自动化学报
ACTA AUTOMATICA SINICA

基于混沌数据加密的切换系统最优控制与隐私保护

齐义文 乔鑫鑫 邓飞其 王云龙

Optimal Control and Privacy Preserving of Switched Systems Based on Chaotic Data Encryption

QI Yi-Wen, QIAO Xin-Xin, DENG Fei-Qi, WANG Yun-Long

在线阅读 View online: https://doi.org/10.16383/j.aas.c250636

基于混沌数据加密的切换系统最优控制与隐私保护

齐义文[1] 乔鑫鑫[1] 邓飞其[2] 王云龙[3]

摘 要 针对控制系统中数据经网络传输存在的隐私泄露以及隐私保护导致的性能损失问题, 本文研究一种具有隐私保护的切换系统最优控制方法. 首先, 根据混沌系统的非周期性及不可预测性, 开发一种基于混沌系统的数据加密方法. 将主混沌系统生成的伪随机序列添加到切换系统输出数据中, 能避免其经非理想网络传输时隐私的泄露. 其次, 设计一种基于粒子群优化算法的混沌形态同步控制器, 降低不确定项的影响, 保障主−从混沌系统的同步性, 确保解密后数据的可用性. 然后, 利用自适应动态规划算法对采用解密后数据构造的代价函数进行优化, 将预更新最优子系统的更新规则作为候选切换律. 通过对比候选切换律与当前切换律作用下系统的性能, 将性能好的切换律作为控制策略的一部分, 确保切换系统性能最优. 最后, 通过仿真对所提方法的可行性进行验证.

关键词 切换系统; 隐私保护; 自适应动态规划; 主−从混沌系统; 粒子群优化算法

引用格式 齐义文, 乔鑫鑫, 邓飞其, 王云龙. 基于混沌数据加密的切换系统最优控制与隐私保护. 自动化学报, 2026, **52**(7): 1360−1371

DOI 10.16383/j.aas.c250636 **CSTR** 32138.14.j.aas.c250636

Optimal Control and Privacy Preserving of Switched Systems Based on Chaotic Data Encryption

QI Yi-Wen[1] QIAO Xin-Xin[1] DENG Fei-Qi[2] WANG Yun-Long[3]

Abstract In control systems, for the problems of privacy leakage caused by network transmission and performance loss caused by privacy preserving, this paper studies an optimal control method with the ability of privacy preserving for switched systems. Due to the non-periodicity and unpredictability of chaotic systems, a data encryption method based on chaotic systems is developed. The pseudo-random sequence generated by the master chaotic system is added to the output data of the switched system, which can avoid privacy leakage during transmission in non-ideal network. Secondly, a chaotic morphology synchronization controller based on the particle swarm optimization algorithm is designed to reduce the influence of uncertain terms, ensure the synchronization of master-slave chaotic systems, and guarantee the availability of decrypted data. Then, an adaptive dynamic programming algorithm is used to optimize the cost function based on decrypted data, and the update rule of the pre-updated optimal subsystem is used as a candidate switching law. By comparing the performance of the system under the action of the candidate switching law and the current switching law, the better one is used as part of the control policy to ensure the optimality of the switched system performance. Finally, the feasibility of the proposed method is verified through simulation.

Keywords switched systems; privacy preserving; adaptive dynamic programming; master-slave chaotic system; particle swarm optimization algorithm

Citation Qi Yi-Wen, Qiao Xin-Xin, Deng Fei-Qi, Wang Yun-Long. Optimal control and privacy preserving of switched systems based on chaotic data encryption. *Acta Automatica Sinica*, 2026, **52**(7): 1360−1371

收稿日期 2025-11-14 录用日期 2026-01-30
Manuscript received November 14, 2025; accepted January 30, 2026
国家自然科学基金 (62373110) 资助
Supported by National Natural Science Foundation of China (62373110)
本文责任编委 罗彪
Recommended by Associate Editor LUO Biao
1. 福州大学电气工程与自动化学院 福州 350108 2. 华南理工大学自动化科学与工程学院 广州 510640 3. 沈阳航空航天大学自动化学院 沈阳 110135
1. College of Electrical Engineering and Automation, Fuzhou University, Fuzhou 350108 2. School of Automation Science and Engineering, South China University of Technology, Guangzhou 510640 3. School of Automation, Shenyang Aerospace University, Shenyang 110135

切换系统作为一类特殊的混合系统, 其由多个子系统组成, 并且运行模式可以根据切换律进行切换[1]. 在实际运用中, 许多系统具有复杂的结构和可变的特性, 这使得单一系统难以描述其特征[2]. 切换系统由于其切换机制, 在设计时更加灵活, 这一特点使其在许多领域得到广泛的应用, 如航空发动机[3]、无人机[4]、无人船[5] 等. 文献 [6] 研究一类单输入连续时间切换线性系统的稳定性问题. 文献 [7] 研究一类切换非线性时滞系统的状态稳定性问题. 文献 [8] 考虑状态依赖的控制器, 保证非线性脉冲

切换系统的稳定性. 文献 [9] 研究触发学习下不确定切换系统的自抗扰控制, 设计一个基于自抗扰控制的切换律, 加快系统跟踪误差的收敛. 然而, 现有的文献对切换系统的研究主要为稳定性分析、控制策略设计、切换律设计等, 对于切换系统的隐私性研究尚存在不足.

近年来, 网络安全愈发受到重视, 特别是隐私保护在国家重要议题中被多次提及. 控制系统的隐私保护是国家网络安全重大战略的需要, 对于保障个人隐私、数据安全与国家安全具有重要意义[10]. 随着物联网与人工智能技术的发展, 控制系统可以利用大规模实时数据来支撑决策, 从而更精确地应对外部环境的变化, 显著提升系统在组织、部署与实施方面的效率. 然而, 网络环境的开放性、数据传输的透明性导致系统存在隐私泄露风险, 将影响系统的可靠性与控制性能, 甚至引发安全事故[11]. 例如, 2010 年, 伊朗核设施遭受震网病毒入侵, 历史隐私数据被泄露, 监控系统被攻击, 导致核项目被严重推迟[10]; 2021 年, 美国最大的燃油运输管道商 Colonial Pipeline 大量的 VPN 账户密码被窃取、敏感数据被泄露, 导致东海岸地区出现燃料短缺的问题[10]. 针对隐私泄露问题, 文献 [12] 提出一种适用于多智能体系统的基于编解码加解密的隐私保护方法. 文献 [13] 提出一种性能依赖的差分隐私方法, 实现切换系统中隐私和性能的平衡. 根据现有的研究, 隐私保护方法主要包括匿名[14]、差分隐私[15]、联邦学习[16] 等. 匿名方法通过删除或替换敏感数据实现隐私保护, 但存在数据可用性差的问题. 差分隐私方法通过对数据集添加噪声, 从而避免隐私信息被获取, 但噪声会在一定程度上影响系统的性能. 联邦学习通过本地训练模型, 将非原始数据传输到中央服务器, 保证了数据的隐私性, 但存在通信成本高、收敛性无法保证的问题. 因此, 如何在保证数据可用性的同时提高隐私保护水平是一个亟须解决的关键问题.

混沌系统作为一类特殊的非线性系统, 具有非周期、不可预测、初值敏感等特点, 曾一度被视为控制界的难题. 文献 [17] 首次提出混沌系统的同步方法. 自此之后, 混沌同步引起学者们的广泛关注, 并衍生出完全同步、时滞同步等方法. 此外, 由于混沌系统的初值敏感特性, 可得到不可预测的伪随机序列, 这与加密要求高度契合, 因此被广泛地应用于加密场景. 其核心思想是通过主混沌系统生成伪随机序列进行加密, 同时从混沌系统在同步控制器的作用下生成与主混沌系统几乎一致的伪随机序列实现解密. 文献 [18] 提出一种基于时空混沌系统的图像加密方法. 文献 [19] 提出一种基于切换分数阶混沌系统的图像加密方法. 现有的混沌加密主要聚焦于图像、音频、视频等场景, 这种加密方法具有较好的隐私性和通信实时性. 此外, 同态加密作为控制系统加密的一种主要方法, 其能够直接利用加密数据求解控制策略, 但是只能支持有限次数的加法和乘法, 并且加解密误差不可控. 基于主–从混沌系统的加密虽然在求解控制策略时需要解密, 但是不存在应用场景的限制, 并且可以通过设计形态同步控制器来降低加解密对系统性能的影响. 因此, 将基于主–从混沌系统的加密应用于控制系统的隐私保护是一个值得研究的问题.

随着神经网络技术的发展, 自适应动态规划 (adaptive dynamic programming, ADP) 算法被提出, 其能够克服动态规划中的维数灾难, 已成为最优控制的主要方法之一. 文献 [20] 系统地描述 ADP 的应用进展, 指出其在非线性系统与多智能体协同中的潜力. 文献 [21] 设计一种具有高效经验重放的 ADP 算法, 能够利用更少的数据来求解最优控制策略. 文献 [22] 开发一种自触发 ADP 算法, 在实现最优控制的同时减少不必要的计算资源浪费. 文献 [23] 针对航天器的姿态控制问题, 设计一种基于 ADP 算法的容错控制, 得到一种能够抑制带宽受限的最优控制策略. 这些研究表明 ADP 算法可以有效地解决各种类型的最优控制问题, 然而, 其对于考虑隐私保护的最优控制问题尚存在不足.

