doi:10.11959/j.issn.1000-436x.2017062

分布式、大规模、多信号系统的混沌族群保密通信研究

孙广明[1]，黄金杰[1]，刘乔[2]
(1. 哈尔滨理工大学计算机科学与技术学院，黑龙江 哈尔滨 150080; 2.哈尔滨理工大学管理学院，黑龙江 哈尔滨 150080)

摘 要：现代复杂通信系统具有分布式、规模大、接入信号多和并行传输等特征，其通信安全问题日益突显。在分析混沌族群系统的演化方法以及混沌族群系统的统一同步问题的基础上，构建三维空间混沌系统的转动模型。以 Newton-Leipnik 系统为研究对象，利用 3 路不同的通信信号，对混沌族群的演化、混沌族群系统的统一同步进行了仿真和验证。实验结果证明了该方法的有效性，应用前景良好。

关键词：混沌；混沌同步；混沌吸引子；保密通信
中图分类号：TN918 **文献标识码**：A

Research on the chaotic group secret communication of the distributed , large-scale and multi-signal system

SUN Guang-ming[1], HUANG Jin-jie[1], LIU Qiao[2]
(1. School Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China;
2. Management School, Harbin University of Science and Technology, Harbin 150080, China)

Abstract: Modern complicated communication system has the characteristics of distributed, large scales, multiple-imput signals and parallel transmission, which result in the increasing urgent problem of communication security. Based on the analysis on the evolution method and the unification-synchronization problem of the chaotic group system, a rotation model of 3D chaotic system was established. With the Newton-Leipnik system as study object, three different types of communication signals to simulate and validate the evolution of chaotic group, and the unification and synchronization of the chaotic group system was utilized. Experimental results show that the method presented in this study is effective and has a good prospect for the application.

Key words: chaos, chaos synchronization, chaotic attractor, security communication

1 引言

混沌信号具有对初始条件的微小变化初值高度敏感以及不稳定性等类似密码系统特征，混沌同步现象的发现[1,2]，使混沌系统引入保密通信领域成为必然。混沌同步研究是当前非线性科学一个非常重要的分支，国内外进行了大量的研究工作[3~5]。文献[3]研究了一种改进的广义函数投影同步方法。文献[4]研究了具有未知参数的时滞混沌系统的自适应脉冲同步。文献[5]研究了不同维混沌系统在不同尺度上的混沌同步问题。

近年来，随着信息安全事件的频发，信息安全尤为重要[6]。2010 年，“震网”病毒出现。2012 年，伊朗石油部和国家石油公司遭病毒攻击，伊朗方面暂时切断海湾附近哈尔克岛石油设施的网络连接。

保障大规模、复杂系统的通信安全，建立健全可靠、安全的复杂通信系统，已经成为当前计算机、通信、工业自动化领域[7,8]重要的课题和研究热点。在

收稿日期：2016-07-22；**修回日期**：2017-01-18
基金项目：黑龙江省自然科学基金资助项目（No.F201222）；黑龙江省教育厅科技基金资助项目（No.12511105）；哈尔滨市科技创新人才研究专项资金资助项目（No.2007RFXXG023）
Foundation Items: The Natural Science Foundation of Heilongjiang Province (No.F201222), The Science Foundation of Educational Department of Heilongjiang Province (No.12511105), The Science and Technology Foundation for Innovative Talents of Harbin (No.2007RFXXG023)

大型工业系统中，均体现多参量采集的特点[9~11]，由于具有混沌和密码系统的相似性，各国学者们进行了大量关于混沌通信的研究。文献[12]提出了利用 2 个半导体激光器的混沌保密通信系统。文献[13]研究了一种基于高功率加密信号的间接耦合同步方案的混沌通信方法。文献[14]研究了一种新的远程多路双向混沌通信系统。文献[15]采用多模光反馈半导体激光器构建了多通道双向混沌通信系统。

综上，对混沌同步、混沌保密通信的研究，仅限于有限的混沌系统(如 2 个或几个混沌系统)之间对少量信号通道的保密通信研究，对于混沌族群的生成方法、混沌族群的统一同步问题和具有分布式、规模大、接入信号多、并行传输的现代复杂通信系统的混沌通信问题的研究较少。

据此，本文主要在以下方面进行了研究：1) 构建了三维空间混沌系统的转动模型；2) 研究了一种混沌族群系统的演化方法，并进行数学描述；3) 对本文提出的混沌族群系统的统一同步问题进行了研究，并以 Newton-Leipnik 系统为研究对象进行了仿真和验证；4) 对于日益突显的现代通信信息安全问题，基于以上混沌族群系统统一同步的研究成果，提出了一种适合分布式、规模大、接入信号多、并行传输的现代复杂通信系统的保密通信系统的方案，并以 Newton-Leipnik 系统为研究对象，加载 3 路不同的通信信号，进行了仿真和验证。

2　三维空间转动模型

动力系统在三维空间转动变换是指系统空间动力轨迹围绕某一坐标轴转动，假定 θ 为围绕坐标轴转动的角度。转动后系统的每一个点轨迹相对于原位置均以角度 θ 转动，轨迹在三维空间内的位置发生变化，形状特征等不发生改变。

2.1　理论模型

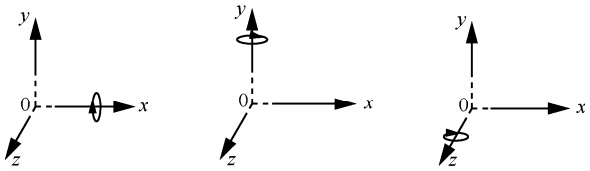
根据三维空间转动的理论，定义三维空间 R^3 内系统围绕坐标轴的转动矩阵 $\boldsymbol{\omega}$ 为

$$\boldsymbol{\omega}_x=\begin{bmatrix}1 & 0 & 0\\ 0 & \cos\theta_x & -\sin\theta_x\\ 0 & \sin\theta_x & \cos\theta_x\end{bmatrix}$$

$$\boldsymbol{\omega}_y=\begin{bmatrix}\cos\theta_y & 0 & \sin\theta_y\\ 0 & 1 & 0\\ -\sin\theta_y & 0 & \cos\theta_y\end{bmatrix}$$

$$\boldsymbol{\omega}_z=\begin{bmatrix}\cos\theta_z & -\sin\theta_z & 0\\ \sin\theta_z & \cos\theta_z & 0\\ 0 & 0 & 1\end{bmatrix}$$

