第 6 卷第 1 期 2008 年 3 月
1672-6553/2008/06(1)/040-5

动力学与控制学报
JOURNAL OF DYNAMICS AND CONTROL

Vol. 6 No. 1
Mar. 2008

单向耦合混沌同步及其在保密通信中的应用

王兴元[1]　古丽孜拉[1,2]　王明军[1]

(1. 大连理工大学电子与信息工程学院,大连　116024)(2. 新疆伊犁师范学院计算机科学与技术系,伊宁　835000)

摘要　采用单向耦合同步法,利用 Lyapunov 稳定性定理、全局同步法及最大 Lyapunov 指数法分别对 Lorenz 系统、变形耦合发电机系统及超混沌 Chen 系统的自同步进行了研究. 为适用于混沌保密通信,使用单路信号实现了驱动系统与响应系统的同步,并给出将超混沌 Chen 系统的自同步用于混沌掩盖保密通信的具体例子. 数值模拟验证了所给方案的有效性.

关键词　耦合同步法,　混沌同步,　Lyapunov 稳定性定理,　全局同步法,　最大 Lyapunov 指数,　混沌掩盖

引言

1990 年,Pecora 和 Corroll 首次提出了“混沌同步”的概念,并在电路实验中实现了两个耦合混沌系统的同步[1,2]. 由于混沌同步在保密通信、信号处理和生命科学等方面有着十分广泛的应用前景和巨大的市场潜在价值,引起了人们极大的关注,并对此进行了广泛而深入地研究[3,5]. 其中,Muradi 和 Kapitaniak 等推广了 Corroll 和 Pecora 的工作,提出了单向耦合同步法,即通过单向状态变量的耦合实现两个相同的混沌系统的自同步[6,7]. 此后,针对不同的混沌系统,人们使用不同的方法实现了混沌同步[8-11],一些学者还对混沌保密通信进行了研究[12,13]. 如,Kocarev 和 Cuomo 等采用混沌掩盖法以掩盖传输信息[14,15];Dedieu 等利用混沌健控法来产生传输信号[16];Halle 和 Itoh 等采用混沌调制法用于保密通信[17-19]. 在上述研究基础上,本文采用单向耦合同步法,利用 Lyapunov 稳定性定理及最大 Lyapunov 指数法分别实现了 Lorenz 系统和超混沌 Chen 系统的单路信号自同步,给出了超混沌 chen 系统用于混沌保密通信的具体例子.

1　混沌系统的单向耦合同步

设某混沌系统表示为

$$\dot{X}=F(X)$$

则由该系统作为驱动系统和响应系统组成的单向耦合的动力学方程组表示为:

$$\begin{cases}\dot{X}_1=F(X_1)\\ \dot{X}_2=F(X_2)+\alpha E(X_1-X_2)\end{cases}\tag{1}$$

E 是一个矩阵,它是确定响应系统与驱动系统变量差的线性组合,α 是耦合强度或反馈系数,通常情况下取 $\alpha E=\mathrm{diag}(k_1,k_2,\cdots,k_n)$($n$ 为变量的个数). 式(1)中两个方程的相应变量差可定义为误差系统:

$e=X_2-X_1$,这里考虑 e 是很小的值,其解取决于误差系统的稳定性. 若驱动系统传递给响应系统的信号能在单路信道中实现,则对保密通信的实现具有重要意义. 下文以 Lorenz 系统为例进行说明.

设具有相同表示形式的两个 Lorenz 系统[20]分别作为驱动系统

$$\begin{cases}\dot{x}_1=a(y_1-x_1)\\ \dot{y}_1=cx_1-y_1-x_1z_1\\ \dot{z}_1=x_1y_1-bz_1\end{cases}\tag{2}$$

和响应系统

$$\begin{cases}\dot{x}_2=a(y_2-x_2)-k_1(x_2-x_1)\\ \dot{y}_2=cx_2-y_2-x_2z_2\\ \dot{z}_2=x_2y_2-bz_2\end{cases}\tag{3}$$

