神经网络的滞后同步及其在保密通信中的应用 *

穆文英, 籍 艳, 崔宝同
(江南大学 通信与控制工程学院, 江苏 无锡 214122)

摘 要: 针对参数不同、结构不同的带离散与分布时滞的混沌神经网络进行了研究。基于 Lyapunov 稳定性理论,提出了自适应滞后同步的控制方法,最后达到同步。仿真示例验证了本方案的有效性;同时应用于计算机保密通信可以掩盖有用信号,且可以无失真恢复有用信号。

关键词: 神经网络; 自适应同步; 时滞; 保密通信
中图分类号: TP273 **文献标志码**: A **文章编号**: 1001-3695(2010)09-3456-02
doi:10.3969/j.issn.1001-3695.2010.09.068

Lag synchronization of neural network and its application in secure communication

MU Wen-ying, JI yan, CUI Bao-tong
(*College of Communication & Control Engineering, Jiangnan University, Wuxi Jiangsu* 214122, *China*)

Abstract: This paper investigated the chaotic neural network of different parameters and different structures with discrete and distributed delays. Proposed an adaptive lag synchronization strategy based on Lyapunov stabilization theory, eventually achieved synchronization. Gave the simulation examples to verify the effectiveness of the proposed method. Apply this method to computer secure communization, the information signal can be concealed and recovered.

Key words: neural network; adaptive synchronization; time delay; secure communication

1990 年,Pecora 和 Carrol 首次提出驱动—响应混沌同步方法及混沌同步控制理论[1]。随后十几年里混沌系统的同步研究受到了极大关注,尤其是同步问题在保密通信方面的应用。至今,人们提出了各种不同的混沌同步方法,如驱动—响应同步、耦合同步、自适应同步、脉冲同步等。在混沌同步中,时滞系统的同步是一个值得关注的现象。文献[2]提出了带离散与分布时滞的神经网络的同步问题,但没有考虑系统结构和参数的变化;文献[3]采用了自适应方法同步两个不同的时滞神经网络,但没有考虑传输信道延迟的影响;文献[4]给出了一类不确定统一混沌系统的脉冲滞后同步;文献[5]实现了混沌系统同步方法在保密通信中的应用。

当混沌同步应用于计算机保密通信时,由于内部因素和外部不确定环境的干扰,驱动 - 响应系统的参数或结构在很多情况下并不相同,而且发射端的信号通过信道传输到接收端时将存在一个时间延迟,因此要求在同一时间内驱动端与响应端同步是不现实的。文献[6]重新定义了混沌同步系统在 $t-\tau$ 时刻的状态 $x(t-\tau)$ 与接收端在 t 时刻的状态 $y(t)$ 渐近同步,即当 $t\to\infty$ 时,$\lim \| x(t-\tau)-y(t) \| =0$。这种同步考虑到了传输信道时间延迟,更符合实际应用。但以前很少有涉及到这些方面的研究,研究这种结构不同参数不同的滞后同步更具有实际应用价值。本文基于 Lyapunov 稳定性理论,利用自适应同步控制法研究了一类带离散与分布时滞的神经网络的滞后同步问题。仿真结果验证了本文所提同步条件的正确性,并给出了在计算机保密通信中的应用。

1 问题描述

考虑如下带离散与分布时滞的神经网络作为驱动系统:

$$\dot{x}(t)=A_0x(t)+A_1f(x(t))+A_2f(x(t-\tau_1))+A_3\int_{t-\tau_2}^{t}f(x(s))\,\mathrm{d}s+I,t\geqslant 0 \tag{1}$$

若在传输中发射端的驱动系统(式(1))滞后 τ 时刻,则在 $t-\tau$ 时刻的状态 $x(t-\tau)$ 变为

$$\dot{x}(t-\tau)=A_0x(t-\tau)+A_1f(x(t-\tau))+A_2f(x(t-\tau_1-\tau))+A_3\int_{t-\tau_2-\tau}^{t-\tau}f(x(x))\,\mathrm{d}s+I,t\geqslant\tau \tag{2}$$