其中，θ_x、θ_y、θ_z 分别为三维空间 R^3 内，系统围绕 X、Y、Z 坐标轴转动的角度，其决定了三维空间 R^3 内，系统运动轨迹转动的方向和位置，如图 1 所示。



(a) 围绕X轴转动　(b) 围绕Y轴转动　(c) 围绕Z轴转动

图 1　空间转动示意

三维空间 R^3 中，令 θ 为转动角度，考虑如下形式的混沌系统为

$$\dot{x}=f(\boldsymbol{x}) \tag{1}$$

其中，$\boldsymbol{x}=[x_1,x_2,x_3]^{\mathrm{T}}\in R^3$ 为系统状态变量，$f(\boldsymbol{x}):R^3\to R^3$，系统非线性状态向量函数。

定义 1　三维空间 R^3 中，设有非线性混沌系统 $\dot{x}\in R^3$，$\dot{x}$ 以角度 θ 围绕坐标轴转动，$\boldsymbol{\omega}$ 为转动矩阵，转动后的系统可以描述为 $\dot{x}_\theta$，称系统 $\dot{x}$ 为转动源系统，$\dot{x}_\theta$ 为以 θ 耦合的转动子系统，称 θ 为转动耦合角度。

给定转动耦合角度为 θ，转动矩阵 $\boldsymbol{\omega}$，则转动源系统和耦合的转动子系统的数学关系模型可以描述为

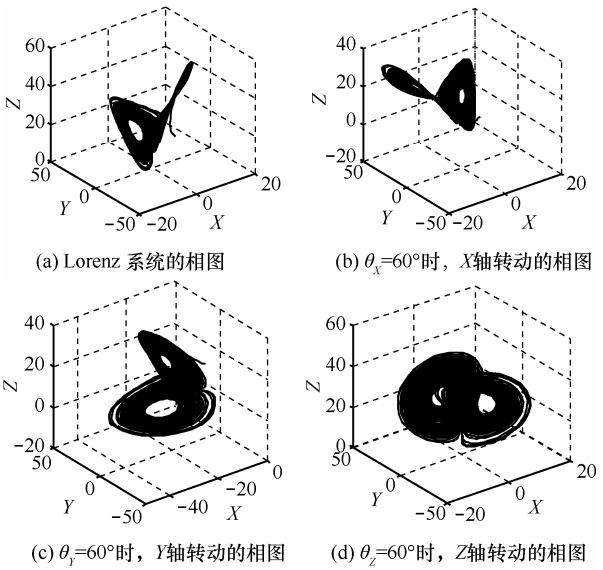
$$\dot{x}_\theta=g(\boldsymbol{x}_\theta)=h(\boldsymbol{\omega}_\theta,f(\boldsymbol{x}))=\boldsymbol{\omega}_\theta\dot{x} \tag{2}$$

其中，$\boldsymbol{x}_\theta=[x_{1\theta},x_{2\theta},x_{3\theta}]^{\mathrm{T}}\in R^3$ 为系统状态变量，$h(\boldsymbol{\omega}_\theta,f(\boldsymbol{x})):R^3\to R^3$，$\boldsymbol{\omega}_\theta$ 为转动矩阵系统，非线性状态向量函数。

图 2 是以 Lorenz 混沌系统[15]为转动源系统，以耦合角度 $\theta=60°$，分别围绕 X、Y、Z 坐标轴转动的情况。从图 2 可见，Lorenz 混沌系统在相空间内转动后，轨迹形态、空间拓扑特征没有发生改变，轨迹在空间的位置发生改变。

2.2　角度耦合混沌族群体系的演化

对于同一转动源系统 $\dot{x}$，若系统的耦合角度分别为 θ_1、θ_2、…、θ_n，n 为整数，转动矩阵分别为 $\boldsymbol{\omega}_1$、$\boldsymbol{\omega}_2$、…、$\boldsymbol{\omega}_n$，当 $\theta_1\neq\theta_2\neq\cdots\neq\theta_n$ 且 $\theta\in(n\pi,(n+2)\pi)$ 时，可以演化出多个转动子系统为 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$。



(a) Lorenz 系统的相图 (b) θ_X=60°时，X轴转动的相图

(c) θ_Y=60°时，Y轴转动的相图 (d) θ_Z=60°时，Z轴转动的相图

图 2 Lorenz 系统转动的相图

定理 1 三维空间 R^3 中，非线性混沌系统 $\dot{x}$ 以角度 θ_1、θ_2、…、θ_n 转动，当 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$ 且 $\theta \in (n\pi,(n+2)\pi)$ 时，可以得到对应的转动子系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$，n 为正整数，那么，$\dot{x}_{\theta_1} \neq \dot{x}_{\theta_2} \neq \cdots \neq \dot{x}_{\theta_n}$。

证明 由于三维空间 R^3 中，存在非线性混沌系统 $\dot{x}$，以角度 θ_1、θ_2、…、θ_n 转动，当 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$ 且 $\theta \in (n\pi,(n+2)\pi)$ 时，可以得到对应的转动子系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$，n 为正整数。

由式(2)知 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$ 可以描述为

$$\begin{cases} \dot{x}_{\theta_1} = \boldsymbol{\omega}_{\theta_1}\dot{x} \\ \dot{x}_{\theta_2} = \boldsymbol{\omega}_{\theta_2}\dot{x} \\ \quad\vdots \\ \dot{x}_{\theta_n} = \boldsymbol{\omega}_{\theta_n}\dot{x} \end{cases}$$

其中，$\boldsymbol{\omega}_{\theta_1}$、$\boldsymbol{\omega}_{\theta_2}$、…、$\boldsymbol{\omega}_{\theta_n}$ 为转动矩阵。当 θ_1、θ_2、…、θ_n 为非线性动力系统 $\dot{x}$ 围绕 X 轴转角时，有

$$\boldsymbol{\omega}_{\theta_1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta_1 & -\sin\theta_1 \\ 0 & \sin\theta_1 & \cos\theta_1 \end{bmatrix}$$

$$\boldsymbol{\omega}_{\theta_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta_2 & -\sin\theta_2 \\ 0 & \sin\theta_2 & \cos\theta_2 \end{bmatrix}$$

$$\vdots$$

$$\boldsymbol{\omega}_{\theta_n} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta_n & -\sin\theta_n \\ 0 & \sin\theta_n & \cos\theta_n \end{bmatrix}$$

