DOI:10.13652/j.spjx.1003.5788.2022.81040 [文章编号] 1003-5788(2023)07-0085-08

面向信息物理系统的食品拣取机器人状态估计与攻击检测

State estimation and attack detection of food picking robot oriented to cyber-physical system

董 旭

DONG Xu

(北华航天工业学院,河北 廊坊 065000)

(*North China Institute of Aerospace Engineering*, *Langfang*, *Hebei* 065000, *China*)

摘要:目的:应对食品拣取机器人信息物理系统受网络攻击的情况。**方法:**基于区间观测器提出了一种用于食品拣取机器人系统状态估计与攻击检测的方法。首先建立位于信息物理系统中的食品拣取机器人数字化模型,应用拉格朗日方法确立机械臂动力学方程并转换为状态空间模型,而后依据反馈控制策略构建系统网络攻击模型。考虑系统中存在的非线性特征和噪声,应用广义系统理论将传感器攻击转换为系统状态,设计区间观测器为攻击检测器,并验证其误差系统的稳定性。**结果:**通过给定参数进行仿真,观测器输出贴近给定真实信号,所提方法正确且有效。由区间估计结果可以重构传感器攻击并检测出执行器攻击。**结论:**试验所提方法可以实现信息物理系统环境中的食品拣取机器人状态估计与执行器攻击检测。

关键词:信息物理系统;食品拣取机器人;区间观测器;状态估计;执行器攻击检测

Abstract: Objective: In order to deal with the impact of cyber attack on the cyber-physical system of food picking robot. **Methods:** A method for states estimation and attacks detection of food picking robot system based on interval observer was proposed. Firstly, the digital model of the food picking robot located in the cyber-physical system was established, using Lagrange method to establish the dynamic equation of the manipulator and convert it into the state-space model, the network attacks model was constructed according to the feedback control strategy. Considering the nonlinear characteristics and noiseand applying the generalized system theory was applied to transform sensor attack into the system state, and the interval observer was designed as the attack detector, and the stability of errors system was proved. **Results:** The simulation results showed that observer output was close to the given real signal. The proposed method was correct and effective. The sensor attack can be reconstructed and the actuator attack can be detected from interval estimation results. **Conclusion:** The proposed method can realize states estimation and actuator attacks detection of food picking robot in cyber-physical system environment.

Keywords: cyber-physical system; food picking robot; interval observer; state estimation; attack detection

工业机器人在食品生产领域的大量应用提高了企业生产效率,机器人代替人工劳动降低了企业人力成本,同时还有效提升了食品品质。具体而言,食品工业机器人在目标抓取、包装、拣取、食品生产流水线等场景均得到了一定的应用[1-5]。伴随着智能制造技术的快速发展,食品企业也在进行数字化转型与智能化升级。在这个过程中,信息技术在食品工业领域的快速应用实现了人与设备,设备与设备之间在互联互通物理环境下的相互感知、理解、融合控制,逐渐形成了面向食品生产的信息物理系统(Cyber-physical system)[6]。食品拣取机器人依靠末端执行器完成分拣、拾取动作,并通过机内传感器和机外传感器与信息系统进行数据联系[7],在食品生产线中发挥着重要作用[8]。机器人末端执行器具有夹取、放置物品功能,有吸附式、机械装置夹持式、专用工具式等形式[9]。然而,处于信息物理系统中的机器人,其附带传感器与执行器均有可能受到网络信号的攻击,导致系统数据丢失或者传输错误,影响机器人乃至整个产线作业。因此,准确估计机器人状态并实时准确地检测出网络攻击信号,对整个系统稳定运行具有重要意义。

基金项目:河北省省级科技计划资助(编号:18211840)

作者简介:董旭(1981—),男,北华航天工业学院副教授,硕士。E-mail:dongxu311@163.com

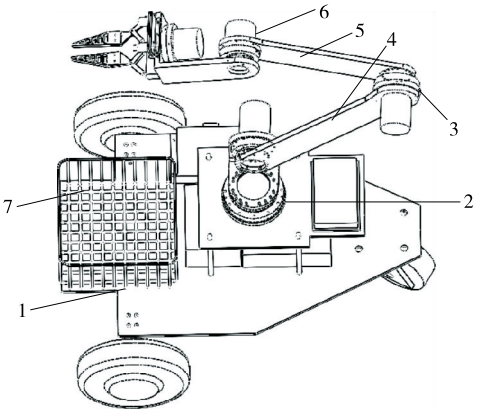
收稿日期:2022-11-12 **改回日期:**2023-05-18

Zhao 等[10]基于卡尔曼滤波动态模型提出了一种同时估计轮式移动机器人状态和描述其车轮滑移参数的方法。杨超群等[11]通过将系统状态和传感器观测变量建立随机有限集模型，并应用滤波器及粒子实现了信息物理系统的状态估计。Na 等[12]引入滤波运算方法，提出了一种未知系统动力学估计器，并用于机器人控制器的设计，获得了良好的运动跟踪响应结果。Lee 等[13]针对线性动力系统受传感器攻击情况，基于状态观测器提出了系统状态估计方案。同时，处在信息物理系统中的工业机器人，可能受到网络中的拒绝服务攻击[14]、数据注入攻击[15]、数据重放攻击[16]影响，所以研究行之有效的系统攻击检测方法受到学术界的广泛关注。Zhao 等[17]借助子空间识别技术设计了数据驱动方法应对信息物理系统的虚假数据注入攻击。Lucia 等[18]通过设计检测器提出了信息物理系统中的定点攻击检测策略。Sayad Haghighi 等[19]针对受到拒绝服务攻击系统，基于经典控制策略提出了网络系统的控制方法。刘一帆等[20]针对传感器网络中的拒绝服务攻击问题，在传感器节点设计了分布式滤波器生成残余信号，从而实现系统故障检测。同时，由于区间观测器具有自带阈值的有利条件[21]，在多领域的系统故障检测方面被成功应用[22]。综上，针对具体系统提出了有效的攻击检测策略的研究较多，但是基于食品拣取机器人信息物理系统攻击检测方面的研究尚未见报道。

