控制与决策
Control and Decision

基于分布式融合的FDI攻击信号快速检测方法

沈家辉, 翁品迪, 陈博, 俞立

引用本文:
沈家辉,翁品迪,陈博,俞立. 基于分布式融合的FDI攻击信号快速检测方法[J]. 控制与决策, 2022, 37(12): 3259−3266.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.0213

基于分布式融合的FDI攻击信号快速检测方法

沈家辉, 翁品迪, 陈 博†, 俞 立

(1. 浙江工业大学 信息工程学院，杭州 310023；2. 浙江工业大学 网络空间安全研究院，杭州 310023)

摘 要: 研究带宽受限下信息物理系统中虚假数据注入(false data injection, FDI)攻击的检测问题. 首先,将执行器遭受的FDI攻击信号建模为系统的未知输入信号, 基于给定的H_∞性能指标, 设计局部残差产生器以实时逼近攻击信号. 其次, 为提高检测系统预警速度, 在分布式融合框架下将所有经对数量化后的残差信号发送至检测中心, 并设计优化目标将分布式加权融合准则的求解问题转化为线性矩阵不等式形式下的凸优化问题. 与单个传感器情况下的检测方法相比, 基于分布式融合方法所确定的检测阈值更加精准, 从而可大幅度提高对攻击信号的预警速度. 最后, 通过移动目标系统的仿真验证所提方法的有效性.

关键词: 信息物理系统；FDI攻击检测；量化；凸优化；信息融合

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.0213 **开放科学(资源服务)标识码(OSID):**

引用格式: 沈家辉, 翁品迪, 陈博, 等. 基于分布式融合的FDI攻击信号快速检测方法[J]. 控制与决策, 2022, 37(12): 3259-3266.

A fast detection method of FDI attack signal based on distributed fusion

SHEN Jia-hui, WENG Pin-di, CHEN Bo†, YU Li

(1. College of Information Science and Engineering，Zhejiang University of Technology，Hangzhou 310023，China；
2. Institute of Cyberspace Security，Zhejiang University of Technology，Hangzhou 310023，China)

Abstract: This paper studies the alarm response of false data injection attack in cyber-physical system under limited bandwidth constraints. Firstly, the false data injected in the actuator is modeled as unknown inputs, and the local residual generators are designed by the given H_∞ performance index to generate the residual signals approaching the attack signal. Subsequently, in order to improve the alarm response, all the residual signals are quantized and then sent to the detection center under the distributed fusion framework, the optimization objective is designed and then the distributed fusion criterion are derived by solving a convex optimization problem in terms of linear matrix inequalities. Comparing with the detection method by single sensor, the detection threshold based on the distributed fusion method is more accurate, thus the alarm response is more effective and the detection time is sharply reduced. Finally, an illustrative example is used to show the effectiveness of the proposed algorithm.

Keywords: cyber-physical systems；FDI attack detection；quantization；convex optimization；information fusion

0 引 言

信息物理系统(cyber-physical systems, CPSs)集感知、计算、通信、控制等技术于一体,通过计算进程和物理进程相互影响的反馈循环实现资源配置的全局协同优化,实时可靠地监测或控制物理实体[1-2]. 不同于传统封闭的工业控制系统, CPSs通过通信网络使用大规模的、分散的传感器和执行器来感知和控制对象. 网络的开放性给保障系统的安全可靠带来了新的挑战. 特别地,来自网络攻击的安全威胁会导致系统的失效甚至瘫痪, 例如: 2010年, 震网病毒导致了伊朗核电站近1 000台离心机在铀浓缩中被销毁[3]; 2015年, “BlackEnergy”木马病毒导致了乌克兰当地遭遇近3小时的断电[4]. 可见在一些关键基础设施上, CPSs存在着潜在的安全隐患. 当攻击发生时, 及时检测攻击的发生并采取应对措施能够将攻击目的遏止于摇篮之中[5]. 在这种情况下, 提高预警速度对保障系统的安全运行至关重要.

面对攻击者对系统的广泛渗透, CPSs在网络攻击面前尤为脆弱[6]. 在各类网络攻击中, 虚假数据注入(false data injection, FDI)攻击通过向系统注入错误数据, 影响系统的稳定性, 是最具威胁的攻击方式之一[7]. FDI攻击作为一类特殊的系统故障, 就残差

收稿日期: 2021-02-01；**录用日期:** 2021-08-09.
基金项目: 国家自然科学基金项目(61973277, 62073292)；浙江省自然科学基金项目(LR20F030004).
†通讯作者. E-mail: bchen@zjut.edu.cn.

生成而言,其目的在于产生反应系统实际行为与期望行为差异的残差信号,因此增强残差信号对外界扰动的鲁棒性及对攻击信号的敏感性是进行FDI攻击检测的关键[8-13]. 其中: Zhou等[8]基于中间观测器实现攻击信号估计; He等[9]基于Lyapunov函数法及LMI设计了鲁棒H_∞滤波器; 钟麦英等[10]运用等价空间方法获得了最优滤波器存在的充要条件; 李岳炀等[11]基于求解Riccati方程的二次型问题获得了最优滤波器参数的显式解. 针对残差信号的故障敏感性, Zhong等[12]给出了H_∞/H_∞或H_-/H_∞指标下的最优解,并于文献[13]中进一步将上述方法拓展至非线性系统. 注意上述文献均未考虑通讯带宽受限的影响,研究带宽受限下的攻击检测问题具有重要意义.

受通讯带宽承受能力的限制,数据量化已成为网络技术发展中不可忽视的问题. 在连续信号经量化映射为有限集的数据后, Fu等[14]采用扇形界方法描述对数量化器,并将量化反馈控制器设计问题转化为鲁棒控制问题; Li等[15]设计中间控制率解决存在输入量化下和执行器故障下的自适应跟踪问题; Chen等[16]通过求解离散界实定理下的凸优化问题获得分布式H_∞滤波器,并于文献[17]中提出了降低通讯成本的数据压缩策略; Hu等[18]研究了具有不确定内部耦合的复杂网络状态估计问题. 针对故障诊断问题, Aliva等[19]设计了测量数据均匀量化下的H_∞故障检测器; Gao等[20]针对残差信号送至融合中心时的量化现象,结合多传感信息融合技术提升了系统的预警速度,然而融合准则的求解局限于线性时不变系统.

