DOI:10.13878/j.cnki.jnuist.20220513001

赖琛[1] 郑柏超[1,2] 陈志鹏[1] 王海凤[1]

虚假数据注入攻击下基于扩张观测器的滑模控制研究

摘要

针对虚假数据注入(FDI)攻击下的信息物理系统(CPS),研究了一种基于滑模和扩张观测器的控制方法.首先对系统进行动态线性化,构造了扩张观测器并对观测误差的收敛条件进行了分析.其次,设计了积分滑模面,通过线性矩阵不等式的形式导出滑动模态系统的渐近稳定判据,求出了系统满足 L_2 增益性能的滑模向量.接着,基于指数趋近律,提出了用来消除量化误差和广义干扰的自适应积分滑模控制器,以使系统能到达滑模面.该方法估计精度高、响应速度快,对 FDI 攻击和量化参数失配具有较强的鲁棒性.最后,数值仿真验证了该方法的有效性.

关键词

信息物理系统(CPS);虚假数据注入攻击(FDI);扩张观测器;滑模控制;安全控制

中图分类号 TP273

文献标志码 A

收稿日期 2022-05-13

资助项目 国家自然科学基金(61973169);江苏省自然科学基金(BK20201392);江苏高校"青蓝工程"项目(R2021Q04)

作者简介

赖琛,女,硕士生,研究方向为网络安全控制.laiichen@163.com

郑柏超(通信作者),男,博士,教授,研究方向为网络安全控制.zhengbochao81@126.com

1 南京信息工程大学 自动化学院,南京,210044

2 南京信息工程大学 大气环境与装备技术协同创新中心,南京,210044

0 引言

信息物理系统(Cyber Physical System,CPS)通过嵌入数字传感器、处理单元和通信设备,促使物理工厂与信息过程进行交互.其主要应用领域涉及城市建设的安全关键行业,如电力、交通和供水[1-3].然而,网络与物理过程的融合开放性是恶意攻击的来源.以国家信息系统为基础的设施在现代社会中发挥着巨大作用,而对其的成功攻击会阻碍社会的正常运转,产生无法预知的后果.虚假数据注入(False Data Injection,FDI)攻击作为一种典型的攻击方式,在控制理论领域引起了许多学者的注意.与其他网络攻击(如拒绝服务攻击[4]、重放攻击[5]、偏差注入攻击[6]等)不同的是,FDI 攻击作为一种典型的攻击方式具有极强的隐蔽性[7-8],一般的被动防御方法几乎无法检测到.因此,攻击检测是防止黑客入侵系统的第一步,特别是,如何及时定位和估计恶意攻击,具有重要的意义.为了应对 FDI 攻击带来的威胁,过去几年开发了几种检测算法如基于模型[9]和基于数据驱动[10],此外,文献[11-13]使用观测器来观测和补偿受 FDI 攻击的系统,而 Zhao 等[14]则从能量转化的角度提出了防御框架.

滑模控制是一种鲁棒的非线性控制方法,其显著特征是系统对于外界干扰和参数不确定能保证良好的控制性能.因此,一些学者开始将滑模控制方法应用于 FDI 攻击的安全控制问题,例如使用滑模观测器[12,15]是一种途径.文献[16-17]研究了马尔可夫跳变系统在 FDI 攻击下的滑模控制问题,其中文献[17]针对随机发生的注入攻击,考虑了更复杂的情况.文献[18]针对一类受干扰的 CPS,提出了积分滑模控制方案来应对 FDI 的执行器攻击.文献[19]以智能电网为例,研究了通信信道受 FDI 攻击的自适应滑模控制方法.上述工作体现了滑模控制的有效性,可以看出考虑 FDI 攻击下滑模控制器的设计,以提高 CPS 抵御外界的抗干扰能力,对提高 CPS 安全性具有重要的理论和实际意义.然而,上述工作均忽略了通信过程中因物理限制引起的量化失配问题.到目前为止,针对量化失配时可能发生 FDI 攻击的情况下,基于滑模方法的 CPS 安全性控制问题的研究比较少见,并且现有的结果不能简单地推广到网络攻击的情况.有鉴于此,本文研究了 FDI 攻击下基于扩张观测器的自适应积分滑模控制问题.主要工作如下:

1)针对非线性 CPS 构造扩张观测器,对扩张观测器观测误差进行收敛性分析;

2)以线性矩阵不等式的形式给出了系统有限时间稳定的充分条件,求出了系统输出满足 L_2 增益性能的滑模向量;

3)结合指数趋近律,设计了基于扩张观测器的滑模控制器,利用广义干扰估计值和自适应律来消除 FDI 攻击、非线性、外部干扰以及量化误差产生的影响.

1 预备知识和问题描述

1.1 预备知识

$\mathbf{R}$ 表示实数集合,$\mathbf{R}^n$ 表示 n 维实数列向量,$\mathbf{R}^{n\times m}$ 表示 $n\times m$ 维的实矩阵,$\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置,$\boldsymbol{A}^{-1}$ 表示矩阵$\boldsymbol{A}$的逆矩阵,$\|\cdot\|_1$ 表示1-范数,$\|\cdot\|$ 表示欧几里德范数,$\mathrm{He}[\boldsymbol{A}]$ 表示 $\boldsymbol{A}+\boldsymbol{A}^{\mathrm{T}}$, 对称矩阵的对称位置用“$*$”表示.

1.2 非线性 CPS

本文将考虑非线性 CPS,其动态方程描述为

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{B}\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{B}\boldsymbol{\omega}(t),\\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{H}\boldsymbol{\omega}(t),\end{cases} \tag{1}$$

其中,$\boldsymbol{x}(t)\in\mathbf{R}^n$,$\boldsymbol{u}(t)\in\mathbf{R}^m$,$\boldsymbol{y}(t)\in\mathbf{R}^p$ 分别是系统的状态变量、控制输入和传感器受控输出,$\boldsymbol{f}(\boldsymbol{x})\in\mathbf{R}^m$ 为非线性项,$\boldsymbol{\omega}(t)\in\mathbf{R}^m$ 为外部干扰. 系统参数$(\boldsymbol{A},\boldsymbol{B})$ 可镇定且$(\boldsymbol{A},\boldsymbol{C})$ 可观测.

假设 1[20] 非线性函数 $\boldsymbol{f}(\boldsymbol{x})$ 对于局部 Lipschitz 导数是连续可微的.

假设 2[21] 外部干扰 $\boldsymbol{\omega}(t)$ 属于紧凑集 $\boldsymbol{D}\in\mathbf{R}^m$,并且 $\boldsymbol{\omega}(t)$ 与 $\dot{\boldsymbol{\omega}}(t)$ 均是有界的.

1.3 量化参数失配

信号量化的过程可以看作是量化器进行编码和解码的过程,量化器由取整函数 $\boldsymbol{q}(\cdot)$ 定义,量化信号表示为

$$\boldsymbol{Q}(\boldsymbol{u}(t))=\boldsymbol{\mu}_{\mathrm{d}}(t)\boldsymbol{q}\left(\frac{\boldsymbol{u}(t)}{\boldsymbol{\mu}_{\mathrm{c}}(t)}\right), \tag{2}$$

其中,$\boldsymbol{\mu}_{\mathrm{c}}(t)$ 为编码器端的量化灵敏度参数,$\boldsymbol{\mu}_{\mathrm{d}}(t)$ 为解码器端的量化灵敏度参数. 在实际应用中,由于硬件条件引起的噪声干扰往往是不可避免的,理想条件下的量化编码器和解码器参数匹配在现实情况下几乎不存在[22],故本文假设 $\boldsymbol{\mu}_{\mathrm{d}}(t)\neq\boldsymbol{\mu}_{\mathrm{c}}(t)$ 并且 $\boldsymbol{\mu}_{\mathrm{d}}(t)$ 和 $\boldsymbol{\mu}_{\mathrm{c}}(t)$ 是时变的.

建立量化时变比率模型:

$$\boldsymbol{r}(t)=\frac{\boldsymbol{\mu}_{\mathrm{d}}(t)}{\boldsymbol{\mu}_{\mathrm{c}}(t)}, \tag{3}$$

其中,$\boldsymbol{r}(t)\in(\boldsymbol{r}_{\min},\boldsymbol{r}_{\max})$,$\boldsymbol{r}_{\min}$ 和 $\boldsymbol{r}_{\max}$ 均为未知的正参数且 $0<\boldsymbol{r}_{\min}\leqslant\boldsymbol{r}_{\max}$.

