基于虚假数据检测的信息物理系统安全学习控制方法

苗金钊[①] 刘金良*[①] 孙 乐[①] 查利娟[②] 田恩刚[③]

[①](南京信息工程大学计算机学院 南京 210044)

[②](南京林业大学理学院 南京 210037)

[③](上海理工大学光电信息与计算机工程学院 上海 200093)

摘 要：随着信息物理系统(CPS)在关键基础设施中的广泛部署，其面临的安全威胁日益严峻，特别是虚假数据注入攻击对系统感知与控制能力构成了实质性挑战。针对这一问题，该文提出了一种融合攻击检测、状态估计与控制策略学习的安全控制框架。该方法通过构建传感器数据的安全评估指标，实现对潜在虚假观测数据的实时检测，并在无攻击先验信息的条件下，动态估计可能存在的攻击信号。在此基础上，进一步提出融合多源传感器观测的状态估计策略，以提高对系统真实状态的重构精度。此外，该文还提出了一种基于动态权重在线更新的自适应学习控制方法，利用梯度下降法逼近最优控制策略，从而增强系统在复杂环境中的稳态性能与抗攻击能力。仿真实验结果验证了该方法在虚假数据注入攻击环境下的有效性与安全性能。

关键词：信息物理系统；虚假数据检测；安全控制；网络攻击

中图分类号：TP274 **文献标识码**：A **文章编号**：1009-5896(2026)04-1434-10

DOI: 10.11999/JEIT250537 **CSTR**: 32379.14.JEIT250537

1 引言

信息物理系统(Cyber-Physical Systems, CPS)是一类融合计算、通信与物理过程的高度集成网络化系统[1,2]，近年来在工业控制、智能电网、自动驾驶等关键领域中发挥着越来越重要的作用[3]。CPS依托嵌入式计算设备实现对物理世界的实时感知与控制，推动物理系统与数字空间的深度融合[4]。这种融合提升了系统效率与智能水平，同时也带来了更加复杂和严峻的安全挑战。因此，如何保障系统的安全性与稳定性已成为CPS设计过程中的关键问题。

在开放式通信环境中，虚假数据攻击、拒绝服务攻击等网络攻击手段已成为影响CPS安全性与稳定性的重要威胁[5]。这些攻击可能导致传感器数据被篡改或中断，从而对系统运行状态造成负面影响，甚至诱发严重的安全事故[6]。为了保障CPS的稳定运行，近年来学术界围绕攻击检测与防御机制提出了多种策略。Zhu等人[7]针对遭受虚假数据攻击的非线性CPS提出了一种基于数据差异的攻击检测方法。Gao等人[8]基于幂积分器技术设计了受损状态变量驱动的CPS自适应控制器，并引入动态切换机制以补偿未知攻击影响。Liu等人[9]提出了一种交替式虚假数据攻击策略，通过不断改变攻击方向规避融合历史信息的攻击检测器。Guibene等人[10]提出了一种基于序列模式挖掘的异常检测方法，通过学习系统正常运行的数据特征实现高精度攻击识别。Zhang等人[11]引入自适应反推技术并结合非线性扰动观测器设计了一种基于径向基神经网络的防御策略。Li等人[12]通过构建基于历史数据动态更新密钥的加密方案，实现了对重放攻击、虚假数据攻击等多类攻击的快速检测。尽管已有研究在攻击检测方面取得了显著进展，但多数方法仍存在攻击检测与控制策略相互割裂的问题，难以构建统一高效的闭环安全控制机制。同时，现有方法普遍缺乏对遭受攻击后系统数据的信任评估与重构能力，难以支撑控制策略的持续优化与动态更新。

虚假数据攻击下传统依赖精确可靠数据的控制策略难以有效应对攻击带来的系统数据偏差，这促使研究者不断探索具有自适应能力的学习控制方法[13]。其中，博弈理论被广泛用于建模控制器与攻击者间的对抗关系，通过构建零和博弈框架可将安全控制问题形式化为哈密顿-雅可比-艾萨克(Hamilton-Jacobi-Isaacs, HJI)方程的求解。然而，HJI方程通常难以直接获取解析解，因此许多研究人员采用自适应学习方法近似求解最优控制策略。Soleimani等人[14]通过引入遗忘因子提出了一种融合强化学习与迭代学习控制的CPS数据驱动控制方法。Fei等人[15]针对虚假数据攻击下的安全控制问题，基于零和博弈理论提出了两种无模型数据驱动的Q学习算法。Li等人[16]提出了混合攻击下无

收稿日期：2025-06-09；改回日期：2025-09-16；网络出版：2025-09-23

*通信作者： 刘金良 liujinliang@vip.163.com

基金项目：国家自然科学基金(62373252, 62273174)

Foundation Items: The National Natural Science Foundation of China (62373252, 62273174)

状态向量需求的改进Q学习算法，并设计了数据驱动最优跟踪控制器。Li等人[17]利用马尔可夫跳变信号建模了网络攻击的不确定性，设计了基于3层神经网络的攻击信号学习方法以及控制策略。Shen等人[18]基于零和博弈提出了并行强化学习框架下的模型驱动与无模型混合学习算法。Ren等人[19]针对具有随机通信约束的CPS控制问题，提出了分组输入数据驱动的自适应学习控制策略。当前主流的学习控制方法多数基于系统状态可直接或精确观测的假设，普遍缺乏面向受攻击数据的辨识与重构机制，在系统状态数据遭到篡改的情况下，难以保障学习过程的有效性以及系统稳定性。

基于上述问题，本文提出了一种融合攻击检测、状态估计与策略更新的安全学习控制方法，突破传统检测与控制割裂、观测可靠性依赖等局限，实现了CPS在未知攻击环境下的稳定性保障与控制性能提升。与现有方法相比，本文的主要创新点与贡献体现在以下3个方面：(1)提出了一种基于传感器数据安全评估指标的实时攻击检测方法，在无须攻击先验知识的前提下，实现了对虚假数据攻击的有效识别与估计；(2)设计了一种融合多源观测信息的状态重构策略，通过多观测通道的信息融合实现了虚假数据注入攻击干扰下的高精度系统状态估计；(3)构建了一种基于动态权重在线更新的自适应学习控制方法，利用梯度下降法优化控制策略，增强了系统在复杂环境下的控制性能与抗攻击能力。

2　系统模型

采用状态空间建模方法，将具有动态特性的CPS构建为如式(1)形式的连续时间系统模型

$$\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{w}(t) \tag{1}$$

其中，$\boldsymbol{x}(t)\in\mathbb{R}^n$是系统状态向量，$\boldsymbol{u}(t)\in\mathbb{R}^m$为控制输入，$\boldsymbol{w}(t)\in\mathbb{R}^n$表示系统受到的外部有界扰动，$\boldsymbol{A}\in\mathbb{R}^{n\times n}$和$\boldsymbol{B}\in\mathbb{R}^{n\times m}$均为已知的系统矩阵。

考虑到实际应用中CPS所处环境的复杂性与资源受限性，通常采用多组分布式传感器协同对系统状态进行观测。每组传感器由于感知能力或部署位置的限制，仅能获取系统状态向量中的部分分量。为描述CPS中的N组分布式传感器对系统状态的观测关系，引入如式(2)观测模型

$$\boldsymbol{y}_i(t)=\boldsymbol{C}_i\boldsymbol{x}(t)+\boldsymbol{v}_i(t) \tag{2}$$

其中，$\boldsymbol{y}_i(t)\in\mathbb{R}^{p_i}$表示第$i$组传感器的观测输出，$\boldsymbol{C}_i\in\mathbb{R}^{p_i\times n}$为观测矩阵，$\boldsymbol{v}_i(t)\in\mathbb{R}^{p_i}$为有界观测噪声。

针对CPS中的分布式传感器网络，本文将第i组传感器设定为本地传感器，其可直接获取系统状态的观测值，用$j\in\mathcal{N}_i$表示与本地传感器节点i通过通信网络相连接的远程传感器节点集合。考虑到传感器之间的网络通信受到虚假数据注入攻击的场景，攻击者篡改远程观测数据的过程可建模为

$$\bar{\boldsymbol{y}}_j(t)=\boldsymbol{y}_j(t)+\boldsymbol{\xi}_j(t) \tag{3}$$

其中，$\bar{\boldsymbol{y}}_j(t)\in\mathbb{R}^{p_j}$表示本地传感器节点$i$实际接收到的第$j$组观测数据，$\boldsymbol{y}_j(t)\in\mathbb{R}^{p_j}$为远程传感器的真实观测值，$\boldsymbol{\xi}_j(t)\in\mathbb{R}^{p_j}$为攻击者注入的虚假数据。

3　主要成果

3.1　虚假数据检测

为了定量评估远程传感器j的观测数据中虚假数据攻击的强度，本文引入定义如式(4)检测指标[20]

$$H_j(t)=\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=1}^{t}\|\hat{\boldsymbol{\xi}}_j(\tau)\|^2 \tag{4}$$

其中，$\hat{\boldsymbol{\xi}}_j(t)\in\mathbb{R}^{p_j}$表示对第$j$组传感器信号中可能存在的攻击信号的估计。该指标反映了攻击信号在时间尺度上的平均能量水平，当$H_j(t)$逐渐增长时，可判断传感器j的观测数据被注入了虚假数据。

为了重构传感器数据中无法直接观测的攻击信号，本文设计了一种形式如式(5)的攻击信号估计器

$$\hat{\boldsymbol{\xi}}_j(t)=\bar{\boldsymbol{y}}_j(t)-\boldsymbol{C}_j\boldsymbol{z}_j(t) \tag{5}$$