响应系统为

$$\dot{y}(t)=B_0y(t)+B_1g(y(t))+B_2g(y(t-\tau_1))+B_3\int_{t-\tau_2}^{t}g(y(s))\,\mathrm{d}s+u(t)+I,t\geqslant 0 \tag{3}$$

其中:$x(t)$ 与 $y(t)$ 分别为神经网络的状态变量;A_0、B_0 为对角矩阵;A_1,B_1,A_2,$B_2\in R^{n\times n}$ 为连接权重矩阵,A_3,$B_3\in R^{n\times n}$ 为分布时滞的连接权重矩阵;f、g 是非线性激励函数;I 是内部输入向量,$u(t)$ 是控制器输入。τ_1 与 τ_2 分别是离散与分布时滞,τ 是传输过程产生的时滞,其中 τ_1、τ_2、τ 都是大于零的常数。驱动系统的初始条件为 $x(t)=\varphi(t)C([-\max\{\tau_1,\tau_2\},0])$,响应系统的初始条件是 $y(t)=\psi(t)\in C([-\max\{\tau_1,\tau_2\},0])$。

假设 1 驱动—响应系统的状态向量是有界的,即 $\| x(t) \| \leqslant B_r$,$\| y(t) \| \leqslant B_u$,其中 B_r 与 B_u 为大于零的常数。

假设 2 非线性激励函数 f、g 满足 Lipschitz 条件:$\| f(x)-f(y) \| \leqslant L\| x-y \|$,$\| g(x)-g(y) \| \leqslant K\| x-y \|$。其中 L、K 为常数,且 $L>0$,$K>0$;$x,y\in R^n$ 且 $f(0)=0$,$g(0)=0$。

引理 1[5] Barbalat 引理。如果 $f(t)\in L_2\cap L_\infty$ 且 $\dot{f}(t)\in L_\infty$,则有 $\lim_{t\to\infty}f(t)=0$。其中:L_2 为所有平方可积函数,即满足 $\int_{-\infty}^{+\infty}\| x(t) \|^2\mathrm{d}t<+\infty$,$L_\infty$ 是满足 $\sup_w \bar{\delta}[f(jw)]<\infty$ 的函数矩阵 $F(jw)$ 全体组成的空间。

收稿日期: 2010-02-03; **修回日期**: 2010-03-19 **基金项目**: 江苏省高校研究生科研创新计划资助项目(CX08B-089Z)

作者简介:穆文英(1985-),女,山东淄博人,硕士,主要研究方向为时滞神经网络(weny815@126.com);籍艳(1979-),女,山东滨州人,博士,主要研究方向为复杂网络;崔宝同(1960-),男,山东淄博人,教授,博导,主要研究方向为复杂系统控制理论与应用.

2　主要结果

定义式(2)(3)的同步误差为

$$e(t)=y(t)-x(t-\tau) \tag{4}$$

可得到如下定理:

定理 1　如果系统的鲁棒自适应控制器和自适应控制率设计如下:

$$\begin{aligned}u(t)=&A_0(t)x(t-\tau)-B_0(t)y(t)+\\&A_3(t)\int_{t-\tau_2-\tau}^{t-\tau}f(x(s))\,\mathrm{d}s-B_3(t)\int_{t-\tau_2}^{t}g(y(s))\,\mathrm{d}s-\\&(p_1+p_2)\,\mathrm{sign}(e(t))-ke(t)\end{aligned} \tag{5}$$

$$\begin{cases}\dot{A}_0(t)=-e(t)x(t-\tau)\\ \dot{B}_0(t)=e(t)y(t)\\ \dot{A}_3(t)=-e(t)\int_{t-\tau_2-\tau}^{t-\tau}f(x(s))\,\mathrm{d}s\\ \dot{B}_3(t)=e(t)\int_{t-\tau_2}^{t}g(x(s))\,\mathrm{d}s\end{cases} \tag{6}$$