根据量化信号式(2) 和量化比率模型式(3) 整理得:

$$\boldsymbol{Q}(\boldsymbol{u}(t))=\boldsymbol{r}(t)(\boldsymbol{u}(t)+\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t)). \tag{4}$$

由此可以定义量化误差表达式为

$$\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t)=\boldsymbol{\mu}_{\mathrm{c}}(t)\boldsymbol{q}\left(\frac{\boldsymbol{u}(t)}{\boldsymbol{\mu}_{\mathrm{c}}(t)}\right)-\boldsymbol{u}(t). \tag{5}$$

不难证得量化误差 $\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t)$ 满足:

$$\|\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t)\|\leqslant\frac{\sqrt{m}}{2}\boldsymbol{\mu}_{\mathrm{c}}(t). \tag{6}$$

1.4 FDI 攻击

在众多网络攻击中,发生在控制器端的 FDI 攻击是一种较为常见的攻击形式. 攻击者通常获取并利用系统的状态信息或测量输出来生成虚假数据. 本文考虑的情况是攻击者将虚假数据注入到控制器与执行器的量化失配通道. 故受到 FDI 攻击的执行器接收到的控制信号模型如下:

$$\bar{\boldsymbol{u}}(t)=\boldsymbol{u}(t)+\boldsymbol{a}(t,\boldsymbol{x}), \tag{7}$$

式中,$\boldsymbol{a}(t,\boldsymbol{x})$ 是攻击信号,即攻击者注入的虚假数据. 其中 $\boldsymbol{a}(t,\boldsymbol{x})$ 的表达式为

$$\boldsymbol{a}(t,\boldsymbol{x})=\boldsymbol{\Lambda}(t)\boldsymbol{\varphi}(t,\boldsymbol{x}), \tag{8}$$

其中,$\boldsymbol{\Lambda}(t)$ 为未知的加权矩阵,表示攻击的注入模式,非线性函数 $\boldsymbol{\varphi}(t,\boldsymbol{x})$ 表示攻击者利用的系统信息.

假设 3 在实际应用中,攻击者注入的信息通常受到信道容量、幅度等物理限制,因此 $\boldsymbol{\varphi}(t,\boldsymbol{x})$ 可以由结构已知的正函数 $\phi(t,\boldsymbol{x})$ 来界定,而加权矩阵 $\boldsymbol{\Lambda}(t)$ 的范数是未知的正常数 λ. 因此 FDI 攻击的表达式满足:

$$\|\boldsymbol{a}(t,\boldsymbol{x})\|=\|\boldsymbol{\Lambda}(t)\boldsymbol{\varphi}(t,\boldsymbol{x})\|\leqslant\lambda\phi(t,\boldsymbol{x}). \tag{9}$$

1.5 量化失配下受 FDI 攻击的 CPS

综合式(1)、(2)、(7),量化参数失配的情况下控制信号遭到 FDI 攻击的系统模型表示如下:

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{Q}(\bar{\boldsymbol{u}}(t))+\boldsymbol{B}\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{B}\boldsymbol{\omega}(t),\\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{H}\boldsymbol{\omega}(t),\end{cases} \tag{10}$$

式中,$\boldsymbol{Q}(\bar{\boldsymbol{u}}(t))=\boldsymbol{\mu}_{\mathrm{d}}(t)\left[\boldsymbol{q}\left(\frac{\boldsymbol{u}(t)}{\boldsymbol{\mu}_{\mathrm{c}}(t)}\right)+\boldsymbol{a}(t,\boldsymbol{x})\right]$ 表示受到 FDI 攻击的量化失配输入信号.

为了方便观测器的估计和补偿,实现非线性模型的动态线性化,系统模型表示成如下形式:

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{Q}(\boldsymbol{u}(t))+\boldsymbol{B}\boldsymbol{g}(\boldsymbol{x},t),\\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{H}\boldsymbol{\omega}(t),\end{cases}\tag{11}$$

其中,$\boldsymbol{g}(\boldsymbol{x},t)=\boldsymbol{\mu}_{\mathrm{d}}(t)\boldsymbol{a}(t,\boldsymbol{x})+\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{\omega}(t)$ 为广义干扰.

为了方便接下来的证明,下面给出定义.

定义 1(L_2 增益性能[23]) 对于给定的正标量 α,当 $\boldsymbol{\omega}(t)=0$ 时,系统是二次稳定的;并且在零初始条件下,$\boldsymbol{\omega}(t)\neq 0$ 时,若系统满足如下不等式:

$$\int_0^{\infty}\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)\mathrm{d}t<\alpha^2\int_0^{\infty}\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)\mathrm{d}t,\tag{12}$$

则称 CPS(10)是具有有界增益性能 α 的二次稳定.

2 扩张观测器的设计和分析

复合扰动的边界是滑模控制过程中的一个大问题.考虑到很难直接确定合适的边界,本文使用扩张观测器来跟踪有限的可用测量值中扰动的实际变化.为了设计观测器,CPS(11)可表示成如下矩阵块形式:

$$\begin{bmatrix}\dot{\boldsymbol{x}}(t)\\ \dot{\boldsymbol{g}}(\boldsymbol{x},t)\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{0}_{n\times n}&\boldsymbol{0}_{1\times 1}\end{bmatrix}\begin{bmatrix}\boldsymbol{x}(t)\\ \boldsymbol{g}(\boldsymbol{x},t)\end{bmatrix}+\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{0}_{1\times 1}\end{bmatrix}\boldsymbol{Q}(\boldsymbol{u}(t))+\begin{bmatrix}\boldsymbol{0}_{n\times 1}\\ \dot{\boldsymbol{g}}(\boldsymbol{x},t)\end{bmatrix}.\tag{13}$$

构造如下的扩张观测器:

$$\begin{cases}\dot{\hat{\boldsymbol{x}}}(t)=\boldsymbol{A}\hat{\boldsymbol{x}}(t)+\boldsymbol{B}\boldsymbol{Q}(\boldsymbol{u}(t))+\boldsymbol{B}\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\\ \qquad\boldsymbol{L}_x(\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t)),\\ \dot{\hat{\boldsymbol{g}}}(\boldsymbol{x},t)=\boldsymbol{L}_g(\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t)),\end{cases}\tag{14}$$

其中,$\boldsymbol{L}_x\in\mathbf{R}^{n\times m}$ 和 $\boldsymbol{L}_g\in\mathbf{R}^{m\times m}$ 是设计的观测器增益.

为了方便观测器的收敛性分析,重构扩张观测器的数学模型:

$$\begin{bmatrix}\dot{\hat{\boldsymbol{x}}}(t)\\ \dot{\hat{\boldsymbol{g}}}(\boldsymbol{x},t)\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}&\boldsymbol{B}\\ \boldsymbol{0}_{n\times n}&\boldsymbol{0}\end{bmatrix}\begin{bmatrix}\hat{\boldsymbol{x}}(t)\\ \hat{\boldsymbol{g}}(\boldsymbol{x},t)\end{bmatrix}+\begin{bmatrix}\boldsymbol{B}\\ \boldsymbol{0}\end{bmatrix}\boldsymbol{Q}(\boldsymbol{u}(t))+\begin{bmatrix}\boldsymbol{L}_x\\ \boldsymbol{L}_g\end{bmatrix}(\boldsymbol{y}(t)-\hat{\boldsymbol{y}}(t)).\tag{15}$$

令状态误差 $\tilde{\boldsymbol{x}}(t)=\boldsymbol{x}(t)-\hat{\boldsymbol{x}}(t)$,广义干扰误差 $\tilde{\boldsymbol{g}}(\boldsymbol{x},t)=\boldsymbol{g}(\boldsymbol{x},t)-\hat{\boldsymbol{g}}(\boldsymbol{x},t)$,总误差 $\boldsymbol{e}(t)=\begin{bmatrix}\tilde{\boldsymbol{x}}(t)\\ \tilde{\boldsymbol{g}}(\boldsymbol{x},t)\end{bmatrix}$,观测误差状态方程可以表示为

$$\dot{\boldsymbol{e}}(t)=\tilde{\boldsymbol{A}}\boldsymbol{e}(t)+\tilde{\boldsymbol{B}}\dot{\boldsymbol{g}}(\boldsymbol{x},t),\tag{16}$$

其中,$\tilde{\boldsymbol{A}}=\begin{bmatrix}\boldsymbol{A}-\boldsymbol{L}_x\boldsymbol{C}&\boldsymbol{B}\\ -\boldsymbol{L}_g\boldsymbol{C}&\boldsymbol{0}\end{bmatrix}$,$\tilde{\boldsymbol{B}}=\begin{bmatrix}\boldsymbol{0}_{n\times 1}\\ 1\end{bmatrix}$.

