第 50 卷 第 11 期 2001 年 11 月
1000-3290/2001/50(11)/2121-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.50,No.11,November,2001

基于广义混沌映射切换的混沌同步保密通信*

张家树[1)2)] 肖先赐[1)]

[1)](电子科技大学电子工程系,成都 610054)

[2)](西南交通大学计算机与通信工程学院,成都 610031)

(2001 年 2 月 19 日收到)

提出了一种基于广义混沌映射切换的混沌同步保密通信方式.这种通信方式首先构建产生多种混沌序列的广义混沌映射模型,然后在不同时段根据切换策略产生不同混沌序列,在发送端,将信号与混沌载波之和取模运算后再嵌入混沌映射的输入端进行迭代运算以实现调制;在接收端,根据切换协议,用同一个相应的广义混沌映射模型从接收信号中提取混沌载波并进而恢复信息信号.研究结果表明:这种基于广义混沌映射切换的混沌同步通信方式比基于单一混沌系统的保密通信方式具有更强的抗干扰能力,保密性能更好,且实现简单.

关键词:混沌,混沌映射切换,同步,保密通信

PACC:0545

1 引 言

近几年来,利用混沌信号的类随机特性实现保密通信是混沌应用研究的一个热点[1—5].根据 Pecora 和 Carroll 提出的驱动-响应混沌同步思想,人们已经提出了多种混沌保密通信方式.但是,这些保密通信方案均存在以下不足:(1)这些系统能够实现保密通信,是基于混沌同步的鲁棒(Robust)性,而这种 Robust 性也可为攻击者所利用,从而降低了系统的保密性[5];(2)这些系统均是基于某一种特定的混沌系统来实现保密通信,利用混沌预测技术已成功地破译、提取出信息信号[6,7],保密性能并非像标榜的那样好;(3)这些系统只能传输相对于混沌载波幅度很小的信息信号,这使得接收端解调后的信噪比很低,抗噪声性能较差;(4)由于实际实现中的有效字长精度效应,混沌映射本身所产生的混沌序列也会退化为周期序列.因此,如何增加混沌信号的复杂度和减小有效字长效应的影响是提高混沌保密通信的保密性能的主要问题.

针对上述问题,本文提出了一种基于混沌映射切换的混沌保密通信方式.这种通信方式首先构建产生多种混沌序列的广义混沌映射模型,然后在不同时段根据切换策略来产生不同混沌序列作为混沌载波,在发送端将信息信号与混沌载波进行相加,对相加的结果进行取模求余变换使其仍然落在混沌区,并将取模求余后的结果用于迭代;在接收端,根据切换协议,通过一个与发送端相对应的非线性动力学系统从接收信号中提取混沌载波,并与接收信号相减以实现解调.理论分析与计算机仿真结果表明:这种直接从接收信号中提取混沌载波的、基于混沌映射切换的保密通信方式具有更好的可靠性和保密性能.

2 混沌切换调制保密通信方案

2.1 广义混沌映射模型的定义

要在统一的结构下实现多种混沌映射,一个主要的问题就是应保证各个混沌映射的输入不能超出它的值域范围,因此,应优先考虑值域范围一致的混沌映射来构造这个广义混沌映射.好在有一些离散混沌映射的值域范围能够满足这一要求,例如虫口映射、立方映射、锯齿映射和 Kent 映射等的值域范围都在 -1—1 之间.为此,定义如下一个广义混沌映射为

$$x_{n+1} = g(x_n) = a_0 + a_1 x_n + a_2 x_n^2 + a_3 x_n^3 + a_4 | x_n | + a_5 \mathrm{sign}(x_n - b). \quad (1)$$

当 $a_i(i=0,1,\cdots,5)$ 和 b 取不同值时,(1)式就分别

* 国防预研基金(批准号 98JS05.4.1.DZ0205)资助的课题.

对应于不同的混沌映射,例如,当 $a_0 = 1, a_2 = -2$,其余的 $a_i = 0$ 时,$x_{n+1} = g(x_n)$ 即为虫口映射;而当 $a_1 = 3, a_3 = -4$,其余的 $a_i = 0$ 时,$x_{n+1} = g(x_n)$ 即为立方映射.显然,(1)式中 $a_i\ (i = 0,1,\cdots,5)$ 和 b 的不同组合能够满足通过混沌映射切换方式的这种参数调制混沌保密通信方案的需求,因而,(1)式可以用于这种保密通信体制.

2.2 广义混沌切换调制保密通信方案

假设用于混沌保密通信的两个广义混沌信号产生模型可描述为

$$x_{n+1} = g(x_n, a), \tag{2}$$

$$y_{n+1} = g(y_n, a), \tag{3}$$

其中 x_n 和 y_n 分别为这两个广义混沌产生模型的输出,取值范围为(-1,1).现用(2)式描述的广义混沌系统产生相同的混沌序列作为混沌载波.

