doi:10.11959/j.issn.1000-436x.2017151

反同步混沌系统群与大规模、多变量系统安全通信研究

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：通过构建混沌系统在相空间内关于点群对称的混沌系统群模型，并对该混沌系统群的反同步问题进行了研究，提出了一种混沌系统群反同步控制器，实现了混沌系统群的反同步。通过实验观察，混沌系统关于点对称变换后的子系统与原系统在相空间内位置发生变化，相空间动力轨迹、空间拓扑等原系统呈现对称结构。利用上述研究结论，提出了一种反同步混沌系统群的载波通信方法，解决了具有分布式、规模大、接入信号多、并行传输等特征的现代复杂通信系统的日益迫切的通信安全问题，并以永磁同步电机混沌模型，进行了仿真和验证。仿真结果表明，所提方法具有良好的应用前景，适用于现代通信系统。

关键词：安全通信；混沌；反同步；载波
中图分类号：TN911 **文献标识码**：A

Research on the anti-synchronization chaos system group & large scale distributed system security communication

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: Chaotic system model about point group symmetry in the phase space was constructed, and the anti-synchronization problem of the chaotic system group was studied. Besides, a kind of chaotic system group anti-synchronization controller was proposed, and the anti-synchronization of the chaos system group was realized. Through experimental observation, the position of chaos system about the subsystem and the source system after the point symmetry transform changed in phase space. The phase space power trajectory, space topology and other original system presented symmetrical structure. By using the above research conclusions, a kind of carrier communication method of anti-synchronization chaos system group was put forward. It solved the increasingly urgent communication security issues of modern complex distributed and large scale communication system with many access signals and parallel transmission. In addition, with permanent magnet synchronous motor chaos model, simulation and validation were conducted. The experimental results show that the method has good application prospect, and is suitable for modern communication system.

Key words: secure communication, chaotic, anti-synchronization, carrier

1 引言

在过去的 20 年里，各国学者进行了大量关于混沌系统及其相关应用的研究，其中混沌通信是一个广泛被关注的研究方向[1~8]。混沌信号具有对初始条件的微小变化初值的高度敏感和不稳定性等类似密码系统特征，以及混沌同步现象的发现[9,10]，使混沌系统引入保密通信领域成为必然。对于混沌保密通信，第一步是对将要传送的信号进行加密。通常采用的方案是对有用的信号与一个或几个混沌信号进行某种方式的混叠或调制，形成一个混合的密文流，然后通过一个开放信道传输到接收器。在开放信道中，其中一些信息可能是被黑客窃取。当接收器得到加密的信号时，利用一定的解密机制，使所

收稿日期：2016-09-30；修回日期：2017-05-26
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）
Foundation Items: The Natural Science Foundation of Heilongjiang Province (No.F201222), The Science Foundation of Educational Department of Heilongjiang Province (No.12511105)

传送的信号可以完全恢复。在信号传送过程中，一旦加密的信号在开放信道上被窃取，窃取者仍然很难恢复实际信号，因为混沌状态的不可预知性和没有相应的解密方法。因此，以上基于混沌系统的保密通信思路是可以实现，其安全性依赖于混沌系统的结构[11~13]。

近年来，随着云计算技术和物联网技术的应用，信息物理系统的拓展研究，对数据通信系统的要求趋于系统复杂化、智能化和信息安全等特点。如目前运行的大型 DCS、PLC、RTU 系统等具有分布式、规模大、多信号量、并行传输[14,15]等特点[16,17]。随着复杂系统的信息安全事件的频发[18]，信息安全尤为重要。2008 年，美国 Hatch 核电厂自动停机事件；2010 年，“震网”病毒出现；2012 年 4 月 22 日，伊朗石油部和国家石油公司遭病毒攻击。

保障系统的通信安全，特别是建立适合具有多变量通信系统[19]的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。对于以上的领域，应用于传统的混沌通信方法[1~8]，需要重复使用一个或有限的、固定的几个相同的混沌系统对多个通信量进行加密通信，由于其他信号量应用的模型完全相同，当黑客对发送端攻击并获取一个发送端的数学描述，则完全可以推理其他发送信号，进而使具有大规模、多信号量的现代通信系统变得不安全。

本文研究了一种混沌系统关于其相空间内任意一点的对称的系统模型。通过研究发现，混沌系统在其相空间关于任意一点对称的系统仍然是混沌系统，是空间拓扑呈对称且不同于原混沌系统的新混沌系统。对于在其相空间内关于不同点的对称系统，其在数学描述和空间位置上均不相同。当混沌系统在其相空间内关于点集 $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，当 $\sigma_1\neq\sigma_2\neq\cdots\neq\sigma_n$ 时，可以对应多个不同的新混沌系统组成的系统群。本文构建了系统群反同步控制器，每个通过点映射的混沌系统均同步于原混沌系统。利用该混沌系统群，研究了一种适合于分布式、大规模通信系统的保密通信方案。将混沌系统群应用于发送端，使每个信号量对应一个新的混沌系统，而后进入开放信道传输，并在接收端使用原混沌系统同步而解密通信信号。发送端的每个混沌系统均不相同，攻击者充分攻击一个或几个发送端，并获取对应的混沌系统特征，应用于其他发送变量，也很难获得其信息内容，具有不依赖单个信道发送端混沌系统结构的安全性等特点。

2 理论模型

考虑如下形式的混沌系统

$$\dot{\boldsymbol{x}}=\boldsymbol{A}_1\boldsymbol{x}+f_1(\boldsymbol{x}) \tag{1}$$

$$\dot{\boldsymbol{y}}=\boldsymbol{A}_2\boldsymbol{y}+f_2(\boldsymbol{y}) \tag{2}$$

其中，$\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$，$\boldsymbol{y}=[y_1,y_2,\cdots,y_n]^{\mathrm{T}}$ 为系统状态变量，$\boldsymbol{A}_1$、$\boldsymbol{A}_2$ 为系数矩阵，$f_1(\boldsymbol{x})$、$f_2(\boldsymbol{x})$ 为系统非线性状态向量函数。