其中:$p_1=\|A_1+A_2\|LB_r$,$p_2=\|B_1+B_2\|KB_u$,k 为大于零的常数,则式(2)(3)是渐近同步的,即驱动系统滞后 τ 时刻后与响应系统渐近同步。

证明　构造 Lyapunov 函数:

$$\begin{aligned}V(t)=&\frac{1}{2}[e^{\mathrm{T}}(t)e(t)+(A_0(t)-A_0)^2+(B_0(t)-B_0)^2+\\&(A_3(t)-A_3)^2+(B_3(t)-B_3)]^2,t\geqslant 0\end{aligned} \tag{7}$$

易证 $V(t)$ 为非负函数,由于

$$\begin{aligned}\dot{e}(t)=&\dot{y}(t)-\dot{x}(t-\tau)=\\&(A_0(t)-A_0)x(t-\tau)-(B_0(t)-B_0)y(t)+B_1g(y(t)+\\&B_2g(y(t-\tau_1))-A_1f(x(t-\tau))-A_2f(x-\tau_1-\tau))+\\&(A_3(t)-A_3)\int_{t-\tau_2}^{t}f(x(s))\,\mathrm{d}s-(B_3(t)-B_3)\int_{t-\tau_2}^{t}g(y(s))\,\mathrm{d}s-\\&(p_1+p_2)\,\mathrm{sign}(e(t))-ke(t)\end{aligned} \tag{8}$$

沿着误差系统的轨迹,计算式(7)的导数可得

$$\begin{aligned}\dot{V}(t)=&e^{\mathrm{T}}(t)\dot{e}(t)+(A_0(t)-A_0)\dot{A}_0(t)+(B_0(t)-B_0)\dot{B}_0+\\&(A_3(t)-A_3)\dot{A}_3(t)+B_3(t)-B_3)\dot{B}_3(t)=\\&e^{\mathrm{T}}(t)[B_1g(y(t))+B_2g(y(t-\tau_1))-\\&A_1f(x(t-\tau))-A_2f(x(t-\tau_1-\tau))-\\&(p_1+p_2)\,\mathrm{sign}(e(t))-ke(t)]\leqslant\\&\|e(t)\|[\|B_1+B_2\|KB_u+\|A_1+A_2\|LB_r-\\&(p_1+p_2)]-e^{\mathrm{T}}ke(t)\leqslant-e^{\mathrm{T}}(t)ke(t)\end{aligned} \tag{9}$$

若 $e(t)\neq 0$ 则 $\dot{V}(t)<0$,且 $e(t)$,$A_0(t)$,$A_3(t)$,$B_3(t)\in L_\infty$。由式(9)可得

$$\int_0^t\|e(t)\|^2\leqslant-\frac{1}{k}\int_0^t[V(e(0))-V(e(t))]\leqslant V(e(0))/k \tag{10}$$

由式(10)得 $e(t)\in L_2$,且由式(8),得到 $\dot{e}(t)\in L_\infty$。根据引理 1 可得 $\lim\limits_{t\to\infty}\|e(t)\|=0$,所以式(2)与(3)渐近同步,即驱动系统(式(1))滞后 τ 时刻后与响应系统(式(3))同步。证毕。

3　数值仿真

考虑如下一类带离散与分布时滞的神经网络:

$$\begin{aligned}\dot{x}(t-\tau)=&A_0x(t-\tau)+A_1f(x(t-\tau))+A_2f(x(t-\tau_1-\tau))+\\&A_3\int_{t-\tau_2-\tau}^{t-\tau}f(x(s))\,\mathrm{d}s+I,t\geqslant\tau\end{aligned} \tag{11}$$

$$\begin{aligned}\dot{y}(t)=&B_0y(t)+B_1g(y(t))+B_2g(y(t-\tau_1))+\\&B_0\int_{t-\tau_2}^{t}g(y(s))\,\mathrm{d}s+u(t)+I,t\geqslant 0\end{aligned} \tag{12}$$