与此同时,考虑到分布式融合技术具有易实现、高容错等优点,本文将研究通讯网络带宽受限下基于分布式融合的CPSs攻击检测问题. 本文贡献概括如下: 1) 基于文献[11]故障检测滤波器的设计方法,设计能够逼近执行器端FDI攻击信号的残差信号; 2) 考虑对数量化下的残差信号,将其分布式融合准则的求解转化为一个凸优化问题,进而采用LMI方法设计融合权重,提升残差信号的H_∞性能; 3) 利用分布式融合准则获得更加准确的检测阈值,相比单传感器下的检测方案,融合检测能够大幅度提升系统的预警速度.

1 问题描述

考虑如下线性时变系统:

$$x(k+1)=A(k)x(k)+B(k)u(k)+E(k)\omega(k). \quad (1)$$

其中: $x(k)\in \boldsymbol{R}^n$表示系统状态向量, $u(k)\in \boldsymbol{R}^z$表示系统控制输入, $w(k)\in l_2[0,m]$表示系统遭受到的能量有界噪声, $A(k)$、$B(k)$、$E(k)$表示适当维数的时变矩阵. 当执行器遭受FDI攻击时,实际控制信号为

$$\tilde{u}(k)=u(k)+a(k),$$

其中$a(k)\in l_2[0,m]$表示能量有界的未知FDI攻击信号. 通过部署N个传感器对系统的状态进行实时观测,测量输出$y_i(k)\in R^m$建模为

$$y_i(k)=H_i(k)x(k)+D_{l_i}(k)\omega(k),\ i=1,2,\dots,N. \quad (2)$$

设计如下形式的残差产生器:

$$\begin{cases} r_i(k)=V_i(k)\chi_i(k),\\ \chi_i(k)=y_i(k+1)-H_i(k+1)A(k)\hat{x}_i(k)-\\ \qquad H_i(k+1)B(k)u(k),\\ \hat{x}_i(k+1)=\\ A(k)\hat{x}_i(k)+B(k)u(k)+L_i(k)\chi_i(k). \end{cases} \quad (3)$$

其中: 时变矩阵$V_i(k)$和$L_i(k)$表示残差产生器待设计的增益矩阵, $r_i(k)$表示残差信号. 定义

$$\begin{cases} \xi(k)\triangleq[a(k),\ \omega^{\mathrm{T}}(k),\ \omega^{\mathrm{T}}(k+1)],\\ \tilde{r}_i(k)\triangleq r_i(k)-a(k),\\ e_i(k)\triangleq x(k)-\hat{x}_i(k). \end{cases}$$

基于式(1)$\sim$(3)建立如下误差系统:

$$\begin{cases} e_i(k+1)=\bar{A}_i(k)e_i(k)+\bar{B}_i(k)\xi(k),\\ \tilde{r}_i(k)=\bar{C}_i(k)e_i(k)+\bar{D}_i(k)\xi(k). \end{cases} \quad (4)$$

其中

$$\begin{cases} C_i(k)=H_i(k+1)A(k),\\ D_{a_i}(k)=H_i(k+1)B(k),\\ \bar{A}_i(k)=A(k)-L_i(k)C_i(k),\\ \bar{B}_i(k)=\\ [B(k)-L_i(k)D_{a_i}(k),B_d(k)-L_i(k)D_{d_i}(k)],\\ \bar{C}_i(k)=V_i(k)C_i(k),\\ \bar{D}_i(k)=[V_i(k)D_{a_i}(k)-I,V_i(k)D_{d_i}(k)],\\ D_{d_i}(k)=[H_i(k+1)E(k),D_{l_i}(k+1)],\\ B_d(k)=[E(k),0]. \end{cases}$$

本文的设计目标为: 设计增益矩阵$V_i(k)$、$L_i(k)$使得系统(4)均方指数稳定[11],并且在零初始条件下,给定抗扰动抑制比$\gamma_i>0$,残差信号与FDI攻击信号的逼近误差$\tilde{r}_i(k)$满足如下H_∞性能指标:

$$\sup_{\|\xi(k)\|_2\neq 0} E\Big\{\frac{\|\tilde{r}_i(k)\|_2}{\|\xi(k)\|_2}\Big\} < {\gamma_i}^2. \tag{5}$$

残差信号$r_i(k)$经过通讯网络前被量化,由于通讯带宽受限,融合中心只能接收到有限量化水平的数据信息. 在这种情况下,本文采取对数量化策略,不同量化程度的量化集合[14]表示为

$$U = \{\pm u_p^{ij} : u_p^{ij} = \rho_{ij}{}^p u_0^{ij}, p = 1, \pm1, \pm2, \ldots\} \bigcup$$
$$\{\pm u_0\} \bigcup \{0\}, 0 < \rho_{ij} < 1, u_0^{ij} > 0. \tag{6}$$

其中: ρ_{ij}表示残差信号$r_i(k)$第j通道处的量化程度; 定义$\delta_{ij} = \dfrac{1-\rho_{ij}}{1+\rho_{ij}}, 0 < \delta_{ij} < 1$,可见随着量化程度的提高($\rho_{ij}$减小),$\delta_{ij}$增大,原始信号数据的信息损失增大. 进一步,对数量化器[14]表示为

$$q_{ij}(\nu) = \begin{cases} u_p^{ij}, \ \dfrac{1}{1+\delta_{ij}} u_p^{ij} < \nu \leqslant \dfrac{1}{1-\delta_{ij}} u_p^{ij}; \\ 0, \ \nu = 0; \\ -q_{ij}(-\nu), \ \nu < 0. \end{cases} \tag{7}$$

定义量化误差$\Delta_i(k) \triangleq \mathrm{diag}\{\Delta_{i1}(k), \Delta_{i2}(k), \ldots, \Delta_{iz}(k)\}, |\Delta_{ij}(k)| \leqslant \delta_{ij}$,则融合中心接收到的残差信号为

$$r_{q_i}(k) = (I + \Delta_i(k)) r_i(k). \tag{8}$$

为提高残差信号的抗扰动能力,设计满足条件$0 \leqslant W_i(k) \leqslant I$和$\sum_{i=1}^{N} W_i(k) = I$的融合权重$W_i(k)$,经分布式融合后的残差信号$r_{q_0}(k)$表示为

$$r_{q_0}(k) = \sum_{i=1}^{N} W_i(k) r_{q_i}(k). \tag{9}$$

定义增广状态误差$\eta(k) \triangleq \mathrm{col}\{e_1(k), e_2(k), \ldots, e_N(k)\}$及融合误差$\tilde{r}_0(k) \triangleq r_{q_0}(k) - a(k)$,基于式(4)、(8)和(9),导出如下融合误差系统:

$$\begin{cases} \eta(k+1) = A_\eta(k)\eta(k) + B_\eta(k)\xi(k), \\ \tilde{r}_0(k) = \bar{C}_\eta(k)\eta(k) + \bar{D}_\eta(k)\xi(k). \end{cases} \tag{10}$$