定义 1 对于混沌系统(1)、系统(2)，如果存在相空间内一点 $\boldsymbol{\sigma}=[\sigma_1,\sigma_2,\cdots,\sigma_n]$，满足 $\dot{\boldsymbol{y}}=2\boldsymbol{\sigma}-\dot{\boldsymbol{x}}$，则称系统(1)、系统(2)关于相空间内点 $\boldsymbol{\sigma}$ 对称。

图 1 为 Lorenz 混沌[15]在选定初始状态为(0.5, 0.5, 1)，关于点(0,0,0)和(10,−3,2)的对称系统的吸引子。可以看出，Lorenz 在点对称映射后，映射后的系统在相空间内位置发生变化，相空间动力轨迹、空间拓扑等原系统呈现对称结构。

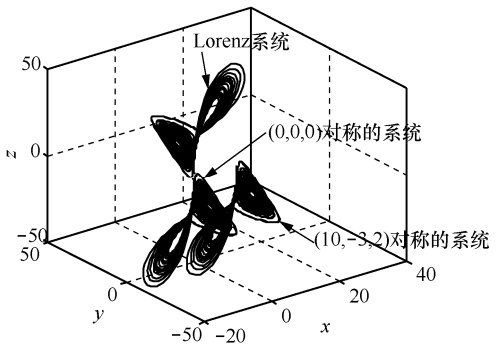


图 1 Lorenz 系统关于点(0,0,0)和点(10,−3,2)对称吸引子

定义 2 对于混沌系统(1)，如果存在相空间内一点，关于点进行对称变换得到混沌系统(2)，则称混沌系统(1)为原系统，混沌系统(2)为混沌系统(1)的对称子系统。

2.1 混沌原系统与对称子系统反同步

令混沌系统(1)作为驱动系统，其关于相空间内一点对称的系统作为响应系统，则可描述为

$$\dot{\boldsymbol{y}}=\boldsymbol{A}_2\boldsymbol{y}+f_2(\boldsymbol{y})+u(\boldsymbol{x},\boldsymbol{y}) \tag{3}$$

则驱动系统(1)和响应系统(3)反同步误差系统可以描述为

$$\begin{aligned}\dot{\boldsymbol{e}}&=\dot{\boldsymbol{y}}+\dot{\boldsymbol{x}}\\&=\boldsymbol{A}_2\boldsymbol{y}+f_2(\boldsymbol{y})+u(\boldsymbol{x},\boldsymbol{y})+\boldsymbol{A}_1\boldsymbol{x}+f_1(\boldsymbol{x})\\&=\boldsymbol{A}_2(\boldsymbol{y}+\boldsymbol{x})-\boldsymbol{A}_2\boldsymbol{x}+f_2(\boldsymbol{y})+\boldsymbol{A}_1\boldsymbol{x}+f_1(\boldsymbol{x})+u(\boldsymbol{x},\boldsymbol{y})\\&=\boldsymbol{A}_2\boldsymbol{e}+(\boldsymbol{A}_1-\boldsymbol{A}_2)\boldsymbol{x}+f_2(\boldsymbol{y})+f_1(\boldsymbol{x})+u(\boldsymbol{x},\boldsymbol{y})\end{aligned} \tag{4}$$

其中，$u(\boldsymbol{x},\boldsymbol{y})$ 为反同步控制器。

定义 3　存在控制器 $u(\boldsymbol{x},\boldsymbol{y})$，使误差系统(4)满足

$$\lim_{t->\infty}\|\dot{\boldsymbol{y}}+\dot{\boldsymbol{x}}\|=0 \tag{5}$$

则称原系统(1)与对称子系统(2)达到反同步，$\|\cdot\|$ 代表欧几里得范数。

定理 1　对于驱动系统(1)和响应系统(3)，存在控制器 $u(\boldsymbol{x},\boldsymbol{y})=-(\boldsymbol{A}_2+\Delta)\boldsymbol{e}-(\boldsymbol{A}_1-\boldsymbol{A}_2)\boldsymbol{x}-f_2(\boldsymbol{y})-f_1(\boldsymbol{x})$，$\Delta$ 为实数，且 $\Delta>0$，使驱动系统和响应系统在任意初始条件下，实现原系统(1)和其关于点对称的子系统反同步。

证明　由反同步误差系统(4)和定义 3 知，当控制器为 $u(\boldsymbol{x},\boldsymbol{y})=-(\boldsymbol{A}_2+\Delta)\boldsymbol{e}-(\boldsymbol{A}_1-\boldsymbol{A}_2)\boldsymbol{x}-f_2(\boldsymbol{y})-f_1(\boldsymbol{x})$ 时，反同步系统(4)可以写作

$$\dot{\boldsymbol{e}}=\dot{\boldsymbol{y}}+\dot{\boldsymbol{x}}=-\Delta\boldsymbol{e}$$

进一步写作如下向量形式。

$$\begin{aligned}\dot{\boldsymbol{e}}_1&=\dot{\boldsymbol{y}}_1+\dot{\boldsymbol{x}}_1=-\Delta\boldsymbol{e}_1\\ \dot{\boldsymbol{e}}_2&=\dot{\boldsymbol{y}}_2+\dot{\boldsymbol{x}}_2=-\Delta\boldsymbol{e}_2\\ &\vdots\\ \dot{\boldsymbol{e}}_n&=\dot{\boldsymbol{y}}_n+\dot{\boldsymbol{x}}_n=-\Delta\boldsymbol{e}_n\end{aligned}$$

