控制与决策
Control and Decision

网络化运动控制系统的分布式攻击重构

朱俊威, 梁朝阳, 何德峰

引用本文:
朱俊威,梁朝阳,何德峰. 网络化运动控制系统的分布式攻击重构[J]. 控制与决策, 2022, 37(11): 2934–2940.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.0509

网络化运动控制系统的分布式攻击重构

朱俊威†, 梁朝阳, 何德峰

(浙江工业大学 信息工程学院，杭州 310023)

摘 要: 针对传感器网络下网络化运动控制系统的攻击重构问题,提出一种新的分布式投影中间估计器,以此估计传感器和执行器攻击信号. 首先,引入投影算子确定受攻击的信道集,同时设计最小二乘算法减轻观测器在估计过程中的计算负担;然后,引入分布式估计框架以提高算法的可伸缩性和扩展性;最后,通过网络化运动控制系统的实验验证所提出方法的有效性. 实验结果表明,所提出算法的估计精度和实时性分别优于现有的扩张状态观测器和梯度下降算法.

关键词: 网络化运动控制系统；攻击重构；中间观测器；传感器网络；分布式估计

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.0509 **开放科学(资源服务)标识码(OSID):**

引用格式: 朱俊威,梁朝阳,何德峰. 网络化运动控制系统的分布式攻击重构[J]. 控制与决策, 2022, 37(11): 2934-2940.

Distributed attack reconstruction for networked motion control systems

ZHU Jun-wei†, LIANG Chao-yang, HE De-feng

(College of Information Engineering，Zhejiang University of Technology，Hangzhou 310023，China)

Abstract: This paper studies the attack reconstruction problem for networked motion control systems under sensor networks. A new distributed projected intermediate estimator (DPIE) is proposed to estimate the actuator and sensor attacks. A projection operator is introduced to determine the set of attacked signal channels. Meanwhile, a least square algorithm is designed to alleviate the computational burden of the observers in the process of generating new estimates. In addition, a distributed estimation framework is introduced to improve the scalability and scalability of the proposed algorithm. It is shown that both the estimation accuracy and real-time performance of the proposed algorithm are better than those of the existing extended state observer and gradient descent algorithm respectively. Finally, the experimental results of the motion control system verify the effectiveness of the proposed methods.

Keywords: networked motion control system；attack reconstruction；intermediate estimator；sensor networks；distributed estimation

0 引 言

网络化运动控制系统由伺服电机、执行器、控制器和传感器组成[1],通过网络实现系统组件间的数据传输和数据交换,进而实现系统的闭环控制. 传感器网络由大量的传感器节点组成,这些节点可部署在网络化运动控制系统周围,用于数据采集、状态和参数估计[2]. 由于网络化运动控制系统通信网络的开放性,其传感器和执行器极易受到网络攻击[3],如虚假数据注入攻击和拒绝服务攻击等. 其中,虚假数据注入攻击[4]具有极强的隐蔽性,对系统的威胁较大. 作为一种重要技术,攻击重构技术可以从被破坏的传感器数据中获取攻击信号形状和幅度等明确信息,吸引了一些学者的关注和研究[5].

现有攻击重构方法大多采用集中式估计策略,可分为几类: 未知输入观测器[6]、扩张状态观测器(ESO)[7]、滑模观测器[8]、梯度下降算法[9]. Corradini等[8]提出了一种基于滑模观测器的攻击检测和重构方案. Ao等[10]研究了信息物理系统中攻击的自适应检测和重构问题,提出了一种具有在线参数估计的自适应滑模观测器. Zhu等[11]提出了一种新颖的中间观测器以重构执行器故障. Mishra等[12]研究了传感器的未知子集被攻击时,有噪声的线性系统的状态

收稿日期: 2021-03-28；**录用日期:** 2021-07-30.

基金项目: 国家自然科学基金项目(61803334)；浙江省自然科学基金项目(LZ21F030004)；浙江省高校基本科研业务费项目(RF-C2020003).

责任编委: 方华京.

†通讯作者. E-mail: junweizhu1001@zjut.edu.cn.

估计问题. Shoukry 等[9] 提出一种投影梯度下降算法, 解决了稀疏传感器攻击下的攻击重构问题. 此外, An 等[13] 和 Lu 等[14] 分别引入约束集划分方法和采用切换梯度下降技术, 在不牺牲估计精度的前提下, 降低了投影梯度下降算法的计算复杂度.

相较于集中式估计策略存在通信要求高、计算量大、灵活性和伸缩性有限等限制, 分布式估计策略具有更强的可扩展性和鲁棒性. 近年来, 基于传感器网络的分布式攻击重构问题取得了一些研究成果. Ju 等[15] 针对遭受传感器欺骗攻击的网联车辆, 提出了一种改进的广义似然比算法, 以检测欺骗攻击. Liu 等[16] 研究了传感器网络中具有传感器饱和和网络攻击的分布式事件触发 H_∞ 滤波问题, 通过事件触发策略减少网络带宽的占用. Song 等[17] 研究了传感器网络受到未知攻击的分布式估计问题, 给出了分布 H_∞ 观测器存在的充分条件. Guan 等[18] 针对遭受两种恶意攻击的信息物理系统, 提出了一种基于传感器网络的分布式攻击检测和安全估计算法. An 等[19] 提出一种基于一致性的分布式投影梯度下降算法, 解决了传感器攻击重构问题.

