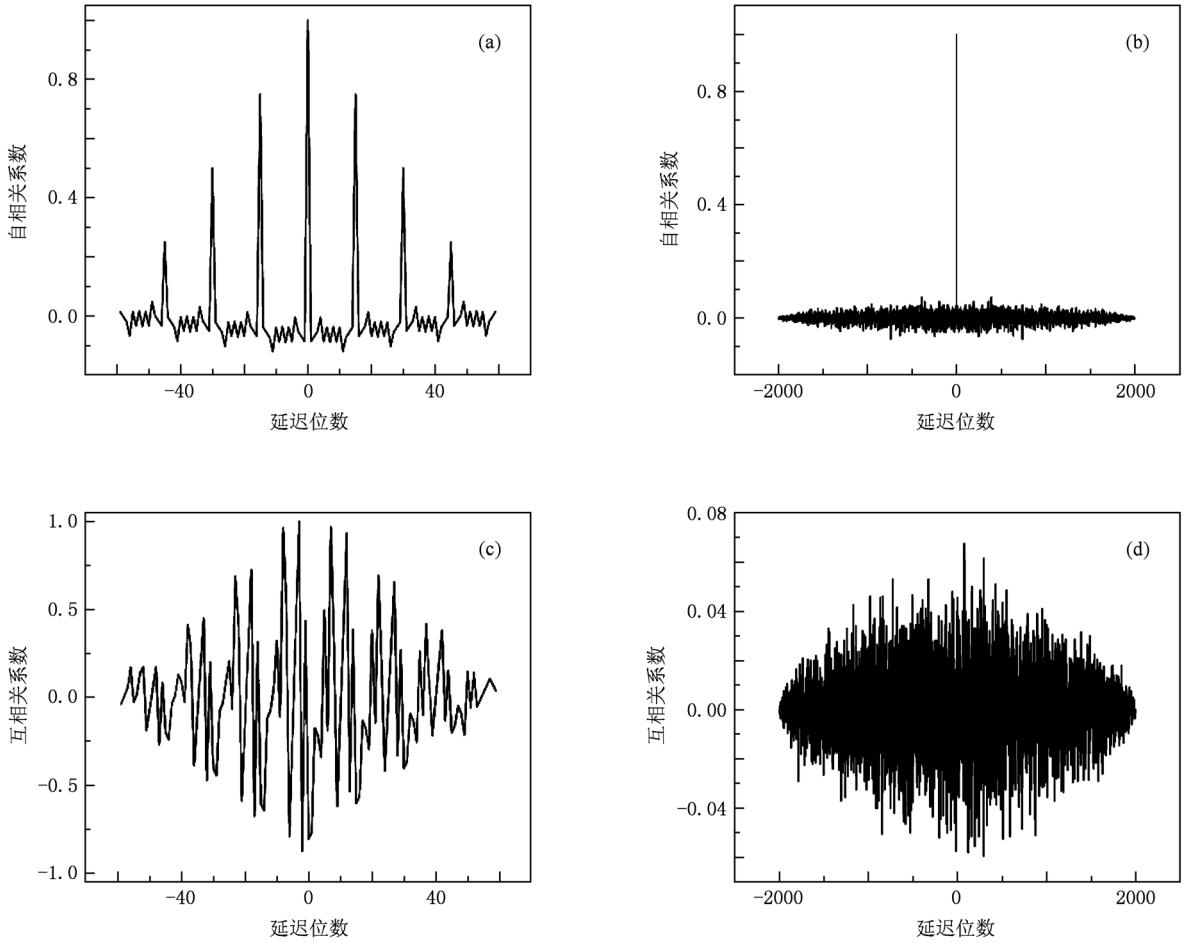

图 3 m 序列和 CL 随机序列的自相关特性和互相关特性 (a)周期为 15 的 m 序列的自相关特性, (b) CL 随机序列的自相关特性, (c)周期为 15 的 m 序列的互相关特性, (d) CL 随机序列的互相关特性

3. 扩频系统方案及仿真

3.1. 扩频系统方案

在发送端,待发送的信息通过信源编码转换为数字信号,与传统的用伪随机序列进行扩频不同的是,本方案是利用 CL 随机序列进行扩频,射频调制后通过天线发射出去. 接收端只要进行与之相反的过程即可恢复出原来的信息.