其中

$$A_\eta(k) = \mathrm{diag}\{\bar{A}_1(k), \bar{A}_2(k), \ldots, \bar{A}_N(k)\},$$
$$B_\eta(k) = \mathrm{col}\{\bar{B}_1(k), \bar{B}_2(k), \ldots, \bar{B}_N(k)\},$$
$$\bar{C}_\eta(k) = C_\eta(k) + C_\delta(k),$$
$$\bar{D}_\eta(k) = D_\eta(k) + D_\delta(k),$$
$$C_\eta(k) =$$
$$[W_1(k)V_1(k)C_1(k), \ldots, W_N(k)V_N(k)C_N(k)],$$
$$C_\delta(k) = [C_{\delta_1}(k), C_{\delta_2}(k), \ldots, C_{\delta_N}(k)],$$
$$C_{\delta_i}(k) = W_i(k)\Delta_i(k)V_i(k)C_i(k),$$
$$D_\eta(k) = \Big[D_\eta^s(k), \sum_{i=1}^{N} W_i(k)V_i(k)D_{d_i}(k)\Big],$$
$$D_\eta^s(k) = \sum_{i=1}^{N} W_i(k)V_i(k)D_{a_i}(k) - I,$$
$$D_\delta(k) = [D_\delta{}^e(k), D_\delta{}^\xi(k)],$$
$$D_\delta{}^e(k) = \sum_{i=1}^{N} W_i(k)\Delta_i(k)V_i(k)D_{a_i}(k),$$
$$D_\delta{}^\xi(k) = \sum_{i=1}^{N} W_i(k)\Delta_i(k)V_i(k)D_{d_i}(k).$$

融合中心获得残差信号$r_{q_i}(k)$后,残差评价阶段采用如下评估函数$J_i(k)$:

$$J_i(k) = \frac{1}{k}\Big\{\sum_{i=0}^{N} r_{q_i}^{\mathrm{T}}(k) r_{q_i}(k)\Big\}^{\frac{1}{2}}, \ i = 0, 1, \ldots, N, \tag{11}$$

相应的检测阈值J_{thi}为

$$J_{thi} = \sup_{a(k)=0} J_i(k), \ i = 0, 1, \ldots, N. \tag{12}$$

由于攻击信号出现将使$J_i(k)$呈上升趋势,决定攻击是否出现的决策逻辑为$J_i(k) < J_{thi}$. 未检测到攻击,$J_i(k) \geqslant J_{thi}$时,触发攻击预警,其中$i = 0$表示融合检测攻击预警,其余表示针对第i个的残差信号的局部攻击预警.

本文要解决的问题为: 针对执行器遭受FDI攻击下的CPSs,首先设计增益矩阵$V_i(k)$和$L_i(k)$并获得量化后的残差信号$r_{q_i}(k)$; 其次,融合误差系统(10)在给定的H_∞性能指标下,优化融合权重$W_i(k)$,使融合检测方法具有更快的检测速度.

注1　提高残差信号对外界扰动的鲁棒性是本文进行FDI攻击检测的关键. 因此,融合目的为: 在给定的性能指标γ下,进一步提高融合误差系统(10)的抗扰动能力. 残差评价的过程中,阈值选取是一个重要的任务,过大的检测阈值会降低检测速度,过小的检测阈值则会增加误报率. 与单传感器的检测方法相比,通过分布式融合准则设计,融合检测方法能够在相同的阈值选取准则下获得更加精确的检测阈值,进而提高预警速度.

2　主要结果

在设计残差产生器(3)的增益矩阵$V_i(k)$和$L_i(k)$前,定义如下矩阵:

$$\Gamma_i(k) = K_i(k) + \Omega_i(k)\Xi_i^{-1}(k)\Omega_i^{\mathrm{T}}(k),$$
$$\Omega_i(k) = C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)\hat{V}_i^{\mathrm{T}}(k) + D_{a_i}(k)(-I+$$

$$\hat{V}_i(k)D_{a_i}(k))^{\mathrm{T}}+D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k)\hat{V}_i^{\mathrm{T}}(k),$$

$$K_i(k)=C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)+D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k)+D_{a_i}(k)D_{a_i}^{\mathrm{T}}(k),$$

$$\Psi_i(k)=B_d(k)D_{d_i}^{\mathrm{T}}(k)\hat{V}_i^{\mathrm{T}}(k)+B(k)(\hat{V}_i(k)D_{a_i}(k)-I)^{\mathrm{T}}+A(k)Q_i(k)C_i^{\mathrm{T}}(k)\hat{V}_i^{\mathrm{T}}(k),$$

$$Z_i(k)=C_i(k)Q_i(k)A^{\mathrm{T}}(k)+D_{a_i}(k)B^{\mathrm{T}}(k)+D_{d_i}(k)B_d^{\mathrm{T}}(k).$$

引理1[11] 针对误差系统(4),给定常数$\beta_i>0$、$\gamma_i>0$及初始状态加权矩阵$Q_i(0)>0$,当且仅当存在矩阵$Q_i(k)$,使得条件

$$Q_i(k+1)=\bar{A}_i(k)Q_i(k)\bar{A}_i^{\mathrm{T}}(k)+\beta_iI+\bar{B}_i(k)\bar{B}_i^{\mathrm{T}}(k)+G_i(k)\Xi_i^{-1}(k)G_i^{\mathrm{T}}(k),\quad \Xi_i(k)>0 \tag{13}$$

成立. 其中

$$\Xi_i(k)=-\bar{C}_i(k)Q_i(k)\bar{C}_i^{\mathrm{T}}(k)-\bar{D}_i(k)\bar{D}_i^{\mathrm{T}}(k)+\gamma_i^2I,$$

$$G_i(k)=\bar{A}_i(k)Q_i(k)\bar{C}_i^{\mathrm{T}}(k)+\bar{B}_i(k)\bar{D}_i^{\mathrm{T}}(k).$$