其中，$\boldsymbol{z}_j(t)\in\mathbb{R}^n$为构造的辅助状态变量，用于逼近远程传感器在无攻击情况下应有的观测输出。辅助状态的演化动态由式(6)状态观测器驱动

$$\dot{\boldsymbol{z}}_j(t)=\boldsymbol{A}\boldsymbol{z}_j(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{K}_j(\tilde{\boldsymbol{y}}_j(t)-\boldsymbol{C}_j\boldsymbol{z}_j(t)) \tag{6}$$

其中，$\boldsymbol{K}_j\in\mathbb{R}^{n\times p_j}$是待设计的增益矩阵，$\tilde{\boldsymbol{y}}_j(t)=\boldsymbol{C}_j\hat{\boldsymbol{x}}_i(t)$为本地状态估计器的观测值，$\hat{\boldsymbol{x}}_i(t)\in\mathbb{R}^n$是本地状态估计，其计算方法由下文的融合状态估计器给出。

定义辅助状态估计误差$\tilde{\boldsymbol{z}}_j(t)=\boldsymbol{x}(t)-\boldsymbol{z}_j(t)$以及攻击估计误差$\tilde{\boldsymbol{\xi}}_j(t)=\boldsymbol{\xi}_j(t)-\hat{\boldsymbol{\xi}}_j(t)$。根据式(5)中攻击信号估计值的计算方法，该估计误差可进一步表示为

$$\tilde{\boldsymbol{\xi}}_j(t)=-\boldsymbol{C}_j\tilde{\boldsymbol{z}}_j(t)+\boldsymbol{v}_j(t) \tag{7}$$

此外，由式(6)和估计误差$\tilde{\boldsymbol{z}}_j(t)$的定义推导可得

$$\dot{\tilde{\boldsymbol{z}}}_j(t)=(\boldsymbol{A}-\boldsymbol{K}_j\boldsymbol{C}_j)\tilde{\boldsymbol{z}}_j(t)+\boldsymbol{K}_j\boldsymbol{C}_j(\boldsymbol{x}(t)-\hat{\boldsymbol{x}}_i(t))+\boldsymbol{w}(t) \tag{8}$$

3.2　融合状态估计

为了提升CPS在攻击环境下的状态估计精度，

本文构建了一种融合多源观测数据的分布式状态估计策略。将本地传感器节点i作为多源观测数据的融合中心，定义融合状态估计为

$$\tilde{\boldsymbol{x}}_i(t)=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\hat{\boldsymbol{x}}_j(t) \tag{9}$$

其中，$\boldsymbol{\Omega}_j(t)\in\mathbb{R}^{n\times n}$为基于检测指标动态调整的加权系数。针对本地传感器节点i，其状态估计器设计为

$$\dot{\hat{\boldsymbol{x}}}_i(t)=\boldsymbol{A}\hat{\boldsymbol{x}}_i(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{K}_i(\boldsymbol{y}_i(t)-\boldsymbol{C}_i\hat{\boldsymbol{x}}_i(t)) \tag{10}$$

对于远程传感器j，由于其通过网络传输的观测数据存在被攻击的可能性，因此本文设计了如式(11)的基于攻击补偿后观测数据的状态估计器

$$\dot{\hat{\boldsymbol{x}}}_j(t)=\boldsymbol{A}\hat{\boldsymbol{x}}_j(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{K}_j(\hat{\boldsymbol{y}}_j(t)-\boldsymbol{C}_j\hat{\boldsymbol{x}}_j(t)) \tag{11}$$

其中，$\hat{\boldsymbol{y}}_j(t)=\overline{\boldsymbol{y}}_j(t)-\hat{\boldsymbol{\xi}}_j(t)$为攻击信号估计值补偿后的远程观测数据。

为了增强融合状态估计器在攻击环境下的可靠性，本文设计了一种基于估计误差分布的自适应加权系数计算方法。首先，定义传感器节点i与其邻居节点$j\in\mathcal{Q}_i$之间的状态估计误差为$\boldsymbol{e}_{ij}(t)=\hat{\boldsymbol{x}}_i(t)-\hat{\boldsymbol{x}}_j(t)$，其中，$\mathcal{Q}_i\subseteq\mathcal{N}_i$ 表示观测数据的攻击检测指标相比前一时刻的检测指标没有增大的远程传感器，即被判定为安全的邻居节点集合。基于上述状态估计误差，构造如式(12)的对角误差矩阵

$$\begin{aligned}\boldsymbol{\Theta}_i(t)=\mathrm{blkdiag}\big\{&\boldsymbol{e}_{i1}(t)\boldsymbol{e}_{i1}^{\mathrm{T}}(t),\boldsymbol{e}_{i2}(t)\boldsymbol{e}_{i2}^{\mathrm{T}}(t),\cdots,\\&\boldsymbol{e}_{iq}(t)\boldsymbol{e}_{iq}^{\mathrm{T}}(t)\big\}\end{aligned} \tag{12}$$

其中，q为安全通信邻居节点的个数。为了实现对多源观测数据的最优加权融合，定义融合权重矩阵为

$$\boldsymbol{\Xi}_i(t)=[\boldsymbol{\Omega}_1(t),\boldsymbol{\Omega}_2(t),\cdots,\boldsymbol{\Omega}_q(t)]^{\mathrm{T}} \tag{13}$$

为保证加权估计保持无偏性，权重应满足的约束为

$$\sum_{j\in\mathcal{Q}_i}\boldsymbol{\Omega}_j(t)=\boldsymbol{I}_n \tag{14}$$

基于最小方差估计原则，本文将权重设计问题转化为如式(15)的凸优化问题

$$\min_{\boldsymbol{\Xi}_i(t)\in\mathbb{R}^{nq\times n}}\mathrm{trace}\left(\boldsymbol{\Xi}_i^{\mathrm{T}}(t)\boldsymbol{\Theta}_i(t)\boldsymbol{\Xi}_i(t)\right) \tag{15}$$

该优化目标通过最小化融合估计的加权均方误差，从而提升融合状态估计器在攻击干扰下的精度与稳定性。上述式(15)中的凸优化问题为带有线性等式约束的二次规划问题，可通过标准数值优化方法高效求解，适合在线部署于CPS中。此外，定义传感器节点i以及其邻居节点j与系统状态之间的估计误差分别为$\hat{\boldsymbol{e}}_i(t)=\boldsymbol{x}(t)-\hat{\boldsymbol{x}}_i(t)$以及$\hat{\boldsymbol{e}}_j(t)=\boldsymbol{x}(t)-\hat{\boldsymbol{x}}_j(t)$。由式(1)、式(10)和式(11)推导可得

$$\begin{aligned}\dot{\boldsymbol{e}}_{ij}(t)=&\boldsymbol{A}\boldsymbol{e}_{ij}(t)+\boldsymbol{K}_i\boldsymbol{C}_i\hat{\boldsymbol{e}}_i(t)-\boldsymbol{K}_j\boldsymbol{C}_j\hat{\boldsymbol{e}}_j(t)-\boldsymbol{K}_j\tilde{\boldsymbol{\xi}}_j(t)\\&+\boldsymbol{K}_i\boldsymbol{v}_i(t)+\boldsymbol{K}_j\boldsymbol{v}_j(t)\end{aligned} \tag{16}$$

$$\dot{\hat{\boldsymbol{e}}}_i(t)=(\boldsymbol{A}-\boldsymbol{K}_i\boldsymbol{C}_i)\hat{\boldsymbol{e}}_i(t)+\boldsymbol{w}(t)-\boldsymbol{K}_i\boldsymbol{v}_i(t) \tag{17}$$

$$\dot{\hat{\boldsymbol{e}}}_j(t)=(\boldsymbol{A}-\boldsymbol{K}_j\boldsymbol{C}_j)\hat{\boldsymbol{e}}_j(t)+\boldsymbol{w}(t)-\boldsymbol{K}_j\tilde{\boldsymbol{\xi}}_j(t)-\boldsymbol{K}_j\boldsymbol{v}_j(t) \tag{18}$$

将基于多源观测数据构建的融合状态估计值$\tilde{\boldsymbol{x}}_i(t)$与真实状态之间的估计误差定义为$\boldsymbol{\rho}_i(t)=\boldsymbol{x}(t)-\tilde{\boldsymbol{x}}_i(t)$。在此基础上，式(10)中传感器节点$i$的本地估计器动态被重写为

$$\begin{aligned}\dot{\hat{\boldsymbol{x}}}_i(t)=&(\boldsymbol{A}-\boldsymbol{K}_i\boldsymbol{C}_i)\hat{\boldsymbol{x}}_i(t)+\boldsymbol{K}_i\boldsymbol{C}_i\tilde{\boldsymbol{x}}_i(t)+\boldsymbol{B}\boldsymbol{u}(t)\\&+\boldsymbol{K}_i\boldsymbol{C}_i\boldsymbol{\rho}_i(t)+\boldsymbol{K}_i\boldsymbol{v}_i(t)\end{aligned} \tag{19}$$

式中的远程传感器的估计器动态被重写为

$$\dot{\tilde{\boldsymbol{x}}}_i(t)=\boldsymbol{A}\tilde{\boldsymbol{x}}_i(t)+\boldsymbol{B}\boldsymbol{u}(t)+\tilde{\boldsymbol{\rho}}_i(t)+\overline{\boldsymbol{\xi}}_i(t)+\tilde{\boldsymbol{v}}_i(t) \tag{20}$$

