doi: 10.3969/j.issn.1006-1576.2011.03.014

超 Lorenz 混沌系统的同步及其在保密通信中的应用

于茜，罗永健，史德阳，吴刚
（西安通信学院 研究生管理大队，西安 710106）

摘要：为了加密并准确解密传输的信息，将超 Lorenz 混沌系统的同步应用在保密通信中。基于线性稳定性定理，对超五阶 Lorenz 系统实现了超混沌系统的输出反馈控制同步，设计了超混沌系统的输出反馈控制器，实现了响应系统与驱动系统的同步，并将同步的混沌系统应用到混沌掩盖保密通信中。仿真结果表明，超 Lorenz 混沌系统能够快速达到同步，且在混沌掩盖通信方案中，有用信号可以有效地在接收端恢复出来。

关键词：反馈控制；超五阶 Lorenz 系统；混沌同步；混沌掩盖
中图分类号：TN918; O231　　**文献标志码**：A

Synchronization of Hyper Chaotic Lorenz System and Its Application in Secure Communications

Yu Qian, Luo Yongjian, Shi Deyang, Wu Gang
(Administrant Brigade of Postgraduate, Xi'an Communications Institute, Xi'an 710106, China)

Abstract: In order to encrypt and decrypt exactly the transformed information, the synchronization of hyper chaotic Lorenz system was proposed to realize secure communications. Based on the linear system stability theory, an output feedback controller was designed to get the output feedback controlling synchronization of hyper chaotic Lorenz system. Also, the synchronized system was used in chaos masking approach. Simulation results show that the synchronization of hyper chaotic Lorenz system was realized fast, and the useful signal can be recovered from the receiver effectively.

Keywords: feedback control; hyper chaotic Lorenz system; chaos synchronization; chaos masking

0　引言

利用混沌进行保密通信大致分为 3 大类[1]：1) 直接利用混沌进行保密通信；2) 利用同步的混沌进行保密通信；3) 混沌数字编码的异步通信。其中，利用同步的混沌进行保密通信是国际上研究的一大热点，正在发展为高新技术的一个新领域。混沌系统对初始条件极为敏感的特性使得人们认为混沌是不能同步的，直到 20 世纪 90 年代初期，混沌系统才出现了同步的契机，其主要标志是 1990 年美国马里兰大学的 Ott、Grebogi 和 Yorke 提出了混沌控制技术。同年，美国海军实验室的 Pecora，Carroll 发现了混沌电路中的自同步现象[2]。他们发现，如果复制一个自治混沌系统的适当子系统，只要子系统的李雅普诺夫指数为负，那么响应系统的混沌信号很快和驱动系统中相应的混沌信号同步。其后，国际上形成了混沌同步技术的研究热潮，并掀起了混沌同步技术在保密通信中的应用研究热潮。此后，许多学者对混沌系统同步做了深入的研究。其中，L. Kocarev 等针对 Pecora 和 Carroll 的研究提出了改进方法，称为主动-被动同步法，该方法采取十分灵活的分解法，将原系统改写成含有某种驱动变量的非自治系统形式，复制相同的响应系统，通过线性化方法或李雅普诺夫函数方法分析 2 个系统的误差，证明它们达到同步；Muradi 和 Kapitaniak 等提出了单向耦合同步法，即通过一个单向状态变量的耦合实现 2 个相同系统的混沌同步；Nijmeijer 提出了一种观测器设计方法[3]，将混沌同步问题看作是观测器设计问题，利用非线性观测器设计理论来确定反馈增益的同步条件。但现有文献大多针对低维混沌系统开展研究，对超混沌系统的研究不多，而且大多仅证明出混沌系统可同步，且给出同步条件，并未将其应用到保密通信系统中，对实际应用研究不足。笔者针对超五阶 Lorenz 混沌系统，利用线性稳定性理论，实现混沌系统的反馈控制同步，并将同步的超混沌系统应用到混沌掩盖保密通信方案中。

1　反馈控制同步理论分析

假设混沌系统的系统方程为：

$$\begin{cases}\dot{x}=f(x)\\ y=\boldsymbol{C}x\end{cases} \tag{1}$$

其中，$x\in R^n, y\in R^n$，y 为系统的输出，$\boldsymbol{C}$ 为输出增益矩阵。

线性输出反馈控制的响应系统具有如下形式：

收稿日期：2010-10-30；修回日期：2010-12-19
作者简介：于茜（1986—），女，河北人，研究生，从事保密通信研究。

$$\begin{cases} \dot{x}_r = f(x_r) + Ke(t) \\ y_r = \boldsymbol{C}x_r \\ e(t) = y(t) - y_r(t) \end{cases} \tag{2}$$

