第37卷 第14期 计 算 机 工 程 2011年7月
Vol.37 No.14 Computer Engineering July 2011

·开发研究与设计技术· 文章编号：1000—3428(2011)14—0259—03 文献标识码：A 中图分类号：TP393

线性反馈控制在保密通信中的应用

张付臣[1]，杨洪亮[2]

(1. 重庆大学数学与统计学院，重庆 401331；2. 临沂大学信息学院，山东 临沂 276005)

摘 要：为解决保密通信中信息解密的混沌同步问题，提出一种混沌同步的线性反馈控制方法。证明混沌保密通信中混沌系统的最终有界性，将该混沌系统的界应用到混沌同步中，用线性反馈控制实现2个混沌系统的完全同步。计算机模拟实验结果验证了该方法的有效性。

关键词：保密通信；超混沌系统；数值模拟；混沌同步

Application of Linear Feedback Control in Secrecy Communication

ZHANG Fu-chen[1], YANG Hong-liang[2]

(1. College of Mathematics and Statistics, Chongqing University, Chongqing 401331, China;
2. School of Informatics, Linyi University, Linyi 276005, China)

【Abstract】To solve the the chaos synchronization problems of Information decryption in secrecy communication, linear feedback control approach is proposed. It proofs that chaos system applied in the communication has boundedness, then the boundedness is used to design the linear controller. It proposes linear control to make two identical new chaotic systems globally asymptotically synchronization. Experimental results demonstrate the effectiveness of the proposed approach.

【Key words】secrecy communication; hyper-chaotic system; numerical simulation; chaos synchronization

DOI: 10.3969/j.issn.1000-3428.2011.14.088

1 概述

经过近几十年的发展，混沌控制与同步及应用研究获得了突破性的进展，目前国内外已经提出了许多不同的控制混沌的方法，如OGY方法、偶然正比反馈技术(Occasional Proportional Feedback, OPF)、自适应控制、线性反馈控制、自适应反馈控制等方法。本文提出一种混沌同步的线性反馈控制方法，对线性反馈控制在保密通信中的应用展开研究。

2 背景介绍

近年来竞争最激烈的应用研究是将混沌同步用于保密通信中。已经发现，当秘密通信的双方都有完全相同的混沌电路时，在特定的条件下可以实现秘密信号从发射机的编码到接收机的解码的全过程信息解密，即达到了2个系统的混沌同步。这里2个系统的同步，是指一个系统的轨道将完全收敛于另一个系统轨道的同一值，它们之间将始终保持步调一致，并且这种步调是结构稳定的。为此，Pceora和Carroll研制了一种能产生混沌的非线性电路，并可以分成一个稳定的子系统及一个不稳定的子系统，然后，把具有负的Lyapunov指数的稳定部分复制成一个响应系统，而原系统称为驱动系统，这样响应系统是稳定的而且是驱动系统的复制品，其轨道就不受初始条件微小波动的影响，而将与驱动系统收敛于同一轨道。这样将非线性映射所产生的混沌序列作为载波，把有用的信号作为调制信号并合在混沌信号中发射出去；在接收端，利用混沌序列的发生规则从接收信号提取混沌载波，再经过简单的信号处理恢复有用的信号。

混沌控制和同步在保密通信、信息处理[1]、生物医学等方面，都具有巨大的应用潜力和发展前景，目前已经提出了许多实现混沌控制和同步的一些可能应用方案，主要是通过电子线路、激光系统、神经网络和计算机系统来实现。同时，由于超混沌比混沌在上述应用中更具优越性，因此人们正在不断探索超混沌控制和同步的有效方法。

混沌系统的最终界在混沌系统的控制和同步中有着广泛的用途[2]。Lü系统是一个重要的混沌系统，是Lorenz系统和Chen系统连接的重要一个纽带[3]，这个系统已被广泛研究[4-9]。Lü系统关于x和z的一个不等式[3-10]如下：

$$\lim_{t\to+\infty}\left[z>\frac{1}{2a}x^2\right]\geqslant 0 \tag{1}$$

当$a=36,b=3,c=20$时，式(1)存在典型的吸引子[3]。

一个新的超混沌系统为[11]：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=cx-xz+w\\ \dot{z}=xy-bz\\ \dot{w}=-dx\end{cases} \tag{2}$$