其中:$x(t)=[x_1(t),x_2(t)]^{\mathrm{T}}$,$y(t)=[y_1(t),y_2(t)]^{\mathrm{T}}$,$f(x(t))=[\tanh(x_1(t)),\tanh(x_2(t))]^{\mathrm{T}}$,$g(y(t))=[\tanh(y_1(t)),\tanh(y_2(t))]^{\mathrm{T}}$,令

$$A_0=\begin{bmatrix}-1&0\\0&-1\end{bmatrix},\quad A_1=\begin{bmatrix}1.8&-0.1\\-5&4.5\end{bmatrix},$$

$$B_0=\begin{bmatrix}-1&0\\0&-1\end{bmatrix},\quad B_1=\begin{bmatrix}2.1&-0.1\\-5.2&3.2\end{bmatrix}$$

$k=\mathrm{diag}[1,1]$,$\tau=1$,$\tau_1=1$,$\tau_2=1.2$。给出初始条件$[x_1(s),x_2(s)]^{\mathrm{T}}=[0.1,0.21]$,$[y_1(s),y_2(s)]^{\mathrm{T}}=[-0.3,0.5]^{\mathrm{T}}$。其中:$-1\leqslant s\leqslant 0$,$B_r=2$,$B_u=2.5$,$L_x=L_y=2$。

两个不同的时滞神经网络式(11)(12)的状态曲线如图 1、2 所示。在仿真中,系统参数的初始值为

$$A_0(0)=\mathrm{diag}[-0.5,-1],B_0(0)=\mathrm{diag}[-0.5,-1]$$

$$A_3(0)=[-1.2,-1.5],B_3(0)=[-0.5,-1]$$

同步误差 $e(t)$,自适应参数 $A_0(t)$、$B_0(t)$、$A_3(t)$、$B_3(t)$ 随时间的变化曲线分别如图 3 ~5 所示。由图中看出,同步误差逐渐趋于零值,即时滞神经网络式(11)(12)渐近同步。

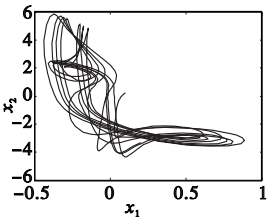

图1　混沌系统式(11)的状态曲线

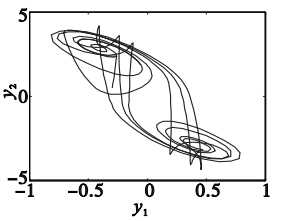

图2　响应系统式(12)不带控制器的状态曲线

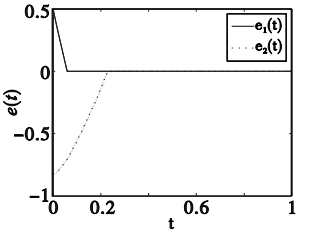

图3　同步误差曲线$e(t)$

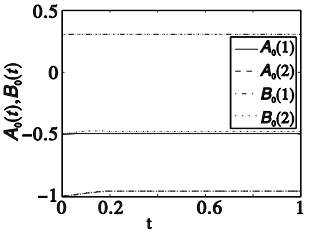

图4　适应参数$A_0(t)$、$B_0(t)$的曲线

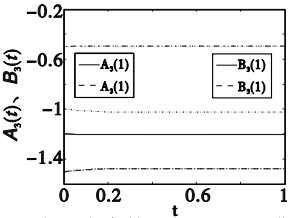

图5　自适应参数$A_3(t)$、$B_3(t)$的曲线

4　保密通信中的应用实例

将混沌同步用于计算机保密通信中。设需要传输的原始数字信号是 10011001,如图 6 所示。在发射端利用混沌信号对它加密,则输出的被加密信号为 $w(t)=s(t)+cx(t)$,这里取 $c=[0,1]^{\mathrm{T}}$,达到保密传输的目的。在接收端,由定理 1 得驱动系统 $y(t)$ 渐近等于 $x(t)$,只需从 $w(t)$ 中减去受控系统产生的混沌信号 $y(t)$,就可获得有用信号 $s(t)$,即

