自动化学报
ACTA AUTOMATICA SINICA

基于模糊协同交互型观测器的柔性关节机械臂信息物理融合系统的安全控制

黄鑫 畅晨旭 肖舒怡 李小杭

Secure Control for Flexible-joint Robotic Manipulator Cyber-physical Systems Based on Fuzzy Cooperative Interaction Observer

HUANG Xin, CHANG Chen-Xu, XIAO Shu-Yi, LI Xiao-Hang

在线阅读 View online: https://doi.org/10.16383/j.aas.c240066

基于模糊协同交互型观测器的柔性关节机械臂信息物理融合系统的安全控制

黄 鑫[1] 畅晨旭[1] 肖舒怡[2] 李小杭[3]

摘 要 本文研究了柔性关节机械臂信息物理融合系统 (Cyber-physical systems, CPS) 在传感器测量和执行器输入受到网络攻击时的安全控制问题. 首先, 用 T-S 模糊模型描述柔性关节机械臂 CPS, 描述后的模型可能存在不可测量或可测量但受传感器攻击影响的前件变量 (Premise variables, PVs), 这些 PVs 直接用于构建模糊控制器会影响控制器的控制效果. 因此, 提出一类模糊协同交互观测器来构造新的、可靠的、可利用的 PVs. 同时, 该观测器能够与包含攻击估计误差 (Attack estimation error, AEE) 信息的辅助系统进行协同交互. 与已有结果相比, 所提出的观测器通过协同交互结构, 充分利用了 AEE 信息, 提高了攻击信号的重构精度. 在此基础上, 提出了一种具有攻击补偿结构的安全控制方案, 从而消除了传感器和执行器攻击对柔性关节机械臂 CPS 性能的影响. 仿真结果验证了所提出的安全控制方案的有效性.

关键词 柔性关节机械臂, 信息物理融合系统, 网络攻击, T-S 模糊模型, 协同交互型观测器, 安全控制

引用格式 黄鑫, 畅晨旭, 肖舒怡, 李小杭. 基于模糊协同交互型观测器的柔性关节机械臂信息物理融合系统的安全控制. 自动化学报, 2024, **50**(12): 2487−2498

DOI 10.16383/j.aas.c240066 **CSTR** 32138.14.j.aas.c240066

Secure Control for Flexible-joint Robotic Manipulator Cyber-physical Systems Based on Fuzzy Cooperative Interaction Observer

HUANG Xin[1] CHANG Chen-Xu[1] XIAO Shu-Yi[2] LI Xiao-Hang[3]

Abstract This paper investigates secure control problems of flexible-joint robotic manipulator cyber-physical systems (CPS) against cyber-attacks on sensor measurements and actuator inputs. Firstly, flexible-joint robotic manipulator CPS are described by the T-S fuzzy model, in which there may exist premise variables (PVs) not measured, or measured but influenced by the sensor attacks. If these PVs are directly used to construct the fuzzy controller, the control performance will be affected. Therefore, a fuzzy cooperative interaction observer is proposed to construct new, reliable and available PVs. And also the observers can cooperate with the auxiliary system which contains attack estimation error (AEE) information. Different from existing results, the proposed observer makes full use of the AEE information by the cooperative interaction structure, resulting in improvement of reconstruction accuracy of the attack signal. Furthermore, a class of secure control scheme with the attack compensation structure is given such that the influence of sensor and actuator attacks on flexible-joint robotic manipulator CPS performances is removed. The effectiveness of the proposed secure control scheme is verified by simulation results.

Key words Flexible-joint robotic manipulator, cyber-physical systems (CPS), cyber-attacks, T-S fuzzy model, cooperative interaction observer, secure control

Citation Huang Xin, Chang Chen-Xu, Xiao Shu-Yi, Li Xiao-Hang. Secure control for flexible-joint robotic manipulator cyber-physical systems based on fuzzy cooperative interaction observer. *Acta Automatica Sinica*, 2024, **50**(12): 2487−2498

近年来, 随着信息化和网络化的发展、信息网络与物理过程的深度融合, 信息物理融合系统 (Cyber-physical systems, CPS) 应运而生. 它利用计算、通信和控制等先进技术分析信息, 并通过反馈机制对物理过程实现实时控制, 以实现在自主性、功能

收稿日期 2024-01-31 录用日期 2024-07-25
Manuscript received January 31, 2024; accepted July 25, 2024
吉林省自然科学基金 (YDZJ202201ZYTS379), 国家自然科学基金 (62103094), 中国国家留学基金, 东北电力大学博士科研启动基金 (BSJXM-2021107), 山西省基础研究计划项目 (202203021222101) 资助
Supported by Natural Science Foundation of Jilin Province (YDZJ202201ZYTS379), National Natural Science Foundation of China (62103094), China Scholarship Council, Doctoral Scientific Research Foundation of Northeast Electric Power University (BSJXM-2021107), and Fundamental Research Program of Shanxi Province (202203021222101)
本文责任编委 莫红
Recommended by Associate Editor MO Hong
1. 东北电力大学自动化工程学院 吉林 132012 2. 太原理工大学电气与动力工程学院 太原 030024 3. 北方信息控制研究院集团有限公司信息系统总体部 南京 211100
1. School of Automation Engineering, Northeast Electric Power University, Jilin 132012 2. College of Electrical and Power Engineering, Taiyuan University of Technology, Taiyuan 030024 3. Department of General Information System, Northern Information Control Research Institute Group Co., Ltd., Nanjing 211100

性、效率、可用性、安全性和可靠性方面远远超过当今系统的工程系统[1−2]. 此类系统和应用的例子包括未来的交通系统[3]、智能物流系统[4] 和智能电网[5]等. 而机械臂信息物理融合系统作为 CPS 的一个重要分支, 其在医疗、工业生产、军事、航空航天等领域, 都有广泛的应用[6−9]. 然而, 随着大规模异构物理单元和开放网络的应用, 机械臂信息物理融合系统容易受到恶意网络攻击, 对机械臂信息物理融合系统的成功攻击可能对工业生产、人民生活产生恶劣影响[10−11]. 因此, 如何保障网络攻击下机械臂信息物理融合系统的安全, 具有十分重要的意义.

当前, 针对机械臂信息物理融合系统受到网络攻击的安全控制研究成果已有许多[12−13]. 例如: Liu 等[14] 研究了具有混合触发机制和随机网络攻击的机械臂信息物理融合系统的量化稳定性, 利用李雅普诺夫稳定性理论和线性矩阵不等式, 给出了保证系统渐近稳定性的控制器的设计条件. Wang 等[15] 提出了一种新的弹性动态事件触发机制和相应的模糊动态事件触发控制器, 解决了存在欺骗攻击的机械臂信息物理融合系统的随机指数稳定性问题. Gu 等[16] 为了保障机械臂信息物理融合系统在欺骗攻击的框架下具有良好的稳定性能, 提出一种具有半马尔科夫参数的安全滑模控制器. Han 等[17] 针对机械臂信息物理融合系统受到的有界网络攻击, 设计了一种基于记忆的事件触发机制, 可以减少错误触发事件的发生, 并基于该事件触发机制设计了弹性控制器来消除网络攻击的影响. Li 等[18] 提出一种比例−积分观测器来重构执行器攻击信号, 并基于观测器设计了容错控制器来保障机械臂信息物理融合系统的稳定. 虽然已经取得了很多成果, 但大多数都只关注传感器测量或执行器控制输入中的一个受到攻击的情况, 对于两者都受到攻击的情况还缺乏研究. 此外, 对于攻击信号估计的研究成果, 其没有充分利用攻击估计误差信息, 如果能充分利用该信息将极大地提高攻击信号的重构精度, 基于重构信号所设计的攻击补偿器也能更及时准确地消除攻击对机械臂信息物理融合系统性能的影响. 这些也是本文的研究动机.

由于机械臂信息物理融合系统通常包含非线性结构, 而近几十年来, T-S 模糊模型被证明能够准确地描述非线性模型[19−21]. 进而, 该模型被广泛应用在非线性系统的稳定性分析与控制综合研究中[22−25]. 因此, 本文基于 T-S 模糊模型, 研究单连杆柔性关节机械臂信息物理融合系统在传感器测量和执行器输入受到网络攻击时的安全控制问题. 然而, 当模型的前件变量不可测量或可测量但受到传感器攻击时, 模糊控制器的控制性能将受到影响, 因此本文的工作量体现在:

1) 采用 T-S 模糊模型描述单连杆柔性关节机械臂信息物理融合系统, 充分考虑了前件变量对模糊控制器的影响. 对于不可测量或可测量但受传感器攻击影响的前件变量, 提出了模糊协同交互型观测器来构建新的、可利用且可靠的前件变量.

2) 构建了包含攻击估计误差信息的辅助系统. 通过观测器与辅助系统的协同交互来充分利用攻击估计误差信息, 提高攻击信号的重构精度.

3) 在此基础上, 利用重构攻击信号构建攻击补偿器, 使得现有的模糊控制器在装备该攻击补偿器后能够有效消除网络攻击的影响, 保证受到攻击的系统能够稳定.

本文采用如下记号: $\mathbf{R}^n$, $\mathbf{R}^{n\times m}$ 分别表示实数域的 n 维向量空间和 $n\times m$ 矩阵空间; $\bar{\mathbf{C}}^+$ 表示具有非负实部的复数集合; $\mathcal{H}^{\mathrm{T}}$ 表示矩阵 $\mathcal{H}$ 的转置; $\mathbf{He}(\cdot)$ 表示 $\mathbf{He}(\mathcal{H}) := \mathcal{H}+\mathcal{H}^{\mathrm{T}}$; "$*$"表示对称矩阵的对称项; 方阵 $\mathcal{X}\geq 0$ ($\mathcal{X}>0$) 表示 $\mathcal{X}$ 是一个具有适当维数的对称半正定 (正定) 矩阵; $\lambda_{\min}(\mathcal{X})$(或 $\lambda_{\max}(\mathcal{X})$) 表示矩阵 $\mathcal{X}$ 的最小 (或最大) 特征值; $\mathbf{0}$ 和 I 分别代表合适维数的零矩阵和单位矩阵; $\|\mathcal{X}\|$ 表示 $\mathcal{X}$ 的 2 范数.

1 问题描述

1.1 单连杆柔性关节机械臂系统模型

考虑机器人动力学和执行器动力学耦合的单连杆柔性关节机械臂, 其基于欧拉−拉格朗日方程的动力学模型[6−8] 为:

$$\begin{cases} J_m\ddot{q}_m - k(q_l-q_m)+\delta_a\dot{q}_m = K_\tau u \\ J_l\ddot{q}_m + k(q_l-q_m)+mgb\sin(q_l)=0 \end{cases} \tag{1}$$

其中, q_m 和 q_l 分别为电机轴和连杆的角位移; J_m 和 J_l 分别为电机轴和连杆的惯量; u 表示控制系统的输入转矩; K_τ 为放大器增益; k 为弹簧的弹性系数; δ_a 为粘滞摩擦系数; m 表示连杆质量; g 为重力加速度; b 为连杆质心到关节轴心的距离.