由矩阵理论知，矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 相等的条件如下。

1) 矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 同型，即行数与列数都相等。

2) 矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$ 对应位置的元素相等。

由于系统 $\dot{x}$ 在相空间内转角 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$ 且 $\theta \in (n\pi,(n+2)\pi)$，所以此时转动矩阵为 $\boldsymbol{\omega}_{\theta_1} \neq \boldsymbol{\omega}_{\theta_2} \neq \cdots \neq \boldsymbol{\omega}_{\theta_n}$，即 $(\dot{x}_{\theta_1} = \boldsymbol{\omega}_{\theta_1}\dot{x}) \neq (\dot{x}_{\theta_2} = \boldsymbol{\omega}_{\theta_2}\dot{x}) \neq \cdots \neq (\dot{x}_{\theta_n} = \boldsymbol{\omega}_{\theta_n}\dot{x})$。

同理，当非线性动力系统 $\dot{x}$ 围绕 Y、Z 轴以角度 θ_1、θ_2、…、θ_n 转动，当 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$ 且 $\theta \in (n\pi,(n+2)\pi)$ 时，均有 $\dot{x}_{\theta_1} \neq \dot{x}_{\theta_2} \neq \cdots \neq \dot{x}_{\theta_n}$ 成立，定理 1 得证。

定义 2 三维空间 R^3 中，设有非线性混沌系统 $\dot{x}$，耦合角度 θ_1、θ_2、…、θ_n，得到转动子系统分别为 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$，其中，θ_1、θ_2、…、$\theta_n \in (n\pi,(n+2)\pi)$，$n$ 为整数，且 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$，那么 $\dot{x}$、$\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$ 组成 θ 耦合混沌族群系统，统一称之为角度耦合混沌族群系统，进一步统一描述为

$$\begin{cases} \dot{x} = f(\boldsymbol{x}) \\ \dot{x}_{\theta_1} = g_{\theta_1}(x_{\theta_1}) = h_{\theta_1}(\boldsymbol{\omega}_{\theta_1}, f(x_{\theta_1})) \\ \quad\vdots \\ \dot{x}_{\theta_n} = g_{\theta_n}(x_{\theta_n}) = h_{\theta_n}(\boldsymbol{\omega}_{\theta_n}, f(x_{\theta_n})) \end{cases} \tag{3}$$

2.3 角度耦合混沌族群系统统一同步

对于系统 $\dot{x}$ 的耦合角度分别为 θ_1、θ_2、…、$\theta_n \in (n\pi,(n+2)\pi)$，$n$ 为整数，则当 $\theta_1 \neq \theta_2 \neq \cdots \neq \theta_n$ 时，对应的角度耦合的混沌族群系统为 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$。系统 $\dot{x}$ 作为驱动系统，系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$ 作为响应系统，那么含有控制器的同步响应系统可统一描述为

$$\begin{cases} \dot{x} = f(\boldsymbol{x}) \\ \dot{x}_{\theta_1} = f_{\theta_1}(x_{\theta_1}) = h_{\theta_1}(\boldsymbol{\omega}_{\theta_1}, f(x_{\theta_1})) + \boldsymbol{u}(\theta)_1 \\ \quad\vdots \\ \dot{x}_{\theta_n} = f_{\theta_n}(x_{\theta_n}) = h_{\theta_n}(\boldsymbol{\omega}_{\theta_n}, f(x_{\theta_n})) + \boldsymbol{u}(\theta)_n \end{cases} \tag{4}$$

其中，$\boldsymbol{u}(\theta)_n$ 为混沌族群同步控制矩阵，其族群动态系统误差为

$$\dot{e}_{\theta_n} = \dot{x}_{\theta_n} - \dot{x} = h_{\theta_n}(\boldsymbol{\omega}_{\theta_n}, f(x_{\theta_n})) - f(x) + \boldsymbol{u}(\theta)_n \tag{5}$$

定义 3 系统 $\dot{x}$ 的 θ 耦合混沌族群系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$，如果存在一个族群同步控制器 $\boldsymbol{u}(\theta)_n$，使在任意初始状态下，均有

$$\lim_{t\to\infty}\left\|e_{\theta_n}(t)\right\|=\lim_{t\to\infty}\left\|x_{\theta_n}(t)-x(t)\right\|=0 \tag{6}$$

其中，θ_1、θ_2、…、$\theta_n\in(n\pi,(n+2)\pi)$，$n$ 为整数，式(6)成立，称为角度耦合混沌族群系统达到统一同步。

由定义 3 可知，角度耦合混沌族群混沌系统在族群同步控制矩阵 $\boldsymbol{u}(\theta)_n$ 的作用下，达到统一同步状态包含如下 2 个含义。

1) 当 $t\to\infty$ 时，群系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$ 统一同步于系统 $\dot{x}$。

2) 当 $t\to\infty$ 时，每个子系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$ 自身均实现同步，即任意 2 个或多个子系统进入同步状态。

定理 2　对于系统 $\dot{x}$ 的族群系统 $\dot{x}_{\theta_1}$、$\dot{x}_{\theta_2}$、…、$\dot{x}_{\theta_n}$，存在族群同步控制矩阵为

$$\boldsymbol{u}(\theta)_n=x-x_{\theta_n}-h_{\theta_n}(\boldsymbol{\omega}_{\theta_n},f(x_{\theta_n}))+f(x)$$

其中，θ_1、θ_2、…、$\theta_n\in(n\pi,(n+2)\pi)$，$n$ 为整数，使在任意条件下，误差系统式(6)成立，即角度耦合混沌族群达到统一同步。

证明　在三维空间 R^3 中，当选取控制器

$$\boldsymbol{u}(\theta)_n=x-x_{\theta_n}-h_{\theta_n}(\boldsymbol{\omega}_{\theta_n},f(x_{\theta_n}))+f(x)$$

其中，θ_1、θ_2、…、$\theta_n\in(n\pi,(n+2)\pi)$，$n$ 为整数时，对于式(5)误差系统，进一步写为

$$\dot{e}_{1\theta_n}=\dot{x}_{1\theta_n}-\dot{x}_1=h_{1\theta_n}(\boldsymbol{\omega}_{1\theta_n},f(x_{1\theta_n}))-f(x_1)+\boldsymbol{u}_1(\theta)_n \tag{7}$$