设需发送的信息信号为序列 $\{s_n\}$,令

$$x'_{n+1} = g(x_n, a) + s_n. \tag{4}$$

因为叠加后,会使得 $|x'_{n+1}| > 1$.若直接将其 x'_{n+1} 用于迭代,则所得序列有可能会很快发散,故应对 x'_{n+1} 进行取模变换后再进行迭代,即

$$x_{n+1} = x'_{n+1}(\mathrm{mod}1) = [g(x_n, a) + s_n](\mathrm{mod}1). \tag{5}$$

由此就将信息信号嵌入到广义混沌产生系统的迭代之中,从而实现了对混沌载波的调制.

现以 x'_{n+1} 作为发送信号在信道中传输,并取初值 $x'_0 = x_0, 0 < x < 1$,在接收端,当收到来自发送端的序列 $\{y'_n = x'_n\}$,令

$$\begin{cases} y_n = y'_n(\mathrm{mod}A), \\ y_{n+1} = g(y_n, a), \end{cases} \tag{6}$$

其中 y_{n+1} 即为从接收序列中提取的混沌载波,将其与下一个接收序列值 y'_{n+1} 相减,得

$$s'_n = y'_{n+1} - y_{n+1} = s_n, \tag{7}$$

s'_n 即为解调结果.图 1 给出按(1)式实现的基于混沌切换的参数调制保密系统框图.

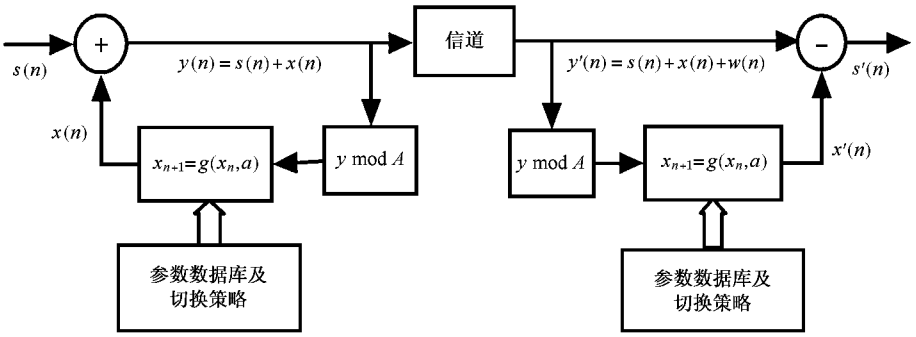


图 1 基于广义混沌映射的混沌切换保密通信系统

2.3 保密性分析

现有的混沌通信方案基本上都是基于单一混沌映射或混沌系统进行设计的,很容易通过预测方法破译其加密信息,原因在于通信信道中传输的混沌加密信息是由一个混沌载波对信息信号调制而成的,当观察时间足够长时,能够建立一个预测模型进行预测破译信息信号.然而,现有的各种混沌预测方法都需要一定的训练样本,预测模型的获得也需要一定的训练时间,且对一种混沌序列有效的预测模型不一定就能对其他混沌序列进行有效预测.因此,在不同时段采用不同的混沌序列作为混沌载波的混沌同步通信方式,既增加了混沌信号的复杂性,也减少了有效字长效应的影响,从而增加了预测破译的难度,其保密性能优于基于单一混沌映射或系统的通信方式,且实现简单.

3 仿真研究

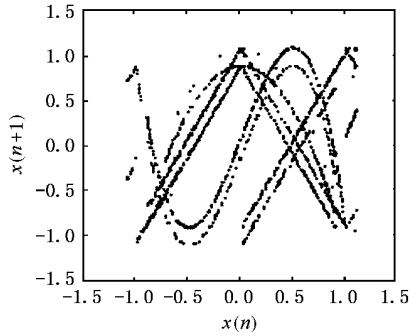
本文对图 1 所示基于广义混沌映射的混沌切换同步保密通信系统进行了计算机仿真.在仿真研究中,1—500 之间的混沌映射选择为虫口映射,510—1000 之间为立方映射、1001—1500 之间为 Tent 映射、1501—2000 之间为锯齿映射.需要加密的信号选择为

(1)方波信号为 $s(n) = \{1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, -1,$

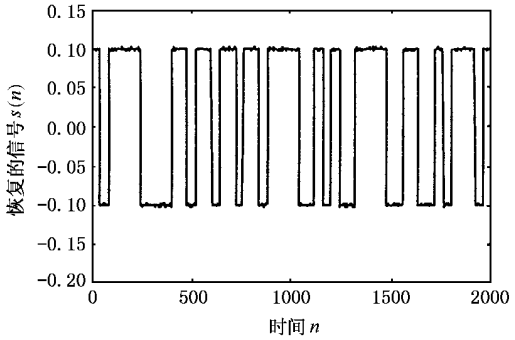
1，－1，1，1，1，－1，1}；

(2)正弦信号为 $s(n)=1.2+0.1\sin(0.01n)$.