这里 k_1 是反馈增益. 则可得误差系统为

$$\begin{cases}\dot{e}_1=a(y_2-x_2)-a(y_2-x_1)-k_1(x_2-x_1)=-(k_1+a)e_1+ae_2\\ \dot{e}_2=cx_2-cx_1+y_1+x_1z_1-y_2-x_2z_2=(c-z_1)e_1-e_2-x_1e_3-e_1e_3\\ \dot{e}_3=x_2y_2-x_1y_1-bz_2+bz_1=y_1e_1+x_1e_2-be_3+e_1e_2\end{cases}\tag{4}$$

2007-04-08 收到第 1 稿,2007-06-30 收到修改稿.
* 国家自然科学基金(60573172)及辽宁省教育厅高等学校科学技术研究项目(20040081)资助

选取 Lyapunov 函数为

$$V(t)=\frac{1}{2}(e_1^2+e_2^2+e_3^2) \tag{5}$$

对式(5)求导,可得

$$\dot{V}(t)=e_1\dot{e}_1+e_2\dot{e}_2+e_3\dot{e}_3 \tag{6}$$

将式(4)代入式(6),整理后可得

$$\dot{V}(t)=-(k_1+a-\frac{y_1^2}{4b}-\frac{1}{4}(a+c-z_1)^2)e_1^2-$$

$$(e_2-\frac{1}{2}(a+c-z_1)e_1)^2-(\sqrt{b}e_3-\frac{y_1}{2\sqrt{b}}e_1)^2$$

显然 $V(t)\geq 0$,若满足

$$k_1>\frac{y_1^2}{4b}+\frac{1}{4}(a+c-z_1)^2-a \tag{7}$$

则 $\dot{V}(t)\leq 0$. 由 Lyapunov 稳定性定理可知误差系统(4)是渐进稳定的,即驱动系统(2)与响应系统(3)可渐进地达到同步. 图 1 为 Lorenz 吸引子在 $y-z$ 平面上的投影,因为 y_1 和 z_1 都是有界的,所以只要 k_1 足够大即可满足式(7).

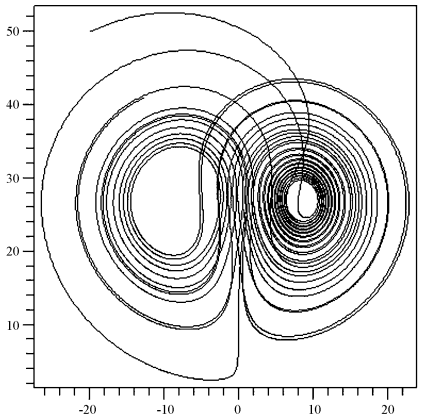

图 1　Lorenz 吸引子在 $y-z$ 平面上的投影

Fig. 1　The projection of the attractor of Lorenz system in the plane of $y-z$

数值仿真实验中,选取时间步长为 $\tau=0.001$ (sec),采用四阶 Runge-Kutta 法去求解方程(2)和(3). 驱动系统(2)与响应系统(3)的初始点分别选取为:$x_1(0)=-15$、$y_1(0)=-20$ 和 $z_1(0)=50$,$x_2(0)=20$、$y_2(0)=30$ 和 $z_2(0)=1$. 因此误差系统(4)的初始值为 $e_1(0)=35$、$e_2(0)=50$ 和 $e_3(0)=-49$. 为使驱动系统处于混沌状态,选取参数 $a=10$、$b=8/3$ 和 $c=28$[20]. 根据图 1 中 Lorenz 吸引子在 $y-z$ 平面投影的取值范围,令 $k_1=500$ 即可满足式(7). 图 2 为驱动系统(2)和响应系统(3)的同步过程模拟结果. 由误差效果图 2 可见,当接近 3 $(sec.)$、4$(sec.)$和 4$(sec.)$时,误差 $e_1(t)$、$e_(t)$和 $e_3(t)$分别基本稳定在零点附近. 即当 $k_1=500$ 时,驱动系统(2)与响应系统(3)渐进达到同步.