定义 $\xi_1=q_m$, $\xi_2=\dot{q}_m$, $\xi_3=q_l$, $\xi_4=\dot{q}_l$, 则模型 (1) 可以描述为:

$$\begin{cases} \dot{\xi}_1=\xi_2 \\ \dot{\xi}_2=\dfrac{k}{J_m}(\xi_3-\xi_1)-\dfrac{\delta_a}{J_m}\xi_2+\dfrac{K_\tau}{J_m}u \\ \dot{\xi}_3=\xi_4 \\ \dot{\xi}_4=-\dfrac{k}{J_l}(\xi_3-\xi_1)-\dfrac{mgb}{J_l}\sin(\xi_3) \end{cases} \tag{2}$$

令 $\xi=[\xi_1,\ \xi_2,\ \xi_3,\ \xi_4]^{\mathrm{T}}$, 则对应的状态方程为:

$$\dot{\xi}=A(t)\xi+Bu \tag{3}$$

式中,

$$A(t)=\begin{bmatrix}0 & 1 & 0 & 0\\ -\dfrac{k}{J_m} & -\dfrac{\delta_a}{J_m} & \dfrac{k}{J_m} & 0\\ 0 & 0 & 0 & 1\\ \dfrac{k}{J_l} & 0 & -\dfrac{1}{J_l}(k+mgbv(t)) & 0\end{bmatrix}$$

$$B=\begin{bmatrix}0 & \dfrac{K_\tau}{J_m} & 0 & 0\end{bmatrix}^{\mathrm{T}}$$

且 $v(t)=\frac{\sin(\xi_3(t))}{\xi_3(t)}$, $v(t)\in[v_{\min},\ v_{\max}]$.

从中可以看出机械臂系统中含有界非线性项 $v(t)$. 而在 T-S 模糊系统的建模方法中, 扇形非线性建模方法[26] 能够很好地处理该非线性项, 进而形成由“IF-THEN”规则连接前件变量与后件线性模型的 T-S 模糊系统. 于是, 可以利用传统的线性系统控制理论研究非线性系统的控制问题. 因此, 本文利用扇形非线性建模方法, 将上述柔性机械臂系统建模为如下的 T-S 模糊模型:

Rule 1:

IF $v(t)$ **is** $S_{\max}$

THEN $\dot{\xi}(t)=A_1\xi(t)+Bu(t)$

Rule 2:

IF $v(t)$ **is** $S_{\min}$

THEN $\dot{\xi}(t)=A_2\xi(t)+Bu(t)$

式中, $S_{\max}$ 和 $S_{\min}$ 分别为 $v(t)$ 在第 1, 2 条模糊规则的模糊集, A_1, A_2 分别为:

$$A_1=\begin{bmatrix}0 & 1 & 0 & 0\\ -\dfrac{k}{J_m} & -\dfrac{\delta_a}{J_m} & \dfrac{k}{J_m} & 0\\ 0 & 0 & 0 & 1\\ \dfrac{k}{J_l} & 0 & -\dfrac{1}{J_l}(k+mgbv_{\max}) & 0\end{bmatrix}$$

$$A_2=\begin{bmatrix}0 & 1 & 0 & 0\\ -\dfrac{k}{J_m} & -\dfrac{\delta_a}{J_m} & \dfrac{k}{J_m} & 0\\ 0 & 0 & 0 & 1\\ \dfrac{k}{J_l} & 0 & -\dfrac{1}{J_l}(k+mgbv_{\min}) & 0\end{bmatrix}$$

采用单点模糊化、乘机推理和中心平均解模糊化, 得到如下系统:

$$\dot{\xi}(t)=A(\mu)\xi(t)+Bu(t)\tag{4}$$

式中, $A(\mu)=\mu_1A_1+\mu_2A_2$, $\mu_1(v(t))=\frac{v(t)-v_{\min}}{v_{\max}-v_{\min}}$, $\mu_2(v(t))=\frac{v_{\max}-v(t)}{v_{\max}-v_{\min}}$ 和 $\mu_1(v(t))+\mu_2(v(t))=1$.

1.2　单连杆柔性关节机械臂信息物理融合系统

随着加密技术的发展, 通信网络的安全性和可靠性不断提高, 现有的加密通信网络通常能确保一些期望的传感器的测量数据可信. 在可信传感器的帮助下, 本文将考虑如下带有可信传感器的单连杆机械臂信息物理融合系统 (如图 1 所示):

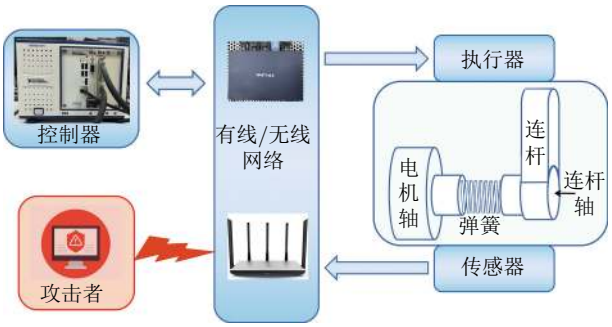

图 1　网络攻击下的单连杆柔性关节机械臂信息物理融合系统

Fig. 1　Single-link flexible-joint robotic manipulator cyber-physical systems under cyber-attacks

$$\begin{cases}\dot{\xi}(t)=A(\mu)\xi(t)+Bu_a(t)\\ y^{(h_1)}=C^{(h_1)}\xi,\quad h_1=1,\ \cdots,\ m-h_a\\ y^{(h_2)}=C^{(h_2)}\xi,\quad h_2=m-h_a+1,\ \cdots,\ m\end{cases}\tag{5}$$

其中, $C^{(h_1)}$、$C^{(h_2)}$ 是具有适当维度的矩阵; h_a 是传感器攻击的维度; $y^{(h_1)}$ 是受加密网络保护的传感器测量值; $y^{(h_2)}$ 是不受加密网络保护的传感器测量值. 定义:

$$y_1=[y^1,\ \cdots,\ y^{(m-h_a)}]^{\mathrm{T}}$$
$$C_1=[C^1,\ \cdots,\ C^{(m-h_a)}]^{\mathrm{T}}$$
$$y_2=[y^{(m-h_a+1)},\ \cdots,\ y^m]^{\mathrm{T}}$$
$$C_2=[C^{(m-h_a+1)},\ \cdots,\ C^m]^{\mathrm{T}}$$

从而可得:

$$\begin{cases}\dot{\xi}(t)=A(\mu)\xi(t)+Bu_a(t)\\ y_1(t)=C_1\xi(t)\\ y_a(t)=C_2\xi(t)+f_s(t)\end{cases}\tag{6}$$

其中, $u_a(t)=u(t)+f_a(t)$, 是由执行器攻击改变的执行器输入; $y_a(t)$ 是由传感器攻击改变的传感器测量值; $f_a(t)\in\mathbf{R}$, $f_s(t)\in\mathbf{R}^{h_a}$ 分别为执行器攻击和传感器攻击. 假设矩阵 C_1 行满秩, 并且系统 (6) 满足 $\mathrm{rank}(C_1B)=\mathrm{rank}(B)$.

为了方便研究, 令 $f(t)=[f_a^{\mathrm{T}}(t)\ \ f_s^{\mathrm{T}}(t)]^{\mathrm{T}}$, 并引入如下攻击模型:

$$\dot{a}(t)=G(t,\ a(t),\ \delta_a(t))\tag{7}$$

$$f(t) = C_f a(t) + D_f \vartheta_f(t) \tag{8}$$

式中, $a(t) \in \mathbf{R}^{a_1}$, $G : \mathbf{R} \times \mathbf{R}^{a_1} \times \mathbf{R}^{a_2} \to \mathbf{R}^{a_1}$; $f(t) \in \mathbf{R}^{h_a+1}$; $C_f \in \mathbf{R}^{(h_a+1)\times a_1}$ 和 $D_f \in \mathbf{R}^{(h_a+1)\times a_3}$ 是未知矩阵; $\delta_a(t) \in \mathbf{R}^{a_2}$ 和 $\vartheta_f(t) \in \mathbf{R}^{a_3}$ 分别是系统 (7) 和 (8) 的输入, 且都是未知有界的; $a_1 \sim a_3$ 为向量相应的维度; 系统 (7) 关于 $(a(t),\ \delta_a(t))$ 局部 Lipschitz 且满足以下假设:

假设 1.

1) $\delta_a = 0$ 时, 系统 (7) 有一个未知但有界的平衡点 a^e;

2) 误差 $\bar{a} = a - a^e$ 的动态 $\dot{\bar{a}} = G(t,\ a,\ \delta_a) - G(t,\ a^e,\ 0)$ 是输入到状态稳定的.

随着信息化和网络化的不断发展, 机械臂系统与网络相结合后, 逐步成为信息物理融合系统. 在信息物理融合系统中, 虚假数据注入攻击作为一种常见的网络攻击, 其主要通过篡改利用网络传输的传感器测量和控制输入信号, 从而影响传输数据质量, 破坏观测器估计性能和控制器控制性能. 在实际应用中, 可以通过中间人攻击[27−28] 实现虚假数据注入攻击, 其通过伪装成受信任的实体, 拦截通信数据并篡改或窃取数据, 实现在网络中将错误数据注入到网络传输的传感器测量和控制输入信号, 使系统的安全运行受到威胁. 此外, 所考虑的攻击模型能够包含已报道的虚假数据注入攻击模型. 例如: 在 $G(t,\ a(t),\ \delta_a(t)) = A_a a(t)$ 且 A_a 为赫尔维兹时, 该模型可以退化为文献 [29] 中的攻击模型; 而当 $C_f = I$, $D_f = 0$ 时, 选择 $G(t,\ a(t),\ \delta_a(t))$ 为一个具有稳态输入 $\delta_a(t)$ 的低通滤波器, 则该模型可以退化为文献 [30] 中的攻击模型.

1.3 研究问题

在使用 T-S 模糊模型描述单连杆机械臂信息物理融合系统时, 模型前件变量 $v(t)$ 依赖于系统状态 $\xi_3(t)$. 1) 当 $\xi_3(t)$ 不可测时, 无法将其用于模糊控制器的设计; 2) 当 $\xi_3(t)$ 可测但受到传感器攻击而失真时, 基于其所设计的模糊控制器的控制效果会受到严重影响. 因此, 本文设计一种模糊观测器来构造新的、可靠的前件变量, 用于替代可能受攻击或不可测的前件变量. 另一方面, 该观测器拟利用攻击估计误差信息来重构攻击信号, 并将重构的攻击信号构造攻击补偿器, 以消除攻击对系统性能的影响.

2 基于模糊协同交互型观测器的安全控制

2.1 模糊协同交互型观测器的设计

首先, 引入一个辅助滤波器:

$$\dot{\xi}_l(t) = -A_l \xi_l(t) + A_l(y_a(t) + u_l(t)) \tag{9}$$

其中, $\xi_l \in \mathbf{R}^{h_a}$ 为滤波器状态; $A_l \in \mathbf{R}^{h_a \times h_a}$ 且 $A_l > \mathbf{0}$, 是一个滤波器矩阵; $u_l(t) \in \mathbf{R}^{h_a}$ 为滤波器输入. 引入的滤波器是为了处理潜在遭受的传感器攻击对信息物理融合系统性能的影响.

