控制与决策
Control and Decision

自适应事件触发通信机制下机理解析与数据驱动融合的ICPS双重安全控制

赵莉, 李炜, 李亚洁

引用本文:
赵莉,李炜,李亚洁. 自适应事件触发通信机制下机理解析与数据驱动融合的ICPS双重安全控制[J]. 控制与决策, 2024, 39(1): 206−218.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2022.0557

自适应事件触发通信机制下机理解析与数据驱动融合的ICPS双重安全控制

赵 莉[1,2], 李 炜[1†], 李亚洁[1]

(1. 兰州理工大学 电气工程与信息工程学院，兰州 730050；2. 陇东学院 电气工程学院，甘肃 庆阳 745000)

摘 要: 针对存在拒绝服务(DoS)攻击与执行器故障的工业信息物理融合系统(ICPS),将机理解析与数据驱动方法相结合,在新型自适应事件触发通信机制下,研究双重安全控制问题. 首先,设计自适应事件触发机制,能够触发参数随系统行为动态自适应变化,节约更多网络通信资源;其次,基于系统最大允许时延建立攻击检测机制,可以有效区分大、小能量DoS攻击;再次,基于极限学习机算法(ELM)建立时序预测模型,用于大能量DoS攻击时重构修正控制量,以主动容侵攻击的影响,并给出与小能量攻击时机理解析的弹性被动容侵来提升系统对攻击的防御能力;然后,借助T-S模糊理论、时滞系统理论、新型Bessel-Legendre不等式等,推证得到系统鲁棒观测器及双重安全控制器的解析求解方法,使双重安全控制与通讯性能得到折衷协同提升;最后,通过实例仿真验证所提出方法的有效性.

关键词: 工业信息物理融合系统(ICPS)；双重安全控制；DoS攻击；主被动容侵；数据驱动；机理解析

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2022.0557

引用格式: 赵莉,李炜,李亚洁. 自适应事件触发通信机制下机理解析与数据驱动融合的ICPS双重安全控制[J]. 控制与决策, 2024, 39(1): 206-218.

Dual security control based on fusion of mechanism analysis and data-driven under adaptive event-triggered communication scheme for ICPS

ZHAO Li[1,2], *LI Wei*[1†], *LI Ya-jie*[1]

(1. College of Electrical and Information Engineering，Lanzhou University of Technology，Lanzhou 730050，China；2. School of Electrical Engineering，Longdong University，Qingyang 745000，China)

Abstract: Under a novel adaptive event-triggered communication scheme, a dual security control problem is investigated by combining mechanistic analysis with a data-driven approach for industrial cyber-physical systems (ICPS) with denial-of-service (DoS) attacks and actuator fault. First, in order to save more network communication resources, the trigger parameters of the designed adaptive event triggered scheme can change dynamically and adaptively with the system behavior. Second, an attack detection mechanism is established based on the maximum allowable delay of the system to effectively distinguish large and low energy DoS attacks. Third, based on extreme learning machine algorithm, a timing prediction model is established to reconfigure and correct the control quantity during high-energy DoS attacks, thus actively tolerating the impact of attacks, which is combined with resilient passive attack tolerance for low-energy attacks to improve the system's defense against attacks. Fourth, with the help of T-S fuzzy theory, time delay theory, and the new Bessel-Legendre inequality, etc., a robust observer and an analytical solution method of the dual security controller are obtained to improve and balance the performance of dual security control and communication. Finally, the effectiveness of the proposed method is verified by simulation examples.

Keywords: industrial cyber-physical systems (ICPS)；dual security control；denial-of-service (DoS) attacks；active-passive attack tolerance；data-driven；mechanism analysis

收稿日期: 2022-04-06；**录用日期:** 2022-08-02.

基金项目: 国家自然科学基金项目(62163022)；甘肃省青年科技基金项目(21JR1RM339)；甘肃省教育厅高等学校创新能力提升项目(2019B-152).

责任编委: 李少远.

†通讯作者. E-mail: liwei@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 system, ICPS)是CPS应用于工业领域的新型智能系统. 通过引入信息系统作为人与物理系统间相互通讯、实时交互的纽带,将人、传输数据、物理系统联系在了一起,从而摒弃了传统的“信息孤岛”[1]. ICPS因其具有高自治性、可实时协同感知且智能化程度高等优势,广泛应用于电力、制造、石化等多个工业领域. 然而,随着系统智能化和开放性的不断提升,其安全问题日益凸显,如Stuxnet病毒攻击致使伊朗核能数千台离心机超载,意大利地方疫苗接种预约系统因网络攻击被迫关闭等. 因此,开展ICPS信息与物理双重安全防御研究已刻不容缓[2].

ICPS遭受的网络攻击主要包括拒绝服务(denial of service, DoS)[3-4]、假数据注入(false data injection, FDI)[5-6]和数据重放(data replay attack, DRA)[7-8]等. DoS攻击属于非隐蔽型攻击,常以阻塞通信信道使得系统通信无法正常进行. 针对CPS中的DoS攻击,弹性控制作为一种经典防御策略受到了学者们的青睐. 文献[9-11]基于弹性控制研究了DoS攻击下的控制问题,防御本质是以鲁棒方式对有限能量DoS攻击的一种被动式容侵策略,一旦DoS攻击能量超过了允许的最大范围,系统安全性将无法保障. 此外,上述成果仅考虑了传感或执行侧的单点攻击,而多点分布式攻击则更符合DoS的实际特点. 因此,若能对更大能量DoS攻击造成的数据包缺失,基于数据驱动技术进行准确重构补偿,则可确保传输信息的完整性,提高系统对DoS攻击的防御能力.

智能制造下全面感知的需求,在信息与物理系统交互的同时,大数据已成为ICPS的鲜明特征,因而庞大的数据量需要通过通讯网络进行传输,随之带来了能耗大、通讯负担重等痛点问题. 传统“周期时间”触发通讯机制,也因浪费网络资源,无法使控制与通信的设计相关联而逐步失宠,取而代之的是“事件触发”通讯机制. 数据的传输依赖“事件”而非“时间”,尤其是离散事件触发机制(discrete event-triggered communication scheme, DETCS),使控制与通讯的协同成为可能,并可有效节约网络资源[12]. 遗憾的是DETCS中触发阈值仍是固定不变的,无法依据系统行为而动态变化,适应能力不足,未能使网络资源节约以及系统性能得到更优的平衡折衷,且Zeno现象不可避免. 因此,可动态调整触发参数的自适应离散事件触发通信机制(adaptive discrete event-triggered communication scheme, ADETCS)应运而生. 文献[13-15]在ADETCS下分别研究了电力系统稳定运行、非线性系统滤波和无人机系统跟踪控制问题. 随着执行、传感等装置智能化的推进,物理系统步入智能转型升级的轨道,这也促使ICPS较传统制造系统性能显著提升,针对故障具有了一定的鲁棒性. 然而,核心元部件的失效仍是致系统失稳甚至崩溃的主要原因[16]. 但在ADETCS下,尚未涉及对DoS攻击和物理器件故障双重安全的考虑.

鉴于此,本文针对DoS攻击与执行器故障共存的非线性ICPS,兼顾安全防御及通讯资源受限问题,基于T-S模糊模型,将机理解析与数据驱动方法相融合,研究了非线性ICPS双重安全控制与通讯的协同设计方法,主要贡献点包括:

1) 在新型ADETCS下,结合弹性控制与故障调节方法设计的双重安全控制器,可对小能量DoS攻击与执行器的时变故障,在被动容侵攻击和主动容错故障的同时,因触发参数随系统行为动态自适应的调整,使网络资源得到更多的节约,促进了系统性能与通信资源间的优化折衷平衡.

2) 对DoS引起时延超过系统最大允许范围的大能量攻击,将数据的动态时间序列转换为静态空间关系,结合ELM算法建立预测模型,提出一种实时补偿控制量丢包的主动防御策略,使基于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,有效提升了ICPS应对更严重DoS攻击的能力.

3) 通过构造合适的Lyapunov函数,使用增广矩阵理论、新型Bessel-Legendre不等式等少保守性技术,得到了非线性ICPS状态和故障的观测器、双重安全控制与通讯协同的解析设计方法,使得ICPS安全运行的同时,协同平衡了系统性能与通信资源.

1 问题描述

1.1 系统架构

对于一类遭受双端DoS攻击与执行器时变故障的非线性ICPS,为进一步节约通信资源,通过引入自适应事件触发机制,建立具有攻击和故障防御能力的双重安全控制架构,如图1所示.

DoS攻击引起的时延若趋近或超过系统最大允许时延,则称为大能量DoS攻击,反之,则称为小能量DoS攻击. 图1中,Y表示系统遭受大能量DoS攻击,N表示系统遭受小能量DoS攻击. 结合图1及系统各部件的功能,分析在ADETCS下数据的传输过程.

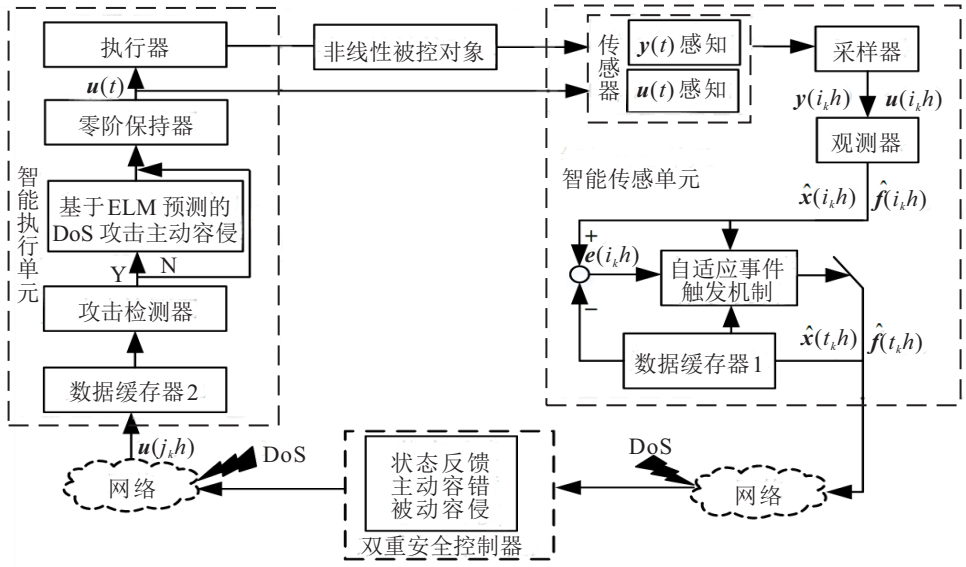


图 1 DoS攻击下自适应事件触发机制ICPS双重安全控制架构

stage I: 智能传感单元对控制量和系统输出采样后,经观测器得到状态与故障的估计值,通过自适应事件触发机制筛选后,传输满足条件的数据;

stage II: 双重安全控制器完成基于弹性控制对小能量DoS攻击的被动容侵、基于补偿对执行器故障主动容错的控制量计算,并传输至智能执行单元;

stage III: 数据缓存器2存储带有时间戳的当前与前期各时刻的控制量,攻击检测器对大、小能量的DoS攻击进行区分识别,若检测到大能量DoS攻击,则基于ELM模型,预测补偿当前丢失的控制量,并发送至执行器,从而实现对大能量DoS攻击的主动容侵,否则接收到的数据将被直接发送给执行器,控制量最终将作用于被控对象.

注1 图1中用ADETCS取代了DETCS,其目的在于触发参数从“静态”不变,变更为可根据系统行为“动态”自适应变化,进而在ADETCS下获得小能量DoS被动容侵和故障主动容错的安全控制器解析解,可更有效地节约网络资源.