其中，

$$\tilde{\boldsymbol{\rho}}_i(t)=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\boldsymbol{K}_j\boldsymbol{C}_j\hat{\boldsymbol{e}}_j(t),$$

$$\overline{\boldsymbol{\xi}}_i(t)=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\boldsymbol{K}_j\tilde{\boldsymbol{\xi}}_j(t),$$

$$\tilde{\boldsymbol{v}}_i(t)=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\boldsymbol{K}_j\boldsymbol{v}_j(t),$$

3.3 安全控制方法

定义增广向量$\eta_i(t)=[\hat{\boldsymbol{x}}_i^{\mathrm{T}}(t),\tilde{\boldsymbol{x}}_i^{\mathrm{T}}(t)]^{\mathrm{T}}$以及$\tilde{\boldsymbol{w}}_i(t)=[\boldsymbol{\rho}_i^{\mathrm{T}}(t),\boldsymbol{v}_i^{\mathrm{T}}(t),\tilde{\boldsymbol{\rho}}_i^{\mathrm{T}}(t),\overline{\boldsymbol{\xi}}_i^{\mathrm{T}}(t),\tilde{\boldsymbol{v}}_i^{\mathrm{T}}(t)]^{\mathrm{T}}$，则增广系统可表示为

$$\dot{\eta}_i(t)=\boldsymbol{\mathcal{A}}_i\eta_i(t)+\mathcal{B}\boldsymbol{u}(t)+\mathcal{D}_i\tilde{\boldsymbol{w}}_i(t) \tag{21}$$

其中，

$$\boldsymbol{\mathcal{A}}_i=\begin{bmatrix}\boldsymbol{A}-\boldsymbol{K}_i\boldsymbol{C}_i & \boldsymbol{K}_i\boldsymbol{C}_i\\ 0 & \boldsymbol{A}\end{bmatrix},\ \boldsymbol{\mathcal{B}}=\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{B}\end{bmatrix},$$

$$\boldsymbol{\mathcal{D}}_i=\begin{bmatrix}\boldsymbol{K}_i\boldsymbol{C}_i & \boldsymbol{K}_i & 0 & 0 & 0\\ 0 & 0 & \boldsymbol{I}_n & \boldsymbol{I}_n & \boldsymbol{I}_n\end{bmatrix}$$

为优化控制性能并抑制扰动影响，本文引入性能指标函数为

$$\begin{aligned}J(\eta_i,\boldsymbol{u},\tilde{\boldsymbol{w}}_i)=\int_t^{\infty}&\left[\eta_i^{\mathrm{T}}(s)\boldsymbol{P}_i\eta_i(s)+\boldsymbol{u}^{\mathrm{T}}(s)\boldsymbol{R}\boldsymbol{u}(s)\right.\\&\left.-\gamma_i^2\tilde{\boldsymbol{w}}_i^{\mathrm{T}}(s)\tilde{\boldsymbol{w}}_i(s)\right]\mathrm{d}s\end{aligned} \tag{22}$$

其中，$\boldsymbol{P}_i>0$和$\boldsymbol{R}>0$为权重矩阵，$\gamma_i>0$为扰动抑制指标。为增强对未来状态的衰减性惩罚，进一步定义加权的指数衰减性能泛函为

$$V(\eta_i)=\int_t^{\infty}\mathrm{e}^{-\kappa(s-t)}\left[\eta_i^{\mathrm{T}}(s)\boldsymbol{P}_i\eta_i(s)+\boldsymbol{u}^{\mathrm{T}}(s)\boldsymbol{R}\boldsymbol{u}(s)-\gamma_i^2\tilde{\boldsymbol{w}}_i^{\mathrm{T}}(s)\tilde{\boldsymbol{w}}_i(s)\right]\mathrm{d}s \tag{23}$$

其中，$\kappa>0$为时间衰减因子。根据式(23)，最优值函数定义为

$$V^*(\eta_i)=\min_{\boldsymbol{u}\in\Pi_{\boldsymbol{u}}}\max_{\tilde{\boldsymbol{w}}_i\in\Pi_{\tilde{\boldsymbol{w}}_i}}V(\eta_i) \tag{24}$$

其中，$\Pi_{\boldsymbol{u}}$和$\Pi_{\tilde{\boldsymbol{w}}_i}$分别为可行控制与扰动策略集合。为推导最优策略，哈密顿函数写为

$$H(\boldsymbol{V}_\eta^*,\eta_i,\boldsymbol{u},\tilde{\boldsymbol{w}}_i)=(\boldsymbol{V}_\eta^*)^{\mathrm{T}}\dot{\eta}_i(t)+\eta_i^{\mathrm{T}}(t)\boldsymbol{P}_i\eta_i(t)+\boldsymbol{u}^{\mathrm{T}}(t)\boldsymbol{R}\boldsymbol{u}(t)-\gamma_i^2\tilde{\boldsymbol{w}}_i^{\mathrm{T}}(t)\tilde{\boldsymbol{w}}_i(t)-\kappa V^*(\eta_i) \tag{25}$$

其中，$\boldsymbol{V}_\eta^*=\partial V^*(\eta_i)/\partial\eta_i$是值函数关于增广状态的偏导数。根据零和博弈理论中的最优性条件，理想的最优控制输入与最差扰动策略分别表示为

$$\boldsymbol{u}^*(\eta_i)=-\frac{1}{2}\boldsymbol{R}^{-1}\mathcal{B}^{\mathrm{T}}\boldsymbol{V}_\eta^* \tag{26}$$

$$\tilde{\boldsymbol{w}}_i^*(\eta_i)=\frac{1}{2\gamma_i^2}\mathcal{D}_i^{\mathrm{T}}V_\eta^* \tag{27}$$

为规避传统最优控制难以解析求解的问题，本文通过多项式基函数和自适应权重向量逼近学习最优值函数$V^*(\eta_i)$，从而构建近似的最优控制器与扰动策略，具体写为

$$V^*(\eta_i)=\boldsymbol{W}^{\mathrm{T}}\boldsymbol{\varphi}(\eta_i)+\epsilon(\eta_i) \tag{28}$$

其中，$\boldsymbol{W}\in\mathbb{R}^d$为理想的权重向量，$\boldsymbol{\varphi}(\boldsymbol{z})\in\mathbb{R}^d$为基函数，$\epsilon(\boldsymbol{z})$表示近似误差。进一步，$\boldsymbol{V}_\eta^*$可写为

$$V_\eta^*=\boldsymbol{\varphi}_\eta^{\mathrm{T}}\boldsymbol{W}+\boldsymbol{\epsilon}_\eta \tag{29}$$

其中，$\boldsymbol{\varphi}_\eta=\partial\boldsymbol{\varphi}(\eta_i)/\partial\eta_i$和$\boldsymbol{\epsilon}_\eta=\partial\boldsymbol{\epsilon}(\eta_i)/\partial\eta_i$分别为基函数和近似误差关于增广状态的偏导数。根据式(28)和式(29)，可构造近似值函数及其偏导数为

$$\overline{V}^*(\eta_i)=\overline{\boldsymbol{W}}^{\mathrm{T}}\boldsymbol{\varphi}(\eta_i) \tag{30}$$

$$\overline{\boldsymbol{V}}_\eta^*=\boldsymbol{\varphi}_\eta^{\mathrm{T}}\overline{\boldsymbol{W}} \tag{31}$$

其中，$\bar{\boldsymbol{W}}\in\mathbb{R}^d$表示用于近似最优值函数的自适应权重向量，通过梯度下降方法不断在线更新以逼近最优控制策略对应的理想权重$\boldsymbol{W}$。基于式(30)和式(31)可以构建近似控制策略与扰动策略为

$$\overline{\boldsymbol{u}}(\eta_i)=-\frac{1}{2}\boldsymbol{R}^{-1}\boldsymbol{\mathcal{B}}^{\mathrm{T}}\boldsymbol{\varphi}_\eta^{\mathrm{T}}\overline{\boldsymbol{W}} \tag{32}$$

$$\overline{\boldsymbol{w}}_i(\eta_i)=\frac{1}{2\gamma_i^2}\boldsymbol{\mathcal{D}}_i^{\mathrm{T}}\boldsymbol{\varphi}_\eta^{\mathrm{T}}\overline{\boldsymbol{W}} \tag{33}$$

将式(32)和式(33)代入式(25)的哈密顿函数中，构造近似哈密顿函数为

$$\bar{H}(\bar{\boldsymbol{V}}_\eta^*,\eta_i,\bar{\boldsymbol{u}},\bar{\boldsymbol{w}}_i)=\bar{\boldsymbol{W}}^{\mathrm{T}}\boldsymbol{\varphi}_\eta\dot{\eta}_i(t)+\eta_i^{\mathrm{T}}(t)\boldsymbol{P}_i\eta_i(t)+\bar{\boldsymbol{u}}^{\mathrm{T}}(\eta_i)\boldsymbol{R}\bar{\boldsymbol{u}}(\eta_i)-\gamma_i^2\bar{\boldsymbol{w}}_i^{\mathrm{T}}(\eta_i)\bar{\boldsymbol{w}}_i(\eta_i)-\kappa\bar{\boldsymbol{W}}^{\mathrm{T}}\boldsymbol{\varphi}(\eta_i) \tag{34}$$