令 $\chi(t) = [\xi^{\mathrm{T}}(t)\ \ \xi_l^{\mathrm{T}}(t)]^{\mathrm{T}}$, 然后, 得到以下的增广系统:

$$\begin{cases} \dot{\chi}(t) = A_\chi(\mu)\chi(t) + B_\chi(U(t) + f(t)) \\ y_\chi(t) = C_\chi \chi(t) \end{cases} \tag{10}$$

式中,

$$A_\chi(\mu) = \begin{bmatrix} A(\mu) & \mathbf{0} \\ A_l C_2 & -A_l \end{bmatrix},\ C_\chi = \begin{bmatrix} C_1 & \mathbf{0} \\ \mathbf{0} & I \end{bmatrix}$$

$$B_\chi = \begin{bmatrix} B & \mathbf{0} \\ \mathbf{0} & A_l \end{bmatrix},\ U(t) = \begin{bmatrix} u(t) \\ u_l(t) \end{bmatrix}$$

引理 1. 如果存在适当的矩阵 $P = P^{\mathrm{T}} > 0$ 和 $M = [\mathcal{M}\ \ 0]$ 满足

$$\mathbf{He}(PA_{\chi,\,11}(\mu) + MA_{\chi,\,12}(\mu)) < 0 \tag{11}$$

式中 $\mathcal{M} \in \mathbf{R}^{(h_a+4-m)\times(m-h_a-1)}$, 则系统 (10) 可线性变换为:

$$\begin{cases} \dot{x}_1(t) = \bar{A}_{11}(\mu)x_1(t) + \bar{A}_{12}(\mu)x_2(t) \\ \dot{x}_2(t) = \bar{A}_{21}(\mu)x_1(t) + \bar{A}_{22}(\mu)x_2(t) + \\ \qquad \bar{B}_2(U(t) + f(t)) \\ y(t) = x_2(t) \end{cases} \tag{12}$$

式中 $\bar{A}_{11}(\mu)$ 使得 $\dot{\epsilon} = \bar{A}_{11}(\mu)\epsilon$ 稳定, 且 $x = [x_1^{\mathrm{T}}\ x_2^{\mathrm{T}}]^{\mathrm{T}} = T_\xi \chi$, $x_1(t) \in \mathbf{R}^{h_a+4-m}$, $x_2(t) \in \mathbf{R}^m$, 矩阵 $T_\xi \in \mathbf{R}^{(h_a+4)\times(h_a+4)}$, $\bar{A}_{11}(\mu) \in \mathbf{R}^{(h_a+4-m)\times(h_a+4-m)}$, $\bar{A}_{12}(\mu) \in \mathbf{R}^{(h_a+4-m)\times m}$, $\bar{A}_{21}(\mu) \in \mathbf{R}^{m\times(h_a+4-m)}$, $\bar{A}_{22}(\mu) \in \mathbf{R}^{m\times m}$, $\bar{B}_2 \in \mathbf{R}^{m\times(h_a+1)}$. 证明见附录 A.

进一步, 可以观测到, 模糊系统的前件变量 $v(t)$ 与连杆的角位移状态 ξ_3 相关, 于是, 可能存在三种情形: 1) 角位移状态 ξ_3 不可测量; 2) 角位移状态可测量但不遭受网络攻击信号影响; 3) 角位移状态可测量但受到网络攻击信号影响. 其中情形 3) 将导致传感器传输信号失真而使得测量得到的角位移状态不可信, 其可能导致基于该前件变量设计的观测器性能受到攻击信号的影响. 于是针对上述问题, 本文设计观测器时, 无论传感器是否可测或可信, 都利用估计的连杆角位移状态构造新的前件变量, 利用构造的新前件变量来作为模糊观测器的前件变量, 这样就能有效避免因传感器不可测或不可信而导致的前件变量失真, 进而对观测器的观

测性能造成影响. 因此, 提出一种具有协同交互结构的观测器, 其结构如下:

Plant Rule (i) :

IF $\hat{v}(t)$ **is** S_i

THEN $\dot{\hat{x}}_1 = \bar{A}_{i,\,11}\hat{x}_1 + \bar{A}_{i,\,12}\hat{x}_2$

$$\dot{\hat{x}}_2 = \bar{A}_{i,\,21}\hat{x}_1 + \bar{A}_{i,\,22}\hat{x}_2 + \bar{B}_2(U+\hat{f}) + (\bar{A}_{i,\,22} - A_i^d)(y-\hat{y})$$

$$y = \hat{x}_2 \tag{13}$$

$$\hat{f} = \eta P_{H_1} H_1 + \eta A_{H_2} H_2 \tag{14}$$

$$\dot{H}_1 = \eta A_{H_1} H_1 + \eta P_{H_2} H_2 \tag{15}$$

$$H_2 = F(y-\hat{y}) - F(y(0)-\hat{y}(0)) - \int_0^t F A_i^d (y(\tau)-\hat{y}(\tau))\mathrm{d}\tau + H_2(0) \tag{16}$$

式中, $i=1,\,2$; $i=1$ 时, $S_1 = S_{\max}$, $i=2$ 时, $S_2 = S_{\min}$. $\hat{v}(t) = \frac{\sin(\hat{\xi}_3(t))}{\hat{\xi}_3(t)}$ 是用观测器估计的系统状态构造的新的前件变量; $\hat{x}_1$, $\hat{x}_2$ 和 $\hat{y}$ 分别是观测器对 x_1, x_2 和 y 的估计; $H_1 \in \mathbf{R}^{h_a+1}$, $H_2 \in \mathbf{R}^{h_a+1}$, $F = (\bar{B}_2^{\mathrm{T}}\bar{B}_2)^{-1}\bar{B}_2^{\mathrm{T}}$, $\eta > 0$ 是一个常数, $H_2(0)$ 是 $H_2(t)$ 的初值, $A_i^d \in \mathbf{R}^{m\times m}$, $P_{H_1} \in \mathbf{R}^{(h_a+1)\times(h_a+1)}$, $A_{H_2} \in \mathbf{R}^{(h_a+1)\times(h_a+1)}$, $A_{H_1} \in \mathbf{R}^{(h_a+1)\times(h_a+1)}$, $P_{H_2} \in \mathbf{R}^{(h_a+1)\times(h_a+1)}$. 令 $e_1 = x_1 - \hat{x}_1$, $e_2 = x_2 - \hat{x}_2$, 则有:

$$\dot{e}_1 = \bar{A}_{11}(\hat{\mu})e_1 + \Omega_{e_1} \tag{17}$$

$$\dot{e}_2 = \bar{A}_{21}(\hat{\mu})e_1 + A^d(\hat{\mu})e_2 + \bar{B}_2(f-\hat{f}) + \Omega_{e_2} \tag{18}$$

式中, $\Omega_{e_1} = (\bar{A}_{11}(\mu) - \bar{A}_{11}(\hat{\mu}))x_1 + \bar{A}_{12}(\hat{\mu})e_2$, $\Omega_{e_2} = (\bar{A}_{21}(\mu) - \bar{A}_{21}(\hat{\mu}))x_1 + \bar{A}_{22}(\hat{\mu})e_2$.

引理 2. 考虑系统 (18), 于是下列等式是等价的:

1) $\dot{H}_2 = F\bar{A}_{21}(\hat{\mu})e_1 + f - \hat{f} + F\Omega_{e_2}$;

2) $H_2 = F(y-\hat{y}) - F(y(0)-\hat{y}(0)) - \int_0^t FA^d \times (\hat{\mu})(y(\tau)-\hat{y}(\tau))\mathrm{d}\tau + H_2(0)$. 证明见附录 B.

定理 1. 考虑模糊系统 (12), 模糊观测器 (13) ~ (16) 以及满足假设 1 的攻击信号 (7) ~ (8), 当给定任意的正标量 σ_{e_1}, σ_{e_2}, γ_1, γ_6 和足够大的 η, 如果存在合适维数的矩阵 $P_{e_1} = P_{e_1}^{\mathrm{T}} > \mathbf{0}$, $P_{e_2} = P_{e_2}^{\mathrm{T}} > \mathbf{0}$, M, $M_{e_2,\,i}$, N_{H_1}, N_{H_2} 和正标量 γ_2, γ_3, γ_4, γ_5, γ_{e_1}, γ_{H_1} 和 γ_{H_2} 满足下列线性矩阵不等式:

$$\begin{bmatrix} N_{H_1} + N_{H_1}^{\mathrm{T}} + (3\gamma_4 + \gamma_{H_1})I & * \\ N_{H_1}^{\mathrm{T}} & -\gamma_5 I \end{bmatrix} < \mathbf{0} \tag{19}$$

$$\begin{bmatrix} -N_{H_2} - N_{H_2}^{\mathrm{T}} + (2\gamma_2 + 2\gamma_3 + \gamma_{H_2})I & * \\ N_{H_2} & -\gamma_1 I \end{bmatrix} < \mathbf{0} \tag{20}$$

$$\begin{bmatrix} \Theta_1 & * & * & * \\ P_{e_2}\bar{A}_{21,\,i} & \mathbf{He}(M_{e_2,\,i}) + \gamma_{e_2} I & * & * \\ P_{e_1} & \mathbf{0} & -\sigma_{e_1}^2 I & * \\ \mathbf{0} & \bar{B}_2^{\mathrm{T}} P_{e_2}^{\mathrm{T}} & \mathbf{0} & -\sigma_{e_2}^2 I \\ F\bar{A}_{21,\,i} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \bar{B}_2^{\mathrm{T}} P_{e_2}^{\mathrm{T}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \bar{B}_2^{\mathrm{T}} P_{e_2}^{\mathrm{T}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \bar{B}_2^{\mathrm{T}} P_{e_2}^{\mathrm{T}} & \mathbf{0} & \mathbf{0} \end{bmatrix}$$

$$\begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ -\gamma_2 I & * & * & * \\ \mathbf{0} & -(1/3)\gamma_4 I & * & * \\ \mathbf{0} & \mathbf{0} & -\gamma_6 I & * \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & -(1/\gamma_1)I \end{bmatrix} < \mathbf{0} \tag{21}$$

式中, $\Theta_1 = \mathbf{He}(P_{e_1}A_{11,\,i} + MA_{12,\,i}) + \gamma_{e_1} I$. 那么, 当 $\Omega = [\Omega_{e_1}; \Omega_{e_2}] = \mathbf{0}$ 时, 观测器的估计误差收敛到零附近的紧集, 且对于足够大的 η, $lim_{t\to\infty} f(t) = lim_{t\to\infty}\hat{f}(t)$; 而当 $\Omega \neq \mathbf{0}$ 时, 观测器的估计误差系统 (17) 和 (18) 对 Ω 有 σ 水平的抑制性能, 其中 $\sigma = \frac{\lambda_{\max}(\sigma_e)}{\lambda_{\min}(\gamma_e)}$, $\gamma_e = \mathrm{diag}\{\gamma_{e_1},\,\gamma_{e_2}\}$, $\sigma_e^2 = \mathrm{diag}\{\sigma_{e_1}^2,\,\sigma_{e_2}^2\}$. 观测器参数 $L = P_{e_1}^{-1}M_{e_1}$, $A_i^d = P_{e_2}^{-1}M_{e_2,\,i}$, $A_{H_1} = N_{H_1}P_{H_1}$, $A_{H_2} = N_{H_2}P_{H_2}$, 其中 $P_{H_1} = P_{H_1}^{\mathrm{T}} > \mathbf{0}$, $P_{H_2} = P_{H_2}^{\mathrm{T}} > \mathbf{0}$ 是任意给定的. 证明请见附录 C.

