参数不确定时延超混沌系统的脉冲同步方法研究*

罗永健[1)] 于 茜[2)†] 张卫东[3)]

1)(西安通信学院军事电子工程系,西安 710106)

2)(西安通信学院研究生管理大队,西安 710106)

3)(西安通信学院指挥信息系统系,西安 710106)

(2010 年 12 月 15 日收到;2011 年 3 月 1 日收到修改稿)

针对一类参数不确定的异构时延超混沌系统,采用响应系统与驱动系统状态变量误差的线性反馈作为脉冲控制信号,基于 Lyapunov 稳定性理论实现了超混沌系统的脉冲同步,给出了渐近稳定条件,并构造了一个具有时延的数字保密通信系统. 该方案保密性高,鲁棒性强. 数值仿真表明系统能快速达到同步,应用混沌密码序列对数字信号进行加密后,信息信号可以在接收端有效地恢复出来.

关键词: 时延, 脉冲同步, 数字保密通信

PACS: 05.45.Gg, 05.45.Vx, 05.45.Jn, 05.45.Pq

1. 引 言

混沌系统具有类似白噪声的宽频谱特性、非周期性、初值敏感性、长期不可预测性、内随机性等极端复杂的特性,特别适用于保密通信[1]. 作为实现保密通信关键环节的混沌同步更是引起学者们的极大关注,尤其是 1990 年 Pecora 和 Carroll 在电子线路上观察到混沌同步现象[2]后,各种不同的混沌同步方法被提出,如线性与非线性反馈同步法[3,4],自适应同步法[5],耦合同步法[6],延迟反馈同步法[7]等. 近年来随着研究的不断深入,杨涛等学者提出了混沌脉冲同步法[8—12]. 该方法无需从发射系统获取连续信号,只需要较小的脉冲量就可以镇定混沌系统,从而使混沌同步系统更直接地调制数字信号. 脉冲同步法在单位时间内传输的有用信息量减少,信道利用率提高,而且由于密钥的"支离破碎",加密的信息即使被窃取后也难以破译,系统的保密性大大增强[12],因此,脉冲同步法是最具发展潜力的一种混沌同步方法. 但是现有脉冲同步方法的研究主要集中于无时延混沌系统[8—12]上,然而时延现象在实际应用中大量存在,它往往是系统不稳定和系统性能退化的根源,所以对于具有传输信道时间延迟,且参数不确定的异构超混沌系统的脉冲同步问题展开研究具有极为重要的应用价值. 为此,本文针对参数不确定的异构时延超混沌系统进行了深入探讨,给出了脉冲同步条件,并将该系统应用于数字保密通信系统中.

2. 参数不确定时延超混沌系统的脉冲同步方法分析

参数不确定超混沌系统可描述为

$$\dot{x}(t) = (A + \Delta A(t))x(t) + f(x(t)), \quad (1)$$

其中, $x \in R^n$ 为状态变量, $A \in R^{n\times n}$ 是参数矩阵, $f: R^n \to R^n$ 为系统非线性部分; $\Delta A(t) \in R^{n\times n}$ 为参数不确定项,它是时变的且不改变系统吸引子的区域. 令 $\Delta A(t)$ 满足 $\Delta A(t) = EF(t)H$, $\| F(t) \| < 1$, 这里, E, H 为适当维数的常数矩阵, $\| \cdot \|$ 为矩阵任意范数.

文献[11]对系统(1)进行了详细讨论,但发射端的信号通过信道传输到接收端通常存在时间延迟,假设时延为 τ, 考虑参数不确定的时延混沌系统

$$\dot{x}(t-\tau) = (A + \Delta A(t-\tau))x(t-\tau) + f(x(t-\tau)), \quad (2)$$

其中, $\Delta A(t-\tau) \in R^{n\times n}$ 为考虑信道延迟的参数不

* 国家自然科学基金(批准号:61179002)和陕西省自然科学基金(批准号:2011JM8030)资助的课题.

† 通讯联系人. E-mail: yuqian0717@yahoo.cn

确定项,它不改变系统吸引子的区域.

将系统(2)作为驱动系统,同时构造一个对应的响应系统

$$\dot{y}(t) = (B + \Delta B(t))y(t) + g(y(t)), \quad (3)$$

其中,$y \in R^n$ 为状态变量,$B \in R^{n\times n}$ 是参数矩阵,$g: R^n \to R^n$ 为非线性部分;$\Delta B(t) \in R^{n\times n}$ 为参数不确定项,它不改变系统吸引子的区域. $\Delta B(t)$ 是时变的,且满足:$\Delta B(t) = E'G(t)H'$,$\| G(t) \| < 1$,这里,E',H' 为适当维数的常数矩阵.