为了衡量当前近似值函数与理想最优值函数之间的误差，构建近似误差为

$$\begin{aligned}\zeta_i(t)&=\bar{H}(\bar{\boldsymbol{V}}_\eta^*,\eta_i,\bar{\boldsymbol{u}},\bar{\boldsymbol{w}}_i)-H(\boldsymbol{V}_\eta^*,\eta_i,\boldsymbol{u},\tilde{\boldsymbol{w}}_i)\\&=\bar{\boldsymbol{W}}^{\mathrm{T}}\boldsymbol{\varrho}_i(t)+\eta_i^{\mathrm{T}}(t)\boldsymbol{P}_i\eta_i(t)+\bar{\boldsymbol{u}}^{\mathrm{T}}(\eta_i)\boldsymbol{R}\bar{\boldsymbol{u}}(\eta_i)-\gamma_i^2\bar{\boldsymbol{w}}_i^{\mathrm{T}}(\eta_i)\bar{\boldsymbol{w}}_i(\eta_i)\end{aligned} \tag{35}$$

其中，$\boldsymbol{\varrho}_i(t)=\boldsymbol{\varphi}_\eta\dot{\eta}_i(t)-\kappa\boldsymbol{\varphi}(\eta_i)$。为了实现对最优值函数的有效近似，基于式(35)构造近似性能指标函数为

$$\mathcal{J}_i(t)=\frac{\zeta_i^2(t)}{2(1+\boldsymbol{\varrho}_i^{\mathrm{T}}(t)\boldsymbol{\varrho}_i(t))^2} \tag{36}$$

基于式(36)采用梯度下降法更新自适应权重向量，写为

$$\dot{\bar{\boldsymbol{W}}}(t)=-\frac{k\varrho_i(t)\zeta_i(t)}{(1+\boldsymbol{\varrho}_i^{\mathrm{T}}(t)\boldsymbol{\varrho}_i(t))^2} \tag{37}$$

其中，$k>0$是用于调整更新速度的学习率。此外，定义权重误差为$\tilde{\boldsymbol{W}}(t)=\boldsymbol{W}-\bar{\boldsymbol{W}}(t)$，进一步推导可得

$$\dot{\tilde{\boldsymbol{W}}}(t)=-\frac{k\boldsymbol{\varrho}_i(t)\boldsymbol{\varrho}_i^{\mathrm{T}}(t)}{(1+\boldsymbol{\varrho}_i^{\mathrm{T}}(t)\boldsymbol{\varrho}_i(t))^2}\tilde{\boldsymbol{W}}(t)+\frac{k\boldsymbol{\varrho}_i(t)}{(1+\boldsymbol{\varrho}_i^{\mathrm{T}}(t)\boldsymbol{\varrho}_i(t))^2}\bar{\boldsymbol{\epsilon}}_i(t) \tag{38}$$

其中，$\bar{\boldsymbol{\epsilon}}_i(t)=-\boldsymbol{\epsilon}_\eta^{\mathrm{T}}\dot{\eta}_i(t)+\kappa\boldsymbol{\epsilon}(\eta_i)$。

为了实现下文的稳定性分析，引入以下假设。

假设1：最优值函数及其关于状态的偏导数满足$\|V^*(\eta_i)\|\le\tilde{V}$和$\|\boldsymbol{V}_\eta^*\|\le\tilde{V}_\eta$，其中$\tilde{V},\tilde{V}_\eta>0$为常数。

假设2：基函数与近似误差关于状态的偏导数满足$\|\boldsymbol{\varphi}_\eta\|\le\tilde{\varphi}_\eta$和$\|\epsilon_\eta\|\le\tilde{\epsilon}_\eta$，其中$\tilde{\varphi}_\eta,\tilde{\epsilon}_\eta>0$为常数。

假设3：权重误差动态中的残差项满足$\|\bar{\epsilon}_i(t)\|\le\tilde{\epsilon}_i$，其中$\tilde{\epsilon}_i>0$为常数。

3.4 稳定性分析

定理1　考虑估计误差系统式(8)、式(16)、式(17)、式(18)，以及融合权重矩阵式(13)，包含估计误差$\boldsymbol{e}_{ij}(t)$, $\hat{\boldsymbol{e}}_i(t)$, $\hat{\boldsymbol{e}}_j(t)$, $\tilde{\boldsymbol{z}}_j(t)$的估计误差系统是一致最终有界(Uniformly Ultimately Bounded, UUB)的以及融合估计误差$\boldsymbol{\rho}_i(t)$是有界的，若存在增益矩阵$\boldsymbol{K}_i$, $\boldsymbol{K}_j$，使得如式(39)的条件成立

$$\left.\begin{aligned}&\lambda_A<-\frac{5}{2}\\&\lambda_i<-1-\frac{1}{2}\|\boldsymbol{K}_i\boldsymbol{C}_i\|^2-\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\\&\lambda_j<-\frac{3}{2}-\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\end{aligned}\right\} \tag{39}$$

其中，$\lambda_A=\lambda_{\max}(\mathrm{sym}(\boldsymbol{A}))$, $\lambda_i=\lambda_{\max}(\mathrm{sym}(\boldsymbol{A}-\boldsymbol{K}_i\boldsymbol{C}_i))$, $\lambda_j=\lambda_{\max}(\mathrm{sym}(\boldsymbol{A}-\boldsymbol{K}_j\boldsymbol{C}_j))$。

证明 构造李雅普诺夫函数为

$$L_1=\frac{1}{2}(\boldsymbol{e}_{ij}^{\mathrm{T}}(t)\boldsymbol{e}_{ij}(t)+\hat{\boldsymbol{e}}_i^{\mathrm{T}}(t)\hat{\boldsymbol{e}}_i(t)+\hat{\boldsymbol{e}}_j^{\mathrm{T}}(t)\hat{\boldsymbol{e}}_j(t)+\tilde{\boldsymbol{z}}_j^{\mathrm{T}}(t)\tilde{\boldsymbol{z}}_j(t)) \tag{40}$$

对$L_1(t)$求导可得

$$\begin{aligned}\dot{L}_1=&\boldsymbol{e}_{ij}^{\mathrm{T}}(t)\boldsymbol{A}\boldsymbol{e}_{ij}(t)+\hat{\boldsymbol{e}}_i^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{K}_i\boldsymbol{C}_i)\hat{\boldsymbol{e}}_i(t)\\&+\hat{\boldsymbol{e}}_j^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{K}_j\boldsymbol{C}_j)\hat{\boldsymbol{e}}_j(t)+\tilde{\boldsymbol{z}}_j^{\mathrm{T}}(t)(\boldsymbol{A}-\boldsymbol{K}_j\boldsymbol{C}_j)\\&\cdot\tilde{\boldsymbol{z}}_j(t)+\boldsymbol{e}_{ij}^{\mathrm{T}}(t)\boldsymbol{K}_i\boldsymbol{C}_i\hat{\boldsymbol{e}}_i(t)-\boldsymbol{e}_{ij}^{\mathrm{T}}(t)\boldsymbol{K}_j\boldsymbol{C}_j\hat{\boldsymbol{e}}_j(t)\\&+\tilde{\boldsymbol{z}}_j^{\mathrm{T}}(t)\boldsymbol{K}_j\boldsymbol{C}_j\hat{\boldsymbol{e}}_i(t)+\boldsymbol{e}_{ij}^{\mathrm{T}}(t)\boldsymbol{K}_j\boldsymbol{C}_j\tilde{\boldsymbol{z}}_j(t)+\hat{\boldsymbol{e}}_j^{\mathrm{T}}(t)\\&\cdot\boldsymbol{K}_j\boldsymbol{C}_j\tilde{\boldsymbol{z}}_j(t)-\boldsymbol{e}_{ij}^{\mathrm{T}}(t)(\boldsymbol{K}_i\boldsymbol{v}_i(t)+2\boldsymbol{K}_j\boldsymbol{v}_j(t))\\&+\hat{\boldsymbol{e}}_i^{\mathrm{T}}(t)(\boldsymbol{w}(t)-\boldsymbol{K}_i\boldsymbol{v}_i(t))+\hat{\boldsymbol{e}}_j^{\mathrm{T}}(t)(\boldsymbol{w}(t)\\&-2\boldsymbol{K}_j\boldsymbol{v}_j(t))+\tilde{\boldsymbol{z}}_j^{\mathrm{T}}(t)\boldsymbol{w}(t)\end{aligned} \tag{41}$$

根据杨氏不等式[8]可得

$$\boldsymbol{e}_{ij}^{\mathrm{T}}\boldsymbol{K}_i\boldsymbol{C}_i\widehat{\boldsymbol{e}}_i\le\frac{1}{2}\|\boldsymbol{e}_{ij}\|^2+\frac{1}{2}\|\boldsymbol{K}_i\boldsymbol{C}_i\|^2\|\widehat{\boldsymbol{e}}_i\|^2 \tag{42}$$

$$-\boldsymbol{e}_{ij}^{\mathrm{T}}\boldsymbol{K}_j\boldsymbol{C}_j\widehat{\boldsymbol{e}}_j\le\frac{1}{2}\|\boldsymbol{e}_{ij}\|^2+\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\|\widehat{\boldsymbol{e}}_j\|^2 \tag{43}$$

$$\tilde{\boldsymbol{z}}_j^{\mathrm{T}}\boldsymbol{K}_j\boldsymbol{C}_j\widehat{\boldsymbol{e}}_i\le\frac{1}{2}\|\tilde{\boldsymbol{z}}_j\|^2+\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\|\widehat{\boldsymbol{e}}_i\|^2 \tag{44}$$

$$\boldsymbol{e}_{ij}^{\mathrm{T}}\boldsymbol{K}_j\boldsymbol{C}_j\tilde{\boldsymbol{z}}_j\le\frac{1}{2}\|\boldsymbol{e}_{ij}\|^2+\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\|\tilde{\boldsymbol{z}}_j\|^2 \tag{45}$$

$$\hat{\boldsymbol{e}}_j^{\mathrm{T}}(t)\boldsymbol{K}_j\boldsymbol{C}_j\tilde{\boldsymbol{z}}_j(t)\le\frac{1}{2}\|\widehat{\boldsymbol{e}}_j\|^2+\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2\|\tilde{\boldsymbol{z}}_j\|^2 \tag{46}$$

