中国科技期刊卓越行动计划项目入选期刊

控制与决策

CONTROL AND DECISION

数据驱动与机理解析方法融合的ICPS自适应综合安全控制

李炜, 陈婧婧, 李亚洁

引用本文:
李炜,陈婧婧,李亚洁. 数据驱动与机理解析方法融合的ICPS自适应综合安全控制[J]. 控制与决策, 2024, 39(9): 3079−3089.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2023.0333

数据驱动与机理解析方法融合的ICPS自适应综合安全控制

李 炜[1,2], 陈婧婧[1], 李亚洁[1,2†]

(1. 兰州理工大学 电气工程与信息工程学院，兰州 730050；
2. 甘肃省工业过程先进控制重点实验室，兰州 730050)

摘 要: 针对一类隐蔽虚假数据注入(FDI)和执行器故障共存的工业信息物理融合系统(ICPS),将数据驱动与机理解析方法有机结合,研究综合安全控制与通讯协同设计问题. 首先,设计一种服从指数型自适应律的离散事件触发通讯机制(ADETCS),并构建可同时抵御网络FDI攻击和物理部件故障的自适应ICPS框架;然后,基于数据驱动技术,通过优选和优化建立FDI攻击的预测模型PSO-CatBoost,对攻击进行准确重构和补偿;接着,借助于增广型Lyapunov-Krasovskii泛函、改进仿射Bessel-Legendre不等式等少保守性技术,推导出鲁棒观测器和综合安全控制器的求解方法;最后,通过四容水箱实例验证所提出方法的有效性. 实验结果表明:将数据驱动的隐蔽FDI重构补偿与机理解析的补偿误差抑制深度融合,主被动协同有效容侵了网络攻击,结合对故障的主动容错,并在ADETCS下随系统行为变化自适应调整触发参数,可显著提升ICPS的双重安全防御能力,节约更多的网络资源.

关键词: 工业信息物理系统；隐蔽FDI攻击；自适应触发机制；数据驱动；机理解析；综合安全控制

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2023.0333

引用格式: 李炜, 陈婧婧, 李亚洁. 数据驱动与机理解析方法融合的ICPS自适应综合安全控制[J]. 控制与决策, 2024, 39(9): 3079-3089.

Adaptive integrated security control of ICPS based on data-driven and mechanism analysis fusion method

LI Wei[1,2], *CHEN Jing-jing*[1], *LI Ya-jie*[1,2†]

(1. College of Electrical and Information Engineering，Lanzhou University of Technology，Lanzhou 730050，China；
2. Key Laboratory of Gansu Advanced Control for Industrial Processes，Lanzhou 730050，China)

Abstract: For a class of industrial cyber-physical systems (ICPS) where stealthy false data injection (FDI) and actuator faults coexist, the data-driven and mechanism analysis methods are combined to study the integrated security control and communication co-design problem. Firstly, a discrete event-triggered communication scheme (ADETCS) obeying exponential adaptive law is designed, and an adaptive ICPS framework is constructed to withstand both network FDI attacks and physical component faults. Secondly, based on data-driven technology, the prediction model PSO-CatBoost of FDI attack is established through optimization to accurately reconstruct and compensate the attack. Then, by means of less conservative techniques such as the augmented Lyapunov-Krasovskii functional and improved affine Bessel-Legendre inequality, the solution methods of the robust observer and integrated safety controller are deduced. Finally, the effectiveness of the proposed method is verified through the example of a quadruple tank. The results show that the deep integration of data-driven stealthy FDI reconstruction compensation and mechanism analysis compensation error suppression, the effective tolerance of active-passive cooperation to network atacks, the combination with active fault tolerance, and adaptive adjustment of trigger parameter with the change of system behavior under the ADETCS can significantly increase ICPS dual security defense capability, save more network resources.

Keywords: industrial cyber-physical systems；stealthy false data injection attack；adaptive triggered scheme；data-driven；mechanism analysis；integrated safety control

收稿日期: 2023-03-22；**录用日期:** 2023-08-21.
基金项目: 国家自然科学基金项目(62163022).
责任编委: 李少远.
†通讯作者. E-mail: liyaj@lut.edu.cn.
*本文附带电子附录文件,可登录本刊官网该文“资源附件”区自行下载阅览.

0 引 言

工业信息物理融合系统(industry cyber-physical systems, ICPS)是决策、控制单元和物理对象在网络环境中高度集成交互而成的工业智能系统,广泛应用于智能电网、航空航天和智能制造等重要领域[1]. 然而,开放网络环境面临的各类攻击、复杂工业环境导致的元部件故障,也已成为ICPS安全运维和未来发展的掣肘[2]. 仅就近年来频发的网络安全事件而言,如2015年乌克兰发生的BlackEnergy 3, 2017年中东石油天然气公司安全仪表系统出现的TRITON攻击,以及2019年挪威铝生产商海德鲁公司遭遇的勒索病毒攻击事件等[3],均严重影响了ICPS的正常运行,造成了巨大的经济损失. 此外,ICPS的状态全面感知、海量数据传输以及智能分析决策与有限的计算、通讯资源间的矛盾也日益凸显[4].

从信息系统安全角度来看,日益开放的网络使得ICPS更易遭受攻击. 典型攻击主要包括拒绝服务、数据重放和虚假数据注入(false data injection, FDI)攻击[5]等. 其中: FDI攻击通过篡改网络层数据,使得控制中心做出误导性决策,并具有隐蔽性强、危害性大、设计复杂等特点,具体表现为可躲避传统检测方法、对系统可靠性甚至稳定性造成了长期影响、FDI攻击策略设计通常需要系统模型知识或实时数据[6]等. 因此,研究FDI的攻击行为对保障ICPS安全可靠运维至关重要.

FDI攻击难测难防且危害大,因此也成为攻击防御关注的热点. 学者们已从通讯和控制两个侧面展开了较为广泛的研究. 从通讯角度而言,主要采用身份认证、访问控制和数据加密等技术[7]来确保FDI攻击下ICPS信息安全问题,但是滋生出的延时往往在实时控制要求较高的ICPS中受限;从控制角度而言,主要采用攻击检测与补偿[8]、控制器对攻击弹性[9]或鲁棒[10]等方法来抵御FDI攻击对系统的损伤,但是多为机理解析法,或对其做出可检测和可分离的严苛假设[11],或将其视为一类系统未知输入,缺乏对FDI自身隐蔽属性的本征揭示,实际防御能力有限. 近年来,随着人工智能、机器学习等数据驱动技术的迅速发展,为ICPS的网络安全问题提供了新的解决方法和途径[12]. 因此,如何将机理解析与数据驱动方法深度融合,透析隐蔽FDI攻击的本征,研究更契合实际的防御策略,无疑是极具挑战性和重要意义的.

从物理系统安全角度来看,庞杂众多的器件故障也不时地威胁着ICPS,学者们已在周期时间触发通讯机制和离散事件触发通讯机制(discrete event-triggered communication scheme, DETCS)下展开了被动、主动和主-被动混合容错研究[13]. 尽管“按需传输”的DETCS已有效提高了网络资源利用率,并使得通信和控制的协同设计成为可能,但是DETCS下静态不变的触发参数,依然难以适应动态变化的系统行为. 近年来出现的自适应离散事件触发通讯机制(adaptive discrete event-triggered communication scheme, ADETCS)可谓是提升通信适应度的利器[14].

在ADETCS中,触发参数的动态变化规律,即自适应律的设计尤为关键. 基于此,学者们分别设计了离散型[15]、连续型[16]等自适应律,它们使得网络资源节约的同时保持了系统所需的控制性能,但是仍然存在切换不平滑、触发参数非全局可调、普适性不足等问题. 因此,对于攻击和故障共存的ICPS容错容侵问题,需要设计一种新型ADETCS,以期提升ICPS性能和资源占用间的动态优化水平.

综上所述,本文针对隐蔽FDI攻击和执行器故障共存的ICPS,兼顾双重安全防御以及通讯资源受限问题,巧妙结合数据驱动和机理解析方法,研究ICPS自适应综合安全控制与通讯协同设计问题. 本文主要内容如下.

1) 提出一种服从指数型自适应律的ADETCS,并在此机制下结合攻击补偿和故障调节思想,构建数据驱动与机理解析方法相融合的ICPS综合安全防御新框架,其兼具主被动协同容侵FDI攻击、主动容错执行器故障的能力;而事件触发参数随着系统行为的自适应全局动态调整,又促进了更多网络资源的节约,并确保了ICPS安全运行.