综上, 本文针对切换系统的性能与数据安全, 设计综合考虑最优性和隐私性的方法. 首先, 基于 ADP 算法设计一个考虑控制输入和性能依赖的切换律, 保证系统的性能最优; 其次, 设计一种基于混沌系统的隐私保护方法, 保证系统的隐私性; 最后, 采用粒子群优化算法 (particle swarm optimization, PSO) 对同步控制器中的参数进行优化, 减少隐私性对最优性的影响. 本文的贡献可以概括为三个方面:

1) 本文设计一种基于主–从混沌系统的隐私保护方法. 主混沌系统生成伪随机序列对系统进行加密, 从混沌系统生成与主混沌系统几乎一致的伪随机序列实现解密, 这种方法可以有效保障切换系统的数据安全. 与差分隐私[24]、匿名[25] 等方法相比, 该方法能够在实现隐私保护的同时, 保证数据的可用性, 即几乎不会影响系统的控制性能. 与同态加密[26] 相比, 该方法计算效率更高, 实时性更好, 更加符合控制系统的实时通信要求.

2) 本文提出一种适用于切换系统的 ADP 控制策略更新方法. 在 ADP 算法迭代过程中, 控制策略综合考虑控制输入和性能依赖的候选切换律. 将预更新的下一次迭代中最优子系统的更新规则作为候选切换律, 通过对比其与当前迭代的切换律作用下系统的性能, 选取最优切换律作为下一次迭代的切换律, 确保迭代过程中控制性能的最优.

3) 本文设计一种智能群体算法优化的形态同步控制器. 通过粒子群算法对主−从混沌系统中形态同步控制器的不确定项相关参数进行优化, 得到一组最优的参数组合, 确保形态同步控制器的最优性. 在该控制器作用下, 从混沌系统几乎完全跟踪主混沌系统, 能够有效降低隐私保护对系统性能的影响.

本文的内容安排如下: 第 1 节介绍问题描述以及控制框架; 第 2 节给出基于 ADP 算法的最优控制策略设计; 第 3 节设计基于混沌系统的隐私保护方法以及基于粒子群算法的参数优化; 第 4 节使用仿真算例证明本文方法的可行性; 第 5 节对本文进行总结.

1 问题描述

1.1 切换系统的最优控制问题描述

考虑如下由多个子系统构成的线性切换系统

$$\dot{x}(t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) \tag{1}$$

其中, $x(t) \in \mathbf{R}^{n_x}$ 是系统状态; $u(t) \in \mathbf{R}^{n_u}$ 是系统控制输入; $\sigma(t)\colon (0,\ 1,\ 2,\ \cdots) \to \underline{N} = \{1,\ 2,\ \cdots,\ S\}$ 是切换信号, S 是子系统数量; $\sigma(t) = i$ 表示第 i 个子系统被激活; $A_{\sigma(t)}$ 和 $B_{\sigma(t)}$ 分别是与系统状态和控制输入相关的已知矩阵.

本文的第一个目标是设计一个最优控制策略使得下面表征系统控制性能的代价函数最小化

$$J = \int_0^{\infty} U_{\sigma(s)}(x(s),\ u(s))\mathrm{d}s \tag{2}$$

其中, $U_{\sigma(t)}(x(t), u(t)) = x^{\mathrm{T}}(t)Qx(t) + u^{\mathrm{T}}(t)Ru(t)$ 是效用函数, $x^{\mathrm{T}}(t)Qx(t)$ 表示与系统状态相关的代价, $u^{\mathrm{T}}(t)Ru(t)$ 表示与控制输入相关的代价, 且 Q、R 都是正定且对称的矩阵; 代价函数 J 用于衡量系统从初始时刻 $t = 0$ 到无穷时间范围的总体代价, 它由效用函数 $U_{\sigma(t)}(x(t), u(t))$ 在时间区间 $[0,\ +\infty)$ 上的积分构成, 在实际应用中可用来评估系统运行过程中的某种累计成本、能量消耗或其他需要最小化的指标.

定义 1. 系统 (1) 和紧集 Ω 上有连续的控制输入 $u(t)$, 若对于任意 $x(0) \in \Omega$, $u(t)$ 都能使系统 (1) 在 Ω 上稳定, 且代价函数 (2) 的值是有限的, 则称 $u(t)$ 在 Ω 上是关于系统 (1) 的容许控制策略[21].

在 t 时刻, 根据式 (2), 定义如下代价函数

$$V_{\sigma(t)}(x(t),\ u(t)) = \int_t^{\infty} U_{\sigma(s)}(x(s),\ u(s))\mathrm{d}s \tag{3}$$

根据贝尔曼原理, 代价函数 (3) 可被改写为

$$V_{\sigma(t)}(t) = U_{\sigma(t)}(t) + V_{\sigma(t)}(t+1) \tag{4}$$

然后, 通过对式 (4) 两边关于 t 求导, 可以构造如下哈密顿−雅可比−贝尔曼方程

$$\frac{\partial V^*_{\sigma(t)}(t)}{\partial t} = -\min_{u(t)\in\Omega}\left\{U_{\sigma(t)}(t) + \left(\frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)}\right)^{\mathrm{T}}\dot{x}(t)\right\} \tag{5}$$

令

$$H\left(x(t), u(t), \frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)}\right) = U_{\sigma(t)}(t) + \left(\frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)}\right)^{\mathrm{T}}\dot{x}(t)$$

则可以将式 (5) 重写为

$$\frac{\partial V^*_{\sigma(t)}(t)}{\partial t} + H\left(x(t),\ u^*(t),\ \frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)}\right) = 0 \tag{6}$$

其中, $u^*(t) = \mathrm{argmin}_{u(t)\in\Omega} H(x(t),\ u(t),\ \frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)})$ 是最优控制策略, 它表示在 Ω 内使哈密顿函数 $H(x(t),\ u(t),\ \frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)})$ 最小的控制策略. 哈密顿函数 $H(x(t),\ u(t),\ \frac{\partial V^*_{\sigma(t)}(t)}{\partial x(t)})$ 综合了系统效用函数 $U_{\sigma(t)}(t)$ 和状态变化率等因素, 描述系统当前状态、控制输入及值函数梯度下的特性, 是求解最优控制的关键.

注 1. 通过引入哈密顿函数对哈密顿−雅可比−贝尔曼方程进行重写, 可以将最优控制问题转化为一个基于哈密顿系统的求解问题. 传统的解析方法往往只适用于一些特定形式的线性或简单非线性方程. 对于式 (6) 所示的偏微分方程, 其非线性特性使得用传统解析方法难以找到一个精确的、用初等函数表示的解析解. 因此, 后续内容中将引入自适应动态规划算法来迭代得到最优控制策略表达式, 然后利用行为−评价 (actor-critic) 神经网络方法来对该方程进行近似求解.

1.2 基于混沌系统的状态加密描述

考虑以下具有内部非线性特性、不确定特性以及外部干扰的主−从混沌系统:

$$\begin{cases}\dot{x}_{m_1}(t)=M_1x_{m_1}(t)+f_{m1}(x_{m_1}(t))+\\ \quad \Delta f_{m_1}(x_{m_1}(t))+D_{m_1}(t)\\ \dot{x}_{m_2}(t)=M_2x_{m_2}(t)+f_{m_2}(x_{m_2}(t))+\\ \quad \Delta f_{m_2}(x_{m_2}(t))+D_{m_2}(t)\\ \qquad\vdots\\ \dot{x}_{m_{n_x}}(t)=M_{n_x}x_{m_{n_x}}(t)+f_{m_{n_x}}(x_{m_{n_x}}(t))+\\ \quad \Delta f_{m_{n_x}}(x_{m_{n_x}}(t))+D_{m_{n_x}}(t)\end{cases}\tag{7}$$

$$\begin{cases}\dot{x}_{s_1}(t)=S_1x_{s_1}(t)+f_{s_1}(x_{s_1}(t))+D_{s_1}(t)+\\ \quad \Delta f_{s_1}(x_{s_1}(t))+u_{s_1}(t)\\ \dot{x}_{s_2}(t)=S_2x_{s_2}(t)+f_{s_2}(x_{s_2}(t))+D_{s_2}(t)+\\ \quad \Delta f_{s_2}(x_{s_2}(t))+u_{s_2}(t)\\ \qquad\vdots\\ \dot{x}_{s_{n_x}}(t)=S_{n_x}x_{s_{n_x}}(t)+f_{s_{n_x}}(x_{s_{n_x}}(t))+D_{s_{n_x}}(t)+\\ \quad \Delta f_{s_{n_x}}(x_{s_{n_x}}(t))+u_{s_{n_x}}(t)\end{cases}\tag{8}$$

其中, 式 (7) 表示主混沌系统, $x_m(t)=[x_{m_1}^{\mathrm{T}}(t),\ x_{m_2}^{\mathrm{T}}(t),\ \cdots,\ x_{m_{n_x}}^{\mathrm{T}}(t)]^{\mathrm{T}}$ 是主混沌系统的状态, $M=[M_1^{\mathrm{T}},\ M_2^{\mathrm{T}},\ \cdots,\ M_{n_x}^{\mathrm{T}}]^{\mathrm{T}}$ 是主混沌系统中状态相关的矩阵, $f_m(\cdot)=[f_{m_1}^{\mathrm{T}}(\cdot),\ f_{m_2}^{\mathrm{T}}(\cdot),\ \cdots,\ f_{m_{n_x}}^{\mathrm{T}}(\cdot)]^{\mathrm{T}}$ 是主混沌系统中满足利普希茨条件的连续非线性光滑函数, $\Delta f_m(\cdot)=[\Delta f_{m_1}^{\mathrm{T}}(\cdot),\ \Delta f_{m_2}^{\mathrm{T}}(\cdot),\ \cdots,\ \Delta f_{m_{n_x}}^{\mathrm{T}}(\cdot)]^{\mathrm{T}}$ 是主混沌系统内部的不确定项, $D_m(t)=[D_{m_1}^{\mathrm{T}}(t),\ D_{m_2}^{\mathrm{T}}(t),\ \cdots,\ D_{m_{n_x}}^{\mathrm{T}}(t)]^{\mathrm{T}}$ 是主混沌系统的外部扰动. 式 (8) 是从混沌系统, $x_s(t)=[x_{s_1}^{\mathrm{T}}(t),\ x_{s_2}^{\mathrm{T}}(t),\ \cdots,\ x_{s_{n_x}}^{\mathrm{T}}(t)]^{\mathrm{T}}$ 是从混沌系统的状态, $S=[S_1^{\mathrm{T}},\ S_2^{\mathrm{T}},\ \cdots,\ S_{n_x}^{\mathrm{T}}]^{\mathrm{T}}$ 是从混沌系统状态相关的矩阵, $f_s(\cdot)=[f_{s_1}^{\mathrm{T}}(\cdot),\ f_{s_2}^{\mathrm{T}}(\cdot),\ \cdots,\ f_{s_{n_x}}^{\mathrm{T}}(\cdot)]^{\mathrm{T}}$ 是从混沌系统中满足利普希茨条件的连续非线性光滑函数, $\Delta f_s(\cdot)=[\Delta f_{s_1}^{\mathrm{T}}(\cdot),\ \Delta f_{s_2}^{\mathrm{T}}(\cdot),\ \cdots,\ \Delta f_{s_{n_x}}^{\mathrm{T}}(\cdot)]^{\mathrm{T}}$ 是从混沌系统内部的不确定项, $D_s(t)=[D_{s_1}^{\mathrm{T}}(t),\ D_{s_2}^{\mathrm{T}}(t),\ \cdots,\ D_{s_{n_x}}^{\mathrm{T}}(t)]^{\mathrm{T}}$ 是从混沌系统的外部扰动, $u_s(t)=[u_{s_1}^{\mathrm{T}}(t),\ u_{s_2}^{\mathrm{T}}(t),\ \cdots,\ u_{s_{n_x}}^{\mathrm{T}}(t)]^{\mathrm{T}}$ 是后续所需要设计的形态同步控制器.