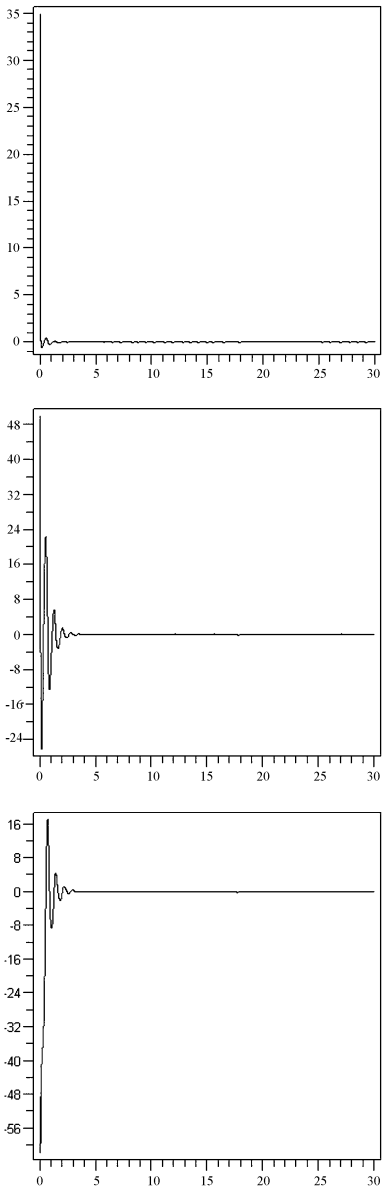

图 2　系统(2)和系统(3)的同步误差曲线

Fig. 2　Error system states of system(2) and system(3)

混沌系统进行耦合同步时往往很难找到合适的 Lyapunov 函数并证明其有效性,因此下面将使用计算最大 Lyapunov 指数的方法. 当误差系统的最大 Lyapunov 指数小于零,响应系统将会与驱动系统达到同步.

2　利用单路组合信号实现超混沌系统单向耦合同步及混沌保密通信的实例

为提高系统的保密性,建议使用高维超混沌系

统来代替低维混沌系统来实现保密通信. 由于高维超混沌系统具有多个正的 Lyapunov 指数,系统的动态行为更加难以预测,因此具有更高的保密性. Pyragas 曾提出猜测:反馈变量的最小个数应与系统正性 Lyapunov 指数的个数相同. 也就是说超混沌系统需要发送多路信号才能使响应系统与其同步,对此 Peng 等提出了发送单路组合信号的改进办法[21],成功实现了超混沌 Rössler 系统的同步控制. 本文也将采用这一方法,实现对超混沌 Chen 系统的单向耦合同步.

设具有相同表示形式的两个超混沌 *Chen* 系统[22,23]分别作为驱动系统

$$\begin{cases}\dot{x}_1 = a(y_1 - x_1) + w_1\\ \dot{y}_1 = dx_1 - x_1z_1 + cy_1\\ \dot{z}_1 = x_1y_1 - bz_1\\ \dot{w}_1 = y_1z_1 + rw_1\end{cases} \tag{8}$$

和响应系统

$$\begin{cases}\dot{x}_2 = a(y_2 - x_2) + w_2\\ \dot{y}_2 = dx_2 - x_2z_2 + cy_2 - ku_1\cos\theta\\ \dot{z}_2 = x_2y_2 - bz_2 - ku_1\sin\theta\\ \dot{w}_2 = y_2z_2 + rw_2\end{cases} \tag{9}$$

这里 k 是反馈增益,控制器 $u_1 = \sin\theta(y_2 - y_1) + \cos\theta(z_2 - z_1)$ $(0 \le \theta < \pi/2)$,即驱动系统(8)只需要发送 $y_1\sin\theta + z_1\cos\theta$ 这一路信号给响应系统(9)即可. 应用 Peng 等的办法进行计算[21],可得到当 $k = 3$, $\theta = 7\pi/24$,驱动系统(8)与响应系统(9)可以达到同步.