2) 对于ICPS所遭受的隐蔽FDI攻击,首先,基于数据驱动技术,通过优选和优化建立攻击的PSO-CatBoost预测模型,对其进行准确重构和补偿;然后,通过机理解析的鲁棒观测器设计,对攻击补偿误差Δ进行抑制,将数据驱动与机理解析方法深度融合,使得主被动容侵策略协同防护,有效提升ICPS抵御隐蔽FDI攻击的能力.

3) 对于观测器、综合安全控制器的求取,通过构造增广型L-K (Lyapunov-Krasovskii)泛函,考虑更多的系统信息和时滞信息,结合改进的仿射Bessel-Legendre不等式来减少结果的保守性,扩大求解空间;在控制器的推导中,引入触发参数的关联项来增强控制和通讯的适应性,而新型ADETCS的加持,则更好地平衡了系统性能与通讯资源.

1 系统构建与FDI隐蔽性描述

1.1 数据驱动与机理解析综合安全ICPS的构建

本文仅考虑传感侧遭受FDI攻击和执行器故障的ICPS. 鉴于隐蔽FDI攻击难测难防的特质和有效节约通讯资源的期冀,考虑数据驱动和机理解析方法的各自优势,构建如图1所示的ADETCS综合安全防御新架构. 其数据传输过程可简述如下. 首先,智能传感单元对系统输出进行等周期采样后,通过ADETCS筛选出满足自适应触发条件的数据,并经传感侧网络传输至控制单元;然后,对遭受FDI攻击的系统输出数据,由攻击补偿器对FDI信息进行重构并主动补偿后,再经观测器得到状态和故障估计值;接着,控制器据此计算相应控制量,并经执行侧网络送至执行单元;最后,执行单元的0阶保持器对控制量进行非均匀周期保持,并将保持结果传输至执行器,控制量最终作用于被控对象.

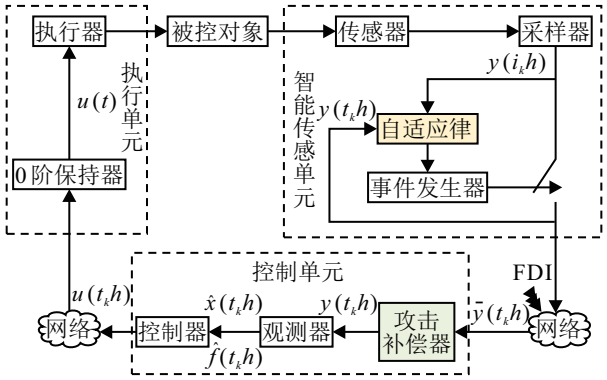


图1　ICPS综合安全控制架构

注1　与前期研究[13-14]不同的是,本文所构建的ICPS框架有两个显著优势:一是为事件发生器中的触发参数设计了更优的自适应律,以一种对系统性能需求更具适应性的新型ADETCS,取代了触发参数静态不变或适应性不足的通讯机制,以期在确保系统性能的同时,进一步降低计算和网络通讯负担;二是在控制单元增加了基于数据驱动技术的攻击补偿器,利用机器学习算法的多样性和灵活性重构隐蔽FDI攻击信号,先对其进行主动补偿,再基于机理解析方法设计鲁棒观测器,对攻击补偿误差予以抑制,以期主被动协同提升ICPS对隐蔽FDI攻击的容侵能力,并规避其可检测、可分离的严苛假设.

考虑如下具有执行器故障、外部扰动和噪声的连续时间被控对象:

$$\begin{cases} \dot{x}(t) = \boldsymbol{A}x(t) + \boldsymbol{B}u(t) + \boldsymbol{E}_f f(t) + \boldsymbol{E}_w w(t), \\ y(i_kh) = \boldsymbol{C}x(i_kh) + \boldsymbol{E}_v v(i_kh). \end{cases} \tag{1}$$

其中: $x(t) \in \mathbb{R}^n$、$u(t) \in \mathbb{R}^{n_u}$ 分别为系统状态和控制输入向量; $y(i_kh) \in \mathbb{R}^{n_y}$ 为传感器量测采样输出向量; $v(i_kh) \in \mathbb{R}^{n_v}$ 为测量噪声; $w(t) \in \mathbb{R}^{n_w}$ 为外部干扰信号; $f(t) \in \mathbb{R}^{n_f}$ 为执行器连续时变故障,假设故障导数范数有界,即存在常数 f_1 使得 $\|\dot{f}(t)\| \leqslant f_1$; $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{E}_f$、$\boldsymbol{E}_w$ 和 $\boldsymbol{E}_v$ 为已知适当维数的矩阵.

1.2 新型ADETCS设计

为了进一步提升通信机制对系统性能约束的适应性,并节约更多的通信和计算资源,设计如下自适应触发条件来筛选当前量测采样值是否需经传感侧网络传输至控制单元:

$$e_y(i_kh)^{\mathrm{T}}\boldsymbol{\Phi}e_y(i_kh) \geqslant \sigma(t_kh)y^{\mathrm{T}}(t_kh)\boldsymbol{\Phi}y(t_kh). \tag{2}$$

其中: $\boldsymbol{\Phi}^{n\times n}$ 为待设计的事件触发权矩阵;事件触发误差 $e_y(i_kh) = y(i_kh) - y(t_kh)$,这里 $y(i_kh)$ 为当前时刻量测采样值, $y(t_kh)$ 为上一时刻满足事件触发条件的传感器量测值,且 $i_kh = t_kh + lh(l \in \mathbb{N})$, h 为采样周期.

与DETCS中预先给定静态触发参数 σ 不同的是,式(2)中的 $\sigma(t_kh)$ 可根据系统动态行为自适应调整,具体如下所示:

$$\sigma(t_kh) = \begin{cases} \sigma_M, \ |e_y(t_kh)| \leqslant \Delta_1; \\ \sigma_M \mathrm{e}^{-\alpha e_y(i_kh)^{\mathrm{T}}\boldsymbol{\Phi}e_y(i_kh)}, \\ \qquad \Delta_1 < |e_y(t_kh)| \leqslant \Delta_2; \\ \sigma_m, \ \Delta_2 < |e_y(t_kh)|. \end{cases} \tag{3}$$

其中: $e_y(t_kh) = (\|y(t_kh)\| - \|y(t_{k-1}h)\|)/\|y(t_kh)\|$ 为传输事件误差的归一值; σ_M 和 σ_m 为触发参数上下界, $\sigma(t)$ 的初值 $\sigma(0) = \sigma_m$,且满足 $0 \leqslant \sigma_m < \sigma_M \leqslant 1$; $\Delta_1 < \Delta_2$ 为允许的事件误差阈值界,其值取决于系统性能约束; $\alpha > 0$ 为已知常数.

注2　ADETCS中自适应律(3)的设计引入了指数型函数,并通过选取适当的事件误差阈值 Δ_1、Δ_2,使得触发参数 $\sigma(t_kh)$ 随系统行为变化,可在 $[\Delta_1, \Delta_2]$ 对应的触发参数 $[\sigma_m, \sigma_M]$ 区间全局连续动态调整. 即当 $e_y(t_kh) \leqslant \Delta_1$,系统平稳时, $\sigma(t_kh) = \sigma_M$,对应较低的事件触发和数据传输频率来节约网络资源;当 $\Delta_2 < |e_y(t_kh)|$,系统因突遭扰动、攻击和故障等明显波动时, $\sigma(t_kh) = \sigma_m$,对应较高的事件触发和数据传输频率来保持期望的控制性能;当 $\Delta_1 < |e_y(t_kh)| \leqslant \Delta_2$ 时, $\sigma(t_kh)$ 随着系统动态事件误差的增大或减小,在 σ_m 与 σ_M 间自适应平滑地减小或增大.

注3　式(2)中的触发参数 $\sigma(t_kh)$,在根据系统性能约束 $[\Delta_1, \Delta_2]$,按照式(3)的规律随着系统动态行为自适应调整的同时,也与 α 的取值大小密切相关. α 越大, $\sigma(t_kh)$ 的变化率越大,反之亦然;当触发参数上下限 $\sigma_m = \sigma_M = 0$ 且 $\alpha = 0$ 时,得到 $t_{k+1}h = t_kh + h$,所提出ADETCS则退化为周期时间触发通信机制;当 $\sigma_m = \sigma_M \neq 0$ 且 $\alpha = 0$ 时,则退化为静态触发参数不变的DETCS.