注2 图1中融入了基于数据驱动方法的控制量主动补偿容侵策略,即利用与当前时刻相关且未遭受或遭受小能量DoS攻击时系统的历史数据,基于ELM算法,通过将动态时间序列转化为静态空间关系,建立非线性动态预测模型,实时补偿控制量因大能量DoS而导致的缺失,进而达到对其的主动容侵.

1.2 被控对象描述

图1中,连续非线性被控对象的输出经过系统采样之后,传输至智能传感和控制单元中,进行估计与计算时均为数字量. 因此,该系统是典型的采样数据系统[17],依据采样系统理论并基于T-S模糊模型,具有执行器连续时变故障的非线性ICPS可描述如下:

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\sum\limits_{i=1}^{r}\xi_i(\theta(t))[\boldsymbol{A}_i\boldsymbol{x}(t)+\boldsymbol{B}_i\boldsymbol{u}(t)+\\ \qquad\boldsymbol{E}_{fi}\boldsymbol{f}(t)+\boldsymbol{E}_{wi}\boldsymbol{w}(t)],\\ \boldsymbol{y}(i_kh)=\sum\limits_{i=1}^{r}\xi_i(\theta(t))[\boldsymbol{C}_i\boldsymbol{x}(i_k(h)+\boldsymbol{E}_{vi}\boldsymbol{v}(i_kh)].\end{cases}\tag{1}$$

其中: $\boldsymbol{x}(t)\in\boldsymbol{R}^n,\boldsymbol{u}(t)\in\boldsymbol{R}^{n_u}$ 分别为系统状态向量和控制输入向量; $\boldsymbol{A}_i,\boldsymbol{B}_i,\boldsymbol{E}_{fi},\boldsymbol{E}_{wi},\boldsymbol{C}_i,\boldsymbol{E}_{vi}$ 为已知适维矩阵; $\boldsymbol{f}(t)\in\boldsymbol{R}^{n_f}$ 为执行器未知连续时变故障,并假设其导数范数有界,即存在常数 f_1 使得 $\|\dot{f}(t)\|\leqslant f_1$; $\boldsymbol{w}(t)\in\boldsymbol{R}^{n_w},\boldsymbol{y}(i_kh)\in\boldsymbol{R}^m,\boldsymbol{v}(i_kh)\in\boldsymbol{R}^{n_v}$ 分别为系统扰动、系统输出采样和测量噪声, $\{i_1h,i_2h,\dots,i_kh,\dots\}$ 表示系统中采样器的采样时刻; $i=1,2,\dots,r,r$ 是If-Then规则数; $\boldsymbol{M}_{is}(i=1,2,\dots,r;s=1,2,\dots,n)$ 是模糊集, $\theta(t)=[\theta_1(t),\dots,\theta_n(t)]^{\mathrm{T}}$ 代表模糊前件变量. $\xi_i(\theta(t))=a_i(t))\Big/\sum\limits_{i=1}^{r}a_i(\theta(t)),\xi_i(\theta(t))$ 代表每一个模糊规则的权重比, $a_i(\theta(t))=\prod\limits_{s=1}^{n}\boldsymbol{M}_{is}(\theta_s(t)),$ $\boldsymbol{M}_{is}(\theta_s(t))$ 是 $\theta_s(t)$ 在模糊集 $\boldsymbol{M}_{is}$ 上的隶属度,且满足 $\xi_i(\theta(t))\geqslant0,\sum\limits_{i=1}^{r}(\xi_i(\theta(t))=1.$

1.3 自适应事件触发机制的设计

在DETCS中,采样数据是否传输取决于当前时刻与上一时刻传输值的误差是否大于固定的阈值,尽管事件触发机制的引入,在确保系统性能的前提下节约了一定的网络资源,但固定不变的阈值若取值不当会引起以下问题: 1) 当系统处于平稳状态时,仍有大量数据包被传输,而实际工程中,系统稳定且具

有良好性能时,需减少数据包的传输;2) 当系统长时间不触发时,会导致时延增大,进而据此设计会增加保守性. ADETCS的提出为上述问题提供了解决思路. 因此,本文借鉴文献[13],提出一种新的ADETCS,依据系统的运行行为通过动态地自动调整触发阈值,试图使系统性能与网络资源节约得以更优的平衡折衷. 定义下一个数据传输时刻为

$$t_{k+1}h = t_kh + \min_{l\in\boldsymbol{N}}\{lh|\boldsymbol{e}^{\mathrm{T}}(i_kh)\boldsymbol{\Phi}\boldsymbol{e}(i_kh) \leqslant \sigma(t_kh)\hat{\boldsymbol{x}}^{\mathrm{T}}(t_kh)\boldsymbol{\Phi}\hat{\boldsymbol{x}}(t_kh)\}. \tag{2}$$

其中:$\boldsymbol{\Phi}$是正定权矩阵,$\boldsymbol{e}(i_kh) = \hat{\boldsymbol{x}}(i_kh) - \hat{\boldsymbol{x}}(t_kh)$是状态估计误差,$\hat{\boldsymbol{x}}(i_kh)$是当前时刻系统状态估计值,$\hat{\boldsymbol{x}}(t_kh)$是上一时刻满足事件触发条件的系统状态估计值. $i_kh = t_kh + lh, l \in \boldsymbol{N}, i_kh \in (t_k, t_{k+1}], t_k(k = 0,1,2,\ldots)$是整数且$\{t_0,t_1,t_2,\ldots\} \subset \{0,1,2\}$,$h$是采样周期. 数据的传输同时依赖于误差$\boldsymbol{e}(i_kh)$、最新时刻的状态估计$\hat{\boldsymbol{x}}(t_kh)$和触发参数$\sigma(t_kh)$. 文中$\sigma(t_kh)$基于以下自适应规则动态变化:

$$\begin{aligned}&\sigma(t_kh) = \min\{\max[\sigma_m, \lambda\sigma(t_{k-1}h)], \sigma_M\},\\ &\lambda = 1 - \frac{2\alpha}{\pi}\mathrm{atan}(\Delta - \varepsilon),\\ &\Delta = \beta\Big(\frac{\|\hat{\boldsymbol{x}}(t_kh)\| - \|\hat{\boldsymbol{x}}(t_{k-1}h)\|}{\|\hat{\boldsymbol{x}}(t_kh)\|}\Big).\end{aligned} \tag{3}$$

其中:$\sigma_m > 0, \sigma_m$和σ_M是$\sigma(t_kh)$的上下界,$\sigma(0) = \sigma_m$;$\alpha \geqslant 0, \beta \geqslant 0, \varepsilon > 0$是给定的常数.

注3　本文使用反正切函数$\mathrm{atan}(\cdot)$结合参数α和β,自动调整阈值参数$\sigma(t_kh)$,$\mathrm{atan}(\cdot) \in (-\pi/2, \pi/2)$. 若$\Delta - \varepsilon > 0$,这时$0 < \lambda < 1, \sigma(t_{k+1}h) < \sigma(t_kh)$,则需更小的$\sigma(t_{k+1}h)$使网络传输频率加快;反之,采用更大的$\sigma(t_{k+1}h)$来减小传输频率,触发参数的动态变化动态调节了数据的传输频率,最终促使系统性能与通信资源间的优化折衷平衡. 特别地,若$\alpha = 0$或$\beta = 0$,则式(3)退化为固定阈值的事件触发机制[12],因此,所提出的ADETCS是固定事件触发机制的广义形式. 与文献[13]的不同之处在于设置了触发阈值的上界σ_M,目的是对系统处于平稳状态时的传输时延予以限制,即防止系统处于平稳状态情况下长时间不传输数据. 引入一个小正数ε,用以适度调整$\mathrm{atan}(\cdot)$的输出.

1.4　CPS相关时延区间的分析

智能传感单元中观测器或控制单元中控制器的计算都是以数字量的形式进行,ADETCS的引入使得满足系统需求的数据以非均匀方式传输. 基于文献[18]的时滞系统分析方法,将非均匀传输属性转化为时延,以连续的方式研究观测器和控制器的设计方法. 借助时滞系统理论,将相邻采样点内的采样周期转化为时滞,以连续的方式进行设计与分析.

定义时延函数

$$\tau_1(t) = t - i_kh, \tag{4}$$

其中$t \in [i_kh, i_{k+1}h]$且$0 \leqslant \tau_1(t) \leqslant h_1 = h$.

非线性CPS数据传输过程中,记i_kh为采样数据序列,经ADETCS对采样数据筛选之后的触发数据序列为t_kh,双端网络发生DoS攻击后传输至ZOH侧的数据序列(不考虑传输时延)为j_kh. DoS攻击发生时造成的连续丢包数为$\tau_{t_k}^{\mathrm{DoS}}$,满足$\tau_{t_k}^{\mathrm{DoS}} \in [0, \tau_M^{\mathrm{DoS}}], j_kh = t_kh + \tau_{t_k}^{\mathrm{DoS}}h_{t_k}$. $h_{t_k}^{\max}$为满足触发条件的非均匀最大触发周期,则DoS攻击的实际最大持续时间为$\tau_M^{\mathrm{DoS}}h_{t_k}^{\max}$. 本文将DoS攻击建模为连续的丢包,并将其对系统的影响通过丢包量大小变化转化为一种特殊的时变时延. 当$\hat{x}(j_kh)$和$\hat{f}(j_kh)$传输至ZOH前端,但$\hat{x}(j_{k+1}h)$和$\hat{f}(j_{k+1}h)$未送至ZOH时,传输区间$\Lambda = [j_kh, j_{k+1}h]$.

定义时延函数

$$\tau_2(t) = t - j_kh, \tag{5}$$

则其上界为

$$h_2 = \max\{h_{t_k} + \tau_{t_k}^{\mathrm{DoS}}h_{t_k}\} = h_{t_k}^{\max} + \tau_M^{\mathrm{DoS}}h_{t_k}^{\max}, \tag{6}$$

下界为$0 < \tau_{\min} = \min\{\tau_{t_k}^{\mathrm{DoS}}h_{t_k}\}$. 其中时延函数满足$0 < \tau_{\min} \leqslant \tau_2(t) \leqslant h_2$. i_kh, t_kh, j_kh分别记为i_k, t_k, j_k.

2　不同能量DoS攻击下机理解析与ELM融合的主被动混合容侵策略

2.1　不同能量DoS攻击的检测识别

假设j_kh时刻和$j_{k+1}h$时刻传输至智能执行单元的控制量为$\boldsymbol{u}(j_kh)$和$\boldsymbol{u}(j_{k+1}h)$,令$h_{j_k} = j_{k+1}h - j_kh$为连续两次接收到控制量的传输间隔. 系统的最大允许时延为h_m^2,为了保障DoS攻击发生时系统具有一定的安全裕度,设置安全因子$\theta, \theta \in (0,1)$,并将θh_2^m作为划分大、小能量DoS攻击的依据,若$h_{j_k} < \theta h_2^m$,则非线性ICPS未遭受DoS攻击或遭受的是小能量DoS攻击;反之,遭受大能量DoS攻击入侵.

2.2　小能量DoS攻击的被动容侵策略

在ADETCS下,小能量DoS攻击造成的时延区间为$(h, \theta h_2^m]$,此时攻击对系统的影响较小,直接实施基于“弹性控制”的被动容侵策略,即对DoS攻击引起的时延予以鲁棒便可保持系统稳定. 由于控制

器的解是基于机理模型解析获得,可称之为对小能量DoS攻击的机理解析被动容侵.

2.3 大能量DoS攻击的主动容侵策略

当$h_{j_k} \geqslant \theta h_2^m$时,图1中智能执行单元中攻击检测器检测到DoS攻击的持续时间接近或超过系统所允许的最大时延,此时大能量DoS攻击入侵系统,被动容侵策略已无法抵御其对系统的影响. 本文提出一种基于数据驱动ELM的时序模型来实时预测补偿控制量的主动容侵策略.