由引理 2 可知, 辅助系统 (15) 和 (16) 含有攻击估计误差信息. 它们通过观测器的协同交互结构 (14) 将攻击估计误差信息传递给观测器, 然后观测器将更新后的信息传递给辅助系统. 通过观测器与辅助系统的协同交互, 提高了攻击估计误差信息的利用率, 从而提高了攻击信号的重构精度. 另一方面, 观测器所运用的前件变量为估计的 $\hat{v}(t)$, 这就能够有效避免因数据不可测以及可测但受传感器攻击导致数据失真的情形, 使得所设计的观测器不会因前件变量失真导致性能降低.

2.2　基于模糊观测器的安全控制方案设计

基于模糊观测器重构的攻击信号 $\hat{f}$, 设计一类控制器以消除攻击影响, 使单连杆机械臂信息物理融合系统能够安全稳定的运行. 选择控制器 $U = U_1 + U_2$, 其中 U_1 是模糊系统 (10) 在不受攻击时保证期望性能稳定的控制器, 例如: 动态输出反馈控制器, H_∞ 模糊控制器和基于观测器状态估计的模糊控制器等. 该控制器的设计方法已比较成熟, 具体可参见文献 [21−24], 本文不再赘述. 但控制器设

计中前件变量的选择与系统相同时, 前件变量不可测或可测但受传感器攻击都会影响控制器性能, 因此, 基于模糊观测器构造新的、可利用且可靠的前件变量用以控制器的设计. 另一方面, 设计 $U_2 = -\hat{f}$, 利用观测器重构的攻击信号 $\hat{f}$ 构建攻击补偿器, 该攻击补偿器装备到现有的能够保证标称系统稳定的模糊控制器上就能有效消除攻击信号的影响, 保证系统具有期望的性能. 方案的有效性将在下一节中被验证.

3 MATLAB 数值仿真与硬件在环实验验证

3.1 MATLAB 数值仿真验证

选择单连杆机械臂信息物理融合系统的参数 $J_m = 0.003\,7\ \mathrm{kg\cdot m^2}$, $J_l = 0.009\,2\ \mathrm{kg\cdot m^2}$, $K_\tau = 0.08\ \mathrm{N\cdot m/V}$, $k = 0.18\ \mathrm{N\cdot m/rad}$, $m = 0.021\ \mathrm{kg}$, $g = 9.81\ \mathrm{m/s^2}$, $b = 0.15\ \mathrm{m}$, $\delta_a = 0.004\,6\ \mathrm{N\cdot m/V}$. 则通过 T-S 模糊模型描述后, 系统参数可以得到:

$$A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -48.6 & -1.24 & 48.6 & 0 \\ 0 & 0 & 0 & 1 \\ 19.5 & 0 & -22.85 & 0 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -48.6 & -1.24 & 48.6 & 0 \\ 0 & 0 & 0 & 1 \\ 19.5 & 0 & -18.78 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 21.6 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$$

前件变量 $v(t) \in [v_{\min},\ v_{\max}]$, 其中, $v_{\min} = -0.217\,2$ 和 $v_{\max} = 1$. 辅助滤波器 (9) 增益选择 $A_l = 1$. 下面考虑前件变量可测 (含不受攻击和受攻击情况) 和前件变量不可测两种情形进行 MATLAB 数值仿真验证.

3.1.1 前件变量可测的情形

传感器参数如下:

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},\ C_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}$$

显然, 与前件变量相关的系统状态 ξ_3 是可测的. 利用 LMI 工具箱求解 (11), (19) ~ (21) 可以得到观测器的参数: $L = [1.371\,3,\ 0]$

$$A_1^d = \begin{bmatrix} -42.150\,5 & 0 & 14.447\,4 & 1.116\,8 \\ 0 & -1 & 0 & 0 \\ 15.074\,3 & 0 & -1\,394.94 & -0.343\,3 \\ 1.179\,3 & 0 & -0.708\,2 & -28.897\,1 \end{bmatrix}$$

$$A_2^d = \begin{bmatrix} -42.242\,0 & 0 & 14.519\,3 & 1.331\,4 \\ 0 & -1 & 0 & 0 \\ 15.772\,7 & 0 & -1\,395.21 & -0.807\,1 \\ 1.124\,9 & 0 & -0.711\,2 & -28.906\,2 \end{bmatrix}$$

$P_{H_1} = I$, $A_{H_2} = \mathrm{diag}\{2.918\,2,\ \ 2.918\,2\}$, $A_{H_1} = \mathrm{diag}\{-43.361\,3,\ -43.361\,3\}$, $P_{H_2} = I$. 选择 $H_2(0) = \mathbf{0}$, $\eta = 200$. 另一方面, 考虑如下攻击信号:

1) $t \in [0,\ 10)$ s 时, 没有发生攻击, 即 $\dot{a}(t) = f(t) = \mathbf{0}$;

2) $t \in [10,\ 20)$ s 时, 发生低频攻击: $\dot{a}(t) = \mathbf{0}$, $f(t) = [5 + \sin(0.8t),\ -3 + \cos(0.8t)]^{\mathrm{T}}$;

3) $t \in [20,\ 40)$ s 时, 发生高频攻击: $\dot{a}(t) = -a(t) - [\sin(t),\ -\cos(t)]^{\mathrm{T}}$, $f(t) = 5a(t) + [-5\sin(80t) \times \cos(0.5t),\ -5\cos(50t)\sin(0.5t)]^{\mathrm{T}}$.

由上述攻击信号可知, $t \in [0,\ 10)$ s 时, 系统并未受到攻击, 其前件变量是可信的; 而在 $t \in [10,\ 40)$ s 时, 系统受到攻击, 其前件变量可能因受到攻击而失真. 为了避免攻击对系统的前件变量的影响, 本文利用协同交互观测器 (Cooperative interaction observer, CIO) 构造新的、可靠的前件变量, 以消除因前件变量失真导致的观测器与控制器的性能下降.

为了验证所提方法的有效性, 考虑文献 [25] 中基于比例积分观测器 (Proportional integral observer, PIO) 的方法和文献 [31] 中基于状态估计观测器 (State/fault estimation observer, SFEO) 的方法与所提出的 CIO 方法进行对比. 仿真结果如图 2 所示, 从图中可以看出, 对于频率较低的攻击信号, 三者均可较为准确地重构攻击信号, 而对于高频攻击信号, 本文所提方法能够更加及时准确地重构攻击信号. 这是因为所提方法利用协同交互结构提高了攻击估计误差信息的利用率, 提高了攻击估计的精度. 进一步, 给出基于上述观测器的安全控制方法下的控制性能, 仿真结果如图 3 所示, 可以看到所提方法的控制效果更好, 这是因为攻击补偿器使用了更加准确的攻击估计信号, 从而有效地消除攻击的影响, 提高控制性能.

3.1.2 前件变量不可测的情形

传感器参数如下:

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},\ C_2 = \begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix}$$

由上可以看出, 与前件变量相关的系统状态 ξ_3 是不可测的. 利用 LMI 工具箱求解 (11), (19) ~ (21) 可以得到观测器的参数: $L = [1.329\,4,\ 0]$

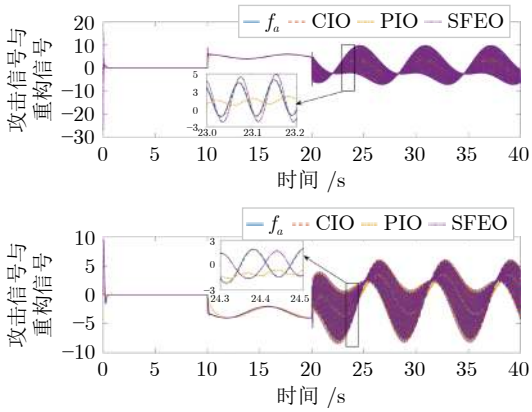

图 2　在第 3.1.1 节中考虑的攻击信号与分别基于所提出的 CIO, 文献 [25] 中的 PIO 和文献 [31] 中的 SFEO 的重构信号的对比

Fig. 2　Comparison of the attack signals considered in section 3.1.1 with the reconstruction signals based on the proposed CIO, the PIO in reference [25] and the SFEO in reference [31], respectively

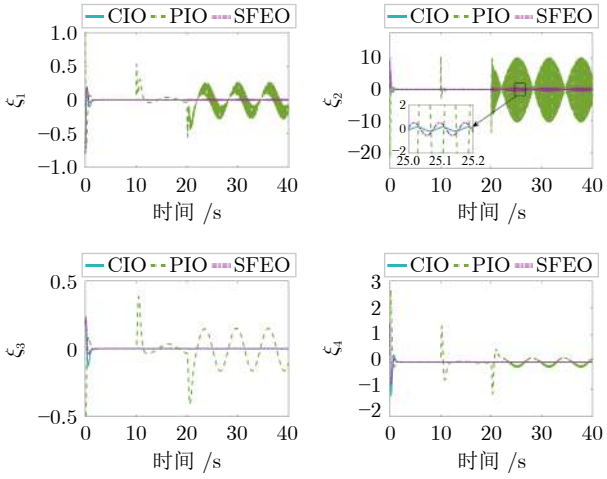

图 3　系统受到第 3.1.1 节中考虑的攻击时, 在分别基于提出的 CIO, 文献 [25] 的 PIO 与文献 [31] 的 SFEO 的安全控制器 U 下的系统状态响应曲线

Fig. 3　System state response curves under the security controller U based on the proposed CIO, the PIO in reference [25] and the SFEO in reference [31], respectively, when the system is attacked by the one considered in section 3.1.1

$$A_1^d=\begin{bmatrix}-41.220\,8 & 0 & 6.831\,1 & 0\\ 0 & -1 & 0 & 0\\ 6.622\,9 & 0 & -658.832\,9 & 0\\ 0 & 0 & 0 & -27.865\,4\end{bmatrix}$$

$$A_2^d=\begin{bmatrix}-41.195\,9 & 0 & 7.087\,8 & 0\\ 0 & -1 & 0 & 0\\ 6.741\,7 & 0 & -659.292\,8 & 0\\ 0 & 0 & 0 & -27.865\,4\end{bmatrix}$$

$P_{H_1}=I$, $A_{H_2}=\mathrm{diag}\{2.811\,5,\ 2.811\,5\}$, $A_{H_1}=\mathrm{diag}\{-39.788\,1,\ -39.788\,1\}$, $P_{H_2}=I$. 选择 $H_2(0)=\mathbf{0}$ 和 $\eta=200$. 考虑如下攻击信号:

1) $t\in[0,\ 10)$ s 时, 没有发生攻击, 即 $\dot{a}(t)=f(t)=\mathbf{0}$;

2) $t\in[10,\ 20)$ s 时, $\dot{a}(t)=\mathbf{0}$, $f(t)=[5+\sin(0.8t),\ -3+\cos(0.8t)]^{\mathrm{T}}$;

3) $t\in[20,\ 40)$ s 时, $\dot{a}(t)=-a(t)-[\sin(t),\ -\cos(t)]^{\mathrm{T}}$, $f(t)=5a(t)+[-5\cos(8t)\cos(0.5t),\ -5\times\sin(5t)\sin(0.5t)]^{\mathrm{T}}$.

