一种通过异结构同步实现混沌保密通信新方法

龚美静 瞿少成 王晓燕
(华中师范大学信息技术系 武汉 430079)

摘 要：该文提出通过异结构混沌同步和参数调制实现保密通信的新方法。在发送端将信息信号调制到混沌系统的某个参数中，根据 Lyapunov 稳定性定理，构造合适的控制器，实现了异结构混沌系统的完全同步；在接受端采用非线型滤波器，使信息信号得以有效地恢复，实现信号安全保密传输。仿真结果表明，系统快速达到同步，经参数调制的信号能有效恢复，成功地实现保密通信，具有较强的保密性和实用性。

关键词：保密通信；混沌同步；异结构；参数调制
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)06-1442-03

A Novel Method of Realizing Chaotic Secure Communication by Synchronization of Different Structure

Gong Mei-jing Qu Shao-cheng Wang Xiao-yan
(*Department of Information and Technology*, *Huazhong Normal University*,*Wuhan* 430079, *China*)

Abstract:Based on two different chaotic systems synchronization and parameter modulation, a novel method of realizing chaotic secure communication is proposed in this paper. Information signals are used to modulate some parameter of a chaotic system in the sending terminal, based on Lyapunov stability theory, the proper controllers are designed to realize two different chaotic systems globally synchronization. The appropriate nonlinear filter is designed in the receiving terminal to make the information signals recover effectively, realizing the secure communication. The simulation results show that systems realize synchronization quickly, and the recovered signals are close to the information signals and it can realize secret communication successfully, having strong security and practicability.

Key words: Secure communication; Chaos synchronization; Different structure; Parameter modulation

1 引言

混沌同步实现保密通信已经成为近几年保密通信技术的研究热点[1−3]。自从 1990 年 Pecora 和 Carroll 提出著名的 PC 同步以来[4]，人们采用主动-被动同步法、自适应同步法、脉冲同步法等多种方法研究混沌同步[5,6]，这些方法主要是对两个结构相同的系统进行研究。然而对于两个不同结构的系统同步并不简单，系统结构的不同使混沌同步面对一定的挑战[7]。在激光、生物系统及感知处理过程中，人们很难假定各个子系统的结构相同，因此，异结构混沌系统的同步的研究具有重要的实际意义和应用价值。而在保密通信中，如果能实现异结构混沌系统的同步，则将明显扩大混沌系统同步的范围，提高通信的保密性，于是一些学者对于不同结构的混沌同步进行了深入研究[8, 9]。不同系统的同步为混沌应用于保密通信奠定了基础，混沌同步应用于通信主要有混沌遮掩、混沌调制和混沌开关技术等[10,11]，其中混沌调制由于它把混沌信号谱的整个范围都用来隐藏信息，增加了对参数变化的敏感性，从而增强了保密性，文献[12]采用混沌信号调制的方式实现了保密通信，但是针对两个相同的系统，具有一定的局限性。

针对上述问题，本文将异结构系统的同步和混沌参数调制方法相结合，在发送端将信息信号调制在混沌系统的一个参数中，采用合适的控制器，使该系统和不同接收系统同步；在接受端采用新型非线性滤波器，将信息信号从接收系统中恢复出来，实现信号安全保密传输。该方法扩大了同步范围，使混沌同步应用于保密通信的实用性更强，通过 Simulink 仿真，可以便捷地选择最佳滤波参数，使信号得到有效恢复，且该设计具有有效性和一般实用性。

2 混沌系统模型及同步

2.1 混沌系统模型

文献[13]提出了一种新的混沌系统，称为统一混沌系统，其描述如下：

$$\left.\begin{aligned}\dot{x}&=(25a+10)(y-x)\\ \dot{y}&=-xz+(28-35a)x+(29a-1)y\\ \dot{z}&=xy-(8+a)z/3\end{aligned}\right\} \tag{1}$$