尽管现有分布式攻击重构方面的研究取得了一些成果, 但是依旧存在局限性. 在基于观测器的分布式攻击重构算法中, 滑模观测器[8] 需要系统满足观测器匹配条件; 鲁棒观测器[7,17] 不需要满足匹配条件, 但存在估计误差且误差上界未知; 中间观测器[6] 虽然给出了估计误差的理论上界, 但是上界往往较大. 另外, 这些算法严重依赖于 LMI 技术和假设攻击分布矩阵已知. 当攻击为高频信号时, 基于观测器的估计往往具有较差的暂态性能和较低的估计精度. 近年来, Shoukry 等[9] 提出了梯度下降算法以解决上述问题. 但是上述算法只考虑传感器攻击重构问题[19], 没考虑传感器和执行器同时遭受攻击的情况. 针对传感器网络下网络化运动控制系统的多攻击重构算法的设计更具实用性和挑战性, 但很少受到重视. 基于上述分析和启发[6,19], 本文研究网络化运动控制系统的分布式攻击重构问题, 主要内容为: 1) 提出一种分布式投影中间观测器 (DPIE), 首次考虑网络化运动控制系统遭受传感器攻击和执行器攻击, 模型更具有一般性; 2) 所提出算法的估计精度和实时性分别优于现有的 ESO[7] 和梯度下降算法[19]. 通过改进终端条件和最小二乘算法, 在不牺牲攻击重构性能的前提下, 解决算法的计算复杂度问题.

符号表示: I_n 为 n 维单位矩阵, 0_n 为 n 维零矩阵, $\lambda_{\max}(Q)$ 为矩阵 Q 的最大特征值, $\Phi[\cdot]$ 为状态转移矩阵, $\|x\|$ 为向量 x 的二范数. 已知具有相同维度的矩阵 $x \in R^p$ 和 $y \in R^q$, $(x, y) = [x^{\mathrm{T}} \quad y^{\mathrm{T}}]^{\mathrm{T}}$. 若 S 为一个集合, 则 $|S|$ 为 S 的基数. 对于向量 $x \in R^\tau$, $\mathrm{supp}(x)$ 为 x 的非零元素指标集. 若 x 最多有 s 个非零元素, 则向量 $x \in R^\tau$ 为 s 稀疏的. 若 q 个相同维度的向量 $x_1, x_2, \ldots, x_q \in R^\tau$, 则 $x = [x_1^{\mathrm{T}}, x_2^{\mathrm{T}}, \ldots, x_q^{\mathrm{T}}]^{\mathrm{T}} \in R^{q\tau}$ 称为块向量. 若块向量 $x \in R^{q\tau}$ 有 s 块非零向量, 则称 $x \in R^{q\tau}$ 为块 s 稀疏. $S_s^\tau \subset R^\tau$ 为所有块 s 稀疏向量的集合. $[q]$ 为集合 $\{1, 2, \ldots, q\}$, $\Lambda_s([q]) = \{\Gamma \subset [q] : ||\Gamma| \leqslant s\}$. 若 $\Gamma \in \Lambda_s([q])$, 则其补集 $\bar{\Gamma} \in [q] \backslash \Gamma$. $K_s^{q(n+(\tau-1)n_u+\tau)}$ 为所有 s 稀疏块向量 $\hat{z} = (\hat{z}_1, \hat{z}_2, \ldots, \hat{z}_q)$ 的集合, $\hat{z}_i = (\hat{x}_i, \hat{\zeta}_i, \hat{G}_i)$, $\hat{G} = [G_1^{\mathrm{T}}, G_2^{\mathrm{T}}, \ldots, G_p^{\mathrm{T}}]^{\mathrm{T}} \in S_s^{\tau q}$, $\mathrm{supp}(G) = \Gamma \in \Lambda_s([q])$. 若给定一个块矩阵 $C = [C_1^{\mathrm{T}}, C_2^{\mathrm{T}}, \ldots, C_q^{\mathrm{T}}]^{\mathrm{T}}$ 和一个集合 $\Gamma \in \Lambda_s([q])$, 则 $C_\Gamma \in R^{p_i|\mathrm{T}| \times n}$ 表示 C 删除了 Γ 索引外的所有的矩阵.

1　问题描述

1.1　网络化运动控制系统模型

考虑到网络传输中存在时延, 根据伺服系统的特性[20], 在速度模型下, 系统的传递函数为

$$G(s) = \frac{Y(s)}{U(s)} = \frac{b}{s^2 + as}. \tag{1}$$

其中: a、b 为模型参数, $U(s)$ 为系统速度设定值, $Y(s)$ 为系统的位置量. 令 $x(t) = (x_p(t), x_v(t))$, $x_p(t)$ 为位置 (mm), $x_v(t)$ 为速度 (mm / s), $u(t)$ 为控制输入 (r / min). 根据上述分析, 可以得到系统的状态空间模型为

$$\dot{x}(t) = A_a x(t) + B_a u(t). \tag{2}$$

其中: $A_a = \begin{bmatrix} 0 & 1 \\ 0 & -a \end{bmatrix}$, $B_a = \begin{bmatrix} 0 \\ b \end{bmatrix}$.

考虑噪声和网络攻击, 系统的离散状态空间模型可写为

$$\begin{aligned} &x(k+1) = Ax(k) + B(u(k) + a_u(k)) + w(k), \\ &y_i(k) = C_i x(k) + a_s^i(k) + v_i(k). \end{aligned} \tag{3}$$

其中: $x(k) \in R^{n_x}$、$u(k) \in R^{n_u}$ 和 $a_u(k) \in R^{n_u}$ 分别为系统的状态、速度控制信号和执行器攻击信号; $y_i(k) \in R^{p_i}$ 和 $a_s^i(k) \in R^{p_i}$ 分别为第 i 个传感器的测量输出和传感器攻击信号; $w(k)$ 和 $v_i(k) \in R^{p_i}$ 分别为有界且随机的过程噪声和输出噪声, $i \in [q]$; $A = \Phi[(k+1)T, kT]$, $B = \int_{kT}^{(k+1)\mathrm{T}} \Phi[(k+1)T, \tau] B_a(\tau) u(\tau) \mathrm{d}(\tau)$, T 为采样周期; $p = p_1 + \ldots + p_i + \ldots + p_q$ 为所有测量输出的数量; $C = [C_1^{\mathrm{T}}, C_2^{\mathrm{T}}, \ldots, C_q^{\mathrm{T}}]^{\mathrm{T}}$ 为系统的总输出矩阵.