构造 Lyapunov 函数 $V=\frac{1}{2}(\boldsymbol{e}_1^2+\boldsymbol{e}_2^2+\cdots+\boldsymbol{e}_n^2)>0$，则有

$$\begin{aligned}\frac{\mathrm{d}V}{\mathrm{d}t}&=\boldsymbol{e}_1\cdot\frac{\mathrm{d}\boldsymbol{e}_1}{\mathrm{d}t}+\boldsymbol{e}_2\cdot\frac{\mathrm{d}\boldsymbol{e}_2}{\mathrm{d}t}+\cdots+\boldsymbol{e}_n\cdot\frac{\mathrm{d}\boldsymbol{e}_2}{\mathrm{d}t}\\ &=-(\Delta\boldsymbol{e}_1^2+\Delta\boldsymbol{e}_2^2+\cdots+\Delta\boldsymbol{e}_n^2)\end{aligned}$$

由于 Δ 为实数，且 $\Delta\geqslant 0$，所以

$$\dot{V}=-(\Delta\boldsymbol{e}_1^2+\Delta\boldsymbol{e}_2^2+\cdots+\Delta\boldsymbol{e}_n^2)<0$$

由 Lyapunov 稳定性定理可得，反同步误差系统渐进稳定，即存在控制器

$$u(\boldsymbol{x},\boldsymbol{y})=-(\boldsymbol{A}_2+\Delta)\boldsymbol{e}-(\boldsymbol{A}_1-\boldsymbol{A}_2)\boldsymbol{x}-f_2(\boldsymbol{y})-f_1(\boldsymbol{x})$$

其中，Δ 为实数，且 $\Delta>0$，使混沌系统(1)与响应系统(3)实现反同步，得证。

2.2　反同步混沌系统群

定义 4　设相空间存在点集 $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，那么当 $\sigma_1\neq\sigma_2\neq\cdots\neq\sigma_n$ 时，混沌原系统(1)在其相空间内，可以对应多个不同的对称子系统 $\dot{\boldsymbol{y}}_{\sigma 1}$，$\dot{\boldsymbol{y}}_{\sigma 2}$，$\cdots$，$\dot{\boldsymbol{y}}_{\sigma n}$，称为系统(1)的对称混沌子群系统，进一步可以描述为

$$\begin{cases}\dot{\boldsymbol{y}}_{\sigma 1}=\boldsymbol{A}_2\boldsymbol{y}_{\sigma 1}+f_2(\boldsymbol{y}_{\sigma 1})=\boldsymbol{A}_1(2\sigma_1-\boldsymbol{x})-f_1(2\sigma_1-\boldsymbol{x})\\ \vdots\\ \dot{\boldsymbol{y}}_{\sigma n}=\boldsymbol{A}_n\boldsymbol{y}_{\sigma n}+f_2(\boldsymbol{y}_{\sigma n})=\boldsymbol{A}_1(2\sigma_n-\boldsymbol{x})-f_1(2\sigma_n-\boldsymbol{x})\end{cases} \tag{6}$$

以原系统(1)为驱动系统，其对称混沌子群系统的响应系统可以同一描述为

$$\begin{cases}\dot{\boldsymbol{y}}_{\sigma 1}=A_{\sigma 1}\boldsymbol{y}_{\sigma 1}+f_2(\boldsymbol{y}_{\sigma 1})+u(\boldsymbol{x},\boldsymbol{y}_{\sigma 1})\\ \vdots\\ \dot{\boldsymbol{y}}_{\sigma n}=A_{\sigma n}\boldsymbol{y}_{\sigma n}+f_2(\boldsymbol{y}_{\sigma n})+u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})\end{cases} \tag{7}$$

其中，$u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})$ 为反同步混沌系统群同步控制器，系统群反同步的动态系统误差群可以表示为

$$\dot{\boldsymbol{e}}_{\sigma n}=\dot{\boldsymbol{x}}+\dot{\boldsymbol{y}}_{\sigma n}=A_1\boldsymbol{x}+f_1(\boldsymbol{x})+A_{\sigma n}\boldsymbol{y}_{\sigma n}+f_2(\boldsymbol{y}_{\sigma n})+u(\boldsymbol{x},\boldsymbol{y}_{\sigma n}),\ n=1,2,3\cdots \tag{8}$$

定义 5　对于系统(1)，在式(7)中，如果存在一个群同步控制器 $u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})$，使在任意初始状态下，均有

$$\lim_{t\to\infty}\|\dot{\boldsymbol{x}}+\dot{\boldsymbol{y}}_{\sigma n}\|=0,\ n=1,2,3\cdots \tag{9}$$

成立，$\|\cdot\|$ 代表欧几里得范数，则称原系统(1)与对称混沌子群系统 $\dot{\boldsymbol{y}}_{\sigma 1}$，$\dot{\boldsymbol{y}}_{\sigma 2}$，$\cdots$，$\dot{\boldsymbol{y}}_{\sigma n}$ 达到反同步。

定理 2　对于驱动系统(1)和对称子群响应系统(7)，存在控制器 $u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})=-(\boldsymbol{A}_{\sigma n}+\Delta_{\sigma n})\boldsymbol{e}_{\sigma n}-(\boldsymbol{A}_1+\boldsymbol{A}_{\sigma n})\boldsymbol{x}-f_{\sigma n}(\boldsymbol{y}_{\sigma n})-f_1(\boldsymbol{x})$，$\Delta_{\sigma n}$ 为实数，且 $\Delta_{\sigma n}>0$，$n=1,2,3\cdots$，使驱动系统和响应系统在任意初始条件下，实现原系统(1)和其关于点 σ 对称的子系统群反同步。

证明　对于反同步误差系统群(9)，构造如下 Lyapunov 函数：$\boldsymbol{V}_{\sigma n}=\frac{1}{2}(\boldsymbol{e}_{\sigma n1}^2+\boldsymbol{e}_{\sigma n2}^2+\cdots+\boldsymbol{e}_{\sigma nn}^2)>0$，$\Delta_{\sigma n}>0$，$n=1,2,3\cdots$，则有

$$\begin{aligned}\dot{\boldsymbol{V}}_{\sigma n}&=\boldsymbol{e}_{\sigma n1}\dot{\boldsymbol{e}}_{\sigma n1}+\boldsymbol{e}_{\sigma n2}\dot{\boldsymbol{e}}_{\sigma n2}+\cdots+\boldsymbol{e}_{\sigma nn}\dot{\boldsymbol{e}}_{\sigma nn}\\ &=-(\Delta_{\sigma n1}\boldsymbol{e}_{\sigma n1}^2+\Delta_{\sigma n2}\boldsymbol{e}_{\sigma n2}^2+\cdots+\Delta_{\sigma nn}\boldsymbol{e}_{\sigma nn}^2)\end{aligned}$$