面向信息物理系统的食品拣取机器人，研究拟提出一种系统状态估计以及攻击信号检测方法。考虑机器人需完成袋装食品物件的分拣与拾取任务，将执行器末端设计为典型的机械夹持式结构，进而建立食品拣取机器人虚拟样机模型。依据状态空间模型理论设计区间观测器估计系统状态，并进一步重构传感器攻击信号以及检测执行器攻击信号，旨在为信息物理系统中的多台食品机器人联合控制提供依据。

1　食品拣取机器人系统描述

食品拣取机器人结构形式整体为单链可移动关节式，主要部件包括底座、腰部、大臂、小臂、末端执行器等，虚拟样机模型如图 1 所示。传感器安装在底座、腰部与执行机构等部位，感知机械臂内部状态与外部产线环境信息。大臂、小臂、腰部与末端执行器均由电机进行驱动，末端执行器设计为机械夹持形式。执行器借助机器视觉系统调整位姿，夹持生产线中袋装食品物件放入指定收集装置。以对整机动力学特性影响比较明显的主要关节组件为研究对象，应用拉格朗日方法进行机械臂动力学建模[23]。机械臂构型简图如图 2 所示。腰部关节、大臂、小臂的回转角度分别为 θ_1、θ_2、θ_3；腰部连杆、大臂、小臂的长度分别为l_1、l_2、l_3，质量分别为m_1、m_2、m_3，转动惯量分别为 J_1、J_2、J_3。



1. 底盘　2. 腰关节　3. 肩关节　4. 大臂　5. 小臂　6. 肘关节　7. 收集装置

图 1　食品拣取机器人虚拟样机模型

Figure 1　Virtual prototype model of food picking robot

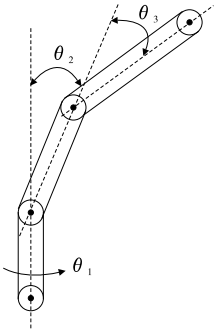


图 2　机械臂构型图

Figure 2　Manipulator configuration diagram

食品拣取机器人信息物理系统架构依据工业信息物理系统的功能要求确定[24]。系统主要包括机器人本体、执行器、传感器、信息层、传输层、决策层。拣取机器人在信息物理系统中除了完成分拣、放置任务外，还充当着物理空间与信息空间的媒介。机器人可以通过机内自带传感器与机外辅助类传感器获取物理环境数据，依托智能算法对数据进行实时处理，经系统传输层将物理空间数据传递给信息空间。控制端接收到机器人传输的数据进行决策后，经网络层发布后续的控制指令。食品拣取机械臂关节变量为角度 $\theta\in R^n$，角速度 $\dot{\theta}\in R^n$，角加速度 $\ddot{\theta}\in R^n$，电机转矩 $\tau\in R^n$，令

$$\boldsymbol{\theta}=\begin{bmatrix}\theta_1\\ \theta_2\\ \theta_3\end{bmatrix}, \tag{1}$$

$$\boldsymbol{\tau}=\begin{bmatrix}\tau_1\\ \tau_2\\ \tau_3\end{bmatrix}。 \tag{2}$$

各关节部件动能总和为：

$$K=\frac{1}{2}J_1\dot{\theta}_1^2+\frac{1}{2}J_2\dot{\theta}_2^2+\frac{1}{2}m_2(d_2\sin\theta_2)^2\dot{\theta}_1^2+\frac{1}{2}m_2(d_2\dot{\theta}_2)^2+\frac{1}{2}J_3(\dot{\theta}_2+\dot{\theta}_3)^2+\frac{1}{2}m_3[\dot{\theta}_1 l_2\sin\theta_2+\dot{\theta}_1 d_3\sin(\theta_2+\theta_3)]^2+\frac{1}{2}m_3(\dot{\theta}_2 l_2\sin\theta_3)^2+\frac{1}{2}m_3[\dot{\theta}_2 l_2\cos\theta_3+(\dot{\theta}_2+\dot{\theta}_3)d_3]^2。\tag{3}$$

各部分构件势能总和为:

$$P=m_1 g d_1+m_2 g(l_1+d_2\cos\theta_2)+m_3 g[l_1+l_2\cos\theta_2+d_3\cos(\theta_2+\theta_3)]。\tag{4}$$

依据 $L=K-P$,建立拉格朗日方程:

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{\partial L}{\partial\dot{\theta}}-\frac{\partial L}{\partial\theta}=\tau。\tag{5}$$

综上,机械臂动力学方程可表示为:

$$\boldsymbol{M}(\boldsymbol{\theta})\ddot{\theta}+\boldsymbol{C}(\boldsymbol{\theta},\dot{\boldsymbol{\theta}})\dot{\theta}+F(\dot{\theta})+\boldsymbol{G}(\theta)+J^T(\theta)h=\tau+\alpha_d,\tag{6}$$

式中:

$u\in R^n$——系统输入;

$y=\theta\in R^n$——系统输出;

$\boldsymbol{M}(\boldsymbol{\theta})\in R^{n\times n}$——系统惯性矩阵;

$\boldsymbol{C}(\boldsymbol{\theta},\dot{\boldsymbol{\theta}})\in R^{n\times n}$——科里奥利力和离心力矩阵;

$F(\dot{\theta})$——系统摩擦项;

$\boldsymbol{G}\in R^n$——重力矩阵;

$J^T(\theta)h$——关节广义力;

α_d——系统扰动;