其中，K 为反馈控制增益，$e(t) = y(t) - y_r(t)$ 为误差向量。

由式 (2) 可以看出，只要选择适当的反馈控制增益 K，就可以使得 $\lim\limits_{t\to\infty} e(t) = 0$，即 $x_r \to x$，即驱动系统和响应系统达到同步。

2 基于线性输出反馈控制的超 Lorenz 系统的同步分析

2.1 超 Lorenz 混沌系统的提出

著名的 Lorenz 系统是美国气象学家 Edward Lorenz 于 1963 年提出来的，其方程为：

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 &= x_1 x_2 - b x_3 \end{aligned} \tag{3}$$

当 $\sigma = 10$，$b = \dfrac{8}{3}$，$\rho = 28$ 时，Lorenz 系统处于混沌状态。在式 (3) 的第一个方程右端引入控制器 x_4 和 x_5，第 2、3 个方程右端引入控制器 x_5，并令 x_4 和 x_5 的变化律分别为 $\dot{x}_4 = -x_2 x_3 + c x_4$ 和 $\dot{x}_5 = -3x_1$，则产生新的系统为：

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1) + x_4 + x_5 \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3 + x_5 \\ \dot{x}_3 &= x_1 x_2 - b x_3 + x_5 \\ \dot{x}_4 &= -x_2 x_3 + c x_4 \\ \dot{x}_5 &= -3x_1 \end{aligned} \tag{4}$$

产生超混沌的必要条件是系统具有耗散性结构，维数至少等于 4，系统具有至少 2 个正的 Lyapunov 指数。仍然让 $\sigma = 10$，$b = \dfrac{8}{3}$，$\rho = 28$，只有当梯度函数（能量函数）

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} + \frac{\partial \dot{x}_4}{\partial x_4} + \frac{\partial \dot{x}_5}{\partial x_5} = c - 13.667 < 0$$

时，才满足耗散性结构，也才有可能产生超混沌行为。参数 c 的上限是 13.667，对 c 取不同的值，文献[5]得到：当 $c = -6$ 时，式 (4) 的 Lyapunov 指数分别为 $L_1 = 0.239\,2$，$L_2 = 0.177\,3$，$L_3 = 0$，$L_4 = -4.539$，$L_5 = -15.72$，可见式 (4) 产生了超混沌行为。

2.2 超 Lorenz 混沌系统反馈控制的同步分析

将式 (4) 作为驱动系统，设计反馈控制器，响应系统为：

$$\begin{aligned} \dot{y}_1 &= \sigma(y_2 - y_1) + y_4 + y_5 + u_1 \\ \dot{y}_2 &= \rho y_1 - y_2 - y_1 y_3 + y_5 + u_2 \\ \dot{y}_3 &= y_1 y_2 - b y_3 + y_5 + u_3 \\ \dot{y}_4 &= -y_2 y_3 + c y_4 + u_4 \\ \dot{y}_5 &= -3y_1 + u_5 \end{aligned} \tag{5}$$

在反馈控制器 $\boldsymbol{u} = [u_1, u_2, u_3, u_4, u_5]^{\mathrm{T}}$ 作用下，响应系统和驱动系统可实现同步。

如果选择 $u_1 = 0$，$u_3 = x_1 x_2 - y_1 y_2$，$u_2 = y_1 y_3 - x_1 x_3 - 56(y_1 - x_1)$，$u_4 = y_2 y_3 - x_2 x_3$，$u_5 = -(y_5 - x_5)$，式 (4) 和式 (5) 取得同步。下面证明这一结论的正确性。

令 $e_1 = y_1 - x_1$，$e_2 = y_2 - x_2$，$e_3 = y_3 - x_3$，$e_4 = y_4 - x_4$，$e_5 = y_5 - x_5$，得到驱动式 (4) 和响应式 (5) 的误差系统方程为：

$$\begin{aligned} \dot{e}_1 &= -10e_1 + 10e_2 + e_4 + e_5 \\ \dot{e}_2 &= -28e_1 - e_2 + e_5 \\ \dot{e}_3 &= -\tfrac{8}{3} e_3 + e_5 \\ \dot{e}_4 &= -6e_4 \\ \dot{e}_5 &= -3e_1 - e_5 \end{aligned} \tag{6}$$