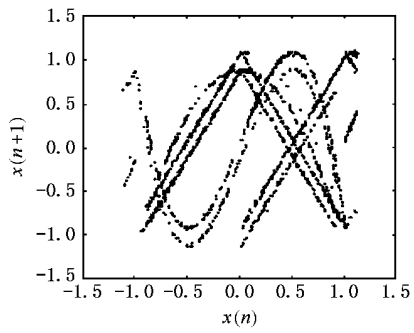
同时假设信道噪声为高斯白噪声,具体的仿真实验结果如图 2 和图 3 所示.



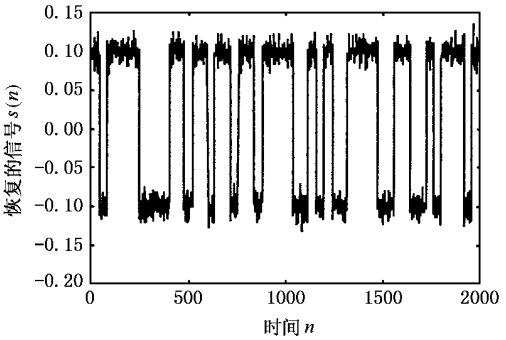
(a) SNR=20 的混沌载波吸引子



(b) SNR=20 时的恢复信号

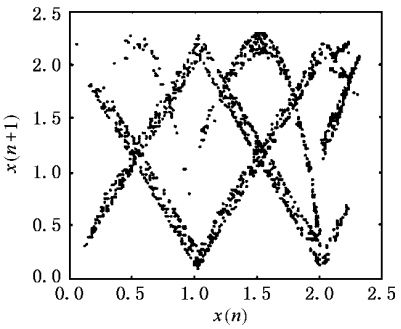


(c) SNR=10 的混沌载波吸引子

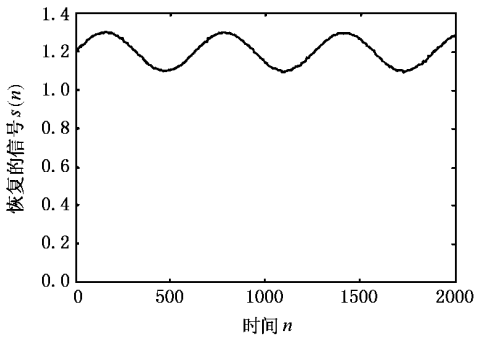


(d) SNR=10 时的恢复信号

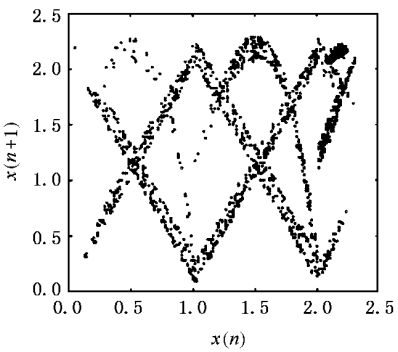
图 2　不同 SNR 时的方波信号恢复结果



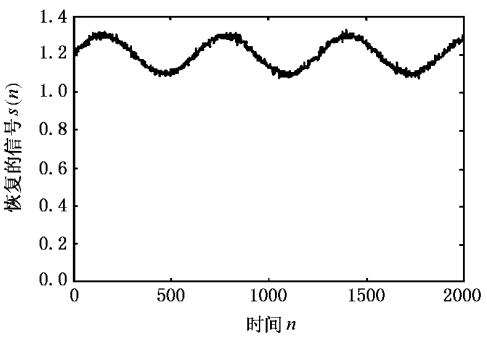
(a) SNR=20 的混沌载波吸引子



(b) SNR=20 时的恢复信号



(c) SNR=10 的混沌载波吸引子



(d) SNR=10 时的恢复信号

图 3　不同 SNR 时的正弦信号恢复结果

从图 2 和图 3 可知:即使 SNR = 10 时,这种方案都能较好地解调出信息信号,这一结果表明了所建议的这种基于混沌映射切换的保密通信方案的可行性;而图 2(a)、(c)和图 3(a)、(c)给出的混沌载波吸引子明显受外加信号的调制表现出不同吸引子结构,相反,同一信号在 SNR = 10 和 SNR = 20 时的吸引子结构具有更多的相似性,且难以从中发现明显的单一混沌吸引子结构,使得已调的发送信号的 x'_{n+1} 表现为一种时变的、更加复杂的混沌序列,即使用前面已经受到的混沌载波信号用于预测建模,由于预测建模本身需要一定的时间,当前载波信号训练好的模型难以有效地预测下一时段不同混沌映射所产生的混沌载波.这一结果表明:难以通过预测手段来破译信息信号,其保密性能明显好于基于单一混沌映射保密通信的保密性能.