基于主–从混沌系统的加密原理: 首先, 切换系统 (1) 的状态 $x(t)$ 在经非理想网络传输之前, 利用主混沌系统产生的伪随机序列 $x_m(t)$ 对其进行加密, 即切换系统的状态 $x(t)$ 加上 $x_m(t)$, 能有效避免隐私数据的泄露; 其次, 从混沌系统的输出 $x_s(t)$ 在形态同步控制器 $u_s(t)$ 的作用下几乎能够完全跟踪主混沌系统的输出 $x_m(t)$; 最后, 加密数据经非理想网络传输, 并在传递给控制器之前, 利用 $x_s(t)$ 对其解密, 即加密数据减去从混沌系统的输出 $x_s(t)$.

因此, 定义解密误差为 $e(t)=x_s(t)-x_m(t)=[e_1(t),\ e_2(t),\ \cdots,\ e_{n_x}(t)]^{\mathrm{T}}$, 得到如下混沌误差系统

$$\begin{cases}\dot{e}_1(t)=S_1x_{s_1}(t)+f_{s_1}(x_{s_1}(t))+D_{s_1}(t)+\\ \quad \Delta f_{s_1}(x_{s_1}(t))+u_{s_1}(t)-M_1x_{m_1}(t)-\\ \quad f_{m_1}(x_{m_1}(t))-\Delta f_{m_1}(x_{m_1}(t))-D_{m_1}(t)\\ \dot{e}_2(t)=S_2x_{s_2}(t)+f_{s_2}(x_{s_2}(t))+D_{s_2}(t)+\\ \quad \Delta f_{s_2}(x_{s_2}(t))+u_{s_2}(t)-M_2x_{m_2}(t)-\\ \quad f_{m_2}(x_{m_2}(t))-\Delta f_{m_2}(x_{m_2}(t))-D_{m_2}(t)\\ \qquad\vdots\\ \dot{e}_{n_x}(t)=S_{n_x}x_{s_{n_x}}(t)+f_{s_{n_x}}(x_{s_{n_x}}(t))+\\ \quad D_{s_{n_x}}(t)+\Delta f_{s_{n_x}}(x_{s_{n_x}}(t))+u_{s_{n_x}}(t)-\\ \quad M_{n_x}x_{m_{n_x}}(t)-f_{m_{n_x}}(x_{m_{n_x}}(t))-\\ \quad \Delta f_{m_{n_x}}(x_{m_{n_x}}(t))-D_{m_{n_x}}(t)\end{cases}\tag{9}$$

后续所设计的形态同步控制器 $u_s(t)$ 中可调参数众多, 不合理的设置会使解密误差增大. 因此, 本文采用粒子群优化算法, 在满足参数约束范围内对其进行自动寻优.

注 2. 从式 (7) 和 (8) 中可以看出, 主混沌系统按照自身的动力学规律运行产生混沌信号, 从混沌系统通过混沌形态同步控制器 $u_s(t)$ 试图跟踪主系统状态以实现与其同步, 这种同步特性在保密通信、信号处理等领域有着广泛的应用. 在给定的初始时刻 $t(0)$ 和初始位置 $x_m(0)$ 下, 主混沌系统在相平面中表现为一条平滑曲线 $c_m(t)=[x_{m_1}(t),\ x_{m_2}(t),\ \cdots,\ x_{m_{n_x}}(t)]^{\mathrm{T}}$, 被称为主系统曲线. 类似地, 从系统也表现为一条平滑曲线 $c_s(t)=[x_{s_1}(t),\ x_{s_2}(t),\ \cdots,\ x_{s_{n_x}}(t)]^{\mathrm{T}}$, 被称为从系统曲线. 由于混沌系统中包含的非线性项和不确定项是其产生复杂、不可预测行为的根源, 使得上述曲线演化具有高度的敏感性和不确定性, 即使微小的初值差异都可能导致解密误差产生较大变化; 而考虑的外部干扰 (如噪声、外部激励等) 会对其性能和稳定性产生影响, 进一步增加了分析和控制难度.

图 1 给出了 PSO 优化下最优切换系统的混沌数据加密框架, 该框架主要包含四部分: 切换系统、混沌系统、ADP 算法和 PSO 算法. 图中非理想网络是指当数据经过该网络传输时, 存在外部入侵者窥探和隐私泄露的风险, 可能破坏系统的安全运行. 切换系统的状态在经过非理想网络传输之前, 利用主混沌系统不可预测的状态 $x_m(t)$ 对其加密, 可得到加密后的数据 $\tilde{x}(t)$, 而 $\tilde{x}(t)$ 经非理想网络传输时, 可以有效避免隐私数据的泄露. PSO 被用于优化混

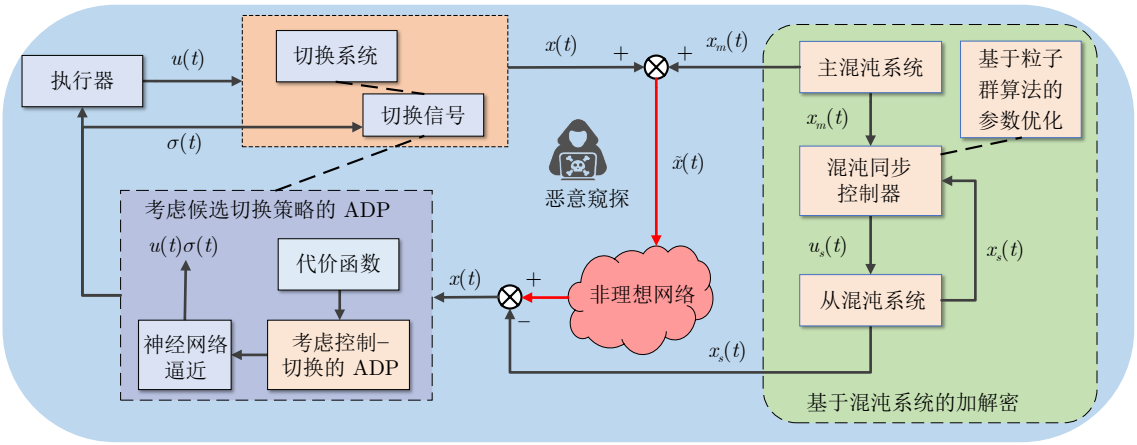

图 1 PSO 优化下最优切换系统的混沌数据加密

Fig. 1 Chaotic data encryption of the optimal switched systems under PSO optimization

沌形态同步控制器 $u_s(t)$ 中不确定项参数, 从而确保从混沌系统状态 $x_s(t)$ 与主混沌系统状态 $x_m(t)$ 的同步. 基于此, $x_s(t)$ 可用于对加密数据 $\tilde{x}(t)$ 的解密, 得到原始状态 $x(t)$. 然后, $x(t)$ 被用于构造待优化的代价函数, 通过 ADP 算法进行迭代和优化, 得到一组最优控制策略, 其包含控制输入 $u(t)$ 和候选切换策略迭代的切换律 $\sigma(t)$. 考虑候选切换策略的 ADP 算法能够保障切换系统的最优性, 混沌系统的加密能够保障切换系统的隐私性, 粒子群算法能够降低隐私保护对系统性能的影响.

2 基于 ADP 算法的切换系统最优控制

本节首先给出了切换系统在 ADP 算法下控制策略的迭代以及 ADP 算法的收敛性和最优性分析, 然后给出了神经网络的搭建.

2.1 基于 ADP 算法的控制策略迭代

由于切换系统由多个子系统组成, 因此在利用 ADP 算法求解最优控制策略时, 不仅需要考虑控制输入 $u(t)$, 还需要考虑子系统 $\sigma(t)$ 的影响, 即找到一个使代价函数最优的子系统. 下面给出了在 ADP 算法下控制策略的迭代过程.