显然，$e_i = 0(i = 1,2,3,4,5)$ 是误差式 (6) 的平衡点。式 (6) 在平衡点处的 Jacobi 矩阵为：

$$\boldsymbol{J} = \begin{bmatrix} -10 & 10 & 0 & 1 & 1 \\ -28 & -1 & 0 & 0 & 1 \\ 0 & 0 & -\frac{8}{3} & 0 & 1 \\ 0 & 0 & 0 & -6 & 0 \\ -3 & 0 & 0 & 0 & -1 \end{bmatrix}$$

令 $\det(\boldsymbol{J} - \lambda \boldsymbol{I}) = 0$，解得特征值为：$\lambda_1 = -2.666\,7$，$\lambda_{2,3} = -5.446\,8 \pm 16.195\,1i$，$\lambda_4 = -1.106\,4$，$\lambda_5 = -6$。可见，所有的特征值都具有负实部，由动力学系统的稳定性理论可以得到：平衡点 $e_i = 0(i = 1,2,3,4,5)$ 是式 (6) 的渐近稳定平衡点，故有 $\lim\limits_{t\to\infty} e_i = 0(i = 1,2,3,4,5)$ 成立，即有 $\lim\limits_{t\to\infty}(y_1 - x_1) = 0$，$\lim\limits_{t\to\infty}(y_2 - x_2) = 0$，$\lim\limits_{t\to\infty}(y_3 - x_3) = 0$，$\lim\limits_{t\to\infty}(y_4 - x_4) = 0$，$\lim\limits_{t\to\infty}(y_5 - x_5) = 0$ 成立，所以响应式 (5) 和驱动式 (4) 可以取得混沌同步。

3 超 Lorenz 系统混沌掩盖保密通信

混沌掩盖通信是最早研究的混沌保密通信[4]，Oppenheim、Kocarev 等人在 1992 年提出了混沌掩盖通信技术，它利用了 Pecora-Carroll 自同步原理。混沌掩盖的基本原理是：利用具有逼近于高斯白噪声统计特性的混沌信号作为一种载体，来掩藏信号所要传送的信息，即在通信时，发送端将信息作为小信号附着在混沌载波上，在接收端与发送端实现同步后，对混沌信号进行去掩盖，从而恢复出有用的信息。

根据混沌掩盖保密通信原理，把 2.2 节实现同步

的 2 个超 Lorenz 混沌系统应用于保密通信中。设需要传输的信息信号是 $m(t)=0.1\sin t$，则在发送端将有用信号与混沌信号 $x_5(t)$ 相加，输出类噪声信号 $s(t)=m(t)+x_5(t)$。

发送端的驱动系统如下：

$$\begin{aligned}\dot{x}_1&=\sigma(x_2-x_1)+x_4+x_5\\ \dot{x}_2&=\rho x_1-x_2-x_1x_3+x_5\\ \dot{x}_3&=x_1x_2-bx_3+x_5\\ \dot{x}_4&=-x_2x_3+cx_4\\ \dot{x}_5&=-3x_1+m(t)\end{aligned}\tag{7}$$

式 (5) 在反馈控制器 $\boldsymbol{u}$ 的作用下得到响应系统：

$$\begin{aligned}\dot{y}_1&=\sigma(y_2-y_1)+y_4+y_5\\ \dot{y}_2&=\rho y_1-y_2+y_5-x_1x_3-56(y_1-x_1)\\ \dot{y}_3&=-by_3+y_5+x_1x_2\\ \dot{y}_4&=cy_4-x_2x_3\\ \dot{y}_5&=-3y_1-(y_5-s)\end{aligned}\tag{8}$$

在接收端混沌信号为 $y_5(t)$，只需从 $s(t)$ 中减去响应系统中产生的混沌信号 $y_5(t)$，就可获得还原的有用信号 $m'(t)=s(t)-y_5(t)$，原始信号与还原信号的信号误差为 $e(t)=m(t)-m'(t)$。

4　仿真分析

将驱动系统和响应系统的初始条件设为 $[3\ \ 2\ \ 1\ \ 2\ \ 3]^{\mathrm{T}}$ 和 $[30\ \ 20\ \ 10\ \ 20\ \ 30]^{\mathrm{T}}$，应用四阶龙格—库塔法，在响应式 (5) 被施加反馈控制后，系统得到同步误差变量 $e_i(i=1,2,3,4,5)$ 随时间 t 变化的特性曲线，如图 1。