其中，a, b, c, d是系统正的参数，当$a=35,b=3,c=35,d=8$时，初值为(10, 11, 12, 13)，系统的李亚普指数$LE_1=0.2788$, $LE_2=0.1470, LE_3=0, LE_4=-38.429$，因为，此时系统有2个正的李亚普指数。此时系统是一个超混沌系统[11]。

另一个新的超混沌系统为[12]：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=bx-xz+w\\ \dot{z}=dxy-cz\\ \dot{w}=-rx\end{cases} \tag{3}$$

其中，a, b, c, d, r是系统的正的参数，当$a=10,b=45,c=25,$

基金项目：中央高校基本科研业务费基金资助项目(CDJXS 10 10 0029)

作者简介：张付臣 (1983－)，男，硕士，主研方向：混沌系统，分岔理论；杨洪亮，副教授

收稿日期：2011-01-14 **E-mail：**zhangfuchen1983@163.com

$d=4, r=5$ 时，系统的李亚普指数 $LE_1=0.8589, LE_2=0.1068$, $LE_3=0, LE_4=-13.4625$，此时系统是一个超混沌系统[12]。

一个新的三维系统如下：

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=abx-axz\\ \dot{z}=-cz+xy\end{cases} \tag{4}$$

当 a=5, b=4, c=2 时，系统存在一个典型的混沌吸引子。

这几个系统的的一些混沌行为，电路实现和自适应反同步问题已经研究过[3-12]，但是是否有一个系统混沌吸引子存在的全局吸引域，即当时间 $t\to\infty$ 时系统的所有轨线被吸引到该吸引域，这个问题还没有研究过，本文将对这个问题进行研究。

3 系统的最终有界性证明

定理 1 对于式(2)，当系统参数满足 $a>0, b>0, 0<d<a^2$ 时，该系统所有的轨道包括超混沌轨道被吸引到一个有界的区域。

证明：构造下列的李雅普函数：

$$V_2(x,y,z,w)=\frac{1}{2}\left[\left(x-\frac{w}{a}\right)^2+y^2+(z-a-c)^2+\frac{(a^2-d)w^2}{a^2d}\right]$$

沿着系统(2)的轨线对时间求导可得：

$$\dot{V}_2(x,y,z,w)=-\frac{a^2-d}{a}x^2-bz^2+b(a+c)z=$$
$$-\frac{a^2-d}{a}x^2-b\left(z-\frac{a+c}{2}\right)^2+\frac{(a+c)^2b}{4}$$

所有存在一个充分大的常数 $d_0>0$，使对于所有满足 $V_2(x,y,z,w)=d_1$ 的 (x,y,z,w) (这里 $d_1>d_0$)，有：

$$\frac{a^2-d}{a}x^2+b\left(z-\frac{a+c}{2}\right)^2>\frac{(a+c)^2b}{4}$$

因此，在表面 $\{(x,y,z,w)|V_2(x,y,z,w)=d_1\}$ 上，有 $\dot{V}_2(x,y,z,w)<0$，表示集合 $\Omega_1=\{(x,y,z,w)|V_2(x,y,z,w)\leqslant d_1\}$ 是式(2)的所有解的一个吸引域。因此，当系统参数满足 $a>0, b>0, 0<d<a^2$ 时，式(2)的所有轨道最终有界。

评注：由式(2)的最终界和有 2 个正的李亚普指数 $LE_1=0.2788, LE_2=0.1470$。参数估计 $a>0, b>0, 0<d<a^2$ 在混沌吸引子的范围之内，因此，式(2)确实存在一个混沌吸引子的吸引域，当时间 $t\to\infty$ 时，式(2)的所有轨线被吸引到该吸引域。式(2)对于参数 $a=35, b=3, c=35, d=8$ 确实存在一个超混沌吸引子，初值为 (10,11,12,13) 时，系统存在一个典型的混沌吸引子[11]。