对于初始容许的控制策略 $\{u^0(t),\ \sigma^0(t)\}$, 控制输入 $u^0(t)$ 是随机生成的, 切换律 $\sigma^0(t)$ 是任意给定的. 定义 l 为迭代次数, 当 $l=0$ 时, 代价函数 (4) 可以重写为

$$V^0(t)=U(t,\ u^0(t),\ \sigma^0(t))+V^0(t+1) \tag{10}$$

其中, $V^0(t)$ 是 $V^0(x(t),\ u^0(t),\ \sigma^0(t))$ 的缩写. 那么通过最小化式 (10) 的右侧, 可求解下一次迭代的控制输入. 首先, 将控制输入的迭代次数加 1, 然后对式 (10) 右侧的 $u^1(t)$ 求偏导, 可得

$$\begin{cases}\dfrac{\partial}{\partial u^1(t)}[U(t,\ u^1(t),\ \sigma^0(t))+V^0(t+1)]=0\\ 2Ru^1(t)+B^{\mathrm{T}}_{\sigma^0(t)}\dfrac{\partial V^0(t+1)}{\partial x(t+1)}=0\end{cases}$$

则下一次迭代预更新的控制输入为

$$u^1(t,\ \sigma^0(t))=-\frac{1}{2}R^{-1}B^{\mathrm{T}}_{\sigma^0(t)}\frac{\partial V^0(t+1)}{\partial x(t+1)} \tag{11}$$

定义一个新的函数 $M_i^1(x)$, 其满足

$$\begin{cases}M_i^1(x)=x^{\mathrm{T}}(t+1)x(t+1)\\ x(t+1)=A_ix(t)+B_iu^1(t,\ \sigma^0(t))\end{cases} \tag{12}$$

其中, $i\in\underline{N}$.

则可以得到一个候选的切换律

$$\sigma^1_{\mathrm{cand}}(t)=\arg\min_{i\in\underline{N}}\{M_i^1(x)\} \tag{13}$$

如果下面不等式成立, 则表明在候选的切换律 $\sigma^1_{\mathrm{cand}}(t)$ 作用下比之前的切换律 $\sigma^0(t)$ 作用下的系统性能更好.

$$V(\breve{x}(t),\ u^1(t,\ \sigma^1_{\mathrm{cand}}(t)),\ \sigma^1_{\mathrm{cand}}(t))\le V(\bar{x}(t),\ u^1(t,\ \sigma^0(t)),\ \sigma^0(t)) \tag{14}$$

其中,

$$\begin{cases}\breve{x}(t+1)=A_{\sigma^1_{\mathrm{cand}}(t)}\breve{x}(t)+B_{\sigma^1_{\mathrm{cand}}(t)}u^1(t,\ \sigma^1_{\mathrm{cand}}(t))\\ \bar{x}(t+1)=A_{\sigma^0(t)}\bar{x}(t)+B_{\sigma^0(t)}u^1(t,\ \sigma^0(t))\end{cases}$$

然后, 可以得到控制策略的更新规则如下

$$\begin{cases}\sigma^1(t)=\begin{cases}\sigma^1_{\mathrm{cand}}(t), & \text{式 (14) 成立}\\ \sigma^0(t), & \text{其他}\end{cases}\\ u^1(t)=\\ \quad -\dfrac{1}{2}R^{-1}B^{\mathrm{T}}_{\sigma^1(t)}\dfrac{\partial V^0(t+1,\ u^0(t+1),\ \sigma^1(t+1))}{\partial x(t+1)}\end{cases} \tag{15}$$

对于第 l 次迭代, 代价函数为

$$V^l(t) = U(t,\ u^l(t),\ \sigma^l(t)) + V^l(t+1) \tag{16}$$

其中, $V^l(t)$ 是 $V^l(x(t),\ u^l(t),\ \sigma^l(t))$ 的缩写. 当切换律为 $\sigma^l(t)$ 时, 预更新的控制输入为

$$u^{l+1}(t,\ \sigma^l(t)) = -\frac{1}{2}R^{-1}B^{\mathrm{T}}_{\sigma^l(t)}\frac{\partial V^l(t+1)}{\partial x(t+1)} \tag{17}$$

定义一个新的函数 $M_i^{l+1}(x)$, 其满足

$$\begin{cases} M_i^{l+1}(x) = x^{\mathrm{T}}(t+1)x(t+1) \\ x(t+1) = A_i x(t) + B_i u^{l+1}(t,\ \sigma^l(t)) \end{cases} \tag{18}$$

其中, $i \in \underline{N}$.

则可以得到一个候选切换律

$$\sigma^{l+1}_{\mathrm{cand}}(t) = \arg\min_{i\in\underline{N}}\left\{M_i^{l+1}(x)\right\} \tag{19}$$

如果下式成立, 则表明在候选切换律 $\sigma^{l+1}_{\mathrm{cand}}(t)$ 作用下的系统性能比之前切换律 $\sigma^l(t)$ 作用下的系统性能更好

$$\begin{aligned} &V(\check{x}(t),\ u^{l+1}(t,\ \sigma^{l+1}_{\mathrm{cand}}(t)),\ \sigma^{l+1}_{\mathrm{cand}}(t)) \le \\ &\quad V(\bar{x}(t),\ u^{l+1}(t,\ \sigma^l(t)),\ \sigma^l(t)) \end{aligned} \tag{20}$$

其中,

$$\begin{cases} \check{x}(t+1) = A_{\sigma^{l+1}_{\mathrm{cand}}(t)}\check{x}(t) + B_{\sigma^{l+1}_{\mathrm{cand}}(t)}u^{l+1}(t,\ \sigma^{l+1}_{\mathrm{cand}}(t)) \\ \bar{x}(t+1) = A_{\sigma^l(t)}\bar{x}(t) + B_{\sigma^l(t)}u^{l+1}(t,\ \sigma^l(t)) \end{cases}$$

然后, 可以得到控制策略的更新规则如下

$$\begin{cases} \sigma^{l+1}(t) = \begin{cases} \sigma^{l+1}_{\mathrm{cand}}(t), & \text{式 (20) 成立} \\ \sigma^l(t), & \text{其他} \end{cases} \\ u^{l+1}(t) = \\ \quad -\dfrac{1}{2}R^{-1}B^{\mathrm{T}}_{\sigma^{l+1}(t)}\dfrac{\partial V^l(x(t+1),u^l(t+1),\sigma^{l+1}(t+1))}{\partial x(t+1)} \end{cases} \tag{21}$$

上述 ADP 算法的控制策略迭代过程设计了一种考虑候选的切换律, 与以往切换律设计存在如下区别: 以往切换律在第 $l+1$ 次迭代时, 通过比较该次所有子系统对应性能, 选择最优的作为第 $l+1$ 次的切换律; 对于考虑候选的切换律, 它先根据以往切换律的设计方法确定第 $l+1$ 次的候选切换律, 再对比该候选切换律和第 l 次切换律作用下的切换系统性能, 选择最优的一个作为第 $l+1$ 次的切换律, 该策略能够确保切换系统随着迭代次数的变化始终处于最优的子系统.

当迭代次数 l 达到最大迭代次数 $l_{\max}$ 时, 迭代停止, 或相邻两次迭代之间的误差小于一个给定的正常数 ϵ 时, 迭代停止, 即

$$\left\|V^{l+1}(u^{l+1}(t),\ \sigma^{l+1}(t)) - V^l(u^l(t),\ \sigma^l(t))\right\| \le \epsilon$$

其中 $V^l(u^l(t),\ \sigma^l(t))$ 是 $V^l(x(t),\ u^l(t),\ \sigma^l(t))$ 的缩写; $V^{l+1}(u^{l+1}(t),\ \sigma^{l+1}(t))$ 是 $V^{l+1}(x(t),\ u^{l+1}(t),\ \sigma^{l+1}(t))$ 的缩写.

此时的控制策略可以被认作近似最优控制策略.

注 3. ϵ 是一个给定的非常小的正常数, 值越小, 需要迭代的次数越多, 代价函数 $V(t)$ 越逼近最优代价函数, 反之亦然. ϵ 的大小的选取需要根据需求而定, 需要较快的收敛, 则给一个相对较大的值; 需要较好的性能, 则给一个相对较小的值.

2.2　ADP 算法的收敛性和最优性分析

本节给出了上述迭代过程中 ADP 算法的收敛性以及得到控制策略的最优性分析.

定理 1. (ADP 算法的收敛性和最优性) 对于任意的 l, 以及给定的可以使系统 (1) 稳定的初始容许控制策略 $\{u^0(t),\ \sigma^0(t)\}$, 如果控制策略按照式 (21) 更新, 那么代价函数是单调非增的, 即

$$V^{l+1}(x(t),\ u^{l+1}(t),\ \sigma^{l+1}(t)) \le V^l(x(t),\ u^l(t),\ \sigma^l(t))$$

并且代价函数收敛到最优代价函数

$$\lim_{l\to\infty} V^l(x(k),\ u^l(k),\ \sigma^l(k)) = V^*(x(k),\ u^*(k),\ \sigma^*(k))$$

证明. 根据式 (20) 和式 (21), 下面不等式一定成立

$$\begin{aligned} &V^{l+1}(x(t),\ u^{l+1}(t),\ \sigma^{l+1}(t)) \le \\ &\quad V^{l+1}(x(t),\ u^{l+1}(t),\ \sigma^l(t)) \end{aligned} \tag{22}$$

因此, 控制策略更新规则 (21) 中所设计的切换律并不会影响迭代的收敛性. 为了方便书写, 后续用 $V^l(t)$ 代替 $V^l(x(t),\ u^l(t),\ \sigma^l(t))$.