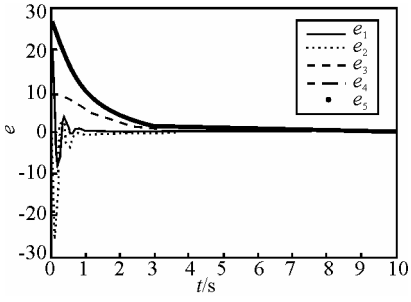
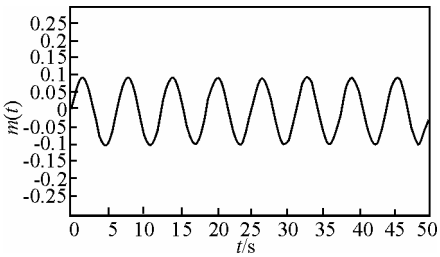


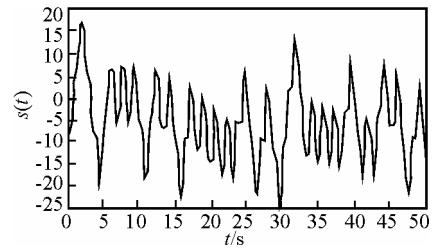
图 1　超 Lorenz 混沌系统同步的误差曲线

仿真结果表明，在反馈控制器 $\boldsymbol{u}=[u_1,u_2,u_3,u_4,u_5]^{\mathrm{T}}$ 的作用下，响应系统能够迅速和驱动系统达到同步，由图 1 可以看出，在 5 s 之内驱动系统的状态和响应系统的状态可以达到同步，并且同步误差小于 0.01，仿真 10 s 以后，同步误差的数量级是 10^{-6}。

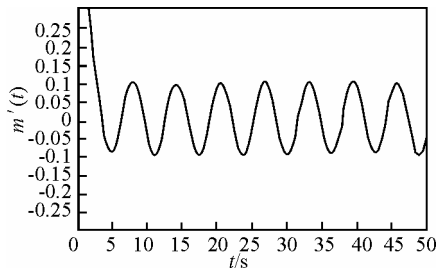
在发送端加入小信号 $m(t)=0.1\sin t$ 后，得到混沌掩盖保密通信的仿真曲线如图 2。



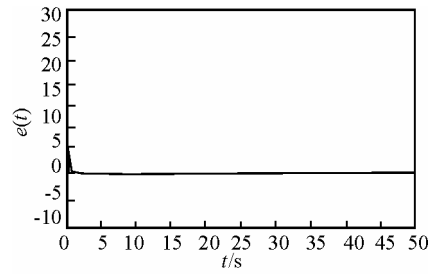
(a) 信息信号 $m(t)$



(b) 发送端发射信号 $s(t)$



(c) 接收端恢复信号 $m'(t)$



(d) 发送端与接收端信号的误差 $e(t)$

图 2　混沌掩盖保密通信仿真结果

从图 2 可以看出，仿真 8 s 后，有用信号与解调出来的恢复信号的误差几乎为 0，即在接收端，有用信号能够在很短的时间内较好地恢复出来。根据混沌信号的性能特性，说明该通信方案有一定的安全性。

5　结论

仿真结果表明，超 Lorenz 混沌系统能够快速达到同步，且在混沌掩盖通信方案中，有用信号可以有效地在接收端恢复出来。但在实际应用中，混沌系统的参数会随着环境的变化而变化，从而会加大混沌系统的同步难度，因此，下一步还需要对不确定参数混沌系统的同步方法进行深入研究。

（下转第 50 页）

7) DOS 和 DDOS 攻击

DOS 攻击，即拒绝服务攻击。通过向服务器发送超负荷的服务请求，耗尽服务器系统资源，使其失去响应正常服务请求的能力。随着硬件技术的发展，服务器的运算能力越来越强，单靠一台或几台计算机 DOS 攻击已经不能拖垮服务器，已经很少使用。因此，出现了 DDOS 攻击，即分布式拒绝服务攻击。攻击者远程遥控成千上万的计算机向目标服务器发起 DOS 攻击。攻击者先要以入侵并植 DDOS 控制软件的方式，控制大量的计算机，在需要攻击时，再通过控制台发送控制指令遥控受控计算机攻击目标。这种攻击的难点是：如何入侵大量计算机？如何管理这些计算机？一般情况下，攻击者为了快速控制大量计算机，使用网络病毒携带 DDOS 控制软件在网上传播，或者使用批量漏洞扫描软件，进行批量入侵。再设置一台 DDOS 服务器管理所有“受控计算机”。因此，防范这种攻击的方式是通过网管监控网络流量异常，发现和制止批量入侵，阻止更多的计算机被控制，并同步检测出 DDOS 服务器的 IP 地址和位置，对该服务器进行安全处理。