将选取的控制器为

$$\boldsymbol{u}_1(\theta)_n=x_1-x_{1\theta_n}-h_{1\theta_n}(\boldsymbol{\omega}_{1\theta_n},f(x_{1\theta_n}))+f(x_1)$$

代入式(7)得

$$\dot{e}_{1\theta_n}=x_1-x_{1\theta_n}=-e_{1\theta_n}$$

同理

$$\dot{e}_{2\theta_n}=x_2-x_{2\theta_n}=-e_{2\theta_n}$$

$$\dot{e}_{3\theta_n}=x_3-x_{3\theta_n}=-e_{3\theta_n}$$

构造如下 Lyapunov 函数[16,17]

$$V_{\theta_n}=\frac{1}{2(e_{1\theta_n}^2+e_{2\theta_n}^2+e_{3\theta_n}^2)}$$

则有

$$\begin{aligned}\frac{\mathrm{d}V_{\theta_n}}{\mathrm{d}t}&=e_{1\theta_n}\dot{e}_{1\theta_n}+e_{2\theta_n}\dot{e}_{2\theta_n}+e_{3\theta_n}\dot{e}_{3\theta_n}\\&=-e_{1\theta_n}^2-e_{2\theta_n}^2-e_{3\theta_n}^2\leqslant 0\end{aligned} \tag{8}$$

所以，$\dfrac{\mathrm{d}V_{\theta_n}}{\mathrm{d}t}$ 为负半定，由 Lyapunov 稳定性定理，可知在三维空间 R^3 中，族群动态误差系统渐进稳定[18,19]，误差系统式(6)成立，定理 2 得证。

2.4　仿真研究

Newton-Leipnik 系统[20]由下列非线性微分方程描述

$$\begin{cases}\dot{x}_1=-ax_1+x_2+10x_2x_3\\ \dot{x}_2=-x_1-0.4x_2+5x_1x_3\\ \dot{x}_3=bx_3-5x_1x_2\end{cases} \tag{9}$$

其中，$\dot{x}_1$、$\dot{x}_2$ 和 $\dot{x}_3$ 是系统状态变量，典型参数为 $a=0.4$，$b=0.175$，系统存在典型吸引子。式(9)以式(8)作为转动源系统，θ_1、θ_2、…、$\theta_n\in(n\pi,(n+2)\pi)$ 为转动角度，由式(4)和定义 3 可得，其围绕 Z 坐标轴角度耦合混沌族群同步系统可以统一描述为

$$\begin{cases}\dot{x}_1=-ax_1+x_2+10x_2x_3\\ \dot{x}_2=-x_1-0.4x_2+5x_1x_3\\ \dot{x}_3=bx_3-5x_1x_2\\ \dot{x}_{1\theta_1}=\dot{x}_1\cos\theta_1-\dot{x}_2\sin\theta_1+\boldsymbol{u}_1(\theta_1)\\ \dot{x}_{2\theta_1}=\dot{x}_1\sin\theta_1+\dot{x}_2\cos\theta_1+\boldsymbol{u}_2(\theta_1)\\ \dot{x}_{3\theta_1}=\dot{x}_3+\boldsymbol{u}_3(\theta_1)\\ \quad\vdots\\ \dot{x}_{1\theta_n}=\dot{x}_1\cos\theta_n-\dot{x}_2\sin\theta_n+\boldsymbol{u}_1(\theta_n)\\ \dot{x}_{2\theta_n}=\dot{x}_1\sin\theta_n+\dot{x}_2\cos\theta_n+\boldsymbol{u}_2(\theta_n)\\ \dot{x}_{3\theta_n}=\dot{x}_3+\boldsymbol{u}_3(\theta_n)\end{cases} \tag{10}$$

其中，$\boldsymbol{u}(\theta_n)$ 为族群同步控制器。由式(5)可得，其动态误差系统可以描述为

$$\begin{cases}\dot{e}_{1\theta_1}(\theta_1)=\dot{x}_{1\theta_1}-\dot{x}_1=\dot{x}_1\cos\theta_1-\dot{x}_2\sin\theta_1-\dot{x}_1+\boldsymbol{u}_1(\theta_1)\\ \dot{e}_{2\theta_1}(\theta_1)=\dot{x}_{2\theta_1}-\dot{x}_2=\dot{x}_1\sin\theta_1+\dot{x}_2\cos\theta_1-\dot{x}_2+\boldsymbol{u}_2(\theta_1)\\ \dot{e}_{3\theta_1}(\theta_1)=\dot{x}_{3\theta_1}-\dot{x}_3+\boldsymbol{u}_3(\theta_1)\\ \quad\vdots\\ \dot{e}_{1\theta_n}(\theta_n)=\dot{x}_{1\theta_n}-\dot{x}_1=\dot{x}_1\cos\theta_n-\dot{x}_2\sin\theta_n-\dot{x}_1+\boldsymbol{u}_1(\theta_n)\\ \dot{e}_{2\theta_n}(\theta_n)=\dot{x}_{2\theta_n}-\dot{x}_2=\dot{x}_1\sin\theta_1+\dot{x}_2\cos\theta_1-\dot{x}_2+\boldsymbol{u}_2(\theta_n)\\ \dot{e}_{3\theta_n}(\theta_n)=\dot{x}_{3\theta_n}-\dot{x}_3+\boldsymbol{u}_3(\theta_n)\end{cases} \tag{11}$$

由定理 2 可知，当选取控制器时，误差系统渐进稳定，当 $t\to\infty$ 时，可以达到式(9)的角度耦合混沌族群系统统一同步。

$$\begin{cases} \boldsymbol{u}_1(\theta_1)=x_1-x_{1\theta_1}-\dot{x}_1\cos\theta_1+\dot{x}_2\sin\theta_1+\dot{x}_1 \\ \boldsymbol{u}_2(\theta_1)=x_2-x_{2\theta_1}-\dot{x}_1\sin\theta_1-\dot{x}_2\cos\theta_1+\dot{x}_2 \\ \boldsymbol{u}_3(\theta_1)=x_3-x_{3\theta_1}-\dot{x}_{3\theta_1}+\dot{x}_3 \\ \quad\vdots \\ \boldsymbol{u}_1(\theta_n)=x_1-x_{1\theta_n}-\dot{x}_1\cos\theta_n+\dot{x}_2\sin\theta_n+\dot{x}_1 \\ \boldsymbol{u}_2(\theta_n)=x_2-x_{2\theta_n}-\dot{x}_1\sin\theta_n-\dot{x}_2\cos\theta_n+\dot{x}_2 \\ \boldsymbol{u}_3(\theta_n)=x_3-x_{3\theta_n}-\dot{x}_{3\theta_n}+\dot{x}_3 \end{cases} \tag{12}$$

