

# 异结构系统混沌同步及其在保密通信中的应用研究

乔佳乐 侯冬梅 张艳鹏\*  
(绥化学院 黑龙江绥化 152061)

**【摘要】** Lyapunov原理对于异结构系统实现稳定同步十分重要, 本文基于该原理, 通过实例研究等方法, 研究了异结构系统混沌同步的实现及同步技术在保密通信中的应用进行了多角度的分析, 以期助力相关工作、研究顺利开展。

**【关键词】** 异结构; 混沌同步; 保密通信

**DOI:** 10.18686/jyyxx.v3i6.47885

1990年, Pecora、Carroll等人提出了混沌同步原理, 并在实际电路中进行了实践。之后, 混沌控制、混沌同步及混沌系统的应用成为相关研究领域的研究热点, 且得到快速发展。依据一些研究表明<sup>[1]</sup>, 在响应子系统变量约束下所有 Lyapunov 指数为负的特定条件下, 可以实现 2 个异结构混沌系统的同步, 然而混沌同步很难保证结构相异的 2 个混沌系统的参数完全相同, 而系统参数不同会对同步产生严重扰动, 甚至可能带来较大信息误差, 因此只有有效改善相关问题, 才能使其在保密通信中应用更具实用性、安全性。

## 1 混沌系统的模型与系统稳定性的判定

### 1.1 混沌系统的模型

统一混沌系统, 是由吕金虎等人最先研究并提出的新型混沌系统, 该系统将 Lorenz、Lü、chen 等之前常应用的系统联合为一个统一混沌系统。此混沌系统的连续性、统一性及全域性等特点, 使其能为保密通信等工作提供更好的支持。系统数学模型如下:

$$\begin{cases} \dot{x}_1 = (25\alpha + 10)(x_2 - x_1) \\ \dot{x}_2 = (28 - 35\alpha)x_1 - x_1x_3 + (29\alpha - 1)x_2 \\ \dot{x}_3 = x_1x_2 - \frac{(8+\alpha)x_3}{3} \end{cases} \quad (1)$$

唯一的控制参数为  $\alpha$ , 当其属于区间 $[0, 0.8]$ 时, 整个混沌系统将归属于广义 Lorenz 系统; 当其为 0.8, 统一系统将归属为 Lü 系统; 当其属于区间 $(0, 8, 1]$ 时, 整个系统将归属为广义上的 Chen 系统; 当其由 0 向 1 逐渐增大时, 整个系统将由广义 Lorenz 系统向广义 Chen 系统逐渐过渡; 当其为 0 时, 整个系统将归属于 Lorenz 系统; 当其为 1 时, 系统将归属为 Chen 系统。

Rössler 系统的雏形是 Lorenz 在研究大气热对流工作中得到的, 其最先获得了一组非线性微分方程, 该方程组数值解出现了特殊的混沌现象: 之后 Rössler 简化了该方程组, 就是现在常用的 Rössler 系统, 由于该方程只含单一非线性项, 且依然存在混沌运动, 这使得该系统在应用

时具有很强的便捷性, 因此被广泛研究与应用。其数学模型为:

$$\begin{cases} \dot{x}_1 = -(x_2 - x_1) \\ \dot{x}_2 = x_1 + \alpha x_2 \\ \dot{x}_3 = b + x_3(x_1 - c) \end{cases} \quad (2)$$

### 1.2 系统稳定性的判定

俄罗斯数学家 Lyapunov 提出了 2 种用于判定系统稳定性的方法, 以直接或间接的判定混沌系统的同步稳定性。采用直接法, 需要寻找合适的函数, 结合 Lyapunov 提出的稳定性理论, 对函数及其一阶导数定号性进行分析, 从而判断系统的稳定性, 根据公式 (3), 当该函数为正定且其一阶导数半负定时, 混沌系统达到稳定。

$$v = \frac{1}{2} \sum_{i=1}^n e_i^2 \quad (3)$$

## 2 异结构混沌系统的同步与数值仿真实例研究

以 Rössler 与 Lü 混沌系统的同步为例。驱动系统为 Rössler, 公式为式 (4):

$$\begin{cases} \dot{x}_1 = -(y_1 - x_1) \\ \dot{y}_1 = x_1 + 0.2y_1 \\ \dot{z}_1 = 0.2 + x_1z_1 \end{cases} \quad (4)$$

Lü 系统是响应系统, 公式为式 (5):

$$\begin{cases} \dot{x}_2 = 10(y_2 - x_2) + u_1 \\ \dot{y}_2 = 40x_2 - x_2z_2 + u_2 \\ \dot{z}_2 = -2.5z_2 + 4x_2^2 + u_3 \end{cases} \quad (5)$$

假设:

$$\begin{cases} a_1 = x_2 - x_1 \\ a_2 = y_2 - y_1 \\ a_3 = z_2 - z_1 \end{cases}$$

则得到:

$$\begin{cases} \dot{a}_1 = x_2 - x_1 \\ \dot{a}_2 = y_2 - y_1 \\ \dot{a}_3 = z_2 - z_1 \end{cases}$$

将假设带入系统公式, 并将 Lyapunov 函数带入关系式, 最终得到:

$$\dot{w} = \frac{1}{2} (e_1^2 + e_2^2 + e_3^2) \geq 0$$

$$\dot{w} = e_1e_1 + e_2e_2 + e_3e_3 = e_1^2 - 2.5e_3^2 \leq 0$$

然后设置系统的初始值:  $x_1=-1, y_1=0, z_1=1, x_2=1, y_2=2, z_2=3$ , 应用 Matlab 及 Simulink 技术进行数值仿真,