进一步可得

$$\begin{aligned}&-\boldsymbol{e}_{ij}^{\mathrm{T}}(\boldsymbol{K}_i\boldsymbol{v}_i+2\boldsymbol{K}_j\boldsymbol{v}_j)\le\|\boldsymbol{e}_{ij}\|^2+\frac{1}{2}\|\boldsymbol{K}_i\|^2\|\boldsymbol{v}_i\|^2\\&+2\|\boldsymbol{K}_j\|^2\|\boldsymbol{v}_j\|^2\end{aligned} \tag{47}$$

$$\hat{\boldsymbol{e}}_i^{\mathrm{T}}(\boldsymbol{w}-\boldsymbol{K}_i\boldsymbol{v}_i)\le\|\widehat{\boldsymbol{e}}_i\|^2+\frac{1}{2}\|\boldsymbol{w}\|^2+\frac{1}{2}\|\boldsymbol{K}_i\|^2\|\boldsymbol{v}_i\|^2 \tag{48}$$

$$\hat{\boldsymbol{e}}_j^{\mathrm{T}}(\boldsymbol{w}-2\boldsymbol{K}_j\boldsymbol{v}_j)\le\|\widehat{\boldsymbol{e}}_j\|^2+\frac{1}{2}\|\boldsymbol{w}\|^2+2\|\boldsymbol{K}_j\|^2\|\boldsymbol{v}_j\|^2 \tag{49}$$

$$\tilde{\boldsymbol{z}}_j^{\mathrm{T}}\boldsymbol{w}\le\frac{1}{2}\|\tilde{\boldsymbol{z}}_j\|^2+\frac{1}{2}\|\boldsymbol{w}\|^2 \tag{50}$$

将上述不等式代入式(41)可得

$$\begin{aligned}\dot{L}_1\le&-\sigma_1\|\boldsymbol{e}_{ij}(t)\|^2-\sigma_2\|\widehat{\boldsymbol{e}}_i(t)\|^2-\sigma_3\|\widehat{\boldsymbol{e}}_j(t)\|^2\\&-\sigma_4\|\tilde{\boldsymbol{z}}_j(t)\|^2+\Gamma(t)\end{aligned} \tag{51}$$

其中，

$$\sigma_1=-\lambda_A-\frac{5}{2},\sigma_2=-\lambda_i-1-\frac{1}{2}\|K_iC_i\|^2-\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2,$$

$$\sigma_3=-\lambda_j-\frac{3}{2}-\frac{1}{2}\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2,\sigma_4=-\lambda_j-1-\|\boldsymbol{K}_j\boldsymbol{C}_j\|^2,$$

$$\Gamma(t)=\frac{3}{2}\|\boldsymbol{w}(t)\|^2+\|\boldsymbol{K}_i\|^2\|\boldsymbol{v}_i(t)\|^2+4\|\boldsymbol{K}_j\|^2\|\boldsymbol{v}_j(t)\|^2。$$

进一步，式(51)可写为

$$\dot{L}_1(t)\le-\tilde{\sigma}L_1(t)+\Gamma(t) \tag{52}$$

其中，$\tilde{\sigma}=\min\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}>0$。由式(52)和Grönwall不等式[15]可得

$$L_1(t)\le L_1(0)\mathrm{e}^{-\tilde{\sigma}t}+\frac{1}{\tilde{\sigma}}\sup_{\tau\in[0,t]}\Gamma(\tau) \tag{53}$$

即估计误差系统是UUB的。此外，根据融合估计误差$\boldsymbol{\rho}_i(t)$的定义可将其重写为

$$\begin{aligned}\boldsymbol{\rho}_i(t)&=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\boldsymbol{x}(t)-\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\hat{\boldsymbol{x}}_j(t)\\&=\sum_{j\in\mathcal{N}_i}\boldsymbol{\Omega}_j(t)\hat{\boldsymbol{e}}_j(t)\end{aligned} \tag{54}$$

因此，融合估计误差$\boldsymbol{\rho}_i(t)$是有界的。

证毕

定理2 考虑近似最优控制输入式(32)和最差扰动策略式(33)，以及权重自适应更新律式(37)，若假设1~假设3成立，则增广状态系统式(21)以及权重误差系统式(38)是UUB的，前提是满足式(55)的条件

$$-\frac{\lambda_{\max}(\boldsymbol{R})}{2\lambda_{\min}^2(\boldsymbol{R})}\|\boldsymbol{\mathcal{B}}\|^2\tilde{\varphi}_\eta^2-\frac{1}{2\gamma_i^2}\|\boldsymbol{\mathcal{D}}_i\|^2\tilde{\varphi}_\eta^2+\frac{k}{2}\lambda_{\min}(\Lambda)>0 \tag{55}$$

其中，$\Lambda=\boldsymbol{\varrho}(t)\boldsymbol{\varrho}^{\mathrm{T}}(t)/(1+\boldsymbol{\varrho}^{\mathrm{T}}(t)\boldsymbol{\varrho}(t))^2$。

证明 定义李雅普诺夫函数为

$$L_2=V^*(\eta_i)+\frac{1}{2}\tilde{\boldsymbol{W}}^{\mathrm{T}}(t)\tilde{\boldsymbol{W}}(t) \tag{56}$$

对$V^*(\eta_i)$求导可得

$$\begin{aligned}\dot{V}^*(\eta_i)=&(\boldsymbol{V}_\eta^*)^{\mathrm{T}}(\mathcal{A}_i\eta_i(t)+\mathcal{B}\boldsymbol{u}^*(\eta_i)+\boldsymbol{\mathcal{D}}_i)\tilde{\boldsymbol{w}}^*(\eta_i))\\&+(\boldsymbol{V}_\eta^*)^{\mathrm{T}}\mathcal{B}(\bar{\boldsymbol{u}}(\eta_i)-\boldsymbol{u}^*(\eta_i))\\&+(\boldsymbol{V}_\eta^*)^{\mathrm{T}}\mathcal{D}_i(\bar{\boldsymbol{w}}(\eta_i)-\tilde{\boldsymbol{w}}^*(\eta_i))\end{aligned} \tag{57}$$

由于$V^*(\boldsymbol{z})$满足哈密顿函数最小化条件，即$H(V_{\boldsymbol{z}}^*,\boldsymbol{z},\boldsymbol{u}^*,\boldsymbol{\xi}^*)=0$，因此可得

$$\begin{aligned}&(\boldsymbol{V}_\eta^*)^{\mathrm{T}}(\boldsymbol{\mathcal{A}}_i(t)\eta_i(t)+\boldsymbol{\mathcal{B}}\boldsymbol{u}^*(\eta_i)+\boldsymbol{\mathcal{D}}_i\tilde{\boldsymbol{w}}^*(t,\eta))\\&=\kappa\boldsymbol{V}^*(\eta_i)-\eta_i^{\mathrm{T}}(t)\boldsymbol{P}_i\eta_i(t)-(\boldsymbol{u}^*(\eta_i))^{\mathrm{T}}\boldsymbol{R}\boldsymbol{u}^*(\eta_i)\\&\quad+\gamma_i^2(\tilde{\boldsymbol{w}}^*(\eta_i))^{\mathrm{T}}\tilde{\boldsymbol{w}}^*(\eta_i)\end{aligned} \tag{58}$$

由式(26)和式(27)推导可得

$$(\boldsymbol{V}_\eta^*)^{\mathrm{T}}\mathcal{B}=-2(\boldsymbol{u}^*(\eta_i))^{\mathrm{T}}\boldsymbol{R} \tag{59}$$

$$(\boldsymbol{V}_\eta^*)^{\mathrm{T}}\mathcal{D}_i=2\gamma_i^2(\tilde{\boldsymbol{w}}^*(\eta_i))^{\mathrm{T}} \tag{60}$$

将式(58)–式(60)代入式(57)可得

$$\begin{aligned}\dot{V}^*(\eta_i)=&\kappa V^*(\eta_i)-\eta_i^{\mathrm{T}}(t)\boldsymbol{P}_i\eta_i(t)-(\boldsymbol{u}^*(\eta_i))^{\mathrm{T}}\boldsymbol{R}\boldsymbol{u}^*(\eta_i)\\&+\gamma_i^2(\tilde{\boldsymbol{w}}^*(\eta_i))^{\mathrm{T}}\tilde{\boldsymbol{w}}^*(\eta_i)\\&+2(\boldsymbol{u}^*(\eta_i))^{\mathrm{T}}\boldsymbol{R}(\boldsymbol{u}^*(\eta_i)-\bar{\boldsymbol{u}}(\eta_i))\\&+2\gamma_i^2(\tilde{\boldsymbol{w}}^*(\eta_i))^{\mathrm{T}}(\bar{\boldsymbol{w}}(\eta_i)-\tilde{\boldsymbol{w}}^*(\eta_i))\end{aligned} \tag{61}$$