为了验证本节方法对于角度耦合混沌族群统一同步的有效性，选取典型参数 $a=0.4$，$b=0.175$，分别选取 60°、151.2°、288° 这 3 组参数对结果进行仿真。选取系统初始值为

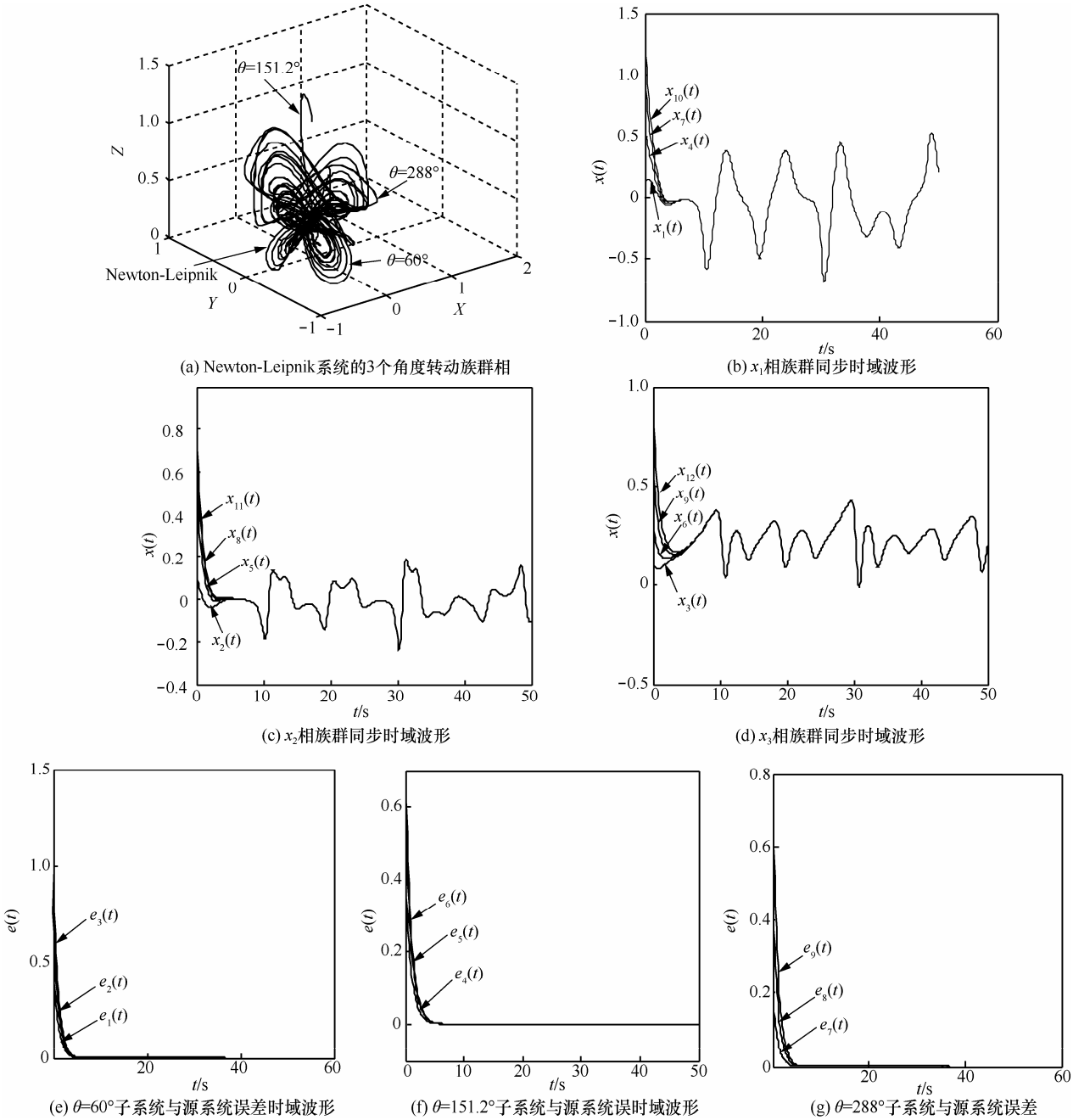
$$[x_1(0),x_2(0),x_3(0)]^{\mathrm{T}}=[0.1,0.1,0.1]^{\mathrm{T}}$$

$$[x_{1\theta_1}(0),x_{2\theta_1}(0),x_{3\theta_1}(0)]^{\mathrm{T}}=[1.1,0.7,0.3]^{\mathrm{T}}$$

$$[x_{1\theta_2}(0),x_{2\theta_2}(0),x_{3\theta_2}(0)]^{\mathrm{T}}=[0.6,0.5,0.9]^{\mathrm{T}}$$

$$[x_{1\theta_3}(0),x_{2\theta_3}(0),x_{3\theta_3}(0)]^{\mathrm{T}}=[1.5,0.8,0.6]^{\mathrm{T}}$$

从图 3 可以看出，当转动角度不同时，吸引子的空间位置不同，在控制器的作用下，7 s 内，各个



(a) Newton-Leipnik系统的3个角度转动族群相

(b) x_1相族群同步时域波形

(c) x_2相族群同步时域波形

(d) x_3相族群同步时域波形

(e) θ=60°子系统与源系统误差时域波形

(f) θ=151.2°子系统与源系统误时域波形

(g) θ=288°子系统与源系统误差

图 3　Newton-Leipnik 系统角度耦合混沌族群系统统一同步仿真

转动子系统的时域波形达到同步，整个转动族群达到统一同步，同理可以推广到 X 轴、Y 轴情况。

Newton-Leipnik 系统作为源系统分别以 60°、151.2° 和 288° 的转动子系统的空间吸引子，如图 3(a)所示，转动子系统的每一个点轨迹相对于转动源系统而言，轨迹在三维空间内的位置发生变化，但形状、空间拓扑等特征没有改变。

图 3(b)~图 3(d)分别为族群系统在相空间内 X 相、Y 相、Z 相的时域波形，从图 3 看出，在 7 s 内整个混沌族群系统达到统一同步状态。图 3(e)~图 3(g)分别为转动子系统与源系统的误差分析，随着时间的推移，在 7 s 左右，族群系统的误差接近于 0，表征整个族群系统达到统一同步。