则误差系统(4)均方指数稳定,并且在给定H_∞性能指标下,最优增益矩阵$\hat{V}_i(k)$和$\hat{L}_i(k)$分别为

$$\hat{V}_i(k)=D_{a_i}^{\mathrm{T}}(k)(C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)+D_{a_i}(k)D_{a_i}^{\mathrm{T}}(k)+D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k))^{-1}, \tag{14}$$

$$\hat{L}_i(k)=(Z_i(k)+\Omega_i(k)\Xi_i^{-1}(k)\Psi_i^{\mathrm{T}}(k))^{\mathrm{T}}\Gamma_i^{-1}(k). \tag{15}$$

证明 定义Lyapunov函数

$$J_i(k)=e_i^{\mathrm{T}}(k)P_i(k)e_i(k), \tag{16}$$

其中$P_i(k)$为对称正定矩阵. 当

$$\mathcal{J}_i(k)=J_i(k+1)-J_i(k)+e_i^{\mathrm{T}}(k)e_i(k)-\gamma_i^2\xi^{\mathrm{T}}(k)\xi(k) \tag{17}$$

为负定时,误差系统(4)均方指数稳定且满足H_∞性能指标[9]. 根据Schur补定理[21],稳定性条件等价于

$$\bar{A}_i^{\mathrm{T}}(k)P_i(k+1)\bar{A}_i(k)+\bar{C}_i^{\mathrm{T}}(k)\bar{C}_i(k)-P_i(k)+\Lambda_{1_i}^{\mathrm{T}}(k)\Lambda_{2_i}^{-1}(k)\Lambda_{1_i}(k)<0. \tag{18}$$

其中:$\Lambda_{2_i}(k)=\gamma_i^2I-\bar{B}_i^{\mathrm{T}}(k)P_i(k+1)\bar{B}_i(k)-\bar{D}_i^{\mathrm{T}}(k)\bar{D}_i(k)>0$,$\Lambda_{1_i}(k)=\bar{A}_i^{\mathrm{T}}(k)P_i(k+1)\bar{B}_i(k)+\bar{C}_i^{\mathrm{T}}(k)\bar{D}_i(k)$.

参照文献[11]定理2的证明过程,当系统在有限时域$[0,m]$运行时,定义算子T为$(e_i(0),\xi(k))$至$\tilde{r}_i(k)$的线性映射,其状态空间表示式为(4),则存在T的伴随算子T^*满足如下内积关系:

$$\langle T(e_i(0),\xi(k)),\tilde{r}_i(k)\rangle=\langle(e_i(0),\xi(k)),T^*\tilde{r}_i(k)\rangle.$$

运用上述内积关系,构建算子T^*的状态空间方程式. 针对该伴随系统,按照式(16)~(18)可得:若存在正定矩阵$Q_i(k)=P_i(m+1-k)$使得

$$\bar{A}_i(k)Q_i(k)\bar{A}_i^{\mathrm{T}}(k)+\bar{B}_i(k)\bar{B}_i^{\mathrm{T}}(k)+G_i(k)\Xi_i^{-1}(k)G_i^{\mathrm{T}}(k)-Q_i(k+1)<0 \tag{19}$$

及$\Xi_i(k)>0$成立,则根据T和T^*范数等价条件,误差系统(4)均方指数稳定. 通过引入常数β_i,不等式(19)等价于式(13)Riccati方程. 限于篇幅,详细证明过程参考文献[11]. 针对$\hat{V}_i(k)$的求解,展开$\Xi_i(k)$可得

$$\Xi_i(k)=\gamma_i{}^2I-V_i(k)C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)V_i{}^{\mathrm{T}}(k)-(V_i(k)D_{a_i}(k)-I)(V_i(k)D_{a_i}(k)-I)^{\mathrm{T}}-V_i(k)D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k)V_i{}^{\mathrm{T}}(k),$$

可见矩阵$\Xi_i(k)$为$V_i(k)$的二次型函数. 其中$Q_i(k)$由式(13)解得,并且每个时刻已知. 在给定的H_∞性能指标下,将提升残差信号$r_i(k)$鲁棒性的优化目标定义为:对于任意适当维数的向量$\theta(k)$,求

$$\max\{\theta^{\mathrm{T}}(k)\Xi_i(k)\theta(k)\}. \tag{20}$$

令$\partial(\theta^{\mathrm{T}}(k)\Xi_i(k)\theta(k))/\partial(V_i^{\mathrm{T}}(k)\theta(k))=0$,可得

$$-\theta^{\mathrm{T}}(k)V_i(k)(C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)+D_{a_i}(k)D_{a_i}^{\mathrm{T}}(k)+D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k))+\theta^{\mathrm{T}}(k)D_{a_i}^{\mathrm{T}}(k)=0, \tag{21}$$

并且当$C_i(k)$行满秩时,得到

$$\partial^2(\theta^{\mathrm{T}}(k)\Xi_i(k)\theta(k))/\partial(V_i^{\mathrm{T}}(k)\theta(k))^2=-(C_i(k)Q_i(k)C_i^{\mathrm{T}}(k)+D_{a_i}(k)D_{a_i}^{\mathrm{T}}(k)+D_{d_i}(k)D_{d_i}^{\mathrm{T}}(k))^{\mathrm{T}}<0, \tag{22}$$

则式(14)为优化目标(20)的最优解. 针对最优$L_i(k)$的求解,选取优化目标$\min\{\theta^{\mathrm{T}}(k)Q_i(k+1)\theta(k)\}$,类似地,令$\partial(\theta^{\mathrm{T}}(k)Q_i(k+1)\theta(k))/\partial(L_i^{\mathrm{T}}(k)\theta(k))=0$,导出最优增益矩阵$\hat{L}_i(k)$为式(15). □

注2 本文的残差生成器是文献[11]故障检测滤波器(FDF)的特殊形式. 由于文献[11]的残差信号依赖于测量模型中故障信号对应的增益矩阵,而执行器端FDI攻击并未破坏测量数据,该FDF无法生成用于检测执行器端FDI攻击信号的残差.