根据第 2.1 节 ADP 算法的迭代及控制策略的迭代可知, 在 $u^{l+1}(t)$ 作用下的效用函数 $U(t,\ u^{l+1}(t),\ \sigma^{l+1}(t))$ 一定不大于 $u^l(t)$ 作用下的效用函数 $U(t,\ u^l(t),\ \sigma^l(t))$, 即

$$U(t,\ u^{l+1}(t),\ \sigma^{l+1}(t)) \le U(t,\ u^l(t),\ \sigma^l(t)) \tag{23}$$

根据式 (16) 和式 (23), 可得代价函数在迭代次数上的差分为

$$\begin{aligned} V^{l+1}(t) - V^l(t) = {}& U(t,\ u^{l+1}(t),\ \sigma^{l+1}(t)) - \\ & U(t,\ u^l(t),\ \sigma^l(t)) + \\ & V^{l+1}(t+1) - V^l(t+1) \le \\ & V^{l+1}(t+1) - V^l(t+1) \le \\ & \cdots \le V^{l+1}(T) - V^l(T) \end{aligned} \tag{24}$$

由于 $u^0(t)$ 可以使系统 (1) 保持稳定的初始容许控制, 并且在运行终端时刻 T, $V^{l+1}(T)=V^l(T)$ 一定成立. 因此, 可以得到

$$V^{l+1}(t)-V^l(t)\le V^{l+1}(T)-V^l(T)=0 \tag{25}$$

故代价函数 $V^l(t)$ 是单调非增的.

定义一个新的代价函数 $G^{l+1}(t)=U(t,\,u^{l+1}(t),\,\sigma^{l+1}(t))+V^l(t+1)$, 当 $l\to\infty$, 根据式 (16) 和式 (25), 可以得到

$$V^\infty(t)=\lim_{l\to\infty}V^l(t)=\lim_{l\to\infty}V^{l+1}(t)\le\lim_{l\to\infty}G^{l+1}(k)$$

那么, 可以得到如下不等式约束

$$V^\infty(t)\le\lim_{l\to\infty}G^{l+1}(k)\le$$
$$\lim_{l\to\infty}\min_{u(t),\,\sigma(t)}\{U(t,\,u^l(t),\,\sigma^l(t))+V^l(t+1)\} \tag{26}$$

假设存在任意给定的实数 δ 以及足够大的正自然数 L, 使得 $V^\infty(t)$ 满足以下约束条件

$$V^L(t)-\delta\le V^\infty(t)\le V^L(t) \tag{27}$$

根据不等式 (27) 可以推导出

$$V^\infty(t)\ge U(t,\,u^L(t),\,\sigma^L(t))+V^L(t+1)-\delta\ge$$
$$\lim_{l\to\infty}\min_{u(t),\,\sigma(t)}\{U(t,\,u^l(t),\,\sigma^l(t))+$$
$$V^l(t+1)-\delta\} \tag{28}$$

由于 δ 是任意给定的, 设 $\delta=0$ 时, 式 (28) 可改写为

$$V^\infty(t)\ge\lim_{l\to\infty}\min_{u(t),\,\sigma(t)}\{U(t,\,u^l(t),\,\sigma^l(t))+$$
$$V^l(t+1)\} \tag{29}$$

最后, 根据不等式 (26) 和 (29) 可以得到

$$V^\infty(t)=\lim_{l\to\infty}\min_{u(t),\,\sigma(t)}\{U(t,\,u^l(t),\,\sigma^l(t))+$$
$$V^l(t+1)\}=V^*(t) \tag{30}$$

故代价函数 $\lim_{l\to\infty}V^l(t)$ 可以收敛到最优代价函数 $V^*(x(k),\,u^*(k),\,\sigma^*(k))$. □

2.3 actor-critic 神经网络的搭建及权重收敛性分析

本节介绍了 actor-critic 神经网络的结构、更新规则和相应的权重收敛分析.

actor 神经网络设计. 神经网络被用于近似系统的控制输入, 该网络的输入为切换系统的状态, 输出为逼近的控制系统的输入, 其结构可设计为

$$\hat{u}^{l,\,j}_{\sigma(t)}(t)=(W^{l,\,j}_{a2\sigma(t)})^{\mathrm{T}}\Theta_a((W^{l,\,j}_{a1\sigma(t)})^{\mathrm{T}}x(t)) \tag{31}$$

其中, Θ_a 是激活函数; $W_{a1\sigma(t)}\in\mathbf{R}^{n_x\times n_a}$ 和 $W_{a2\sigma(t)}\in\mathbf{R}^{n_o\times n_a}$ 分别是 actor 神经网络的第一层和第二层权重, n_a 和 n_o 分别是激活层和输出层的神经元数量; j 是近似过程的迭代次数.

定义如下二次型的逼近误差

$$E^{l,\,j}_{a\sigma(t)}=\frac{1}{2}(\tilde{u}^l_{\sigma(t)}(t))^{\mathrm{T}}\tilde{u}^l_{\sigma(t)}(t) \tag{32}$$

其中, $\tilde{u}^l_{\sigma(t)}(t)=\hat{u}^{l,\,j}_{\sigma(t)}(t)-u^l_{\sigma(t)}(t)$ 为逼近误差. 可以得到 actor 网络权重的更新规则如下

$$\begin{cases}W^{l,\,j+1}_{a1\sigma(t)}=W^{l,\,j}_{a1\sigma(t)}-\gamma_a\dfrac{\partial E^{l,\,j}_{a\sigma(t)}}{\partial W^{l,\,j}_{a1\sigma(t)}}\\[2ex] W^{l,\,j+1}_{a2\sigma(t)}=W^{l,\,j}_{a2\sigma(t)}-\gamma_a\dfrac{\partial E^{l,\,j}_{a\sigma(t)}}{\partial W^{l,\,j}_{a2\sigma(t)}}\end{cases} \tag{33}$$

其中, γ_a 为 actor 神经网络的学习率.

critic 神经网络设计. critic 神经网络被用于近似系统的代价函数, 该网络的输入为切换系统的控制输入, 输出为逼近的代价函数, 其结构可设计为如下形式

$$\hat{V}^{l,\,j}_{\sigma(t)}(t)=(W^{l,\,j}_{c2\sigma(t)})^{\mathrm{T}}\Theta_c((W^{l,\,j}_{c1\sigma(t)})^{\mathrm{T}}x(t)) \tag{34}$$

其中, Θ_c 是激活函数; $W_{c1\sigma(t)}\in\mathbf{R}^{n_x\times n_c}$ 和 $W_{c2\sigma(t)}\in\mathbf{R}^{n_o\times n_c}$ 分别是 critic 神经网络的第一层和第二层权重, n_c 是激活层的神经元数量. critic 神经网络的目标是最小化如下的代价误差函数

$$E^{l,\,j}_{c\sigma(t)}=\frac{1}{2}(\tilde{V}^l_{\sigma(t)}(t))^{\mathrm{T}}\tilde{V}^l_{\sigma(t)}(t) \tag{35}$$

其中, $\tilde{V}^l_{\sigma(t)}(t)=\hat{V}^{l,\,j}_{\sigma(t)}(t)-\hat{V}^{l,\,j}_{\sigma(t)}(t+1)-U_{\sigma(t)}(t)$ 是贝尔曼方程的误差. 可以得到 critic 网络权重的更新规则如下

$$\begin{cases}W^{l,\,j+1}_{c1\sigma(t)}=W^{l,\,j}_{c1\sigma(t)}-\gamma_c\dfrac{\partial E^{l,\,j}_{c\sigma(t)}}{\partial W^{l,\,j}_{c1\sigma(t)}}\\[2ex] W^{l,\,j+1}_{c2\sigma(t)}=W^{l,\,j}_{c2\sigma(t)}-\gamma_c\dfrac{\partial E^{l,\,j}_{c\sigma(t)}}{\partial W^{l,\,j}_{c2\sigma(t)}}\end{cases} \tag{36}$$

其中, γ_c 为 critic 神经网络的学习率.

注 4. actor-critic 神经网络权重收敛性分析已经在很多文章中有介绍, 其非本文的重点, 因此不再单独证明其收敛性. 只需要保证学习率足够小, 即可保证网络权重的收敛性.

3 基于混沌系统的切换系统隐私保护

混沌系统实现对敏感数据保护的前提是主–从混沌系统 (7) ~ (8) 能够在有限时间内实现同步. 基

于此, 本节给出混沌误差系统的稳定性分析, 以及基于 PSO 算法的混沌形态同步控制器参数的优化.

3.1 混沌误差系统的稳定性分析

本节设计了一种基于滑模的混沌形态同步控制器, 能够使得混沌误差系统 (9) 在有限时间内收敛. 为了便于后续证明, 下面给出一些合理的假设和引理.

假设 1. 针对混沌系统中的非线性项, 对于任意的状态 $x_1(t)\in\mathbf{R}$ 和 $x_2(t)\in\mathbf{R}$, 一定存在正常数 F_1 使得下面连续光滑约束成立

$$\begin{cases}|f_{m_i}(x_1(t))-f_{m_i}(x_2(t))|\le F_1\,|x_1(t)-x_2(t)|\\ |f_{s_i}(x_1(t))-f_{s_i}(x_2(t))|\le F_1\,|x_1(t)-x_2(t)|\end{cases}$$

假设 2. 针对混沌系统中的不确定项, 对于任意的状态 $x_{m_i}(t)\in\mathbf{R}$ 和 $x_{s_i}(t)\in\mathbf{R}$, 一定存在正常数 B_{m_i} 和 B_{s_i} 使得下面约束成立

$$\begin{cases}|\Delta f_{m_i}(x_{m_i}(t))|\le\ B_{m_i}|x_{m_i}(t)|\\ |\Delta f_{s_i}(x_{s_i}(t))|\le\ B_{s_i}|x_{s_i}(t)|\end{cases}$$

假设 3. 针对混沌系统中的外部扰动项, 一定存在正常数 D_{m_i} 和 D_{s_i} 使其满足下面有界约束

$$|D_{m_i}(t)|\le D_{m_i},\ |D_{s_i}(t)|\le D_{s_i}$$

引理 1. 存在一个连续可微函数 $\mathcal{F}(\nu)$, 对于给定的常数 $\gamma_1>0$, $\gamma_2>0$, $0<k_1<1$ 和 $k_2=1$, 若其满足不等式约束 (37), 则轨迹 $\nu(t)$ 会在式 (38) 给出的有限时间内收敛到原点[27].