$\tau\in R^n$——电机转矩。

令系统状态向量 $\boldsymbol{x}=[\alpha_1\quad\alpha_2]^T=[\theta\quad\dot{\theta}]^T\in R^{2n}$,由式(6)及系统状态向量 x 确定系统的解析模型为[25]:

$$\begin{cases}\dot{x}(t)=\begin{bmatrix}\dot{\alpha}_1(t)\\ \dot{\alpha}_2(t)\end{bmatrix}=\begin{bmatrix}0_n & I_n\\ 0_n & 0_n\end{bmatrix}\begin{bmatrix}\alpha_1(t)\\ \alpha_2(t)\end{bmatrix}+\\ \quad\begin{bmatrix}0_n\\ -M^{-1}(\alpha_1)(C(\alpha_1,\alpha_2)\alpha_2-F(\alpha_2)-G(\alpha_1))\end{bmatrix}+\\ \quad\begin{bmatrix}0_n\\ M^{-1}(\alpha_1)\alpha_d\end{bmatrix}+\begin{bmatrix}0_n\\ M^{-1}(\alpha_1)\end{bmatrix}\tau+\\ \quad\begin{bmatrix}0_n\\ -M^{-1}(\alpha_1)J^T(\alpha_1)\end{bmatrix}h\\ y=\theta=[I_n\quad 0_n]\begin{bmatrix}\alpha_1(t)\\ \alpha_2(t)\end{bmatrix}\end{cases}。\tag{7}$$

2　系统状态模型

将食品拣取机器人系统简化为线性离散时间系统模型,当执行器与传感器受到攻击时,系统可以描述为:

$$\begin{cases}x_{k+1}=A\boldsymbol{x}_k+Bu_k+w_k+Gg_k\\ y_k=C\boldsymbol{x}_k+q_k+Hf_k\end{cases},\tag{8}$$

式中:

$\boldsymbol{x}_k\in R^n$——系统状态向量(系统初始状态为 x_0);

$y_k\in R^p$——系统量测输出;

$u_k\in R^m$——系统控制输入;

w_k——系统非线性项和外部干扰噪声;

q_k——量测噪声。

当系统未受到网络攻击时,执行器攻击信号 $g_k=0$,传感器攻击信号 $f_k=0$。状态方程中系数矩阵 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$、$\boldsymbol{H}$、$\boldsymbol{G}$ 具有合适的维数,其中 $\boldsymbol{A}\in R^{n\times n}$,$\boldsymbol{B}\in R^{n\times m}$,$\boldsymbol{G}\in R^{n\times g}$,$\boldsymbol{C}\in R^{p\times n}$,$\boldsymbol{H}\in R^{p\times q}$,$w_k\in R^n$,$q_k\in R^p$。$g_k\in R^v$ 代表执行器攻击信号,$f_k\in R^q$ 代表传感器量测攻击信号。当系统未受到网络攻击时,建立系统状态模型[26]:

$$\begin{cases}x_{k+1}=A_0\boldsymbol{x}_k+B_0u_k+w_k\\ y_k=C_0\boldsymbol{x}_k+q_k\end{cases}。\tag{9}$$

反馈控制器可以表示为:

$$\begin{cases}\varepsilon_{k+1}=A_k\boldsymbol{\varepsilon}_k+B_ky_k\\ u_k=C_k\boldsymbol{\varepsilon}_k+D_ky_k\end{cases},\tag{10}$$

式中:

$\boldsymbol{\varepsilon}_k$——反馈控制向量。

令向量 $\boldsymbol{\varphi}_k=\begin{bmatrix}x_k\\ \varepsilon_k\end{bmatrix}$,$\boldsymbol{\omega}_k=\begin{bmatrix}w_k\\ q_k\end{bmatrix}$,则闭环系统可以表示为:

$$\begin{cases}\varphi_{k+1}=M\boldsymbol{\varphi}_k+N\boldsymbol{\omega}_k\\ y_k=U\boldsymbol{\varphi}_k+V\boldsymbol{\omega}_k\\ u_k=E\boldsymbol{\varphi}_k+G\boldsymbol{\omega}_k\end{cases}。\tag{11}$$

由式(11)可得:

$$\varphi_{k+1}=\begin{bmatrix}x_{k+1}\\ \varepsilon_{k+1}\end{bmatrix}=\begin{bmatrix}A_0\boldsymbol{x}_k+B_0u_k+w_k\\ A_k\boldsymbol{\varepsilon}_k+B_ky_k\end{bmatrix}=M\begin{bmatrix}\boldsymbol{x}_k\\ \boldsymbol{\varepsilon}_k\end{bmatrix}+N\begin{bmatrix}w_k\\ q_k\end{bmatrix}=\begin{bmatrix}M_{11} & M_{12}\\ M_{21} & M_{22}\end{bmatrix}\begin{bmatrix}x_k\\ \varepsilon_k\end{bmatrix}+\begin{bmatrix}N_{11} & N_{12}\\ N_{21} & N_{22}\end{bmatrix}\begin{bmatrix}w_k\\ q_k\end{bmatrix},\tag{12}$$

所以

$$M_{11}\boldsymbol{x}_k+M_{12}\boldsymbol{\varepsilon}_k+N_{11}w_k+N_{12}q_k=A_0\boldsymbol{x}_k+B_0u_k+w_k。\tag{13}$$

因为

$$u_k=C_k\boldsymbol{\varepsilon}_k+D_kC_0\boldsymbol{x}_k+D_kq_k,\tag{14}$$

所以由式(13)可以得到:

$$M_{11}\boldsymbol{x}_k+M_{12}\boldsymbol{\varepsilon}_k+N_{11}w_k+N_{12}q_k=A_0\boldsymbol{x}_k+B_0(C_k\boldsymbol{\varepsilon}_k+D_kC_0\boldsymbol{x}_k+D_kq_k)+w_k。\tag{15}$$

$M_{11}=A_0+B_0D_kC_0$,$M_{12}=B_0C_k$,$N_{11}=I$,$N_{12}=B_0D_k$。

由式(12)可得:

$$M_{21}\boldsymbol{x}_k+M_{22}\boldsymbol{\varepsilon}_k+G_{21}Dw_k+G_{22}Hq_k=A_k\boldsymbol{\varepsilon}_k+B_ky_k,\tag{16}$$