为了使观测误差收敛,可通过选择合适的 $\boldsymbol{L}_x$ 和 $\boldsymbol{L}_g$ 使 $\tilde{\boldsymbol{A}}$ 满足 Hurwitz 稳定,即对于任意给定的对称正定矩阵 $\boldsymbol{Q}$,存在唯一对称正定矩阵 $\boldsymbol{P}$,使得等式 $\tilde{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}\tilde{\boldsymbol{A}}=-\boldsymbol{Q}$ 成立.

为了证明观测器的稳定性,对观测误差的收敛条件进行分析.

首先,构造李雅普诺夫函数 $\boldsymbol{V}_e(t)=\boldsymbol{e}^{\mathrm{T}}(t)\boldsymbol{P}\boldsymbol{e}(t)$.其次,对李雅普诺夫函数沿观测器误差轨迹(16)进行求导:

$$\begin{aligned}\dot{\boldsymbol{V}}_e(t)=&[\tilde{\boldsymbol{A}}\boldsymbol{e}(t)+\tilde{\boldsymbol{B}}\dot{\boldsymbol{g}}(\boldsymbol{x},t)]^{\mathrm{T}}\boldsymbol{P}\boldsymbol{e}(t)+\\ &\boldsymbol{e}^{\mathrm{T}}(t)\boldsymbol{P}[\tilde{\boldsymbol{A}}\boldsymbol{e}(t)+\tilde{\boldsymbol{B}}\dot{\boldsymbol{g}}(\boldsymbol{x},t)]=\\ &\boldsymbol{e}^{\mathrm{T}}(t)[\tilde{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}\tilde{\boldsymbol{A}}]\boldsymbol{e}(t)+\\ &\mathrm{He}[\boldsymbol{e}^{\mathrm{T}}(t)\boldsymbol{P}\tilde{\boldsymbol{B}}\dot{\boldsymbol{g}}(\boldsymbol{x},t)].\end{aligned}\tag{17}$$

接着,结合等式 $\tilde{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}\tilde{\boldsymbol{A}}=-\boldsymbol{Q}$,可以得到如下不等式关系:

$$\dot{\boldsymbol{V}}_e(t)\leqslant-\boldsymbol{e}^{\mathrm{T}}(t)\boldsymbol{Q}\boldsymbol{e}(t)+2\|\boldsymbol{e}(t)\|\,\|\boldsymbol{P}\tilde{\boldsymbol{B}}\|\,\|\dot{\boldsymbol{g}}(\boldsymbol{x},t)\|\leqslant-\lambda_{\min}(\boldsymbol{Q})\|\boldsymbol{e}(t)\|^2+2\|\boldsymbol{e}(t)\|\,\|\boldsymbol{P}\tilde{\boldsymbol{B}}\|\,\|\dot{\boldsymbol{g}}(\boldsymbol{x},t)\|,\tag{18}$$

其中,$\lambda_{\min}(\boldsymbol{Q})$ 是 $\boldsymbol{Q}$ 的最小特征值,因为 $\boldsymbol{Q}$ 是对称正定矩阵,所以它的特征值是正的.

最后,由 $\dot{\boldsymbol{V}}_e(t)<0$ 可得扩展观测器观测误差收敛条件为

$$\|\boldsymbol{e}(t)\|\geqslant\frac{2\|\boldsymbol{P}\tilde{\boldsymbol{B}}\|\,\|\dot{\boldsymbol{g}}(\boldsymbol{x},t)\|}{\lambda_{\min}(\boldsymbol{Q})}.\tag{19}$$

3 积分滑模函数的设计

滑模控制的主要特征是根据系统当前状态有目的地调节控制律,使系统按照预定的滑动模态的状态轨迹运动,其中滑动模态可以进行设计,且与对象参数及扰动无关,因此具有优越的鲁棒性[24].本节将设计一种积分型滑模面,并通过 Lyapunov 方法和线性矩阵不等式技术,得到滑动模态渐近稳定的充分条件.相比于传统滑模面,积分滑模面可以通过设计合适的初始位置使系统从一开始就位于滑模面上,具有更好的动态性能和鲁棒性.

设计如下的积分滑模函数:

$$\boldsymbol{s}(t)=\boldsymbol{G}\boldsymbol{x}(t)-\boldsymbol{G}\boldsymbol{x}(0)-\int_0^t\boldsymbol{G}(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{K})\boldsymbol{x}(\tau)\mathrm{d}\tau,\tag{20}$$

其中,$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是式(10)中的系统矩阵,切换向量 $\boldsymbol{G}\in\mathbf{R}^{m\times n}$ 满足 $\boldsymbol{G}\boldsymbol{B}$ 为非奇异矩阵.同时,选择向量 $\boldsymbol{K}\in\mathbf{R}^{m\times n}$ 使得 $\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}$ 是 Hurwitz 矩阵.为了证明的方便,本文设计 $\boldsymbol{G}=\boldsymbol{B}^{+}$.

对滑模函数沿系统状态(10)求导得:

$$\dot{\boldsymbol{s}}(t)=\boldsymbol{G}[\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{Q}(\bar{\boldsymbol{u}}(t))+\boldsymbol{B}\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{B}\boldsymbol{\omega}(t)]-$$

$$\boldsymbol{G}(\boldsymbol{A}-\boldsymbol{BK})\boldsymbol{x}(t)=\boldsymbol{GBQ}(\bar{\boldsymbol{u}}(t))+\boldsymbol{GBf}(\boldsymbol{x})+\boldsymbol{GB}\boldsymbol{\omega}(t)+\boldsymbol{GBKx}(t). \tag{21}$$

根据滑模面的性质,由 $\dot{\boldsymbol{s}}(t)=0$ 可以得到等效控制为

$$\boldsymbol{Q}_{\mathrm{eq}}(\bar{\boldsymbol{u}}(t))=-\boldsymbol{Kx}(t)-\boldsymbol{f}(\boldsymbol{x})-\boldsymbol{\omega}(t). \tag{22}$$

将等效控制带入式(10)得到等效系统状态:

$$\dot{\boldsymbol{x}}(t)=\boldsymbol{Ax}(t)+\boldsymbol{BQ}_{\mathrm{eq}}(\bar{\boldsymbol{u}}(t))+\boldsymbol{Bf}(\boldsymbol{x})+\boldsymbol{B}\boldsymbol{\omega}(t)=\boldsymbol{Ax}(t)+\boldsymbol{B}[-\boldsymbol{Kx}(t)-\boldsymbol{f}(\boldsymbol{x},t)]+\boldsymbol{Bf}(\boldsymbol{x})+\boldsymbol{B}\boldsymbol{\omega}(t)=\bar{\boldsymbol{A}}\boldsymbol{x}(t). \tag{23}$$

其中,$\bar{\boldsymbol{A}}=\boldsymbol{A}-\boldsymbol{BK}$.

注 1 此处的等效控制律仅作为分析滑动模态稳定性的工具使用,并不作为实际的控制律使用.实际滑模控制律将在本文第 4 章中设计.

下面给出滑动模态下等效系统(23)渐近稳定的充分条件.

定理 1 对于受到 FDI 攻击和量化失配的 CPS(10),如果存在对称正定矩阵 $\boldsymbol{Q}$,常规矩阵 $\boldsymbol{W}$,使得下列线性矩阵不等式

$$\begin{bmatrix}\mathrm{He}[\boldsymbol{AQ}-\boldsymbol{BW}] & \boldsymbol{QC}^{\mathrm{T}}\boldsymbol{H} & \boldsymbol{QC}^{\mathrm{T}}\\ * & \boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}-\alpha^2\boldsymbol{I} & \boldsymbol{0}\\ * & * & -\boldsymbol{I}\end{bmatrix}<0 \tag{24}$$

有解,其中 $\alpha>0$,那么,滑动模态(23)是全局渐近稳定的,并且满足 L_2 增益性能(12),此时滑模向量由 $\boldsymbol{K}=\boldsymbol{WQ}^{-1}$ 给出.