考虑到图1中被控对象是连续的,而传感、控制

单元均为数字量的自适应筛选和传输,因此,所构建ICPS综合安全控制架构为一类典型的均匀采样但非均匀传输数据系统. 对于此类系统的分析和综合,可将非均匀传输对系统的影响转化为时延,进而采用相对成熟的时滞系统理论[17]对其进行研究. 此外,鉴于CPU计算力的提升和5 G技术的普及,网络传输和计算时延等亦可忽略.

在ADETCS下,其数据传输序列与在DETCS下类似,故对于此类非均匀传输问题,可定义如下时延函数:

$$\tau = t - t_k h,\ t \in [t_k h, t_{k+1} h). \tag{4}$$

其中:时延函数满足$h \leqslant \tau(t) < h_1$, h_1为系统允许最大时延,且依赖于ADETCS中σ_M所确定的触发间隔.

1.3 隐蔽FDI攻击本征描述

考虑传感侧网络存在FDI攻击的威胁,结合时延函数(4),传输至控制单元的量测输出可表示为

$$\bar{y}(t) = \boldsymbol{C}x(t-\tau(t)) + \boldsymbol{E}_v v(t-\tau(t)) + \boldsymbol{E}_a a_s(t). \tag{5}$$

其中:$\bar{y}(t)$为受到FDI攻击后的量测输出信号,$a_s(t) \in \mathbb{R}^{n_a}$为传感侧FDI攻击信号,$\boldsymbol{E}_a$为适当维数的攻击加权矩阵.

工业控制领域的异常检测广泛基于残差机制,因此,可从攻击者视角以躲避其检测的思维方式来描述具有隐蔽特征的FDI攻击模型.

由式(1)和(5),得到如下系统描述:

$$\begin{cases} \dot{x}(t) = \boldsymbol{A}x(t) + \boldsymbol{B}u(t) + \boldsymbol{E}_f f(t) + \boldsymbol{E}_w w(t), \\ \bar{y}(t) = \boldsymbol{C}x(t-\tau(t)) + \boldsymbol{E}_v v(t-\tau(t)) + \boldsymbol{E}_a a_s(t). \end{cases} \tag{6}$$

在基于残差的异常检测中,通常可设计如下观测器:

$$\begin{cases} \dot{\hat{x}}(t) = \boldsymbol{A}\hat{x}(t) + \boldsymbol{B}u(t) - \boldsymbol{L}_1(\bar{y}(t) - \hat{\bar{y}}(t)), \\ \hat{\bar{y}}(t) = \boldsymbol{C}\hat{x}(t-\tau(t)). \end{cases} \tag{7}$$

其中:$\hat{x}(t)$、$\hat{\bar{y}}(t)$分别为系统状态和输出的观测值;$\boldsymbol{L}_1$为待求的观测器增益矩阵,具体求解参见本文第3节中的定理1.

定义$e_x(t) = \hat{x}(t) - x(t)$, $r(t) = \bar{y}(t) - \hat{\bar{y}}(t)$,得到

$$\begin{cases} \dot{e}_x(t) = \boldsymbol{A}e_x(t) + \boldsymbol{E}_f f(t) + \boldsymbol{L}_1\boldsymbol{C}e_x(t-\tau(t)) + \\ \qquad \boldsymbol{L}_1\boldsymbol{E}_v v(t-\tau(t)) + \boldsymbol{L}_1\boldsymbol{E}_a a_s(t) + \boldsymbol{E}_w w(t), \\ r(t) = \\ \boldsymbol{C}e_x(t-\tau(t)) + \boldsymbol{E}_v v(t-\tau(t)) + \boldsymbol{L}_1\boldsymbol{E}_a a_s(t). \end{cases} \tag{8}$$

这里$r(t)$为系统输出的残差. 定义$g(t) = r^{\mathrm{T}}(t)r(t)$,则异常检测机制可表示为

$$\begin{cases} H_0 : g(t) \leqslant J_{\mathrm{th}}, \\ H_1 : g(t) > J_{\mathrm{th}}. \end{cases} \tag{9}$$

其中:J_{th}为检测阈值,一般取值为$g_{\max} = r^{\mathrm{T}}_{\max}(t) \times r_{\max}(t)$,即在无攻击、扰动最大情况下的残差值;$H_0$和$H_1$分别表示系统正常和异常状态.

对于异常检测机制(9),攻击者为了躲避检测,需综合考虑检测阈值、系统输出以及外部扰动等信息,精心设计FDI攻击信号,方可躲过检测而伤及系统.

假设攻击模型可参数化[18]为

$$a_s(t) = \boldsymbol{\Lambda}\boldsymbol{\Phi}(y,t). \tag{10}$$

其中:$\boldsymbol{\Lambda}$为攻击策略;$\boldsymbol{\Phi}(y,t)$为攻击者所掌握的系统信息,如传感器输出y等.

当系统中仅遭受隐蔽FDI攻击,即当$f(t) = 0$、$w(t) = 0$、$v(t) = 0$、$a_s(t) \neq 0$时,由式(8)可得到如下系统描述:

$$\begin{cases} \dot{e_x}(t) = \boldsymbol{A}e_x(t) + \boldsymbol{L}_1\boldsymbol{C}e_x(t-\tau(t)) + \boldsymbol{L}_1\boldsymbol{E}_a a_s(t), \\ r_a(t) = \boldsymbol{C}e_x(t-\tau(t)) + \boldsymbol{L}_1\boldsymbol{E}_a a_s(t). \end{cases} \tag{11}$$

其中$r_a(t)$为在攻击(10)的作用下系统所产生的残差. 定义$g_a = r_a^{\mathrm{T}}(t)r_a(t)$,根据检测机制(9),为了成功躲避异常检测机制,攻击(10)需满足以下不等式:

$$\begin{cases} g_a(t) \leqslant J_{\mathrm{th}}, \\ \|g_a(t)\|^2 \leqslant \varepsilon \|a_s(t)\|^2. \end{cases} \tag{12}$$

这里:$\varepsilon > 0$为误差系统(11)中残差$r_a(t)$与攻击$a_s(t)$间的H_∞性能指标约束,进一步可得到隐蔽FDI攻击$a_s(t)$的限制条件为$\|a_s(t)\| \leqslant J_1$,其中$J_1 = \sqrt{(1/\varepsilon)J_{\mathrm{th}}}$.

对于通讯网络存在FDI攻击的误差系统(11),设计攻击信号$a_s(t)$,若使得

$$\lim_{t\to\infty} \|e_x(t)\| \geqslant e_{\mathrm{th}},\ \|r_a(t)\| \leqslant J_{\mathrm{th}}, \tag{13}$$

其中e_{th}和J_{th}分别为系统稳定运行时允许的误差和残差阈值,则称$a_s(t)$为具有隐蔽性的FDI攻击[19].

2 数据驱动隐蔽FDI攻击信号的重构与补偿

从前述分析讨论可知,当隐蔽FDI攻击出没于网络时,ICPS中的异常检测机制对此并不敏感. 因此,如何设计有效的攻击补偿器,消除隐蔽FDI攻击对系统性能的影响,是极富挑战性的研究工作.

从防御者角度来看:一方面,FDI攻击扑朔迷离,既难于精确机理表达,又难以满足可检测、可分离的严苛条件,因而限制了对其准确估计和补偿;另一方面,遭到FDI攻击下的系统,又会源源不断地产生隐

含攻击机理和系统运行状态的海量数据,因此,利用数据驱动技术对FDI重构和补偿无疑是可行之径.

2.1 CatBoost算法

CatBoost是2018年俄罗斯Yandex团队基于梯度提升树(gradient boost decision tree, GBDT)改进的一种集成学习算法框架[20],其在建模准确性和鲁棒性方面更优,因此本文基于此模型对攻击信号进行重构. 算法原理可表示为

$$\hat{y}_i^{(k+1)} = \hat{y}_i^{(k)} + \eta f_{k+1}(x_i),$$
$$\hat{y}_i = \sum_{k=1}^{K} \hat{y}_i^{(k)}. \tag{14}$$

其中: η为学习率, $f_{k+1}(x_i)$为第i个样本在第$k+1$棵树上的输出值, $\hat{y}_i^{(k+1)}$为第i个样本在第$k+1$棵树上的预测值, $\hat{y}_i$为第i个样本的最终预测值. 其目标函数可表示为

$$\text{Obj} = \sum_{i=1}^{N} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k). \tag{15}$$

其中: $l(\cdot)$为最小二乘损失函数; $\Omega(\cdot)$用于控制模型复杂度,从而不予考虑易过拟合的子模型.