由于文献 [25] 与 [31] 的观测器均依赖可测的前件变量, 因此其对于前件变量不可测的情况无法进行对比, 所以只呈现本方法的仿真效果. 仿真结果如图 4 和图 5 所示, 从图中可以看出, 本文所提方法能及时准确地重构攻击信号, 且基于所提观测器的控制器能够有效消除攻击对系统性能的影响.

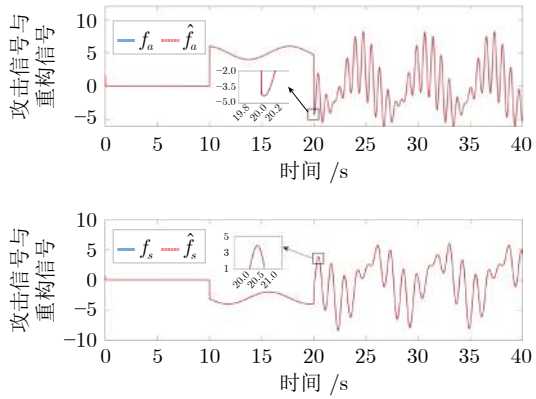

图 4　在第 3.1.2 节中考虑的攻击信号与所提出观测器的重构信号的对比

Fig. 4　Comparison of the attack signals considered in section 3.1.2 with the reconstruction signals of the proposed observer

3.2　硬件在环仿真实验验证

本节搭建了如图 6 所示的硬件在环仿真实验平台, 以验证所设计方案的有效性, 其中, StarSim 实时软件模块模拟机械臂系统; 快速反应控制器执行所提控制算法; 输入/输出接口用于控制器与被控对象之间的信号传递; 系统状态检测器用于监测系统运行状态; 攻击估计信号显示器用于显示观测器重构的攻击信号. 下面将从前件变量可测和不可测两种情形, 验证所提方案的有效性.

3.2.1　前件变量可测的情形

考虑文献 [25], [31] 和本文所提方法, 并进行硬件在环对比仿真实验来验证所提方法的有效性, 其中, 相关观测器和控制器参数与第 3.1.1 节的参数相同. 考虑如下攻击信号:

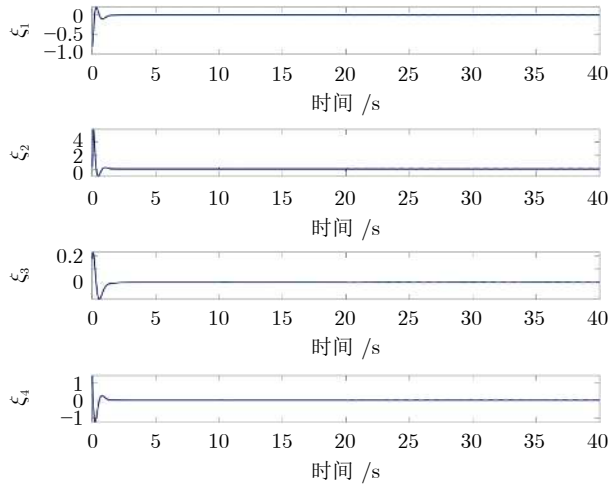

图 5 系统受到第 3.1.2 节考虑的攻击时, 在基于所提出观测器的安全控制器 U 下的系统状态响应曲线

Fig. 5 System state response curves under the security controller U based on the proposed observer when the system is attacked by the one considered in section 3.1.2

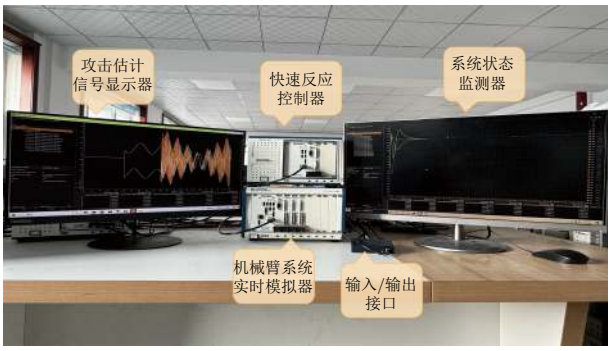

图 6 硬件在环实验平台

Fig. 6 The hardware-in-the-loop experimental platform

1) $t \in [0,\ 10)$ s 时, 没有发生攻击, 即 $\dot{a}(t) = f(t) = \mathbf{0}$;

2) $t \in [10,\ 20)$ s 时, 发生低频攻击: $\dot{a}(t) = \mathbf{0}$, $f(t) = [2 + \sin(t),\ -3 + \cos(t)]^{\mathrm{T}}$;

3) $t \in [20,\ 40)$ s 时, 发生高频攻击: $\dot{a}(t) = -5 \times a(t) - [\sin(2t),\ -\cos(2t)]^{\mathrm{T}}$, $f(t) = 8a(t) + [-5\cos(30t) \times \sin(-0.1t),\ -3\sin(-0.1t)\cos(20t)]^{\mathrm{T}}$.

基于硬件在环实验平台的实验结果如图 7、图 8 所示, 可以看出所设计的方案相较于其他两种能够更有效地重构攻击信号, 同时, 基于所提观测器的安全控制器也实现了更好的控制性能.

3.2.2 前件变量不可测的情形

同样地, 对于前件变量不可测的情况, 选择与第 3.1.2 节相同的参数并基于该硬件在环实验平台来验证方法的有效性, 考虑如下攻击信号:

1) $t \in [0,\ 10)$ s 时, 没有发生攻击, 即 $\dot{a}(t) = f(t) = \mathbf{0}$;

2) $t \in [10,\ 20)$ s 时, $\dot{a}(t) = \mathbf{0}$, $f(t) = [4,\ -2]^{\mathrm{T}}$;

3) $t \in [20,\ 40)$ s 时, $\dot{a}(t) = \mathbf{0}$, $f(t) = 2[\sin(5t) + 3,\ -\cos(5t) - 2]^{\mathrm{T}}$;

4) $t \in [40,\ 60)$ s 时, $\dot{a}(t) = -a(t) - [\sin(2t),\ -\cos(2t)]^{\mathrm{T}}$, $f(t) = 5a(t) + [-0.5\cos(0.3t)\sin(-3t)\mathrm{e}^{0.05t},$

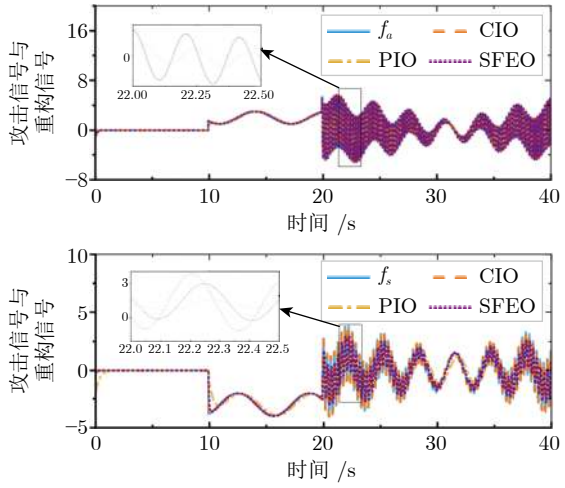

图 7 在第 3.2.1 节中考虑的攻击信号与分别基于所提出的 CIO, 文献 [25] 中的 PIO 和文献 [31] 中的 SFEO 的重构信号的对比

Fig. 7 Comparison of the attack signals considered in section 3.2.1 with the reconstruction signals based on the proposed CIO, the PIO in reference [25] and the SFEO in reference [31], respectively

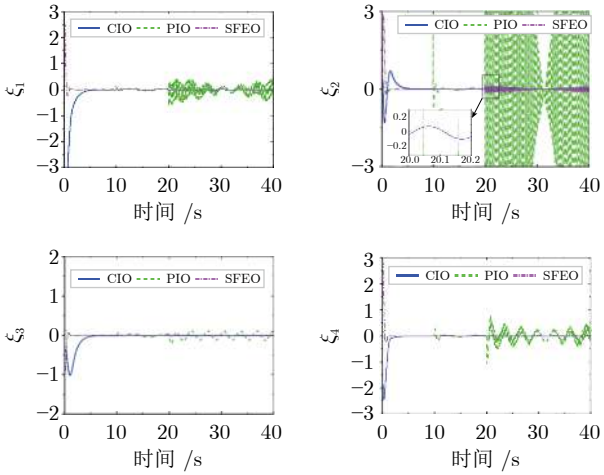

图 8 系统受到第 3.2.1 节中考虑的攻击时, 在分别基于提出的 CIO, 文献 [25] 的 PIO 与文献 [31] 的 SFEO 的安全控制器 U 下的系统状态响应曲线

Fig. 8 System state response curves under the security controller U based on the proposed CIO, the PIO in reference [25] and the SFEO in reference [31], respectively, when the system is attacked by the one considered in section 3.2.1

$-0.5\sin(0.5t)\cos(5t)\mathrm{e}^{0.05t}]^{\mathrm{T}}$.

实验结果如图 9 和图 10 所示, 可以看出所设计的方案针对前件变量不可测的情况, 也能够有效完成攻击信号重构与安全控制.

综上所述, 本文所提出的协同交互型观测器能够准确重构单连杆机械臂信息物理融合系统所受到的网络攻击信号, 且基于该观测器所设计的控制器能够有效消除网络攻击对系统的影响, 保障单连杆机械臂信息物理融合系统的稳定运行.