所以 $M_{21}=B_kC_0$,$M_{22}=A_k$,$N_{21}=0$,$N_{22}=B_k$。

综上，$\boldsymbol{M}=\begin{bmatrix}A_0+B_0D_kC_0 & B_0C_k\\ B_kC_0 & A_k\end{bmatrix}$，$\boldsymbol{N}=\begin{bmatrix}I & B_0D_k\\ 0 & B_k\end{bmatrix}$。

同时，由式(11)可以得出：

$$y_k=U\boldsymbol{\varphi_k}+Vf_k=[U_1\quad U_2]\begin{bmatrix}\boldsymbol{x_k}\\ \boldsymbol{\varepsilon_k}\end{bmatrix}+[V_1\quad V_2]\begin{bmatrix}w_k\\ q_k\end{bmatrix}=C_0\boldsymbol{x_k}+q_k, \tag{17}$$

$$u(k)=E\begin{bmatrix}\boldsymbol{x_k}\\ \boldsymbol{\varepsilon_k}\end{bmatrix}+G\begin{bmatrix}w_k\\ q_k\end{bmatrix}=[E_1\quad E_2]\begin{bmatrix}\boldsymbol{x_k}\\ \boldsymbol{\varepsilon_k}\end{bmatrix}+[G_1\quad G_2]\begin{bmatrix}w_k\\ q_k\end{bmatrix}=C_k\boldsymbol{\varepsilon_k}+D_kC_0\boldsymbol{x_k}+D_kq_k, \tag{18}$$

所以 $U=[C_0\quad 0]$，$V=[0\quad I]$，$E=[D_kC_0\quad C_k]$，$G=[0\quad D_k]$。

当系统含有攻击信号时，建立系统状态模型[27]：

$$\begin{cases}x_{k+1}=A_0\boldsymbol{x_k}+B_0u_k+w_k+Gg_k\\ \tilde{y}_k=C_0\boldsymbol{x_k}+q_k+Hf_k\end{cases}。 \tag{19}$$

反馈控制器：

$$\begin{cases}\varepsilon_{k+1}=A_k\boldsymbol{\varepsilon_k}+B_k(y_k+Hf_k)\\ \tilde{u}_k=C_k\boldsymbol{\varepsilon_k}+D_k(y_k+Hf_k)+Gg_k\end{cases}。 \tag{20}$$

攻击向量定义为 $[g_k\quad f_k]^T$，则系统受到攻击后的闭环模型为：

$$\begin{cases}\varphi_{k+1}=M\boldsymbol{\varphi_k}+Nf_k+Q_1\begin{bmatrix}g_k\\ f_k\end{bmatrix}\\ \tilde{y}_k=U\boldsymbol{\varphi_k}+Vf_k+Q_2\begin{bmatrix}g_k\\ f_k\end{bmatrix}\\ \tilde{u}_k=E\boldsymbol{\varphi_k}+Gf_k+Q_3\begin{bmatrix}g_k\\ f_k\end{bmatrix}\end{cases}。 \tag{21}$$

由式(21)中 $\varphi_{k+1}=\begin{bmatrix}A_0\boldsymbol{x_k}+B_0u_k+w_k\\ A_k\boldsymbol{\varepsilon_k}+B_ky_k\end{bmatrix}+Q_1\begin{bmatrix}g_k\\ f_k\end{bmatrix}=\begin{bmatrix}A_0\boldsymbol{x_k}+B_0u_k+w_k+Gg_k\\ A_kz_k+B_k(y_k+Hf_k)\end{bmatrix}$，可得 $Q_1=\begin{bmatrix}G & 0\\ 0 & B_kH\end{bmatrix}$，由 $\tilde{y}_k=C\boldsymbol{\varphi_k}+Vf_k+Q_2\begin{bmatrix}g_k\\ f_k\end{bmatrix}=C_0\boldsymbol{x_k}+q_k+Hf_k$，可得 $Q_2=[0\quad H]$，由 $\tilde{u}_k=C_k\boldsymbol{\varepsilon_k}+D_k(y_k+Hf_k)+Gg_k=C_k\boldsymbol{\varepsilon_k}+D_ky_k+Q_3\begin{bmatrix}g_k\\ f_k\end{bmatrix}$，可得 $Q_3=[G\quad D_kH]$。

3　观测器设计

假设 $\delta_k=\begin{bmatrix}x_k\\ f_k\end{bmatrix}\in R^{n+q}$，$E=\begin{bmatrix}I_n & 0\\ 0 & 0_q\end{bmatrix}\in R^{(n+q)\times(n+q)}$，$A_1=\begin{bmatrix}A & 0\\ 0 & 0_q\end{bmatrix}\in R^{(n+q)\times(n+q)}$，$B_1=\begin{bmatrix}B\\ 0_q\end{bmatrix}\in R^{(n+q)\times m}$，$G_1=\begin{bmatrix}G\\ 0_q\end{bmatrix}\in R^{(n+q)\times g}$，$C_1=[C\quad H]\in R^{p\times(n+q)}$，所以式(8)转换为：

$$\begin{cases}E\delta_{k+1}=A_1\delta_k+B_1u_k+w_k+G_1g_k\\ y_k=C_1\delta_k+q_k\end{cases}。 \tag{22}$$

确定系统变量上下边界为 $\bar{\delta}_0=\begin{bmatrix}\bar{x}_0\\ \bar{f}_0\end{bmatrix}$ 以及 $\underline{\delta}_0=\begin{bmatrix}\underline{x}_0\\ \underline{f}_0\end{bmatrix}$，且 $\underline{\delta}_0\leqslant\delta_0\leqslant\bar{\delta}_0$，此时

$$\operatorname{rank}\begin{bmatrix}E\\ C_1\end{bmatrix}=\operatorname{rank}\begin{bmatrix}I_n & 0\\ 0 & 0_q\\ C & H\end{bmatrix}=n+q。 \tag{23}$$