定义同步误差系统为[13]

$$e = y(t) - x(t-\tau).$$

假设离散时刻集合 $\{t_k\}$ 满足 $0 < t_1 < t_2 < \cdots < t_k < t_{k+1} < \cdots$,$\lim\limits_{k\to\infty} t_k = \infty$ $(k = 1,2,\cdots)$,初始时刻 t_0 满足 $0 < t_0 < t_1$,信息信号在 t_k 时刻传输.

采用系统(2)与系统(3)状态变量误差的线性反馈作为脉冲控制信号,可得如下脉冲被控响应系统:

$$\begin{aligned}
&\dot{y} = (B + \Delta B(t))y(t) + g(y(t)), && t \neq t_k,\\
&\Delta y = y(t_k^+) - y(t_k^-) = y(t_k^+) - y(t_k) = B_k(y(t) - x(t-\tau)) = B_k e, && t = t_k, k = 1,2,\cdots, \quad (4)\\
&y(t_0^+) = y_0,
\end{aligned}$$

其中 $y(t_k^+) = \lim\limits_{t\to t_k^+} y(t)$,$y(t_k^-) = \lim\limits_{t\to t_k^-} y(t)$,$t_k^+$ 和 t_k^- 分别表示脉冲时刻 t_k 前后的瞬时,假定响应系统在 t_k 时刻满足左连续,即 $y(t_k^-) = y(t_k)$. 脉冲同步的目标就是设计控制增益 $B_k \in R^{n\times n}$ 与脉冲间距 $\Delta_k = t_{k+1} - t_k < \infty$ $(k = 1,2,\cdots)$,使得具有不同初始条件的脉冲被控响应系统(4)与时延驱动系统(2)实现全局渐近同步.

假设非线性函数 f 满足 Lipshictz 条件

$$\begin{aligned}
&|g(y(t)) - g(x(t-\tau))|\\
&= |g(x(t-\tau) + e) - g(x(t-\tau))|\\
&\leqslant \mu |g(t-\tau) + e - g(t-\tau)| = \mu e, \quad (5)
\end{aligned}$$

则

$$\begin{aligned}
&g(y) - g(x(t-\tau))\\
&= M(x(t-\tau), y(t))e, \quad (6)
\end{aligned}$$

其中 $M \in R^{n\times n}$,$\| M(x(t-\tau), y(t)) \| \leqslant \mu$.

令

$$\begin{aligned}
&g(x(t-\tau)) - f(x(t-\tau))\\
&= D(x(t-\tau))x(t-\tau), \quad (7)
\end{aligned}$$

其中 $D(x(t-\tau)) \in R^{n\times n}$,$\| D(x(t-\tau)) \| \leqslant \delta$.

考虑系统时延,根据混沌信号的有界性,令 $|x(t-\tau)| \leqslant \alpha|x(t)|$,$|x(t)| \leqslant \chi$,则 $|x(t-\tau)| \leqslant \alpha\chi$.

假设驱动系统的状态在时间上是连续的,所以在 t_k 时刻,$\Delta x = 0$,由(2)—(7)式可解出误差系统

$$\begin{aligned}
&\dot{e} = (B + \Delta B(t) + M(x(t-\tau), y(t)))e + (B + \Delta B(t) - A\\
&\quad - \Delta A(t-\tau) + D(x(t-\tau)))x(t-\tau), && t \neq t_k\\
&\Delta e = B_k e, && t = t_k, k = 1,2,\cdots, \quad (8)\\
&e(t_0^+) = e_0.
\end{aligned}$$

显然 $e(t) = 0$ 是误差系统(8)的平衡点,若系统(2)和(3)同步,则误差系统(8)在平衡点 $e(t) = 0$ 处稳定. 于是,混沌同步问题转化为:设计矩阵 B_k 和脉冲间距 $\Delta_k = t_{k+1} - t_k < \infty$ $(k = 1,2,\cdots)$,使得误差系统(8)渐近稳定,也就是对于 $t \geqslant t_0$,有 $|y(t) - x(t-\tau)| = |e(t)| \leqslant \varepsilon, 0 < \varepsilon < +\infty$.

为了得到控制增益 B_k 与脉冲间距 Δ_k 的关系式,使得具有不同初始条件的脉冲被控响应系统(4)与时延驱动系统(2)实现全局渐近同步,引入以下定理.