引理2[22] 给定适当维数矩阵A、H、E和F,其中$FF^{\mathrm{T}}<I$,X为对称正定矩阵,α为任意正常数且满足条件$\alpha^{-1}I-EXE^{\mathrm{T}}>0$,则下列不等式成立:

$$(A+HFE)X(A+HFE)^{\mathrm{T}}\leqslant$$

$$A(X^{-1}-\alpha E^{\mathrm{T}}E)^{-1}A^{\mathrm{T}}+\alpha^{-1}HH^{\mathrm{T}}. \tag{23}$$

求解残差产生器的最优增益矩阵后,进一步设计融合准则,使得$r_{q_0}(k)$对$\xi(k)$有更好的抑制效果. 给出主要结果前, 定义如下矩阵:

$$\begin{cases} W(k)=[W_1(k),W_2(k),\dots,W_N(k)],\\ \Theta(k)=\gamma^2 I+\Theta_V(k),\\ C_{\Delta}(k)=Q(k)(C_{\Delta}^V(k))^{\mathrm{T}}(k)\hat{\Delta},\\ C_{\Delta}^V(k)=\mathrm{diag}\{V_1(k)C_1(k),\dots,V_N(k)C_N(k)\},\\ \hat{\Delta}=\mathrm{diag}\{\varepsilon\delta_1,\varepsilon\delta_2,\dots,\varepsilon\delta_N\},\\ \delta_i=\mathrm{diag}\{\delta_{i1},\delta_{i2},\dots,\delta_{iz}\},\\ D_{\Delta}(k)=(D_{\Delta}^V(k))^{\mathrm{T}}\hat{\Delta},\\ D_{\Delta}^V(k)=\mathrm{col}\{\bar{D}_1^V(k),\bar{D}_2^V(k),\dots,\bar{D}_N^V(k)\},\\ \bar{D}_i^V(k)=[V_i(k)D_{a_i}(k),V_i(k)D_{d_i}(k)],\\ \Pi_1=A_{\eta}(k)Q(k)C_{\eta}^{\mathrm{T}}(k)+B_{\eta}(k)D_{\eta}^{\mathrm{T}}(k),\\ \Pi_2=A_{\eta}(k)Q(k)(C_{\Delta}(k))^{\mathrm{T}}+B_{\eta}(k)(D_{\Delta}^V(k))^{\mathrm{T}},\\ \Theta_L(k)=\\ \Pi_1(k)(-\Theta_V(k)-\alpha W(k)W^{\mathrm{T}}(k))\Pi_1^{\mathrm{T}}(k)+\\ \alpha^{-1}\Pi_2(k)\Pi_2^{\mathrm{T}}(k). \end{cases}$$

定理1　给定局部残差产生器的最优增益矩阵$\hat{V}_i(k)$和$\hat{L}_i(k)$,融合误差系统(10)的H_∞性能指标γ及初始矩阵$Q(0)$,最优加权融合权重$W_i(k)$由以下凸优化问题确定:

$$\begin{cases} \min\limits_{0\leqslant W_i(k)\leqslant I,\,0<\varepsilon,\,\Theta_V(k)<0} \mathrm{Tr}\{\Theta_V(k)\};\\ \text{s.t.}\begin{bmatrix} -\varepsilon I & W^{\mathrm{T}}(k) & 0 & 0 & 0\\ * & -\Theta(k) & C_{\eta}(k)Q(k) & D_{\eta}(k) & 0\\ * & * & -Q(k) & 0 & C_{\Delta}(k)\\ * & * & * & -I & D_{\Delta}(k)\\ * & * & * & * & -\varepsilon I \end{bmatrix}<0,\\ \quad\sum\limits_{i=1}^{N}W_i(k)=I. \end{cases} \tag{24}$$

其中: $Q(k)$通过下式递推求得:

$$\begin{aligned} Q(k)=\beta I+A_{\eta}(k-1)Q(k-1)A_{\eta}^{\mathrm{T}}(k-1)+\\ B_{\eta}(k-1)B_{\eta}^{\mathrm{T}}(k-1)+\Theta_L(k-1). \end{aligned} \tag{25}$$

证明　基于引理1, 针对给定的H_∞性能指标γ, 当且仅当存在$Q(k)>0$使得

$$\begin{aligned} Q(k+1)>\\ A_{\eta}(k)Q(k)A_{\eta}^{\mathrm{T}}(k)+\\ B_{\eta}(k)B_{\eta}^{\mathrm{T}}(k)+G_{\eta}(k)\Xi^{-1}(k)G_{\eta}^{\mathrm{T}}(k), \end{aligned} \tag{26}$$

其中: $\Xi(k)=-\bar{C}_{\eta}(k)Q(k)\bar{C}_{\eta}^{\mathrm{T}}(k)-\bar{D}_{\eta}(k)\bar{D}_{\eta}^{\mathrm{T}}(k)+\gamma^2 I>0, G_{\eta}(k)=A_{\eta}(k)Q(k)\bar{C}_{\eta}^{\mathrm{T}}(k)+B_{\eta}(k)\bar{D}_{\eta}^{\mathrm{T}}(k)$. 则融合误差系统(10)均方指数稳定并且满足$H_\infty$性能. 类似于增益矩阵$\hat{V}_i(k)$和$\hat{L}_i(k)$的求解,针对融合权重$W_i(k)$的选取,定义优化目标为

$$\max\{\phi^{\mathrm{T}}(t)\Xi(k)\phi(k)\}, \tag{27}$$

其中$\phi(k)$为任意适当维数的向量. 由于量化误差的存在,难以通过求解二次型问题获得最优融合权重$W_i(k)$的显示表达式. 在这种情况下,引入矩阵$\Theta_V(k)<0$,使得下列条件成立:

$$\bar{C}_{\eta}(k)Q(k)\bar{C}_{\eta}^{\mathrm{T}}(k)+\bar{D}_{\eta}(k)\bar{D}_{\eta}^{\mathrm{T}}(k)<\gamma^2 I+\Theta_V(k). \tag{28}$$

可见优化目标(27)等价于$\min\{\phi^{\mathrm{T}}(k)\Theta(k)\phi(k)\}$, 其中$\Theta(k)=\gamma^2 I+\Theta_V(k)>0$. 针对正定矩阵$\Theta(k)$, 存在不等式

$$\phi^{\mathrm{T}}(k)\Theta(k)\phi(k)\leqslant\lambda_{\max}\{\phi(k)\phi^{\mathrm{T}}(k)\}\mathrm{Tr}\{\Theta(k)\}, \tag{29}$$