由此可以确定 $[E\quad C_1]^T$ 是一个列满秩矩阵，即存在行满秩矩阵 $[T\quad J]\in R^{(n+q)\times(n+p+q)}$，使得 $TE+JC_1=I_{n+q}$，所以

$$TE\delta_{k+1}=TA_1\delta_k+TB_1u_k+Tw_k+TG_1g_k, \tag{24}$$

$$Jy_{k+1}=JC_1\delta_{k+1}+Jq_{k+1}。 \tag{25}$$

由式(24)与式(25)可以得到：

$$\delta_{k+1}=TA_1\delta_k+TB_1u_k+Tw_k+TG_1g_k+Jy_{k+1}-Jq_{k+1}。 \tag{26}$$

若令 $\delta_k=z_k+Jy_k$，则

$$z_{k+1}=\delta_{k+1}-Jy_{k+1}=TA_1z_k+TA_1Jy_k+TB_1u_k+Tw_k+TG_1g_k-Jq_{k+1}, \tag{27}$$

所以 $z_0=\delta_0-Jy_0$，且 z_0 的上界与下界为：$\bar{z}_0=\bar{\delta}_0-Jy_0$，$\underline{z}_0=\underline{\delta}_0-Jy_0$。

假设系统变量 $x_k\in R^n$ 满足 $\underline{x}_k\leqslant x_k\leqslant\bar{x}_k$，那么对任意矩阵 $\boldsymbol{\Phi}\in R^{m\times n}$，满足以下条件[28]：

$$\Phi^+\underline{x}_k-\Phi^-\bar{x}_k\leqslant\boldsymbol{\Phi}x_k\leqslant\Phi^+\bar{x}_k-\Phi^-\underline{x}_k。 \tag{28}$$

当系统不存在执行器攻击时，设计区间观测器为：

$$\begin{cases}\bar{z}_{k+1}=(TA_1)^+\bar{z}_k-(TA_1)^-\underline{z}_k+TA_1Jy_k+TB_1u_k+(T)^+\bar{w}-(T)^-\underline{w}-(J^+\underline{q}-J^-\bar{q})\\ \underline{z}_{k+1}=(TA_1)^+\underline{z}_k-(TA_1)^-\bar{z}_k+TA_1Jy_k+TB_1u_k+(T)^+\underline{w}-(T)^-\bar{w}-(J^+\bar{q}-J^-\underline{q})\end{cases}。 \tag{29}$$

若 TA_1 是 Schur 且为非负矩阵时，$(TA_1)^+=TA_1$，$(TA_1)^-=0$，式(29)可转换为：

$$\begin{cases}\bar{z}_{k+1}=(TA_1)^+\bar{z}_k+TA_1Jy_k+TB_1u_k+(T)^+\bar{w}-(T)^-\underline{w}-(J^+\underline{q}-J^-\bar{q})\\ \underline{z}_{k+1}=(TA_1)^+\underline{z}_k+TA_1Jy_k+TB_1u_k+(T)^+\underline{w}-(T)^-\bar{w}-(J^+\bar{q}-J^-\underline{q})\end{cases}。 \tag{30}$$

上界估计误差为:

$$\overset{\sim}{\underline{z}}_{k+1}=\bar{z}_{k+1}-z_{k+1}=(TA_1)^{+}\bar{z}_k+TA_1Jy_k+TB_1u_k+(T)^{+}\bar{w}-(T)^{-}\underline{w}-(J^{+}\underline{q}-J^{-}\bar{q})-TA_1z_k-TA_1Jy_k-TB_1u_k-Tw_k+Jq=TA\overset{\sim}{\underline{z}}_k+(T)^{+}\bar{w}-(T)^{-}\underline{w}-Tw_k+Jq-J^{+}\underline{q}+J^{-}\bar{q}+Jq。\tag{31}$$

下界估计误差为:

$$\overset{\sim}{\underline{z}}_{k+1}=z_{k+1}-\underline{z}_{k+1}=TA_1z_k+TA_1Jy_k+TB_1u_k+Tw_k-Jq-(TA_1)^{+}\underline{z}_k-TA_1Jy_k-TB_1u_k-(T)^{+}\underline{w}+(T)^{-}\bar{w}+J^{+}\bar{q}-J^{-}\underline{q}=TA_1\overset{\sim}{\underline{z}}_k+Tw_k-T^{+}\underline{w}+T^{-}\bar{w}-Jq+J^{+}\bar{q}-J^{-}\underline{q}。\tag{32}$$

因为 $(T)^{+}\underline{w}_k-(T)^{-}\bar{w}_k\leqslant(T)w_k\leqslant(T)^{+}\bar{w}_k-(T)^{-}\underline{w}_k$ 以及 $(J)^{+}\underline{q}-(J)^{-}\bar{q}\leqslant(J)q\leqslant(J)^{+}\bar{q}-(J)^{-}\underline{q}$,所以 $\overset{\sim}{\underline{z}}_{k+1}\geqslant0$,$\overset{\sim}{\underline{z}}_{k+1}\geqslant0$,式(31)与式(32)均是稳定的,即式(29)是系统式(27)的区间观测器。

4　状态估计与攻击检测

为了验证所提方法的正确性和有效性,进行仿真试验。基于上述机器人虚拟样机模型,基座、腰部、大臂、小臂材质均为铝,模型参数见表1。

由模型参数确定系数矩阵:

$$\boldsymbol{A}_1=\begin{bmatrix}0&0&0&1&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\\0&0&0&0&0&0&0\end{bmatrix},\tag{33}$$

$$\boldsymbol{B}_1=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\\0.894\,5&0&0\\0&0.741\,3&-1.242\,0\\0&-1.242\,0&5.004\,9\\0&0&0\end{bmatrix},\tag{34}$$

$$\boldsymbol{C}_1=\begin{bmatrix}1&0&0&0&0&-10\\0&1&0&0&0&-17\\0&0&1&0&0&-10\end{bmatrix},\tag{35}$$

$$\boldsymbol{T}=\begin{bmatrix}0.602\,2&0.173\,8&0.102\,2&0&0&0&0\\0.173\,8&0.795\,5&0.173\,8&0&0&0&0\\0.102\,2&0.173\,8&0.602\,2&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\\0.020\,4&0.034\,8&0.020\,4&0&0&0&0\end{bmatrix},\tag{36}$$

$$\boldsymbol{J}=\begin{bmatrix}0.397\,8&-0.173\,8&-0.102\,2\\-0.173\,8&0.204\,5&-0.173\,8\\-0.102\,2&-0.173\,8&0.397\,8\\0&0&0\\0&0&0\\0&0&0\\-0.020\,4&-0.034\,8&-0.020\,4\end{bmatrix}。\tag{37}$$