2.3.1 极限学习机(ELM)

数据驱动建模方法中,传统常用的机器学习模型包含前馈神经网络模型、多层感知机、贝叶斯网、支持向量机等,极限学习机(extreme learning machine, ELM)[19]是一种单隐层前馈神经网络模型,因其训练速度高且泛化能力强,在众多的数据驱动技术中脱颖而出. ELM建模过程如下.

基于时间序列的训练样本集$\boldsymbol{S}=\{(\boldsymbol{u}_{j_i},\boldsymbol{l}_{j_i})\}_{i=1}^{k}$,其中$\boldsymbol{u}_{j_i}=[u_{j_i},u_{j_{i+1}},u_{j_{i+2}},\ldots,u_{j_{i+n-1}}]^{\mathrm{T}}$,$\boldsymbol{l}_{j_i}=\boldsymbol{u}_{j_{i+n}}$,$k$为训练样本的数量,$u_{j_i}$为时间序列数据,$n$为嵌入维数. ELM的回归模型表示为

$$\sum_{i=1}^{m}\beta_i f(\boldsymbol{\omega}_i\boldsymbol{u}_{j_k}+b_i)=\boldsymbol{l}_{j_k}. \tag{7}$$

其中:m为隐含层神经元个数;$f(\cdot)$为隐含层神经元激活函数;$\boldsymbol{\omega}_i$为输入层与隐含层之间的连接权值,且$\boldsymbol{\omega}_i=[\omega_{i1}\ \ \omega_{i2}\ \ \ldots\ \ \omega_{in}]$;$\beta_i$为隐含层与输出层之间的连接权值,$\boldsymbol{\beta}=[\beta_1\ \ \beta_2\ \ \ldots\ \ \beta_m]^{\mathrm{T}}$;$b_i$为第$i$个隐含层神经元的阈值.

进一步,式(7)的矩阵形式为

$$\boldsymbol{H}_k\boldsymbol{\beta}_k=\boldsymbol{L}_k. \tag{8}$$

其中

$$\boldsymbol{L}_k=[l_{j_1}\ \ l_{j_2}\ \ \ldots\ \ l_{j_k}]^{\mathrm{T}},$$

$$\boldsymbol{H}_k=\begin{bmatrix} f(\omega_1u_{j_1}+b_1) & \ldots & f(\omega_mu_{j_1}+b_m)\\ \vdots & \ddots & \vdots\\ f(\omega_1u_{j_k}+b_1) & \ldots & f(\omega_mu_{j_k}+b_m)\end{bmatrix},$$

则

$$\boldsymbol{\beta}_k=(\boldsymbol{H}_k{}^{\mathrm{T}}\boldsymbol{H}_k)^{-1}\boldsymbol{H}_k\boldsymbol{L}_k. \tag{9}$$

ELM的核心是通过求解式(8)得到输出权值(9),最终获得训练后的预测模型

$$\boldsymbol{l}_j=\sum_{i=1}^{m}\beta_i f(\boldsymbol{\omega}_i\boldsymbol{u}_j+b_i). \tag{10}$$

其中:$\boldsymbol{u}_j$为预测模型输入,$\boldsymbol{l}_j$为预测模型输出.

2.3.2 基于ELM的控制量补偿主动容侵策略

对于控制系统的控制量序列,通常存在时间关联性,因而可以通过适当的映射关系,基于过去的控制量序列预测未来控制量. 但ELM本属静态建模算法,如果将控制量的动态时间序列转换为静态空间序列,即以过去控制量时间序列为ELM输入,当前控制量为输出,则可建立基于ELM的控制量动态预测模型. 当大能量DoS攻击造成控制量丢失时,基于此模型和图1数据缓存器2的历史控制量序列,即可对丢失控制量进行预测补偿,从而以数据驱动的方式主动容侵大能量DoS的影响. 具体实施步骤如下.

step 1: 将未遭受和遭受小能量DoS攻击的控制量序列作为训练和测试样本,利用ELM算法得到控制量的预测模型,并将其封装于图1的“基于ELM预测的DoS攻击主动容侵”补偿器中;

step 2: 获取连续两次接收到控制量的时间间隔,假设传输间隔$h_{j_k}=j_{k+1}h-j_kh$;

step 3: 判断$h_{j_k}\geqslant\theta h_2^m$? 若成立,则利用ELM模型在线预测补偿当前控制量,输出$j_{k+1}h$时刻的控制量$\boldsymbol{l}(j_{k+1}h)$;反之,直接输出当前控制量$\boldsymbol{u}(j_{k+1}h)$.

3 DoS攻击下鲁棒状态与故障观测器的设计

设计目标 基于ADETCS,针对DoS攻击与执行器故障,求取观测器可准确估计系统状态与执行器故障,并具有H_∞性能指标性能.

在一个采样周期中,将系统的输出特性视为时滞[20],结合式(1)和(4),得到系统的连续时变时滞输出

$$\boldsymbol{y}(t)=\sum_{i=1}^{r}\xi_i(\theta(t))[\boldsymbol{C}_i\boldsymbol{x}(t-\tau_1(t))+\boldsymbol{E}_{vi}\boldsymbol{v}(t-\tau_1(t))]. \tag{11}$$

构造状态与故障估计观测器

$$\begin{cases}\dot{\hat{\boldsymbol{x}}}(t)=\displaystyle\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[\boldsymbol{A}_i\hat{\boldsymbol{x}}(t)+\\ \qquad\boldsymbol{B}_i\boldsymbol{u}(t)+\boldsymbol{E}_{fi}\hat{\boldsymbol{f}}(t)-\boldsymbol{L}_j(\hat{\boldsymbol{y}}(t)-\boldsymbol{y}(t))],\\ \hat{\boldsymbol{y}}(t)=\displaystyle\sum_{i=1}^{r}\xi_i(\theta(t))[\boldsymbol{C}_i\hat{\boldsymbol{x}}(t-\tau_1(t))],\\ \dot{\hat{\boldsymbol{f}}}(t)=\displaystyle\sum_{i=1}^{r}\xi_i(\theta(t))[-\boldsymbol{F}_j\boldsymbol{e}_y(t)].\end{cases} \tag{12}$$

其中:$\hat{\boldsymbol{x}}(t),\hat{\boldsymbol{y}}(t),\hat{\boldsymbol{f}}(t)$分别为系统状态、观测器输出和故障的估计值,$\boldsymbol{L}_j$和$\boldsymbol{F}_j$为观测器和故障估计增益矩阵.

定义$\boldsymbol{e}_{\boldsymbol{x}}(t)=\hat{\boldsymbol{x}}(t)-\boldsymbol{x}(t),\boldsymbol{e}_y(t)=\hat{\boldsymbol{y}}(t)-\boldsymbol{y}(t)$, $\boldsymbol{e}_{\boldsymbol{f}}(t)=\hat{\boldsymbol{f}}(t)-\boldsymbol{f}(t)$,得到如下误差系统:

$$\begin{aligned}\dot{\boldsymbol{e}}_{\boldsymbol{x}}(t)=&\dot{\hat{\boldsymbol{x}}}(t)-\dot{\boldsymbol{x}}(t)=\\&\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[\boldsymbol{A}_i\boldsymbol{e}_{\boldsymbol{x}}(t)+\\&\boldsymbol{E}_{fi}\boldsymbol{e}_{\boldsymbol{f}}(t)-\boldsymbol{L}_j\boldsymbol{C}_i\boldsymbol{e}_x(t-\tau_1(t))+\\&\boldsymbol{L}_j\boldsymbol{E}_{vi}(t-\tau_1(t))-\boldsymbol{E}_{wi}\boldsymbol{w}(t)],\\\boldsymbol{e}_y(t)=&\sum_{i=1}^{r}\xi_i(\theta(t))[\boldsymbol{C}_i\boldsymbol{e}_x(t-\tau_1(t))-\\&\boldsymbol{E}_{vi}\boldsymbol{v}(t-\tau_1(t))].\end{aligned}\tag{13}$$

故障估计误差对时间的导数为

$$\begin{aligned}&\dot{\boldsymbol{e}}_{\boldsymbol{f}}(t)=\\&\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[-\boldsymbol{F}_j\boldsymbol{C}_i\boldsymbol{e}_x(t-\tau_1(t))+\\&\boldsymbol{F}_j\boldsymbol{E}_{vi}\boldsymbol{v}(t-\tau_1(t))-\dot{\boldsymbol{f}}(t)].\end{aligned}\tag{14}$$

进一步,得到状态与增广故障的动态误差系统

$$\begin{aligned}&\dot{\bar{e}}(t)=\\&\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[\bar{\boldsymbol{A}}_i\bar{\boldsymbol{e}}(t)-\bar{\boldsymbol{E}}_{wi}\bar{\boldsymbol{w}}(t)-\\&\bar{\boldsymbol{L}}_j\bar{\boldsymbol{C}}_i\bar{\boldsymbol{e}}(t)(t-\tau_1(t))+\bar{\boldsymbol{L}}_j\boldsymbol{E}_{vi}\boldsymbol{v}(t-\tau_1(t))].\end{aligned}\tag{15}$$

其中

$$\bar{\boldsymbol{A}}_i=\begin{bmatrix}\boldsymbol{A}_i&\boldsymbol{E}_{fi}\\\boldsymbol{0}&\boldsymbol{0}\end{bmatrix},\ \bar{\boldsymbol{e}}(t)=\begin{bmatrix}\boldsymbol{e}_{\boldsymbol{x}}(t)\\\boldsymbol{e}_{\boldsymbol{f}}(t)\end{bmatrix},\ \bar{\boldsymbol{L}}_j=\begin{bmatrix}\boldsymbol{L}_j\\\boldsymbol{F}_j\end{bmatrix},$$

$$\bar{\boldsymbol{E}}_{wi}=\begin{bmatrix}\boldsymbol{E}_{wi}&\boldsymbol{0}\\\boldsymbol{0}&\boldsymbol{I}\end{bmatrix},\ \bar{\boldsymbol{w}}(t)=\begin{bmatrix}\boldsymbol{w}(t)\\\dot{\boldsymbol{f}}(t)\end{bmatrix},\ \bar{\boldsymbol{C}}_i=[\boldsymbol{C}_i\ \ 0].$$