定理 假设 $I + B_k$ 的谱半径 ρ 满足 $\rho(I + B_k) \leqslant 1$,$w_k$ 是 $(I + B_k)^{\mathrm{T}}(I + B_k)$,$k = 1,2,\cdots$ 的最大特征值,λ_1 是 $[B + \Delta B(t) + M(x(t-\tau), y(t))]^{\mathrm{T}} + [B + \Delta B(t) + M(x(t-\tau), y(t))]$ 的最大特征值,λ_2 是 $[B + \Delta B(t) - A - \Delta A(t-\tau) + D(x(t-\tau))]^{\mathrm{T}} + [B + \Delta B(t) - A - \Delta A(t-\tau) + D(x(t-\tau))]$ 的最大特征值,$g(y(t))$ 满足 Lipschitz 条件. 因此如果

存在一个常数 $\xi_k > 1$ 使得

$$\ln(\xi_k w_k) + (\lambda_1 + \lambda_2\alpha\zeta\chi)\Delta_k < 0, \quad k = 1,2,\cdots, \tag{9}$$

即脉冲间隔 Δ_k 满足

$$0 \leqslant \Delta_k \leqslant -\frac{\ln(\xi_k w_k)}{\lambda_1 + \lambda_2\alpha\zeta\chi}, \quad \xi_k > 1, k = 1,2,\cdots. \tag{10}$$

那么误差系统(8)对于 $|e| \geqslant \frac{1}{\zeta}$ 达到渐近稳定,其中 ζ 是一个足够大的正数.

证明 选择 Lyapunov 函数为 $V(e) = 0.5e^{\mathrm{T}}e$

1) 对于 $t \in (t_{k-1}, t_k)(k = 1,2,\cdots)$, 对 Lyapunov 函数沿着系统(8)求导得

$$\begin{aligned}
\dot{V}(e) &= 0.5\dot{e}^{\mathrm{T}}e + 0.5e^{\mathrm{T}}\dot{e} \\
&= 0.5[(B + \Delta B(t) + M(x(t-\tau), y(t)))e \\
&\quad + (B + \Delta B(t) - A - \Delta A(t-\tau) \\
&\quad + D(x(t-\tau)))x(t-\tau)]^{\mathrm{T}}e \\
&\quad + 0.5e^{\mathrm{T}}[(B + \Delta B(t) \\
&\quad + M(x(t-\tau), y(t)))e + (B + \Delta B(t) - A \\
&\quad - \Delta A(t-\tau) + D(x(t-\tau)))x(t-\tau)] \\
&= 0.5e^{\mathrm{T}}[B + \Delta B(t) + M(x(t-\tau), y(t))]^{\mathrm{T}}e \\
&\quad + 0.5(x(t-\tau))^{\mathrm{T}}[B + \Delta B(t) - A \\
&\quad - \Delta A(t-\tau) + D(x(t-\tau))]^{\mathrm{T}}e \\
&\quad + 0.5e^{\mathrm{T}}[B + \Delta B(t) + M(x(t-\tau), y(t))]e \\
&\quad + 0.5e^{\mathrm{T}}[B + \Delta B(t) - A - \Delta A(t-\tau) \\
&\quad + D(x(t-\tau))]x(t-\tau) \\
&= 0.5e^{\mathrm{T}}\{[B + \Delta B(t) + M(x(t-\tau), y(t))]^{\mathrm{T}} \\
&\quad + [B + \Delta B(t) + M(x(t-\tau), y(t))]\}e \\
&\quad + 0.5(x(t-\tau))^{\mathrm{T}}[B + \Delta B(t) \\
&\quad - A - \Delta A(t-\tau) + D(x(t-\tau))]^{\mathrm{T}}e \\
&\quad + 0.5e^{\mathrm{T}}[B + \Delta B(t) - A - \Delta A(t-\tau) \\
&\quad + D(x(t-\tau))]x(t-\tau) \\
&\leqslant 0.5\lambda_1 e^{\mathrm{T}}e + 0.5\{[B + \Delta B(t) - A \\
&\quad - \Delta A(t-\tau) + D(x(t-\tau))]^{\mathrm{T}} \\
&\quad + [B + \Delta B(t) - A - \Delta A(t-\tau) \\
&\quad + D(x(t-\tau))]\}|e||x(t-\tau)| \\
&\leqslant \lambda_1 V(e) + 0.5\lambda_2|e|\alpha\chi, \\
&\quad t \in (t_{k-1}, t_k], \quad k = 1,2,\cdots.
\end{aligned}$$

假设对于足够大的常数 ζ, 存在 $\zeta|e| \geqslant 1$, 则有 $\zeta|e|^2 \geqslant |e|$, 因此得到

$$\begin{aligned}
\dot{V}(e) &\leqslant \lambda_1 V(e) + 0.5\lambda_2\zeta|e|^2\alpha\chi \\
&= (\lambda_1 + \lambda_2\alpha\zeta\chi)V(e),
\end{aligned} \tag{11}$$