为了构造投影中间观测器, 首先定义一个中间变

量,即

$$\xi(k)=a_u(k)-\omega B^{\mathrm{T}}x(k), \tag{4}$$

其中$\omega>0$为一个可调节的参数. 采集$k-\tau+1$到k时刻的$\tau\in N(\tau\leqslant n)$个测量信息,第$i$个传感器簇的输出向量可写为

$$\begin{aligned}&\tilde{Y}_i(k)=\\&O_ix(k-\tau+1)+F_i(U(k-1)+\zeta(k-1))+\\&M_iW(k-1)+G_i(k)+V_i(k).\end{aligned} \tag{5}$$

其中

$$\begin{aligned}&\tilde{Y}_i(k)=(y_i(k-\tau+1),\dots,y_i(k)),\\&V_i(k)=(v_i(k-\tau+1),\dots,v_i(k)),\\&G_i(t)=(a_s^i(k-\tau+1),\dots,a_s^i(k)),\\&\zeta(k-1)=(\xi(k-\tau+1),\dots,\xi(k-1)),\\&U(k-1)=(u(k-\tau+1),\dots,u(k-1)),\\&W(k-1)=(w(k-\tau+1),\dots,w(k-1)),\\&O_i=[C_i^{\mathrm{T}}\quad(C_i(A+wBB^{\mathrm{T}}))^{\mathrm{T}}\quad\dots\quad\to\\&\qquad\leftarrow(C_i(A+wBB^{\mathrm{T}})^{\tau-1})^{\mathrm{T}}]^{\mathrm{T}},\\&F_i=M_i\bar{B},\ M_i=\begin{bmatrix}0&0&\cdots&0\\C_i&0&\cdots&0\\\vdots&\vdots&&\vdots\\C_i\Lambda^{\tau-2}&C_i\Lambda^{\tau-3}&\cdots&C_i\end{bmatrix},\\&\bar{B}=\mathrm{diag}\{B,\dots,B\},\ \Lambda=A+\omega BB^{\mathrm{T}}.\end{aligned}$$

由于输入向量$U(k-1)$已知,式(5)可进一步简化为

$$Y_i(k)=Q_iz_i(k)+\psi_i(k). \tag{6}$$

其中:$Y_i(k)=\tilde{Y}_i(k)-F_iU(k-1)$,$Q_i=[O_i\quad F_i\quad I]$,$z_i(k)=(x(k-\tau+1),\zeta(k),G_i(k))$,$\psi_i(k)=M_iW(k-1)+V_i(k)$.

本文考虑了网络化运动控制系统同时遭受传感器和执行器攻击,模型更具有一般性. 在攻击重构问题中常见的传感器攻击模型是s稀疏攻击模型. 攻击者可在任意时刻任意访问传感器和执行器的传输通道,其中传感器攻击子集是未知的. 若第i个传感器簇被攻击,则相应的传感器攻击向量$a_s^i(k)\in R^{p_i}$是非0的. 另一方面,许多基于观测器的攻击重构方法均假设被攻击的传感器和执行器的集合是已知的.

1.2 问题描述

传感器网络如图1所示,4个传感器分布于物理层的不同区域,所有估计节点分布在网络层,每个估计节点利用局部感知测量,通过传感器网络相互交换估计值,重构攻击信号. 图1中的箭头为传感器估计节点传递信息的方向. 进一步,定义$Y(k)=Qz(k)+\psi(k)$,$Y(k)=[Y_1^{\mathrm{T}}(k)\quad\dots\quad Y_q^{\mathrm{T}}(k)]^{\mathrm{T}}$,$Q=\mathrm{diag}\{Q_1\dots Q_q\}$,$\psi(k)=[\psi_1^{\mathrm{T}}(k)\quad\dots\quad\psi_q^{\mathrm{T}}(k)]^{\mathrm{T}}$,$z(k)=(z_1(k),z_2(k),\dots,z_q(k))$,$v(k)=(v_1(k),v_2(k),\dots,v_q(k))$,$p_i=1$,$i\in[q]$.

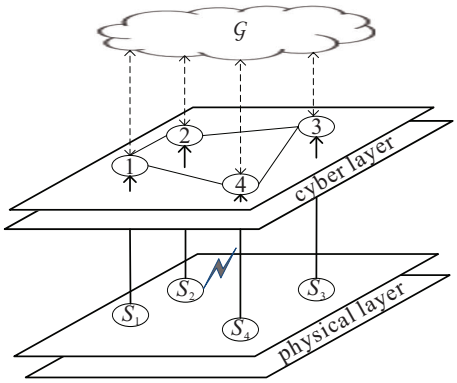

图1 分布式传感器网络

定义1 [9](联合$2s$稀疏能观性) 对于任意集合$\Gamma\in\Lambda_{2s}([q])$,$(A,C_{\bar{\Gamma}})$是能观的,则线性系统(3)可被认为是联合$2s$稀疏能观.