定理1　针对存在DoS攻击与执行器连续时变故障$\boldsymbol{f}(t)$的增广误差系统(15),给定正数h_1,γ_1,n_1,n_2,n_3,若存在对称矩阵$\boldsymbol{P}>\boldsymbol{0}$及适维矩阵$\boldsymbol{X}$和$\boldsymbol{Y}_j$满足下式:

$$\begin{bmatrix}\boldsymbol{\Gamma}_{11}&\boldsymbol{\Gamma}_{12}&\boldsymbol{\Gamma}_{13}&\boldsymbol{\Gamma}_{14}&\boldsymbol{0}\\*&\boldsymbol{\Gamma}_{22}&\boldsymbol{\Gamma}_{23}&\boldsymbol{\Gamma}_{24}&h_1n_1\bar{\boldsymbol{C}}^{\mathrm{T}}\boldsymbol{Y}_j^{\mathrm{T}}\\*&*&\boldsymbol{\Gamma}_{33}&\boldsymbol{\Gamma}_{34}&\boldsymbol{0}\\*&*&*&\boldsymbol{\Gamma}_{44}&\boldsymbol{0}\\*&*&*&*&-h_1n_1\boldsymbol{P}\end{bmatrix}<\boldsymbol{0},\tag{16}$$

$$\begin{bmatrix}\boldsymbol{\Gamma}'_{11}&\boldsymbol{\Gamma}'_{12}&\boldsymbol{\Gamma}_{13}&\boldsymbol{\Gamma}_{14}&\boldsymbol{X}^{\mathrm{T}}\\*&\boldsymbol{\Gamma}'_{22}&\boldsymbol{\Gamma}_{23}&\boldsymbol{\Gamma}_{24}&\boldsymbol{X}^{\mathrm{T}}\\*&*&\boldsymbol{\Gamma}_{33}&\boldsymbol{\Gamma}_{34}&\boldsymbol{X}^{\mathrm{T}}\\*&*&*&\boldsymbol{\Gamma}_{44}&\boldsymbol{X}^{\mathrm{T}}\\*&*&*&*&-\dfrac{1}{9h_1n_1}\boldsymbol{P}^{-1}\end{bmatrix}<\boldsymbol{0},\tag{17}$$

$$\begin{bmatrix}\boldsymbol{\Lambda}_{11}&\boldsymbol{\Lambda}_{12}&\boldsymbol{\Lambda}_{13}&\boldsymbol{\Lambda}_{14}&\boldsymbol{\Lambda}_{15}&\boldsymbol{\Lambda}_{16}&\boldsymbol{0}\\*&\boldsymbol{\Lambda}_{22}&\boldsymbol{\Lambda}_{23}&\boldsymbol{\Lambda}_{24}&\boldsymbol{\Lambda}_{25}&\boldsymbol{\Lambda}_{26}&\boldsymbol{\Lambda}_{27}\\*&*&\boldsymbol{\Lambda}_{33}&\boldsymbol{\Lambda}_{34}&\boldsymbol{0}&\boldsymbol{0}&\boldsymbol{0}\\*&*&*&\boldsymbol{\Lambda}_{44}&\boldsymbol{0}&\boldsymbol{0}&\boldsymbol{0}\\*&*&*&*&\boldsymbol{\Lambda}_{55}&\boldsymbol{\Lambda}_{56}&\boldsymbol{\Lambda}_{57}\\*&*&*&*&*&\boldsymbol{\Lambda}_{66}&\boldsymbol{0}\\*&*&*&*&*&*&\boldsymbol{\Lambda}_{77}\end{bmatrix}<\boldsymbol{0},\tag{18}$$

$$\begin{bmatrix}\boldsymbol{\Lambda}'_{11}&\boldsymbol{\Lambda}'_{12}&\boldsymbol{\Lambda}'_{13}&\boldsymbol{\Lambda}'_{14}&\boldsymbol{\Lambda}'_{15}&\boldsymbol{\Lambda}'_{16}&\boldsymbol{X}^{\mathrm{T}}\\*&\boldsymbol{\Lambda}'_{22}&\boldsymbol{\Lambda}'_{23}&\boldsymbol{\Lambda}'_{24}&\boldsymbol{0}&\boldsymbol{0}&\boldsymbol{X}^{\mathrm{T}}\\*&*&\boldsymbol{\Lambda}'_{33}&\boldsymbol{\Lambda}'_{34}&\boldsymbol{0}&\boldsymbol{0}&\boldsymbol{X}^{\mathrm{T}}\\*&*&*&\boldsymbol{\Lambda}'_{44}&\boldsymbol{0}&\boldsymbol{0}&\boldsymbol{X}^{\mathrm{T}}\\*&*&*&*&\boldsymbol{\Lambda}'_{55}&\boldsymbol{0}&\boldsymbol{0}\\*&*&*&*&*&\boldsymbol{\Lambda}'_{66}&\boldsymbol{0}\\*&*&*&*&*&*&\boldsymbol{\Lambda}'_{77}\end{bmatrix}<\boldsymbol{0}.\tag{19}$$

则系统(15)具有H_∞性能指标

$$\|\bar{\boldsymbol{e}}(t)\|_2^2\leqslant\gamma_1^2\Big[\bar{\boldsymbol{w}}(t)\|_2^2+\sum_{k_1=0}^{+\infty}(i_{k_1+1})-i_{k_1}\|\boldsymbol{v}(i_{k_1})\|_2^2\Big],$$

状态观测器和故障估计增益矩阵$\boldsymbol{L}_j$和$\boldsymbol{F}_j$通过$\bar{\boldsymbol{L}}_j=\begin{bmatrix}\boldsymbol{L}_j\\\boldsymbol{F}_j\end{bmatrix}$求取.其中

$$\begin{aligned}\boldsymbol{\Gamma}_{11}=&\boldsymbol{P}\bar{\boldsymbol{A}}_i+\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}-n_2\boldsymbol{P}+h_1n_1\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}\bar{\boldsymbol{A}}_i+\\&h_1n_2(\boldsymbol{P}\bar{\boldsymbol{A}}_i+\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P})+3\boldsymbol{X}+3\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}_{12}=&n_2\boldsymbol{P}-\boldsymbol{Y}_j\bar{\boldsymbol{C}}_i-h_1n_2\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}-h_1n_1\boldsymbol{Y}_j\bar{\boldsymbol{C}}_i-\\&\boldsymbol{X}^{\mathrm{T}}-h_1n_1\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{Y}_j\bar{\boldsymbol{C}}_i+3\boldsymbol{X},\\\boldsymbol{\Gamma}_{13}=&3\boldsymbol{X}-8\boldsymbol{X}^{\mathrm{T}},\ \boldsymbol{\Gamma}_{14}=3\boldsymbol{X}+12\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}_{22}=&h_1n_3\boldsymbol{P}-n_2\boldsymbol{P}-\boldsymbol{X}-\boldsymbol{X}^{\mathrm{T}}+h_1n_2\boldsymbol{Y}_j\bar{\boldsymbol{C}}_i+\\&h_1n_2\bar{\boldsymbol{C}}_i^{\boldsymbol{T}}\boldsymbol{Y}_j^{\mathrm{T}},\\\boldsymbol{\Gamma}_{23}=&-\boldsymbol{X}-8\boldsymbol{X}^{\mathrm{T}},\ \boldsymbol{\Gamma}_{24}=-\boldsymbol{X}+12\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}_{33}=&-8\boldsymbol{X}-8\boldsymbol{X}^{\mathrm{T}},\ \boldsymbol{\Gamma}_{34}=-8\boldsymbol{X}+12\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}_{44}=&12\boldsymbol{X}+12\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}'_{11}=&\boldsymbol{P}\bar{\boldsymbol{A}}_i+\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}-n_2\boldsymbol{P}+3\boldsymbol{X}+3\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}'_{12}=&-\boldsymbol{Y}_j\bar{\boldsymbol{C}}_i+n_2\boldsymbol{P}+3\boldsymbol{X}-\boldsymbol{X}^{\mathrm{T}},\\\boldsymbol{\Gamma}'_{22}=&-n_2\boldsymbol{P}-\boldsymbol{X}-\boldsymbol{X}^{\mathrm{T}}-h_1n_3\boldsymbol{P},\\\boldsymbol{\Lambda}_{11}=&\boldsymbol{P}\bar{\boldsymbol{A}}_i+\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}-n_2\boldsymbol{P}+3\boldsymbol{X}+3\boldsymbol{X}^{\mathrm{T}}+\\&\boldsymbol{I}+h_1n_1\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}\bar{\boldsymbol{A}}_i+h_1n_2(\boldsymbol{P}\bar{\boldsymbol{A}}_i+\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}),\\\boldsymbol{\Lambda}_{12}=&\boldsymbol{\Gamma}_{12},\ \boldsymbol{\Lambda}_{13}=\boldsymbol{\Gamma}_{13},\ \boldsymbol{\Lambda}_{14}=\boldsymbol{\Gamma}_{14},\\\boldsymbol{\Lambda}_{15}=&\boldsymbol{Y}_j\boldsymbol{E}_{vi}+h_1n_1\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{Y}_j\boldsymbol{E}_{vi}+h_1n_2\boldsymbol{Y}_j\boldsymbol{E}v_i,\\\boldsymbol{\Lambda}_{16}=&-\boldsymbol{P}\bar{\boldsymbol{E}}_{wi}-h_1n_1\bar{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{P}\bar{\boldsymbol{E}}_{wi}-h_1n_2\boldsymbol{P}\bar{\boldsymbol{E}}_{wi},\\\boldsymbol{\Lambda}_{22}=&\boldsymbol{\Gamma}_{22},\ \boldsymbol{\Lambda}_{23}=\boldsymbol{\Gamma}_{23},\ \boldsymbol{\Lambda}_{24}=\boldsymbol{\Gamma}_{24},\\\boldsymbol{\Lambda}_{25}=&-h_1n_2\boldsymbol{Y}_j\boldsymbol{E}_{vi},\end{aligned}$$

$$\boldsymbol{\Lambda}_{26}=h_1n_1\bar{\boldsymbol{C}}_i^{\mathrm{T}}\boldsymbol{Y}_j^{\mathrm{T}}\bar{\boldsymbol{E}}_{wi}+h_1n_2\boldsymbol{P}\bar{\boldsymbol{E}}_{wi},$$
$$\boldsymbol{\Lambda}_{27}=h_1n_1\bar{\boldsymbol{C}}_i^{\mathrm{T}}\boldsymbol{Y}_j^{\mathrm{T}},$$
$$\boldsymbol{\Lambda}_{33}=\boldsymbol{\Gamma}_{33},\ \boldsymbol{\Lambda}_{34}=\boldsymbol{\Gamma}_{34},\ \boldsymbol{\Lambda}_{44}=\boldsymbol{\Gamma}_{44},$$
$$\boldsymbol{\Lambda}_{55}=-\gamma_1^2\boldsymbol{I},\ \boldsymbol{\Lambda}_{56}=-h_1n_1\boldsymbol{E}_{vi}^{\mathrm{T}}\boldsymbol{Y}_j^{\mathrm{T}}\bar{\boldsymbol{E}}_{wi},$$
$$\boldsymbol{\Lambda}_{57}=h_1n_1\boldsymbol{E}_{vi}^{\mathrm{T}}\boldsymbol{Y}_j^{\mathrm{T}},$$
$$\boldsymbol{\Lambda}_{66}=-\gamma_1^2\boldsymbol{I}+h_1n_1\bar{\boldsymbol{E}}_{wi}^{\mathrm{T}}\boldsymbol{P}\bar{\boldsymbol{E}}_{wi},\ \boldsymbol{\Lambda}_{77}=-h_1n_1\boldsymbol{P},$$
$$\boldsymbol{\Lambda}'_{11}=\boldsymbol{\Gamma}'_{11}+\boldsymbol{I},\ \boldsymbol{\Lambda}'_{12}=\boldsymbol{\Gamma}'_{12},\ \boldsymbol{\Lambda}'_{13}=\boldsymbol{\Gamma}_{13},$$
$$\boldsymbol{\Lambda}'_{14}=\boldsymbol{\Gamma}_{14},\ \boldsymbol{\Lambda}'_{15}=\boldsymbol{Y}_j\boldsymbol{E}_{vi},\ \boldsymbol{\Lambda}'_{16}=-\boldsymbol{P}\bar{\boldsymbol{E}}_{wi},$$
$$\boldsymbol{\Lambda}'_{22}=h_1n_3\boldsymbol{P}-n_2\boldsymbol{P}-\boldsymbol{X}-\boldsymbol{X}^{\mathrm{T}},$$
$$\boldsymbol{\Lambda}'_{23}=\boldsymbol{\Gamma}_{23},\ \boldsymbol{\Lambda}'_{24}=\boldsymbol{\Gamma}_{24},\ \boldsymbol{\Lambda}'_{33}=\boldsymbol{\Gamma}_{33},$$
$$\boldsymbol{\Lambda}'_{34}=\boldsymbol{\Gamma}_{34},\ \boldsymbol{\Lambda}'_{44}=\boldsymbol{\Gamma}_{44},\ \boldsymbol{\Lambda}'_{55}=-\gamma_1^2\boldsymbol{I},$$
$$\boldsymbol{\Lambda}'_{66}=-\gamma_1^2\boldsymbol{I},\boldsymbol{\Lambda}'_{77}=-\frac{1}{9h_1n_1}\boldsymbol{P}^{-1}.$$

限于篇幅,定理1的证明略.