那么

$$V(e(t)) \leqslant V(e(t_{k-1}^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_{k-1})}, \quad t \in (t_{k-1}, t_k], k = 1,2,\cdots. \tag{12}$$

2) 当 $t = t_k(k = 1,2,\cdots)$ 时,由系统(8)可得到

$$\begin{aligned}
V(e(t_k^+)) &= 0.5(e(t_k) + \Delta e)^{\mathrm{T}}(e(t_k) + \Delta e) \\
&= 0.5[(I + B_k)e(t_k)]^{\mathrm{T}}[(I + B_k)e(t_k)] \\
&= 0.5[e(t_k)]^{\mathrm{T}}(I + B_k)^{\mathrm{T}}(I + B_k)e(t_k) \\
&\leqslant w_k V(e(t_k)), \quad k = 1,2,\cdots.
\end{aligned} \tag{13}$$

根据(12)式,当 $k = 1$ 时,对于 $t \in (t_0, t_1]$, 得到

$$V(e(t)) \leqslant V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_0)},$$

令 $t = t_1$, 有

$$V(e(t_1)) \leqslant V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_1-t_0)},$$

由(13)式可得到

$$\begin{aligned}
V(e(t_1^+)) &\leqslant w_1 V(e(t_1)) \\
&\leqslant w_1 V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_1-t_0)}.
\end{aligned}$$

当 $k = 2$ 时,对于 $t \in (t_1, t_2]$ 得到

$$\begin{aligned}
V(e(t)) &\leqslant V(e(t_1^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_1)} \\
&\leqslant w_1 V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_1-t_0)}\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_1)} \\
&\leqslant w_1 V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_0)}.
\end{aligned}$$

同理,当 $k = 3$ 时,对于 $t \in (t_2, t_3]$ 有

$$V(e(t)) \leqslant w_1 w_2 V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_0)}.$$

根据数学归纳法,可得到对于 $t \in (t_k, t_{k+1}]$,

$$V(e(t)) \leqslant \prod_{i=1}^{k} w_i V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_0)}. \tag{14}$$

从定理中的假设可以得到 $\xi_i w_i \exp(\lambda_1 + \lambda_2\alpha\zeta\chi)\Delta_k < 1, (k = 1,2,\cdots; i = 1,2,\cdots,k)$, 因此对于任意 $t \in (t_k, t_{k+1}], k = 1,2,\cdots$, 可以得到

$$\begin{aligned}
V(e(t)) &\leqslant \prod_{i=1}^{k} w_i V(e(t_0^+))\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_0)} \\
&= V(e(t_0^+))[w_1\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_1-t_0)}] \\
&\quad \times [w_2\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_2-t_1)}]\cdots \\
&\quad \times [w_k\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t_k-t_{k-1})}]\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_k)} \\
&\leqslant V(e(t_0^+)) \prod_{i=1}^{k} \frac{1}{\xi_i}\mathrm{e}^{(\lambda_1+\lambda_2\alpha\zeta\chi)(t-t_k)}.
\end{aligned}$$

上式表明,对于定理中给定的假设, $V(e) = 0.5e^{\mathrm{T}}e$ 是递增函数,因此只要 $|e| \geqslant \frac{1}{\zeta}$, 误差系统(8)就可以达到渐近稳定,响应系统与驱动系统实现同步.

3. 参数不确定时延系统脉冲同步方法在数字保密通信中的应用

对于参数不确定且具有传输信道时延的混沌系统,同样可以利用脉冲控制法实现收发两端混沌系统的同步,实现保密通信.

如图 1 所示,保密通信的实现思想是:在发送端,发射信号包含一系列的时间帧,每一个时间帧长 T(为了提高保密性,需使时间帧的长度小于最大脉冲间隔[14],即 $T < \Delta_{\max}$),其结构如图 2 所示.每个时间帧中,状态变量产生 50 个采样值,第一个值用作同步脉冲,后 49 个值加密与信息信号形成混合信号,再组合成一个时间帧进行传输;在接收端,将接收到的各个时间帧分解,第一个值是同步脉冲,用作混沌系统的同步,后 49 个值参与混沌信号解密,恢复出信息信号.