由于 $\Delta_{\sigma n}$ 为实数，且 $\Delta_{\sigma n}>0$，所以

$$\dot{\boldsymbol{V}}_{\sigma n}=-(\Delta_{\sigma n1}\boldsymbol{e}_{\sigma n1}^2+\Delta_{\sigma n2}\boldsymbol{e}_{\sigma n2}^2+\cdots+\Delta_{\sigma nn}\boldsymbol{e}_{\sigma nn}^2)\leqslant 0$$

由 Lyapunov 稳定性定理可得，反同步误差系统群(9)渐进稳定，即混沌系统(1)与响应系统(7)实现反同步。

定理 3　当原混沌系统与相空间内对称的混沌子群系统达到反同步时，有如下描述。

命题(1)：对称子系统均与原系统进入反同步状态。

命题(2)：任意 2 个对称子系统之间，均达到正同步状态。

证明　设有原混沌系统(1)，其相空间内存在点集：$\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，且 $\sigma_1\neq\sigma_2\neq\cdots\neq\sigma_n$，其对应的对称混沌子群系统为 $\dot{\boldsymbol{y}}_{\sigma 1}$，$\dot{\boldsymbol{y}}_{\sigma 2}\cdots;\dot{\boldsymbol{y}}_{\sigma n}$，子群系统与

原系统(1)进入反同步状态。

关于命题(1)：由定理 2 知，原系统与子系统群进入反同步状态时，每个对称子系统均与原系统进入反同步状态。

关于命题(2)：设原系统为 $\dot{\boldsymbol{x}}$，任选 2 个子系统 $\boldsymbol{y}_{\sigma m}$、$\boldsymbol{y}_{\sigma n}$，其中，$m \neq n$。

由于对称子系统和原系统之间均达到反同步状态，存在控制器 $u(\boldsymbol{x}, \boldsymbol{y}_{\sigma m})$、$u(\boldsymbol{x}, \boldsymbol{y}_{\sigma n})$，使 $t \to \infty$ 时，有

$$\lim_{t\to\infty}\left\|\dot{\boldsymbol{y}}_{\sigma m}+\dot{\boldsymbol{x}}\right\|=0$$

$$\lim_{t\to\infty}\left\|\dot{\boldsymbol{y}}_{\sigma n}+\dot{\boldsymbol{x}}\right\|=0$$

$$\lim_{t\to\infty}\left\|\dot{\boldsymbol{y}}_{\sigma n}-\dot{\boldsymbol{y}}_{\sigma m}\right\|$$

$$=\lim_{t\to\infty}\left\|\dot{\boldsymbol{y}}_{\sigma n}+\dot{\boldsymbol{x}}\right\|+\lim_{t\to\infty}\left\|-\dot{\boldsymbol{x}}-\dot{\boldsymbol{y}}_{\sigma m}\right\|=0$$

所以，任意 2 个对称子系统之间，均达到正同步状态。命题(2)得证。

2.3 反同步混沌系统群仿真

永磁同步电机在转子磁场定向坐标系中，可描述为如下状态方程[20,21]。

$$\begin{cases}\dfrac{\mathrm{d}i_d}{\mathrm{d}t}=\dfrac{-R_i i_d+\omega L_q i_q+u_d}{L_d}\\ \dfrac{\mathrm{d}i_q}{\mathrm{d}t}=\dfrac{-R_i i_q+\omega L_d i_d+u_d-\omega\psi_r}{L_q}\\ \dfrac{\mathrm{d}\omega}{\mathrm{d}t}=\dfrac{n_p\psi_r i_d+n_p(L_d-L_q)i_d i_q-T_L-\beta\omega}{J}\end{cases}\tag{10}$$

其中，i_d、i_q 和 u_d、u_q 分别为定子电流、定子电压向量的直轴和交轴分量；ω 是转子角速度；ψ_r 为转了磁通量；R_s 是定子电阻；n_p 是极对数；J 是转子惯量；β 是粘性阻尼系数；T_L 是负载转矩；L_d 和 L_q 分别是直轴和交轴电感。

可以进一步简化为

$$\begin{cases}\dot{\boldsymbol{x}}_1=5.46(\boldsymbol{x}_2-\boldsymbol{x}_1)\\ \dot{\boldsymbol{x}}_2=-\boldsymbol{x}_1\boldsymbol{x}_3-\boldsymbol{x}_2+\gamma\boldsymbol{x}_1\\ \dot{\boldsymbol{x}}_3=-\boldsymbol{x}_3-\boldsymbol{x}_1\boldsymbol{x}_2\end{cases}\tag{11}$$

其中，γ 为常数，$\boldsymbol{x}_1$、$\boldsymbol{x}_2$、$\boldsymbol{x}_3$ 为系统控制变量。$\gamma=16.9$ 时，系统处于混沌状态。有定义 1 知，在其相空间内选取点 $A=(0,0,0)$、$B=(5,-3,-5)$、$C=(-2,4,10)$，$\Delta_{\sigma n}=1$ 时，则由定义 1 和式(7)知，其对称系统群反同步响应系统可以表示为