4 DoS攻击下具有多目标约束的CPS双重安全控制与通讯协同设计

协同设计目标 在ADETCS下,考虑有限能量的DoS攻击,协同求取系统的双重安全控制增益矩阵和事件触发矩阵,确保闭环故障系统渐近稳定,并具有H_∞性能,即在DoS攻击与执行器故障的双重威胁下具有良好的双重安全性,同时可节约网络资源.

基于ADETCS,将非均匀传输周期转化为时变时滞$\tau_2(t)$,兼顾攻击容侵与故障调节,采用动态输出反馈安全控制器如下:

$$\boldsymbol{u}(t)=\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[\boldsymbol{K}_j\hat{\boldsymbol{x}}(t-\tau_2(t))-\boldsymbol{B}_i^{+}\boldsymbol{E}_{fi}\hat{\boldsymbol{f}}(t-\tau_2(t))]. \tag{20}$$

其中:$t\in[j_k,j_{k+1})$,双重安全控制器增益矩阵为$\boldsymbol{K}_j\in\boldsymbol{R}^{n_u\times n}$,故障调节矩阵$\boldsymbol{B}_i^{+}\in\boldsymbol{R}^{n_u\times n}$满足$(\boldsymbol{I}-\boldsymbol{B}_i\boldsymbol{B}_j^{+})\boldsymbol{E}_{fi}=0,\mathrm{rank}(\boldsymbol{B}_i,\boldsymbol{E}_{fi})=\mathrm{rank}(\boldsymbol{B}_i)$. 将式(20)代入(1),可得ADETCS下集DoS攻击容侵与执行器故障容错控制于一体的闭环模型

$$\dot{\boldsymbol{x}}(t)=\sum_{i=1}^{r}\sum_{j=1}^{r}\xi_i(\theta(t))\xi_j(\theta(t))[\boldsymbol{A}_i\boldsymbol{x}(t)+\boldsymbol{B}_i\boldsymbol{K}_j\boldsymbol{x}(t-\tau_2(t))+\boldsymbol{B}_i\boldsymbol{K}_j\boldsymbol{e}_x(t-\tau_2(t))-\boldsymbol{E}_{fi}\boldsymbol{e}_f(t-\tau_2(t))+\boldsymbol{E}_{wi}\boldsymbol{w}(t)+\tau_2(t)\boldsymbol{E}_{fi}\dot{\boldsymbol{f}}(t)]. \tag{21}$$

定理2 基于ADETCS,针对存在DoS攻击与执行器连续时变故障$\boldsymbol{f}(t)$的ICPS (21),给定正数$n_i,m_i,i=1,2,3,h_2,\gamma_2,\sigma_m$,若存在对称正定矩阵$\tilde{\boldsymbol{P}}>0$以及适维矩阵$\tilde{\boldsymbol{X}},\boldsymbol{K}_{1j},\boldsymbol{Q}_1,\boldsymbol{Q}_3,\boldsymbol{Q}_5$满足

$$\begin{bmatrix}\boldsymbol{\Pi}_{11}&\boldsymbol{\Pi}_{12}&\boldsymbol{\Pi}_{13}&\boldsymbol{\Pi}_{14}&\boldsymbol{0}&\boldsymbol{0}\\ *&\boldsymbol{\Pi}_{22}&\boldsymbol{\Pi}_{23}&\boldsymbol{\Pi}_{24}&\boldsymbol{\Pi}_{25}&\boldsymbol{\Pi}_{26}\\ *&*&\boldsymbol{\Pi}_{33}&\boldsymbol{\Pi}_{34}&\boldsymbol{0}&\boldsymbol{0}\\ *&*&*&\boldsymbol{\Pi}_{44}&\boldsymbol{0}&\boldsymbol{0}\\ *&*&*&*&\boldsymbol{\Pi}_{55}&\boldsymbol{0}\\ *&*&*&*&*&\boldsymbol{\Pi}_{66}\end{bmatrix}<\boldsymbol{0}; \tag{22}$$

$$\begin{bmatrix}\boldsymbol{\Pi}'_{11}&\boldsymbol{\Pi}'_{12}&\boldsymbol{\Pi}_{13}&\boldsymbol{\Pi}_{14}&\boldsymbol{0}&\tilde{\boldsymbol{X}}^{\mathrm{T}}\\ *&\boldsymbol{\Pi}'_{22}&\boldsymbol{\Pi}_{23}&\boldsymbol{\Pi}_{24}&\boldsymbol{\Pi}_{25}&\tilde{\boldsymbol{X}}^{\mathrm{T}}\\ *&*&\boldsymbol{\Pi}_{33}&\boldsymbol{\Pi}_{34}&0&\tilde{\boldsymbol{X}}^{\mathrm{T}}\\ *&*&*&\boldsymbol{\Pi}_{44}&0&\tilde{\boldsymbol{X}}^{\mathrm{T}}\\ *&*&*&*&\boldsymbol{\Pi}_{55}&\boldsymbol{0}\\ *&*&*&*&*&\boldsymbol{\Pi}'_{66}\end{bmatrix}<\boldsymbol{0}; \tag{23}$$

$$\begin{bmatrix}\boldsymbol{T}_{11}&\boldsymbol{T}_{12}\\ *&\boldsymbol{T}_{22}\end{bmatrix}<\boldsymbol{0},\ \begin{bmatrix}\boldsymbol{T}'_{11}&\boldsymbol{T}'_{12}\\ *&\boldsymbol{T}'_{22}\end{bmatrix}<\boldsymbol{0}; \tag{24}$$

$$\begin{bmatrix}\boldsymbol{Q}_1&\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\\ *&m_1\tilde{P}\end{bmatrix}>\boldsymbol{0},\ \begin{bmatrix}\boldsymbol{Q}_3&n_1\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\\ *&m_2\tilde{\boldsymbol{P}}\end{bmatrix}>\boldsymbol{0},$$
$$\begin{bmatrix}\boldsymbol{Q}_5&n_2\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\\ *&m_3\tilde{\boldsymbol{P}}\end{bmatrix}>\boldsymbol{0}. \tag{25}$$

则系统(21)满足H_∞性能指标

$$\|\boldsymbol{\eta}(t)\|_2^2\leqslant\gamma_2^2\Big[\|\boldsymbol{w}(t)\|_2^2+\sum_{k=0}^{+\infty}(j_{k+1}-j_k)(\|\boldsymbol{e}_x(j_k)\|_2^2+\|\boldsymbol{e}_f(j_k)\|_2^2)\Big],$$

通过协同求取得到触发权矩阵$\boldsymbol{\Phi}$与安全控制器增益$\boldsymbol{K}_j=(\tilde{\boldsymbol{P}}\boldsymbol{B}_i)^{+}\boldsymbol{K}_{1j}$. 其中

$$\boldsymbol{\Pi}_{11}=\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i+\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}-n_1\tilde{\boldsymbol{P}}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i+\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}+h_2n_2\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i+h_2n_1(\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i+\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}})+3\tilde{\boldsymbol{X}}+3\tilde{\boldsymbol{X}}^{\mathrm{T}},$$
$$\boldsymbol{\Pi}_{12}=\boldsymbol{K}_{1j}+n_1\tilde{\boldsymbol{P}}+h_2n_1\boldsymbol{K}_{1j}-h_2n_1\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}+3\tilde{\boldsymbol{X}}-\tilde{\boldsymbol{X}}^{\mathrm{T}}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j}-\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}+h_2n_2\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j},$$
$$\boldsymbol{\Pi}_{13}=3\tilde{\boldsymbol{X}}-8\tilde{\boldsymbol{X}}^{\mathrm{T}},\ \boldsymbol{\Pi}_{14}=3\tilde{\boldsymbol{X}}+12\tilde{\boldsymbol{X}}^{\mathrm{T}},$$
$$\boldsymbol{\Pi}_{22}=-n_1\tilde{\boldsymbol{P}}+h_2n_3\tilde{\boldsymbol{P}}+\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}-h_2n_1(\boldsymbol{K}_{1j}+\boldsymbol{K}_{1j}^{\mathrm{T}}-\tilde{\boldsymbol{X}}-\tilde{\boldsymbol{X}}^{\mathrm{T}}),$$
$$\boldsymbol{\Pi}_{23}=-\tilde{\boldsymbol{X}}-8\tilde{\boldsymbol{X}}^{\mathrm{T}},\ \boldsymbol{\Pi}_{24}=-\tilde{\boldsymbol{X}}+12\tilde{\boldsymbol{X}}^{\mathrm{T}},$$
$$\boldsymbol{\Pi}_{25}=\frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}},\ \boldsymbol{\Pi}_{26}=h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}},$$
$$\boldsymbol{\Pi}_{33}=-8\tilde{\boldsymbol{X}}-8\tilde{\boldsymbol{X}}^{\mathrm{T}},\ \boldsymbol{\Pi}_{34}=-8\tilde{\boldsymbol{X}}+12\tilde{\boldsymbol{X}}^{\mathrm{T}},$$

$$\boldsymbol{\Pi}_{44}=12\tilde{\boldsymbol{X}}+12\tilde{\boldsymbol{X}}^{\mathrm{T}},\ \boldsymbol{\Pi}_{55}=\frac{h_2^2}{4}m_3\tilde{\boldsymbol{P}},$$

$$\boldsymbol{\Pi}_{66}=-h_2n_2\tilde{\boldsymbol{P}},$$

$$\begin{aligned}\boldsymbol{\Pi}'_{11}=&\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i^{\mathrm{T}}+\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}+\tilde{\boldsymbol{P}}\breve{\boldsymbol{A}}_i+\\&\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}-n_1\tilde{\boldsymbol{P}}+h_2m_1\tilde{\boldsymbol{P}}+3\tilde{\boldsymbol{X}}+3\tilde{\boldsymbol{P}}^{\mathrm{T}},\end{aligned}$$

$$\begin{aligned}\boldsymbol{\Pi}'_{12}=&\boldsymbol{K}_{1j}+n_1\tilde{\boldsymbol{P}}+3\tilde{\boldsymbol{X}}-\tilde{\boldsymbol{X}}^{\mathrm{T}}-\\&\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j},\end{aligned}$$

$$\boldsymbol{\Pi}'_{22}=-h_2n_3\tilde{\boldsymbol{P}}-n_1\tilde{\boldsymbol{P}}+\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}-\tilde{\boldsymbol{X}}-\tilde{\boldsymbol{X}}^{\mathrm{T}},$$

$$\boldsymbol{\Pi}'_{66}=-\frac{1}{9h_2n_2}\tilde{\boldsymbol{P}}^{-1},$$

$$\boldsymbol{T}_{11}=\begin{bmatrix}\boldsymbol{\Pi}_{11}+\boldsymbol{I} & \boldsymbol{\Pi}_{12} & \boldsymbol{\Pi}_{13} & \boldsymbol{\Pi}_{14} & \boldsymbol{\Psi}_{15} & \boldsymbol{\Psi}_{16}\\ * & \boldsymbol{\Psi}_{22} & \boldsymbol{\Pi}_{23} & \boldsymbol{\Pi}_{24} & -h_2n_1\boldsymbol{K}_{1j} & \boldsymbol{\Psi}_{26}\\ * & * & \boldsymbol{\Pi}_{33} & \boldsymbol{\Pi}_{34} & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & \boldsymbol{\Pi}_{44} & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & * & -\gamma_2^2\boldsymbol{I} & \boldsymbol{\Psi}_{56}\\ * & * & * & * & * & \boldsymbol{\Psi}_{56}\end{bmatrix},$$