2008-06-03收到，2008-12-31改回
高等学校博士学科点专项科研基金(20070511017)资助课题

其中 $a\in[0,1]$。当 $a=0$ 时，上述系统属于 Lorenz 系统；当 $a=1$ 时，系统属于陈氏系统；当 $a=0.8$ 时，系统属于 Lü 系统；当 $a\in[0,0.8)$ 时，系统属于广义 Lorenz 系统；当 $a\in(0.8,1]$ 时，系统属于广义陈氏系统。于是，系统式(1)在 Lorenz 系统与陈氏系统之间架起了一座桥梁，a 由 0 逐渐增加到 1，系统由广义 Lorenz 系统逐渐过渡到广义陈氏系统。而且，系统式(1)在整个区间 $a\in[0,1]$ 里都是混沌的。

2.2 混沌同步描述

设混沌系统可描述为

$$\dot{\boldsymbol{x}}(\boldsymbol{t})=\boldsymbol{f}(\boldsymbol{x},\boldsymbol{\mu},\boldsymbol{t}) \tag{2}$$

$$\dot{\boldsymbol{y}}(\boldsymbol{t})=\boldsymbol{f}(\boldsymbol{y},\hat{\boldsymbol{\mu}},\boldsymbol{t})+\boldsymbol{u} \tag{3}$$

其中 $\boldsymbol{x},\boldsymbol{y}\in R^n$ 为系统的状态，$\boldsymbol{\mu},\hat{\boldsymbol{\mu}}\in R^m$ 为系统参数，$\boldsymbol{u}\in R^n$ 为控制器，式(2)为驱动系统，式(3)为响应系统。

若令 $\boldsymbol{e}=\boldsymbol{y}-\boldsymbol{x}$ 为误差向量，由式(3)减去式(2)得同步误差方程：

$$\dot{\boldsymbol{e}}(\boldsymbol{t})=\boldsymbol{f}(\boldsymbol{y},\hat{\boldsymbol{\mu}},\boldsymbol{t})-\boldsymbol{f}(\boldsymbol{x},\boldsymbol{\mu},\boldsymbol{t})+\boldsymbol{u} \tag{4}$$

如果存在控制 $\boldsymbol{u}$，使得任意初始条件 $x(t_0)$，$y(t_0)$ 出发的系统式(2)，式(3)有 $\lim\limits_{t\to\infty}\|\boldsymbol{e}(\boldsymbol{t})\|\to 0$ 成立，则称响应系统式(3)和驱动系统式(2)是完全同步的。即可将混沌同步问题转化为式(4)在原点的渐进稳定问题。

3　基于混沌同步和新方法的保密通信

3.1 参数调制异结构混沌系统的同步

考虑Lorenz系统与Lü系统的同步。发送端Lorenz系统方程如下

$$\left.\begin{aligned}\dot{x}&=a(y-x)\\ \dot{y}&=bx-y-xz\\ \dot{z}&=xy-rz\end{aligned}\right\} \tag{5}$$

当 $a=10$，$b=28$，r 在 $8/3$ 附近时，该系统处于混沌状态。对于发送端Lorenz混沌系统式(5)，适当处理信息信号 $m(t)$ 使其调制在混沌参数 r 中。选取复合信号 $s(t)=rz$ 作为传输信号。由于信息信号 $m(t)$ 与发送混沌信号 $s(t)$ 没有直接的关联关系，且信息信号已完全融入混沌系统，而不是浮在混沌载体上，从而可以实现更有效的保密传输。

接受端Lü系统为

$$\left.\begin{aligned}\dot{x}_1&=a_1(y_1-x_1)+u_1(t)\\ \dot{y}_1&=b_1y_1-x_1z_1+u_2(t)\\ \dot{z}_1&=x_1y_1-s(t)+u_3(t)\end{aligned}\right\} \tag{6}$$