证明 构建 Lyapunov 函数 $V_x(t)=\boldsymbol{x}^{\mathrm{T}}(t)\boldsymbol{Px}(t)$,其中 $\boldsymbol{P}>0$.对其沿着(23)求导:

$$\dot{\boldsymbol{V}}_x(t)=[\bar{\boldsymbol{A}}\boldsymbol{x}(t)]^{\mathrm{T}}\boldsymbol{Px}(t)+\boldsymbol{x}^{\mathrm{T}}(t)\boldsymbol{P}[\bar{\boldsymbol{A}}\boldsymbol{x}(t)]=\boldsymbol{x}^{\mathrm{T}}(t)\mathrm{He}[\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}]\boldsymbol{x}(t), \tag{25}$$

令 $\boldsymbol{M}=\dot{\boldsymbol{V}}_x+\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)-\alpha^2\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)$,那么,

$$\begin{aligned}\boldsymbol{M}=&\ \boldsymbol{x}^{\mathrm{T}}(t)\mathrm{He}[\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}]\boldsymbol{x}(t)+[\boldsymbol{Cx}(t)+\boldsymbol{H}\boldsymbol{\omega}(t)]^{\mathrm{T}}[\boldsymbol{Cx}(t)+\boldsymbol{H}\boldsymbol{\omega}(t)]-\alpha^2\sum_{i=1}^{N}\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)=\\ &\boldsymbol{x}^{\mathrm{T}}(t)[\mathrm{He}[\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}]+\boldsymbol{C}^{\mathrm{T}}\boldsymbol{C}]\boldsymbol{x}(t)+\\ &\boldsymbol{\omega}^{\mathrm{T}}(t)[\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}-\alpha^2\boldsymbol{I}]\boldsymbol{\omega}(t)+\\ &2\boldsymbol{x}^{\mathrm{T}}(t)\boldsymbol{C}^{\mathrm{T}}\boldsymbol{H}\boldsymbol{\omega}(t).\end{aligned} \tag{26}$$

令向量 $\boldsymbol{\xi}(t)=[\boldsymbol{x}^{\mathrm{T}}(t)\quad\boldsymbol{\omega}^{\mathrm{T}}(t)]^{\mathrm{T}}$,分块矩阵 $\boldsymbol{\Gamma}=\begin{bmatrix}\mathrm{He}[\bar{\boldsymbol{A}}^{\mathrm{T}}\boldsymbol{P}]+\boldsymbol{C}^{\mathrm{T}}\boldsymbol{C} & \boldsymbol{C}^{\mathrm{T}}\boldsymbol{H}\\ * & \boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}-\alpha^2\boldsymbol{I}\end{bmatrix}$,可得 $\boldsymbol{M}=\boldsymbol{\xi}^{\mathrm{T}}(t)\boldsymbol{\Gamma}\boldsymbol{\xi}(t)$.

运用舒尔补引理,线性矩阵不等式条件(24)可以表示成:

$$\begin{bmatrix}\mathrm{He}[\boldsymbol{AQ}-\boldsymbol{BW}]+\boldsymbol{QC}^{\mathrm{T}}\boldsymbol{CQ} & \boldsymbol{QC}^{\mathrm{T}}\boldsymbol{H}\\ * & \boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}-\alpha^2\boldsymbol{I}\end{bmatrix}<0. \tag{27}$$

对式(27)两边左右同时乘以矩阵 $\mathrm{diag}\{\boldsymbol{Q}^{-1},\boldsymbol{I}\}$,令 $\boldsymbol{Q}^{-1}=\boldsymbol{P}$ 以及 $\boldsymbol{W}=\boldsymbol{KQ}$,式(27)可以转化成 $\boldsymbol{\Gamma}<0$.综上,当线性矩阵不等式条件(24)成立时,可以得到 $\boldsymbol{\Gamma}<0$.因为 $\boldsymbol{\xi}(t)$ 是非零向量,故 $\boldsymbol{M}<0$ 成立.

结合定义 1,令 $\boldsymbol{J}=\int_0^{\infty}[\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)-\alpha^2\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)]\mathrm{d}t$,对 $\boldsymbol{J}$ 变形得:

$$\begin{aligned}\boldsymbol{J}=&\int_0^{\infty}[\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)-\alpha^2\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)+\dot{\boldsymbol{V}}_x]\mathrm{d}t-\int_0^{\infty}\dot{\boldsymbol{V}}_x\mathrm{d}t=\int_0^{\infty}[\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)-\alpha^2\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)+\\ &\dot{\boldsymbol{V}}_x]\mathrm{d}t-[\boldsymbol{V}_x(\infty)-\boldsymbol{V}_x(0)],\end{aligned} \tag{28}$$

在零初始条件下有:

$$\boldsymbol{J}=\int_0^{\infty}[\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)-\alpha^2\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)+\dot{\boldsymbol{V}}_x]\mathrm{d}t=\int_0^{\infty}\boldsymbol{M}\mathrm{d}t<0, \tag{29}$$

不难看出 $\dot{\boldsymbol{V}}_x>0$,故可以得到 L_2 性能:

$$\int_0^{\infty}\boldsymbol{y}^{\mathrm{T}}(t)\boldsymbol{y}(t)\mathrm{d}t<\alpha^2\int_0^{\infty}\boldsymbol{\omega}^{\mathrm{T}}(t)\boldsymbol{\omega}(t)\mathrm{d}t. \tag{30}$$

定理 1 证明完毕.

4 基于扩张观测器的滑模控制器设计

本节将设计滑模控制律,保证系统状态轨迹能在有限时间内到达滑模面 $\boldsymbol{s}(t)=0$ 上,并在接下来的时间不离开滑模面.因此,针对 CPS(11),利用广义干扰观测值,设计滑模控制器以消除 FDI 攻击、量化失配、非线性以及外部干扰对系统产生的影响.

首先,为了保证系统快速到达滑动面,选择指数趋近律:

$$\dot{\boldsymbol{s}}(t)=-\varepsilon\mathrm{sgn}(\boldsymbol{s}(t))-k\boldsymbol{s}(t), \tag{31}$$

其中,$\varepsilon>0,k>0$.为了保证快速趋近律的同时削弱抖振,应在增大 k 的同时减小 ε.

设计如下的滑模控制器:

$$\boldsymbol{u}(t)=-\hat{\boldsymbol{r}}(t)\mathrm{sgn}(\boldsymbol{s}(t))[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\mathrm{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]-\frac{\sqrt{m}}{2}\boldsymbol{\mu}_{\mathrm{c}}(t)\mathrm{sgn}(\boldsymbol{s}(t)), \tag{32}$$

其中,$\hat{\boldsymbol{r}}(t)$ 是 $\boldsymbol{r}(t)$ 的估计值且 $\hat{\boldsymbol{r}}(0)>0$,用以消除量化误差,满足如下自适应律:

$$\dot{\hat{\boldsymbol{r}}}(t)=\frac{\hat{\boldsymbol{r}}^3(t)}{\eta}\{\|\boldsymbol{s}(t)\|_1[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\mathrm{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]\}. \tag{33}$$

下面证明所设计的滑模控制律(32)—(33)能够保证滑模面的可达性.

定理 2 对于满足假设 1—3 的系统(11),在滑模控制律(32)—(33)作用下,能保证系统状态轨迹在有限时间内被吸引到滑模面 $\boldsymbol{s}(t)=0$ 上.