下面以超混沌 chen 系统为例说明混沌掩盖保密通信系统原理. 这里采用 Milanovic 和 Zaghloul 改进后的混沌掩盖保密通信系统方案[24],图 3 为其原理图. 假设 $m(t)$ 为有用信号,$u(t)$ 为驱动系统发出的信号,则信道中信号为 $s(t) = u(t) + m(t)$,同时要由 $m(t)$ 产生信号使驱动系统变为非自治系统;响应系统输出 $v(t)$,恢复出来的有用信号 $\hat{m}(t) = s(t) - v(t)$.

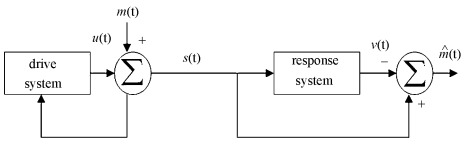

图 3 改进后的混沌掩盖保密通信系统方案原理图

Fig. 3 Pictorial diagram of the improved chaotic masking method

以超混沌 chen 系统为例,此时驱动系统变为

$$\begin{cases}\dot{x}_1 = a(y_1 - x_1) + w_1\\ \dot{y}_1 = dx_1 - x_1z_1 + cy_1 + km(t)\cos\theta\\ \dot{z}_1 = x_1y_1 - bz_1 + km(t)\sin\theta\\ \dot{w}_1 = y_1z_1 + rw_1\end{cases} \tag{10}$$

响应系统变为

$$\begin{cases}\dot{x}_2 = a(y_2 - x_2) + w_2\\ \dot{y}_2 = dx_2 - x_2z_2 + cy_2 - ku_1\cos\theta + km(t)\cos\theta\\ \dot{z}_2 = x_2y_2 - bz_2 - ku_1\sin\theta + km(t)\sin\theta\\ \dot{w}_2 = y_2z_2 + rw_2\end{cases} \tag{11}$$

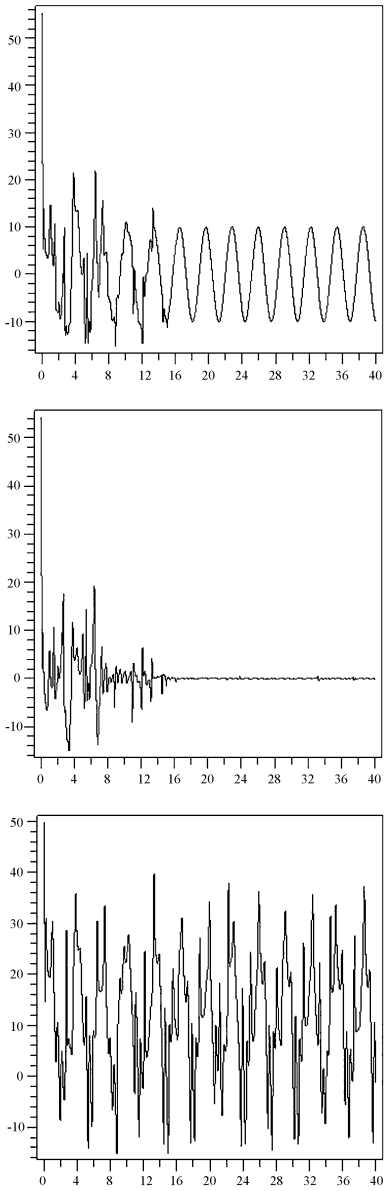

图 4 超混沌 chen 系统同步保密通信的模拟结果

Fig. 4 The simulation results of the chaotic masking secure communication using Hyperchaotic *Chen* system

这里 k 是反馈增益,则误差系统为

$$\begin{cases} \dot{e}_1 = -ae_1 + ae_2 + e_4 \\ \dot{e}_2 = (d - z_1)e_1 + (c - k\cos\theta\sin\theta)e_2 - \\ \quad (x_1 + k\cos\theta\cos\theta)e_3 - e_1e_3 \\ \dot{e}_3 = y_1e_1 + (x_1 - k\sin\theta\sin\theta)e_2 - \\ \quad (b + k\cos\theta\sin\theta)e_3 + e_1e_2 \\ \dot{e}_4 = z_1e_2 + y_1e_3 + re_4 + e_2e_3 \end{cases} \tag{12}$$