传输信号到达接收端，且 $a_1=36$，$b_1=20$ 时，该系统处于混沌状态。设 $e_1=x_1-x$，$e_2=y_1-y$，$e_3=z_1-z$，则系统误差方程为

$$\left.\begin{aligned}\dot{e}_1&=\dot{x}_1-\dot{x}=a_1(y_1-x_1)+u_1(t)-a(y-x)\\ \dot{e}_2&=\dot{y}_1-\dot{y}=-x_1z_1+b_1y_1+u_2(t)-(bx-y-xz)\\ \dot{e}_3&=\dot{z}_1-\dot{z}=x_1y_1-s(t)+u_3(t)-(xy-s(t))\end{aligned}\right\} \tag{7}$$

整理得 $\dot{e}_1=e_2-e_1+(a_1-1)(y_1-x_1)-(a-1)(y-x)+u_1(t)$，$\dot{e}_2=-(e_1+e_2)+(b_1+1)y_1+x_1-(b+1)x-x_1z_1+xz+u_2(t)$，$\dot{e}_3=x_1y_1-xy+u_3(t)$。

根据相关推理，令

$$\left.\begin{aligned}u_1(t)&=(1-a_1)(y_1-x_1)+(a-1)(y-x)\\ u_2(t)&=-(b_1+1)y_1-x_1+(b+1)x+x_1z_1-xz\\ u_3(t)&=-x_1y_1+xy\end{aligned}\right\} \tag{8}$$

构造Lyapunov函数 V 如下：$V=(1/2)({e_1}^2+{e_2}^2+{e_3}^2)$。则 V 沿误差系统轨迹对时间的求导为 $\dot{V}=e_1\dot{e}_1+e_2\dot{e}_2+e_3\dot{e}_3=e_1(e_2-e_1)-e_2(e_2+e_1)=-{e_1}^2-{e_2}^2<0$。当 $e_1=e_2$ 时，则 $V=\dot{V}$。由Lyapunov稳定性定理，误差系统式(7)渐近稳定，于是采用式(8)控制时，可实现发送系统式(5)和接收系统式(6)同步。

3.2 调制与滤波解调的实现

混沌参数调制的基本思想是利用所传输的信号来调制混沌系统的参数或变量，发送的信息信号隐藏在系统的参数中，然后发送混沌驱动信号，使响应系统与驱动系统同步。在接受端，利用混沌同步信号提取出相应的混沌系统参数，进而恢复出信息信号。

在发送端式(5)，设信息信号为 $m(t)=\sin(t/5)$，$r=m(t)+8/3$，将 r 作为混沌参数，从而将信息隐藏在混沌信号中。由前述证明可知，在控制器式(8)的作用下，接收系统式(6)与发送系统式(5)达到同步。于是在接受端设计合适的滤波器，解调出信息信号。

在接受端，为把参数 r 解调出来，需要作以下变换

$$\dot{z}_1=x_1y_1-rz_1-x_1y_1+xy=xy-rz_1=rg_0+g_1 \tag{9}$$

其中 $g_0=-z_1$，$g_1=xy$，则 $r=\dfrac{\dot{z}_1-g_1}{g_0}$。为了得到调制参数 r 的估计值，可以在初始条件未知的情况下，引入一个因式 e^{kt} 得

$$(z_1e^{kt})'=\dot{z}_1e^{kt}+kz_1e^{kt}=e^{kt}(rg_0+g_1+kz_1) \tag{10}$$

其中 k 为任意正常数，调整 k 的值可以使解调滤波器得到较好的输出。从开始时间 t_0 到现有时间 t 对式(10)两端积分并除以 e^{kt} 得

$$\begin{aligned}z_1&=\int_{t_0}^{t}e^{k(\tau-t)}rg_0\mathrm{d}\tau+\int_{t_0}^{t}e^{k(\tau-t)}rg_0\mathrm{d}\tau+\int_{t_0}^{t}e^{k(\tau-t)}(g_1+kz_1)\mathrm{d}\tau\\ &=\int_{t_0}^{t}e^{k(\tau-t)}rg_0\mathrm{d}\tau+\int_{t_0}^{t}e^{k(\tau-t)}(g_1+kz_1)\mathrm{d}\tau\end{aligned} \tag{11}$$