$$\boldsymbol{T}_{12}=\begin{bmatrix}\boldsymbol{\Psi}_{17} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\\ \boldsymbol{\Psi}_{27} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\\ \boldsymbol{\Psi}_{57} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & h_1n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\\ \boldsymbol{\Psi}_{67} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\end{bmatrix},$$

$$\boldsymbol{T}_{22}=\begin{bmatrix}\boldsymbol{\Psi}_{77} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\\ * & \sigma_m\boldsymbol{\Phi} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & * & -h_2n_2\tilde{\boldsymbol{P}}\end{bmatrix},$$

$$\boldsymbol{T}'_{11}=\begin{bmatrix}\boldsymbol{\Pi}'_{11}+\boldsymbol{I} & \boldsymbol{\Pi}'_{12} & \boldsymbol{\Pi}_{13} & \boldsymbol{\Pi}_{14} & \boldsymbol{\Psi}'_{15} & \boldsymbol{\Psi}'_{16}\\ * & \boldsymbol{\Psi}'_{22} & \boldsymbol{\Psi}'_{23} & \boldsymbol{\Psi}'_{24} & \boldsymbol{0} & \boldsymbol{\Psi}'_{26}\\ * & * & \boldsymbol{\Psi}'_{33} & \boldsymbol{\Psi}'_{34} & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & \boldsymbol{\Psi}'_{44} & \boldsymbol{0} & \boldsymbol{0}\\ * & * & * & * & \boldsymbol{\Psi}'_{55} & \boldsymbol{\Psi}'_{56}\\ * & * & * & * & * & \boldsymbol{\Psi}'_{66}\end{bmatrix},$$

$$\boldsymbol{T}'_{12}=\begin{bmatrix}\boldsymbol{\Psi}'_{17} & \boldsymbol{0} & \boldsymbol{0} & \tilde{\boldsymbol{X}}^{\mathrm{T}} & \boldsymbol{0}\\ \boldsymbol{\Psi}'_{27} & \boldsymbol{0} & \boldsymbol{0} & \tilde{\boldsymbol{X}}^{\mathrm{T}} & \frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}\\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \tilde{\boldsymbol{X}}^{\mathrm{T}} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \tilde{\boldsymbol{X}}^{\mathrm{T}} & \boldsymbol{0}\\ \boldsymbol{\Psi}'_{57} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}\\ \boldsymbol{\Psi}'_{67} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0}\end{bmatrix},$$

$$\begin{aligned}\boldsymbol{\Psi}_{15}=&\boldsymbol{K}_{1j}+h_2n_2\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j}+h_2n_1\boldsymbol{K}_{1j}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j},\end{aligned}$$

$$\begin{aligned}\boldsymbol{\Psi}_{16}=&-\boldsymbol{P}\boldsymbol{E}_{fi}-\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi}-\\&h_2n_2\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi}-h_2n_1\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi},\end{aligned}$$

$$\boldsymbol{\Psi}_{17}=\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi}+h_2n_1\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi},$$

$$\begin{aligned}\boldsymbol{\Psi}_{22}=&h_2n_3\tilde{\boldsymbol{P}}-n_1\tilde{\boldsymbol{P}}-\tilde{\boldsymbol{X}}-\tilde{\boldsymbol{X}}^{\mathrm{T}}+\\&\frac{h_2^2}{4}m_2\tilde{\boldsymbol{P}}-h_2n_1(\boldsymbol{K}_{1j}+\boldsymbol{K}_{1j}^{\mathrm{T}}),\end{aligned}$$

$$\boldsymbol{\Psi}_{26}=h_2n_1\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi}-\frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{fi}-h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{fi},$$

$$\boldsymbol{\Psi}_{27}=-\frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{wi}-h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{wi}-h_2n_1\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi},$$

$$\boldsymbol{\Psi}_{56}=-\frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{fi}-h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{fi},$$

$$\boldsymbol{\Psi}_{57}=h_2n_2\boldsymbol{K}_{1j}^{\mathrm{T}}\boldsymbol{E}_{wi}+\frac{h_2^2}{4}m_3\boldsymbol{K}_{1j}^{\mathrm{T}}wi,$$

$$\boldsymbol{\Psi}_{66}=-\gamma_2^2\boldsymbol{I}+\frac{h_2^2}{4}m_3\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi}+h_2n_2\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi},$$

$$\boldsymbol{\Psi}_{67}=-\frac{h_2^2}{4}m_3\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi}-h_2n_2\boldsymbol{E}_{fi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi},$$

$$\boldsymbol{\Psi}_{77}=-\gamma_2^2\boldsymbol{I}+\frac{h_2^2}{4}m_3\boldsymbol{E}_{wi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi}+h_2n_2\boldsymbol{E}_{wi}^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi},$$

$$\boldsymbol{\Psi}'_{15}=K_{1j}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{1j},$$

$$\boldsymbol{\Psi}'_{16}=-\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi}-\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\tilde{\boldsymbol{P}}\boldsymbol{E}_{fi},$$

$$\boldsymbol{\Psi}'_{17}=\tilde{\boldsymbol{P}}\boldsymbol{E}_{wi}+\frac{h_2^2}{4}m_3\breve{\boldsymbol{A}}_i^{\mathrm{T}}\boldsymbol{K}_{wi}.$$

定理2的证明略.

注4　当限定指标γ_2时,可通过下式求取使系统安全运行的最大允许时延h_2^m:

$$\begin{aligned}&\max_{\tilde{P},\tilde{X},K_{1j},Q_1,Q_3,Q_5,\gamma_2}\ h_2^m;\\&\text{s.t. }\tilde{\boldsymbol{P}}>\boldsymbol{0},\text{式(22)}\sim\text{(25)}.\end{aligned}\tag{26}$$

进而通过式(6)可得被动容侵下DoS攻击下系统最大允许连续丢包数

$$\tau_{\mathrm{Ma}}^{\mathrm{DoS}}=\Big\lfloor\frac{h_2^m-h_{t_{k_2}}^{\max}}{h_{t_k}^{\max}}\Big\rfloor.\tag{27}$$

其中:$\lfloor\ \rfloor$为向下取整符号,$\tau_{\mathrm{Ma}}^{\mathrm{DoS}}$为被动容侵下DoS攻击引起的最大连续丢包上界.

5　仿真研究与结果分析

5.1　实验描述

采用四容水箱仿真实例[21]验证本文研究结果的有效性,具体模型参数如下:

$$\boldsymbol{A}_1=\begin{bmatrix}-0.016 & 0 & 0.042 & 0\\ 0 & -0.011 & 0 & 0.033\\ 0 & 0 & -0.042 & 0\\ 0 & 0 & 0 & -0.033\end{bmatrix},$$

$$\boldsymbol{A}_2=\begin{bmatrix}-0.022 & 0 & 0.061 & 0\\ 0 & -0.018 & 0 & 0.049\\ 0 & 0 & -0.064 & 0\\ 0 & 0 & 0 & -0.049\end{bmatrix},$$

$$\boldsymbol{A}_3=\begin{bmatrix}-0.031 & 0 & 0.053 & 0\\ 0 & -0.021 & 0 & 0.067\\ 0 & 0 & -0.083 & 0\\ 0 & 0 & 0 & -0.061\end{bmatrix},$$

$$\boldsymbol{A}_4=\begin{bmatrix}-0.039 & 0 & 0.106 & 0\\ 0 & -0.027\,6 & 0 & 0.082\,6\\ 0 & 0 & -0.107 & 0\\ 0 & 0 & 0 & -0.082\,7\end{bmatrix},$$

$$\boldsymbol{B}_1=\begin{bmatrix}0.083 & 0\\ 0 & 0.063\\ 0 & 0.048\\ 0.031 & 0\end{bmatrix},\ \boldsymbol{B}_2=\begin{bmatrix}0.124\,6 & 0\\ 0 & 0.093\\ 0 & 0.071\\ 0.045 & 0\end{bmatrix},$$

$$\boldsymbol{B}_3=\begin{bmatrix}0.165 & 0\\ 0 & 0.125\\ 0 & 0.097\\ 0.063 & 0\end{bmatrix},\ \boldsymbol{B}_4=\begin{bmatrix}0.207\,6 & 0\\ 0 & 0.157\,6\\ 0 & 0.13\\ 0.077\,6 & 0\end{bmatrix},$$

$$\boldsymbol{C}_1=\mathrm{diag}\{0.5\ \ 0.5\ \ 0.5\ \ 0.5\},$$

$$\boldsymbol{C}_2=\mathrm{diag}\{0.48\ \ 0.48\ \ 0.48\ \ 0.48\},$$

$$\boldsymbol{C}_3=\mathrm{diag}\{0.46\ \ 0.46\ \ 0.46\ \ 0.46\},$$

$$\boldsymbol{C}_4=\mathrm{diag}\{0.52\ \ 0.52\ \ 0.52\ \ 0.52\},$$

$$\boldsymbol{E}_{f1}=-[0.083\ \ 0\ \ 0\ \ 0.031]^{\mathrm{T}},$$

$$\boldsymbol{E}_{f2}=-[0.124\,6\ \ 0\ \ 0\ \ 0.046\,4]^{\mathrm{T}},$$

$$\boldsymbol{E}_{f3}=-[0.167\ \ 0\ \ 0\ \ 0.061]^{\mathrm{T}},$$

$$\boldsymbol{E}_{f4}=[0.207\,6\ \ 0\ \ 0\ \ 0.077\,4]^{\mathrm{T}},$$

$$\boldsymbol{E}_{v1}=[0.015\ \ 0\ \ 0.015\ \ 0.015]^{\mathrm{T}},$$

$$\boldsymbol{E}_{v2}=[0.022\,4\ \ 0\ \ 0.022\,4\ \ 0.022\,4]^{\mathrm{T}},$$

$$\boldsymbol{E}_{v3}=[0.030\ \ 0\ \ 0.025\ \ 0.027]^{\mathrm{T}},$$

$$\boldsymbol{E}_{v4}=[0.037\,4\ \ 0\ \ 0.031\ \ 0.032\,6]^{\mathrm{T}},$$

$$\boldsymbol{E}_{\omega1}=\begin{bmatrix}0.01\\ 0.01\\ 0\\ 0.01\end{bmatrix},\ \boldsymbol{E}_{\omega2}=\begin{bmatrix}0.016\\ 0.016\\ 0\\ 0.016\end{bmatrix},$$

$$\boldsymbol{E}_{\omega3}=\begin{bmatrix}0.02\\ 0.02\\ 0\\ 0.02\end{bmatrix},\ \boldsymbol{E}_{\omega4}=\begin{bmatrix}0.024\\ 0.024\\ 0\\ 0.024\end{bmatrix}.$$

系统扰动$\boldsymbol{w}(t)$和噪声$v(i_k)$均服从$N(0.1,0.01)$的独立白噪声过程,初始状态$x(0)=[4\ \ 4\ \ 2\ \ 2]^{\mathrm{T}}$,采样周期$h=0.1\,\mathrm{s}$,令$\sigma_m=0.001,\sigma_M=0.01,\sigma(0)=\sigma_m,\alpha=0.01,\beta=1,\varepsilon=0.01,n_1=1.2,n_2=5.6,n_3=10,\gamma_1=3.2,h_1=0.1\,\mathrm{s}$. 执行器时变故障为

$$\boldsymbol{f}(t)=\begin{cases}0,\ t\leqslant 200;\\ 2+2\sin 0.01\pi(t-200),\ 200<t\leqslant 800.\end{cases}$$