假设发送端发送的信息信号为$m(t)$,其抽样

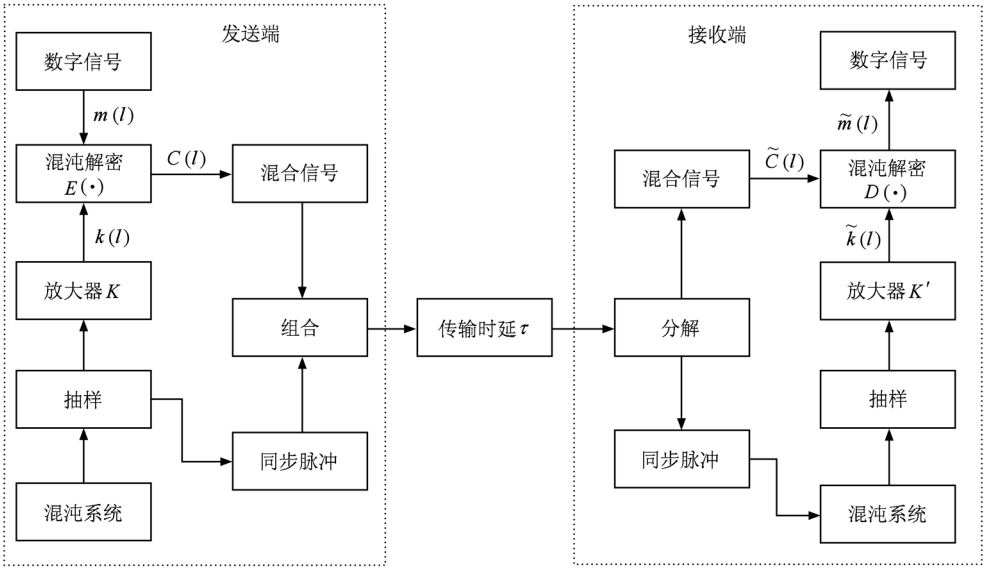

图 1 基于时延混沌系统的保密通信系统框图

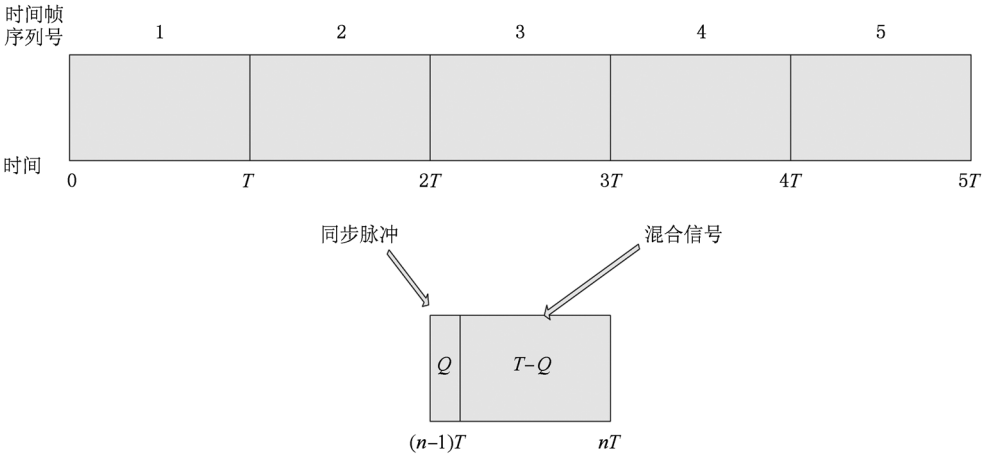

图 2 时间帧结构

值为 $m(l)$,那么发送端的混合信号 $C(l)$ 为

$$C(l) = E(\hat{m}(l), k(l)). \quad (15)$$

其中,发送端的密码序列 $k(l)$ 是混沌状态变量 (x_1, x_2, x_3, x_4) 的抽样值,令

$$k(l) = K \cdot \left(\frac{x_1^4(l) + x_2^4(l) + x_3^4(l) + x_4^4(l)}{4}\right)^{1/4},$$

这里, K 是密钥参数,用于提高通信系统的保密性[15]. 选择 h 使得 $k(l)$ 满足 $k(l) \in [-h,h]$.

$\hat{m}(l)$ 是 $m(l)$ 的变换值,且有 $\hat{m}(l) = \begin{cases} (0,h] \text{ 的随机数}, m(l) = \text{'0'} \\ [-h,0) \text{ 的随机数}, m(l) = \text{'1'}. \end{cases}$

$E(*,*)$ 是加密函数,参照文献[14]提出的复杂传统加密算法,有

$$\begin{aligned} C(l) &= E(\hat{m}(l), k(l)) \\ &= \underbrace{f_1(\cdots f_1\{f_1}_{n}[\hat{m}(l), \\ &\quad \underbrace{k(l)], k(l)\}, \cdots, k(l))}_{n}. \end{aligned} \tag{16}$$