问题1 若系统(3)是联合$2s$稀疏能观,传感器网络拓扑是无向且连通,则可构造观测器$\hat{z}_i=(\hat{x}_i,\hat{\zeta}_i,\hat{G}_i)$,$\hat{x}_i$、$\hat{\zeta}_i$、$\hat{G}_i$分别为第$i$个传感器节点的系统状态、中间变量、传感器攻击的估计值,使得下式成立:

$$\begin{aligned}&\frac{1}{2}\sum_{i=1}^{q}\|Q_i\hat{z}_i-Y_i\|^2\leqslant\rho(\bar{w},\bar{v});\\&\text{s.t. }\mathcal{L}\hat{z}=0.\end{aligned} \tag{7}$$

其中:$\mathcal{L}=L\otimes\mathcal{I}_s$,$L\in R^{q\times q}$为传感器网络$\mathcal{G}$的拉普拉斯矩阵,$\mathcal{I}_s=\mathrm{diag}(I_{n_x},I_{(\tau-1)n_u},0_\tau)$;$\rho(\bar{w},\bar{v})$为一个有界函数,$\max\|w(k)\|\leqslant\bar{w}$,$\max\|v(k)\|\leqslant\bar{v}$,$\rho(0,0)=0$. 全局估计$\hat{z}=[\hat{z}_1^{\mathrm{T}}\dots\hat{z}_q^{\mathrm{T}}]^{\mathrm{T}}\in K_s^{q(n+(\tau-1)n_u+\tau)}$为一个非凸可行解. 由于每个时刻都要求解问题(7),时间参数k可以在书写中省略.

在无噪声的情况下,问题1等价于如下分布式估计问题[19]:

$$\begin{aligned}&\arg\min_{\hat{z}\in K_s^{q(n_x+(\tau-1)n_u+\tau)}}\frac{1}{2}\sum_{i=1}^{q}\|Q_i\hat{z}_i-Y_i\|^2;\\&\text{s.t. }\mathcal{L}\hat{z}=0.\end{aligned} \tag{8}$$

其中$\mathcal{L}\hat{z}=0$等价于$(\hat{z}_1,\hat{\zeta}_1)=\dots=(\hat{z}_q,\hat{\zeta}_q)$,这意味着每个传感器节点的局部估计会达到一致性.

联合能观性是分布式估计中一个重要的定义[21],即(A,C_i)不一定能观,(A,C)能观. 同时,$2s$稀疏能观是保证攻击重构问题有唯一解的充分条件[9]. 本文没有假设局部$2s$稀疏能观,即任何传感器估计节点均不能根据其局部测量值估计攻击信

号. 联合$2s$稀疏能观性是一个必要的定义,它意味着传感器网络作为一个整体估计攻击信号.

2　分布式攻击重构算法

本节给出DPIE的实施过程和收敛性证明.

2.1　DPIE

在讨论所提出算法如何实施前,需要引入投影算符子Π的概念.

定义 2[19](投影算子)　给定块向量$z \in R^{q(n_x+(\tau-1)n_u+\tau)}$,$\Pi(z)$表示集合$K_s^{q(n+(\tau-1)n_u+\tau)}$中在2范数意义上最接近$z$的元素,有

$$\Pi(z)=\arg\min_{z'\in K_s^{q(n_x+(\tau-1)n_u+\tau)}\bigcap J(z)}\|z'-z\|^2. \quad (9)$$

其中: $J(z)=\{z'\in R^{q(n_x+(\tau-1)n_u+\tau)}: I(z'-z)=0\}$, $I=I_q\otimes\mathcal{I}_s$,即对于任意$z'\in K_s^{q(n_x+(\tau-1)n_u+\tau)}\bigcap J(z)$, $\|\Pi(z)-z\|\leqslant\|z'-z\|$. $\Pi(z)$具体计算步骤为: 在$\hat{G}=[G_1^{\mathrm{T}},G_2^{\mathrm{T}},\ldots,G_q^{\mathrm{T}}]^{\mathrm{T}}$中,求取$G_i(i\in[q])$中元素的平方和,将平方和较小的$q-s(s<q)$个$G_i(i\in[q])$置0,确保传感器攻击估计的$s$稀疏性. 令$\Pi(\hat{z})=\hat{z}_\Pi=(\Pi_1(\hat{z}_1),\Pi_2(\hat{z}_2),\ldots,\Pi_q(\hat{z}_q))=(\hat{z}_{\Pi_1},\hat{z}_{\Pi_2},\ldots,\hat{z}_{\Pi_q})$.

定理 1　对于任意集合$\Gamma\in\Lambda_{2s}([p])$和$z\in K_{2s}^{q(n_x+(\tau-1)n_u+\tau)}$,若其是$2s$稀疏块向量,则存在一个常数$\delta_{2s}>0$,使得下式恒成立:

$$z^{\mathrm{T}}(Q^{\mathrm{T}}Q+v^2\mathcal{L}^2)z\geqslant\delta_{2s}^2z^{\mathrm{T}}z. \quad (10)$$

证明　假设存在一个$2s$稀疏块向量$z\in K_{2s}^{q(n_x+(\tau-1)n_u+\tau)}$使得$z^{\mathrm{T}}(Q^{\mathrm{T}}Q+v^2\mathcal{L}^2)z=0$. 由于$Q^{\mathrm{T}}Q$和$\mathcal{L}$为半正定矩阵,可得$z^{\mathrm{T}}Q^{\mathrm{T}}Qz=0,\mathcal{L}z=0$, 其中$\mathcal{L}z=0$等价于$(x_1,\zeta_1)=\ldots=(x_q,\zeta_q)=(x,\zeta)$,进而可知

$$\|Qz\|^2=\left\|\begin{matrix}O_1x_1+F_1\zeta_1+G_1\\ \vdots\\ O_qx_q+F_q\zeta_q+G_q\end{matrix}\right\|=\|\bar{Q}\tilde{z}\|=0. \quad (11)$$