定理 2 对于式(3)，当系统参数满足 $a>0, b>0, c>0, d>0, 0<r<\frac{a^2}{d}$ 时，该系统所有的轨道包括超混沌轨道被吸引到一个有界的区域。

证明：构造下列的李雅普函数：

$$V_3(x,y,z,w)=\frac{1}{2}\left[\left(x-\frac{dw}{a}\right)^2+dy^2+\left(z-\frac{a+bd}{d}\right)^2+\frac{d(a^2-dr)w^2}{a^2r}\right]$$

沿着式(3)的轨线对时间求导可得：

$$\dot{V}_3(x,y,z,w)=-\frac{(a^2-dr)}{a}x^2-cz^2+\frac{c(a+bd)}{d}z=$$
$$-\frac{(a^2-dr)}{a}x^2-c\left(z-\frac{a+bd}{2d}\right)^2+\frac{c(a+bd)^2}{4d^2}$$

可以证明存在一个充分大的 $d_3>0$，使得集合：

$$\Omega_3=\{(x,y,z,w)|V_3(x,y,z,w)\leqslant d_3\}$$

是式(3)的所有轨线的一个吸引域。因此，当系统参数满足 $a>, b>0, c>0, d>0, 0<r<\frac{a^2}{d}$ 时，式(3)的所有轨道最终有界。

从式(3)的最终界和有 2 个正的李亚普指数 $LE_1=0.8589$, $LE_2=0.1068$ 可知，式(3)对于系统参数 $a=10, b=45, c=25, d=4, r=5$ 确实存在一个超混沌吸引子，系统存在一个典型的混沌吸引子[12]。同时，参数估计 $a>0, b>0, c>0, d>0, 0<r<a^2/d$ 在混沌吸引子的范围之内，因此，式(3)确实存在一个混沌吸引子的吸引域，即当时间 $t\to\infty$ 时系统式(3)的所有轨线被吸引到该吸引域。

引理 当式(4)的参数满足 $2a\geqslant c>0$，式(4)有下列两维抛物式最终界估计：

$$\lim_{t\to+\infty}\left[z-\frac{1}{2a}x^2\right]\geqslant 0 \tag{5}$$

证明：定义李雅普函数 $V(x,y,z)=\frac{1}{2a}x^2-z$，沿着式(4)的轨线对时间求导得：

$$\dot{V}=\frac{1}{2a}\times 2x\dot{x}-\dot{z}=-x^2+cz$$

因此，

$$\dot{V}+cV=\left(\frac{c}{2a}-1\right)x^2$$

当 $2a\geqslant c>0$ 时，有 $\dot{V}+cV\leqslant 0$。对任何初值 $V(t_0)=V_0$，根据微分方程比较定理有：

$$V(t)\leqslant V_0e^{-c(t-t_0)}\to 0(t\to+\infty)$$

因此，

$$\lim_{t\to+\infty}V(t)=\lim_{t\to+\infty}\left[\frac{1}{2a}x^2-z\right]\leqslant 0,\quad 2a\geqslant c>0$$

证毕。

定理 3 当系统(4)参数满足 $2a\geqslant c>0$, $b>0$ 时，式(4)有下列最终有界集：

$$\Omega=\{(x,y,z)|mx^2+(y-nx)^2+a(z-\tau)^2\leqslant R\} \tag{6}$$

其中，

$$m>0,\quad 1\geqslant\frac{c}{2a}>n>0,\quad \tau=\frac{ma+an+ab+an^2}{a}$$
$$l=2am+2n(an+ab),\quad \beta=2an,\quad \gamma=2a(c-2an)$$
$$\Gamma=\left\{(x,y,z)|lx^2+\beta y^2+\gamma\left(z-\frac{\tau ac}{\gamma}\right)^2=\frac{\tau^2a^2c^2}{\gamma}\right\}$$
$$R=\max_{(x,y,z)\in\Gamma}\{mx^2+(y-nx)^2+a(z-\tau)^2\}$$