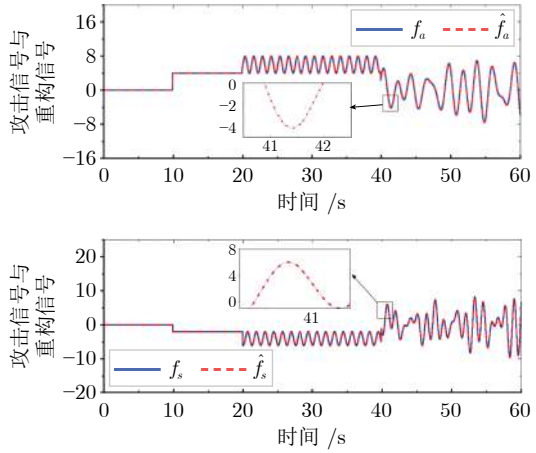

图 9　在第 3.2.2 节中考虑的攻击信号与所提出观测器的重构信号的对比

Fig. 9　Comparison of the attack signals considered in section 3.2.2 with the reconstruction signals of the proposed observer

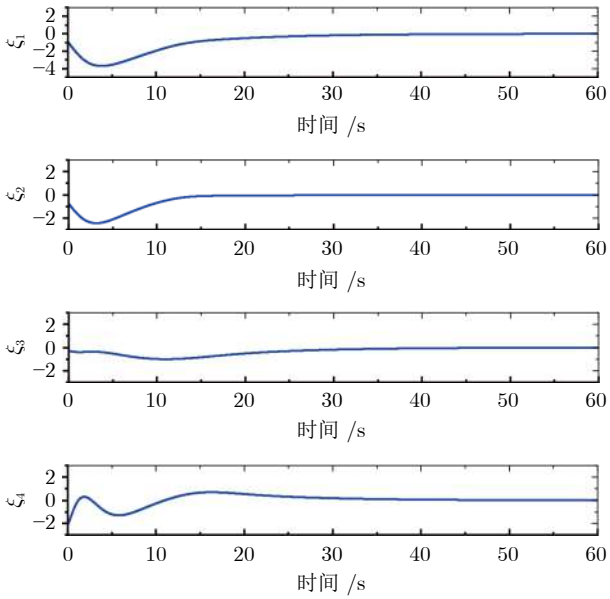

图 10　系统受到第 3.2.2 节考虑的攻击时, 在基于所提出观测器的安全控制器 U 下的系统状态响应曲线

Fig. 10　System state response curves under the security controller U based on the proposed observer when the system is attacked by the one considered in section 3.2.2

4　结论

本文利用 T-S 模糊模型对单连杆机械臂进行描述, 并研究了单连杆机械臂信息物理融合系统的传感器测量和执行器输入受到网络攻击时的安全控制问题. 对于前件变量不可测量或可测量但受传感器攻击影响, 提出了一种模糊协同交互观测器来构建新的、可靠的、可用的前件变量. 进一步, 给出了包含攻击估计误差信息的辅助系统, 这些辅助系统与观测器估计误差进行协同交互, 充分利用攻击估计误差信息, 提高攻击信号的重构精度. 在此基础上, 提出包含攻击补偿器的控制器, 以消除网络攻击的影响, 保证单连杆机械臂信息物理融合系统的稳定性.

附录 A　引理 1 的证明

对 C_χ 进行奇异值分解, 可以得到 $C_\chi = S_{C_\chi} \times V_{C_\chi} D_{C_\chi}$, 其中 S_{C_χ} 和 D_{C_χ} 都是酉矩阵, $V_{C_\chi} = [X_{C_\chi}\ 0]$, X_{C_χ} 是一个对角矩阵. 存在 $T_C^{-1} = D_{C_\chi}^{\mathrm{T}}\ E\bar{S}_{C_\chi}^{\mathrm{T}}$ 使得 $C_\chi T_C^{-1} = [\mathbf{0}\quad I]$, 其中 $E = [0\ 1;\ 1\ 0]$; $\bar{S}_{C_\chi}^{\mathrm{T}} = \begin{bmatrix} I & \mathbf{0} \\ \mathbf{0} & X_{C_\chi}^{-1} S_{C_\chi}^{\mathrm{T}} \end{bmatrix}$. 而且 $T_{C_\xi} B_\chi = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$, 由相关假设可得 $\mathrm{rank}(C_\chi B_\chi) = \mathrm{rank}(B_\chi) = l + h_a$. 且 $C_\chi B_\chi = B_2$, 因此 B_2 是列满秩的. 根据奇异值分解, 可以得到 $T_{B_2} = E S_{B_2}^{\mathrm{T}}$ 且

$$T_{B_2} B_2 = \mathcal{B}_2 = \begin{bmatrix} \mathbf{0} \\ \bar{B}_2 \end{bmatrix} \tag{A1}$$

式中 $B_2 = S_{B_2} V_{B_2}$, 其中, $V_{B_2} = [\bar{B}_2;\ 0]$, S_{B_2} 是酉矩阵, 且 $\bar{B}_2$ 是列满秩的. 之后有

$$T_B = \begin{bmatrix} I & -B_1 B_2^{\dagger} \\ \mathbf{0} & T_{B_2} \end{bmatrix} \tag{A2}$$

令 $T_{BC} = T_B T_C$, 系统 (10) 可以转变为:

$$T_{BC} A_\chi(\mu) T_{BC}^{-1} = \begin{bmatrix} A_{11}(\mu) & A_{12}(\mu) \\ A_{21}(\mu) & A_{22}(\mu) \end{bmatrix} \tag{A3}$$

$$T_{BC} B_\chi = \begin{bmatrix} \mathbf{0} \\ \mathcal{B}_2 \end{bmatrix},\ C_\chi T_{BC}^{-1} = [\mathbf{0}\quad T_{B_2}^{-1}] \tag{A4}$$

基于上述变换, 可以得到 $T_{ABC} = \begin{bmatrix} I & \bar{L} \\ \mathbf{0} & T_{B_2}^{-1} \end{bmatrix}$ 且 $\bar{L} = [L\quad \mathbf{0}]$, $L \in \mathbf{R}^{(h_a+4-m)\times(m-h_a-1)}$. 之后通过变换矩阵 $T = T_{ABC} T_{BC}$, 系统 (10) 转变为 (12), 其中 $\bar{A}_{11}(\mu) = A_{11}(\mu) + \bar{L} A_{12}(\mu)$, 并且

$$\begin{cases} \bar{A}(\mu) = T A_\chi(\mu) T^{-1} = \begin{bmatrix} \bar{A}_{11}(\mu) & \bar{A}_{12}(\mu) \\ \bar{A}_{21}(\mu) & \bar{A}_{22}(\mu) \end{bmatrix} \\ \bar{B} = T B_\chi = \begin{bmatrix} \mathbf{0}_{(h_a+4-m)\times(h_a+1)} \\ \bar{B}_2 \end{bmatrix} \\ \bar{C} = B_\chi T^{-1} = [\mathbf{0}_{m\times(h_a+4-m)}\quad I_m] \end{cases} \tag{A5}$$

另一方面, 我们考虑李雅普诺夫函数 $\mathcal{V}=\epsilon^{\mathrm{T}}P\epsilon$. 则 $\dot{\mathcal{V}}=2\epsilon^{\mathrm{T}}(PA_{11}(\mu)+P\bar{L}A_{12}(\mu))$. 令 $\mathcal{M}=PL$, 由式 (11) 可得 $\dot{\mathcal{V}}<0$. 因此, 我们得到了想要的坐标变换 T. □

附录 B 引理 2 的证明

根据式 (18), 可以得到:

$$F\dot{e}_2-FA^d(\hat{\mu})e_2=F\bar{A}_{21}(\hat{\mu})e_1+f-\hat{f}+F\Omega_{e_2} \tag{B1}$$

于是, 引理 2 中的 1) 可以写为:

$$\dot{H}_2=F\dot{e}_2-FA^d(\hat{\mu})e_2 \tag{B2}$$

对上式从 0 到 t 进行积分得到

$$H_2=F(y-\hat{y})-F(y(0)-\hat{y}(0))-\int_0^t FA^d(\hat{\mu})(y(\tau)-\hat{y}(\tau))\mathrm{d}\tau+H_2(0) \tag{B3}$$

另一方面, 对 H_2 进行求导可得:

$$\dot{H}_2=F(\dot{y}-\dot{\hat{y}})-FA^d(\hat{\mu})(y-\hat{y})=F(\dot{e}_2-A^d(\hat{\mu})e_2)=F\bar{A}_{21}(\hat{\mu})e_1+f-\hat{f}+F\Omega_{e_2} \tag{B4}$$

□

附录 C 定理 1 的证明

根据文献 [32] 中的定义 4.7 和 4.16 以及文献中的相关假设可知 $\bar{a}(t)$ 满足 $\|\bar{a}(t)\|\leq\beta(\|\bar{a}(0)\|,\,t)+\varepsilon(\sup_{0\leq\tau\leq t}\|\varrho_a(\tau)\|)$, $\tau\in[0,\,t)$, 且 $\|\varrho_a(\tau)\|\equiv0$ 时, 可以得到 $\|\bar{a}(t)\|\leq\beta(\|\bar{a}(0)\|,t)$, 其中 $\varepsilon(\cdot)$ 属于 K 类函数, $\beta(\cdot,\cdot)$ 属于 KL 类函数. 李雅普诺夫函数 $V_a(t,\,\bar{a})$ 满足

$$\begin{cases}\rho_1(\|\bar{a}\|)\leq V_a(t,\,\bar{a})\leq\rho_2(\|\bar{a}\|)\\ \dfrac{\partial V_a(t,\,\bar{a})}{\partial t}+\dfrac{\partial V_a(t,\,\bar{a})}{\partial\bar{a}}(G(t,\,a,\,0)-G(t,\,a^e,\,0))\leq\\ \qquad-\rho_3(\|\bar{a}\|)\\ \left\|\dfrac{\partial V_a(t,\,\bar{a})}{\partial\bar{a}}\right\|\leq\rho_4(\|\bar{a}\|)\end{cases}$$

式中 ρ_1, ρ_2, ρ_3 和 ρ_4 都是 K 类函数. 另外, 由于 $G(t,\,a,\,\delta_a)$ 在 $(a,\,\delta_a)$ 中是局部 Lipschitz, 因此可以得到:

$$\begin{cases}\|G(t,\,a,\,0)-G(t,\,a^e,\,0)\|\leq\rho_5\|\bar{a}\|\\ \|G(t,\,a,\,\delta_a)-G(t,\,a,\,0)\|\leq\rho_6\|\delta_a\|\end{cases} \tag{C1}$$

式中 ρ_5 和 ρ_6 是大于零的常数. 进一步, 可以得到 $\dot{V}_a=\frac{\partial V_a}{\partial t}+\frac{\partial V_a}{\partial\bar{a}}\dot{\bar{a}}\leq-\rho_3(\|\bar{a}\|)+\rho_6\rho_4(\|\bar{a}\|)\|\delta_a\|$.

基于引理 2、式 (17) 和式 (18), 考虑李雅普诺夫函数 $V=\sum_{i=1}^6V_i$, 其中 $V_1=e_1^{\mathrm{T}}P_{e_1}e_1$, $V_2=e_2^{\mathrm{T}}P_{e_2}e_2$, $V_3=V_a$, $V_4=\eta H_2^{\mathrm{T}}P_{H_2}H_2$, $V_5=\eta H_1^{\mathrm{T}}P_{H_1}H_1$, $V_6=-2H_1^{\mathrm{T}}C_f\bar{a}$.

由于 $2H_1^{\mathrm{T}}C_f\bar{a}\leq\frac{1}{\gamma_1}\|C_f\|^2\|H_1\|^2+\gamma_1\|\bar{a}\|^2$, $-2H_1^{\mathrm{T}}C_f\bar{a}\leq\frac{1}{\gamma_2}\|C_f\|^2\|H_1\|^2+\gamma_2\|\bar{a}\|^2$, 容易推断出: 对于足够大的 η, 可以保证 $\eta\lambda_{\min}(P_{H_1})-\frac{1}{\gamma_1}\|C_f\|^2>0$, 且 $\rho_1(\|\bar{a}\|)-\gamma_1\|\bar{a}\|^2$ 属于 K 类函数. 于是 $\kappa_1(\|e_1\|,\,\|e_2\|,\,\|a\|,\,\|H_1\|,\,\|H_2\|)\leq V\leq\kappa_2(\|e_1\|,\,\|e_2\|,\,\|a\|,\,\|H_1\|,\,\|H_2\|)$, 其中 $\kappa_1(\cdot)$ 和 $\kappa_2(\cdot)$ 是 K 类函数. 这意味着对于任意的 $[\|e_1\|\;\|e_2\|\;\|a\|\;\|H_1\|\;\|H_2\|]\neq\mathbf{0}$, V 是有界的.