矩阵 $\boldsymbol{TA}_1$ 为 Schur 且非负矩阵。假设系统控制输入为:

$$u(k)=10\sin(0.5k);1\leqslant k\leqslant200,\tag{38}$$

当系统不含执行器故障时估计系统状态,此时可以将传感器攻击信号设置为:

表1　机器人样机模型参数

Table 1　Model parameters of the robot prototype

参数	单位	描述	数值
l_1	m	腰部连接杆长度	0.05
l_2	m	大臂	0.47
l_3	m	小臂	0.37
m_1	kg	腰部关节质量	0.899
m_2	kg	大臂质量	2.476
m_3	kg	小臂质量	1.632
d_1	m	腰部连接杆质心到腰关节旋转中心距离	0.12
d_2	m	大臂质心到肩关节旋转中心距离	0.23
d_3	m	小臂质心到肘关节旋转中心距离	0.30
J_1	kg·m^2	腰部连接杆旋转惯量	0.006
J_2	kg·m^2	大臂旋转惯量	0.111
J_3	kg·m^2	小臂旋转惯量	0.012

$$f(k)=\begin{cases}0,0<k<30\\6,30\leqslant k<50\\0,50\leqslant k<70\\5\cos(5k),70\leqslant k<100\\0,100\leqslant k<120\\0.017k,120\leqslant k<180\\0,180\leqslant k\leqslant 200\end{cases}。\tag{39}$$

估计结果如图 3 所示。系统状态设定为六维，包括关节转角与关节转动角速度。由图 3 可知，估计值上下界均贴近真实值，说明应用试验方法可以取得良好的状态估计效果。由图 4 可知，传感器攻击信号重构效果良好。

考虑系统中含有执行器攻击信号的情况，将执行器攻击信号设置为 3 种形式。

第 1 种攻击信号设置为：

$$g_1(k)=\begin{cases}0,0\leqslant k<35\\0.1k,35\leqslant k<65,\\0,65\leqslant k<200\end{cases}\tag{40}$$

第 2 种执行器攻击信号设置为：

$$g_2(k)=\begin{cases}0,0\leqslant k<35\\10\sin(k),35\leqslant k<65,\\0,65\leqslant k<200\end{cases}\tag{41}$$

第 3 种执行器攻击信号设置为：

$$g_3(k)=\begin{cases}0,0\leqslant k<35\\10,35\leqslant k<65。\\0,65\leqslant k<200\end{cases}\tag{42}$$

当系统不存在执行器攻击信号时，可以定义出区间观测器的输出区间为$(\underline{y}_k,\bar{y}_k)$以及定义系统观测器的输出误差$e^+=y_k-\bar{y}_k$，$e^-=\underline{y}_k-y_k$，设定阈值为0.05。当

