隐蔽式攻击下的离散系统区间观测器设计

刘 坤[1], 张淇瑞[1], 郭 航[1], 刘 涛[2†], 夏元清[1]

(1. 北京理工大学 自动化学院, 北京 100081; 2. 北京物资学院 信息学院, 北京 101149)

摘要: 本文研究了隐蔽式攻击下的网络化控制系统的安全估计问题. 首先, 根据攻击保持隐蔽的条件, 得到了攻击信号的上界和下界. 其次, 基于边界信息设计了一类原坐标系下的区间观测器, 并进一步通过坐标变换放宽增益矩阵的设计条件, 给出了变换下的区间观测器设计方法. 然后, 提出了基于H_∞滤波理论计算隐蔽式攻击下的最优观测器增益的方法, 并通过求解线性矩阵不等式获得最优增益矩阵. 最后, 通过仿真算例验证了所提方法的有效性.

关键词: 隐蔽式攻击; 区间观测器; 网络化控制系统

引用格式: 刘坤, 张淇瑞, 郭航, 等. 隐蔽式攻击下的离散系统区间观测器设计. 控制理论与应用, 2020, 37(8): 1673 – 1680

DOI: 10.7641/CTA.2020.90618

Interval observer design of discrete-time systems under stealthy attacks

LIU Kun[1], ZHANG Qi-rui[1], GUO Hang[1], LIU Tao[2†], XIA Yuan-qing[1]

(1. School of Automation, Beijing Institute of Technology, Beijing 100081, China;
2. School of Information, Beijing Wuzi University, Beijing 101149, China)

Abstract: This paper investigates the security estimation of networked control system under stealthy attacks. Firstly, the upper and lower bounds of the attack signals are obtained according to the condition that the attacks remain stealthy. Secondly, based on the bounds of the attacks, an interval observer is designed in the original coordinates. Furthermore, the design conditions of the gain matrix are relaxed by a transformation of coordinates, and the design method of this interval observer is given. Then, an approach is proposed to calculate the optimal observer gain based on the theory of H_∞ filtering, and the optimal gain matrix is obtianed by solving a linear matrix inequality. Finally, a numerical example is given to verify the effectiveness of the proposed method.

Key words: stealthy attacks; interval observer; networked control system

Citation: LIU Kun, ZHANG Qirui, GUO Hang, et al. Interval observer design of discrete-time systems under stealthy attacks. *Control Theory & Applications*, 2020, 37(8): 1673 – 1680

1 引言

随着网络技术的迅猛发展和互联网的广泛应用, 网络系统和控制系统结合日益紧密, 并逐渐形成了一种分布式、智能化、网络化的反馈控制系统–网络化控制系统[1–3](networked control system, NCS). 通信网络固有的开放性使得NCS容易受到数据篡改、窃听和拦截等恶意威胁. 近几年来, NCS的安全研究逐步成为了控制理论界的热门研究方向之一[4–6].

为了保证系统安全, NCS一般通过攻击检测器检测攻击[7–9], 然而某些网络攻击可以逃避检测. 常用的攻击检测器是χ^2检测器. 针对具有χ^2检测器的线性时不变系统, 文献[10]研究了隐蔽式攻击下系统的可达集, Chen等人设计了使χ^2检测器报警率保持在一定范围之内的最优隐蔽式攻击策略[11]. 针对任意的攻击检测器, Pasqualetti等人从系统论和图论角度描述了完全不可检测和识别的隐蔽式攻击[12]. 文献[13]给出了在已知部分系统初始状态信息的情况下, 攻击对于任意检测器保持隐蔽的条件. Gupta等人通过分析系统遭受攻击和未遭受攻击时量测信号间的相对熵, 给出了任意检测器误警率衰减指数的上界[14]. 文献[15]设计了使任意检测器误警率衰减指数在一定范围之内的最优攻击策略. 攻击的隐蔽性给保护系统的安全带

收稿日期: 2019−07−25; 录用日期: 2020−04−08.

†通信作者. E-mail: liutao19832001@163.com.

本文责任编委: 高会军.

国家自然科学基金项目(61873034), 北京市自然科学基金项目(4182057), 北京市智能物流系统协同创新中心开放课题(BILSCIC–2019KF–13), 北京理工大学研究生创新项目(2019CX20031)资助.

Supported by the National Natural Science Foundation of China (61873034), the Beijing Natural Science Foundation (4182057), the Open Subject of Beijing Intelligent Logistics System Collaborative Innovation Center (BILSCIC–2019KF–13) and the Graduate Technological Innovation Project of Beijing Institute of Technology (2019CX20031).