证明 构造李雅普诺夫函数 $\boldsymbol{V}(t)=\frac{1}{2}\boldsymbol{s}^{\mathrm{T}}(t)\boldsymbol{s}(t)$,沿着系统状态(11)对其求导得:

$$\dot{\boldsymbol{V}}(t)=\boldsymbol{s}^{\mathrm{T}}(t)[\boldsymbol{GBQ}(\boldsymbol{u}(t))+\boldsymbol{GBg}(\boldsymbol{x},t)+\boldsymbol{GBKx}(t)], \tag{34}$$

注意到 $\boldsymbol{G}=\boldsymbol{B}^{+}$,并且结合量化误差得到:

$$\dot{\boldsymbol{V}}(t)=\boldsymbol{s}^{\mathrm{T}}(t)[\boldsymbol{r}(t)(\boldsymbol{u}(t)+\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t))+\boldsymbol{g}(\boldsymbol{x},t)+\boldsymbol{Kx}(t)]. \tag{35}$$

构造李雅普诺夫函数 $\tilde{\boldsymbol{V}}(t)=\boldsymbol{V}(t)+\frac{1}{2}\eta\tilde{\boldsymbol{r}}^{2}(t)$,其中 $\tilde{\boldsymbol{r}}(t)=\boldsymbol{r}(t)-\hat{\boldsymbol{r}}^{-1}(t)$,对其进行求导得:

$$\dot{\tilde{\boldsymbol{V}}}(t)=\boldsymbol{s}^{\mathrm{T}}(t)[\boldsymbol{r}(t)(\boldsymbol{u}(t)+\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t))+\boldsymbol{g}(\boldsymbol{x},t)+\boldsymbol{Kx}(t)]+\eta\frac{\tilde{\boldsymbol{r}}(t)\dot{\hat{\boldsymbol{r}}}(t)}{\hat{\boldsymbol{r}}^{2}(t)}. \tag{36}$$

将自适应律 $\dot{\hat{\boldsymbol{r}}}(t)$ 和控制器 $\boldsymbol{u}(t)$ 带入,并结合 $\|\boldsymbol{e}_{\boldsymbol{\mu}_{\mathrm{c}}}(t)\|\leqslant\frac{\sqrt{m}}{2}\boldsymbol{\mu}_{\mathrm{c}}(t)$ 整理得到:

$$\begin{aligned}\dot{\tilde{\boldsymbol{V}}}(t)\leqslant&\left\{-\hat{\boldsymbol{r}}(t)\operatorname{sgn}(\boldsymbol{s}(t))[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]+\frac{\sqrt{m}}{2}\boldsymbol{\mu}_{\mathrm{c}}(t)[1-\operatorname{sgn}(\boldsymbol{s}(t))]\right\}\times\\&\boldsymbol{s}^{\mathrm{T}}(t)\boldsymbol{r}(t)+\boldsymbol{s}^{\mathrm{T}}(t)[\boldsymbol{g}(\boldsymbol{x},t)+\boldsymbol{Kx}(t)]+\\&\|\boldsymbol{s}(t)\|_{1}\tilde{\boldsymbol{r}}(t)\hat{\boldsymbol{r}}(t)[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\\&\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)].\end{aligned} \tag{37}$$

结合量化时变比率模型 $\boldsymbol{r}(t)=\frac{\boldsymbol{\mu}_{\mathrm{d}}(t)}{\boldsymbol{\mu}_{\mathrm{c}}(t)}$ 以及符号函数的性质,式(37)可以整理如下:

$$\begin{aligned}\dot{\tilde{\boldsymbol{V}}}(t)\leqslant&-\|\boldsymbol{s}(t)\|_{1}\boldsymbol{r}(t)\hat{\boldsymbol{r}}(t)[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]+\frac{\sqrt{m}}{2}\boldsymbol{\mu}_{\mathrm{d}}(t)(\|\boldsymbol{s}(t)\|-\|\boldsymbol{s}(t)\|_{1})+\boldsymbol{s}^{\mathrm{T}}(t)[\boldsymbol{g}(\boldsymbol{x},t)+\boldsymbol{Kx}(t)]+\\&\|\boldsymbol{s}(t)\|_{1}\tilde{\boldsymbol{r}}(t)\hat{\boldsymbol{r}}(t)[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\\&\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)].\end{aligned} \tag{38}$$

因为有不等式关系 $\|\boldsymbol{s}(t)\|_{1}>\|\boldsymbol{s}(t)\|$,所以有

$$\begin{aligned}\dot{\tilde{\boldsymbol{V}}}(t)\leqslant&-\|\boldsymbol{s}(t)\|_{1}\boldsymbol{r}(t)\hat{\boldsymbol{r}}(t)[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]+\\&\|\boldsymbol{s}(t)\|_{1}\tilde{\boldsymbol{r}}(t)\hat{\boldsymbol{r}}(t)[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\\&\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]+\\&\|\boldsymbol{s}(t)\|_{1}[\boldsymbol{g}(\boldsymbol{x},t)+\boldsymbol{Kx}(t)].\end{aligned} \tag{39}$$

因为 $\tilde{\boldsymbol{r}}(t)-\boldsymbol{r}(t)=-\hat{\boldsymbol{r}}^{-1}(t)$,故

$$\begin{aligned}\dot{\tilde{\boldsymbol{V}}}(t)\leqslant&-\|\boldsymbol{s}(t)\|_{1}[\boldsymbol{Kx}(t)+\hat{\boldsymbol{g}}(\boldsymbol{x},t)+\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)]+\\&\|\boldsymbol{s}(t)\|_{1}[\boldsymbol{Kx}(t)+\boldsymbol{g}(\boldsymbol{x},t)]\leqslant\\&-\|\boldsymbol{s}(t)\|_{1}[\hat{\boldsymbol{g}}(\boldsymbol{x},t)-\boldsymbol{g}(\boldsymbol{x},t)]-\\&\|\boldsymbol{s}(t)\|_{1}[\varepsilon\operatorname{sgn}(\boldsymbol{s}(t))+k\boldsymbol{s}(t)].\end{aligned} \tag{40}$$

因为 $0\leqslant|\hat{\boldsymbol{g}}(\boldsymbol{x},t)-\boldsymbol{g}(\boldsymbol{x},t)|\leqslant\kappa$,且在有限时间内观测器误差能趋于零,即 $\lim\limits_{t\to t_0}\kappa=0$.因此,当 t 趋于无穷时,有:

$$\dot{\tilde{\boldsymbol{V}}}(t)\leqslant-k\boldsymbol{s}^{2}(t)-\varepsilon\|\boldsymbol{s}(t)\|_{1}<0, \tag{41}$$

因此,在本节设计的滑模控制律作用下,定理 1 所确定的滑模面的可达性成立.定理 2 证明完毕.

5 数值仿真

本文运用 Matlab/Simulink 实验仿真来验证 FDI 攻击下基于扩张观测器的非线性系统的自适应积分滑模控制研究的可行性.

本文控制目标是设计滑模控制律,使得系统可以在有限的时间内到达指定的滑模面,并沿着该滑模面渐近稳定.针对具有 FDI 攻击、量化失配、非线性项以及外部干扰的系统(10),为了说明本文算法的有效性,仿真中考虑以下情况的仿真进行对比.

情况 1.本文系统在控制器(32)—(33)作用下进行仿真.仿真的主要参数如表 1—3 所示.为了减弱抖振带来的影响,仿真中使用 $\boldsymbol{s}(t)/(\|\boldsymbol{s}(t)\|+0.01)$ 代替符号函数 $\operatorname{sgn}(\boldsymbol{s}(t))$.为了防止观测器引起的峰值现象,引入观测器参数 γ.

系统中考虑的攻击模型已经被研究过[25],恶意攻击者可以通过修改通道上传输的数据来破坏控制指令.因此,假设恶意攻击者能够在系统中获得完整的系统状态是合理的,它们都可以被用来设计隐蔽式欺骗攻击信号,故可以考虑参数化 $\boldsymbol{a}(t,\boldsymbol{x})$.满足假设 3 的 FDI 攻击的表达式 $\boldsymbol{a}(t,\boldsymbol{x})=2\|\boldsymbol{Cx}(t)\|\sin(t)+6$,则相应地未知加权矩阵 $\boldsymbol{\Lambda}(t)=2\sin(t)$,攻击者利用的系统信息 $\boldsymbol{\varphi}(t,\boldsymbol{x})=\|\boldsymbol{Cx}(t)\|+6$,正常数 $\lambda=2$,结构已知的正函数 $\boldsymbol{\varphi}(t,\boldsymbol{x})=\|\boldsymbol{Cx}(t)\|+8$.

情况 2.本文系统在文献[25]控制器作用下进行仿真.仿真中,系统参数的参数选取与表 1 一致,控制器参数如表 4 所示.