为了进一步提高保密性,可进行多级 f_1 非线性加密运算. 这里非线性函数 f_1 有如下形式:

$$f_1(x,k) = \begin{cases} (x+k) + 2h & -2h \leqslant x + k \leqslant -h, \\ x + k & -h < x + k < h, \\ (x+k) - 2h & h \leqslant x + k \leqslant 2h. \end{cases} \tag{17}$$

接收端的恢复信号 $\hat{\tilde{m}}(l)$ 为

$$\hat{\tilde{m}}(l) = D(\tilde{C}(l), \tilde{k}(l)), \tag{18}$$

其中 $\tilde{C}(l)$ 为密文信号,接收端的密码序列 $\tilde{k}(l)$ 是混沌状态变量 (y_1, y_2, y_3, y_4) 的抽样值,令

$$\tilde{k}(l) = K' \cdot \left(\frac{y_1^4(l) + y_2^4(l) + y_3^4(l) + y_4^4(l)}{4}\right)^{1/4},$$

K' 为密钥参数,与前面加密器中的 K 一致.

同样参照文献[14]提供的复杂传统解密算法,得到

$$\begin{aligned} \hat{\tilde{m}}(l) &= D(\tilde{C}(l), \tilde{k}(l)) \\ &= \underbrace{f_1(\cdots f_1\{f_1}_{n}[\tilde{C}(l), \\ &\quad \underbrace{-\tilde{k}(l)], -\tilde{k}(l)\}, \cdots, -\tilde{k}(l))}_{n}. \end{aligned} \tag{19}$$

令 $\tilde{C}(l), \tilde{k}(l)$ 满足

$\tilde{C}(l) \in [-h,h]$ (密文),

$\tilde{k}(l) \in [-h,h]$ (密码序列),

最后经变换得到

$$\tilde{m}(l) = \begin{cases} 0 & \hat{\tilde{m}}(l) > 0, \\ 1 & \hat{\tilde{m}}(l) < 0, \end{cases}$$

就可恢复平文信息 $\tilde{m}(l)$.

在以上过程中,当且仅当收发两端的混沌系统实现同步得到 $k(l) = \tilde{k}(l)$, 即两个密码序列相同,才能准确地解密出信息信号,即 $\tilde{m}(l) = m(l)$, 可见脉冲同步是整个系统实现保密通信的前提和关键.

4. 数值仿真

为了评估所提出理论的正确性与有效性,采用 Matlab 软件,对超陈和超吕混沌系统进行仿真研究.

时延超陈系统

$$\begin{aligned} \dot{x}_1(t-\tau) &= -ax_1(t-\tau) + ax_2(t-\tau) \\ &\quad + x_4(t-\tau), \\ \dot{x}_2(t-\tau) &= dx_1(t-\tau) \\ &\quad - x_1(t-\tau)x_3(t-\tau) \\ &\quad + cx_2(t-\tau), \\ \dot{x}_3(t-\tau) &= x_1(t-\tau)x_2(t-\tau) \\ &\quad - bx_3(t-\tau), \\ \dot{x}_4(t-\tau) &= x_2(t-\tau)x_3(t-\tau) \\ &\quad + dx_4(t-\tau). \end{aligned}$$

超吕系统

$$\begin{aligned} \dot{y}_1 &= -a_1y_1 + a_1y_2 + y_4, \\ \dot{y}_2 &= -y_1y_3 + c_1y_2, \\ \dot{y}_3 &= y_1y_2 - b_1y_3, \\ \dot{y}_4 &= y_1y_3 + d_1y_4. \end{aligned}$$

其中 a,b,c,d,a_1,b_1,c_1,d_1 为系统参数,当 $a = 35, b = 3, c = 12, d = 7, a_1 = 36, b_1 = 3, c_1 = 20, d_1 = 1.3$ 时,两个系统处于混沌状态.

根据(2)式与(3)式的描述,取参数不确定项

$$\Delta A(t-\tau) = 0.007 \cdot \begin{bmatrix} \cos(t-\tau) & 0 & 0 & 0 \\ 0 & \sin(t-\tau) & 0 & 0 \\ 0 & 0 & \cos(t-\tau) & 0 \\ 0 & 0 & 0 & \sin(t-\tau) \end{bmatrix},$$

$$\Delta B(t) = 0.007 \cdot \begin{bmatrix} \sin(t) & 0 & 0 & 0 \\ 0 & \cos(t) & 0 & 0 \\ 0 & 0 & \sin(t) & 0 \\ 0 & 0 & 0 & \cos(t) \end{bmatrix}.$$

假设驱动系统与响应系统的初始条件分别为 $(x_{10}, x_{20}, x_{30}, x_{40}) = (3,5,7,9)$, $(y_{10}, y_{20}, y_{30}, y_{40}) = (5,7,4,2)$, 时延常数 $\tau = 3$s, 矩阵 $B_i = \mathrm{diag}(k, k, k, k)$, 其中 $k = -1.2$, 令 $\chi = 70$, $\alpha = 2$, $\zeta = 2$, $\xi_k = 6$, 根据定理,得到 $w_i = w = 0.04$, $\lambda_1 = 45$, $\lambda_2 = 8$, $\Delta_k < 0.0056$, 误差系统(8)可达到渐近稳定. 为方便起见,选取等距脉冲间隔 $\Delta = \Delta_k = 0.005$, 令采样率为 0.0001s,得到脉冲同步的仿真结果如图 3 所示.