其中 z_{10} 为 z_1 在 $t=t_0$ 时得初始条件，当 $t\to\infty$ 时，$z_{10}e^{k(t_0-t)}\to 0$。则很容易得到调制参数的估计值

$$\hat{r}=\frac{z_1-\beta}{\alpha} \tag{12}$$

其中 $\alpha=\int_{t_0}^{t}e^{k(\tau-t)}g_0\mathrm{d}\tau$，$\beta=\int_{t_0}^{t}e^{k(\tau-t)}(g_1+kz_1)\mathrm{d}\tau$。由于 α,β 的这种表达形式不容易计算，利用牛顿-莱布尼兹公式，可以将 α,β 变形为：$\dot{\alpha}=g_0-k\alpha$，$\dot{\beta}=g_1+kz_1-k\beta$。

对于式(12)，当 $\alpha=0$ 时，参数瞬间估计值是奇异的，在实际应用中，这个奇点限制了对参数的估计，于是设计一个

低通滤波器

$$\hat{r}_f = \frac{q|\alpha|}{1+|\alpha|}(\hat{r} - r_f - 1) \tag{13}$$

其中 $\frac{q|\alpha|}{1+|\alpha|}$ 为滤波参数，q 是任意常数。由式(12)和式(13)得到

$$\hat{r}_f = \frac{q\,\mathrm{sgn}(\alpha)}{1+|\alpha|}(z_1 - \beta - \alpha r_f - \alpha) \tag{14}$$

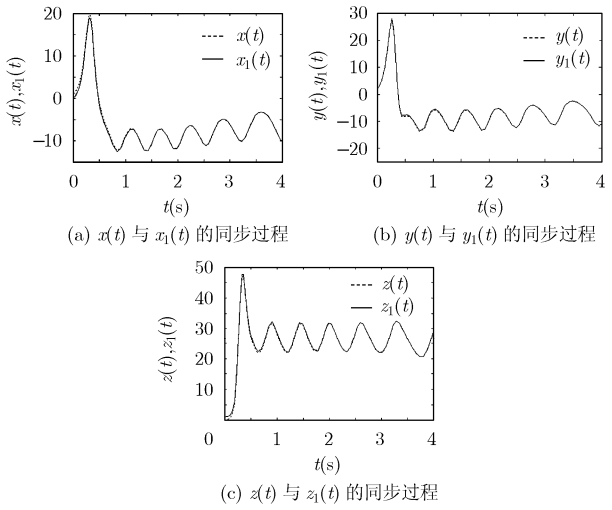
其中 sgn( ) 为符号函数，r_f 是调制参数 r 的滤波估计值。合理选择 q，就可以得到恢复的信息信号 $m(t)$。

3.3 数值仿真

用Matlab对所提出的方法进行了仿真验证，选取发送Lorenz系统式(5)和接收Lü系统式(6)的任意初始值(1,2,0)和(0,2,1)，只要设定的初值使系统处于混沌状态，在控制器式(8)的作用下，Lorenz系统与Lü系统快速达到同步。图1为两个系统的同步过程；图2为两个系统的同步误差，可见两系统误差快速趋近于零，同步效果良好；图3为信息信号为 $m(t) = \sin(t/5)$，$k = 30$，$q = 90$ 时信息信号 $m(t)$ 和恢复信号 $m'(t)$ 的图形，由图3可知，在较短的时间内，解调信号 $m'(t)$ 很快地逼近了信息信号 $m(t)$，实现信号的有效恢复。

4 结论

本文提出了利用异结构混沌同步和参数调制及其滤波的方式，实现了保密通信的实用简便方法。异结构混沌同步的实现，有效改善系统参数的扰动对同步产生的影响，使得混沌同步应用到保密通信中实用性更强。参数调制方法具有更强的保密性，并利用一个合适的滤波器有效恢复信息信号，解调的可靠性更高。通过仿真证明，该方法能够取得较好的效果，并能应用于一般的混沌系统中，实用性较强，具有很好的应用前景。