$$\begin{cases}\dot{\boldsymbol{y}}_{A1}=5.46(\boldsymbol{y}_{A2}-\boldsymbol{y}_{A1})+u_{A1}(\boldsymbol{x},\boldsymbol{y}_A)\\ \dot{\boldsymbol{y}}_{A2}=\boldsymbol{y}_{A1}\boldsymbol{y}_{A3}-\boldsymbol{y}_{A2}+16.9\boldsymbol{y}_{A1}+u_{A2}(\boldsymbol{x},\boldsymbol{y}_A)\\ \dot{\boldsymbol{y}}_{A3}=-\boldsymbol{y}_{A3}-\boldsymbol{y}_{A1}\boldsymbol{y}_{A2}+u_{A3}(\boldsymbol{x},\boldsymbol{y}_A)\\ \dot{\boldsymbol{y}}_{B1}=5.46(\boldsymbol{y}_{A2}-\boldsymbol{y}_{A1})+87.36+u_{B1}(\boldsymbol{x},\boldsymbol{y}_B)\\ \dot{\boldsymbol{y}}_{B2}=(10-\boldsymbol{y}_{B1})(-10-\boldsymbol{y}_{B3})-\boldsymbol{y}_{B2}+16.9\boldsymbol{y}_{B1}+\\ \qquad 163+u_{B2}(\boldsymbol{x},\boldsymbol{y}_B)\\ \dot{\boldsymbol{y}}_{B3}=(-10-\boldsymbol{y}_{B3})-(10-\boldsymbol{y}_{B1})(-6-\boldsymbol{y}_{B2})+u_{B3}(\boldsymbol{x},\boldsymbol{y}_B)\\ \dot{\boldsymbol{y}}_{C1}=5.46(\boldsymbol{y}_{C2}-\boldsymbol{y}_{C1})-131.04+u_{C1}(\boldsymbol{x},\boldsymbol{y}_C)\\ \dot{\boldsymbol{y}}_{C2}=(-4-\boldsymbol{y}_{C1})(20-\boldsymbol{y}_{C3})-\boldsymbol{y}_{C2}+16.9\boldsymbol{y}_{C2}-\\ \qquad 32+u_{C2}(\boldsymbol{x},\boldsymbol{y}_C)\\ \dot{\boldsymbol{y}}_{C3}=(20-\boldsymbol{y}_{C3})+(4+\boldsymbol{y}_{C1})(8-\boldsymbol{y}_{C2})+u_{B3}(\boldsymbol{x},\boldsymbol{y}_B)\end{cases}\tag{12}$$

由定义 5 和定理 2 知，选取如下群控制器 $u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})$ 时，系统群反同步响应系统与原系统同步。

$$\begin{cases}\boldsymbol{u}_{A1}(\boldsymbol{x},\boldsymbol{y}_A)=-5.46(\boldsymbol{x}_2+\boldsymbol{y}_{A2})\\ \boldsymbol{u}_{A2}(\boldsymbol{x},\boldsymbol{y}_A)=\boldsymbol{x}_1\boldsymbol{x}_3-16.9\boldsymbol{x}_1-\boldsymbol{y}_{A1}\boldsymbol{y}_{A3}-16.9\boldsymbol{y}_{A1}\\ \boldsymbol{u}_{A3}(\boldsymbol{x},\boldsymbol{y}_A)=-\boldsymbol{x}_1\boldsymbol{x}_2+\boldsymbol{y}_{A1}\boldsymbol{y}_{A2}\\ \boldsymbol{u}_{B1}(\boldsymbol{x},\boldsymbol{y}_B)=-5.46(\boldsymbol{x}_2+\boldsymbol{y}_{B2})-91.2\\ \boldsymbol{u}_{B2}(\boldsymbol{x},\boldsymbol{y}_B)=\boldsymbol{x}_1\boldsymbol{x}_3-16.9\boldsymbol{x}_1+\\ \qquad (10-\boldsymbol{y}_{B1})(10+\boldsymbol{y}_{B3})-16.9(10-\boldsymbol{y}_{B1})\\ \boldsymbol{u}_{B3}(\boldsymbol{x},\boldsymbol{y}_B)=-\boldsymbol{x}_1\boldsymbol{x}_2+(10+\boldsymbol{y}_{B1})(6+\boldsymbol{y}_{B3})+10\\ \boldsymbol{u}_{C1}(\boldsymbol{x},\boldsymbol{y}_C)=-5.46(\boldsymbol{x}_2+\boldsymbol{y}_{C2})+76.44\\ \boldsymbol{u}_{C2}(\boldsymbol{x},\boldsymbol{y}_C)=\boldsymbol{x}_1\boldsymbol{x}_3-16.9\boldsymbol{x}_1+\\ \qquad (-4-\boldsymbol{y}_{C1})(20+\boldsymbol{y}_{C3})+16.9(4+\boldsymbol{y}_{C1})\\ \boldsymbol{u}_{C3}(\boldsymbol{x},\boldsymbol{y}_C)=-\boldsymbol{x}_1\boldsymbol{x}_2-(4+\boldsymbol{y}_{C1})(20-\boldsymbol{y}_{C2})-20\end{cases}\tag{13}$$