3　多通道、族群保密通信

随着信息安全事件的频发[6]，信息安全尤为重要。保障系统的通信安全，特别是建立适合具有分布式、大规模、并行传输安全通信已经成为当前计算机、通信领域重要的课题和研究热点。前文研究了混沌系统在相空间内转动形成角度耦合的混沌族群系统，并研究了族群系统的统一同步方法。本文在利用上述模型的基础上，提出了一种适合大规模数据传输系统的保密通信方法。

3.1　多数据通道的族群保密通信系统

n 路信号的大规模、并行传输的信号族群保密通信系统如图 4 所示，其保密通信的基本原理为：设有混沌系统 $\dot{x}\in R^3$，指定 n 个 θ_1、θ_2、…、$\theta_n\in(n\pi,(n+2)\pi)$，$n$ 为整数，且 $\theta_1\neq\theta_2\neq\cdots\neq\theta_n$。采集端各路独立明文数据，经过相对应的各不相同的转动子系统，由单路加密算法代换加密，后经信道传输至转动源系统解密服务器，前文已经证明，角度耦合的转动族群系统在族群同步控制器作用下，可同步于转动源系统，所以将转动源系统作为同步解密服务器，即恢复各通道明文数据。

3.2　单路加密算法

由定义 1 和式(2)知，三维空间 R^3 中，设有非线性混沌系统 $\dot{x}=f(\boldsymbol{x})$，$\boldsymbol{x}=[x_1,x_2,x_3]^{\mathrm{T}}\in R^3$，$\dot{x}$ 以角度 θ 围绕坐标轴转动的转动子系统描述为 $\dot{x}_\theta$，$\boldsymbol{x}_\theta=[x_{\theta1},x_{\theta2},x_{\theta3}]^{\mathrm{T}}\in R^3$。

对于单路数据的加密，可采用图 5 的方案。加

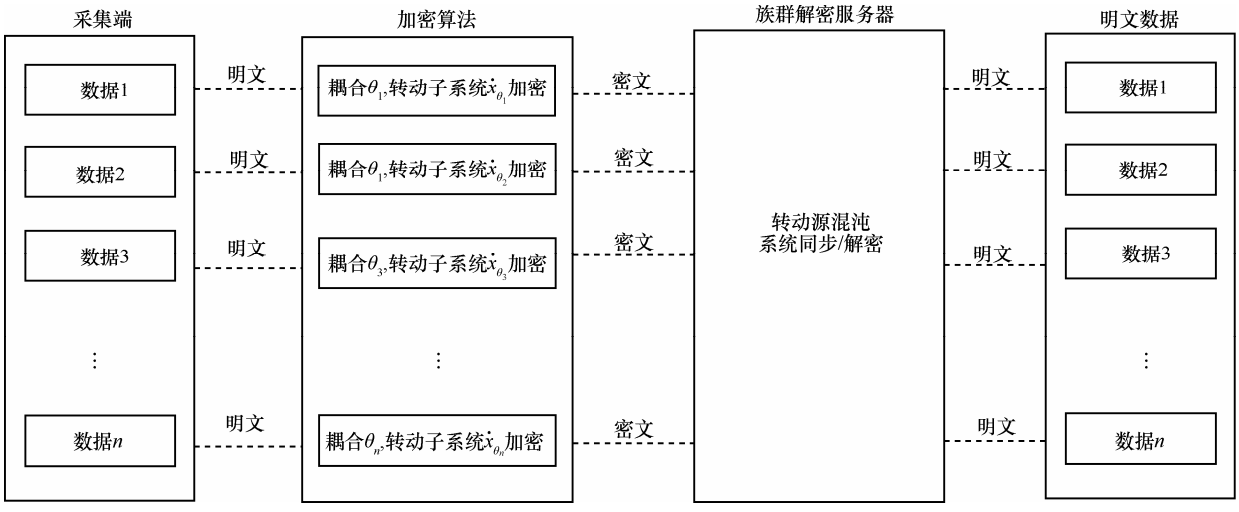


图 4　无限数据通道的族群保密通信系统

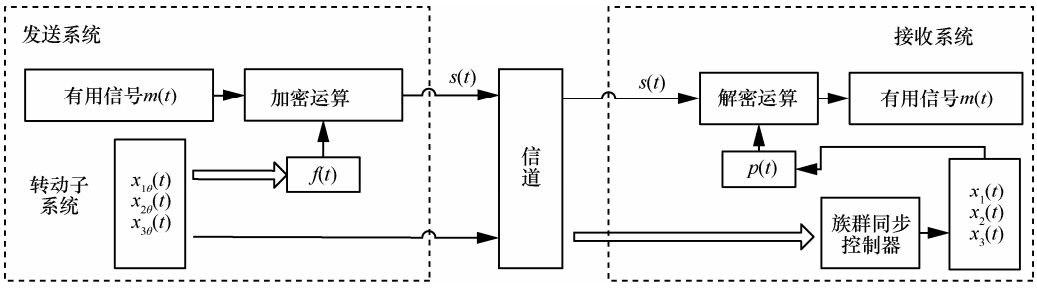


图 5　转动子系统保密通信方案

密的基本原理为其通信的基本原理，是发送端的转动子混沌系统，输出类似噪声的混沌信号，通过载波信源合成函数 $f(t)$，选择混沌载波信源，在这个混沌信源上叠加需要的有用信号 $m(t)$，通过信道将合成信号 $s(t)$发送出去；在接收端通过族群同步控制器，实现转动源系统与子系统的同步状态，从接收的混合信号中去掉同步重构的混沌信号，从而解调出发送的有用信息 $m(t)$。

设有用信号为 $m(t)$，合成密文信号为 $s(t)$、$f(t)$为载波信源函数。

在发送系统为

$$s(t) = f(t) - km(t) \tag{13}$$

其中，k 为有用信号比例系数，k 的选择使有用信号小于混沌信号的 $\frac{1}{4}$。

由转动子系统式(2)，定义发送系统的比较判别函数为

$$f(t) = \begin{cases} x_{1\theta}(t), & x_{2\theta}(t) > x_{3\theta}(t) \\ x_{2\theta}(t), & x_{2\theta}(t) < x_{3\theta}(t) \\ x_{3\theta}(t), & x_{2\theta}(t) = x_{3\theta}(t) \end{cases} \tag{14}$$