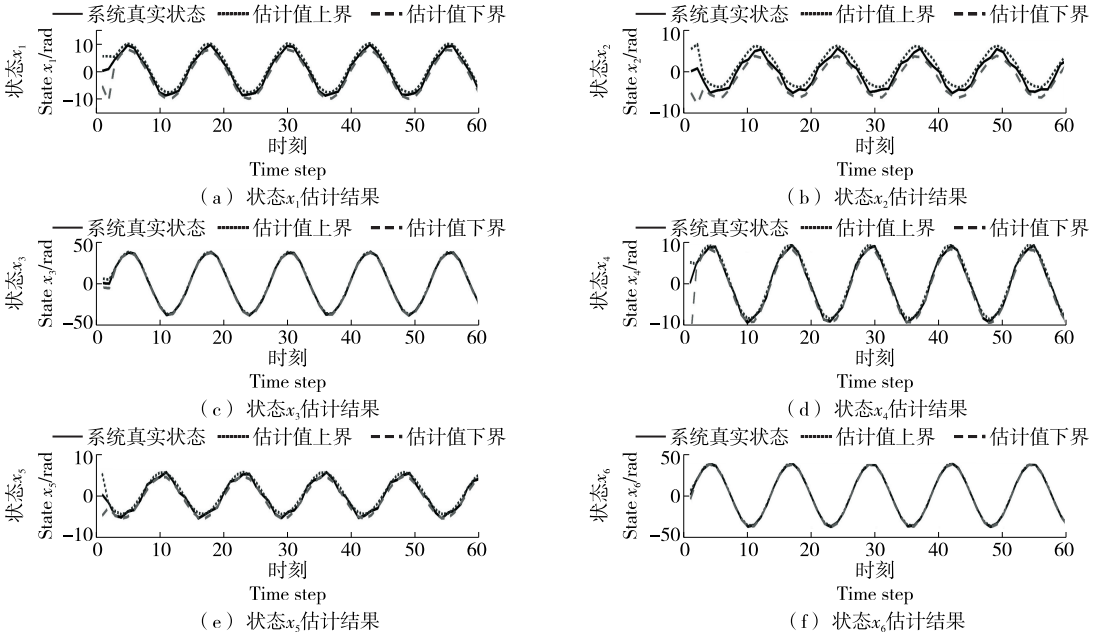


图 3　系统状态区间估计结果

Figure 3　Interval estimation results of system states

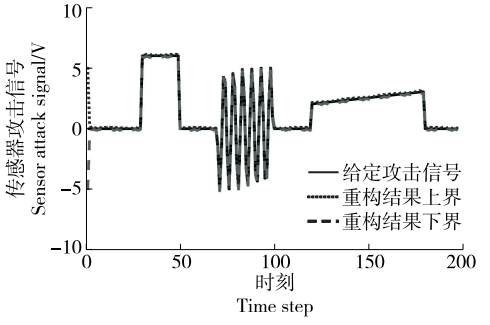


图 4　传感器攻击重构

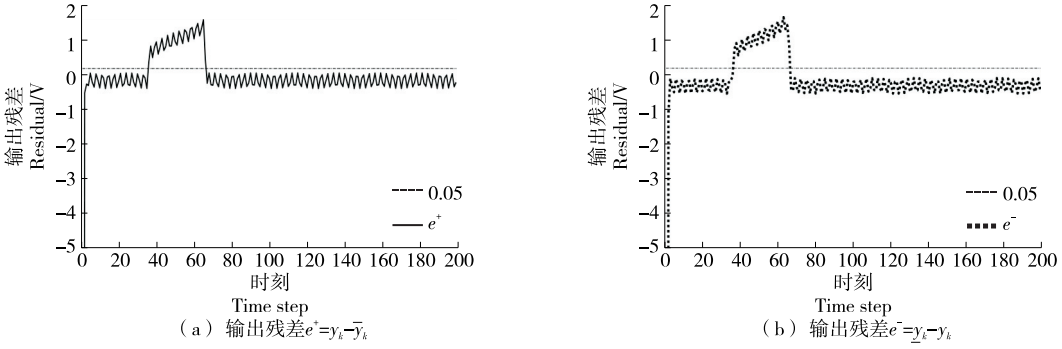
Figure 4　Sensor attack reconstruction

$e^+>0.05$ 或 $e^->0.05$，说明出现了攻击信号；若 $e^+\leqslant 0.05$或 $e^-\leqslant 0.05$，说明系统无攻击信号。

在 $35\leqslant k<65$ 时间段分别设置线性、正弦、突变等攻击信号进行仿真。由图 5～图 7 可知，在设定攻击时间段均有残差>0.05 情况，通过试验方法可以检测出执行器攻击信号。

5　结论

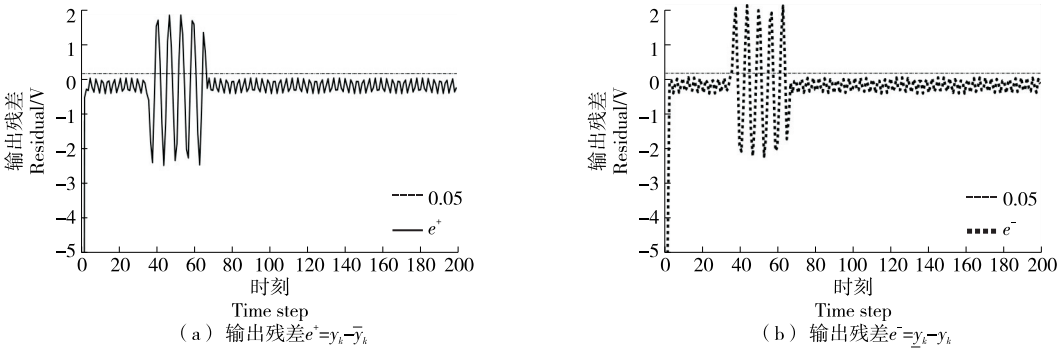
为了应对信息物理系统中食品拣取机器人传感器与执行器受到网络信号攻击的影响，提出了一种基于区间观测器的系统状态估计与攻击检测方法。通过仿真比较



（a）输出残差$e^+=y_k-\bar{y}_k$　　（b）输出残差$e^-=\underline{y}_k-y_k$

图 5　执行器受斜波信号攻击检测

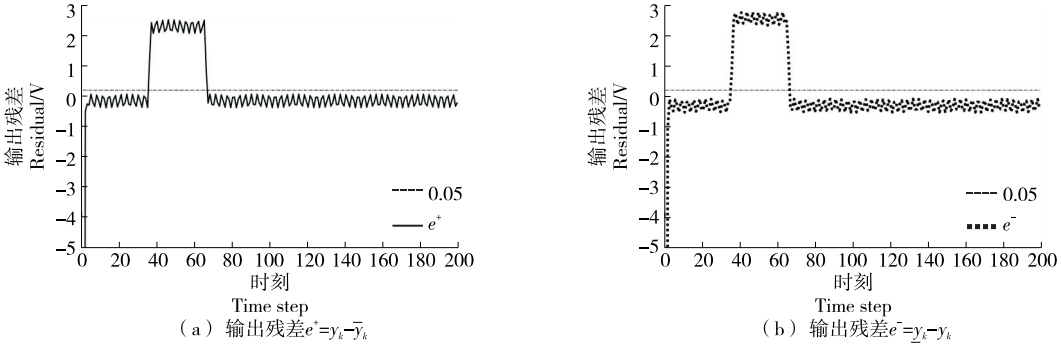
Figure 5　Detection of actuator attacked by ramp singal



（a）输出残差$e^+=y_k-\bar{y}_k$　　（b）输出残差$e^-=\underline{y}_k-y_k$

图 6　执行器受正弦信号攻击检测

Figure 6　Detection of actuator attacked by sinusoidal singal



（a）输出残差$e^+=y_k-\bar{y}_k$　　（b）输出残差$e^-=\underline{y}_k-y_k$

图 7　执行器受突变信号攻击检测

Figure 7　Detection of actuator attacked by abrupt singal

系统的真实输出与观测器输出，传感器的攻击信号得以重构，估计值贴近实际值，系统状态也同时得到估计，所提方法有效且正确。通过系统残差与设定阈值可以检测出 3 种类型的执行器的攻击信号，而准确设定阈值以避免系统误检与漏检仍需进一步研究。系统所受到的攻击可能是外部攻击也可能是内部攻击，针对具体的攻击场景，通过实际装备进行验证，能否准确定位受攻击传感器位置也是今后需要研究的问题。

参考文献

[1] 毕宪东, 王振, 李朝龙. 基于 Delta 机器人的食品生产线动态目标抓取方法[J]. 食品与机械, 2022, 38(6): 117-122.
BI X D, WANG Z, LI C L. Dynamic target grasping method of food production line based on Delta robot[J]. Food & Machinery, 2022, 38(6): 117-122.