表 1　本文的系统参数

Table 1　Parameters of the proposed system

参数	数值	参数	数值
$\boldsymbol{A}$	[2　4;5　4]	$\boldsymbol{f}(\boldsymbol{x})$	$0.5\cos(\boldsymbol{x}_1(t))\sin(\boldsymbol{x}_2(t))$
$\boldsymbol{B}$	$[2\quad 5]^{\mathrm{T}}$	$\boldsymbol{\omega}(t)$	$\sin(\|\boldsymbol{x}(t)\|)$
$\boldsymbol{C}$	[3　2]	$\boldsymbol{a}(t,\boldsymbol{x})$	$2\|\boldsymbol{Cx}(t)\|\sin(t)+6$
$\boldsymbol{H}$	0.1	$\boldsymbol{x}(0)$	$[1\quad 1]^{\mathrm{T}}$
$\boldsymbol{\mu}_{\mathrm{c}}(t)$	$\begin{cases}1.0, & t\leqslant 0.6,\\ 0.8, & 0.6<t\leqslant 4,\\ 0.7, & 4<t\leqslant 8\end{cases}$	$\mu_{\mathrm{d}}(t)$	$\begin{cases}0.8, & t\leqslant 0.3,\\ 0.7, & 0.3<t\leqslant 3,\\ 0.6, & 3<t\leqslant 5\end{cases}$

表 2　本文的观测器参数

Table 2　Parameters of the proposed observer

参数	数值	参数	数值	参数	数值
$\boldsymbol{L}_x$	$\left[\frac{25}{9}\gamma\quad\frac{16}{3}\gamma^2\right]$	$\boldsymbol{L}_g$	$\frac{14}{9}\gamma^3$	γ	$\begin{cases}100t^3, & 0\leqslant t\leqslant 1,\\ 100, & t>1\end{cases}$

表 3　本文的控制器参数

Table 3　Parameters of the proposed controller

参数	数值	参数	数值
$\boldsymbol{G}$	[0.069 0　0.172 4]	$\boldsymbol{K}$	[3.300 6　2.434 6]
k	20	ε	1
$\hat{\boldsymbol{r}}(0)$	3	η	50

表 4　文献[25]设计方法的控制器参数

Table 4　Controller parameters of method in [25]

参数	数值	参数	数值
$\boldsymbol{G}$	[0.069 0　0.172 4]	$\boldsymbol{K}$	[3.300 6　2.434 6]
κ	4.101 4	β	2
$\hat{\boldsymbol{r}}(0)$	0.1	η_1	0.01
$\hat{\boldsymbol{\varepsilon}}_{\mathrm{d}}(0)$	1	η	0.20
$\hat{\boldsymbol{\delta}}(0)$	1	η_3	0.01
$\phi(t,\boldsymbol{x})$	$2\|\boldsymbol{Cx}(t)\|+6$	σ	0.85

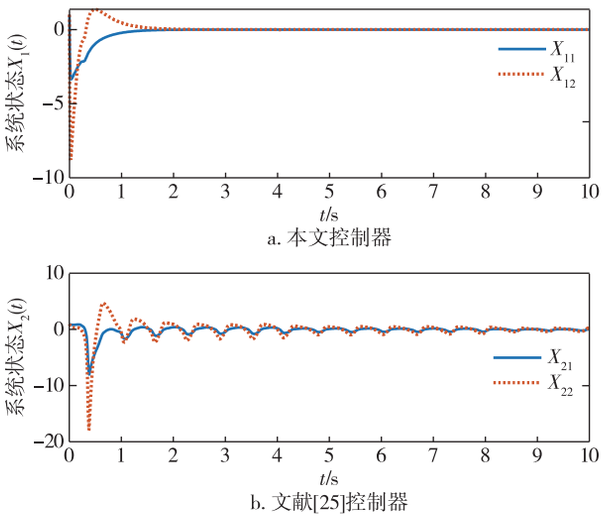
通过 Matlab/Simulink,对以上情况 1 和情况 2 的算例进行仿真,系统的状态轨迹、控制输入和滑模函数的响应曲线分别如图 1—3 所示.

图 1 表明系统状态在本文控制器作用下能实现渐近稳定,而在对比控制器下抖振明显.图 2 表明本文控制器能实现稳定,而对比控制器的控制性能较差.图 3 表明滑模面在本文算法下能快速收敛并实现稳定,而在对比算法下抖振明显.图 4 给出了本文仿真中利用扩张观测器得到的广义干扰估计曲线.

情况 3.为了说明本文算法对 FDI 攻击的防御效果的有效性,系统的线性化模型修改成如下形式:

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{Ax}(t)+\boldsymbol{BQ}(\bar{\boldsymbol{u}}(t))+\boldsymbol{Bg}'(\boldsymbol{x},t),\\ \boldsymbol{y}(t)=\boldsymbol{Cx}(t)+\boldsymbol{H\omega}(t),\end{cases}\tag{42}$$

其中广义干扰 $\boldsymbol{g}'(\boldsymbol{x},t)=\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{\omega}(t)$,由此,观测器

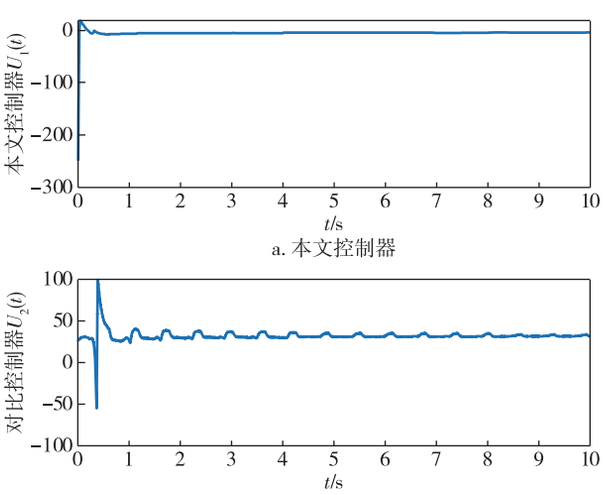


a. 本文控制器

b. 文献[25]控制器

图 1　系统状态响应曲线对比

Fig. 1　Comparison of state response curves under the proposed controller (top) and controller in [25] (bottom)



a. 本文控制器

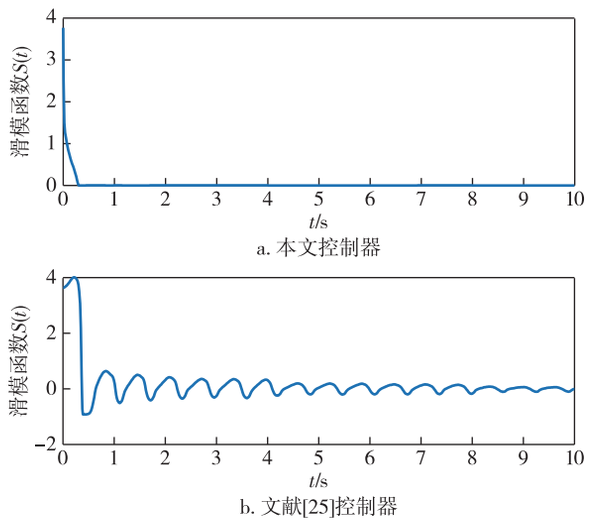
b.文献[25]控制器

图 2　控制器输入响应曲线对比

Fig. 2　Comparison of input response curves of the proposed controller (top) and controller in [25] (bottom)

不对攻击值 $\boldsymbol{a}(t,\boldsymbol{x})$ 进行估计,即 $\hat{\boldsymbol{g}}'(\boldsymbol{x},t)$ 不包含 FDI 攻击的估计值 $\hat{\boldsymbol{a}}(t,\boldsymbol{x})$,故控制器(32)—(33)中的观测值 $\hat{\boldsymbol{g}}'(\boldsymbol{x},t)$ 对 FDI 攻击无防御效果.

运用 Matlab/Simulink 对表 5—7 中的算例进行仿真,在控制器(32)—(33)作用下,系统(42)的状态轨迹和控制输入的仿真情形分别如图 5—6 所示.可以看出,当系统遭受 FDI 攻击而控制器中不含 FDI 攻击的防御信息时,状态轨迹和控制输入呈现出明显的发散趋势,即控制算法无法保证系统的稳定性.



a. 本文控制器

b. 文献[25]控制器

图 3　滑模函数响应曲线对比

Fig. 3　Comparison of sliding mode function response curves under the proposed controller (top) and controller in [25] (bottom)