$$\hat{s}(t)=w(t)-cy(t)\to w(t)-cx(t)=s(t)。$$

其中:$\hat{s}(t)$ 为接收端恢复出的信号,$x(t)$ 和 $y(t)$ 分别为式(11)(12)表示的信号。由图 7 看出,接收系统有效地解密出了传送的信号 $\hat{s}(t)$,随着时间的推移,通过解密所得的信息 $\hat{s}(t)$ 与真实信息 $s(t)$ 几乎是重合的,即验证了本文结论的有效性。

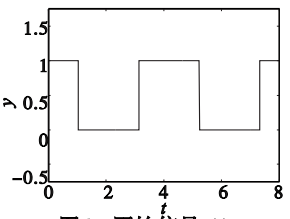

图6　原始信号$s(t)$

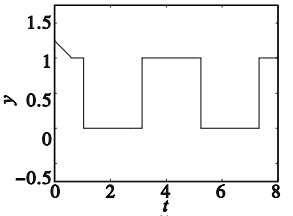

图7　解密信号$\hat{s}(t)$

(下转第 3461 页)

着信任度与实际情况吻合度的提高,文件传送的时间逐渐减少,这也主要是因为对恶意节点的抵制效果和对网络环境变化的感知度的增加。

图 7 从任务完成效率上反映了三种算法的差异,从图 7 中可以看出 TRABPT 在效率上要更高一些。这主要是因为在算法中,进行路由选择时除了考虑到节点的信任度,还利用了前景理论,进一步增加了抵制恶意节点的效果。由于节点具有风险规避和风险追求的特点,使得效率进一步得到了提高。

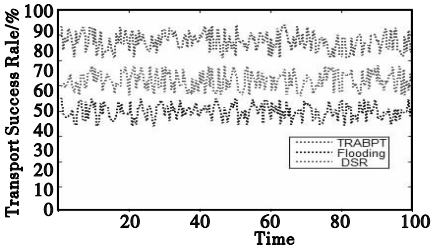

图7　任务完成效率比较

3　结束语

移动 P2P 网络是下一代互联网的重要表现形式,在资源共享、媒体分发、即时通信等领域具有广阔的应用前景。本文主要针对移动 P2P 网络环境中的安全路由问题提出了一种基于前景理论的路由选择算法。移动 P2P 网络中的节点在进行下一跳节点的选择时,利用一定的前景值来选择可信路径信任度最大的节点作为下一跳节点。本文的算法不仅降低了网络节点被恶意节点攻击的可能,也在一定程度上增强了路由的可信度。下一步的工作将集中在如何提高 TRABPT 的效率方面。

参考文献:

[1] SHAH N, QIAN De-pei. Context-aware routing for peer-to-peer network on MANETs[C]//Proc of IEEE International Conference on Network, Architecture, and Storeage. Washington DC: IEEE Computer Society, 2009: 135-139.

[2] CAKMAK J, VUCAK L, KUSEK M. Agent and SIP base mobile peer to peer[C]//Proc of the 10th International Conference on Telecommunications. 2009: 119-124.

[3] YANG Wen-chuan, CHENG Jie, HONG Yuan-yuan. Research on a new billing model for mobile P2P network[C]//Proc of International Conference on Web Information Systems and Mining. 2009: 464-467.

[4] KAHNEMAN D, TVERSKEY A. Prospect theory: an analysis of decision under risk[J]. Econometrical, 1979, 47(2): 263-292.

[5] TVERSKY A, KAHNEMAN D. Advances in prospect theory: cumulative representation of uncertainty[J]. Journal of Risk and Uncertainty, 1992, 5(4): 297-323.

[6] MICHLMAYR E, PANY A, KAPPEL G. Using taxonomies for content-based routing with ants[J]. Journal of Computer and Telecommunications Networking, 2007, 51(16): 4514-4528.