分别选取 4 组初始值对结果进行仿真。选取系统初始值

$$[x_1(0),x_2(0),x_3(0)]^{\mathrm{T}}=[5,3,2]^{\mathrm{T}}$$

$$[x_{A1}(0),x_{A2}(0),x_{A3}(0)]^{\mathrm{T}}=[12,-12,-3]^{\mathrm{T}}$$

$$[x_{B1}(0),x_{B2}(0),x_{B2}(0)]^{\mathrm{T}}=[-6,6,7]^{\mathrm{T}}$$

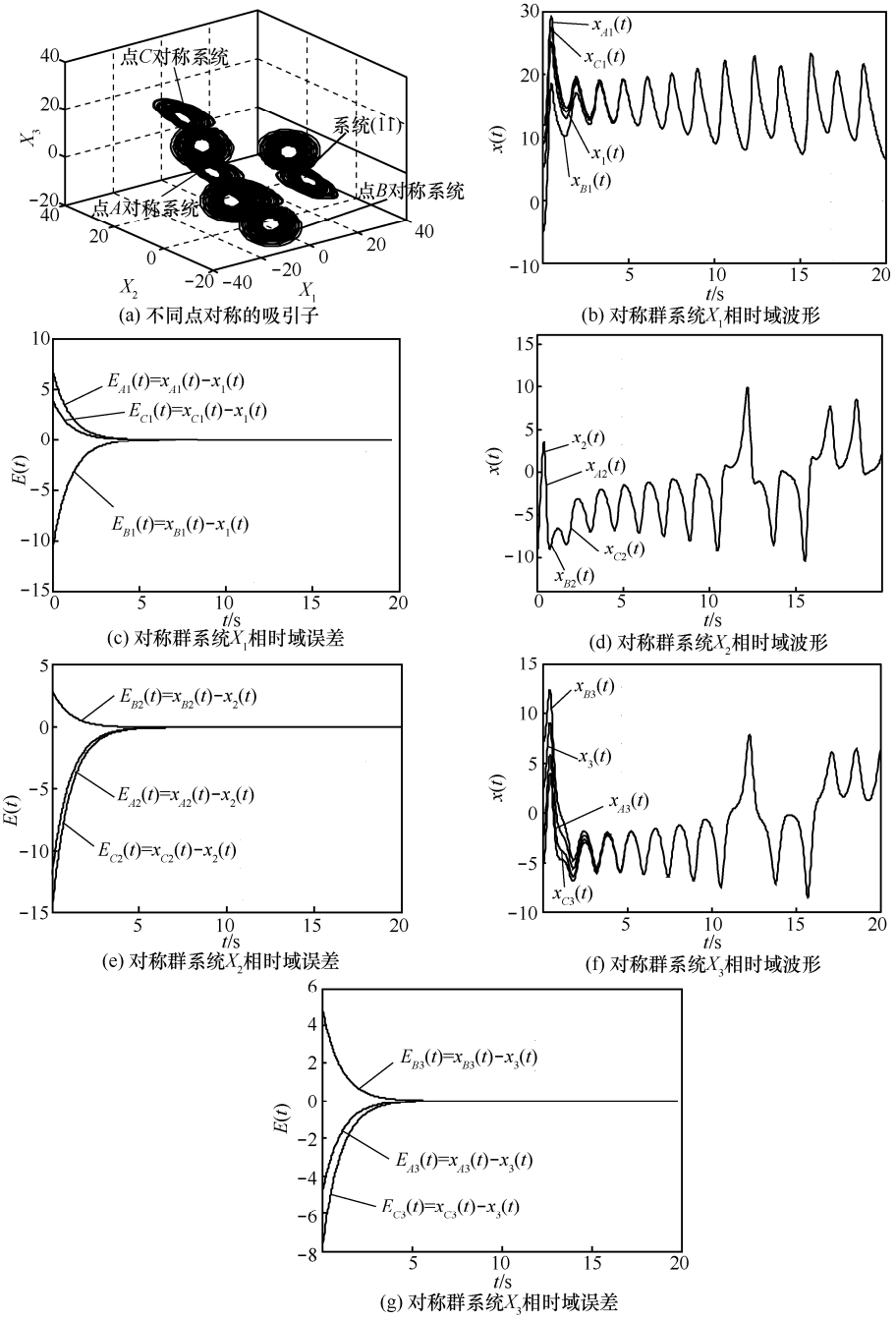
$$[x_{C1}(0),x_{C2}(0),x_{C3}(0)]^{\mathrm{T}}=[9,-9,-6]^{\mathrm{T}}$$

从图 2 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 $u(\boldsymbol{x},\boldsymbol{y}_{\sigma n})$ 的作用下，在 5 s 内，各个子系统均与原系统达到反同步，并且子系统之间进入反同步状态，进一步验证了定理 3。

3 反同步混沌群系统载波通信

3.1 建立系统模型

对于具有分布式、规模大、多信号量等特点的现代通信系统，本文利用反同步混沌系统群和永磁



(a) 不同点对称的吸引子　(b) 对称群系统X_1相时域波形　(c) 对称群系统X_1相时域误差　(d) 对称群系统X_2相时域波形　(e) 对称群系统X_2相时域误差　(f) 对称群系统X_3相时域波形　(g) 对称群系统X_3相时域误差

图 2　对称群系统反同步实验

同步电机混沌系统(11)，提出了一种基于混沌系统群载波的安全通信方法，其基本原理如图 3 所示。

图 3 为本文提出的反同步混沌系统群载波安全通信的系统，其中，$m_1(t)$、$m_2(t)$、…、$m_n(t)$ 为多信号量输入，设混沌系统(11)的相空间内存在点集 $\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，$\sigma_1\neq\sigma_2\neq\cdots\neq\sigma_n$，则系统(11)关于点集对称的系统群可以描述为 $\dot{\boldsymbol{y}}_{\sigma1},\dot{\boldsymbol{y}}_{\sigma2},\cdots,\dot{\boldsymbol{y}}_{\sigma n}$。设反同步群控制器 $u_{\sigma1}(\boldsymbol{x},\boldsymbol{y}_{\sigma1})$，$u_{\sigma2}(\boldsymbol{x},\boldsymbol{y}_{\sigma2})$，…，$u_{\sigma n}(\boldsymbol{x},\boldsymbol{y}_{\sigma n})$，使混沌系统群 $\dot{\boldsymbol{y}}_{\sigma1},\dot{\boldsymbol{y}}_{\sigma2},\cdots,\dot{\boldsymbol{y}}_{\sigma n}$ 反同步于原系统(11)。

有用信号 $m_n(t)$ 经过函数 $f(t)$ 载波函数调制，合成密文信号 $m_n'(t)$。

在发送端，有

$$m_n'(t)=f(t)+km_n(t) \tag{14}$$

$$f(t)=\begin{cases}y_{\sigma n1}+y_{\sigma n2}, & y_{\sigma n1}>y_{\sigma n3}\\ y_{\sigma n3}, & y_{\sigma n1}=y_{\sigma n3}\\ y_{\sigma n1}-y_{\sigma n2}, & y_{\sigma n1}<y_{\sigma n3}\end{cases} \tag{15}$$