传统GBDT算法中,将标签平均值作为叶子节点分割的依据,即

$$\hat{x}_k^i = \frac{\sum_{j=1}^{N} [x_j^i = x_k^i] y_j}{\sum_{j=1}^{N} [x_j^i = x_k^i]}. \tag{16}$$

其中: x_k^i为第k个训练样本的第i个特征, $\hat{x}_k^i$为其平均值; y_j为第j个样本的标签; 当$x_j^i = x_k^i$时, $[\cdot]=1$, 否则为0.

通常特征比标签包含更多的信息,若使用标签的平均值来表示特征,则当训练集与测试集的数据结构和分布不同时,会出现条件偏移问题. CatBoost算法加入先验项和权重系数,从而减少噪声和低频率特征数据对数据分布的影响,有

$$\hat{x}_k^i = \frac{\sum_{j=1}^{N} [x_j^i = x_k^i] y_j + ap}{\sum_{j=1}^{N} [x_j^i = x_k^i] + a}. \tag{17}$$

其中: p为添加的先验项, a为权重系数.

2.2 基于PSO-CatBoost隐蔽FDI攻击重构的补偿

考虑CatBoost中超参数众多,其中对称树数目(iterations)和树深(depth)对模型性能影响较大,故将二者作为寻优参数,利用PSO算法对其初始值寻优,并以CatBoost训练模型的均方根误差RMSE作为PSO的适应度函数.

基于PSO-CatBoost的隐蔽FDI攻击重构和补偿,可分为两个阶段,具体如图2所示. 阶段1为FDI攻击信息的重构,其本质是通过建立FDI攻击的预测模型来获得精准的$\hat{a}_s(t)$; 阶段2为基于攻击重构信息的补偿,即在式(6)输出方程中引入$-\boldsymbol{E}_a\hat{a}_s(t)$,消除隐蔽FDI攻击的影响. 显然,建立优质的FDI攻击预测模型是关键.

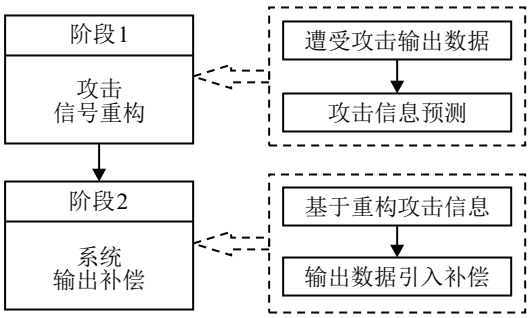


图 2　FDI攻击重构和补偿过程

基于PSO-CatBoost算法,分别以遭受攻击(10)下的系统输出序列作为输入、系统所遭受的攻击信息作为输出,通过采集相应的样本进行训练测试,即可获得FDI攻击的重构模型.

系统实际运行时,基于上述模型可对隐蔽FDI攻击进行预测,并据此对隐蔽FDI攻击进行补偿,从而以数据驱动的方式抵御FDI攻击的影响,达到主动容侵的目的. 具体实施步骤如下.

step 1: 采集FDI攻击下的系统输出序列$\bar{y}_i(k)$,与无攻击系统的输出$y_i(k)$作差,得到攻击量$a_s(k)$,分别以$\bar{y}_i(k)$和$a_s(k)$作为预测模型的输入和输出,划分训练集和测试集;

step 2: 利用PSO-CatBoost算法得到攻击量的预测模型,并将其与补偿策略$-\boldsymbol{E}_a\hat{a}_s(t)$封装于图1的"攻击补偿器"中;

step 3: 系统运行时,基于前述预测模型得到攻击重构信息$\hat{a}_s(k)$,并按照式(18)主动补偿系统遭受FDI攻击的影响.

3 鲁棒观测器设计

利用PSO-CatBoost模型对隐蔽FDI攻击信号进行重构后,进而可依据重构的攻击信号$\hat{a}_s(t)$对系统(6)的输出方程进行补偿,由此系统输出可表示为

$$y(t) = \bar{y}(t) - \boldsymbol{E}_a\hat{a}_s(t) =$$
$$\boldsymbol{C}x(t-\tau(t)) + \boldsymbol{E}_v v(t-\tau(t)) + \Delta, \tag{18}$$

其中$\Delta = \boldsymbol{E}_a(a_s(t) - \hat{a}_s(t))$为隐蔽FDI攻击信号的补偿误差. 考虑隐蔽FDI攻击的重构模型势必存在一定误差,且随系统运行存在不确定性,这里可视其为一

种特殊的测量噪声. 结合式(1)系统描述如下:

$$\begin{cases}\dot{x}(t)=\boldsymbol{A}x(t)+\boldsymbol{B}u(t)+\boldsymbol{E}_f f(t)+\boldsymbol{E}_w w(t),\\ y(t)=\boldsymbol{C}x(t-\tau(t))+\boldsymbol{E}_v v(t-\tau(t))+\Delta.\end{cases}\tag{19}$$

在FDI攻击主动容侵策略下,设计如下鲁棒观测器来实现系统状态和执行器故障的准确估计:

$$\begin{cases}\dot{\hat{x}}(t)=\boldsymbol{A}\hat{x}(t)+\boldsymbol{B}u(t)+\boldsymbol{E}_f\hat{f}(t)-\boldsymbol{L}[\hat{y}(t)-y(t)],\\ \hat{y}(t)=\boldsymbol{C}\hat{x}(t-\tau(t)),\\ \dot{\hat{f}}(t)=-\boldsymbol{F}[\hat{y}(t)-y(t)].\end{cases}\tag{20}$$

其中: $\boldsymbol{L}^{n\times n}$ 和 $\boldsymbol{F}^{1\times n}$ 分别为待设计的状态、故障增益矩阵, $\hat{f}(t)$ 为故障估计值.

定义: $e_x(t)=\hat{x}(t)-x(t), e_f=\hat{f}(t)-f(t), e_y(t)=\hat{y}(t)-y(t)$,由式(19)和(20),得到如下误差系统:

$$\begin{cases}\dot{e}_x(t)=\boldsymbol{A}e_x(t)+\boldsymbol{E}_f e_f(t)+\boldsymbol{L}\boldsymbol{C}e_x(t-\tau(t))+\\ \qquad\boldsymbol{L}\boldsymbol{E}_v v(t-\tau(t))-\boldsymbol{E}_w w(t)+\boldsymbol{L}\Delta,\\ \dot{e}_f(t)=-\boldsymbol{F}\boldsymbol{C}e_x(t-\tau(t))+\boldsymbol{F}\boldsymbol{E}_v v(t-\tau(t))-\\ \qquad\dot{f}(t)+\boldsymbol{F}\Delta.\end{cases}\tag{21}$$

为了便于分析,将 $e_x(t)$ 和 $e_f(t)$ 增广为一个整体. 定义 $\bar{e}(t)=[e_x^{\mathrm{T}}(t)\quad e_f^{\mathrm{T}}(t)]^{\mathrm{T}}$,则由式(21),得到如下增广误差系统:

$$\begin{aligned}\dot{\bar{e}}=&\bar{\boldsymbol{A}}\bar{e}(t)-\bar{\boldsymbol{L}}\bar{\boldsymbol{C}}\bar{e}(t-\tau(t))-\bar{\boldsymbol{E}}_w\bar{w}(t)+\\ &\bar{\boldsymbol{L}}(\boldsymbol{E}_v v(t-\tau(t))+\Delta).\end{aligned}\tag{22}$$

其中

$$\bar{\boldsymbol{A}}=\begin{bmatrix}\boldsymbol{A}&\boldsymbol{E}_f\\ \boldsymbol{0}&\boldsymbol{0}\end{bmatrix},\ \bar{e}(t)=\begin{bmatrix}e_x(t)\\ e_f(t)\end{bmatrix},\ \bar{\boldsymbol{C}}=[\boldsymbol{C}\quad\boldsymbol{0}],$$

$$\bar{\boldsymbol{L}}=\begin{bmatrix}\boldsymbol{L}\\ \boldsymbol{F}\end{bmatrix},\ \bar{\boldsymbol{E}}_w=\begin{bmatrix}\boldsymbol{E}_w&\boldsymbol{0}\\ \boldsymbol{0}&\boldsymbol{I}\end{bmatrix},\ \bar{w}(t)=\begin{bmatrix}w(t)\\ \dot{f}(t)\end{bmatrix}.$$