$$\dot{\mathcal{F}}(\nu)+\gamma_1\mathcal{F}^{k_1}(\nu)+\gamma_2\mathcal{F}^{k_2}(\nu)\le 0,\ \forall\nu(0)\in\mathbf{R}\tag{37}$$

$$T_F=\frac{\ln[1+\gamma_2\frac{\mathcal{F}^{1-k_1}(\nu(0))}{\gamma_1}]}{k_2(1-k_1)}\tag{38}$$

定理 2. 对于任意的 $i=1,\,2,\,\cdots,\,n_x$ 以及初始误差 $e_i(0)>0$, 在选定的滑模面 (39) 和所设计的混沌形态同步控制器 (40) 的作用下, 混沌误差系统 (9) 的轨迹将在有限时间内到达滑模面.

$$s_i(t)=e_i(t)+\eta_1\int_0^t\mathrm{sign}(e_i(\nu))\mathrm{d}\nu+\eta_2\int_0^t e_i(\nu)\mathrm{d}\nu\tag{39}$$

$$\begin{aligned}u_{s_i}(t)=\ &M_i x_{m_i}(t)-S_i x_{s_i}(t)+f_{m_i}(x_{m_i}(t))-\\ &f_{s_i}(x_{s_i}(t))-\eta_1\mathrm{sign}(e_{m_i}(t))-\\ &\eta_2(e_{m_i}(t))-\eta_3\mathrm{sign}(s_i(t))-\eta_4 s_i(t)-\\ &(B_{m_i}|x_{m_i}(t)|+B_{s_i}|x_{s_i}(t)|+D_{m_i}+\\ &D_{s_i})\mathrm{sign}(s_i(t))\end{aligned}\tag{40}$$

其中, η_1、η_2、η_3、η_4 均为给定的正常数.

证明. 对于任意的 $i=1,\,2,\,\cdots,\,n_x$, 选择如下 Lyapunov 函数

$$V_i(t)=\frac{1}{2}s_i^2(t)\tag{41}$$

对 Lyapunov 函数 (41) 求导, 并结合 (39) 和 (40) 可得

$$\begin{aligned}\dot{V}_i(t)=\ &s_i(t)[\Delta f_{s_i}(x_{s_i}(t))-\Delta f_{m_i}(x_{m_i}(t))+\\ &D_{s_i}(t)-D_{m_i}(t)-\eta_3\mathrm{sign}(s_i(t))-\\ &\eta_4 s_i(t)-(B_{m_i}|x_{m_i}(t)|+B_{s_i}|x_{s_i}(t)|+\\ &D_{m_i}+D_{s_i})\mathrm{sign}(s_i(t))]=\\ &s_i(t)[\Delta f_{s_i}(x_{s_i}(t))-\Delta f_{m_i}(x_{m_i}(t))+\\ &D_{s_i}(t)-D_{m_i}(t)]-\eta_3|s_i(t)|-\eta_4 s_i^2(t)-\\ &|s_i(t)|(B_{m_i}|x_{m_i}(t)|+B_{s_i}\,|x_{s_i}(t)|\ +\\ &D_{m_i}+D_{s_i})\le\\ &-(\eta_3|s_i(t)|+\eta_4 s_i^2(t))\le 0\end{aligned}\tag{42}$$

从式 (42) 可以看出, 其满足引理 1. 因此, 可以得到 V_i 能够在有限时间内收敛, 从而保证了混沌误差系统 (9) 的状态对于滑模面 (39) 的可达性. □

3.2 基于 PSO 算法的控制器参数优化

由于混沌控制器中具有较多参数, 部分参数 (例如 B_{m_i} 和 B_{s_i}) 设置不合理可能会给解密误差带来显著的负面影响. 因此, 本文采用粒子群优化算法, 在参数约束范围内对其进行自动寻优, 步骤如下.

算法初始化. 首先, 定义初始化参数: 粒子群规模 N_p, 最大迭代次数 $k_{p,\max}$, 惯性权重 ω, 个体学习系数 c_1 以及全局学习系数 c_2. 其次, 确定待优化的参数, 本文主要考虑不确定项对解密误差的影响, 因此 B_{m_i} 和 B_{s_i} 被设计为待优化的参数, 并将每个粒子表示为一个 $2n_x$ 维的向量. 然后, 对于首次优化过程 ($k=0$), 生成一个包含 N_p 个粒子的粒子群 $P^k=\{p_1,\,p_2,\,\cdots,\,p_{N_p}\}$. 对于第 m 个粒子 p_m^k, 其位置 $X_m^k=[\alpha_{x1,\,m}^k,\,\alpha_{x2,\,m}^k,\,\cdots,\,\alpha_{xn_x,\,m}^k,\,\beta_{x1,\,m}^k,\,\beta_{x2,\,m}^k,\,\cdots,\,\beta_{xn_x,\,m}^k]$ 和速度 $v_m^k=[\alpha_{v1,\,m}^k,\,\alpha_{v2,\,m}^k,\,\cdots,\,\alpha_{vn_x,\,m}^k,\,\beta_{v1,\,m}^k,\,\beta_{v2,\,m}^k,\,\cdots,\,\beta_{vn_x,\,m}^k]$ 是在合理区间 [0, 2] 内随机选取的.

算法迭代过程. 该过程主要包含五个步骤.

1) 局部适应度值计算. 对于第 k 次迭代中第 m 个粒子, 其局部目标函数 J_m^k 可以通过以下方式计算

$$J_m^k=\int_0^T e_{p,\,m}^k(t)\mathrm{d}t\tag{43}$$

其物理含义是在有限时间 T 内, 将第 k 次迭代中第 m 个粒子的位置参数 $X_m^k=[\alpha_{x1,\,m}^k,\,\alpha_{x2,\,m}^k,\,\cdots,$

$\alpha^k_{xn_x,\,m},\ \beta^k_{x1,\,m},\ \beta^k_{x2,\,m},\ \cdots,\ \beta^k_{xn_x,\,m}]$ 代入系统 (9), 得到误差 $e^k_{p,\,m}(t)$ 并对其进行积分.

2) 个体最优更新. 若局部目标函数 J^k_m 优于该粒子的个体最优值 J^{best}_m, 则更新个体最优值和位置

$$J^{best}_m = J^k_m,\ X^{best}_m = X^k_m \tag{44}$$

其中, X^{best}_m 表示第 m 个粒子的个体最优位置.

3) 全局最优更新. 将每个粒子的个体最优值 J^{best}_m $(m = 1,\ 2,\ \cdots,\ N_p)$ 与全局最优值 J^{gbest} 对比, 若某个粒子 (以 m 为例) 的局部最优值函数优于全局最优值函数, 则更新全局最优值函数和位置

$$J^{gbest} = J^{best}_m,\ X^{gbest} = X^{best}_m \tag{45}$$

4) 粒子速度更新. 粒子速度的更新规则为

$$v^{k+1}_m = \omega v^k_m + c_1 r_1(X^{best}_m - X^k_m) + c_2 r_2(X^{gbest} - X^k_m) \tag{46}$$

其中, r_1 和 r_2 是介于 $[0,\ 1]$ 之间的随机数, 用于引入随机性, 避免算法过早陷入局部最优.

5) 粒子位置更新. 基于当前速度 v^{k+1}_m 来更新粒子位置 X^{k+1}_m, 其更新规则为

$$X^{k+1}_m = X^k_m + v^{k+1}_m \tag{47}$$

4 仿真验证

考虑如下由两个子系统组成的连续切换系统

$$A_1 = \begin{bmatrix} -1.0 & 0.1 & -2.0 \\ 0.0 & -2.0 & -1.0 \\ -1.0 & 0.0 & -1.5 \end{bmatrix},\ B_1 = [1.0\quad -0.5\quad 0.0]^{\mathrm{T}}$$

$$A_2 = \begin{bmatrix} -0.2 & 0.0 & 1.0 \\ 1.0 & 0.0 & -1.0 \\ -1.0 & 0.0 & -0.1 \end{bmatrix},\ B_2 = \begin{bmatrix} 0.0 & 0.0 & 1.0 \end{bmatrix}^{\mathrm{T}}$$

设置系统初始状态为 $x(0) = \begin{bmatrix} 10 & -10 & 15 \end{bmatrix}^{\mathrm{T}}$, 代价函数的权重矩阵为 $Q = I_3$, $R = 1$, 迭代停止阈值 $\epsilon = 0.000\,5$.

主–从混沌系统被设计为

$$\begin{cases} \dot{x}_{m_1}(t) = -0.5x_{m_1}(t) + x^2_{m_2}(t) + \Delta f_{m_1}(x_{m_1}(t)) + D_{m_1}(t) \\ \dot{x}_{m_2}(t) = 2.5x_{m_2}(t) - x_{m_1}(t)x_{m_3}(t) + \Delta f_{m_2}(x_{m_2}(t)) + D_{m_2}(t) \\ \dot{x}_{m_3}(t) = x_{m_2}(t) - 4x_{m_3}(t) + \Delta f_{m_3}(x_{m_3}(t)) + D_{m_3}(t) \end{cases}$$

$$\begin{cases} \dot{x}_{s_1}(t) = 10x_{s_2}(t) - 10x_{s_1}(t) + \Delta f_{s_1}(x_{s_1}(t)) + D_{s_1}(t) + u_{s_1}(t) \\ \dot{x}_{s_2}(t) = 30x_{s_1}(t) - x_{s_2}(t) - x_{s_1}(t)x_{s_3}(t) + \Delta f_{s_2}(x_{s_2}(t)) + D_{s_2}(t) + u_{s_2}(t) \\ \dot{x}_{s_3}(t) = -\dfrac{8}{3}x_{s_3}(t) + x_{s_1}(t)x_{s_2}(t) + \Delta f_{s_3}(x_{s_3}(t)) + D_{s_3}(t) + u_{s_3}(t) \end{cases}$$

其中, $\Delta f_{m_i}\,(i = 1,\ 2,\ 3)$ 和 $\Delta f_{s_i}\,(i = 1,\ 2,\ 3)$ 为混沌系统中的不确定项, 具体被设置为 $\Delta f_{m_1}(x_{m_1}(t)) = 0.15x_{m_1}(t)\sin(t)$, $\Delta f_{m_2}(x_{m_2}(t)) = 0.2x_{m_2}(t)\sin(t)$, $\Delta f_{m_3}(x_{m_3}(t)) = 0.25x_{m_3}(t)\sin(t)$, $\Delta f_{s_1}(x_{s_1}(t)) = 0.1x_{s_1}(t)\cos(t)$, $\Delta f_{s_2}(x_{s_2}(t)) = 0.15x_{s_2}(t)\cos(t)$, $\Delta f_{s_3}(x_{s_3}(t)) = 0.1x_{s_3}(t)\cos(t)$; $D_{m_i}\ (i = 1,\ 2,\ 3)$ 和 $D_{s_i}\ (i = 1,\ 2,\ 3)$ 是均匀分布的随机噪声.