3 军网安全防护工作的注意事项

1) 防火墙并非万能

病毒防火墙。不能过于迷信杀毒软件。网络上是先有病毒，而且这个病毒足够“嚣张”以致被杀毒软件的病毒监测网络捕获到样本，然后工程师们从样本中提取“特征码”并导入病毒库，杀毒软件才能查杀。所以病毒总是先于杀毒软件一周或更长时间流行。一些特制的流行不广的病毒很可能逃脱监控，在杀毒软件的眼皮底下搞破坏。网络防火墙。没有攻不破的防火墙，计算机上安装的防火墙都是简单的基于 IP 规则检测的软件防火墙，阻止来自外部的非授权连接，并检测本地监听端口，判断是否存在木马程序，对计算机起到一定的保护作用，但这种保护非常有限。“端口反弹”技术可以轻松破除这种防火墙，木马程序通过“进程注入”加载到 IE 进程空间中，打着 IE 的伪装，从防火墙内部向外连接，从而顺利突破防火墙。

2) 网络安全人人有责

网络安全并不完全是管理员的事，每个人都要管好自己的计算机，不要让自己的计算机沦为攻击者的帮凶。目前网络上被成功入侵的计算机，90% 以上是用户缺乏安全意识，没有设密码、打补丁的习惯。批量扫描软件上只要设置一下要扫描的网段，不到几分钟，就能检测到大量存在问题的计算机。这些不是单靠管理员能解决的，设密码、打补丁不是很能难的技术问题，关键是用户自己要提高安全防护的意识。

3) 用好 Windows

近年来，Windows 的安全性一直被诟病，可是事实上 Windows 是一个优秀的操作系统，安全性并不差，只是没有用好它，多数人根本不知道如何进行 Windows 安全设置，对 Windows 的一些高级设置更是所知甚少。要真正用好 Windows 必须要深入掌握控制面板、组策略管理、CMD 命令行等。

4 结束语

研究表明，分析军网自身存在的安全漏洞，掌握敌方网络攻击手段，有针对性地采用军网安全防护措施，能有效阻止网络攻击，对做好军网安全防护工作意义重大。

参考文献：

[1] 连一峰, 王航. 网络攻击原理与技术[M]. 北京: 科学出版社, 2004.
[2] 沈伟锋. 面向攻击的网络漏洞扫描[D]. 西安: 西北工业大学硕士学位论文, 2004.
[3] 马闯. 军网安全漏洞检测系统的研究与实现[D]. 吉林: 吉林大学硕士学位论文, 2008.
[4] 王晓飞. 基于入侵检测技术的军网安全模型分析[D]. 哈尔滨: 哈尔滨工业大学硕士学位论文, 2008.

****

（上接第 47 页）

参考文献：

[1] 赵耿, 郑德玲, 方锦清. 混沌保密通信的最新进展[J]. 自然杂志, 2001, 23(2): 97-106.
[2] L. M. Pecora, T. L. Carroll. The Synchronization in Chaotic Systems[J]. Physical Review Letters, 1990, 64(4): 821-830.
[3] H. Nijmeijer, M. Ymareels. An observer looks at synchronization[C]. IEEE Trans on Circuits Syst I, 1997, 44(10): 882-890.
[4] 方锦清. 驾驭混沌与发展高新技术[M]. 北京: 原子能出版社, 2002: 231-239.
[5] 李华青, 罗小华, 代祥光. 一个超混沌系统及其投影同步[C]. 电子学报, 2007, 37(3): 654-657.
[6] 申敏, 刘娟. Rossler 超混沌系统的同步及其在保密通信中的应用[J]. 重庆邮电大学学报, 2009, 21(3): 372-375.
[7] 王晓燕, 瞿少成, 等. 异结构混沌系统同步及其在保密通信中的应用[J]. 计算机应用研究, 2009, 26(5): 1874-1876.
[8] 张静, 等. MATLAB 在控制系统中的应用[M]. 北京: 电子工业出版社, 2007: 137-140.
[9] 求是科技. MATLAB 7.0 从入门到精通[M]. 北京: 人民邮电出版社, 2006.