根据定理1求取观测器增益矩阵$\boldsymbol{L}_j$和故障估计增益矩阵$\boldsymbol{F}_j$分别为

$$\boldsymbol{L}_1=\begin{bmatrix}5.187\,9 & -1.974\,8 & 0.035\,2 & -0.365\,9\\ 0.245\,5 & 1.866\,5 & 0.009\,0 & 0.014\,6\\ -0.006\,3 & 0.015\,0 & 1.918\,8 & -0.005\,1\\ 1.370\,6 & -0.809\,3 & -0.003\,7 & 1.785\,4\end{bmatrix},$$

$$\boldsymbol{L}_2=\begin{bmatrix}6.497\,3 & -4.393\,3 & 0.042\,6 & -1.733\,8\\ 0.203\,8 & 2.058\,0 & 0.016\,4 & 0.123\,7\\ -0.010\,3 & 0.028\,4 & 1.921\,9 & -0.000\,6\\ 1.816\,4 & -0.588\,3 & -0.003\,1 & 1.350\,0\end{bmatrix},$$

$$\boldsymbol{L}_3=\begin{bmatrix}8.153\,5 & -7.582\,7 & 0.010\,0 & -3.700\,8\\ 0.186\,1 & 2.182\,4 & 0.018\,0 & 0.200\,1\\ -0.017\,0 & 0.044\,9 & 1.928\,9 & 0.012\,2\\ 2.392\,7 & -2.681\,0 & -0.011\,4 & 0.683\,6\end{bmatrix},$$

$$\boldsymbol{L}_4=\begin{bmatrix}7.949\,1 & -9.253\,7 & 0.078\,3 & -4.929\,9\\ 0.020\,9 & 2.222\,2 & 0.013\,8 & 0.202\,3\\ 0.005\,6 & 0.022\,0 & 1.784\,1 & -0.013\,1\\ 2.240\,2 & -3.224\,1 & -0.013\,5 & 1.060\,0\end{bmatrix},$$

$$\boldsymbol{F}_1=[-35.224\,0\ \ 44.736\,1\ \ 1.017\,19\ \ 18.254\,3],$$

$$\boldsymbol{F}_2=[-48.858\,6\ \ 81.347\,1\ \ 1.441\,6\ \ 40.078\,2],$$

$$\boldsymbol{F}_3=[-62.536\,5\ \ 116.107\,4\ \ 1.514\,5\ \ 63.165\,9],$$

$$\boldsymbol{F}_4=[-57.355\,3\ \ 121.416\,2\ \ 1.527\,4\ \ 64.566\,4].$$

在定理2中,选取$n_1=5,n_2=0.1,n_3=0.01,m_1=m_2=m_3=2,\gamma_2=2.8,h_2=2.6\,\mathrm{s},h_{t_k}^{\max}=0.5\,\mathrm{s}$. 根据定理2协同求取矩阵$\boldsymbol{\Phi}$和$\boldsymbol{K}_j$分别为

$$\boldsymbol{\Phi}=\mathrm{diag}\{39.987\,1\ \ 39.987\,1\ \ 39.987\,1\ \ 39.987\,1\},$$

$$\boldsymbol{K}_1=\begin{bmatrix}-9.247\,3 & -0.556\,5 & -0.184\,6 & -3.004\,7\\ 0.058\,4 & -7.536\,6 & -7.495\,3 & -1.220\,6\end{bmatrix},$$

$$\boldsymbol{K}_2=\begin{bmatrix}-6.124\,0 & -0.380\,7 & -0.342\,6 & -1.886\,3\\ -0.017\,6 & -5.018\,7 & -4.783\,6 & -0.942\,6\end{bmatrix},$$

$$\boldsymbol{K}_3=\begin{bmatrix}-4.450\,0 & -0.309\,7 & -0.182\,5 & -1.449\,3\\ -0.020\,3 & -3.652\,7 & -3.386\,4 & -0.794\,9\end{bmatrix},$$

$$\boldsymbol{K}_4=\begin{bmatrix}-3.522\,8 & -0.249\,9 & -0.489\,1 & -1.080\,1\\ -0.060\,2 & -2.692\,8 & -2.522\,8 & -0.654\,2\end{bmatrix}.$$

由式(26)求得系统安全运行时最大允许时延 $h_2^m=3.252\,7\,\mathrm{s}$,则攻击发生时系统所允许的最大丢包数为 $\tau_{\mathrm{Ma}}^{\mathrm{DoS}}=0.5$. 取安全因子 $\theta=0.85$,结合DoS攻击检测算法中 $h_{j_{k_3}}\geqslant\theta h_2^m$,则在安全裕度内的最大连续丢包数 $\tau_{\mathrm{Ma}}^{\mathrm{DoS}}=4$. 若实际系统中遭受到大于此丢包数的DoS攻击,则认为是大能量的. 假设DoS攻击发生在100 s至800 s之间, 其中在100 s $<t<$ 400 s内为小能量DoS攻击,400 s $\leqslant t<$ 800 s内为大能量DoS攻击.

为了凸显本文方法的优越性,在ADETCS下,从3个方面进行实验分析,包括:被动容侵/主动容错,本文方法与其他主被动容侵/主动容错的比较,不同触发机制在节约网络通讯资源方面的差异.

5.2　ADETCS下主被动与被动的容侵方法对比分析

5.2.1　ADETCS下被动容侵/主动容错控制方法

这里不进行DoS攻击能量等级的区分,仅以弹性控制(即定理2)求取的控制器对系统实施被动容侵,其结果如图2所示. 可以看出,$t\leqslant$ 100 s时无故障、无攻击,只存在外部扰动,系统状态已逐渐收敛至0,系统具有扰动抑制能力;100 s $<t\leqslant$ 200 s时,无故障,但存在小能量DoS攻击,在弹性被动容侵控制下,系统状态保持在0附近;200 s $<t\leqslant$ 400 s时增加了执行器故障,除故障峰值处波动较大外,其他时刻均趋于0,说明存在小能量DoS攻击和执行器故障时,被动容侵/主动容错方法具有良好的控制作用;而400 s $<t\leqslant$ 800 s时,大能量DoS攻击入侵系统,除系统状态 x_2 保持稳定外,其余状态均在400 s后已开始发散,说明被动容侵/主动容错控制策略即使在ADETCS下也不能确保系统正常运行.

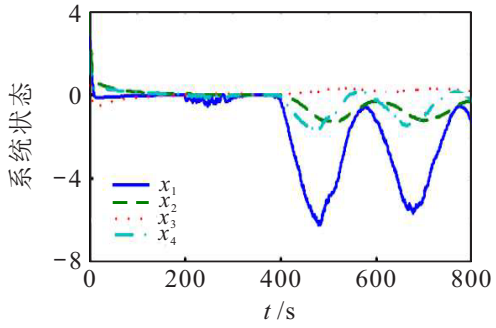
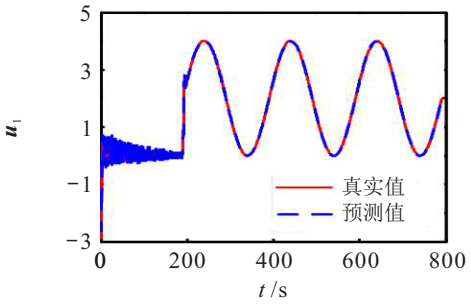


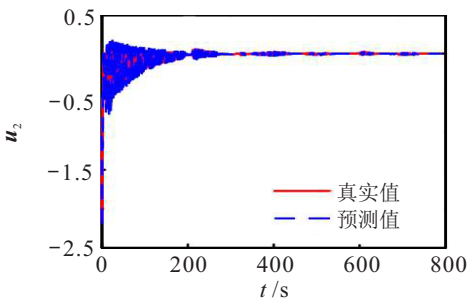
图 2　ADETCS下被动容侵/主动容错控制系统状态

5.2.2　ADETCS下附加ELM的主被动容侵/主动容错控制方法

以ADETCS下未遭受和遭受小能量DoS攻击时系统为对象,采集控制分量 $\boldsymbol{u}_1$ 的时间序列 $u_{1j_1},u_{1j_2},\ldots,u_{1j_N}$,数据集共计 $N=6\,000$ 个样本;进一步令嵌入维数 $n=10$,将该数据集转化为样本集 $\boldsymbol{S}_1=\{(\boldsymbol{u}_{1j_1},\boldsymbol{l}_{1j_1}),(\boldsymbol{u}_{1j_2},\boldsymbol{l}_{1j_2}),\ldots,(\boldsymbol{u}_{1jk},\boldsymbol{l}_{1jk})\}_{k-1}^{N-n}$,并将 $\boldsymbol{S}_1$ 的80 %作为训练集训练 $\boldsymbol{u}_1$ 的ELM1预测模型,20 %作为测试集用于模型测试. 其中,$\boldsymbol{u}_{1j_k}=[u_{1j_k},u_{1j_{k+1}},\ldots,u_{1j_{k+n+1}}]^{\mathrm{T}}$ 为预测模型输入,$\boldsymbol{l}_{1j_k}=\boldsymbol{u}_{1j_{k+n}}$ 为预测模型输出. 同样对控制分量 $\boldsymbol{u}_2$ 建立样本集 $\boldsymbol{S}_2=\{(\boldsymbol{u}_{2j_1},\boldsymbol{l}_{2j_1}),(\boldsymbol{u}_{2j_2},\boldsymbol{l}_{2j_2}),\ldots,(\boldsymbol{u}_{2j_k},\boldsymbol{l}_{2j_k})\}_{k-1}^{N-n}$,亦可得到 $\boldsymbol{u}_2$ 的ELM2预测模型. 图3给出了控制量的真实值与基于ELM预测值的对比.



(a)　$\boldsymbol{u}_1$ 真实值与预测值对比

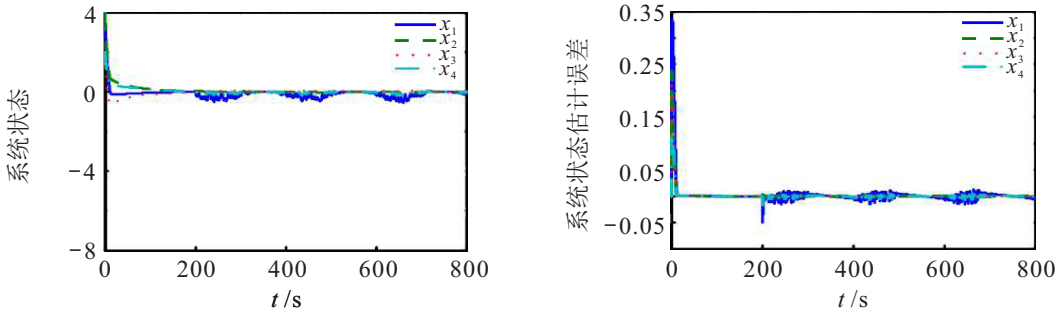


(b)　$\boldsymbol{u}_2$ 真实值与预测值对比

图 3　控制量真实值与预测值对比

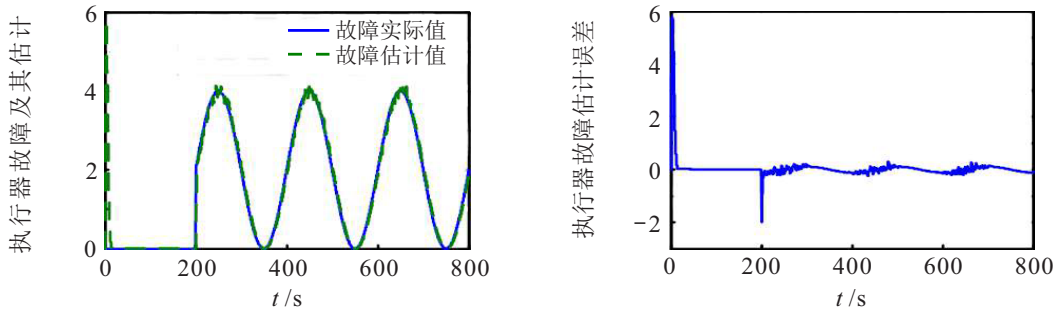
根据ELM预测模型对因大能量DoS攻击造成的控制量丢失进行实时补偿,系统状态及其估计、执行器故障及其估计变化如图4和图5所示. 为显现文中基于ELM预测模型主动容侵的优势,在ADETCS下采用文献[4]基于PD的主被动混合容侵方法,选用 $k_{\mathrm{P}}=1.2$、$k_{\mathrm{D}}=0.3$,得到系统的状态及状态估计误差如图6所示.