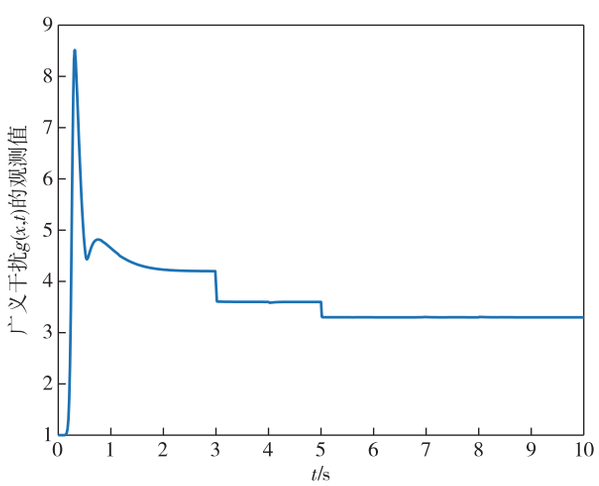


图 4　广义干扰估计曲线

Fig. 4　Generalized disturbance estimation curve

表 5　系统参数

Table 5　System parameters

参数	数值	参数	数值
$\boldsymbol{A}$	[4　3;3　5]	$\boldsymbol{f}(\boldsymbol{x})$	$0.2\cos(\boldsymbol{x}_1(t))\sin(\boldsymbol{x}_2(t))$
$\boldsymbol{B}$	$[1\quad 2]^{\mathrm{T}}$	$\boldsymbol{\omega}(t)$	$\sin(\|\boldsymbol{x}(t)\|)$
$\boldsymbol{C}$	[4　5]	$\boldsymbol{a}(t,\boldsymbol{x})$	$10\|\boldsymbol{C}\boldsymbol{x}(t)\|\sin(t)+10$
$\boldsymbol{H}$	0.1	$\boldsymbol{x}(0)$	$[2\quad 1]^{\mathrm{T}}$
$\boldsymbol{\mu}_{\mathrm{c}}(t)$	$\begin{cases}1.2, & t\leqslant 2,\\ 0.8, & 2<t\leqslant 4,\\ 0.7, & 4<t\leqslant 8\end{cases}$	$\boldsymbol{\mu}_{\mathrm{d}}(t)$	$\begin{cases}0.8, & t\leqslant 0.3,\\ 0.7, & 0.3<t\leqslant 3,\\ 0.6, & 3<t\leqslant 5\end{cases}$

表 6　未使用 FDI 攻击值 $\boldsymbol{a}(t,\boldsymbol{x})$ 的观测器参数

Table 6　Parameters of the proposed observer without using FDI attack $\boldsymbol{a}(t,\boldsymbol{x})$

参数	数值	参数	数值	参数	数值
$\boldsymbol{L}_x$	$\left[\frac{425}{159}\gamma\quad\frac{137}{159}\gamma^2\right]^{\mathrm{T}}$	$\boldsymbol{L}_g$	$\frac{8}{3}\gamma^3$	γ	$\begin{cases}100t^3, & 0\leqslant t\leqslant 1,\\ 100, & t>1\end{cases}$

表 7　未使用 FDI 攻击估计值 $\hat{\boldsymbol{a}}(t,\boldsymbol{x})$ 的控制器参数

Table 7　Parameters of the proposed controller without using FDI attack $\hat{\boldsymbol{a}}(t,\boldsymbol{x})$

参数	数值	参数	数值
$\boldsymbol{G}$	[0.2　0.4]	$\boldsymbol{K}$	[3.210 3　4.819 4]
k	20	ε	1
$\hat{\boldsymbol{r}}(0)$	1	η	200

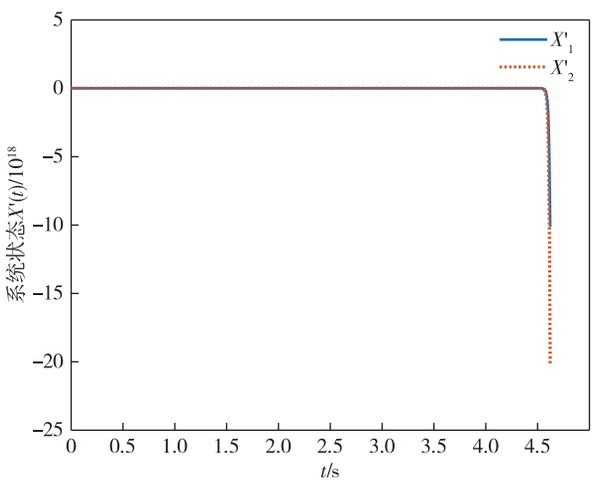


图 5　未考虑 FDI 攻击防御的控制器作用下的系统状态响应曲线

Fig. 5　System state response curve under controller without considering defense against FDI attack

情况 4.为了更好地阐述本文所设计的基于观测器的滑模控制算法的有效性,与情况 3 的仿真设计相对比,本文的线性化系统(11)在控制器(32)—(33)的作用下进行仿真实验.在本次情况设计中,广义干扰 $\boldsymbol{g}(\boldsymbol{x},t)=\boldsymbol{\mu}_{\mathrm{d}}(t)\boldsymbol{a}(t,\boldsymbol{x})+\boldsymbol{f}(\boldsymbol{x})+\boldsymbol{\omega}(t)$,观测器能对攻击值 $\boldsymbol{a}(t,\boldsymbol{x})$ 进行估计,即 $\hat{\boldsymbol{g}}(\boldsymbol{x},t)$ 包含了 FDI 攻击的估计值 $\hat{\boldsymbol{a}}(t,\boldsymbol{x})$,控制器(32)—(33)的观测值 $\hat{\boldsymbol{g}}(\boldsymbol{x},t)$ 对 FDI 攻击有防御效果.

运用 Matlab/Simulink 对本文系统进行仿真,仿真的主要参数如表 5—7 所示.在控制器(32)—(33)作用下,系统状态轨迹和控制输入响应曲线分别如图 7—8 所示.可以看出,当系统遭受 FDI 攻击而观测器包含了 FDI 攻击的防御信息时,系统状态在限时间内收敛到原点,从而实现闭环系统的鲁棒稳定,

系统的滑模函数收敛到零,系统状态轨迹在有限时间内到达了滑模面,故本文所设计的控制算法能保证系统实现渐近稳定.

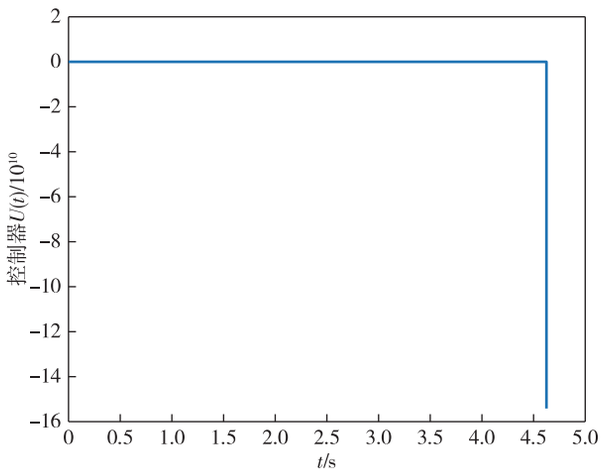


图 6　未考虑 FDI 攻击防御的控制器响应曲线

Fig. 6　Controller response curve without considering defense against FDI attack

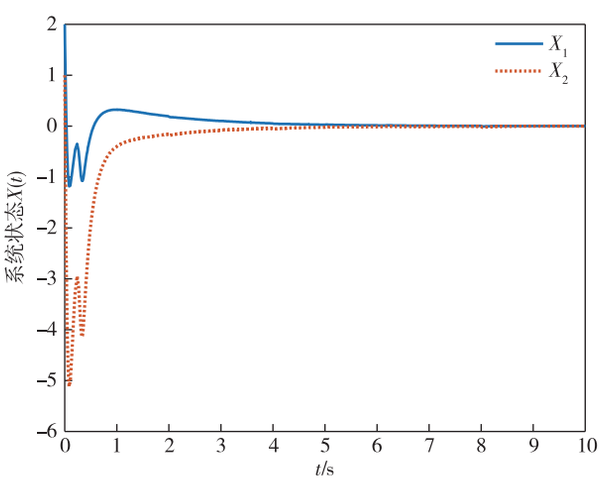


图 7　考虑 FDI 攻击防御的控制器作用下的系统状态响应曲线

Fig. 7　System state response curve under controller considering defense against FDI attack

6　结论

本文针对非线性信息物理系统,研究了当量化失配下执行器遭到 FDI 攻击时,通过线性矩阵不等式求出系统满足 L_2 性能稳定的判据,证明了基于扩张观测器和指数趋近律的自适应滑模控制算法能使系统实现渐近稳定.数值对比仿真验证了本文算法的有效性和优越性.