其中: $\bar{Q}=[[O_1^{\mathrm{T}},O_2^{\mathrm{T}},\ldots,O_q^{\mathrm{T}}]^{\mathrm{T}}\ \ [F_1^{\mathrm{T}},F_2^{\mathrm{T}},\ldots,F_q^{\mathrm{T}}]^{\mathrm{T}}\ \ II]$, $II=\mathrm{diag}\{I_\tau,\ldots,I_\tau\},\tilde{z}=(x,\zeta,G_1,\ldots,G_q)$. 由文献[9]命题3.4,对于任意向量$\tilde{z}$,由于系统是$2s$稀疏能观,存在一个正定常数$\bar{\delta}_{2s}$,使得$\|Qz\|^2=\|\bar{Q}\tilde{z}\|^2>\bar{\delta}_{2s}\tilde{z}^{\mathrm{T}}\tilde{z}>0$,这与假设相矛盾. □

定理1表明,$Q^{\mathrm{T}}Q+v^2\mathcal{L}\mathcal{L}$具有非零的$2s$限制性特征值[22]且不小于$\delta_{2s}$. 分布式投影迭代算法通过遵循最小化李亚普诺夫能量函数$V_i(\hat{z}_i)=\|Y_i-Q\hat{z}_i\|+\hat{z}_i^{\mathrm{T}}\sum_{j\in N_i}\mathcal{I}_s(\hat{z}_i-\hat{z}_j)$的原则更新估计值$\hat{z}_i^{(n,m+1)}$. 局部的中间观测器的更新步骤为

$$\hat{z}_i^{(n,m+1)}=\hat{z}_i^{(n,m)}+Q_i^+(Y_i-Q_i\hat{z}_i^{(n,m)})-v\sum_{j\in\mathcal{N}_i}\mathcal{I}_s(\hat{z}_i^{(n,m)}-\hat{z}_j^{(n,m)}). \quad (12)$$

其中: $v>0$为耦合增益,$\mathcal{N}_i$为第i传感器节点的邻域. 全局的中间观测器可写为

$$\hat{z}^{(n,m+1)}=\hat{z}^{(n,m)}+Q^+(Y-Q\hat{z}^{(n,m)})-v\mathcal{L}\hat{z}^{(n,m)}, \quad (13)$$

其中Q^+为Q的穆尔-彭罗斯广义逆矩阵[23].

本文每个局部估计节点仅利用自身的局部测量信息和邻域的估计信息. 相比之下,现有的基于观测器的分布式估计算法均假设传感器网络的拉普拉斯矩阵是已知的,且观测器的增益需要通过求解一组LMI矩阵获得,这使得LMI矩阵可能存在无解的情况. 然而,DPIE无需知道拉普拉斯矩阵和求解LMI矩阵,克服了这种局限性. DPIE的具体实施步骤如下.

step 1: 初始化. $m:=0,n:=1,\hat{z}_{\Pi_i}^{(0)}=0$;
step 2: while $n<\alpha$ do
step 3: $\hat{z}_i^{(n,0)}:=\hat{z}_{\Pi_i}^{(n-1)}$;
step 4: 令$m:=0,V_{\mathrm{temp}}^i:=V_i(\hat{z}_{\Pi_i}^{(n-1)})$;
step 5: while $V_{\mathrm{temp}}^i\geqslant(1-\beta)V_i(\hat{z}_{\Pi_i}^{(n-1)})$ do
step 6: $\hat{z}_i^{(n,m+1)}=\hat{z}_i^{(n,m)}+Q_i^+(Y_i-Q_i\hat{z}_i^{(n,m)})-v\sum_{j\in N_i}\mathcal{I}_s(\hat{z}_i^{(n,m)}-\hat{z}_j^{(n,m)})$;
step 7: $V_{\mathrm{temp}}^i:=V_i(\Pi_i(\hat{z}_i^{(n,m+1)}))$;
step 8: $m:=m+1$;
step 9: endwhile
step 10: $\hat{z}_{\Pi_i}^{(n)}=\Pi_i(\hat{z}_i^{(n,m)})$;
step 11: $n:=n+1$;
step 12: endwhile
step 13: 返回$\hat{z}_{\Pi_i}^{(n-1)}$.

2.2　收敛性证明

定理2　若系统(3)具有联合$2s$稀疏能观性且传感器网络拓扑$\mathcal{G}$为无向连通,DPIE算法的内循环迭代次数不大于

$$\frac{\log(1/2)}{\log(\|I-Q^+Q-v\mathcal{L}\|)} \quad (14)$$

时,则DPIE的估计满足$\|z^*-\hat{z}\|\leqslant\beta/\alpha$. α和β在后文中给出.