之后

$$\begin{cases}\dot{V}_1=2e_1^{\mathrm{T}}P_{e_1}(\bar{A}_{11}(\hat{\mu})e_1+\Omega_{e_1})\\ \dot{V}_2=2e_2^{\mathrm{T}}P_{e_2}(\bar{A}_{21}(\hat{\mu})e_1+A^d_{\xi,\,2}(\hat{\mu})e_2+\\ \qquad\bar{B}_{\xi,\,2}(f-\eta A_{H_2}H_2-\eta P_{H_1}H_1)+\Omega_{e_2})\\ \dot{V}_3\leq\;-\rho_3(\|\bar{a}\|)+\rho_6\rho_4(\|\bar{a}\|)\|\delta_a\|\\ \dot{V}_4=2\eta H_2^{\mathrm{T}}P_{H_2}(F\bar{A}_{\xi,\,21}(\hat{\mu})e_1+f\times\\ \qquad\eta A_{H_2}H_2-\eta P_{H_1}H_1+F\Omega_{e_2})\\ \dot{V}_5=2\eta H_1^{\mathrm{T}}P_{H_1}(\eta A_{H_1}H_1+\eta P_{H_2}H_2)\\ \dot{V}_6=\;-2\eta H_1^{\mathrm{T}}A_{H_1}^{\mathrm{T}}C_f\bar{a}-2\eta H_2^{\mathrm{T}}P_{H_2}C_f\bar{a}\times\\ \qquad2H_1^{\mathrm{T}}C_f(G(t,\,a,\,\delta_a)-G(t,\,a^e,\,0))\end{cases} \tag{C2}$$

由杨氏不等式可得:

$$-2\eta e_2^{\mathrm{T}}P_{e_2}\bar{B}_{\xi,\,2}A_{H_2}H_2\leq\frac{1}{\gamma_1}\eta^2H_2^{\mathrm{T}}A_{H_2}^{\mathrm{T}}A_{H_2}H_2+\gamma_1e_2^{\mathrm{T}}P_{e_2}\bar{B}_{\xi,\,2}\bar{B}_{\xi,\,2}^{\mathrm{T}}P_{e_2}e_2$$

$$2\eta H_2^{\mathrm{T}}P_{H_2}G\bar{A}_{\xi,\,21}(\hat{\mu})e_1\leq\gamma_2\eta^2H_2^{\mathrm{T}}P_{H_2}P_{H_2}H_2+\frac{1}{\gamma_2}e_1^{\mathrm{T}}\bar{A}_{\xi,\,21}^{\mathrm{T}}(\hat{\mu})G^{\mathrm{T}}G\bar{A}_{\xi,\,21}(\hat{\mu})e_1$$

$$2\eta H_2^{\mathrm{T}}P_{H_2}(C_fa^e+D_f\varrho_a)\leq2\gamma_3\eta^2H_2^{\mathrm{T}}P_{H_2}P_{H_2}H_2+\frac{1}{\gamma_3}(\|C_f\|^2\|a^e\|^2+\|D_f\|^2\|\varrho_a\|^2)$$

$$2\eta H_2^{\mathrm{T}}P_{H_2}F\Omega_{e_2}\leq\gamma_2\eta^2H_2^{\mathrm{T}}P_{H_2}P_{H_2}H_2+\frac{1}{\gamma_2}\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}-$$

$$2\eta e_2^{\mathrm{T}}P_{e_2}\bar{B}_{\xi,\,2}P_{H_1}H_1\leq\gamma_4\eta^2H_1^{\mathrm{T}}P_{H_1}P_{H_1}H_1+\frac{1}{\gamma_4}e_2^{\mathrm{T}}P_{e_2}\bar{B}_{\xi,\,2}\bar{B}_{\xi,\,2}^{\mathrm{T}}P_{e_2}e_2$$

$$-2\eta H_1^{\mathrm{T}}A_{H_1}C_f\bar{a}\leq\frac{1}{\gamma_5}\eta^2H_1^{\mathrm{T}}A_{H_1}A_{H_1}^{\mathrm{T}}H_1+\gamma_5\|C_f\|^2\|\bar{a}\|^2$$

$$-H_1^{\mathrm{T}}C_f(G(t,\,a,\,\varrho_a)-G(t,\,a^e,\,0))\leq2\eta^2\gamma_4H_1^{\mathrm{T}}P_{H_1}P_{H_1}H_1+\frac{1}{\eta^2}\frac{1}{\gamma_4}\|P_{H_1}^{-1}C_f\|^2(\rho_5^2\|\bar{a}\|^2+\rho_6^2\|\varrho_a\|^2) \tag{C3}$$

由式 (19) 和式 (20) 可得 $-\mathbf{He}(P_{H_2}A_{H_2})+\frac{1}{\gamma_1}\times A_{H_2}^{\mathrm{T}}A_{H_2}+2(\gamma_2+\gamma_3)P_{H_2}P_{H_2}<0$, $\mathbf{He}(P_{H_1}A_{H_1})+\frac{1}{\gamma_5}A_{H_1}A_{H_1}^{\mathrm{T}}+\gamma_4P_{H_1}P_{H_1}<0$, 且由式 (21) 可得:

$$\begin{aligned}\dot{V}\leq&-\gamma_{e_1}e_1^{\mathrm{T}}e_1-\gamma_{e_2}e_2^{\mathrm{T}}e_2+\\&\sigma_{e_1}^2\Omega_{e_1}^{\mathrm{T}}\Omega_{e_1}+\left(\sigma_{e_2}^2+\frac{1}{\gamma_2}\right)\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}-\\&\eta^2\gamma_{H_2}\lambda_{\min}(P_{H_2}P_{H_2}^{\mathrm{T}})H_2^{\mathrm{T}}H_2-\\&\eta^2\gamma_{H_1}\lambda_{\min}(P_{H_1}P_{H_1}^{\mathrm{T}})H_1^{\mathrm{T}}H_1-\\&\rho_3(\|\bar{a}\|)+\gamma_6\|C_f\|^2\|\bar{a}\|^2+\gamma_8\rho_6^2\rho_4^2(\|\bar{a}\|)+\\&\frac{1}{\eta^2}\frac{1}{\gamma_4}\|P_{H_1}^{-1}C_f\|^2\rho_5^2\|\bar{a}\|^2+\gamma_5\|C_f\|^2\|\bar{a}\|^2+\\&\left(\frac{1}{\gamma_3}\|D_f\|^2+\frac{1}{\eta^2}\frac{1}{\gamma_4}\|P_{H_1}^{-1}C_f\|^2\rho_6^2+\gamma_4\|D_f\|^2+\right.\\&\left.\frac{1}{\gamma_8}\right)\|\varrho_a\|^2+\left(\frac{1}{\gamma_3}+\gamma_4\right)\|C_f\|^2\|a^e\|^2\end{aligned}\tag{C4}$$

令

$$\begin{aligned}\Delta_a=&\frac{1}{\eta^2}\frac{1}{\gamma_4}\|P_{H_1}^{-1}C_f\|^2\rho_5^2\|\bar{a}\|^2+\gamma_5\|C_f\|^2\|\bar{a}\|^2+\\&\left(\frac{1}{\gamma_3}\|D_f\|^2+\frac{1}{\eta^2}\frac{1}{\gamma_4}\|P_{H_1}^{-1}C_f\|^2\rho_6^2+\gamma_4\|D_f\|^2+\right.\\&\left.\frac{1}{\gamma_8}\right)\|\varrho_a\|^2+\left(\frac{1}{\gamma_3}+\gamma_4\right)\|C_f\|^2\|a^e\|^2\end{aligned}$$

定义 $\rho_a(\|\bar{a}\|)=\rho_3(\|\bar{a}\|)-\gamma_6\|C_f\|^2\|\bar{a}\|^2-\gamma_8\times\rho_6^2\rho_4^2(\|\bar{a}\|)$, 选择 γ_6 和 γ_8, 令 $\rho_a(\|\bar{a}\|)$ 属于 K 类函数, 则有

$$\begin{aligned}\dot{V}\leq&-\gamma_{e_1}e_1^{\mathrm{T}}e_1-\gamma_{e_2}e_2^{\mathrm{T}}e_2+\left(\sigma_{e_2}^2+\frac{1}{\gamma_2}\right)\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}+\\&\Delta_a-\eta^2\lambda_{\min}(P_H)\|H\|^2+\sigma_{e_1}^2\Omega_{e_1}^{\mathrm{T}}\Omega_{e_1}-\rho_a(\|\bar{a}\|)\end{aligned}\tag{C5}$$

式中 $H=[H_1;H_2]$, $P_H=\mathrm{diag}\{\gamma_{H_1}\lambda_{\min}(P_{H_1}P_{H_1}^{\mathrm{T}}),\ \gamma_{H_2}\lambda_{\min}(P_{H_2}P_{H_2}^{\mathrm{T}})\}$.

对于 $\Omega_{e_1}=\mathbf{0}$ 和 $\Omega_{e_2}=\mathbf{0}$ 的情况, 当 $\|H\|>\frac{1}{\eta}\times\sqrt{\Delta_a}$ 时, 可以保证 $\dot{V}<0$, 这意味着观测器的估计误差几乎为零且 $\|H\|\leq\frac{1}{\eta}\sqrt{\Delta_a}$. 对于足够大的 η, $\lim_{\eta\to\infty}\|H\|=0$. 根据式 (15) 可得 $\lim_{t\to\infty}f(t)=\lim_{t\to\infty}\hat{f}(t)$.