由于有用信号 $m(t)$ 直接融入到发射系统和接收系统中,因此它可以取比较大的强度. 令 $k = 3, \theta = 7\pi/24$,所有参数以及系统初始状态的取值与前述相同. 将 $s(t) = u(t) + m(t) = y_1\sin\theta + z_1\cos\theta + m(t)$, $v(t) = y_2\sin\theta + z_2\cos\theta$,代入 $\hat{m}(t) = s(t) - v(t)$,可得到 $\hat{m}(t)$,恢复信号的误差值 $e(t) = \hat{m}(t) - m(t)$.

图 4 为仿真结果. 其中图 4(*a*) ~4(*c*)分别给出了恢复信号、误差信号和信道中信号随时间的变化曲线. 由图 4 可见,当接近 17(*sec.*)时,有用信号基本得到了恢复. 由于超混沌系统动态行为更加难以预测,驱动系统(10)发送的又是组合信号,所以隐蔽性更好,即使有用信号是较强的周期信号也不易从中寻找规律. 同时由于混沌载波与有用信号融为一体,在不破坏原驱动系统混沌性质的前提下可以使用较大强度的有用信号,也可以使系统同步对噪声具有较好的鲁棒性.

3　结论

本文采用单向耦合同步法,利用 Lyapunov 稳定性定理及最大 Lyapunov 指数法分别对 Lorenz 系统和超混沌 Chen 系统的自同步进行了研究,使用单路信号实现了驱动系统与响应系统的同步,并给出将超混沌 Chen 系统的自同步用于混沌掩盖保密通信的具体例子;数值模拟进一步验证了所给方案的有效性.

参　考　文　献

1　Pecora L M, Carroll T L. Synchronization of chaotic systems. *Physical Review Letters*, 1990, 64 (8): 821 ~ 830

2　Carroll T L, Pecora L M. Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems*, 1991, 38(4): 453 ~ 456

3　王光瑞,于熙龄,陈式刚. 混沌的控制、同步与利用. 北京:国防工业出版社,2001 (Wang G R, Yu X L, Chen S G. Chaotic control, synchronization and utilizing. Beijing: National Defence Industry Press, 2001 (in Chinese))

4　王兴元. 复杂非线性系统中的混沌. 北京:电子工业出版社,2003 (Wang X Y. Chaos in the complex nonlinearity system. Bejjing: Electronics Industry Press, 2003 (in Chinese))

5　陈关荣,吕金虎. Lorenz 系统族的动力学分析、控制与同步. 北京:科学出版社,2003 (Chen G R, Lü J H. Dynamical analyses, control and synchronization of the lorenz system family . Beijing: Science Press, 2003 (in Chinese))

6　Murali K, Lakshmanan M. Chaos in nonlinear oscillators controlling and synchronization. Singapore: World Scientific, 1996

7　Kapitaniak T. Controlling chaos: Theoretical and practical methods in nonlinear dynamics. London: Academic Press, 1996

8　陈保颖,包芳勋. 连续混沌系统的混沌同步控制. 动力学与控制学报,2004,2(4):16 ~ 20 (Chen B Y, Bao F X. Chaos synchronization control of continuous chaotic systems. *Journal of Dynamics and Control*, 2004, 2(4): 16 ~ 20 (in Chinese))

9　陈保颖. 线性反馈实现 Liu 系统的混沌同步. 动力学与控制学报,2006,1(1): 1 ~4 (Chen B Y. Linear feedback control for synchronization of Liu chaotic system. *Journal of Dynamics and Control*, 2006, 1(1): 1 ~4 (in Chinese))