定理1 给定标量 γ_1、h_1、$n_i(i=1,2,3)$,若存在对称正定矩阵 $\boldsymbol{P}$ 以及实矩阵 $\boldsymbol{X}$、$\boldsymbol{Y}$ 满足以下线性矩阵不等式:

$$\begin{bmatrix}\boldsymbol{N}_{11}&\boldsymbol{N}_{12}\\ *&\boldsymbol{N}_{22}\end{bmatrix}<\boldsymbol{0},\ \begin{bmatrix}\boldsymbol{U}_{11}&\boldsymbol{U}_{12}\\ *&\boldsymbol{U}_{22}\end{bmatrix}<\boldsymbol{0},\tag{23}$$

其中 $\boldsymbol{L}$ 和 $\boldsymbol{F}$ 可通过 $\bar{\boldsymbol{L}}=\boldsymbol{P}^{-1}\boldsymbol{Y}=[\boldsymbol{L}^{\mathrm{T}}\quad\boldsymbol{F}^{\mathrm{T}}]^{\mathrm{T}}$ 求得,则分别存在状态、故障增益矩阵 $\boldsymbol{L}$、$\boldsymbol{F}$,使得增广误差系统(22)在无扰动时渐近稳定,在有扰动时满足性能指标 $\|\bar{e}(t)\|_2^2\leqslant\gamma_1^2(\|\bar{w}(t)\|_2^2+h_1\|v(t_kh)+\Delta\|_2^2)$.

限于篇幅, $\boldsymbol{N}_{11}\sim\boldsymbol{U}_{22}$ 元素表达式以及定理1的证明略.

注4 对于数据驱动补偿FDI攻击后的误差 Δ,本文利用机理解析方法,在观测器的设计部分,将其视为一类特殊噪声并鲁棒应对,从而使得数据驱动的主动容侵策略与机理解析的被动容侵策略巧妙融合,以期有效提升ICPS抵御FDI攻击的能力.

注5 文中构造的L-K泛函,在原有基础[13]上引入了如 $V_3(t)$、$V_4(t)$ 中的 $h_1^2\int_{t_kh}^{t}\dot{e}^{\mathrm{T}}(s)\boldsymbol{Q}\dot{e}(s)\mathrm{d}s$ 等增广项,使得系统状态、时延紧密耦合;在处理L-K泛函沿系统的导数时,采用改进的仿射Bessel-Legendre不等式. 二者结合有利于少保守性观测器和后续综合安全控制器的获得.

4 综合安全控制器设计

基于第3节得到的状态和故障估计值,本节给出综合安全控制器与通讯协同设计方法. 在状态和故障的估计中,已采用前述数据驱动与机理解析相融合的方法,以主被动协同方式对隐蔽FDI攻击的影响进行了重构补偿和鲁棒. 因此,这里的控制器除应具有故障容错功能,也隐含了容侵功能,依旧可称之为综合安全控制器. 结合时延函数(4),综合安全控制策略可表示为

$$u(t)=-\boldsymbol{K}\hat{x}(t-\tau(t))-\boldsymbol{B}^*\boldsymbol{E}_f\hat{f}(t-\tau(t)).\tag{24}$$

其中: $\boldsymbol{K}^{n_u\times n}$ 为待设计的控制器增益矩阵,故障调节矩阵 $\boldsymbol{B}^*$ 满足 $(\boldsymbol{I}-\boldsymbol{B}\boldsymbol{B}^*)\boldsymbol{E}_f=\boldsymbol{0}$; $\boldsymbol{K}\hat{x}(t-\tau(t))$ 为基于状态观测的反馈控制量; $\boldsymbol{B}^*\boldsymbol{E}_f\hat{f}(t-\tau(t))$ 为对执行器故障的主动补偿量.

结合式(1)和(24),得到如下ICPS闭环模型:

$$\begin{aligned}&\dot{x}(t)=\\ &\boldsymbol{A}x(t)-\boldsymbol{B}\boldsymbol{K}x(t-\tau(t))-\boldsymbol{B}\boldsymbol{K}e_x(t-\tau(t))-\\ &\boldsymbol{E}_f e_f(t-\tau(t))+\boldsymbol{E}_w w(t)+\tau(t)\boldsymbol{E}_f\dot{f}(t).\end{aligned}\tag{25}$$

由定理1可知,式(25)中的状态估计误差、故障估计误差 $e_x(t-\tau(t))$、$e_f(t-\tau(t))$ 均渐近收敛,因此这些估计误差亦可视为一种特殊扰动;对于描述连续故障内采样特性的 $\tau(t)\boldsymbol{E}_f\dot{f}(t)$,本文借助交叉项不等式处理技术来获取更少保守性的结果.

定理2 给定标量 γ_2、h_1、σ、α、m_i、$\rho_i(i=1,2,3)$,若存在正定对称矩阵 $\bar{\boldsymbol{P}}$ 以及实矩阵 $\boldsymbol{Q}_1$、$\boldsymbol{Q}_2$、$\boldsymbol{Q}_3$、$\boldsymbol{Q}_4$、$\boldsymbol{Q}_5$、$\boldsymbol{Q}_6$、$\bar{\boldsymbol{X}}$、$\bar{\boldsymbol{K}}$ 满足如下线性矩阵不等式以及自适应事件触发条件(2),则存在控制器增益矩阵 $\boldsymbol{K}$ 和事件触发权矩阵 $\boldsymbol{\Phi}$,使得闭环系统(25)在无扰动时渐近稳定,在有扰动时满足性能指标 $\|x\|_2^2\leqslant\gamma_2^2\times(\|\bar{w}\|_2^2+h_1(\|e_x(t_kh)\|_2^2+\|e_f(t_kh)\|_2^2))$,控制器增益矩阵 $\boldsymbol{K}=(\bar{\boldsymbol{P}}\boldsymbol{B})^{-1}\bar{\boldsymbol{K}}$ 与事件触发权矩阵 $\boldsymbol{\Phi}$ 可协同求取,其中 $\sigma=\sigma_m$,有

$$\begin{bmatrix}\boldsymbol{\Pi}_{11}&\boldsymbol{\Pi}_{12}\\ *&\boldsymbol{\Pi}_{22}\end{bmatrix}<\boldsymbol{0},\ \begin{bmatrix}\boldsymbol{Z}_{11}&\boldsymbol{Z}_{12}\\ *&\boldsymbol{Z}_{22}\end{bmatrix}<\boldsymbol{0}.\tag{26}$$

$$\begin{bmatrix} \boldsymbol{Q}_2 & \boldsymbol{E}_f^{\mathrm{T}}\bar{\boldsymbol{P}} \\ * & \boldsymbol{Q}_1 \end{bmatrix} > \boldsymbol{0},\ \begin{bmatrix} \boldsymbol{Q}_4 & \boldsymbol{E}_f^{\mathrm{T}}\bar{\boldsymbol{R}} \\ * & \boldsymbol{Q}_3 \end{bmatrix} > \boldsymbol{0},$$

$$\begin{bmatrix} \boldsymbol{Q}_6 & \boldsymbol{E}_f^{\mathrm{T}}\bar{\boldsymbol{Q}} \\ * & \boldsymbol{Q}_5 \end{bmatrix} > \boldsymbol{0}. \tag{27}$$

这里, $\boldsymbol{\Pi}_{11} \sim \boldsymbol{Z}_{22}$ 元素表达式不再给出.

定理2的证明与定理1类似, 不再赘述.

注6　为了提升控制与通信间的适应性, 在定理2的证明中, 在定理1证明的L-K泛函基础上, 又添加了自适应触发参数的直接关联项 $V_5(t)=\sigma(t)/\alpha\sigma_M$ 来进一步提升控制器设计对ADETCS的依赖性, 减少解的保守性, 并对隐蔽FDI攻击以及执行器故障更具弹性.

注7　在ADETCS下, 触发参数 σ 可随系统行为自适应变化, 且 $\sigma\in[\sigma_m,\sigma_M]$, 更有利于节约通讯资源. 但是控制器的设计依赖于触发参数 σ, 考虑ICPS会同时遭遇隐蔽FDI攻击和执行器故障的双重影响, 故在综合安全控制器的设计中, 选取 $\sigma=\sigma_m$, 在确保系统安全的前提下, 节约更多的通讯资源.