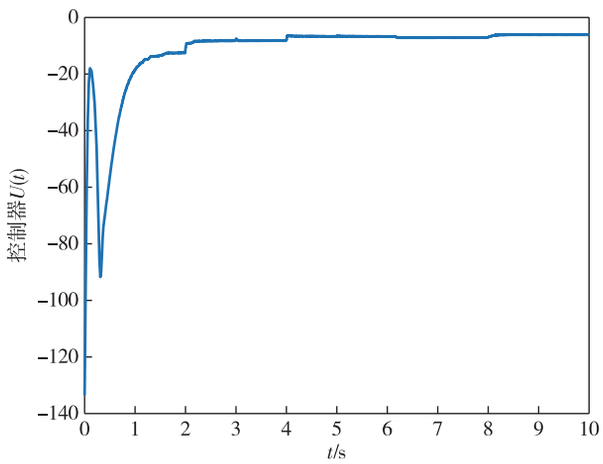


图 8　考虑 FDI 攻击防御的控制器响应曲线

Fig. 8　Controller response curve considering defense against FDI attack

参考文献

References

[1] 景轩,姚锡凡.走向社会信息物理生产系统[J].自动化学报,2019,45(4):637-656
JING Xuan, YAO Xifan. Towards social cyber-physical production systems[J].Acta Automatica Sinica,2019,45(4):637-656

[2] 郭戈,张文安,周彬."信息物理系统理论、方法及应用"专栏序言[J].控制与决策,2019,34(11):2273-2276

[3] 翁品迪,陈博,俞立.虚假数据注入攻击信号的融合估计[J].自动化学报,2021,47(9):2292-2300
WENG Pindi, CHEN Bo, YU Li. Fusion estimate of FDI attack signals[J].Acta Automatica Sinica,2021,47(9):2292-2300

[4] 黄玲,郭婧,张恒艳.基于观测器的周期拒绝服务攻击网络化系统动态事件触发控制[J].控制理论与应用,2021,38(6):851-861
HUANG Ling, GUO Jing, ZHANG Hengyan. Observer-based dynamic event triggering control for networked systems with periodic denial-of-service attack[J]. Control Theory & Applications,2021,38(6):851-861

[5] 杨佳佳,张正道,谢林柏.基于控制性能指标的重放攻击编码检测方案[J].信息与控制,2021,50(3):329-336
YANG Jiajia, ZHANG Zhengdao, XIE Linbo. Coding detection scheme for replay attack based on the control performance index[J]. Information and Control, 2021, 50(3):329-336

[6] 徐彬彬,洪榛,赵磊,等.网络化倒立摆系统的偏差攻击及其检测方法[J].上海交通大学学报,2020,54(7):697-704
XU Binbin, HONG Zhen, ZHAO Lei, et al. Bias attack and detection method for networked inverted pendulum system[J]. Journal of Shanghai Jiao Tong University,

2020,54(7):697-704
[7] Zhang T Y,Ye D.False data injection attacks with complete stealthiness in cyber-physical systems:a self-generated approach[J].Automatica,2020,120:109117
[8] Bai C Z,Pasqualetti F,Gupta V.Data-injection attacks in stochastic control systems:detectability and performance tradeoffs[J].Automatica,2017,82:251-260
[9] Zhao J B,Gómez-Expósito A,Netto M,et al.Power system dynamic state estimation:motivations,definitions,methodologies,and future work[J].IEEE Transactions on Power Systems,2019,34(4):3188-3198
[10] Esmalifalak M,Liu L C,Nguyen N,et al.Detecting stealthy false data injection using machine learning in smart grid[J].IEEE Systems Journal,2017,11(3):1644-1652
[11] Li M,Chen Y,Zhang Y Y,et al.Adaptive sliding-mode tracking control of networked control systems with false data injection attacks[J].Information Sciences,2022,585:194-208
[12] Barzegari Y,Zarei J,Razavi-Far R,et al.Resilient consensus control design for DC microgrids against false data injection attacks using a distributed bank of sliding mode observers[J].Sensors,2022,22(7):2644
[13] Dong L W,Xu H L,Wei X J,et al.Security correction control of stochastic cyber-physical systems subject to false data injection attacks with heterogeneous effects[J].ISA Transactions,2022,123:1-13
[14] Zhao Y,Chen Z,Zhou C J,et al.Passivity-based robust control against quantified false data injection attacks in cyber-physical systems[J].IEEE/CAA Journal of Automatica Sinica,2021,8(8):1440-1450
[15] Ma R J,Shi P,Wu L G.Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks[J].IEEE Transactions on Cybernetics,2021,51(5):2306-2318
[16] Chen B,Niu Y G,Zou Y Y.Security control for Markov jump system with adversarial attacks and unknown transition rates via adaptive sliding mode technique[J].Journal of the Franklin Institute,2019,356(6):3333-3352
[17] Cao Z R,Niu Y G,Song J.Finite-time sliding-mode control of Markovian jump cyber-physical systems against randomly occurring injection attacks[J].IEEE Transactions on Automatic Control,2020,65(3):1264-1271
[18] Lü S,Jin X Z,Ding L J,et al.Adaptive sliding-mode control of a class of disturbed cyber-physical systems against actuator attacks[J].Computers & Electrical Engineering,2021,96:107492
[19] Li J,Yang D F,Gao Y C,et al.An adaptive sliding-mode resilient control strategy in smart grid under mixed attacks[J].IET Control Theory & Applications,2021,15(15):1971-1986
[20] Freidovich L B,Khalil H K.Performance recovery of feedback-linearization-based designs[J].IEEE Transactions on Automatic Control,2008,53(10):2324-2334
[21] Ball A A,Khalil H K.High-gain observers in the presence of measurement noise:a nonlinear gain approach[C]//2008 47th IEEE Conference on Decision and Control.December 9 - 11,2008,Cancun,Mexico.IEEE,2008:2288-2293
[22] 郑柏超,傅曦雨,杨鑫,等.执行器退化的遥机器人系统量化反馈容错控制[J].南京信息工程大学学报(自然科学版),2016,8(6):499-504
ZHENG Bochao,FU Xiyu,YANG Xin,et al.Quantized feedback fault-tolerant control of teleoperated robot systems subject to actuator degradation[J].Journal of Nanjing University of Information Science & Technology(Natural Science Edition),2016,8(6):499-504
[23] 谷志锋,朱长青,杨润生,等.互联多输入系统的分散自适应 L_2 增益控制[J].控制理论与应用,2014,31(6):805-813
GU Zhifeng,ZHU Changqing,YANG Runsheng,et al.Decentralized adaptive L_2-gain control for interconnected multi-input system[J].Control Theory & Applications,2014,31(6):805-813
[24] 王伟超,褚晓广,王文轩,等.基于滑模状态观测器的两自由度磁悬浮球控制[J].南京信息工程大学学报(自然科学版),2021,13(3):355-362
WANG Weichao,CHU Xiaoguang,WANG Wenxuan,et al.Two degree of freedom magnetic levitation ball control based on sliding mode state observer[J].Journal of Nanjing University of Information Science & Technology(Natural Science Edition),2021,13(3):355-362
[25] 贾欣婷.网络量化环境下信息物理系统的安全控制研究[D].南京:南京信息工程大学,2020
JIA Xinting.Research on security control of cyber-physical systems under network quantization environments[D].Nanjing:Nanjing University of Information Science & Technology,2020

Sliding mode control based on extended observer against false data injection attack

LAI Chen[1] ZHENG Bochao[1,2] CHEN Zhipeng[1] WANG Haifeng[1]
1 School of Automation,Nanjing University of Information Science & Technology,Nanjing 210044
2 Collaborative Innovation Center of Atmospheric Environment and Equipment Technology,
Nanjing University of Information Science & Technology,Nanjing 210044

Abstract Aiming at the cyber physical system (CPS) subject to false data injection (FDI) attack, a control method based on sliding mode and extended observer is proposed. First, the system is dynamically linearized, an extended observer is constructed, and the convergence condition of the observation error is analyzed. Second, the integral sliding mode surface is designed, the asymptotic stability criterion of the sliding mode system is derived by using linear matrix inequality, and the sliding mode vector satisfying the gain performance of the system is obtained. Then, based on the exponential reaching law, an adaptive integral sliding mode controller is proposed to eliminate quantization errors and generalized disturbances, so that the system can reach the sliding surface. The advantages of this method include high estimation accuracy, fast response speed, and strong robustness to FDI attack and quantization parameter mismatch. Finally, numerical simulation verifies the effectiveness of the method.

Key words cyber physical system (CPS); false data injection (FDI) attack; extended observer; sliding mode control; securing control