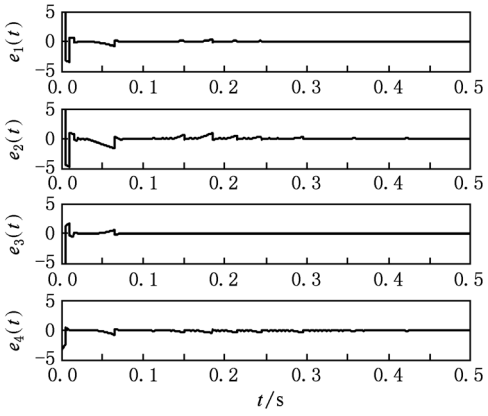

图 3 脉冲同步仿真曲线

从图 3 仿真结果可以看出,在较短的时间内,收发两端的混沌系统可以实现同步,且同步效果良好.

信道传输信号由时间帧序列组成,时间帧长度设置为 $T = 0.005 < \Delta_{\max}$, 脉冲占空比为 0.02. 在系统仿真中,加密器端取密钥参数 $K = 2$, $h = 80$ 且经过 20 级 f_1 加密运算,解密器端取密钥参数 $K' = K = 2$, $h = 80$, 且经过 20 级 f_1 解密运算. 系统发送端的原始信号由(16)式加密算法运算后,组合成时间帧进行传输,接收端先将时间帧分解,再由(19)式解密算法运算后恢复出原始信息. 系统仿真结果如图 4 所示.

从图 4 结果来看,通过加密-解密运算后,信息信号能够较好地恢复出来,并且信道中传输的“时间帧”信号具有较高的保密性,破译难度较大.