结合假设1以及矩阵范数的性质对式(61)进行放缩可得

$$\begin{aligned}\dot{V}^*(\eta_i) \leq\ & \kappa\tilde{V}-\lambda_{\min}(\boldsymbol{P}_i)\|\eta_i(t)\|^2+2\gamma_i^2\|\tilde{\boldsymbol{w}}^*(\eta_i)\|^2\\ &+\lambda_{\max}(\boldsymbol{R})\|u^*(\eta_i)-\overline{\boldsymbol{u}}(\eta_i)\|^2\\ &+\gamma_i^2\|\overline{\boldsymbol{w}}(\eta_i)-\tilde{\boldsymbol{w}}^*(\eta_i)\|^2\end{aligned}\tag{62}$$

根据假设2、式(26)和式(32)推导可得

$$\|\boldsymbol{u}^*(\eta_i)-\overline{\boldsymbol{u}}(\eta_i)\|^2\leq\frac{1}{2\lambda_{\min}^2(\boldsymbol{R})}\|\mathcal{B}\|^2(\tilde{\varphi}_\eta^2\|\tilde{\boldsymbol{W}}(t)\|^2+\tilde{\epsilon}_\eta^2)\tag{63}$$

根据假设2、式(27)和式(33)推导可得

$$\|\overline{\boldsymbol{w}}(\eta_i)-\tilde{\boldsymbol{w}}^*(\eta_i)\|^2\leq\frac{1}{2\gamma_i^4}\|\mathcal{D}_i\|^2(\tilde{\varphi}_\eta^2\|\tilde{\boldsymbol{W}}(t)\|^2+\tilde{\epsilon}_\eta^2)\tag{64}$$

此外，由式(27)推导可得

$$\|\tilde{\boldsymbol{w}}^*(\eta_i)\|^2=\|\frac{1}{2\gamma_i^2}\mathcal{D}_i^{\mathrm{T}}V_\eta^*\|^2\leq\frac{1}{4\gamma_i^4}\|\mathcal{D}_i\|^2\tilde{V}_\eta^2\tag{65}$$

将式(63)–式(65)代入式(62)可得

$$\begin{aligned}\dot{V}^*(\eta_i)\leq\ & \kappa\tilde{V}-\lambda_{\min}(\boldsymbol{P}_i)\|\eta_i(t)\|^2+\frac{1}{2\gamma_i^2}\|\mathcal{D}_i\|^2\tilde{V}_\eta^2\\ &+\frac{\lambda_{\max}(\boldsymbol{R})}{2\lambda_{\min}^2(\boldsymbol{R})}\|\mathcal{B}\|^2(\tilde{\varphi}_\eta^2\|\tilde{\boldsymbol{W}}(t)\|^2+\tilde{\epsilon}_\eta^2)\\ &+\frac{1}{2\gamma_i^2}\|\mathcal{D}_i\|^2(\tilde{\varphi}_\eta^2\|\tilde{\boldsymbol{W}}(t)\|^2+\tilde{\epsilon}_\eta^2)\end{aligned}\tag{66}$$

对式(56)中权重误差项求导可得

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{1}{2}\tilde{\boldsymbol{W}}^{\mathrm{T}}(t)\tilde{\boldsymbol{W}}(t)\right)=\ & -\tilde{\boldsymbol{W}}^{\mathrm{T}}(t)\frac{k\boldsymbol{\varrho}(t)\boldsymbol{\varrho}^{\mathrm{T}}(t)}{\left(1+\boldsymbol{\varrho}^{\mathrm{T}}(t)\boldsymbol{\varrho}(t)\right)^2}\tilde{\boldsymbol{W}}(t)\\ &+\tilde{\boldsymbol{W}}^{\mathrm{T}}(t)\frac{k\boldsymbol{\varrho}(t)}{\left(1+\boldsymbol{\varrho}^{\mathrm{T}}(t)\boldsymbol{\varrho}(t)\right)^2}\overline{\boldsymbol{\epsilon}}_i(t)\end{aligned}\tag{67}$$

由假设3和式(67)推导可得

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{1}{2}\tilde{\boldsymbol{W}}^{\mathrm{T}}(t)\tilde{\boldsymbol{W}}(t)\right)\leq-\frac{k}{2}\lambda_{\min}(\Lambda)\|\tilde{\boldsymbol{W}}(t)\|^2+\frac{k}{2}\tilde{\epsilon}_i^2\tag{68}$$

结合式(66)与式(68)可得

$$\dot{L}_2\leq-\lambda_{\min}(\boldsymbol{P}_i)\|\eta_i(t)\|^2-\Phi_1\|\tilde{\boldsymbol{W}}(t)\|^2+\Phi_2\tag{69}$$

其中，

$$\Phi_1=-\frac{\lambda_{\max}(\boldsymbol{R})}{2\lambda_{\min}^2(\boldsymbol{R})}\|\mathcal{B}\|^2\tilde{\varphi}_\eta^2-\frac{1}{2\gamma_i^2}\|\mathcal{D}_i\|^2\tilde{\varphi}_\eta^2+\frac{k}{2}\lambda_{\min}(\Lambda)$$

$$\begin{aligned}\Phi_2=\ & \kappa\tilde{V}+\frac{1}{2\gamma_i^2}\|\mathcal{D}_i\|^2\tilde{V}_\eta^2+\frac{\lambda_{\max}(\boldsymbol{R})}{2\lambda_{\min}^2(\boldsymbol{R})}\|\mathcal{B}\|^2\tilde{\epsilon}_\eta^2\\ &+\frac{1}{2\gamma_i^2}\|\mathcal{D}_i\|^2\tilde{\epsilon}_\eta^2+\frac{k}{2}\tilde{\epsilon}_i^2\end{aligned}$$

由式(69)以及Grönwall不等式[15]推导可得

$$L_2(t)\leq L_2(0)\mathrm{e}^{-\Phi_3 t}+\frac{\Phi_2}{\Phi_3}\left(1-\mathrm{e}^{-\Phi_3 t}\right)\tag{70}$$

其中，$\Phi_3=\min\{\lambda_{\min}(\boldsymbol{P}_i),\Phi_1\}$。由式(70)可知，增广状态系统以及权重误差系统是UUB的。

证毕

4　仿真实验

为验证所提出的安全学习控制框架在受到虚假数据攻击时的有效性与鲁棒性，本文选取了一类基于超声速运输机的横向-方向通道动力学系统进行仿真实验[3]。系统状态向量$\boldsymbol{x}(t)=[\boldsymbol{x}^1(t),\boldsymbol{x}^2(t),\boldsymbol{x}^3(t),\boldsymbol{x}^4(t)]^{\mathrm{T}}$由4个关键的飞行参数组成，包括侧滑角$\boldsymbol{x}^1(t)$、横滚角$\boldsymbol{x}^2(t)$、横滚角速率$\boldsymbol{x}^3(t)$以及偏航角速率$\boldsymbol{x}^4(t)$。系统的控制输入为$\boldsymbol{u}(t)=[\boldsymbol{u}^1(t),\boldsymbol{u}^2(t)]^{\mathrm{T}}$，其中$\boldsymbol{u}^1(t)$和$\boldsymbol{u}^2(t)$分别代表副翼与方向舵的偏转角，用于调整飞行器的方向和滚转姿态。该系统的状态空间模型写为

$$\begin{aligned}&\begin{bmatrix}\dot{\boldsymbol{x}}^1(t)\\ \dot{\boldsymbol{x}}^2(t)\\ \dot{\boldsymbol{x}}^3(t)\\ \dot{\boldsymbol{x}}^4(t)\end{bmatrix}\\ &=\begin{bmatrix}-0.037 & 0.012\,3 & 0.000\,55 & -1.0\\ 0 & 0 & 1.0 & 0\\ -6.37 & 0 & -0.23 & 0.061\,8\\ 1.25 & 0 & 0.016 & -0.045\,7\end{bmatrix}\\ &\quad\cdot\begin{bmatrix}\boldsymbol{x}^1(t)\\ \boldsymbol{x}^2(t)\\ \boldsymbol{x}^3(t)\\ \boldsymbol{x}^4(t)\end{bmatrix}+\begin{bmatrix}0.000\,84 & 0.000\,236\\ 0 & 0\\ 0.08 & 0.804\\ -0.086\,2 & -0.066\,5\end{bmatrix}\\ &\quad\cdot\begin{bmatrix}\boldsymbol{u}^1(t)\\ \boldsymbol{u}^2(t)\end{bmatrix}\end{aligned}\tag{71}$$

该系统中同时配备了$N=6$组传感器，每组传感器分别用于测量系统的部分状态变量。第一组传感器i被指定为本地传感器节点，其余传感器$j\in\mathcal{N}_i$为通过网络向本地传感器节点发送观测数据的远程传感器。传感器的观测矩阵$\boldsymbol{C}_i$和$\boldsymbol{C}_j$写为

$$\boldsymbol{C}_1=\begin{bmatrix}1&0&0&0\\0&1&0&0\end{bmatrix},\ \boldsymbol{C}_2=\begin{bmatrix}1&0&0&0\\0&0&1&0\end{bmatrix},$$

$$\boldsymbol{C}_3=\begin{bmatrix}1&0&0&0\\0&0&0&1\end{bmatrix},\ \boldsymbol{C}_4=\begin{bmatrix}0&1&0&0\\0&0&1&0\end{bmatrix},$$

$$\boldsymbol{C}_5=\begin{bmatrix}0&1&0&0\\0&0&0&1\end{bmatrix},\ \boldsymbol{C}_6=\begin{bmatrix}0&0&1&0\\0&0&0&1\end{bmatrix}$$