证明　为了更容易证明算法的收敛性,选择李亚普诺夫能量函数为

$$W(\hat{z})=\|z^*-\hat{z}\|=\|e\|. \quad (15)$$

其中: z^*为全局状态z的真实值,$\hat{z}$为全局状态z的估计值. 当$z^*=\hat{z}$时,$W(\hat{z})$具有唯一的最小值. 对于任意$\hat{z}\in K_s^{q(n+(\tau-1)n_u+\tau)}$,有如下不等式成立:

$$Wo\Pi(\hat{z})=\|z^*-\Pi(\hat{z})\|\overset{(a)}{\leqslant}\|z^*-\hat{z}\|+\|\Pi(\hat{z})-\hat{z}\|\overset{(b)}{\leqslant}2\|z^*-\hat{z}\|=2W(\hat{z}). \quad (16)$$

根据三角形不等式和定义2分别得到式(16)的第1个不等子式(a)和第2个不等子式(b). 由式(13)和(16),得到

$$W(\hat{z}_{\Pi}^{(n)}) \leqslant (2\|(I-Q^{+}Q-v\mathcal{L})\|)^{m}W(\hat{z}^{(n,m-1)})+ 2\|Q^{+}\psi\|. \tag{17}$$

由式(17)和泰勒公式,进一步可知

$$W(\hat{z}_{\Pi}^{(n)}) \leqslant (2\|(I-Q^{+}Q-v\mathcal{L})\|)^{m}W(\hat{z}_{\Pi}^{(n-1)})+ \frac{2\|Q^{+}\psi\|}{1-\|(I-Q^{+}Q-v\mathcal{L})\|}. \tag{18}$$

根据李亚普诺夫的稳定性理论,为了保证估计误差的收敛性,内循环终止条件应满足

$$2(\|(I-Q^{+}Q-v\mathcal{L})\|)^{m}<1. \tag{19}$$

根据穆尔-彭罗斯广义逆矩阵的性质,得到

$$I-Q^{+}Q-v\mathcal{L} \leqslant (1-\delta_{2s}\lambda_{\max}^{-1}(Q^{\mathrm{T}}Q+v^{2}\mathcal{L}^{2}))I. \tag{20}$$

通过定理1,进一步得到$0<\|I-Q^{+}Q-v\mathcal{L}\|<1$. 另外,由于过程噪声和输出噪声均为有界函数,总存在一个标量$\varpi_b=\max\|Q^{+}\psi\|$.

根据上述分析,可得出如下结论:当内循环的次数不大于

$$\frac{\log(1/2)}{\log(\|(I-Q^{+}Q-v\mathcal{L})\|)} \tag{21}$$

时,存在参数α、β使得

$$W(\hat{z}_{\Pi}^{(n)}) \leqslant (1-\alpha)W(\hat{z}_{\Pi}^{(n-1)})+\beta, \tag{22}$$

其中α和β满足

$$0<\alpha<1-2(\|(I-Q^{+}Q-v\mathcal{L})\|)^{m},$$
$$\beta=\frac{2\varpi_b}{1-\|(I-Q^{+}Q-vL)\|}. \tag{23}$$

为了证明李雅普诺夫能量函数的有界性,定义一个估计误差$e(n-1)=z^{*}-\hat{z}_{\Pi}$和一个集合$\Omega$,有

$$\Omega=\left\{e(n-1)|W(\hat{z}_{\Pi}^{(n-1)})\leqslant\frac{\beta}{\alpha}\right\}. \tag{24}$$

令Ω_s为集合Ω的补集,若估计误差$e(n-1)\in\Omega_s$,则由式(22),有

$$\Delta W(\hat{z}(n-1))=W(\hat{z}_{\Pi}^{(n)})-W(\hat{z}_{\Pi}^{(n-1)})<0. \tag{25}$$

根据李亚普诺夫的稳定性理论,可得出如下结论:当$e(n-1)\in\Omega_s$时,估计误差$e(n-1)$会指数收敛于集合Ω,即李雅普诺夫能量函数小于等于β/α. □

对于遭受传感器和执行器攻击的网络化运动控制系统,现有的集中式梯度下降算法不能直接扩展到分布式算法以重构多攻击信号,这是梯度下降算法存在一些本质的缺陷造成的. 如$2s$限制特征根δ_{2s}要大于$(4/9)\lambda_{\max}(Q^{\mathrm{T}}Q)$,梯度下降的步长满足$0<\eta<\lambda_{\max}^{-1}(Q^{\mathrm{T}}Q)$. 另外,现有的梯度下降算法只考虑传感器攻击. 这是因为在多重攻击的情况下,梯度下降算法[9,19]需要更多迭代达到预期的估计精度. 本文采用中间观测器的思想,通过引入中间变量作为设计参数,从而实现了对传感器和执行器攻击信号的重构. 另外,本文通过改进终止条件和最小二乘,提高了算法的估计精度,同时降低了所提出算法的计算复杂度,为网络化运动控制系统的多攻击重构提供了新的解决方案.

DPIE的具体实施步骤中,step 6是一种改进的最小二乘解,用于减少算法1的计算时间. step 7(投影算子)可确定被攻击的传感器集合,提高了DPIE的估计精度. 在外循环的设计中,采用计数阈值α作为外循环的终止条件,而不是$V<\alpha$[9],可减少冗余迭代次数并防止算法陷入死循环,进而提高算法1的计算效率. 另外,DPIE算法的参数设置可以总结如下:当DPIE算法陷入无限循环或执行时间较长时,重新选择ω或减小α和β.

3 实验结果

本文使用的网络化运动控制系统如图2所示. 该系统主要由主机、电机(台达ECMA-C 10604 RS)、交流伺服系统(台达ASDA-A2系列伺服驱动器)、ARM处理器(STM 32 F 407 ZGT 6)以及CAN总线组成. 在电机运行过程中,按照设定的采样频率,交流伺服系统通过编码器获取电机的速度、位置等状态信息,并且通过CAN总线将信息传输至ARM处理器. ARM处理器将接收到的数据进行封装,通过以太网将数据包发送给主机. 然后,主机将接收到的数据包进行解析和处理,根据算法计算出控制量并且通过以太网将控制信号发至ARM处理器. 最后ARM处理器将其转发给交流伺服系统. 为了模拟系统遭受的网络攻击场景,对主机接收到的数据包和下发的控制指令进行人为篡改,以达到运动控制系统同时遭受传感器和执行器攻击的效果.