扩频通信中存在的干扰主要可分为多径干扰和多用户干扰,多径干扰主要与扩频码自身的相关性(自相关性)有关,而多用户干扰主要与扩频码的互相关性有关. 因此,在选择扩频码的过程中,应尽量挑选正交性较好的码作为扩频码,以使其不同码之间的相关性降到最低. 实验发现,CL 随机序列的自相关系数和互相关系数都随着序列长度的增大而减小. 同时,扩频通信系统抗多径干扰和抗多用户干扰的性能可以由扩频码的自相关旁瓣均方值和互相关均方值来表征[4],因此我们只需选取适当长度的随机序列作为扩频码,就可以降低系统的干扰. 另外,自相关旁瓣均方值 $\delta_{ac}^2(m)$ 和互相关均方

值 $\delta^2_{cc}(m)$ 可分别表示为

$$\delta^2_{ac}(m) = \frac{1}{M}\sum_{m=1}^{M}(R_{ac}(m))^2, \quad (3)$$

$$\delta^2_{cc}(m) = \frac{1}{2M+1}\sum_{m=-M}^{M}(R_{cc}(m))^2, \quad (4)$$

其中 M 为相关范围，$R_{ac}(m)$ 和 $R_{cc}(m)$ 分别表示序列的自相关函数和互相关函数.

CL 随机序列的均方值曲线如图 4 所示. 由图 4 可看出，CL 随机序列的自相关旁瓣均方值和互相关均方值都随着序列长度的增加而减小. 当序列长度大于 2000 时，自相关旁瓣均方值和互相关均方值都小于 0.0006. 当序列长度大于 5000 时，序列长度的增大对这两个均方值的改善越来越小，因此可以选取 2000—5000 的 CL 随机序列作为扩频码进行分析.

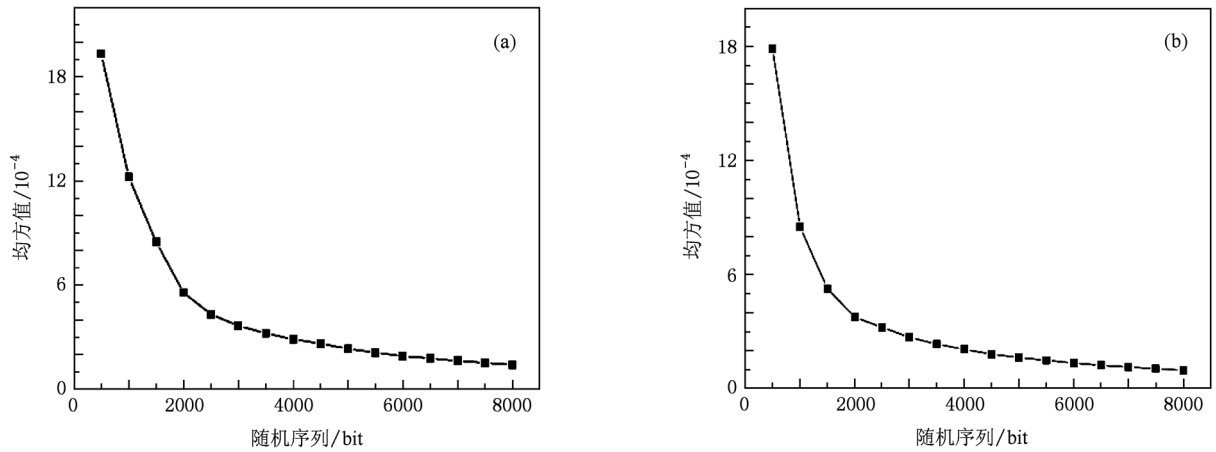

图 4 CL 随机序列的自相关旁瓣均方值和互相关均方值曲线 (a) 自相关旁瓣均方值，(b) 互相关均方值

3.2. 用 Simulink 软件仿真

本文用 Simulink 软件建立了直接扩频通信系统的仿真模型，如图 5 所示.