(a) $x(t)$ 与 $x_1(t)$ 的同步过程　(b) $y(t)$ 与 $y_1(t)$ 的同步过程

(c) $z(t)$ 与 $z_1(t)$ 的同步过程

图1 Lorenz系统与Lü系统的同步过程

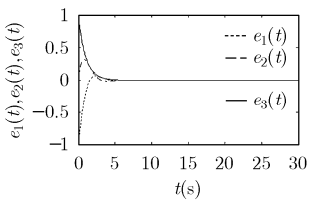


图 2 Lorenz 系统与 Lü 系统同步误差

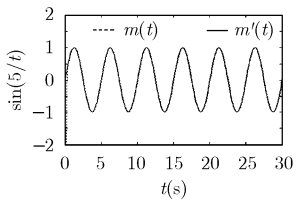


图 3 信息信号 $m(t)$ 和恢复信号 $m'(t)$ 的波形

参 考 文 献

[1] Wang Y W, Guan Z H, and Wen X J. Adaptive synchronization for Chen chaotic system with fully unknown parameters [J]. *Chaos, Solitons & Fractals*, 2004, 19(4): 899–903.

[2] Kocarev L and Parlitz U. General approach for chaotic synchronization with application to communication [J]. *Phys. Rev. Lett*, 1995, 74(25): 5028–5031.

[3] Yang T and Chua L O. Secure communication via chaotic parameter modulation[J]. *IEEE Trans. on Circuits Syst.* I, 1996, 43(9): 817–819.

[4] Peccora L M and Carroll T L. Synchronization in chaotic system [J]. *Phys Rev Lett*, 1990, 64(8): 821–824.

[5] Yu Y G. Adaptive synchronization of a unified chaotic system [J]. *Chaos, Solitons & Fractals*, 2008, 36(2): 329–333.

[6] Chen D L, Sun J T, and Huang C S. Impulsive control and synchronization of general chaotic system[J]. *Chaos, Solitons & Fractals*, 2006, 28(1): 213–218.

[7] Yassen M T. Controlling, synchronization and tracking chaotic Liu system using active backstepping design[J]. *Phys. Rev Lett*, 2007, 360(4–5): 582–587.

[8] Hassan S and Mohammad S. Adaptive synchronization of two different chaotic systems with time varying unknown parameters [J]. *Chaos, Solitons & Fractals*, 2008, 37(1): 125–136.

[9] Mohammad H and Mahsa D. Impulsive synchronization of different hyperchaotic (chaotic) systems[J]. *Chaos, Solitons & Fractals*, 2008, 38(1): 120–131.

[10] 韩建群, 朱义胜.一种利用数字信道实现混沌保密通信方法[J]. 电子与信息学报, 2006, 28(12): 2359–2361.
Han J Q and Zhu Y S. A method of realizing chaotic secure communication by using digital channel[J]. *Journal of Electronics & Information Technology*, 2006, 28(12): 2359–2361.

[11] 赵柏山, 朱义胜.一种改进的混沌掩盖技术[J]. 电子与信息学报, 2007, 29(3): 699–710.
Zhao B S and Zhu Y S. An improved secure communication system based on chaotic masking[J]. *Journal of Electronics & Information Technology*, 2007, 29(3): 699–710.

[12] Corron N J and Hahs D W. A new approach to communication using chaotic signals[J]. *IEEE Trans. on CAS*, 1997, 44(5): 373–382.

[13] Lü J H, Chen G, and Zhang S. Dynamical analysis of a new chaotic attractor[J]. *Int. J. Bifurcat Chaos*, 2002, 12(1): 1001–1015.

龚美静： 女，1983 年生，硕士生，研究方向为混沌控制与保密通信、信息处理.

瞿少成： 男，1972 年生，副教授，硕士生导师，研究方向为智能控制、混沌控制与保密通信、非线型控制.

王晓燕： 女，1983 年生，硕士生，研究方向为混沌控制与保密通信、系统仿真.