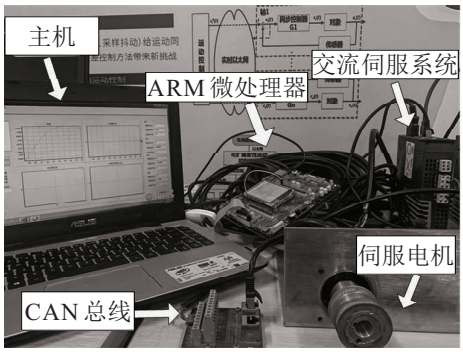

图2 网络化运动控制系统

电机的伺服系统的模型参数经过辨识后[20], $a=-41.101\,5, b=3.441\,4$. 采样周期设定为$T=0.1$ s, 系统的输出矩阵为

$$C_1=C_2=C_3=[1\quad 0],\ C_4=[0\quad 1],$$
$$A=\begin{bmatrix}1 & 0.023\,9\\ 0 & 0.016\,4\end{bmatrix},\ B=\begin{bmatrix}0.006\,4\\ 0.824\end{bmatrix}. \tag{26}$$

本文选择将局部估计的平均值作为最终估计值, 这种做法在工程中是常见的, 即$\hat{x}=(\hat{x}_1+\hat{x}_2+\ldots+\hat{x}_q)/q$. 另外, 对于系统受到攻击信号的估计也是如此. 传感器攻击和执行器攻击的设计如表1所示.

表 1　攻击信号

攻击	时间k
传感器攻击a_s^2	$3\sin(0.05k)$
执行器攻击a_u	$5\sin(0.05k)$

通过与分布式投影最小切换次梯度下降算法[19] (DPMSD)、ESO[7]进行对比研究, 验证了DPIE的优越性. 为了与DPMSD进行比较, 基于中间观测器的框架, 将DPMSD推广到可同时估计传感器和执行器攻击. 另外, 为了分析算法的估计准确性, 采用均方根误差进行定量分析, 即

$$\mathrm{RMSE}(x,\hat{x})=\sqrt{\frac{1}{N}\sum_{k=1}^{N}(x(k)-\hat{x}(k))^2}.$$

传感器攻击和DPIE、ESO、DPMSD的估计如图3所示. 由图3可见, DPIE、ESO和DPMSD对传感器攻击的估计效果均令人接受. 执行器攻击和DPIE、ESO、DPMSD的估计如图4所示. 由图4可见, DPIE对执行器攻击的估计精度明显优于ESO和DPMSD. 攻击信号如表2所示. 结合表2可知, DPIE对传感器和执行器攻击估计的均方根误差分别为0.003和0.639. 相较于ESO、DPIE分别减少了0.182和0.57. 相较于DPMSD、DPIE分别减少了0.065和0.12. 综上所述, DPIE的估计精度优于现有的ESO和DPMSD.

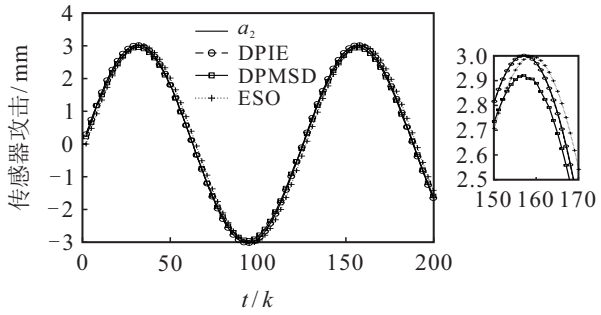

图 3　传感器攻击和DPIE、ESO、DPMSD的估计

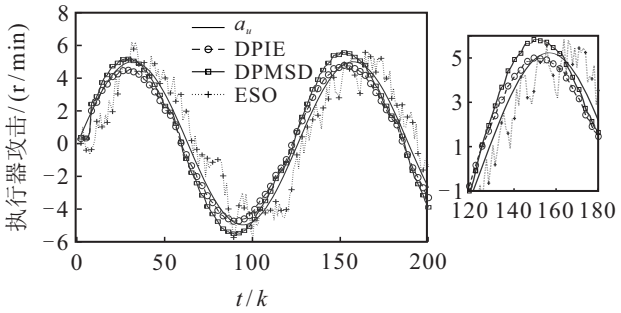

图 4　执行器攻击和DPIE、ESO、DPMSD的估计

表 2　攻击信号

估计方法	估计误差(RMSE)	
	传感器攻击a_2	执行器攻击a_u
DPIE	0.003	0.639
DPMSD	0.068	0.759
ESO	0.185	1.209

表3为迭代次数和估计时间的比较. 由表3可见, DPIE的平均迭代次数和估计时间分别为3 997和0.019 4 s, 而DPMSD的平均迭代次数和估计时间分别为14 671和0.069 5 s. 其中, DPMSD的平均估计时间远超于DPIE估计时间和系统的采样时间. 这是因为DPMSD需要更多的迭代次数以得到可接受的估计性能, 而DPIE采用改进的最小二乘解有效地降低了算法的计算复杂度. 因此, DPIE的实时性可得到满足. 综上所述, DPIE的实时性和估计性能均优于DPMSD.