由信号源产生二进制单极性信息码 A，经极性转换器转换为双极性信号 A'；同时，由 CL 随机序列发生器产生单极性扩频码 P，经极性转换器转换为双极性信号 P'；将 A' 与 P' 相乘进行扩频，然后送入高斯信道. 在接收端，将收到的信号与 P' 相乘进行解扩，经累积器和判决器后得到双极性信号 B'，再经极性转换器转换为单极性信号 B. 将信息码 A 延迟后与收到的信号 B 送到误码分析仪进行误码统计.

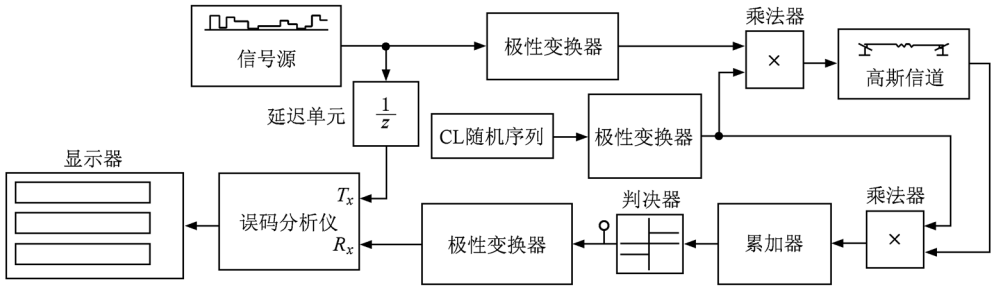

图 5 直接扩频通信系统仿真模型框图

如图 6 所示，扩频增益 G_p 给定后，传输速率为 100 Hz，9.6 kHz 和 2 MHz 时得到的曲线很接近，说明传输速率对误码率的影响不大. 这是因为在仿真过程中，增大传输速率，信道带宽也会相应增大. 从图 6 可以看到：当扩频增益 $G_p = 0$ dB 时，误码率为 0.4623；当扩频增益 $G_p = 10$ dB 时，误码率为 0.3765；当扩频增益 $G_p = 20$ dB 时，误码率为 0.1567. 这说明在信息速率一定时，扩频增益越大，误码率越低. 在信噪比很差 (-20 dB) 的情况下，增大扩频增益可以有效地降低信号的误码率. 与伪随机序列作为扩频码相比，系统抗高斯噪声的能力相当. 同时，该系统用一段随机序列来表示信息码 1，用另一段随机序列的反码来表示信息码 0，这与正交码相比噪声容限增大了一倍.

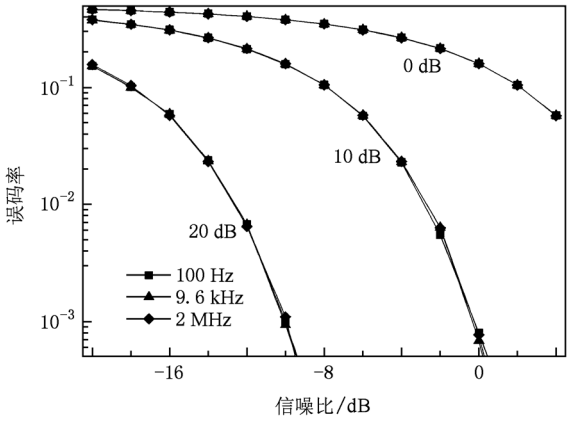

图6 误码率与信噪比、扩频增益的关系

4. 结 论

传统扩频通信系统所用的伪随机序列具有周期性,扩频码容量有限,存在被破译的危险. 本文针对这一问题提出了用 CL 随机序列作为扩频码的方案,并用 Simulink 软件对该扩频通信系统进行了仿真. 仿真结果与理论相符,证实了采用 CL 随机序列作为扩频码的可行性. 与传统扩频通信系统相比,本文所给出的硬件加密扩频通信方案具有易于实现、扩频码容量大、非周期性、保密性强等优势,可用于新一代移动通信、军事、商业等领域.