证明：定义李雅普函数：

$$V=mx^2+(y-nx)^2+a(z-\tau)^2$$

沿着式(4)的轨线对 V 求导得：

$$\dot{V}=2mx\dot{x}+2(y-nx)(\dot{y}-n\dot{x})+2a(z-\tau)\dot{z}=$$
$$-(2am+2an^2+2nab)x^2-2any^2-2acz^2+2ac\tau z+$$
$$(2am+2an+2ab+2an^2-2a\tau)xy+2anx^2z$$

由引理，有：

$$\dot{V}\leqslant-(2am+2an^2+2nab)x^2-2any^2-2a(c-2an)z^2+2\tau acz=$$
$$-(2am+2an^2+2nab)x^2-2any^2-$$

$$2a(c-2an)\left(z-\frac{\tau c}{2(c-2an)}\right)^2+\frac{a\tau^2c^2}{2(c-2an)}=$$

$$-lx^2-\beta y^2-\gamma\left(z-\frac{\tau ac}{\gamma}\right)^2+\frac{\tau^2a^2c^2}{\gamma}$$

在 Γ 外部，即当：

$$(2am+2an^2+2nab)x^2+2any^2+$$

$$2a(c-2an)\left(z-\frac{\tau c}{2(c-2an)}\right)^2>\frac{ac^2\tau^2}{2(c-2an)}$$

等价于：

$$lx^2+\beta y^2+\gamma\left(z-\frac{\tau ac}{\gamma}\right)^2>\frac{a^2c^2\tau^2}{\gamma}$$

有 $\dot{V}<0$，在 Γ 内部有 $\dot{V}>0$，因此，函数 V 的最大值只能在 Γ 面上取得。

容易证得此时式(6)是式(4)的最终有界集。

评注：对于式(4)的参数 a=5, b=4, c=2，参数估计 $2a\geqslant c>0$，$b>0$ 在该系统的混沌吸引子范围之内，因此，式(4)的最终界得到完美解决。下一步就是要确定函数 $V=mx^2+(y-nx)^2+a(z-\tau)^2$ 在三维曲面：

$$\Gamma=\left\{(x,y,z)\middle|lx^2+\beta y^2+\gamma\left(z-\frac{\tau ac}{\gamma}\right)^2=\frac{\tau^2a^2c^2}{\gamma}\right\}$$

上的最大值。

4　有界性在的同步中的应用

让式(4)的系统为驱动系统，响应系统如下：

$$\begin{cases}\dot{x}_1=a(y_1-x_1)\\ \dot{y}_1=abx_1-ax_1z_1-k(y_1-y)\\ \dot{z}_1=-cz_1+x_1y_1\end{cases}\tag{7}$$

其中，$k>0$ 为控制系数，从定理 3 可以知道，变量 x, y, z 均有界。不妨设 $|x|\leqslant M_1$, $|y|\leqslant M_2$, $|z|\leqslant M_3$，则有下列定理：

定理 4　当 $k>\max\left\{\frac{a(b+\rho+M_3)^2}{4\rho},\frac{ac(b+\rho+M_3)^2}{4c\rho-M_2^2}\right\}$ 时，响应系统(式(7))能和驱动系统(式(4))达到完全同步。

证明：令向量误差为 $e_1=x_1-x, e_2=y_1-y, e_3=z_1-z$，则误差系统为：

$$\begin{cases}\dot{e}_1=a(e_2-e_1)\\ \dot{e}_2=abe_1-axe_3-aze_1-ae_1e_3-ke_2\\ \dot{e}_3=-ce_3+e_1e_2+xe_2+ye_1\end{cases}\tag{8}$$