进而可将优化目标(27)转化为$\min \mathrm{Tr}\{\Theta(k)\}$. 由于$\gamma$是给定值, $\min \mathrm{Tr}\{\Theta(k)\}$等价于$\min \mathrm{Tr}\{\Theta_V(k)\}$. 根据Schur补引理[22],式(28)等价于

$$\begin{bmatrix} -\Theta(k) & \bar{C}_{\eta}(k)Q(k) & \bar{D}_{\eta}(k)\\ * & -Q(k) & 0\\ * & * & -I \end{bmatrix}<0. \tag{30}$$

注意$\bar{C}_{\eta}(k)$和$\bar{D}_{\eta}(k)$中存在对数量化引入的不确定项,令$F_{\Delta_{ij}}(k)=\dfrac{\Delta_{ij}(k)}{\delta_{ij}}$, $F_{\Delta_{ij}}(k)F_{\Delta_{ij}}^{\mathrm{T}}(k)\leqslant I$. 由于

$$\begin{bmatrix} 0 & C_{\delta}(k)Q(k) & D_{\delta}(k)\\ 0 & 0 & 0\\ 0 & 0 & 0 \end{bmatrix}=\begin{bmatrix} W(k)\\ 0\\ 0 \end{bmatrix}F_{\Delta}(k)Z(k). \tag{31}$$

其中

$$\begin{cases} Z(k)=[0,\Delta C_{\Delta}^V(k)Q(k),\Delta D_{\Delta}^V(k)],\\ \Delta=\mathrm{diag}\{\delta_1,\delta_2,\dots,\delta_N\},\\ F_{\Delta_i}=\mathrm{diag}\{F_{\Delta_{i1}},F_{\Delta_{i2}},\dots,F_{\Delta_{iz}}\},\\ F_{\Delta}(k)=\mathrm{diag}\{F_{\Delta_{11}},F_{\Delta_{12}},\dots,F_{\Delta_N}\}. \end{cases}$$

根据S-procedure[23], 令$\boldsymbol{W}(k)=\mathrm{col}\{W(k),0,0\}$, 则不等式(30)成立当且仅当存在标量$\varepsilon>0$使得下列

不等式成立:

$$\begin{bmatrix} -\Theta(k) & \bar{C}_\eta(k)Q(k) & \bar{D}_\eta(k) \\ * & -Q(k) & 0 \\ * & * & -I \end{bmatrix} + \varepsilon Z^{\mathrm{T}}(k)Z(k) + \varepsilon^{-1}\boldsymbol{W}(k)\boldsymbol{W}^{\mathrm{T}}(k) < 0. \tag{32}$$

利用Schur补引理,并左乘右乘$\mathrm{diag}\{I,I,I,I,\varepsilon I\}$消除所得线性矩阵不等式中的非线性项,最终获得凸优化问题(24).

另外,求解凸优化问题(24)前,要求给定满足条件(26)的正定矩阵$Q(k)$. 由于$\Delta_{ij}(k)$未知,与局部残差产生器设计过程相比,引入正常数$\beta>0$后,还需进一步处理未知项$G_\eta(k)\Xi^{-1}(k)G_\eta^{\mathrm{T}}(k)$. 将$G_\eta(k)$展开为

$$\begin{aligned} G_\eta(k) = {} & A_\eta(k)Q(k)C_\eta^{\mathrm{T}}(k) + B_\eta(k)D_\eta^{\mathrm{T}}(k) + \\ & A_\eta(k)Q(k)(C_\Delta(k))^{\mathrm{T}}F_\Delta(k)W^{\mathrm{T}}(k) + \\ & B_\eta(k)(D_\Delta^V(k))^{\mathrm{T}}F_\Delta(k)W^{\mathrm{T}}(k) = \\ & \Pi_1(k) + \Pi_2(k)F_\Delta(k)W^{\mathrm{T}}(k). \end{aligned} \tag{33}$$

由不等式(28)可得$-\Theta_V(k)<\Xi(k)$,并结合引理2得到:给定满足条件$\alpha^{-1}I+W^{\mathrm{T}}(k)\Theta_V^{-1}(k)W(k)$的正常数$\alpha$,有下列不等式成立:

$$\begin{aligned} & G_\eta(k)\Xi^{-1}(k)G_\eta^{\mathrm{T}}(k) < \\ & -G_\eta(k)\Theta_V^{-1}(k)G_\eta^{\mathrm{T}}(k) \leqslant \Theta_L(k) = \\ & \alpha^{-1}\Pi_2(k)\Pi_2^{\mathrm{T}}(k) + \Pi_1(k)(-\Theta_V(k) - \\ & \alpha W(k)W^{\mathrm{T}}(k))\Pi_1^{\mathrm{T}}(k), \end{aligned} \tag{34}$$

其中$\Theta_V(k)$通过求解凸优化问题(24)得到. 结合不等式(26)与(34),并引入正常数β,则$Q(k)$由Riccati方程(25)获得. □

注3 忽视残差信号的量化作用必然导致融合性能的降低. 为了提升融合后残差信号的鲁棒性,本文通过引入未知矩阵$\Theta_V(k)$,将融合权重$W_i(k)$的选取问题转化为LMI形式的凸优化问题,并通过Matlab LMI工具箱中的“mincx”函数求解. 注意优化目标$\min \mathrm{Tr}\{\Theta_V(k)\}$类似于线性时不变系统下最小化$H_\infty$性能指标[9],因此残差信号$H_\infty$性能的提升取决于是否能够获得更加负定的$\Theta_V(k)$,即使得$\mathrm{Tr}\{\Theta_V(k)\}$更小.

基于引理1和定理1,线性时变系统的融合攻击检测算法实现如下.

算法1 基于分布式融合的FDI攻击信号检测.

step 1: 选取适当大小的β、γ和矩阵$Q(0)$.

step 2: 利用式(14)和(15)求出增益矩阵$\hat{V}_i(k)$、$\hat{L}_i(k)$.

step 3: 利用式(24)求解出最优权重矩阵$W_i(k)$.

step 4: 利用式(11)和(12),通过50次Monte Carlo实验获得融合检测阈值.

step 5: 利用式(3)计算局部残差信号$r_i(k)$,并利用(9)计算出每个时刻的残差信号$r_{q_0}(k)$.

step 6: 利用式(11)计算$r_{q_0}(k)$的评估函数.

step7: 当$J_0(k)\geqslant J_{th0}$时,检测到攻击信号并发出预警;当$J_0(k)<J_{th0}$时,跳转至step 2继续运行.