攻击者向传感器通信网络中注入的攻击信号设置为

$$\boldsymbol{\xi}_j(t)=\begin{bmatrix}1.2\cos(0.8t)+0.8\cos(2.1t)\sin(t)\\ 0.9\sin(1.2t)+1.1\cos(t)\sin(1.7t)\end{bmatrix}$$

与本地传感器节点i通信的第2, 3, 4, 5组远程传感器分别在[30, 35] s, [36, 41] s, [38, 43] s, [55, 60] s的时间段内发生了虚假数据攻击。估计系统的增益矩阵设计为

$$\boldsymbol{K}_1=\begin{bmatrix}1.06&-0.52\\-0.52&3.17\\-2.71&4.65\\-0.25&-0.43\end{bmatrix},\ \boldsymbol{K}_2=\begin{bmatrix}0.69&-1.04\\1.05&0.05\\-1.04&3.41\\-0.30&0.12\end{bmatrix},$$

$$\boldsymbol{K}_3=\begin{bmatrix}0.97&0.11\\10.09&10.20\\-2.25&-1.87\\0.11&1.06\end{bmatrix},\ \boldsymbol{K}_4=\begin{bmatrix}-0.10&-1.27\\1.40&0.82\\0.82&3.84\\-0.06&0.19\end{bmatrix},$$

$$\boldsymbol{K}_5=\begin{bmatrix}-0.84&0.09\\3.58&-0.51\\6.06&-1.39\\-0.51&0.91\end{bmatrix},\ \boldsymbol{K}_6=\begin{bmatrix}-1.08&-0.11\\-0.14&0.83\\3.62&-0.12\\-0.12&0.80\end{bmatrix}$$

值函数中的权重矩阵设置为$\boldsymbol{P}_i=\mathrm{diag}\{1,0.5,0.9,1,1,0.5,0.9,1\}$，$\boldsymbol{R}=0.09\boldsymbol{I}_2$，$\gamma_i=1.2$，时间衰减因子为$\kappa=1$。自适应权重更新的学习率为$k=1$。系统初始状态为$\boldsymbol{x}(0)=[0.12,0.18,0.12,0.2]^{\mathrm{T}}$。

仿真实验的结果如图1–图6所示。图1展示了在多组传感器遭受虚假数据攻击的条件下，系统状态的动态响应情况。可以观察到，在所提出自适应学习控制算法的作用下，各状态变量均在有限时间内收敛至非常小的稳定区间内，系统实现安全稳定运行。该结果表明，本文设计的控制方法在面对攻击干扰时，仍具备良好的稳定性与控制性能。

图2给出了融合状态估计$\tilde{\boldsymbol{x}}_1^1(t)$、本地状态估计$\hat{\boldsymbol{x}}_1^1(t)$与系统真实状态$\boldsymbol{x}^1(t)$的对比情况。从图中可以看出，融合估计的侧滑角$\tilde{\boldsymbol{x}}_1^1(t)$、本地估计的测滑角$\hat{\boldsymbol{x}}_1^1(t)$与真实的测滑角$\boldsymbol{x}^1(t)$误差非常小，说明本文提出的融合估计方法在传感器遭受攻击干扰的情况下，仍能准确重构系统的真实状态。

图3展示了真实的侧滑角观测值$\boldsymbol{y}_2^1(t)$、侧滑角观测估计值$\hat{\boldsymbol{y}}_2^1(t)$以及攻击后的侧滑角观测值$\bar{\boldsymbol{y}}_2^1(t)$。实验结果表明，经攻击估计器补偿后的侧滑角观测估计值$\hat{\boldsymbol{y}}_2^1(t)$与原始真实的侧滑角观测值$\boldsymbol{y}_2^1(t)$高度重合，表明该方法能有效抑制虚假数据攻击对观测数据的影响，确保观测数据的可靠性。

图4为远程传感器攻击检测指标$H_j(t)$随时间变化的结果。可以看到，第2～5组传感器的检测指标在攻击发生时迅速上升，而第6组未遭受攻击的传感器检测指标始终保持在零值附近。上述结果验证了所构建的攻击检测机制能够有效检测是否存在虚假数据攻击以及定位受攻击的传感器节点。图5进一步展示了攻击信号与其估计值的动态演化过程。从图中可见，所设计的攻击估计方法能够较准确地跟踪攻击信号的变化趋势，为后续的观测修正与控制策略调整提供了支持。

为进一步验证本文方法的优越性，本文选取文献[15]中提出的控制策略作为对比方案，并在相同的虚假数据攻击环境下进行了对比实验。文献[15]中采用容错控制机制，通过提升系统的鲁棒性以缓

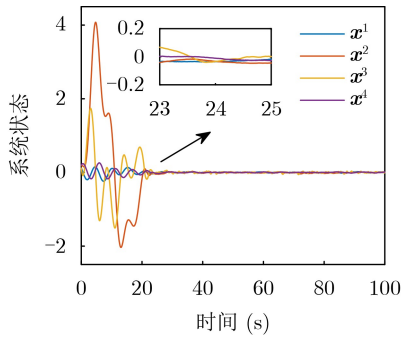

图 1 虚假数据攻击下的系统状态响应

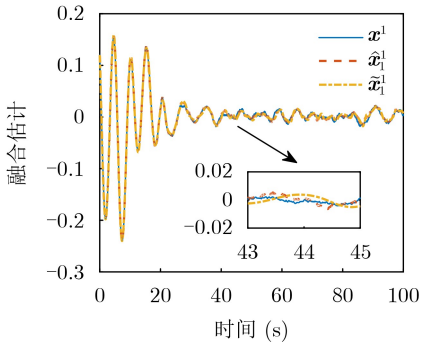

图 2 融合状态估计与真实系统状态的对比

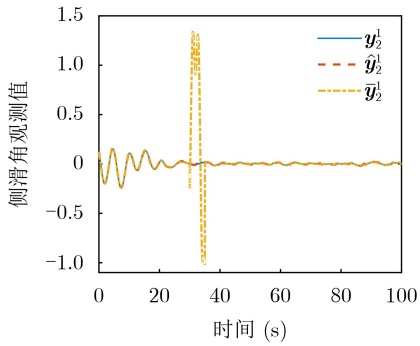

图 3 攻击前后观测值以及观测估计值的对比

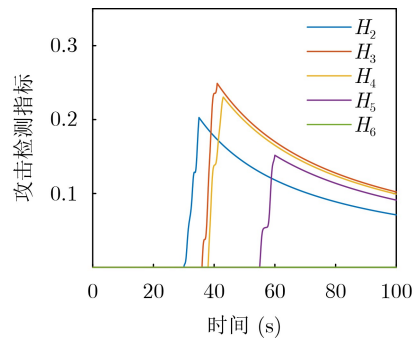

图 4 远程观测数据的攻击检测指标

解攻击带来的影响，本文方法则引入攻击信号估计器对被攻击的观测值进行补偿，从而减少攻击信号对控制策略的影响。实验结果如图6所示，在相同攻击条件下，采用文献[15]中的控制方法时，侧滑角$\boldsymbol{x}^1(t)$与横滚角速率$\boldsymbol{x}^3(t)$在攻击发生后出现较大幅度的扰动，最大偏差显著高于本文方法，且恢复至稳定状态所需时间更长。而采用本文提出的攻击检测与补偿机制后，系统状态扰动幅度明显减小，收敛速度更快，表现出更强的稳态性能与抗攻击能力。综上所述，各项实验结果充分验证了本文所提出的攻击检测、融合状态估计与自适应学习的安全控制方法，在面对复杂攻击环境时具备良好的稳定性、鲁棒性与控制性能。

5　结束语

本文围绕CPS在遭受虚假数据注入攻击情况下的安全感知与控制问题，构建了一套集检测、估计与控制于一体的自适应学习控制方法框架。通过引入面向传感器数据安全性的虚假数据检测机制，有效增强了系统对攻击信号的识别能力，基于多源融合的状态估计方法也进一步提升了系统对真实状态的观测准确性。在控制层面，设计了权重在线更新的自适应学习控制器，实现了在无先验攻击信息下对最优控制策略的逐步逼近。未来研究可进一步将自适应学习控制方法拓展至CPS的多种应用场景，并系统探讨其在不同网络攻击环境下的防御策略。

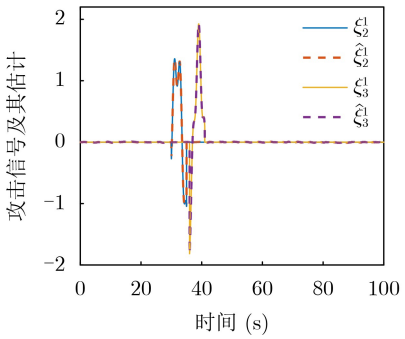

图 5 虚假数据攻击信号及其估计值

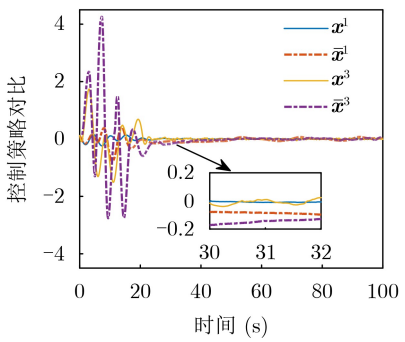

图 6 不同控制策略下的系统状态响应对比

参 考 文 献

[1] YU Rongrong, ZHAO Xu, LU Si, *et al*. Intelligent game-theoretic approach for resilient robust control design of cyber-physical systems: Application to intelligent transportation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(11): 16072–16083. doi: 10.1109/TITS.2024.3407721.