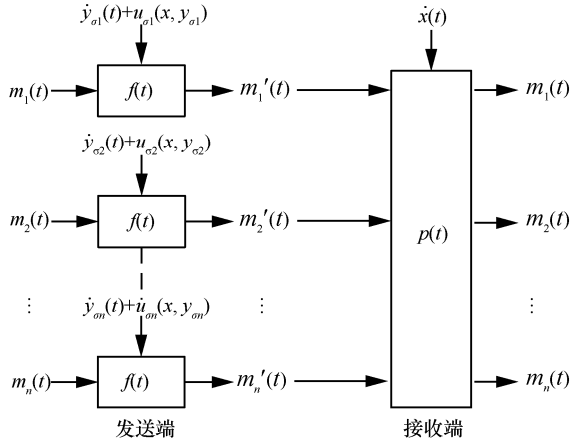


图 3　反同步混沌系统群载波安全通信

在接收端，由于发送混沌与接收混沌为反同步，所以

$$m_n(t)=-p(t)-km_n'(t) \tag{16}$$

$$p(t)=\begin{cases}x_1+x_2, & x_1>x_2\\ x_3, & x_1=x_3\\ x_1-x_2, & x_1<x_3\end{cases} \tag{17}$$

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 $\frac{1}{4}$。

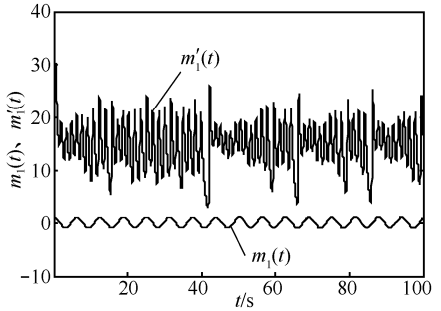
3.2　仿真研究

本文选择 2 路常见信号类型进行实验。

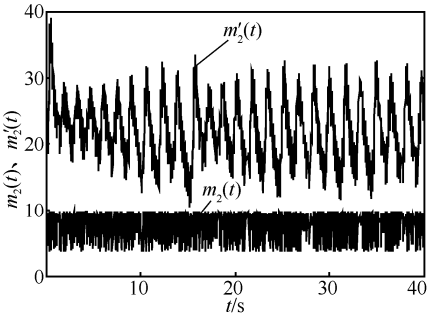
第一路为连续模拟量信号 $m_1(t)=\cos t$，第二路为指数分布的信号 $m_2(t)$。

对于系统(11)，在其相空间内选取点 $A=(0,0,0)$、$B=(5,-3,-5)$。选取系统参数 $\gamma=16.9$，系统初始值为

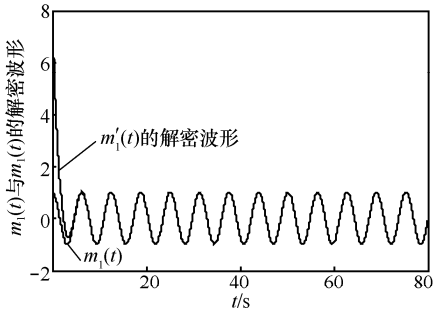
$$[x_1(0),x_2(0),x_3(0)]^{\mathrm{T}}=[5,3,2]^{\mathrm{T}}$$
$$[x_{A1}(0),x_{A2}(0),x_{A3}(0)]^{\mathrm{T}}=[12,-12,-3]^{\mathrm{T}}$$



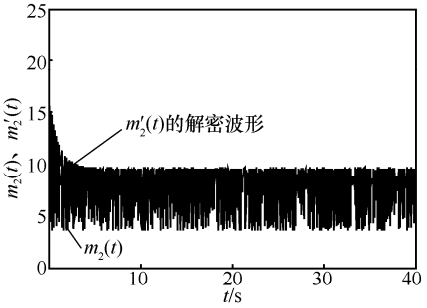
(a) $m_1(t)$与 $m_1'(t)$时域波形



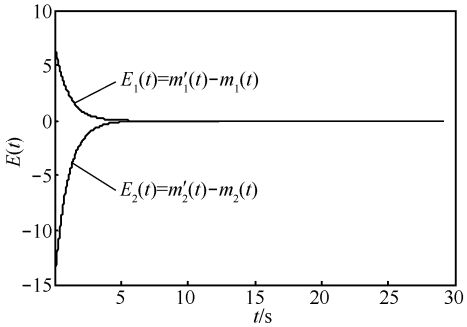
(b) $m_2(t)$与 $m_2'(t)$时域波形



(c) $m_1(t)$与 $m_1'(t)$解密波形



(d) $m_2(t)$与 $m_2'(t)$解密波形

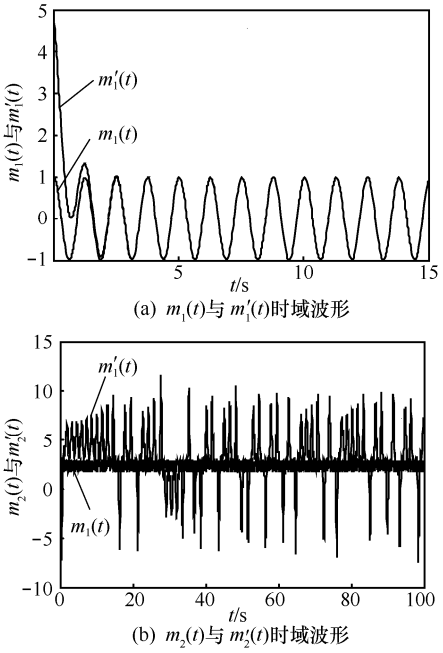


(e) 时域误差波形

图 4　对称混沌系统群载波传输实验

$$[x_{B1}(0),x_{B2}(0),x_{B2}(0)]^{\mathrm{T}}=[-6,6,7]^{\mathrm{T}}$$

仿真结果如图 5 所示。



(a) $m_1(t)$与 $m_1'(t)$时域波形

(b) $m_2(t)$与 $m_2'(t)$时域波形

图 5　信道窃取实验

从图 5(a)和图 5(b)可以看出，选取有用信号 $m_1(t)$、$m_1'(t)$经过反同步混沌系统群载波后，完全掩盖了有用信号的特征，经过信道传输，在接收端经过混沌系统同步并解密，恢复有用信号。从图 4(e)看出，接收端与发送端混沌系统在 10 s 内快速反同步。有用信号被保密通信系统加密和传输，并且不失真的恢复，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 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，可以指定相空间内多个不相同的点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。