图4中,400 s $\leqslant$ 800 s时,即使大能量DoS攻击入侵,系统状态均能保持稳定,且系统状态估计误差在±0.01之间波动. 图5中,执行器故障估计值除在故障发生瞬间有较大波动外,其余时刻估计误差在±0.1之间波动. 原因在于附加了基于ELM预测补偿的主



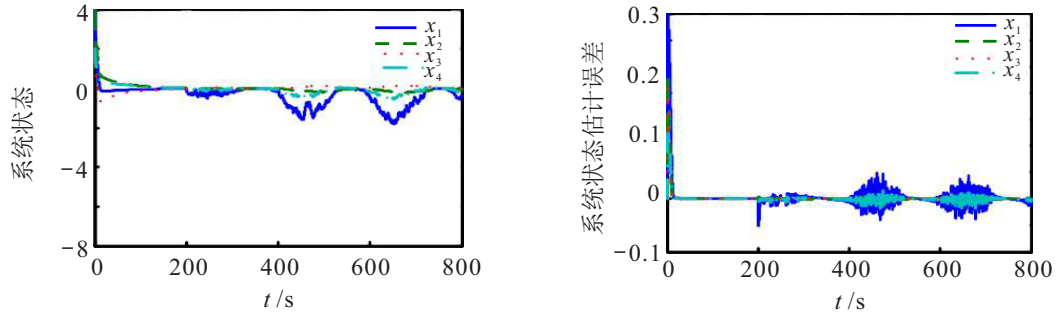
(a) 系统状态 (b) 系统状态估计误差

图 4 ADETCS下主被动容侵/主动容错系统状态估计结果



(a) 执行器故障及其估计 (b) 执行器故障估计误差

图 5 ADETCS下主被动容侵/主动容错的故障估计结果



(a) 系统状态 (b) 系统状态估计误差

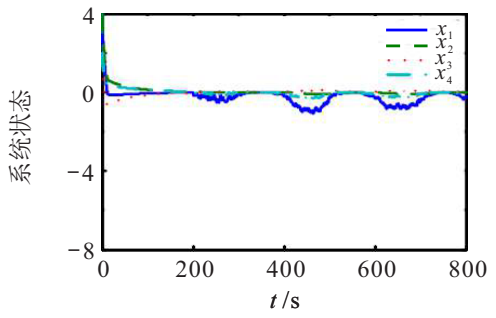
图 6 ADETCS下基于PD主被动容侵/主动容错的系统状态估计结果

动容侵策略后,即使DoS攻击致使控制量的传输间隔趋近系统最大允许时延,超出被动弹性容侵范围,但由于ELM模型进行了有针对性的控制量预测补偿,系统防御能力得到了有效提升,实现了对更严重DoS攻击的主动精准应对. 对比图4与图6,基于ELM的主被动混合容侵方法,系统性能明显优于基于PD的方法,原因是基于ELM预测模型更精准地描述了控制量时序之间关系,可更精确地补偿控制量的缺失. 基于PD的方法需经过试探选择参数k_{P}与k_{D},无规律可循,控制量补偿不准确亦是必然.

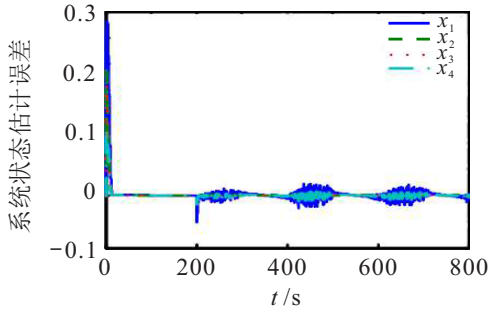
5.3 DETCS下基于ELM主动与弹性被动容侵/主动容错控制方法

为进一步验证新型ADETCS的优势,与文献[12]固定触发阈值的DETCS进行比较. 与ADETCS下构造样本集类似,在DETCS下同样取6 000组数据,通过ELM建立相应的预测模型,图7给出了DETCS下基于ELM主动与弹性被动容侵/主动容错的系统状态及估计. 对比图4与图7,在同样的DoS攻击与执行器故障下,基于ADETCS的系统控制性能更好. 图8给出了ADETCS下触发阈值的变化,表1进一步列出了不同触发机制的数据传输量比较.

图8中,触发参数在ADETCS下是动态变化的,触发参数大则数据传输量少,由于一味地增大触发参数会使系统稳定性变差,限定其最大值为0. 01,在确保系统稳定性的前提下,使触发参数根据系统性能动态变化,从而动态调整数据传输量. 与周期时间触发机制需传输8 000个数据相比,ADETCS下仅需传输1 475个数据,传输周期为0.542 s,传输率为18.4 %. 观察表1,DETCS下数据传输量为4 950,传输周期为0.162 s,传输率为61.8 %; ADETCS使“静态”



(a)　系统状态



(b)　系统状态估计误差

图 7　DETCS下主被动容侵/主动容错系统状态估计结果

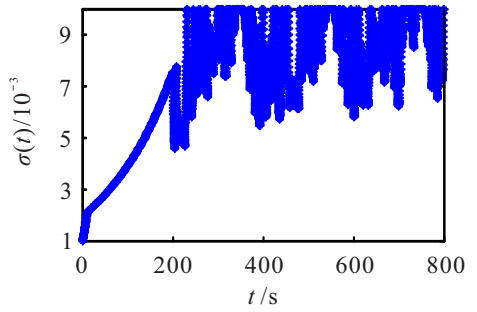


图 8　ADETCS下触发阈值变化

表 1　不同触发机制的数据传输量比较

触发机制	数据传输量	传输率/%	传输周期/s
DETCS[12]	4 950	61.8	0.162
ADETCS[13]	1 592	19.9	0.503
本文ADETCS	1 475	18.4	0.542

不变的触发参数转换为“动态”自适应的变化,网络资源得到了最大化地节约. 此外,与文献[13]相比,本文的ADETCS因引入了触发阈值的上界σ_M使得数据传输的更少,更有利于网络资源的节约.

6　结　论

本文针对具有DoS攻击与执行器故障非线性ICPS,研究了ADETCS下双重安全控制与通讯的协同设计问题. 通过自适应事件触发机制中“动态”变化的触发参数节约了更多的网络通信资源,促使系统性能与网络资源得以优化折衷. 基于系统最大允许时延,建立了攻击检测机制以区分不同能量等级的DoS攻击,将小能量DoS攻击的机理解析被动容侵与大能量DoS攻击的数据驱动主动容侵相融合,较单一弹性控制扩大了系统对DoS攻击的防御范围. 在ADETCS下,结合新型Bessel-Legendre不等式、相互凸组合引理等,分别得到了满足系统性能的鲁棒观测器及双重安全控制器,使双重安全控制与网络通信得到了自适应协同. 最后通过四容水箱仿真案例验证了本文方法的有效性. 在ADETCS下,如何随触发参数的变化获取自适应的控制器,将是未来可期和极具挑战性的工作.

参考文献(References)

[1] Zhang D, Wang Q G, Feng G, et al. A survey on attack detection, estimation and control of industrial cyber-physical systems[J]. ISA Transactions, 2021, 116: 1-16.

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

[3] 孙洪涛, 彭晨, 王志文. DoS攻击下的信息物理系统事件触发预测控制设计[J]. 控制与决策, 2019, 34(11): 2303-2309.
(Sun H T, Peng C, Wang Z W. Event-triggered predictive control of cyber-physical systems under DoS attacks[J]. Control and Decision, 2019, 34(11): 2303-2309.)

[4] 李炜, 韩小武, 李亚洁. 基于DoS攻击能量分级的ICPS综合安全控制与通信协同设计[J]. 信息与控制, 2022, 51(3): 257-270.
(Li W, Han X W, Li Y J. Co-design of integrated security control and communication of ICPS based on DoS attack energy classification[J]. Information and Control, 2022, 51(3): 257-270.)

[5] 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.

[6] Li F F, Tang Y. False data injection attack for cyber-physical systems with resource constraint[J]. IEEE Transactions on Cybernetics, 2020, 50(2): 729-738.

[7] Tahoun A H, Arafa M. Secure control design for nonlinear cyber-physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels[J]. ISA Transactions, 2022, 128: 294-308.

[8] Zhang K K, Keliris C, Polycarpou M M, et al. Discrimination between replay attacks and sensor faults for cyber-physical systems via event-triggered communication[J]. European Journal of Control, 2021, 62: 47-56.

[9] Zhang Z P, Wang H M. Resilient decentralized adaptive tracking control for nonlinear interconnected systems

with unknown control directions against DoS attacks[J]. Applied Mathematics and Computation, 2022, 415: 126717.

[10] Wang P B, Ren X M, Zheng D D. Event-triggered resilient control for cyber-physical systems under periodic DoS jamming attacks[J]. Information Sciences, 2021, 577(C): 541-556.

[11] Zhang X M, Han Q L, Ge X H, et al. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(8): 3616-3626.

[12] Peng C, Yang T C. Event-triggered communication and H_∞ control co-design for networked control systems[J]. Automatica, 2013, 49(5): 1326-1332.

[13] 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.

[14] 相赟, 林崇, 陈兵. 自适应事件触发网络化非线性系统滤波器设计[J]. 控制理论与应用, 2021, 38(1): 1-12.
(Xiang Y, Lin C, Chen B. Filter design of networked nonlinear systems with adaptive event trigger[J]. Control Theory & Applications, 2021, 38(1): 1-12.)

[15] Ye Z H, Zhang D, Wu Z G. Adaptive event-based tracking control of unmanned marine vehicle systems with DoS attack[J]. Journal of the Franklin Institute, 2021, 358(3): 1915-1939.

[16] Zhang K, Jiang B, Staroswiecki M. Dynamic output feedback-fault tolerant controller design for Takagi-Sugeno fuzzy systems with actuator faults[J]. IEEE Transactions on Fuzzy Systems, 2010, 18(1): 194-201.

[17] 肖会芹, 何勇, 吴敏, 等. 基于T-S模糊模型的采样数据网络控制系统H_∞输出跟踪控制[J]. 自动化学报, 2015, 41(3): 661-668.
(Xiao H Q, He Y, Wu M, et al. H_∞ output tracking control for sampled-data networked control systems in T-S fuzzy model[J]. Acta Automatica Sinica, 2015, 41(3): 661-668.)

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

[19] Huang G B, Wang D H, Lan Y. Extreme learning machines: A survey[J]. International Journal of Machine Learning and Cybernetics, 2011, 2(2): 107-122.

[20] Qiu A B, Zhang J, Jiang B, et al. Event-triggered sampling and fault-tolerant control co-design based on fault diagnosis observer[J]. Journal of Systems Engineering and Electronics, 2018, 29(1): 176-186.

[21] Johansson K H, Nunes J L R. A multivariable laboratory process with an adjustable zero[C]. Proceedings of the 1998 American Control Conference. Philadelphia, 2002: 2045-2049.

作者简介

赵莉(1987−), 女, 博士生, 从事信息物理融合系统容错与容侵控制的研究, E-mail: zhaoliwwd@163.com;

李炜(1963−), 女, 教授, 博士生导师, 从事复杂系统建模与预测、CPS安全控制等研究, E-mail: liwei@lut.edu.cn;

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的研究, E-mail: 184129282 @qq.com.