[2] 杨挺, 刘亚闯, 刘宇哲, 等. 信息物理系统技术现状分析与趋势综述[J]. 电子与信息学报, 2021, 43(12): 3393–3406. doi: 10.11999/JEIT211135.

YANG Ting, LIU Yachuang, LIU Yuzhe, *et al*. Review on cyber-physical system: Technology analysis and trends[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3393–3406. doi: 10.11999/JEIT211135.

[3] ZHOU Yuanqiang, VAMVOUDAKIS K G, HADDAD W M, *et al*. A secure control learning framework for cyber-physical systems under sensor and actuator attacks[J]. IEEE Transactions on Cybernetics, 2021, 51(9): 4648–4660. doi: 10.1109/TCYB.2020.3006871.

[4] 张志鹏, 许倩, 夏承遗. 基于矩阵半张量积的信息物理融合系统状态不透明性分析与控制[J]. 电子与信息学报, 2021, 43(12): 3434–3441. doi: 10.11999/JEIT210492.

ZHANG Zhipeng, XU Qian, and XIA Chengyi. Semi-tensor product of matrices-based approach to the opacity analysis of cyber physical systems[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3434–3441. doi: 10.11999/JEIT210492.

[5] 金增旺, 刘茵, 刁靖东, 等. 针对信息物理系统远程状态估计的隐蔽虚假数据注入攻击[J]. 自动化学报, 2025, 51(2): 356–365. doi: 10.16383/j.aas.c240527.

JIN Zengwang, LIU Yin, DIAO Jingdong, *et al*. Stealthy false data injection attacks on remote state estimation of cyber-physical systems[J]. Acta Automatica Sinica, 2025, 51(2): 356–365. doi: 10.16383/j.aas.c240527.

[6] WANG Zhe, ZHANG Heng, YANG Chaoqun, *et al*. Improved zero-dynamics attack scheduling with state estimation[J]. IEEE/CAA Journal of Automatica Sinica, 2025, 12(2): 472–474. doi: 10.1109/JAS.2024.124737.

[7] ZHU Panpan, JIN Shangtai, BU Xuhui, *et al*. Model-free adaptive control for a class of MIMO nonlinear cyberphysical systems under false data injection attacks[J]. IEEE Transactions on Control of Network Systems, 2023, 10(1): 467–478. doi: 10.1109/TCNS.2022.3203354.

[8] GAO Yang, MA Jiali, WANG Jiaqi, *et al*. Event-triggered adaptive fixed-time secure control for nonlinear cyber-physical system with false data-injection attacks[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70(1): 316–320. doi: 10.1109/TCSII.2022.3217823.

[9] LIU Yifa, CHENG Long, and YE Dan. Stealthy false data

injection attacks against the summation detector in cyber-physical systems[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024, 2: 391–403. doi: 10.1109/TICPS.2024.3446469.

[10] GUIBENE K, MESSAI N, AYAIDA M, *et al*. A pattern mining-based false data injection attack detector for industrial cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 2969–2978. doi: 10.1109/TII.2023.3297139.

[11] ZHANG Qiang and HE Dakuo. Adaptive neural control of nonlinear cyber–physical systems against randomly occurring false data injection attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2023, 53(4): 2444–2455. doi: 10.1109/TSMC.2022.3212391.

[12] LI Tongxiang, CHEN Bo, LIU Shichao, *et al*. Fast attack detection for cyber–physical systems using dynamic data encryption[J]. IEEE Transactions on Cybernetics, 2024, 54(5): 3251–3264. doi: 10.1109/TCYB.2023.3332079.

[13] REN Yan, ZHANG Heng, YANG Wen, *et al*. Transferable adversarial attack against deep reinforcement learning-based smart grid dynamic pricing system[J]. IEEE Transactions on Industrial Informatics, 2024, 20(6): 9015–9025. doi: 10.1109/TII.2024.3379645.

[14] SOLEIMANI E, SEDIGH A K, and NIKOOFARD A. Data-driven reinforcement learning-based forgetting factor iterative learning control[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 12245–12256. doi: 10.1109/TASE.2025.3540699.

[15] FEI Cheng, SHEN Jun, QIU Hongling, *et al*. Learning secure control design for cyber-physical systems under false data injection attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024, 2: 60–68. doi: 10.1109/TICPS.2024.3373715.

[16] LI Jinyan, LI Xiaomeng, CHEN Guangdeng, *et al*. Optimal tracking control for cyber-physical systems under mixed attacks via game-theoretical Q-learning[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 11944–11954. doi: 10.1109/TASE.2025.3540401.

[17] LI Xiaohang, CHADLI M, TIAN Zhaoyang, *et al*. Resilient-learning control of cyber-physical systems against mixed-type network attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2024, 54(9): 5692–5703. doi: 10.1109/TSMC.2024.3408413.

[18] SHEN Hao, WANG Yun, WU Jiacheng, *et al*. Secure control for Markov jump cyber-physical systems subject to malicious attacks: A resilient hybrid learning scheme[J]. IEEE Transactions on Cybernetics, 2024, 54(11): 7068–7079. doi: 10.1109/TCYB.2024.3448407.

[19] REN Hongru, LONG Yinren, LI Hongyi, *et al*. Data-driven group formation control of cyber-physical systems via distributed cloud computing[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2025, 3: 341–350. doi: 10.1109/TICPS.2025.3561726.

[20] SUO Yuhan, CHAI Runqi, CHAI Senchun, *et al*. Attack detection and secure state estimation of collectively observable cyber-physical systems under false data injection attacks[J]. IEEE Transactions on Automatic Control, 2024, 69(3): 2067–2074. doi: 10.1109/TAC.2023.3316160.

苗金钊：男，博士生，研究方向为网络安全、无人系统和智能控制.

刘金良：男，教授，研究方向为强化学习、网络化系统优化、网络安全和隐私保护.

孙　乐：女，教授，研究方向为数据挖掘、深度学习、云计算和服务计算.

查利娟：女，教授，研究方向为最优化控制、数据驱动、智能控制和网络化系统.

田恩刚：男，教授，研究方向为网络控制系统、网络攻击、非线性随机控制和数据驱动.

责任编辑：廖海贝

A Learning-Based Security Control Method for Cyber-Physical Systems Based on False Data Detection

MIAO Jinzhao[①]　LIU Jinliang[①]　SUN Le[①]　ZHA Lijuan[②]　TIAN Engang[③]

[①](*School of Computer Science, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*)

[②](*College of Science, Nanjing Forestry University, Nanjing* 200037, *China*)

[③](*School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

Abstract:

Objective　Cyber-Physical Systems (CPS) constitute the backbone of critical infrastructures and industrial

applications, but the tight coupling of cyber and physical components renders them highly susceptible to cyberattacks. False data injection attacks are particularly dangerous because they compromise sensor integrity, mislead controllers, and can trigger severe system failures. Existing control strategies often assume reliable sensor data and lack resilience under adversarial conditions. Furthermore, most conventional approaches decouple attack detection from control adaptation, leading to delayed or ineffective responses to dynamic threats. To overcome these limitations, this study develops a unified secure learning control framework that integrates real-time attack detection with adaptive control policy learning. By enabling the dynamic identification and mitigation of false data injection attacks, the proposed method enhances both stability and performance of CPS under uncertain and adversarial environments.

Methods　To address false data injection attacks in CPS, this study proposes an integrated secure control framework that combines attack detection, state estimation, and adaptive control strategy learning. A sensor grouping-based security assessment index is first developed to detect anomalous sensor data in real time without requiring prior knowledge of attacks. Next, a multi-source sensor fusion estimation method is introduced to reconstruct the system's true state, thereby improving accuracy and robustness under adversarial disturbances. Finally, an adaptive learning control algorithm is designed, in which dynamic weight updating via gradient descent approximates the optimal control policy online. This unified framework enhances both steady-state performance and resilience of CPS against sophisticated attack scenarios. Its effectiveness and security performance are validated through simulation studies under diverse false data injection attack settings.

Results and Discussions　Simulation results confirm the effectiveness of the proposed secure adaptive learning control framework under multiple false data injection attacks in CPS. As shown in Fig. 1, system states rapidly converge to steady values and maintain stability despite sensor attacks. Fig. 2 demonstrates that the fused state estimator tracks the true system state with greater accuracy than individual local estimators. In Fig. 3, the compensated observation outputs align closely with the original, uncorrupted measurements, indicating precise attack estimation. Fig. 4 shows that detection indicators for sensor groups 2–5 increase sharply during attack intervals, while unaffected sensors remain near zero, verifying timely and accurate detection. Fig. 5 further confirms that the estimated attack signals closely match the true injected values. Finally, Fig. 6 compares different control strategies, showing that the proposed method achieves faster stabilization and smaller state deviations. Together, these results demonstrate robust control, accurate state estimation, and real-time detection under unknown attack conditions.

Conclusions　This study addresses secure perception and control in CPS under false data injection attacks by developing an integrated adaptive learning control framework that unifies detection, estimation, and control. A sensor-level anomaly detection mechanism is introduced to identify and localize malicious data, substantially enhancing attack detection capability. The fusion-based state estimation method further improves reconstruction accuracy of true system states, even when observations are compromised. At the control level, an adaptive learning controller with online weight adjustment enables real-time approximation of the optimal control policy without requiring prior knowledge of the attack model. Future research will extend the proposed framework to broader application scenarios and evaluate its resilience under diverse attack environments.

Key words: Cyber-Physical Systems (CPS); False data detection; Secure control; Network attacks