3.3　信道窃取实验

以上述实验为研究对象，假定攻击者通过信道破译第一路信号发送端数学模型与参数，并将其应用于第二路信号，试图破译第二路有用信息，实验结果如图 5 所示。

从图 5(a)可知，当攻击者获取了第一路信号的发送模型及参数，并完全恢复了第一路发送信号。从图 5(b)可知，攻击者将第一路的参数和数学模型应用于第二路信号，并不能获取有用信息。由于混沌系统关于不同的点对称映射所获得的混沌系统，只是空间拓扑相似，但空间位置各不相同，2 路发送信号本质上为采用不同的结构，所以即使获取了一个信道的参数，也很难应用于其他信道。

4　结束语

本文首先研究了混沌系统在相空间内点对称映射的模型，同时提出了一种实现混沌系统群的方法，该方法利用混沌系统以不同的点在相空间对称映射，构成多个混沌对称子系统。本文研究了对称混沌子系统群与原系统同步问题，以永磁同步电机系统为实验对象，进行了理论和仿真验证，实验结果支持了本文的研究结论。基于本文的研究成果，提出了一种适合于大规模、多信号等现代通信系统特征的保密通信方案，并对方案进行研究和验证，仿真结果表明，该方法适用于大规模、多信号的通信系统。

参考文献：

[1] HUA C, YANG B, OUYANG G, et al. A new chaotic secure communication scheme[J]. Physics Letters A: General, Atomic and Solid State Physics, 2005, 342(4): 305-308.

[2] AN X L, YU J N, LI Y Z., et al. Design of a new multistage chaos synchronized system for secure communications and study on noise perturbation[J]. Mathematical and Computer Modelling, 2011, 54(1-2): 7-18.

[3] HUANG Y C, LIAO T L, YAN J J. Adaptive variable structure control for chaos suppression of unified chaotic systems[J]. Applied Mathematics and Computation, 2009, 209(2): 391-398.

[4] YANG X, YANG Z, NIE X, Exponential synchronization of discontinuous chaotic systems via delayed impulsive control and its application to secure communication[J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(5): 1529-1543.

[5] JI Y, WEN C, LI Z G, Chaotic communication systems in the presence of parametric uncertainty and mismatch[J]. International Journal of Communication Systems, 2008, 21(11): 1137-1154.

[6] JOVIC B, UNSWORTH C P, SANDHU G S, et al. A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems[J].Signal Processing, 2007, 87(7): 1692-1708.

[7] CHENG C C, LIN Y S, WU S W, Design of adaptive sliding mode tracking controllers for chaotic synchronization and application to secure communications[J]. Journal of the Franklin Institute, 2012, 349(8): 2626-2649.

[8] HASSAN M F. Observer design for constrained nonlinear systems with application to secure communication[J].Journal of the Franklin Institute, 2014, 351(2): 1001-1026.

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

[10] BOCCALETTI S, KURTHSC J, OSIPOV D L, et al. The synchronization of chaotic systems[R]. Physics, Reports. 2002, 366: 1-101.

[11] SARAH H, ABDESSELEM B. A generalized function projective synchronization scheme for uncertain chaotic systems subject to input nonlinearities[J]. International Journal of General Systems, 2016, 45(6):

689-710.

[12] 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.

[13] ADEL O, 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.

[14] RICHTER H. Controlling chaotic system with multiple strange attractors[J]. Phys Lett A, 2002, 300: 182-188.

[15] NGO H Q, LARSSON E G, MARZETTA T L. Energy and spectral efficiency of very large multiuser MIMO systems[J]. IEEE Trans Commun, 2012, 61(4): 1436-1449.

[16] 曹旺斌, 尹成群, 谢志远, 等, 多输入多输出宽带电力线载波通信信道模型研究[J]. 中国电机工程学报，2017,37(4):1137-1141.
CAO W B, YIN C Q, XIE Z Y, et al, Research on broadband MIMO power line communications model[J]. Proceedings of the CSEE, 2017,37(4):1137-1141.

[17] 高昊, 王剑, 高艳涛, 等. 分布式多输入多输出雷达的侦察分析[J]. 清华大学学报, 2014, 54(10):1367-1372.
GAO H, WANG J, GAO Y T, et al. Reconnaissance analysis of MIMO radars with widely separated antennas[J]. J Tsinghua Univ(Sci& Technol), 2014, 54(10): 1367-1372.

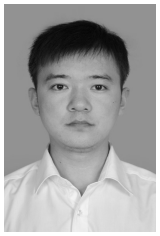
[18] JON R, LINDSAY. Stuxnet and the limits of cyber warfare[J]. Security Studies, 2013, 22 (3): 365-404.

[19] 王海荣, 王玉辉, 黄永明, 等. 大规模MIMO 蜂窝网络系统中的导频污染减轻方法[J]. 通信学报, 2014,35(1):24-33.
WANG H R , WANG Y H, HUANG Y M, et al. Pilot contamination reduction in very large MIMO cellular network[J]. Journal on Communications, 2014,35(1):24-33.

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

[21] 王磊, 李颖晖, 朱喜华, 等. 存在扰动的永磁同步电机混沌运动模糊自适应同步[J]. 电力系统保护与控制, 2011,39(11):33-43.
WANG L, LI Y H, ZHU X H, et al. Chaos synchronization of permanent magnet synchronous motor with disturbance using fuzzy adaptive logic [J]. Power System Protection and Control, 2011, 39(11): 33-43.

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，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，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，哈尔滨理工大学讲师，主要研究方向为管理科学与工程。