5　仿真实验和结果分析

5.1　实例描述

为了验证所提出方法的可行性, 引用典型工业案例四容水箱进行试验, 模型参数[21]为

$$\boldsymbol{A}=\begin{bmatrix} -0.016 & 0 & 0.042 & 0 \\ 0 & -0.011 & 0 & 0.033 \\ 0 & 0 & -0.042 & 0 \\ 0 & 0 & 0 & -0.033 \end{bmatrix},$$

$$\boldsymbol{B}=\begin{bmatrix} 0.083 & 0 \\ 0 & 0.063 \\ 0 & 0.048 \\ 0.031 & 0 \end{bmatrix},\ \boldsymbol{E}_w=\begin{bmatrix} 0.01 \\ 0.01 \\ 0 \\ 0.01 \end{bmatrix},$$

$$\boldsymbol{E}_v=\begin{bmatrix} 0.01 \\ 0 \\ 0.01 \\ 0.01 \end{bmatrix},\ \boldsymbol{C}=0.5\boldsymbol{I}_4,\ \boldsymbol{E}_a=[1\ \ 1\ \ 1\ \ 1]^{\mathrm{T}}.$$

与式(1)系统模型对应, $x_i(t)(i=1,2,3,4)$ 为第 i 个水箱的液位变化量, $y_i(t)$ 为液位变化量的观测值, 水箱由两个水泵(执行器)供水, $u_i(t)(i=1,2)$ 为施加在供水水泵上的电压值. 假设故障发生在第1个输入通道, 连续时变故障 $f(t)$ 描述如下, 可令故障矩阵 $\boldsymbol{E}_f=[-0.083\ \ 0\ \ 0\ \ 0.031]^{\mathrm{T}}$, 有

$$f(t)=\begin{cases} 0,\ t\leqslant 300; \\ 2+2\sin(0.1\pi(t-300)),\ 300<t\leqslant 800. \end{cases}$$

取传感器采样周期 $h=0.1$ s, 假设扰动 $w(t)$ 和噪声 $v(i_kh)$ 分别为0均值、方差为0.01的白噪声过程和序列, 初始状态 $x_0=[4\ \ 4\ \ 2\ \ 2]^{\mathrm{T}}$.

5.2　隐蔽FDI攻击模型描述实验

选择 $\gamma_1=3.2, h_1=2.6, n_1=n_2=0.1, n_3=0.5$, 由式(8)和定理1, 得到

$$\boldsymbol{L}_1=\begin{bmatrix} 1.301\,7 & -3.459\,8 & -4.730\,3 & 5.393\,1 \\ -0.014\,6 & 2.878\,5 & -0.027\,9 & 0.066\,1 \\ 0.078\,1 & 0.131\,8 & 1.574\,1 & -0.220\,9 \\ -0.543\,6 & -1.194\,3 & -2.587\,7 & 4.750\,3 \end{bmatrix}.$$

在无攻击且扰动最大的情况下, 对系统分析、计算得到检测阈值和误差阈值分别为 $J_{\mathrm{th}}=0.55$、$e_{\mathrm{th}}=0.1$. 由式(11)、(12)以及 ε 的求解方法, $\varepsilon=1.6$, 进而得到 $J_1=0.59$.

基于以上分析和计算, 设计一类满足上述有效性和隐蔽性条件的FDI攻击模型, 如下所示:

$$a_s(t)=0.2\|y\|\sin(\pi t)+0.18,\ 200<t\leqslant 600.$$

图3和图4分别为所设计FDI攻击模型的仿真结果. 由图3和图4可见, 在FDI攻击(10)作用下, $e>e_{\mathrm{th}}$, 但是 $g_{\max}<J_{\mathrm{th}}$, 即在系统误差大于误差阈值的情况下, 异常检测机制(9)并不会报警, 表明所设计FDI攻击模型满足其有效和隐蔽的属性.

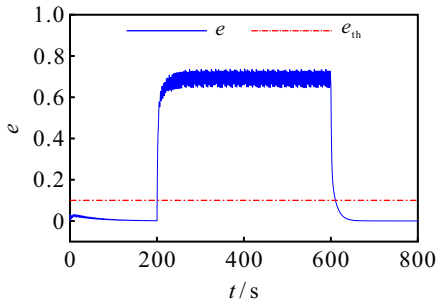


图 3　FDI攻击有效性

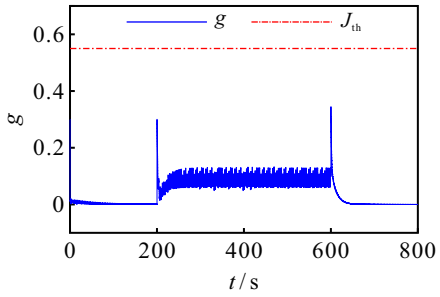


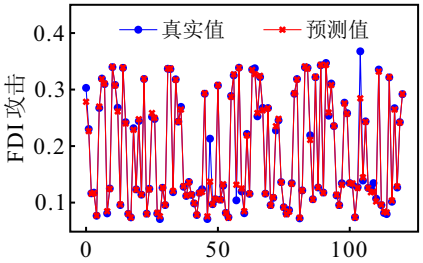
图 4　FDI攻击隐蔽性

5.3　PSO-CatBoost攻击重构模型评价

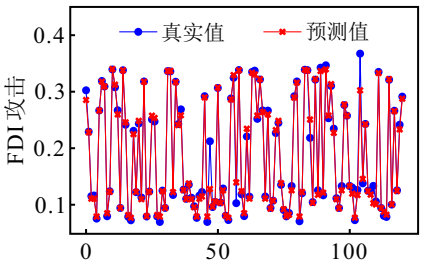
通过四容水箱实例, 分别模拟有无FDI攻击的两类运行工况, 按照第2.2节中的step 1描述, 采集600组 $(y_i(k),a_s(k))$ 运行数据. 随机抽取数据集中80%的样本作为训练集, 剩余20%的样本作为测试集. 将

$y_i(k)$ 作为输入, $a_s(k)$ 作为输出进行 PSO-CatBoost 的训练, 先经 PSO 优化得到 CatBoost 的关键初始参数 depth = 9, iterations = 150, 再利用 CatBoost 算法得到攻击预测模型.

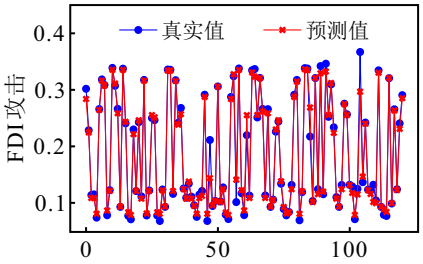
为了体现 PSO-CatBoost 建模的优越性, 将其与未进行参数寻优的 CatBoost、集成学习 Bagging 中的随机森林 (random forest, RF) 以及经典机器学习算法 SVM 进行对比, 并采用网格搜索确定几种模型的初始参数. 以 RMSE 和 R^2 作为性能评价指标. 基于不同模型的 FDI 攻击重构效果如图 5 所示, 具体性能对比如表 1 所示.



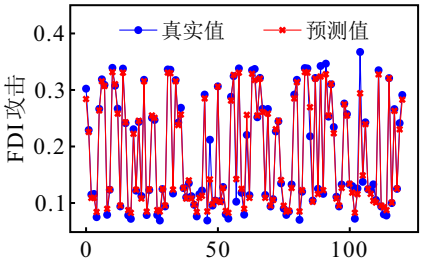
(a) 基于PSO-CatBoost的攻击重构效果



(b) 基于CatBoost的攻击重构效果



(c) 基于RF的攻击重构效果



(d) 基于SVM的攻击重构效果

图 5 基于不同算法模型的攻击重构效果

表 1 不同模型重构性能评价

重构模型	RMSE	R^2
PSO-CatBoost	0.032 2	0.986 7
CatBoost	0.086 2	0.984 1
RF	0.176 8	0.938 8
SVM	0.209 6	0.965 4

由图 5 和表 1 可知, 在 4 种模型重构的 FDI 中, 两种 CatBoost 的重构误差和波动明显小于其他模型, RF 次之, SVM 最差, 表明 CatBoost 模型更适合 FDI 的重构, 而引入 PSO 优化 CatBoost 后的 RMSE 更小, 且决定系数 R^2 值亦优于其他重构模型, 表明 PSO-CatBoost 能够更好地逼近具有较强隐蔽性的 FDI 攻击.