10　高洁,陆君安. 不确定参数下的四维超混沌吕系统的最优同步. 动力学与控制学报,2006,4(4): 320 ~ 325 (Gao J, Lu J A. Optimal synchronization of hyperchaotic Lü system with uncertain parameters. *Journal of Dynamics and Control*, 2006, 4(4): 320 ~ 325 (in Chinese))

11　单梁,李军. 参数不确定 Liu 混沌系统的自适应同步. 动力学与控制学报,2006,4(4): 338 ~ 343 (Shan L, Li J. Adaptive synchronization of Liu Chaotic system with uncertain parameters. *Journal of Dynamics and Control*, 2006, 4(4): 338 ~ 343 (in Chinese))

12　Li Z G, Xu D L. A secure communication scheme using projective chaos synchronization. *Chaos, Solitons & Fractals*, 2004, 22(2): 477 ~ 481

13　Lu J G. Multiple access chaotic digital communication based on generalized synchronization. *Chaos, Solitons & Fractals*, 2005, 25(1): 221 ~ 227

14　Kocarev L, Halle K S, Eckert K, et al. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Cha-*

os, 1993, 2(3): 709 ~ 713

15 Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of lorenzed – based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems – II*, 1993; 40(10): 626 ~ 633

16 Dedieu H, Kennedy M P, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self – synchronizing chua's circuit. *IEEE Transactions on Circuits and Systems – II*, 1993; 40(10): 634 ~ 642

17 Halle K S, Wu C W, Itoh M, et al. Spread spectrum communications through modulation of chaos. *International Journal of Bifurcation and Chaos*, 1993, 3(1): 469 ~ 477

18 Itoh, M, Murakami H. New communication systems via chaotic synchronizations and modulations. *IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences*, 1995, E78 – A(3): 285 ~ 290

19 Itoh M, Wu C W, Chua L O. Communication systems via chaotic signals from a reconstruction viewpoint. *International Journal of Bifurcation and Chaos*, 1997, 7(2): 275 ~ 286

20 Lorenz E N. Deterministic nonperodic flow. *J Atmos Sci*, 1963, 20: 130 ~ 141

21 Peng J H, Ding E J, Ding M etc. Sychronizing hyperchaos with a scalar transmitted signal. *Phys Rev Lett*, 1996, 76(6): 904 ~ 907

22 Li Y X, Tang W K S, Chen G R. Generating hyperchaos via state feedback control. *International Journal of Bifurcation and Chaos*, 2005, 15(10): 3367 ~ 3375

23 Yan Z Y. Controlling hyperchaos in the new hyperchaotic Chen system. *Applied Mathematics and Computation*, 2005, 168(2): 1239 ~ 1250

24 Mianovic V, Zaghloul M E. Improved masking algorithm chaotic communication systems. *Electronic Lett*, 1996, 1: 11 ~ 12

CHAOS SYNCHRONIZATION VIA UNIDIRECTIONAL COUPLING AND ITS APPLICATION TO SECURE COMMUNICATION

Wang Xingyuan[1] Gulzila[1,2] Wang Mingjun[1]

(1. *School of Electronic & Information Engineering*, *Dalian University of Technology*, *Dalian* 116024, *China*)

(2. *Department of Computer Science & Technology*, *Xinjiang Yili Normal Collage*, *Yining* 835000, *China*)

Abstract This paper studied chaos synchronization via unidirectional coupling. The self – synchronization of Lorenz system, modified coupled dynamos system and hyperchaotic Chen system was studied by three methods: the Lyapunov stability method, the global synchronization method, and the numerical calculation of the largest Lyapunov exponent method. In regard to application to communication, we show that, by transmitting single signal, one can achieve synchronization of the drive system and the response system. An example of applying self – synchronization of hyperchaotic Chen systems to chaotic masking secure communication was addressed. Simulation results show the effectiveness of the method.

Key words synchronization via coupling, chaos synchronization, Lyapunov stability theory, global synchronization, the largest Lyapunov exponent, chaotic masking

Received 8 April 2007, revised 30 June 2007.

* The project supported by the National Natural Science Foundation of China (60573172) and Superior University Science Technology Research Project of Liao Ning province (20040081)