[7] COMELLI F, DAMIANI E, VIMERCATI S D C, *et al*. Choosing reputable servants in a P2P network[C]//Proc of the 11th International World Wide Web Conference. 2002: 376-386.

[8] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.

[9] JAMES B D, ELISA B, USMAN L, *et al*. A generalized temporal role-based access control model[J]. IEEE Trans on Knowledge and Data Engineering, 2005, 17(1): 4-23.

[10] LI Ning-hui, MICHELL J C, WINSBOROUGH W H. Design of a role-based trust-management framework[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2002: 114-130.

[11] RAJAGOPALAN R, MOHAN C K, VARSHNEY P, *et al*. Multi-objective mobile agent routing in wireless sensor networks[J]. IEEE Trans on Congress on Evolutionary Computation, 2005, 5(5): 1730-1737.

[12] 柳毅, 伍前红, 王育民. 基于移动代理的可变路由安全协议[J]. 计算机学报, 2005, 28(7): 1118-1122.

[13] SULTANIK E A, REGLI W C. Service discovery on dynamic peer-to-peer networks using mobile agents[C]//Proc of the 3rd International Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer, 2000: 132-143.

[14] DAVID B J, DAVID A M, CAMEGIE M, *et al*. The dynamic source routing protocol for mobile Ad hoc networks (DSR)[EB/OL]. (2004-07-23). http://www.rfc_archive.org/rfc Internet-Draft, draft-ietf-manet-dsr-10.txt.

(上接第 3457 页)

5　结束语

本文讨论了关于神经网络的同步和在计算机保密通信中应用的问题,提出一种基于 Lyapunov 理论和自适应同步方法的控制,实现了性能良好的混沌控制。随着混沌理论的不断完善和发展,混沌同步必然会在计算机通信领域发挥更大的作用。

参考文献:

[1] PECORA L M, CARROL T L. Synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(8): 821-824.

[2] WANG Kai, TENG Zhi-dong, JIANG Hai-jun. Adaptive synchronization of neural networks with time-varying delay and distributed delay[J]. Physica A, 2008, 387(2-3): 631-642.

[3] ZHANG Hua-guang, XIE Ying-hui, WANG Zhi-liang. Adaptive synchronization between two different chaotic neural networks with time delay[J]. IEEE Trans on Neural Networks, 2007, 18(6): 1841-1844.

[4] 马铁东, 张华光, 王智良. 一类参数不确定统一混沌系统的脉冲滞后同步[J]. 物理学报, 2007, 56(7): 3796-3801.

[5] 谢英慧, 张华光. 一类时滞 Ikeda 混沌系统的自适应同步研究[J]. 东北大学学报, 2007, 28(4): 481-484.

[6] YU Wen-wu, CAO Jin-de. Adaptive synchronization and lag synchronization of uncertain dynamical system with time delay based on parameter identification[J]. Physica Letters A, 2007, 375(2): 476-482.

[7] SUN Yong-hui, CAO Jin-de. Adaptive synchronization between two different noise-perturbed chaotic systems with fully unknown parameters[J]. Physica A, 2007, 376(15): 253-265.

[8] 王晓燕, 瞿少成, 田文汇, 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.

[9] 涂建军, 何汉林. 混沌 Lurie 系统同步在保密通信中的应用[J]. 海军工程大学学报, 2009, 21(10): 33-35.

[10] TANG Yang, QIU Run-he, FANG Jian-an. Adaptive lag synchronization in unknown stochastic chaotic neural networks with discrete and distributed time-varying delays[J]. Physics Letter A, 2008, 372(24): 4425-4433.

[11] TANG Yang, FANG Jian-an. Adaptive synchronization in an array of chaotic neural networks with mixed delays and jumping stochastically hybrid couping[J]. Communications Nonlinear Science Numerical Simulation, 2009, 14(9-10): 3615-3628.