接收系统为

$$m(t) = s(t) + kp(t) \tag{15}$$

其中，$p(t)$为接收系统信源合成函数，由转动源系统式(1)定义如下

$$p(t) = \begin{cases} x_1(t), & x_2(t) > x_3(t) \\ x_2(t), & x_2(t) < x_3(t) \\ x_3(t), & x_2(t) = x_3(t) \end{cases} \tag{16}$$

有用信号 $m(t)$经过发送端转换，合成密文信号 $s(t)$，由信道传输到达接收系统，经过转动族群同步控制器使转动子系统与转动源系统同步，进入接收端合成函数 $p(t)$，得到恢复的信号 $m(t)$。

3.3 多数据通道族群保密系统性能测试

本文选择 3 路常见信号类型进行如下实验。

第 1 路：连续模拟量信号 $m_1(t)$=cos(t)。

第 2 路：指数分布的信号 $m_2(t)$。

第 3 路：音频片段信号 $m_3(t)$。

选取 Newton-Leipnik 系统，选取典型参数 $a = 0.4$，$b = 0.175$，有用信号比例系数 k=1，分别选取 60°、151.2°和 288°这 3 组参数对结果进行仿真。选取系统初始值为

$$[x_1(0), x_2(0), x_3(0)]^{\mathrm{T}} = [0.1, 0.1, 0.1]^{\mathrm{T}}$$
$$[x_{1\theta_1}(0), x_{2\theta_1}(0), x_{3\theta_1}(0)]^{\mathrm{T}} = [15, 13, 14]^{\mathrm{T}}$$
$$[x_{1\theta_2}(0), x_{2\theta_2}(0), x_{3\theta_2}(0)]^{\mathrm{T}} = [5, 2, 4]^{\mathrm{T}}$$
$$[x_{1\theta_3}(0), x_{2\theta_3}(0), x_{3\theta_3}(0)]^{\mathrm{T}} = [5, 2, 4]^{\mathrm{T}}$$

图 6 为 3 路信号的保密通信系统测试实验结果。3 路有用信号 $m_1(t)$、$m_2(t)$、$m_3(t)$ 如图 6(a)所示，分别以 60°、151.2°、288° 耦合的转动子系统构成的混沌族群系统混合传输，图 6(b)分别为有用信号 $m_1(t)$、$m_2(t)$、$m_3(t)$ 实现单路加密后的信号。从图 6 看出，信号经过单路转动子系统混沌混合后，完全掩盖了原信号的内容。图 6(c)~图 6(e)分别为接收端恢复的有用信号 $m_1'(t)$、$m_2'(t)$、$m_3'(t)$ 的误差实验，从图 6 看出，接收端同发送端的信号在 7 s 内快速同步。

3 路有用信号被保密通信系统加密和传输，并且不失真地恢复，证明了该方法的有效性。由于加密系统和解密系统同步存在时间差，可以先启动保密系统，经过时间 $\tau > 10$ s 后，再进行待加密信息发送，以保证待加密信息的完整性。对于多路信号传输，可以指定多个不相同的角度对应的子系统共同完成。理论上，可以扩展到无限通道信号同时传输。

4 结束语

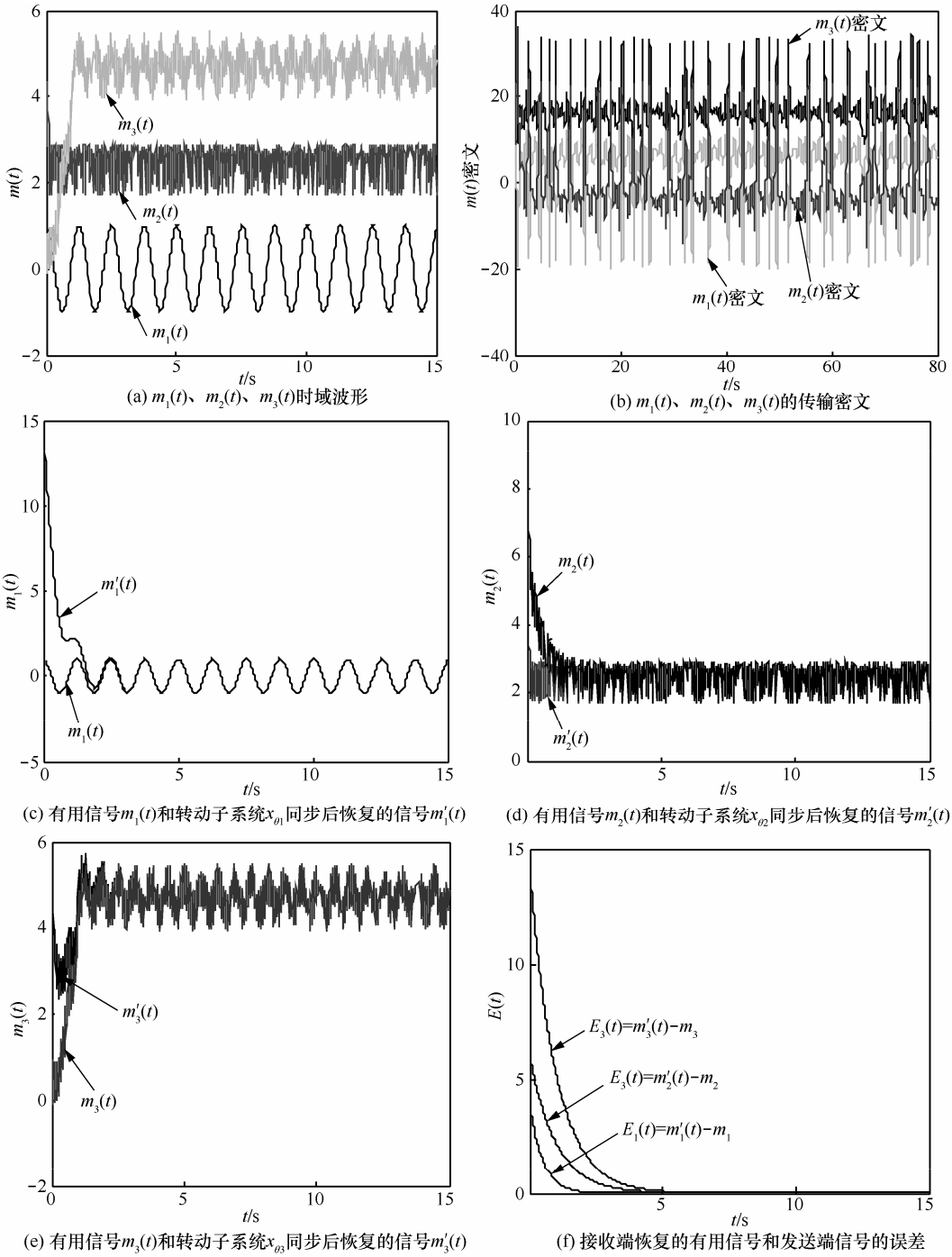
本文首先研究了混沌系统在相空间内转动的模型，提出了一种实现混沌族群系统的方法，该方法利用混沌系统以不同的角度在相空间转动，构成多个混沌转动子系统。研究了多个混沌转动子系统的统一同步问题，以 Newton-Leipnik 系统为实验对象，进行了理论和仿真验证，实验结果支持了本文的研究结论。基于本文混沌族群同步的研究成果，提出了一种适合于大规模、多信号、并行传输的复杂通信系统的保密通信方案，并对方案进行研究和验证，对系统的保密通信仿真结果表明，该方法适合大规模、多信号、并行传输的通信系统，具有很强的实用性。