4 结束语

本文研究了一种基于广义混沌映射的混沌映射切换同步保密通信方案.这种通信方案首先建立能够产生多种混沌序列的广义混沌映射模型,然后在不同时段根据权值切换策略来更换调整产生混沌序列的混沌映射,在发送端将信号与混沌载波之和经取模运算之后再嵌入广义混沌映射的输入端进行迭代,以实现调制;在接收端,根据权值切换协义,用一个相应的广义混沌映射从接收信号中提取混沌载波,并进而恢复信息信号.仿真研究结果表明:(1)即使在 SNR = 10 时,这种基于广义混沌映射的混沌映射切换保密通信方案都能较好地解调出信息信号,表明了这种混沌保密通信方式的可行性;(2)混沌载波的吸引子结构无明显的单一混沌吸引子结构,已调的发送信号表现为一种时变的、更加复杂的混沌序列,难以通过预测手段来破译信息信号,其保密性能明显好于基于单一混沌映射保密通信的保密性能.(3)基于广义混沌映射的混沌映射切换同步通信方案能够在统一的系统结构下实现产生多种混沌序列,实现简单.若辅以非均匀跳时策略,结合现有的保密通信技术,其保密性能会更好.

[1] K. M. Cuomo, A. V. Oppenheim, S. H. Strogatz, *IEEE Trans. CAS-II*, **40**(1996), 626.

[2] L. M. Pecora, T. L. Carrol, *Phys. Rev. Lett.*, **64**(1990), 821.

[3] D. S. Morrantes, D. M. Rodriggues, *Electron. Lett.*, **34**(1998), 225.

[4] U. Feldmann, M. Hasler, W. Schwartz, *Int. J. Circuit Theory and Applications*, **24**(1996), 551.

[5] B. Ji, J. R. Lu, *J. China Institute of Commun.*, **19**(1998), 47(in Chinese) [纪 飚、陆佶人,通信学报, **19**(1998), 47].

[6] K. M. Short, *Int. J. Bifurcation and Chaos*, **4**(1994), 959.

[7] K. M. Short, *Int. J. Bifurcation and Chaos*, **7**(1997), 1579.

[8] D. J. Farmer, J. J. Sidorowich, *Phys. Rev. Lett.*, **59**(1987), 845.

[9] J. S. Zhang, X. C. Xiao, *Chin. Phys. Lett.*, **17**(2000), 88.

[10] J. S. Zhang, X. C. Xiao, *Chin. Phys.*, **9**(2000), 433.

[11] J. S. Zhang, X. C. Xiao, *Acta Phys. Sin.*, **49**(2000), 403 (in Chinese) [张家树、肖先赐, 物理学报, **49**(2000), 403].

[12] J. S. Zhang, X. C. Xiao, *Acta Phys. Sin.*, **49**(2000), 1221 (in Chinese) [张家树、肖先赐, 物理学报, **49**(2000), 1221].

[13] J. S. Zhang, X. C. Xiao, *Acta Phys. Sin.*, **49**(2000), 2333 (in Chinese) [张家树、肖先赐, 物理学报, **49**(2000), 2333].

CHAOTIC SYNCHRONIZATION SECURE COMMUNICATIONS BASED ON THE EXTENDED CHAOTIC MAPS SWITCH*

ZHANG JIA-SHU[1)2)] XIAO XIAN-CI[1)]

[1)] (*Department of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu* 610054, *China*)

[2)] (*School of Computer and Communication Engineering, Southwest Jiaotong University, Chengdu* 610031, *China*)

(Received 19 February 2001)

ABSTRACT

A chaotic synchronization secure communication method based on chaotic maps switch is proposed. The extended chaotic model is first built to generate many kinds of chaotic signals based on changing parameters during different time durations. In the transmitter, the modulation is implemented by adding the information signal to chaotic carriers, taking a modular operation on the sum, and embedding the result of the modular operation in the iteration of the extended chaotic generating systems. In the receiver, the chaotic carriers are retrieved from the received signals by using the corresponding nonlinear dynamical system, and then the information signals are recovered. The simulation results show that this chaotic synchronization secure communication method based on chaotic maps switch has the good immunity to interference and can be realized easily. It is also shown that this chaotic secure communication system is better in security than that based on single chaotic map.

Keywords: chaos, chaotic maps switch, synchronization, secure communication.

PACC: 0545

* Project supported by the National Defense Foundation of China (Grant No. 98JS05. 4. 1. DZ0205).