考虑到 $\Omega_{e_1}\neq\mathbf{0}$ 或 $\Omega_{e_2}\neq\mathbf{0}$ 的情况, 当 η 足够大时, 可以得到

$$\begin{aligned}&\int_0^\infty\left(\gamma_{e_1}e_1^{\mathrm{T}}e_1+\gamma_{e_2}e_2^{\mathrm{T}}e_2-\sigma_{e_1}^2\Omega_{e_1}^{\mathrm{T}}\Omega_{e_1}-\right.\\&\left.\left(\sigma_{e_2}^2+\frac{1}{\gamma_2}\right)\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}\right)\mathrm{d}\tau\leq\int_0^\infty\left(\gamma_{e_1}e_1^{\mathrm{T}}e_1+\right.\\&\left.\gamma_{e_2}e_2^{\mathrm{T}}e_2-\sigma_{e_1}^2\Omega_{e_1}^{\mathrm{T}}\Omega_{e_1}-\left(\sigma_{e_2}^2+\frac{1}{\gamma_2}\right)\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}+\dot{V}\right)\mathrm{d}\tau+\\&V(0)-V(\infty)\leq0\end{aligned}\tag{C6}$$

可得 $\int_0^\infty\gamma_{e_1}e_1^{\mathrm{T}}e_1+\gamma_{e_2}e_2^{\mathrm{T}}e_2\mathrm{d}\tau\leq\int_0^\infty\sigma_{e_1}^2\Omega_{e_1}^{\mathrm{T}}\Omega_{e_1}+(\sigma_{e_2}^2+\frac{1}{\gamma_2})\Omega_{e_2}^{\mathrm{T}}\Omega_{e_2}\mathrm{d}\tau+V(\infty)$. 令 $\gamma_e=\mathrm{diag}\{\gamma_{e_1},\ \gamma_{e_2}\}$, $\sigma_e^2=\mathrm{diag}\{\sigma_{e_1}^2,\ \sigma_{e_2}^2\}$, $\sigma=\frac{\lambda_{\max}(\sigma_e)}{\lambda_{\min}(\gamma_e)}$. 定义 $e=[e_1;e_2]$ 和 $\Omega=[\Omega_{e_1};\Omega_{e_2}]$, 可得到 $\int_0^\infty e^{\mathrm{T}}e\mathrm{d}\tau\leq\int_0^\infty\sigma^2\Omega^{\mathrm{T}}\Omega\mathrm{d}\tau+\frac{1}{\lambda_{\min}(\gamma_e^2)}V(\infty)$, 这表明观测器的误差系统有 σ 水平的 H_∞ 性能. □

References

1 Li Hong-Yang, Wei Mu-Heng, Huang Jie, Qiu Bo-Hua, Zhao Ye, Luo Wen-Cheng, et al. Survey on cyber-physical systems. *Acta Automatica Sinica*, 2019, **45**(1): 37−50
(李洪阳, 魏慕恒, 黄洁, 邱伯华, 赵晔, 骆文城, 等. 信息物理系统技术综述. 自动化学报, 2019, **45**(1): 37−50)

2 Huang X, Li J, Su Q Y. An observer with cooperative interaction structure for biasing attack detection and secure control. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **53**(4): 2543−2553

3 Yuan Hao-Nan, Guo Ge. Vehicle cooperative optimization scheduling in transportation cyber physical systems. *Acta Automatica Sinica*, 2019, **45**(1): 143−152
(原豪男, 郭戈. 交通信息物理系统中的车辆协同运行优化调度. 自动化学报, 2019, **45**(1): 143−152)

4 Guo Z G, Zhang Y F, Zhao X B, Song X Y. CPS-based self-adaptive collaborative control for smart production-logistics systems. *IEEE Transactions on Cybernetics*, 2021, **51**(1): 188−198

5 Yang Fei-Sheng, Wang Jing, Pan Quan, Kang Pei-Pei. Resilient event-triggered control of grid cyber-physical systems against cyber attack. *Acta Automatica Sinica*, 2019, **45**(1): 110−119
(杨飞生, 汪璟, 潘泉, 康沛沛. 网络攻击下信息物理融合电力系统的弹性事件触发控制. 自动化学报, 2019, **45**(1): 110−119)

6 Ma H, Zhou Q, Li H Y, Lu R Q. Adaptive prescribed performance control of a flexible-joint robotic manipulator with dynamic uncertainties. *IEEE Transactions on Cybernetics*, 2022, **52**(12): 12905−12915

7 Chang W M, Li Y M, Tong S C. Adaptive fuzzy backstepping tracking control for flexible robotic manipulator. *IEEE/CAA Journal of Automatica Sinica*, 2021, **8**(12): 1923−1930

8 Wang X M, Niu B, Zhao X D, Zong G D, Cheng T T, Li B. Command-filtered adaptive fuzzy finite-time tracking control algorithm for flexible robotic manipulator: A singularity-free approach. *IEEE Transactions on Fuzzy Systems*, DOI: 10.1109/TFUZZ.2023.3298367

9 Yang F S, Liang X H, Guan X H. Resilient distributed economic dispatch of a cyber-power system under DoS attack. *Frontiers of Information Technology & Electronic Engineering*, 2021, **21**(1): 40−50

10 Li Z Q, Li Q, Ding D W, Sun X M. Robust resilient control for nonlinear systems under denial-of-service attacks. *IEEE Transactions on Fuzzy Systems*, 2021, **29**(11): 3415−3427

11 Yan J J, Yang G H, Liu X X. A multigain-switching-mechanism-based secure estimation scheme against DoS attacks for nonlinear industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 2023, **70**(5): 5094−5103

12 Qi W H, Lv C Y, Zong G D, Ahn C K. Sliding mode control for fuzzy networked semi-markov switching models under cyber attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2022, **69**(12): 5034−5038

13 Jiao S Y, Xu S Y, Park J. Hybrid-triggered-based control against denial-of-service attacks for fuzzy switched systems with persistent dwell-time. *IEEE Transactions on Fuzzy Systems*, DOI: 10.1109/TFUZZ.2023.3305349

14 Liu J L, Wei L L, Xie X P, Tian E, Fei S. Quantized stabiliza-

tion for T-S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. *IEEE Transactions on Fuzzy Systems*, 2018, **26**(6): 3820−3834

15 Wang X, Park J, Li H Q. Fuzzy secure event-triggered control for networked nonlinear systems under DoS and deception attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023, **53**(7): 4165−4175

16 Gu Z, Shi P, Yue D, Yan S, Xie X P. Memory-based continuous event-triggered control for networked T-S fuzzy systems against cyberattacks. *IEEE Transactions on Fuzzy Systems*, 2021, **29**(10): 3118−3129

17 Han C S, Lv C Y, Xie K, Qi W H, Cheng J, Shi K B, et al. Security SMC for networked fuzzy singular systems with semi-markov switching parameters. *IEEE Access*, 2022, **10**: 45093−45101

18 Li X H, Zhu F H, Chakrabarty A, Zak S. Nonfragile fault-tolerant fuzzy observer-based controller design for nonlinear systems. *IEEE Transactions on Fuzzy Systems*, 2016, **24**(6): 1679−1689

19 Lian Hong-Hai, Xiao Shen-Ping, Luo Yi-Ping, Zhou Bi-Feng. Robust dissipative control for sampled-data system based on T-S fuzzy model. *Acta Automatica Sinica*, 2022, **48**(11): 2852−2862 (练红海, 肖伸平, 罗毅平, 周笔锋. 基于 T-S 模糊模型的采样系统鲁棒耗散控制. 自动化学报, 2022, **48**(11): 2852−2862)

20 Huang X, Dong J X. An adaptive secure control scheme for T-S fuzzy systems against simultaneous stealthy sensor and actuator attacks. *IEEE Transactions on Fuzzy Systems*, 2021, **29**(7): 1978−1991

21 Mao J, Meng X, Ding D. Fuzzy set-membership filtering for discrete-time nonlinear systems. *IEEE/CAA Journal of Automatica Sinica*, 2022, **9**(6): 1026−1036

22 Liu Y, Wu F, Ban X J. Dynamic output feedback control for continuous-time T-S fuzzy systems using fuzzy lyapunov functions. *IEEE Transactions on Fuzzy Systems*, 2017, **25**(5): 1155−1167

23 Zhang Z, Zhang Z X, Zhang H. Distributed attitude control for multispacecraft via Takagi-Sugeno fuzzy approach. *IEEE Transactions on Aerospace and Electronic Systems*, 2018, **54**(2): 642−654

24 Gao Q, Zeng X J, Feng G, Wang Y, Qiu J B. T-S-fuzzy-model-based approximation and controller design for general nonlinear systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 2012, **42**(4): 1143−1154

25 Mu Y F, Zhang H G, Xi R P, Wang Z L, Su J Y. Fault-tolerant control of nonlinear systems with actuator and sensor faults based on T-S fuzzy model and fuzzy observer. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **52**(9): 5795−5804

26 Tanaka K, Wang H O. *Fuzzy Control Systems Design and Analysis: A Linear Matrix Inequality Approach*. New York: John Wiley & Sons, 2001.

27 Wang Shao-Yu, Huang Kai-Zhi, Xu Xiao-Ming, Ma Ke-Ming, Chen Ya-Jun. Man-in-the-middle pilot attack for physical layer authentication. *Journal of Electronics & Information Technology*, 2021, **43**(11): 3141−3148 (王少禹, 黄开枝, 许晓明, 马克明, 陈亚军. 物理层认证的中间人导频攻击分析. 电子与信息学报, 2021, **43**(11): 3141−3148)

28 Yao Zhi-Qiang, Zhu Zhi-Rong, Ye Guo-Hua. Achieving resist against DHCP man-in-the-middle attack scheme based on key agreement. *Journal on Communications*, 2021, **42**(8): 103−110 (姚志强, 竺智荣, 叶帼华. 基于密钥协商的防范 DHCP 中间人攻击方案. 通信学报, 2021, **42**(8): 103−110)

29 Chen X L, Hu S L, Li Y, Yue D, Dou C X, Ding L. Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks. *IEEE Transactions on Smart Grid*, 2022, **13**(3): 2357−2368

30 Teixeira A, Shames I, Sandberg H, Johansson K H. A secure control framework for resource-limited adversaries. *Automatica*, 2015, **51**: 135−148

31 Ladel A, Benzaouia A, Outbib R, Ouladsine M. Integrated state/fault estimation and fault-tolerant control design for switched T-S fuzzy systems with sensor and actuator faults. *IEEE Transactions on Fuzzy Systems*, 2021, **30**(8): 3211−3223

32 Khalil H K. *Nonlinear Systems*. London: Prentice-Hall, 2002. 175−180

黄 鑫 东北电力大学自动化工程学院教授. 主要研究方向为信息物理系统安全控制, 模糊控制, 容错控制, 多智能体系统协同控制及其应用. 本文通信作者.
E-mail: huangxin@neepu.edu.cn
(**HUANG Xin** Professor at the School of Automation Engineering, Northeast Electric Power University. His research interest covers cyber-physical system security control, fuzzy control, fault-tolerant control, multi-agent system cooperative control, and their applications. Corresponding author of this paper.)

畅晨旭 东北电力大学自动化工程学院硕士研究生. 主要研究方向为信息物理系统的安全控制.
E-mail: ccxzhongshuo@163.com
(**CHANG Chen-Xu** Master student at the School of Automation Engineering, Northeast Electric Power University. His main research interest is secure control of cyber-physical systems.)

肖舒怡 太原理工大学电气与动力工程学院讲师. 主要研究方向为多智能体系统协同控制, 鲁棒自适应控制和容错控制.
E-mail: xiaoshuyi@tyut.edu.cn
(**XIAO Shu-Yi** Lecturer at the College of Electrical and Power Engineering, Taiyuan University of Technology. Her research interest covers cooperative control of multi-agent systems, robust adaptive control and fault-tolerant control.)

李小杭 北方信息控制研究院集团有限公司工程师. 主要研究方向为网络信息体系及信息物理系统的安全控制.
E-mail: 18640349807@163.com
(**LI Xiao-Hang** Engineer at Northern Information Control Research Institute Group Co., Ltd. His research interest covers network information systems and security control of cyber-physical systems.)