[1] Kurosawa K, Sato F, Sakata T, Kishimoto W 2000 *IEEE Trans. Inform. Theory* **46** 694

[2] Zhong Z, Zhao X T, Ren G H 2009 *Inform. Technol. J.* **8** 1076

[3] Wang X G, Zhan M, Gong X F, Lai C H, Lai Y C 2005 *Phys. Lett.* A **334** 30

[4] Yu Z B, Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese) [余振标、冯久超 2008 物理学报 **57** 1409]

[5] Petrie C S, Connelly J A 2000 *IEEE Trans. Circuits Syst.* I **47** 615

[6] Bucci M, Germani L, Luzzi R, Trifiletti A, Varanonuovo M 2003 *IEEE Trans. Computers* **52** 403

[7] Liao J, Liang C, Wei Y J, Wu L A, Pan S H 2001 *Acta Phys. Sin.* **50** 467 (in Chinese) [廖 静、梁 创、魏亚军、吴令安、潘少华 2001 物理学报 **50** 467]

[8] Feng M M, Qin X L, Zhou C Y, Xiong L, Ding L E 2003 *Acta Phys. Sin.* **52** 72 (in Chinese) [冯明明、秦小林、周春源、熊利、丁良恩 2003 物理学报 **52** 72]

[9] Huang Z, Zhou T, Bai G Q, Chen H Y 2004 *Chin. J. Semicond.* **25** 333 (in Chinese) [黄 谆、周 涛、白国强、陈弘毅 2004 半导体学报 **25** 333]

[10] Zhou Q, Hu Y, Liao X F 2008 *Acta Phys. Sin.* **57** 5413 (in Chinese) [周 庆、胡 月、廖晓峰 2008 物理学报 **57** 5413]

[11] Dynes J F, Yuan Z L, Sharpe A W, Shields A J 2008 *Appl. Phys. Lett.* **93** 031109

[12] Wang Y C, Tang J H, Zhang M J 2007 *Chinese Patent* ZL200710062140.1 (in Chinese) [王云才、汤君华、张明江 2007 中国发明专利 ZL200710062140.1]

[13] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Owada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K, Davis P 2008 *Nat. Photon.* **2** 728

[14] Hirano K, Amano K, Uchida A, Naito S, Inoue M, Yoshimori S, Yoshimura K, Davis P 2009 *IEEE J. Quantum Electron.* **45** 1367

[15] Reidler I, Aviad Y, Rosenbluh M, Kanter I 2009 *Phys. Rev. Lett.* **103** 024102

[16] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluh M 2010 *Nat. Photon.* **4** 58

[17] Kanter I, Butkovski M, Peleg Y, Zigzag M, Aviad Y, Reidler I, Rosenbluh M, Kinzel W 2010 *Opt. Express* **18** 17

[18] Zhang J B, Zhang J Z, Yang Y B, Liang J S, Wang Y C 2010 *Acta Phys. Sin.* **59** 7679 (in Chinese) [张继兵、张建忠、杨毅彪、梁君生、王云才 2010 物理学报 **59** 7679]

[19] Wang A B, Wang Y C, He H C 2008 *IEEE Photon. Technol. Lett.* **20** 1633

Spread spectrum communication based on hardware encryption*

Xiao Bao-Jin[1)] Tong Hai-Li[1)] Zhang Jian-Zhong[2)] Zhang Chao-Xia[2)] Wang Yun-Cai[2)3)†]

1) (*Department of Information and Communication, Taiyuan University of Technology, Taiyuan* 030024, *China*)

2) (*Department of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan* 030024, *China*)

3) (*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Shanxi University, Taiyuan* 030006, *China*)

(Received 30 September 2010; revised manuscript received 11 February 2011)

Abstract

The scheme of 1 Gbit/s random sequence generated by chaotic laser as spreading code is proposed. Theoretical analysis indicates that the pseudo random sequence exhibited periodic behavior is eliminated by the random sequence and the capability of spreading code is enlarged. Meanwhile, the communication security can be improved by variable spreading code. The corresponding spread spectrum system is numerically simulated by Simulink software and the results demonstrate that the greater the used spreading gain, the lower the obtained error rate will be when the information speed is constant, which is consistent with the theoretical results. The anti-jamming ability of the spread spectrum system is strengthened and the security is enhanced compared with those of the traditional spreading system.

Keywords: spread spectrum communication, random sequence, chaos laser

PACS: 05.45.Vx

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60927007, 60872019) and the Foundation of State Key Laboratory of Quantum Optics and Quantum Optics Devices, China (Grant No. 200903).

† Corresponding author. E-mail: wangyc@tyut.edu.cn