PSO 的参数设置为: 粒子群规模 $N_p = 20$, 最大迭代次数 $k_{p,\,\max} = 20$, 待优化的变量 $[B_{m_1},\ B_{m_2},\ B_{m_3},\ B_{s_1},\ B_{s_2},\ B_{s_3}]$ 的取值范围设定为 $[0,\ 2]$, 惯性权重 $\omega = 1$, 个体学习系数 $c_1 = 1.5$, 全局学习系数 $c_2 = 2$.

通过执行 PSO 算法的迭代过程, 可得 PSO 算法优化过程中适应度值的变化曲线, 如图 2 所示. 在迭代的初期 (迭代次数 0 ~ 4), 适应度值约为 0.106 并保持不变, 但随着迭代次数的增加, 其值逐渐减小, 并在大约第 17 次迭代时趋于最小值, 表明所优化的参数达到了最优. 优化后的最优参数分别为 $B_{m_1} = 0.482\,0$, $B_{m_2} = 1.000\,0$, $B_{m_3} = 0.911\,4$, $B_{s_1} = 1.000\,0$, $B_{s_2} = 0.904\,1$, $B_{s_3} = 0.751\,7$. 将这些优化后的参数代入 $u_{s_i}(t)$, 可以得到如图 3 ~ 8 所示的仿真结果.

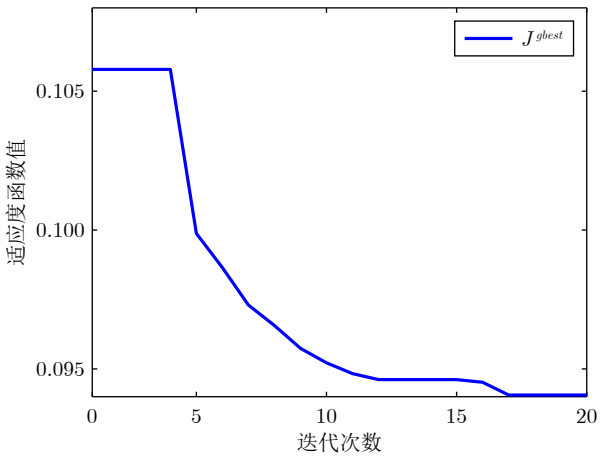

图 2 PSO 优化过程中的适应度值

Fig. 2 Fitness values during the PSO optimization process

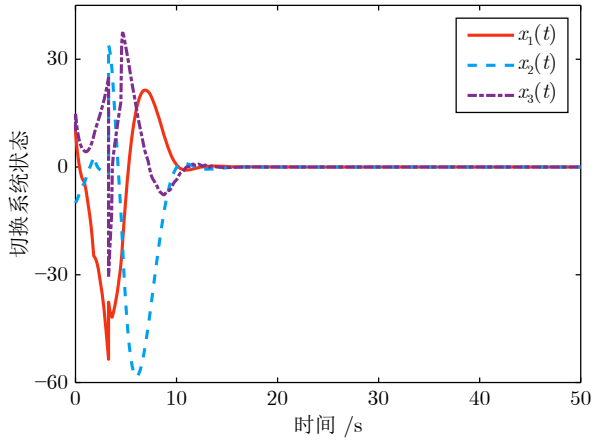

图 3　切换系统的状态轨迹

Fig. 3　State trajectories of switched systems

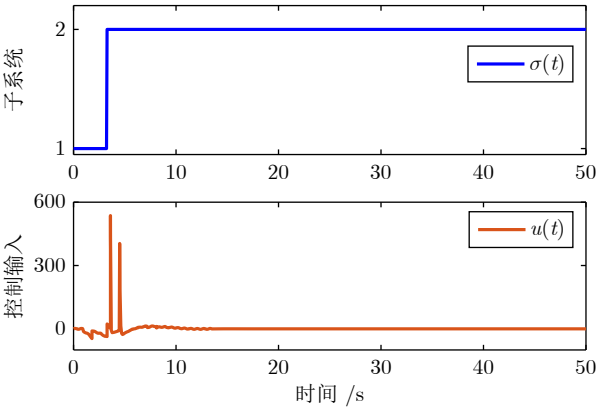

图 4　ADP 算法优化的最优控制策略

Fig. 4　Optimal control policy optimized by ADP algorithm

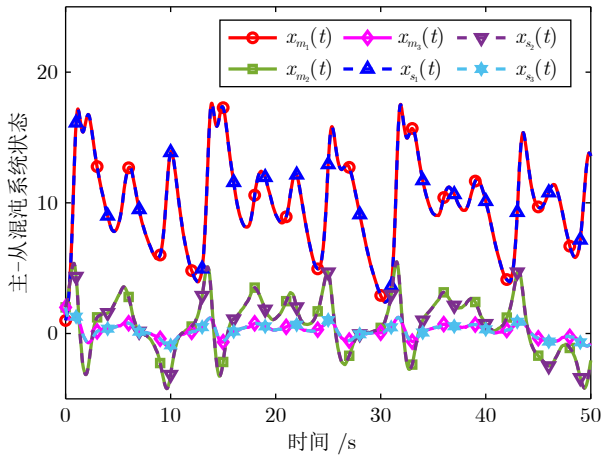

图 5　主−从混沌系统的状态轨迹

Fig. 5　State trajectories of master-slave chaotic systems

图 3 为 ADP 算法优化后的切换系统状态轨迹, 在系统运行的初始阶段虽有波动, 但随着运行时间的增加能够很快地收敛. 图 4 为 ADP 算法优化后的最优控制策略, 上图为切换信号, 下图为控制输入. 该切换信号基于每个子系统性能实时调整, 当其为 1 时表示子系统 1 的性能优于子系统 2, 反之亦然. 对于控制输入, 在系统运行初始阶段其状态存在较大波动, 因此, 需要一个较大的控制输入来保证系统的状态能够快速收敛. 当系统状态逐渐收敛时, 控制输入也逐渐减小并趋于稳定.

图 5 为主−从混沌系统的状态, 从中可以看出其运行轨迹并无固定规律. 因此, 将主混沌系统的状态与通过网络传输的切换系统状态进行叠加, 能够达到很好的隐私保护效果. 此外, 在所设计混沌形态同步控制器的作用下, 从混沌系统能够很好地跟随主混沌系统. 因此, 利用从混沌系统可以对送往控制器的加密信号进行解密. 由主−从混沌系统

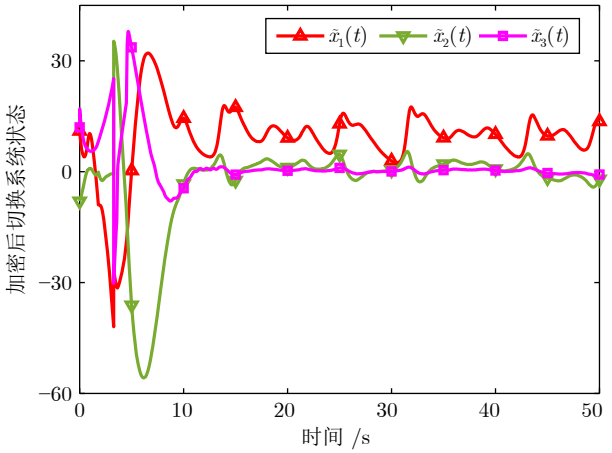

图 6　主混沌系统加密后的切换系统状态轨迹

Fig. 6　State trajectories of switched systems encrypted by a master chaotic system

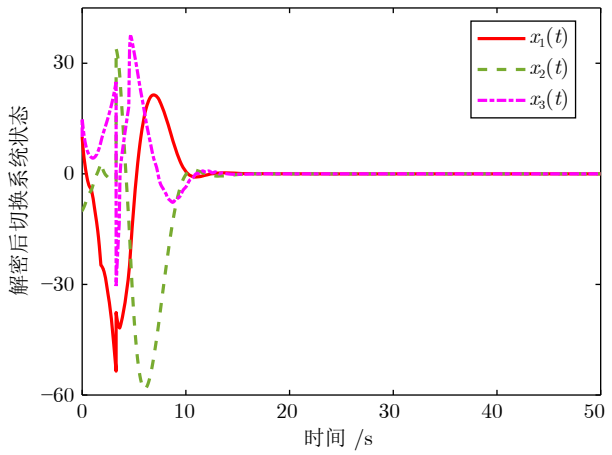

图 7　从混沌系统解密后的切换系统状态轨迹

Fig. 7　State trajectories of switched systems decrypted by slave chaotic system

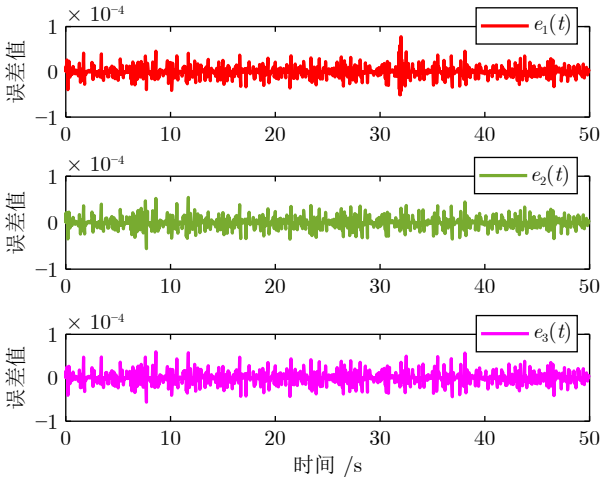

图 8 切换系统加解密之后的误差

Fig. 8 Error of switched systems after encryption and decryption

状态几乎一致证明了所设计混沌形态同步控制器是可行的, 并进一步说明所设计加解密方法的有效性.