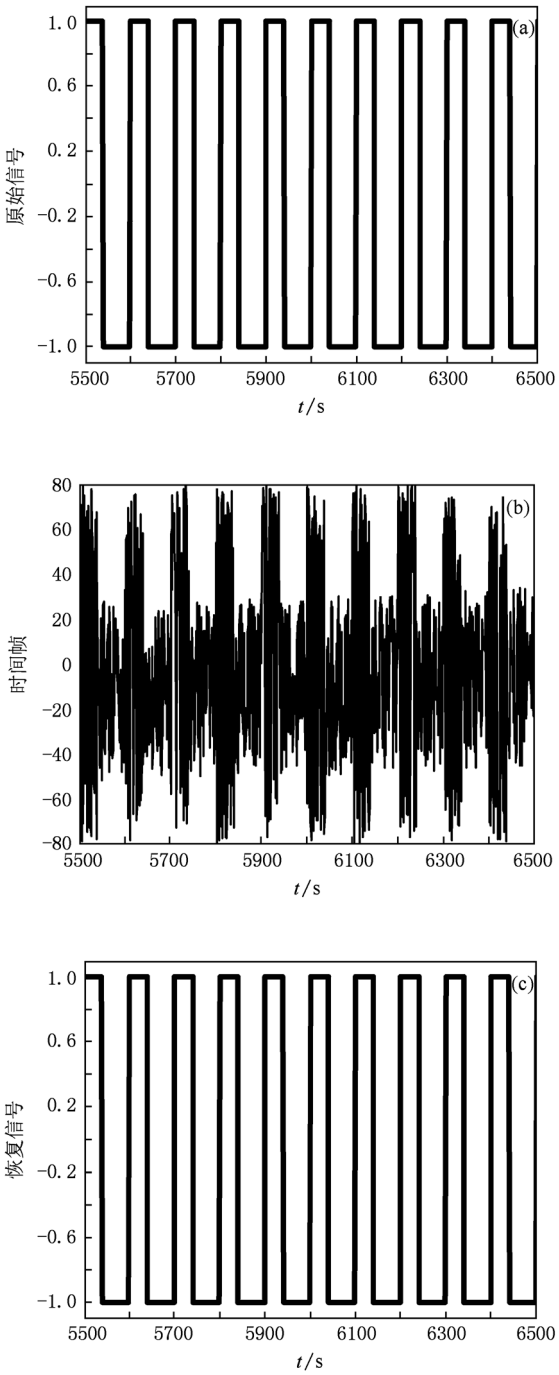

图 4 数字保密通信系统仿真结果 (a)原始信号 $m(l)$; (b)信道传输信号(时间帧); (c)接收端恢复信号 $\tilde{m}(l)$

5. 结 论

文中提出了超陈与超吕混沌系统的脉冲同步方法,给出了脉冲间隔范围,并以此为基础构造了一个数字保密通信系统,具有较高的保密性. 该方法适用于大多数已知的混沌系统与超混沌系统. 下一步将深入研究可变长脉冲间隔同步方法及其保密通信中的应用.

[1] Fang J Q 2002 *Rein Chaos and Develop High and New Technology* (Beijing: Atomic Energy Press) p14 (in Chinese) [方锦清 2002 驾驭混沌与发展高新技术(北京:原子能出版社) 第 14 页]

[2] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[3] Li N, Li J F, Liu Y P, Ma J 2008 *Acta Phys. Sin.* **57** 1404 (in Chinese) [李 农、李建芬、刘宇平、马 健 2008 物理学报 **57** 1404]

[4] Chen M Y, Han Z Z 2003 *Chaos, Solit. & Frac.* **17** 709

[5] Zhang R X, Tian G, Li P, Yang S P 2008 *Acta Phys. Sin.* **57** 2073 (in Chinese) [张若洵、田 钢、栗 苹、杨世平 2008 物理学报 **57** 2073]

[6] Zhou J, Lu J A, Wu X Q 2007 *Chaos, Soli. & Frac.* **31** 230

[7] Lai H H, Zhang X H 2009 *Comp. Appl. and Soft.* **26** 38 (in Chinese) [赖宏慧、张小红 2009 计算机应用与软件 **26** 38]

[8] Yang T, Chua L O 1997 *IEEE Trans. on Circ. and Sys.* ——I: *Fund. Theor. and Appl.* **44** 976

[9] Li L Q, Xu H L 2008 *Comm. Tech.* **41** 168 (in Chinese) [李丽勤、许弘雷 2008 通信技术 **41** 168]

[10] Ma T D, Zhang H G 2008 *J. Sys. Sim.* **20** 4923 (in Chinese) [马铁东、张化光 2008 系统仿真学报 **20** 4923]

[11] Mohammad H, Mahsa D 2009 *Comm. in Nonl. Sci. and Num. Sim.* **14** 880

[12] Sheng S Y, Zhu C Y 2007 *Microcom. Appl.* **28** 306 (in Chinese) [盛苏英、朱灿焰 2007 微计算机应用 **28** 306]

[13] Jiang G P, Zheng W X, Chen G R 2004 *Chaos, Soli. and Frac.* **20** 267

[14] Yang T, Wu C W, Chua L O 1997 *IEEE Trans. on Circ. and Sys.* ——I: *Fund. Theor. and Appl.* **44** 469

[15] Li Z G, Li K, Wen C Y 2003 *IEEE Trans. on Comm.* **51** 1306

Research on impulsive synchronization approach of parameter uncertain hyperchaotic systems with time-delay*

Luo Yong-Jian[1)] Yu Qian[2)†] Zhang Wei-Dong[3)]

1) (*Institute of Military Electronic Engineering, Xi'an Communications Institute, Xi'an* 710106, *China*)

2) (*Administrant Brigade of Postgraduate, Xi'an Communications Institute, Xi'an* 710106, *China*)

3) (*Institute of Command Information Systems, Xi'an Communications Institute, Xi'an* 710106, *China*)

(Received 15 December 2010; revised manuscript received 1 March 2011)

Abstract

In this paper, based on the Lyapunov stability theory, the impulsive synchronization asymptotic stability condition for different hyperchaotic systems with time delay and parameter uncertainty is first presented by using the linear feedback of state variable error between the slave system and the master system as the impulsive control signal. After the synchronization, a digital communication system with time delay is provided to achieve secure communication. This scheme is of high security and robustness. Moreover, computer simulations show that in the communication system, the synchronization of the systems could be achieved quickly, and by using chaotic cipher sequence to encrypt the digital signal, the useful information signal can be recovered effectively from the receiver.

Keywords: time-delay, impulsive synchronization, digital secure communication

PACS: 05.45.Gg, 05.45.Vx, 05.45.Jn, 05.45.Pq

* Project supported by the National Natural Science Foundation of China (Grant No. 61179002) and the Natural Science Foundation of Shaanxi Province, China (Grant No. 2011JM8030).

† Corresponding author. E-mail: yuqian0717@yahoo.cn