最终显示经过一小段时间的延时, 系统误差为 0, 表明 Rössler 与 Lü 两个异结构混沌系统已经达到同步。

### 3 异结构混沌同步在保密通信中的应用分析

#### 3.1 混沌遮掩保密通信

该技术的发展较早, 也是较早将混沌信号应用于保密通信的方法<sup>[2]</sup>。由发送端混沌系统, 通过在输出信号时迭加想要传递的有用信号, 利用信道合成信息并将最终的信号传输出去; 当接收端系统收到信息后, 会在信息驱动下与发送端进行信息等价, 最终使本地系统与发送端系统实现信号同步, 并根据相应的解析规则从接收的遮掩信号中去除迭加的无用信号, 获得有用信息。

#### 3.2 混沌键控保密通信

简单混沌系统应用键控保密通信这一方法, 接收端混沌系统被动同步, 因此存在抗干扰性差的等缺点。应用该方法时, 发射端系统发射数字信号, 由高低电平控制开关来控制输出信号, 使其转变为包含两类信息的随机交替混合信号, 当发送一类信息时, 两个响应系统中的其中一个因同步信号而进行混沌同步, 而另一个系统会受到非同步信号驱动, 因此不会有同步现象, 当发送另一类信息时, 两个响应系统的驱动情况、同步现象将于前面相反。根据以上工作原理可得到相应的方程及 Lyapunov 函数结果, 一些研究中利用该方法进行系统测试, 最终显示数字信号通过混沌键控系统被成功传输。

#### 3.3 混沌参数调制保密通信

该方法是当前混沌系统应用在保密通信上的主要技术, 其技术思想为: 通过调制传输信号中各项参数/变量, 以将所发送的有用信息隐藏于系统复杂的参数之中, 驱动信号被发送后, 响应系统将在短时间内与驱动系统实现信号同步, 接受并获取有用信号。在接收端, 参数调制可能产生同步信号误差, 因此需要在接收端, 检测驱动系统接收信号和响应系统输出信号间误差, 以解调有用的信号。进行数值仿真测试上课, 可将有用信息设置为数字信息, 然后用数字信息来调制系统参数, 当传输不同的数字信息时, 系统获得不同的参数, 而不同参数下驱动系统和相应系统的同步状态是不一样的, 在某些参数下, 二者是不同步的, 因此存在信息误差, 而传输另一些数字信息时, 两个系统同步。在完整的通信过程中, 混沌系统需要频繁转换同步状态, 而接收端根据自身检测到的信号同步误差的幅值情况, 来判断信号并解调出有用信息。

### 4 异结构系统混沌同步应用于保密通信的效果分析

#### 【参考文献】

- [1] 林美丽, 袁正中, 蔡建平. 带有不确定性异结构混沌系统的有限时间同步[J]. 福建工程学院学报, 2019(1): 14-18.
- [2] 毛北行, 李巧利. 分数阶参数不确定系统的异结构混沌同步[J]. 中国海洋大学学报, 2017(3): 99-103.

本文结合异结构同步实验, 对异结构系统同步方法进行了研究, 也进行了数值模拟, 而测试显示该方法能较好地实现异结构系统的混沌同步。但混沌系统的种类很多, 实际应用中, 需要合适的选择驱动系统、响应系统, 来增加攻击者判断系统类型、破译通信信息的难度; 一些混沌系统能极端敏感的感知参数及其变化, 因此实际应用中可选取较大范围的系统参数, 这样一来即使攻击者能够确定采用的混沌系统, 也很难完整的得到系统参数进行同步破译, 所获得的信息将有很大的偏差。基于混沌遮掩等保密通信方法, 还可适当变换有用信号的函数, 从而进一步增加信息破译难度, 这样一来攻击者即使获得了变换后的信号, 也很难全面、准确找出相应函数将信号还原, 这样就进一步提高了通信信息的安全保密性。

混沌遮掩、键控、参数调制作为常用的混沌同步保密通信方法, 有各自的特点及应用优缺点, 因此实际应用中因合理的选择并加以优化。混沌遮掩技术发展时间最早, 其应用时间长, 具有明显的类随机性, 实际应用中易被攻击者当作噪声而忽略, 因此保密性能良好; 然而, 若有用信息的误差幅值过大, 将会影响整个系统的信息同步质量, 应用混沌键控时, 需要采取相关方法来有效避免简单键控中响应混沌系统因被动同步而容易被干扰的问题, 采用积分比较等方法更好的避免延时引起的信号误差; 由于混沌参数调制的基本思想是将信息隐藏于系统复杂参数中, 从而能获得比前两种技术更号的保密性能, 具有更好研究前景, 实际应用中可采用提取能量均值等解调方法以获取有用信息, 这样一来即能有效地避免信号在传输时因延时出现信号误差, 又克服了传输的信号存在大量毛刺的弊病, 最终提升了异结构同步传输加密信息的质量。

**作者简介:** 乔佳乐 (1990.6—), 女, 黑龙江绥化人, 硕士, 助教, 研究方向: 纳米天线, 混沌同步; 侯冬梅 (1980.12—), 女, 黑龙江齐齐哈尔人, 硕士, 讲师, 研究方向: 控制理论, 混沌同步; 通讯作者: 张艳鹏 (1979.8—), 男, 黑龙江宁安人, 硕士, 副教授, 研究方向: 混沌同步, 保密通信, 信号处理, 邮箱: zyp\_shxy@163.com。

**项目:** 黑龙江省省属高校基本科研项目《混沌同步理论及其在保密通信系统中的应用研究》(KYYWF1023619 0109); 黑龙江省省属高校基本科研项目《混沌信号的随机化处理相关研究》(KYYWF180102)。