图 6 为经过主混沌系统加密后的切换系统状态. 从中可以看出加密后的状态轨迹相较于原本系统的状态轨迹存在较大变化, 最终的收敛趋势存在显著差异. 当系统数据被泄露时, 外部入侵者所得到的是加密处理后的数据, 与原始数据存在差异, 这证明了加密方法的可行性. 图 7 为经过从混沌系统解密后的系统状态, 从中可以看出解密后的状态和原本的状态轨迹几乎一致, 这表明所提基于主−从混沌系统加密的隐私保护方法并不会影响原系统的性能.

图 8 为在混沌形态同步控制器作用下, 主混沌系统与从混沌系统状态的差值. 从中可以看出, 误差的量级是非常小的, 即解密误差基本为 0. 这一方面说明了基于 PSO 优化的混沌形态同步控制器可以保障主−从混沌系统的同步性, 另一方面说明了基于主−从混沌系统的隐私保护方法, 在保护隐私的同时, 并不会影响系统数据的可用性.

5 结束语

本文提出一种基于混沌数据加密的切换系统最优控制与隐私保护, 解决了最优切换系统的数据在非理想网络传输过程中的隐私泄露问题. 首先, 利用 PSO 算法对混沌形态同步控制器参数进行优化, 确保主−从混沌系统在有限时间内达到状态同步, 以减小加解密对原数据可用性的影响; 其次, 利用基于策略迭代的 ADP 算法, 生成一个考虑候选切换律的控制策略, 以保证切换系统的最优性能; 然后, 分别证明了 ADP 算法的收敛性和最优性以及主−从混沌系统误差的稳定性; 最后, 仿真实验验证了以上所提方法的可行性, 证明了所提方法能够在保护系统隐私的同时不影响系统数据的可用性.

参考文献

1 Zhu Y Z, Che J X, Wu F, Chen X K, Zheng W X, Zhou D H. Stability, control and fault diagnosis of switched linear parameter varying systems: A survey. *IEEE/CAA Journal of Automatica Sinica*, 2025, **12**(9): 1745−1761

2 Qi Y W, Qu Z Y, Shen D. Iterative learning control for performance-driven switched systems under all unknown channel gains. *Automatica*, 2026, **183**: Article No. 112607

3 Wang K, Wu F, Sun X M. Switching anti-windup control for aircraft engines. *IEEE Transactions on Industrial Electronics*, 2023, **70**(2): 1830−1840

4 Wu Z Y, Wang Y, Xiong J L, Xie M. Switching periodic event-triggered H_∞ control for NCSs and its application to UAVs. *IEEE Transactions on Vehicular Technology*, 2024, **73**(4): 5078−5088

5 Ma L, Wang Y L, Han Q L. Event-triggered dynamic positioning for mass-switched unmanned marine vehicles in network environments. *IEEE Transactions on Cybernetics*, 2022, **52**(5): 3159−3171

6 Zhu Y, Peng Z H. Stabilizing design for a class of continuous-time switched linear control systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2024, **71**(8): 3900−3904

7 Wang Z C, He W, Sun J, Wang G, Chen J. Event-triggered control of switched nonlinear time-delay systems with asynchronous switching. *IEEE Transactions on Cybernetics*, 2024, **54**(7): 4348−4358

8 Yang D, Li X D, Zhang G F, Lee H W J. State-dependent switching control for nonlinear impulsive switched systems with dwell time. *IEEE Transactions on Automation Science and Engineering*, 2025, **22**: 12093−12101

9 Qi Y W, Zhang S M, Shi Y. Optimized active disturbance rejection control for switched systems: A triggered-learning approach. *IEEE Transactions on Automatic Control*, 2025, **70**(9): 6347−6354

10 Wang Ji-Min, Zhang Ji-Feng, Chen Jia-Long. A survey of privacy protection in control systems. *Acta Automatica Sinica*, 2025, **51**(10): 2178−2200
(王继民, 张纪峰, 陈嘉龙. 控制系统隐私保护研究综述. 自动化学报, 2025, **51**(10): 2178−2200)

11 Qi Y W, Guo S T, Chi R H, Tang Y W, Qu Z Y. Privacy preserving for switched systems under robust data-driven predictive control. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2025, **55**(1): 480−490

12 Chen W, Wang Z D, Hu J, Liu G P. Differentially private average consensus with logarithmic dynamic encoding-decoding scheme. *IEEE Transactions on Cybernetics*, 2023, **53**(10): 6725−6736

13 Qi Y W, Wang C, Zhang S W, Ahn C K. Performance-dependent privacy preserving for switched multiple systems under active disturbance rejection control. *IEEE Transactions on Automation Science and Engineering*, 2025, **22**: 17209−17220

14 Qian J, Jiang H Y, Yu Y, Wang H, Miao D Q. Multi-level personalized k-anonymity privacy-preserving model based on sequential three-way decisions. *Expert Systems With Applications*, 2024, **239**: Article No. 122343

15 Hassan M U, Rehmani M H, Chen J J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials*, 2020, **22**(1): 746−789

16 Zhang C S, Weng J, Weng J S, Zhong Y J, Liu J N, Deng C L. Robust and secure federated learning with verifiable differential privacy. *IEEE Transactions on Dependable and Secure Comput-*

ing, 2025, **22**(5): 5713−5729

17 Carroll T L, Pecora L M. Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems*, 1991, **38**(4): 453−456

18 Teng L, Cao P F, Liu Y. Multi-image encryption algorithm based on novel spatiotemporal chaotic system and dynamical chaotic trajectories. *IEEE Transactions on Circuits and Systems for Video Technology*, 2025, **35**(2): 1562−1575

19 Hou J L, Xi R, Liu P, Liu T L. The switching fractional order chaotic system and its application to image encryption. *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(2): 381−388

20 Wang D, Gao N, Liu D R, Li J N, Lewis F L. Recent progress in reinforcement learning and adaptive dynamic programming for advanced control applications. *IEEE/CAA Journal of Automatica Sinica*, 2024, **11**(1): 18−36

21 Yang Y L, Pan Y P, Xu C Z, Wunsch D C. Hamiltonian-driven adaptive dynamic programming with efficient experience replay. *IEEE Transactions on Neural Networks and Learning Systems*, 2024, **35**(3): 3278−3290

22 Zhao B, Zhang S C, Liu D R. Self-triggered approximate optimal neuro-control for nonlinear systems through adaptive dynamic programming. *IEEE Transactions on Neural Networks and Learning Systems*, 2025, **36**(3): 4713−4723

23 Liu M, Liu Q H, Zhang L X, Duan G R, Cao X B. Adaptive dynamic programming-based fault-tolerant attitude control for flexible spacecraft with limited wireless resources. *Science China Information Sciences*, 2023, **66**(10): Article No. 202201

24 Qi Y W, Guo S T, Ahn C K, Huang J. Privacy for switched systems under MPC: A privacy-preserved rolling optimization strategy. *IEEE Transactions on Cybernetics*, 2025, **55**(5): 2085−2097

25 Kim J Y, Jeong J H, Kim J H, Kim J M. ABDM: Anonymity-based big data management for protecting healthcare data from privacy breach. *IEEE Network*, 2025, **39**(11): 298−305

26 Chen Y, Huang D Q, Tan S Q. Privacy-enabled secure iterative learning control of networked systems subject to disclosure attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2024, **71**(1): 196−200

27 Yu X, Man Z. Fast terminal sliding-mode control design for nonlinear dynamical systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2002, **49**(2): 261−264

齐义文 福州大学电气工程与自动化学院教授. 2012 年获得哈尔滨工业大学博士学位. 主要研究方向为切换系统, 隐私保护, 学习控制.
E-mail: qiyiwen@fzu.edu.cn
(**QI Yi-Wen** Professor at the College of Electrical Engineering and Automation, Fuzhou University. He received his Ph.D. degree from Harbin Institute of Technology in 2012. His research interests include switched systems, privacy preserving, and learning control.)

乔鑫鑫 福州大学电气工程与自动化学院硕士研究生. 主要研究方向为隐私保护, 安全约束, 自适应动态规划.
E-mail: qiaoxinxin107@163.com
(**QIAO Xin-Xin** Master student at the College of Electrical Engineering and Automation, Fuzhou University. His research interests include privacy preserving, security constraint, and adaptive dynamic programming.)

邓飞其 华南理工大学自动化科学与工程学院教授. 1997 年获得华南理工大学博士学位. 主要研究方向为智能控制系统, 系统工程. 本文通信作者.
E-mail: aufqdeng@scut.edu.cn
(**DENG Fei-Qi** Professor at the School of Automation Science and Engineering, South China University of Technology. He received his Ph.D. degree from South China University of Technology in 1997. His research interests include intelligent control system and system engineering. Corresponding author of this paper.)

王云龙 沈阳航空航天大学自动化学院硕士研究生. 主要研究方向为切换系统, 隐私保护, 自适应动态规划.
E-mail: yunlong_sau@126.com
(**WANG Yun-Long** Master student at the School of Automation, Shenyang Aerospace University. His research interests include switched systems, privacy preserving, and adaptive dynamic programming.)