参考文献：

[1] PECORA L M, CARROLL T L. The synchronization in chaotic systems[J]. Physical Review Letters, 1990, 64(4): 821-830.

[2] BOCCALETTI S, OSIPOV J K, VALLADARES D L, et al. The synchronization of chaotic systems[J]. Physics Reports, 2002, 366(1): 1-101.

[3] HAMEL S, BOULKROUNE A. A generalized function projective



(a) $m_1(t)$、$m_2(t)$、$m_3(t)$时域波形　(b) $m_1(t)$、$m_2(t)$、$m_3(t)$的传输密文

(c) 有用信号$m_1(t)$和转动子系统$x_{\theta 1}$同步后恢复的信号$m_1'(t)$　(d) 有用信号$m_2(t)$和转动子系统$x_{\theta 2}$同步后恢复的信号$m_2'(t)$

(e) 有用信号$m_3(t)$和转动子系统$x_{\theta 3}$同步后恢复的信号$m_3'(t)$　(f) 接收端恢复的有用信号和发送端信号的误差

图 6　多通道的族群保密通信系统测试

synchronization scheme for uncertain chaotic systems subject to input nonlinearities[J]. International Journal of General Systems, 2016, 45 (6): 689-710.

[4] GAO X J, CHENG M F, HU H P. Adaptive impulsive synchronization of uncertain delayed chaotic system with full unknown parameters via discrete-time drive signals[J]. Complexity, 2016, 21 (5):43-51.

[5] OUANNAS A, AL-SAWALHA M M. Synchronization between different dimensional chaotic systems using two scaling matrices[J]. Optik-International Journal for Light and Electron Optics, 2016,127(2): 959-963.

[6] JON R, LINDSA Y. Stuxnet and the limits of cyber warfare[J]. Security Studies, 2013, 22 (3):365-404.

[7] GAO J C, LIU J, RAJAN B, et al. Scada communication and security issues[J]. Security Comm Networks, 2014, 7 (1):175-194.

[8] SHUAIB K, KHALIL I, ABDEL-HAFEZ M. Communications in smart grid: a review with performance, reliability and security consideration[J]. Journal of Networks,2013,8(6):1229-1240.

[9] ZHANG Q S, FAN Y S, LIANG H, et al. The research of China made DCS application on supercritical and ultra supercritical units of Guohua electric company[J]. Applied Mechanics and Materials, 2013,

7(336): 1217-1224.

[10] GAO Q, LI H, LI J F, et al. Research and development of DCS test software based on the OPC technology[C]//National Conference for Engineering Sciences. 2012: 2089-2091.

[11] ZHANG X Y, WU Y, MO C J. Generic and automatic multi-channel control system[J]. Advanced Materials Research, 2014, 1046: 310-314.

[12] MENGUE A D, ESSIMBI B Z. Secure communication using chaotic synchronization in mutually coupled semiconductor lasers[J]. Nonlinear Dynamics, 2012, 70 (2):1241-1253.

[13] SENOUCI A, BOUKABOU A, BUSAWON K, et al. Robust chaotic communication based on indirect coupling synchronization[J]. Circuits, Systems, and Signal Processing, 2015,34 (2):393-418.

[14] XIE Y Y, LI J C, HE C, et al. Long-distance multi-channel bidirectional chaos communication based on synchronized VCSELs subject to chaotic signal injection[J]. Optics Communications, 2016, 377(15) : 1-9.

[15] LORENZ. Deterministic non-periodic flows[J]. J Atmos Sci, 1963,20: 130-141.

[16] PARK J H. On synchronization of unified chaotic systems via nonlinear control[J]. Chaos, Solitons and Fractals, 2005,25:699-704.

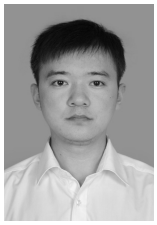
[17] WANG H, HAN Z Z, ZHANG W, et al. Chaos control and synchronization of unified chaotic systems via linear control[J]. Journal of Sound and Vibration, 2009,320(1): 365-372.

[18] LI C D, ZHOU Y H, WANG H, et al. Stability of nonlinear systems with variable-time impulses: B-equivalence method[J]. International Journal of Control, Automation and Systems, 2013,11(3): 643-647.

[19] LI C J, YU X H, YU W W, et al. Distributed event-triggered scheme for economic dispatch in smart grids[J]. IEEE Transactions on Industrial Informatics, 2015, 12(5): 1775-1785.

[20] WANG X, TIAN L. Bifurcation analysis and linear control of the Newton-Leipnik system[J]. Chaos, Solitons & Fractals, 2006, 27(1): 31-38.

作者简介：



孙广明（1981-），男，黑龙江绥化人，哈尔滨理工大学博士生、工程师，主要研究方向为数据安全、工业过程控制系统、非线性系统等。

黄金杰（1967-），男，山东莱阳人，博士（后），哈尔滨理工大学教授、博士生导师，主要研究方向为人工智能、非线性系统等。

刘乔（1980-），女，黑龙江绥化人，博士，哈尔滨理工大学副教授，主要研究方向为管理科学与工程。