3 仿真结果

考虑一个多传感器监测的移动目标系统,目标运动过程由其位置和速度表示,定义系统状态向量$x(k)\triangleq \mathrm{col}\{S_x(k),V_x(k),S_y(k),V_y(k)\}$. 其中:$S_x(k)$和$S_y(k)$分别为目标于$X$轴和$Y$轴的位置坐标,$V_x(k)$和$V_y(k)$分别对应其速度. 当控制信号被篡改时,目标移动轨迹由以下状态空间模型[24]表示:

$$x(k+1) = \begin{bmatrix} 1 & f(k) & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & f(k) \\ 0 & 0 & 0 & 1 \end{bmatrix} x(k) + \begin{bmatrix} 0 \\ f(k) \\ 0 \\ f(k) \end{bmatrix} [u(k) + a(k)] + [0.4,0.2,0.2,0.1]^{\mathrm{T}}\omega(k).$$

其中:采样周期$f(k)=0.9+0.1\sin k$;反馈控制信号$u(k)=[0,0.01,0,-0.01]x(k)$;系统于$[0,200]$时刻遭受的噪声$\omega(k)=0.25\mu(k)\sin(1.5\mu(k))$,$\mu(k)\in[-1,1]$可由Matlab的rand函数生成. 通过3个传感器实时监测目标运动,对应的测量矩阵分别为

$$H_1(k)=\begin{bmatrix} 0.5 & 0.7 & 0 & 0 \\ 0 & 0 & 0.9 & 0.6 \end{bmatrix},\ D_{l_1}(k)=\begin{bmatrix} 0.2 \\ 0.3 \end{bmatrix};$$

$$H_2(k)=\begin{bmatrix} 0.9 & 0.8 & 0 & 0 \\ 0 & 0 & 0.5 & 0.1 \end{bmatrix},\ D_{l_2}(k)=\begin{bmatrix} 0.2 \\ 0.4 \end{bmatrix};$$

$$H_3(k)=\begin{bmatrix} 0 & 0.2 & 0 & 0.2 \\ 0.8 & 0 & 0.8 & 0 \end{bmatrix},\ D_{l_3}(k)=\begin{bmatrix} 0.3 \\ 0.3 \end{bmatrix}.$$

进行融合检测时,给定常数$\gamma_i=\gamma=0.8,\beta_i=\beta=0.01$,初始矩阵$Q_i(0)=0.1I,Q(0)=0.1I$,其中下标$i$表示局部残差产生器的初始值设定.

令$\delta_{11}=\delta_{21}=\delta_{31}=0.2$,在$[0,200]$时刻内,取未知FDI攻击信号$a(k)=0.04\sin(k/15)$. 在图1中,实线为FDI攻击信号真实轨迹,虚线为融合残差信号轨迹. 可见经对数量化后,融合算法获得的残差信号对注入的攻击信号仍有较好的逼近能力.

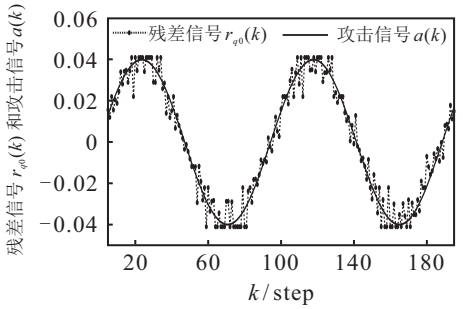
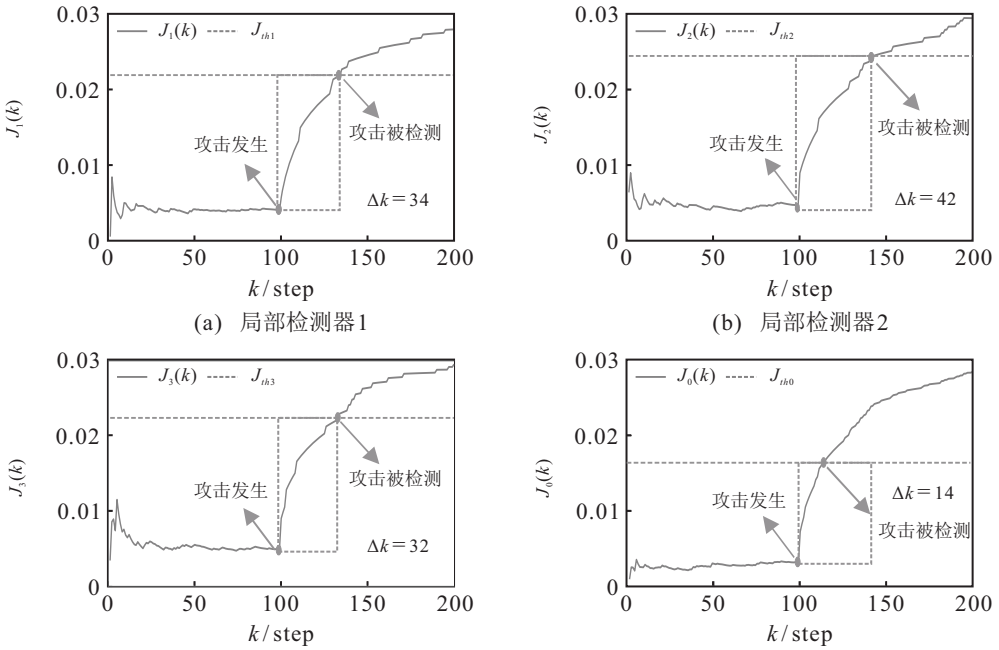


图 1　攻击信号 $a(k)$ 和残差信号 $r_{q_0}(k)$ 轨迹

令3个量化通道量化程度同为 $\delta_{ij}=0.3$,同时为突出融合检测的优势,选取阈值时将系统遭受的噪声设置为 $\omega(k)=0.75\mu(k)\sin(1.5\mu(k))$. 将系统遭受的FDI攻击信号设定为

$$a(k)=\begin{cases}0.05,\ 100<k<200;\\ 0,\ \text{otherwise.}\end{cases}\tag{35}$$

执行算法1,检测结果如图2所示. 图2中实线表示残差信号 $r_{q_i}(k)$ 对应的评估函数曲线,虚线表示检测阈值,具体检测时间见表1. 由此可知,相比使用局部残差信号的检测方式,融合检测拥有更快的预警速度. 值得注意的是,量化程度影响融合权重的变化,当量化程度同为 $\delta_{ij}=0.3$ 时,对应的权重均值可见表1,当量化程度分别为 $\delta_{11}=\delta_{21}=0.2,\delta_{31}=0.3$ 时,相应的权重均值分别为0.460 1, 0.427 6, 0.112 3,即本文设计的融合准则能够有效赋予数据损失少的通道较大权重,进一步提升了检测系统的可靠性.