取李雅普函数 $V(e_1,e_2,e_3)=\rho e_1^2+e_2^2+ae_3^2$，这里 $\rho>\frac{M_2^2}{4c}$ 为实数。沿着式(8)的轨线求导可得：

$$\frac{1}{2}\dot{V}(e_1,e_2,e_3)=\rho e_1\dot{e}_1+e_2\dot{e}_2+ae_3\dot{e}_3=-a\rho e_1^2-ke_2^2-ace_3^2+$$

$$(ab+a\rho-az)e_1e_2+aye_1e_3\leqslant-a\rho e_1^2-ke_2^2-$$

$$ace_3^2+(ab+a\rho+aM_3)|e_1||e_2|+aM_2|e_1||e_3|=$$

$$-\boldsymbol{E}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{E}$$

其中，$\boldsymbol{E}=(|e_1|,|e_2|,|e_3|)^{\mathrm{T}}$；

$$\boldsymbol{P}=\begin{bmatrix}a\rho & -\frac{a(b+\rho+M_3)}{2} & -\frac{aM_2}{2}\\ -\frac{a(b+\rho+M_3)}{2} & k & 0\\ 0 & -\frac{aM_2}{2} & ac\end{bmatrix}$$

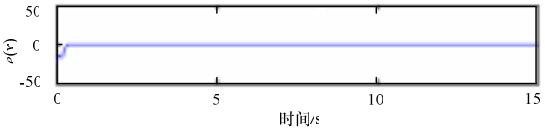
经过简单计算可知，当：

$$k>\max\left\{\frac{a(b+\rho+M_3)^2}{4\rho},\frac{ac(b+\rho+M_3)^2}{4c\rho-M_2^2}\right\}$$

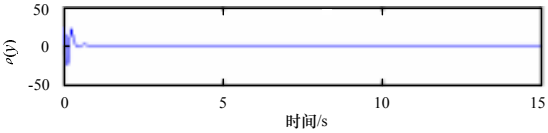
时，矩阵 $\boldsymbol{P}$ 为正定矩阵，从而误差系统(式(8))的原点是渐进稳定的，即响应系统(式(7))能和驱动系统(式(4))达到完全同步。证毕。

5　数值模拟

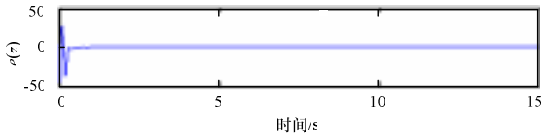
利用计算机仿真来验证控制器的有效性。取系统参数 a=5, b=4, c=2，式(4)和式(7)的初值分别为(25, –2, 18)和(0, 0, 0)。取控制系数 k=15 时，在线性反馈控制下，式(4)和式(7)的同步曲线如图 1 所示，其中，$e(x)=x_1-x$; $e(y)=y_1-y$; $e(z)=z_1-z$。



(a)$e(x)$随时间演化的曲线



(b)$e(y)$随时间演化的曲线



(c)$e(z)$随时间演化的曲线

图 1　线性反馈控制下 2 个系统的同步曲线

从图 1 可以看出，在线性反馈控制下，式(4)和式(7)经过很短的时间达到了完全同步，验证了线性控制器的有效性。

6　结束语

本文提出了混沌同步的线性反馈控制，数值模拟实验证明了该方法的有效性。以该方法设计的控制器简单易于操作，在保密通信中具有一定的实用价值。同时，该方法也适用于其他混沌系统的同步，具有较好的应用前景。

参考文献

[1] 朱延钊. 一种语言混沌保密通信方案的 DSP 实现[J]. 计算机工程, 2010, 36(15): 151-152.

[2] Shu Yonglu, Xu Hongxing, Zhao Yunhong. Estimating the Ultimate Bound and Positively Invariant Set for a New Chaotic System and Its Application in Chaos Synchronization[J]. Chaos, Solitons & Fractals, 2009, 42(5): 2852-2857.

[3] Lü Jinhu, Chen Guanrong. A New Chaotic Attractor Coined[J]. International Journal of Bifurcation and Chaos, 2002, 12(3): 659-661.

[4] Agiza H Z. Chaos Synchronization of Lü Dynamical System[J]. Nonlinear Analysis: Theory, Methods & Applications, 2004, 58(1/2): 11-20.

[5] Li Dequan. TS Fuzzy Realization of Chaotic Lü System[J]. Physics Letters A, 2006, 356(1): 51-58.

[6] Han Xiuping, Lu Junan, Wu Xiaoqun. Adaptive Feedback Synchronization of Lü System[J]. Chaos Solitons & Fractals, 2004, 24(1): 221-227.

(下转第 264 页)