5.4 具有攻击补偿的状态、故障估计与综合安全控制实验研究

5.4.1 状态、故障估计实验研究

给定参数 $\gamma_1 = 3.8, h_1 = 2.6$, 令 $n_1 = 0.1, n_2 = 1.5, n_3 = 0.8, \Delta = 0.032\,2$. 由定理 1, 得到状态和故障估计增益矩阵分别为

$$\boldsymbol{L} = \begin{bmatrix} 0.943\,3 & -0.998\,0 & -0.040\,0 & 1.208\,4 \\ 0.003\,6 & 1.201\,4 & 0.021\,9 & 0.103\,5 \\ 0.010\,9 & -0.014\,4 & 0.933\,5 & -0.029\,5 \\ -0.089\,9 & -0.371\,5 & -0.187\,8 & 1.576\,8 \end{bmatrix},$$

$$\boldsymbol{F} = [3.760\,3 \quad 5.945\,4 \quad 7.185\,0 \quad -13.620\,1].$$

采用前述 PSO-CatBoost 模型重构隐蔽 FDI 攻击, 并在观测器之前对其影响按照式 (18) 补偿后, 系统状态估计误差、执行器故障估计及其估计误差分别如图 6 和图 7 所示.

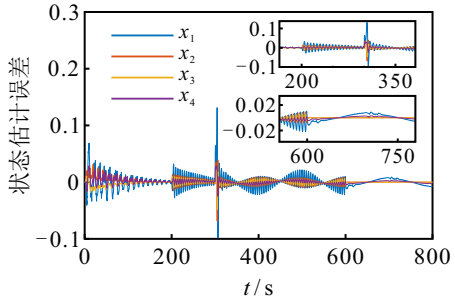


图 6 系统状态估计误差

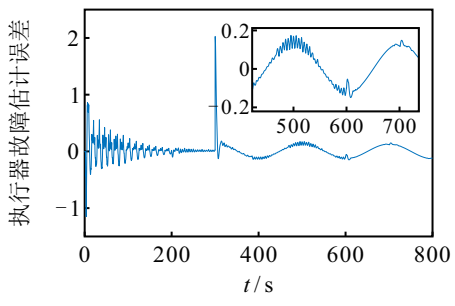


图 7 执行器故障估计误差

由图 6 和图 7 的仿真结果可知:

1) 当 $0 \leqslant t < 200$ s, 系统在无攻击、无故障, 但是存在外部干扰时, 状态和故障估计误差均趋于 0, 扰动可抑制在一定水平;

2) 当 $200\text{ s} \leqslant t < 300$ s, 系统无故障、有 FDI 攻击和外部干扰, 在 $t = 200$ s 时, 状态估计误差瞬间增至 0.03 附近, 此后保持在 ± 0.016 的误差带内;

3) 当 $300\text{ s} \leqslant t < 600$ s, 系统同时遭受 FDI 攻击、故障和外部干扰, 在 $t = 300$ s 时, 状态和故障估计误差又瞬间增至 0.13 和 2.03 附近, 之后二者便分别保持在 ± 0.02 和 ± 0.18 的误差带内;

4) 当 $600\text{ s} \leqslant t < 800$ s, 系统无攻击、有故障和外部干扰, 状态和故障估计误差分别保持在 ± 0.01 和 ± 0.14 的误差带内.

综上结果, 表明通过 PSO-CatBoost 模型对隐蔽 FDI 攻击准确重构和有效补偿后, 再采用所设计的观测器, 可对系统状态、连续时变故障进行快速、准确地估计, 且对外部干扰和 FDI 补偿误差具有较强的鲁棒性, 从而为综合安全控制奠定了基础.

考虑到改进仿射 Bessel-Legendre 不等式在处理 L-K 泛函导数项的少保守性已在文献 [22] 中得到了验证, 下面仅就构造的增广 L-K 泛函对减少结果的少保守性进行说明. 较文献 [13], 本文泛函中增加了如 $V_3(t)$、$V_4(t)$ 中的 $h_1^2 \int_{i_k h}^{t} \dot{\bar{e}}^{\mathrm{T}}(s)\boldsymbol{Q}\dot{\bar{e}}(s)\mathrm{d}s$ 等项. 在相同性能指标 $\gamma_1 = 3.8$ 约束下, 计算两种结果的系统最大允许事件触发间隔, 本文和原有工作[13] 的 h_1 分别为 2.6 和 2.1, 可见通过对 Lyapunov 泛函项进行增广, 获得了更少保守性观测器设计方法, 提升了解的优性.

5.4.2　综合安全控制实验研究

选择 $\gamma_2 = 1.6, h_1 = 2.6, \sigma = 0.001, \alpha = 1.75$, 令 $m_1 = 0.5, m_2 = m_3 = 0.1, \rho_1 = 1.5, \rho_2 = 0.8, \rho_3 = 0.1, \sigma_m = 0.001, \sigma_M = 0.004, \Delta_1 = 0.02, \Delta_2 = 0.79$. 由定理 2, 得到

$$\boldsymbol{K} = \begin{bmatrix} 5.8855 & 0.7908 & -0.0026 & 2.5732 \\ 0.7654 & 4.6651 & 4.8148 & -0.0503 \end{bmatrix},$$

$$\boldsymbol{\Phi} = 10^{-9} \times \mathrm{diag}\,[0.4379 \quad 0.4379 \quad 0.4379 \quad 0.4379].$$

进一步地, 由 $(\boldsymbol{I} - \boldsymbol{B}\boldsymbol{B}^{*})\boldsymbol{E}_f = \boldsymbol{0}$, 得到

$$\boldsymbol{B}^{*} = \begin{bmatrix} 11.9550 & -10.5732 & 0 & 0.2496 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

由于在观测器之前, 已通过 PSO-CatBoost 模型重构了隐蔽 FDI 攻击, 先对其影响予以主动补偿, 观测器又对补偿误差予以被动鲁棒, 结合上述控制器, 在数据驱动与机理解析融合的综合安全控制策略协同作用下, 系统输出响应曲线如图 8 所示.

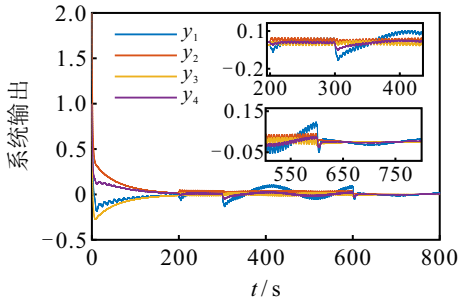


图 8　系统输出响应曲线

观察对应的 4 种情形系统输出结果可知:

1) 当 $0 \leqslant t < 200$ s 时, 系统输出快速趋于平衡状态, 并将扰动影响抑制在一定水平;

2) 当 $200\text{ s} \leqslant t < 300$ s 时, 仅在 $t = 200$ s 时, 系统输出受攻击的影响, 出现了较小波动, 但是仍然在 ± 0.03 的误差带内;

3) 当 $300\text{ s} \leqslant t < 600$ s 时, 也仅在 $t = 300$ s 时, 系统输出瞬间减至 -0.2 左右, 此后便保持在 ± 0.079 的误差带内;

4) 当 $600\text{ s} \leqslant t < 800$ s 时, 除在 $t = 600$ s 时, 系统输出瞬间增至 0.1 左右, 此后也保持在 ± 0.02 的误差带内.

上述结果充分揭示出, 由于数据驱动 PSO-CatBoost 模型对隐蔽 FDI 攻击的准确重构和提前补偿, 结合观测器对 FDI 攻击补偿误差的鲁棒以及控制器对 ICPS 中执行器故障的调节和更具弹性的反馈控制, 不仅有效抵御了 FDI 攻击和执行器故障的影响, 且对各类干扰表现出较强的鲁棒性.

对于相同隐蔽 FDI 攻击、执行器故障, 采用相同

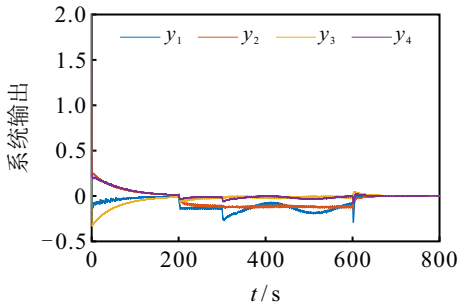


图 9　基于文献 [9] 方法的输出曲线

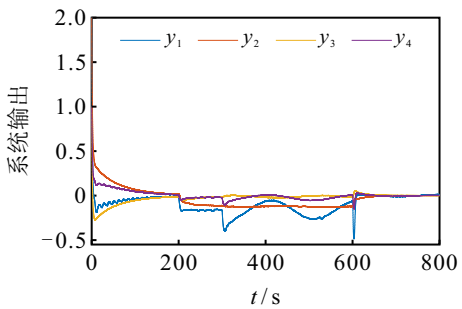


图 10　基于文献 [13] 方法的输出曲线

的ADETCS, 图9和图10分别为利用文献[9]弹性控制、文献[13]主动容侵和容错时的系统输出. 对比图8可以看出, 数据驱动与机理解析融合的综合安全控制方法, 其收敛速度和系统性能均更优.