[2] DAI J S, CALDWELL D G. Origami-based robotic paper-and-board packaging for food industry [J]. Trends in Food Science & Technology, 2010, 21(3): 153-157.

[3] BAGHERI M, NASERADINMOUSAVI P, KRSTIC M. Feedback linearization based predictor for time delay control of a high-DOF robot manipulator[J]. Automatica, 2019, 108: 108485.

[4] TALPUR M S H, SHAIKH M H. Automation of mobile pick and place robotic system for small food industry[J]. Computer Science,

2012, 11: 39-44.

[5] KHAN Z H, KHALID A, IQBAL J. Towards realizing robotic potential in future intelligent food manufacturing systems [J]. Innovative Food Science & Emerging Technologies, 2018, 48: 11-24.

[6] VANDERROOST M, RAGAERT P, VERWAEREN J, et al. The digitization of a food package's life cycle: Existing and emerging computer systems in the logistics and post-logistics phase [J]. Computers in Industry, 2017, 87: 15-30.

[7] IQBAL J, KHAN Z H, KHALID A. Prospects of robotics in food industry[J]. Food Science and Technology, 2017, 37: 159-165.

[8] CHUA P Y, ILSCHNER T, CALDWELL D G. Robotic manipulation of food products: A review [J]. Industrial Robot, 2003, 30(4): 345-354.

[9] HONG J, WANG D, GUAN Y. Synergistic integrated design of an electrochemical mechanical polishing end-effector for robotic polishing applications [J]. Robotics and Computer-Integrated Manufacturing, 2019, 55: 65-75.

[10] ZHAO M, ANZAI T, SHI F, et al. Versatile multilinked aerial robot with tilted propellers: Design, modeling, control, and state estimation for autonomous flight and manipulation[J]. Journal of Field Robotics, 2021, 38(7): 933-966.

[11] 杨超群, 张恒, 何立栋, 等. 基于随机有限集的信息物理系统状态估计[J]. 控制工程, 2022, 29(8): 1 424-1 428.
YANG C Q, ZHANG H, HE L D, et al. State estimation of cyber physical system based on random finite set[J]. Control Engineering of China, 2022, 29(8): 1 424-1 428.

[12] NA J, JING B, HUANG Y, et al. Unknown system dynamics estimator for motion control of nonlinear robotic systems[J]. IEEE Transactions on Industrial Electronics, 2019, 67(5): 3 850-3 859.

[13] LEE J G, KIM J, SHIM H. Fully distributed resilient state estimation based on distributed median solver [J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3 935-3 942.

[14] PESSIM P S P, PEIXOTO M L C, PALHARES R M, et al. Static output-feedback control for Cyber- physical LPV systems under DoS attacks [J]. Information Sciences: An International Journal, 2021, 563: 241-255.

[15] JAIN H, KUMAR M, JOSHI A M. Intelligent energy cyber physical systems (iECPS) for reliable smart grid against energy theft and false data in jection[J]. Electrical Engineering, 2022, 104: 331-346.

[16] BHARATH K P, KUMAR M R. New replay attack detection using iterative adaptive inverse filtering and high frequency band [J]. Expert Systems with Application, 2022, 195: 116597.

[17] ZHAO Z, HUANG Y, ZHEN Z, et al. Data-driven false data-injection attack design and detection in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2020, 51(12): 6 179-6 187.

[18] LUCIA W, GHEITASI K, GHADERI M. Set point attack detection in cyber-physical systems [J]. IEEE Transactions on Automatic Control, 2020, 66(5): 2 332-2 338.

[19] SAYAD HAGHIGHI M, FARIVAR F, JOLFAEI A, et al. Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack[J]. The Journal of Supercomputing, 2020, 76(4): 3 063-3 085.

[20] 刘一帆, 左稳, 张之津, 等. 传感器网络 DoS 攻击下随机系统的故障检测设计[J]. 哈尔滨工程大学学报, 2022, 43(3): 377-384.
LIU Y F, ZUO W, ZHANG Z J, et al. Fault detection design for uncertain systems over sensor network under DoS attacks [J]. Journal of Harbin Engineering University, 2022, 43(3): 377-384.

[21] GUO S, ZHU F, ZHU S, et al. State and sensor fault interval estimations for discrete- time systems[C]// 36th Chinese Control Conference (CCC). Dalian: IEEE, 2017: 7 280-7 284.

[22] GUO S, JIANG B, ZHU F, et al. Luenberger-like interval observer design for discrete-time descriptor linear system [J]. Systems & Control Letters, 2019, 126: 21-27.

[23] 张丹丹. 柔性关节机器人动力学建模及控制[D]. 南京: 南京理工大学, 2017: 12-22.
ZHANG D D. Dynamic modeling and control of flexible joint robot[D]. Nanjing: Nanjing University of Science and Technology, 2017: 12-22.

[24] BAGULA A, AJAYI O, MALULEKE H. Cyber physical systems dependability using cps-iot monitoring[J]. Sensors, 2021, 21(8): 2 761.

[25] CACCAVALE F, CILIBRIZZI P, PIEER F, et al. Actuators fault diagnosis for robot manipulators with uncertain model[J]. Control Engineering Practice, 2009, 17(1): 146-157.

[26] TEIXEIRA A, SHAMES I, SANDBERG H, et al. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51: 135-148.

[27] 孙子文, 张炎棋. 工业信息物理系统的攻击建模研究[J]. 控制与决策, 2019, 34(11): 2 323-2 329.
SUN Z W, ZHANG Y Q. Research on attack modeling of industrial cyber physical systems[J]. Control and Decision, 2019, 34(11): 2 323-2 329.

[28] DE SOUZA A R, EFIMOV D, RAISSI T, et al. Robust output feedback model predictive control for constrained linear systems via interval observers[J]. Automatica, 2022, 135: 109951.