(a) 局部检测器1　(b) 局部检测器2

(c) 局部检测器3　(d) 融合检测器

图 2　FDI攻击检测

表 1　攻击信号检测

检测器	δ	权重均值	阈值	检测时间/s
局部检测器1	0.3	0.302 6	0.021 9	34
局部检测器2	0.3	0.330 5	0.024 5	42
局部检测器3	0.3	0.366 9	0.022 4	32
融合检测器	*	*	0.016 4	14

4　结　论

本文研究了带宽受限下CPSs的FDI攻击检测问题. 首先基于给定 H_∞ 性能指标,给出了局部残差产生器未知增益矩阵的显式表达式,并获得了能够逼近攻击信号的残差信号;进而采用基于分布式融合的检测方法,设计融合权重提升残差信号的抗扰动能力,并在残差评估阶段大幅度提升了检测系统的预警速度;最后通过仿真算例验证了所提算法的有效性.

参考文献(References)

[1] Cao X H, Cheng P, Chen J M, et al. An online optimization approach for control and communication codesign in networked cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 439-450.

[2] Leitao P, Karnouskos S, Ribeiro L, et al. Smart agents in industrial cyber−physical systems[J]. Proceedings of the IEEE, 2016, 104(5): 1086-1101.

[3] Langner R. Stuxnet: Dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[4] Liu J P, Zhang W X, Ma T Y, et al. Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection[J]. Expert Systems with Applications, 2020, 158: 113578.

[5] Shi D W, Elliott R J, Chen T W. On finite-state stochastic

modeling and secure estimation of cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2017, 62(1): 65-80.

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

[7] Amin S, Litrico X, Sastry S, et al. Cyber security of water SCADA systems — Part I: Analysis and experimentation of stealthy deception attacks[J]. IEEE Transactions on Control Systems Technology, 2013, 21(5): 1963-1970.

[8] Zhou J, Chen B, Yu L. Intermediate-variable-based estimation for FDI attacks in cyber-physical systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(11): 2762-2766.

[9] He X, Wang Z D, Ji Y D, et al. Robust fault detection for networked systems with distributed sensors[J]. IEEE Transactions on Aerospace and Electronic Systems, 2011, 47(1): 166-177.

[10] 钟麦英, 刘帅, 赵辉宏. 基于Krein空间的线性离散时变系统H_∞故障估计 [J]. 自动化学报, 2008, 34(12): 1529-1533.
(Zhong M Y, Liu S, Zhao H H. Krein space-based H_∞ fault estimation for linear discrete time-varying systems[J]. Acta Automatica Sinica, 2008, 34(12): 1529-1533.)

[11] 李岳炀, 钟麦英. 存在多步测量数据包丢失的线性离散时变系统鲁棒H_∞故障检测滤波器设计[J]. 自动化学报, 2010, 36(12): 1788-1796.
(Li Y Y, Zhong M Y. On designing robust H_∞ fault detection filter for linear discrete time-varying systems with multiple packet dropouts[J]. Acta Automatica Sinica, 2010, 36(12): 1788-1796.)

[12] Zhong M Y, Ding S X, Ding E L. Optimal fault detection for linear discrete time-varying systems[J]. Automatica, 2010, 46(8): 1395-1400.

[13] Zhong M Y, Zhang L G, Ding S X, et al. A probabilistic approach to robust fault detection for a class of nonlinear systems[J]. IEEE Transactions on Industrial Electronics, 2017, 64(5): 3930-3939.

[14] Fu M Y, Xie L H. The sector bound approach to quantized feedback control[J]. IEEE Transactions on Automatic Control, 2005, 50(11): 1698-1711.

[15] Li Y X, Yang G H. Adaptive asymptotic tracking control of uncertain nonlinear systems with input quantization and actuator faults[J]. Automatica, 2016, 72: 177-185.

[16] Chen B, Yu L, Zhang W A, et al. Distributed H_∞ fusion filtering with communication bandwidth constraints[J]. Signal Processing, 2014, 96: 284-289.

[17] Chen B, Hu G Q, Zhang W A, et al. Distributed mixed H_2/H_∞ fusion estimation with limited communication capacity[J]. IEEE Transactions on Automatic Control, 2016, 61(3): 805-810.

[18] Hu J, Wang Z D, Liu G P, et al. Variance-constrained recursive state estimation for time-varying complex networks with quantized measurements and uncertain inner coupling[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(6): 1955-1967.

[19] Alavi S M M, Saif M. Fault detection in nonlinear stable systems over lossy networks[J]. IEEE Transactions on Control Systems Technology, 2013, 21(6): 2129-2142.

[20] Gao L J, Chen B, Yu L. Fusion-based FDI attack detection in cyber-physical systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(8): 1487-1491.

[21] Yaz E E. Linear matrix inequalities in system and control theory[J]. Proceedings of the IEEE, 1998, 86(12): 2473-2474.

[22] Xie L H, Soh Y C, de Souza C E. Robust Kalman filtering for uncertain discrete-time systems[J]. IEEE Transactions on Automatic Control, 1994, 39(6): 1310-1314.

[23] Bu X Y, Dong H L, Wang Z D, et al. Non-fragile distributed fault estimation for a class of nonlinear time-varying systems over sensor networks: The finite-horizon case[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2019, 5(1): 61-69.

[24] Chen B, Ho D W C, Zhang W A, et al. Networked fusion estimation with bounded noises[J]. IEEE Transactions on Automatic Control, 2017, 62(10): 5415-5421.

作者简介

沈家辉 (1996−), 男, 硕士生, 从事信息物理系统攻击检测的研究, E-mail: jhshen_0918@126.com;

翁品迪 (1996−), 男, 博士生, 从事信息物理系统中攻击信号融合检测的研究, E-mail: pwd2gg@aliyun.com;

陈博 (1984−), 男, 教授, 博士, 从事信息融合、信息物理系统安全、分布式估计与控制等研究, E-mail: bchen@zjut.edu.cn;

俞立 (1961−), 男, 教授, 博士生导师, 从事网络控制、信息融合、信息物理系统安全等研究, E-mail: lyu@zjut.edu.cn.

(责任编辑：闫 妍)