表 3　迭代次数和估计时间比较

	DPIE	DPMSD
平均迭代次数	3 997	14 671
最大迭代次数	5 426	373 998
平均估计时间/s	0.019 4	0.069 5
最大估计时间/s	0.033 7	2.282 7

4　结　论

本文研究了传感器网络下运动控制系统的多攻击重构问题, 提出了DPIE算法用于估计传感器和执行器攻击信号. 为了保证算法的可行性, 在不牺牲估计精度的前提下, 引入投影算子和改进的最小二乘算法降低算法的计算复杂度. 实验结果表明, 所提出算法的估计性能优于现有的ESO和梯度下降算法. 未来的研究方向将是网络化多轴运动控制系统的分布式事件触发容侵控制.

参考文献(References)

[1] 顾曹源, 朱俊威, 张文安, 等. 网络化多轴运动控制系统的容侵同步控制[J]. 控制与决策, 2019, 34(11): 2289-2296.
(Gu C Y, Zhu J W, Zhang W A, et al. Intrusion-tolerant synchronous control for networked multi-axis motion control system[J]. Control and Decision, 2019, 34(11): 2289-2296.)

[2] 张玲玲, 张亚. 传感器网络分布式事件触发多目标估

计[J]. 控制理论与应用, 2020, 37(5): 1135-1144.
(Zhang L L, Zhang Y. Distributed event-triggered multi-target filtering in sensor networks[J]. Control Theory & Applications, 2020, 37(5): 1135-1144.)

[3] Lu A Y, Yang G H. Secure state estimation for multiagent systems with faulty and malicious agents[J]. IEEE Transactions on Automatic Control, 2020, 65(8): 3471-3485.

[4] Pang Z H, Liu G P, Zhou D H, et al. Two-channel false data injection attacks against output tracking control of networked systems[J]. IEEE Transactions on Industrial Electronics, 2016, 63(5): 3242-3251.

[5] Zhu J W, Wang Q, Zhang W A, et al. Sensor attack reconstruction for mobile robots via a switching Kalman fusion mechanism[J]. Nonlinear Dynamics, 2020, 102(1): 151-161.

[6] Zhu J W, Gu C Y, Ding S X, et al. A new observer-based cooperative fault-tolerant tracking control method with application to networked multiaxis motion control system[J]. IEEE Transactions on Industrial Electronics, 2021, 68(8): 7422-7432.

[7] Zhang K, Jiang B, Shi P. Observer-based integrated robust fault estimation and accommodation design for discrete-time systems[J]. International Journal of Control, 2010, 83(6): 1167-1181.

[8] Corradini M L, Cristofaro A. Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes[J]. IET Control Theory & Applications, 2017, 11(11): 1756-1766.

[9] Shoukry Y, Tabuada P. Event-triggered state observers for sparse sensor noise/attacks[J]. IEEE Transactions on Automatic Control, 2016, 61(8): 2079-2091.

[10] Ao W, Song Y D, Wen C Y. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.

[11] Zhu J W, Wu J, Yu F, et al. Performance-guaranteed fault reconstruction for mobile robots via a two-dimensional gain-regulation mechanism[J]. IEEE/ASME Transactions on Mechatronics, 2022, 27(1): 169-179.

[12] Mishra S, Shoukry Y, Karamchandani N, et al. Secure state estimation against sensor attacks in the presence of noise[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 49-59.

[13] An L W, Yang G H. State estimation under sparse sensor attacks: A constrained set partitioning approach[J]. IEEE Transactions on Automatic Control, 2019, 64(9): 3861-3868.

[14] Lu A Y, Yang G H. Switched projected gradient descent algorithms for secure state estimation under sparse sensor attacks[J]. Automatica, 2019, 103: 503-514.

[15] Ju Z Y, Zhang H, Tan Y. Distributed deception attack detection in platoon-based connected vehicle systems[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 4609-4620.

[16] Liu J L, Gu Y Y, Cao J, et al. Distributed event-triggered H_∞ filtering over sensor networks with sensor saturations and cyber-attacks[J]. ISA Transactions, 2018, 81: 63-75.

[17] Song H Y, Shi P, Zhang W A, et al. Distributed H_∞ estimation in sensor networks with two-channel stochastic attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(2): 465-475.

[18] Guan Y P, Ge X H. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4(1): 48-59.

[19] An L W, Yang G H. Distributed secure state estimation for cyber-physical systems under sensor attacks[J]. Automatica, 2019, 107: 526-538.

[20] 吴麒, 王瑶为, 张文安, 等. 基于综合学习策略粒子群优化算法的永磁同步电机模型辨识[J]. 机械设计与制造工程, 2017, 46(11): 78-82.
(Wu Q, Wang Y W, Zhang W A, et al. Model identification of PMSM based on the comprehensive learning particle swarm optimization[J]. Machine Design and Manufacturing Engineering, 2017, 46(11): 78-82.)

[21] Millán P, Orihuela L, Vivas C, et al. Sensor-network-based robust distributed control and estimation[J]. Control Engineering Practice, 2013, 21(9): 1238-1249.

[22] Raskutti G, Wainwright M J, Yu B. Restricted eigenvalue properties for correlated Gaussian designs[J]. Journal of Machine Learning Research, 2010, 11: 2241-2259.

[23] Ben-Israel A, Greville T N E. Generalized inverses: theory and applications[M]. New York: Springer Science & Business Media, 2003: 1-415.

作者简介

朱俊威(1985−), 男, 副教授, 博士, 从事信息物理系统安全等研究, E-mail: junweizhu1001@zjut.edu.cn;

梁朝阳(1994−), 男, 硕士生, 从事信息物理系统安全的研究, E-mail: Liangchaoyang0812@gmail.com;

何德峰(1979−), 男, 教授, 博士生导师, 从事智能系统预测控制理论与应用等研究, E-mail: hdfzj@zjut.edu.cn.

(责任编辑：魏 冰)