对于通讯资源, 图11为所设计新型ADETCS下事件触发参数的变化曲线. 由图11可见: 在$t = 200$ s和$t = 300$ s时, 即当系统遭受FDI攻击和执行器发生故障的初始时刻, 事件触发参数σ随系统波动自动骤减, 使得数据传输量增加; 而当系统在综合安全控制策略作用下平稳运行时, σ则随之自适应变大, 减少数据量传输.

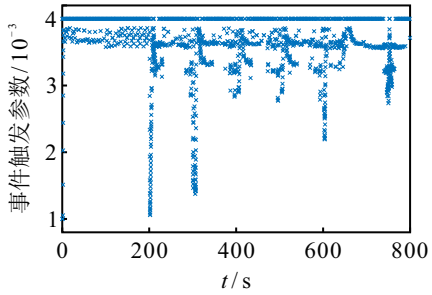


图 11 事件触发参数变化曲线

表2和表3分别为在文献[13]DETCS、文献[15]ADETCS以及所提出新型ADETCS下, 综合安全控制器设计取不同σ值, 在前述情形下数据传输量和数据平均传输周期h_{av}. 由表2和表3可见, 在所提出ADETCS下, 只需传输较少的数据量和更长的平均传输周期, 亦可确保系统更优的性能. 原因如下: 所提出ADETCS下的事件触发参数, 不仅可依据系统性能约束, 随系统行为自适应全局变化, 且有少保守性观测器、控制器的共同加持, 从而使得网络通讯资源节约与系统性能间得到了更优的折衷平衡.

表 2 不同触发机制下数据传输量对比

σ	0	0.001	0.002	0.003	0.004
文献[13]DETCS	8 000	4 583	3 619	2 106	1 674
文献[15]ADETCS	8 000	4 418	3 508	1 752	1 362
本文ADETCS	8 000	4 216	3 247	1 648	1 225

表 3 不同触发机制下平均传输周期对比

触发机制	h_{av}
文献[13]DETCS	1.521 3
文献[15]ADETCS	1.754 6
本文ADETCS	1.931 8

6 结 论

本文以通信资源有效利用和双重安全防御为着眼点, 在一种新型ADETCS下, 研究了隐蔽FDI攻击和执行器故障共存的ICPS综合安全控制与通讯协同设计问题. 本文将数据驱动与机理解析方法深度融合, 利用重构的攻击信息主动补偿ICPS遭受的FDI攻击, 并在统一的非均匀数据传输机制下, 基于时滞系统理论和少保守性技术, 给出了鲁棒观测器、综合安全控制与通讯协同设计的方法, 经工业四容水箱系统验证了所提出方法的有效性. 在ADETCS下, 如何随触发参数的变化进一步提升控制器的适应性, 将是未来努力的方向.

参考文献(References)

[1] 杨光红, 芦安洋, 安立伟. 网络攻击下的信息物理系统安全状态估计研究综述[J]. 控制与决策, 2023, 38(8): 2093-2105.
(Yang G H, Lu A Y, An L W. A survey on secure state estimation of cyber-physical systems under cyber attacks[J]. Control and Decision, 2023, 38(8): 2093-2105.)

[2] Ding D, Han Q L, Xiang Y, et al. A survey on security control and attack detection for industrial cyber-physical systems[J]. Neurocomputing, 2018, 275: 1674-1683.

[3] 叶丹, 靳凯净, 张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252.
(Ye D, Jin K J, Zhang T Y. A survey on security of cyber-physical systems under network attacks[J]. Control and Decision, 2023, 38(8): 2243-2252.)

[4] 杨飞生, 汪璟, 潘泉. 基于事件触发机制的网络控制研究综述[J]. 控制与决策, 2018, 33(6): 969-977.
(Yang F S, Wang J, Pan Q. A survey of networked event-triggered control[J]. Control and Decision, 2018, 33(6): 969-977.)

[5] Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51: 135-148.

[6] Li Y Z, Shi D W, Chen T W. False data injection attacks on networked control systems: A stackelberg game analysis[J]. IEEE Transactions on Automatic Control, 2018, 63(10): 3503-3509.

[7] Miao F, Zhu Q Y, Pajic M, et al. Coding schemes for securing cyber-physical systems against stealthy data injection attacks[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 106-117.

[8] Wang D, Wang Z D, Shen B, et al. Recent advances on filtering and control for cyber-physical systems under security and resource constraints[J]. Journal of the Franklin Institute, 2016, 353(11): 2451-2466.

[9] Sun Z W, Xue W F, Liu J L, et al. Adaptive event-triggered resilient control of industrial cyber physical systems under asynchronous data injection

attack[J]. Journal of the Franklin Institute, 2022, 359(7): 3000-3023.

[10] Lee P, Clark A, Bushnell L, et al. A passivity framework for modeling and mitigating wormhole attacks on networked control systems[J]. IEEE Transactions on Automatic Control, 2014, 59(12): 3224-3237.

[11] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2013, 58(11): 2715-2729.

[12] Zhang J, Pan L, Han Q L, et al. Deep learning based attack detection for cyber-physical system cybersecurity: A survey[J]. IEEE/CAA Journal of Automatica Sinica, 2022, 9(3): 377-391.

[13] 李炜, 张建军. 攻击与故障共存的ICPS综合安全控制方法[J]. 浙江大学学报: 工学版, 2021, 55(6): 1185-1198.
(Li W, Zhang J J. Integrated security control method for industrial cyber-physical system with attack and fault[J]. Journal of Zhejiang University: Engineering Science, 2021, 55(6): 1185-1198.)

[14] 李炜, 程雪, 李亚洁, 等. 新型ADETCS下工业信息物理系统综合安全控制[J]. 北京航空航天大学学报, DOI: 10.13700/j.bh.1001-5965.2022.0734.
(Li W, Cheng X, Li Y J, et al. Industrial cyber-physical systems integrated security control based on the new type ADETCS[J]. Journal of Beijing University of Aeronautics and Astronautics, DOI: 10.13700/j.bh.1001-5965.2022.0734.)

[15] 乔伟豪, 朱凤增, 彭力. 基于自适应事件触发的时滞系统分布式l_2-l_∞滤波[J]. 控制与决策, 2022, 37(4): 1074-1080.
(Qiao W H, Zhu F Z, Peng L. Distributed l_2-l_∞ filtering based on adaptive event triggering for time-delay systems[J]. Control and Decision, 2022, 37(4): 1074-1080.)

[16] Peng C, Zhang J, Yan H C. Adaptive event-triggering H_∞ load frequency control for network-based power systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(2): 1685-1694.

[17] Fridman E. A refined input delay approach to sampled-data control[J]. Automatica, 2010, 46(2): 421-427.

[18] Huang X, Dong J X. Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks[J]. IEEE Transactions on Cybernetics, 2018, 48(12): 3432-3439.

[19] 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.

[20] Prokhorenkova L, Gusev G, Vorobev A, et al. CatBoost: Unbiased boosting with categorical features[C]. Proceedings of the 32nd International Conference on Neural Information Processing Systems. Montréal, 2018: 6639-6649.

[21] 邱爱兵, 吉虹钢, 顾菊平. 非均匀采样数据系统时变故障估计与调节最优集成设计[J]. 自动化学报, 2014, 40(7): 1493-1504.
(Qiu A B, Ji H G, Gu J P. Optimal integrated design of time-varying fault estimation and accommodation for nonuniformly sampled data systems[J]. Acta Automatica Sinica, 2014, 40(7): 1493-1504.)

[22] Lee W I, Lee S Y, Park P G. Affine Bessel-Legendre inequality: Application to stability analysis for systems with time-varying delays[J]. Automatica, 2018, 93: 535-539.

作者简介

李炜(1963−), 女, 教授, 博士生导师, 从事复杂系统建模与预测、CPS安全控制、动态系统故障诊断与自主健康维护等研究, E-mail: liwei@lut.edu.cn;

陈婧婧(1997−), 女, 硕士生, 从事工业信息物理融合系统综合安全控制的研究, E-mail: 3299891145@qq.com;

李亚洁(1981−), 女, 副教授, 博士, 从事动态系统故障诊断与容错控制、数字孪生、机器人应用技术等研究, E-mail: liyaj@lut.edu.cn.