来了很大困难.

另一方面, 系统中的噪声通常是有界的, 区间观测器可以利用噪声的边界信息估计出状态的上、下界, 由于其具有良好的处理不确定输入的能力, 关于区间观测器的研究现已引起了广泛的关注. Wang等人针对具有参数不确定性的线性变参数连续系统, 通过直接构造Hurwitz和Metzler矩阵设计区间观测器[16]. 文献[17]研究了一类非线性连续系统的区间观测器设计问题, 并通过利用静态坐标变换放宽观测器增益的设计条件. Wang等人针对具有未知但有界的扰动和测量噪声的不确定离散线性系统, 提出了一种无需坐标变换的区间观测器设计方法[18], 其基本思想是引入更多的自由度放宽设计条件. 文献[19]设计了离散线性时变系统的区间观测器, 并提出了时变的相似变换以放宽假设条件.

进一步, 文献[20]设计了一种结合区间观测器和降维观测器的方法以检测NCS中的执行器故障. 文献[21]研究了基于区间观测器的鲁棒故障诊断方法的保守性问题. 这些方法同样可推广到网络攻击的检测当中. 然而, 针对隐蔽的网络攻击, 如何设计区间观测器以保证系统安全仍是需要解决的问题.

基于以上的分析讨论, 本文主要研究隐蔽式攻击下的离散线性系统的区间观测器设计. 首先, 根据攻击者保持隐蔽的条件, 获得了攻击信号的上、下界. 其次, 基于攻击信号边界信息, 设计了两种不同的区间观测器. 然后, 提出了基于H_∞ 滤波理论计算最优观测器增益的方法. 最后, 通过仿真实例证明了所提方法的有效性.

记号: $\mathbb{R}$和$\mathbb{N}$分别表示实数域和自然数域; $\mathbb{R}_+$代表非负实数集; $\mathbb{R}^n$表示n维欧几里得空间; $\mathbb{R}^{n\times m}$表示所有$n\times m$维实数矩阵的集合; I_n表示n阶单位矩阵; $M\succ 0 (M\succcurlyeq 0)$表示矩阵$M$是正定(半正定)矩阵; $A\geqslant B$表示矩阵$A-B$中的元素均大于等于0, 并称$A-B$是非负的; $x\geqslant y (x>y)$表示向量$x-y$中的元素均大于等于(大于)0; 对于矩阵$M\in\mathbb{R}^{m\times n}$, M^{T}表示它的转置, 定义$M^+=\max(M,0)$, $M^-=M^+-M$且$\tilde{M}=M^++M^-$; "$\star$" 表示对称矩阵中的对称块; 对于向量$x\in\mathbb{R}^n$, $\|x\|_2$表示其$\mathfrak{L}_2$范数; 对于一系列向量u_0, u_1, $\cdots$, $u_k\in\mathbb{R}^n$, 令$u_{0:\,k}=[u_0^{\mathrm{T}}\ \ u_1^{\mathrm{T}}\ \cdots\ u_k^{\mathrm{T}}]^{\mathrm{T}}$.

2 问题描述

2.1 离散NCS模型

考虑以下离散线性时不变系统:

$$x_{k+1}=Ax_k+\omega_k, \tag{1}$$

$$y_k=Cx_k+\upsilon_k, \tag{2}$$

其中: $x_k\in\mathbb{R}^n$是系统状态向量, $\omega_k\in\mathbb{R}^n$和$\upsilon_k\in\mathbb{R}^p$分别是未知过程噪声和量测噪声, $y_k\in\mathbb{R}^p$是输出信号, $A\in\mathbb{R}^{n\times n}$和$C\in\mathbb{R}^{p\times n}$是已知的常数矩阵. 给定初始状态$x_0\in\mathbb{R}^n$, 用$x(x_0,\omega_{0:\,k-1})$表示系统(1)−(2)在噪声$\omega_0,\cdots,\omega_{k-1}$的作用下$k$时刻的状态, 则$k$时刻系统输出$y(x_0,\omega_{0:\,k-1},\upsilon_k)=Cx(x_0,\omega_{0:\,k-1})+\upsilon_k$.

对于系统(1)−(2), 本文给出以下假设:

假设 1 系统初始状态满足

$$\underline{x}_0\leqslant x_0\leqslant\bar{x}_0,$$

其中$\underline{x}_0$, $\bar{x}_0\in\mathbb{R}^n$是已知的向量.

假设 2 过程噪声ω_k满足

$$\underline{\omega}_k\leqslant\omega_k\leqslant\bar{\omega}_k,\ \forall k\geqslant 0,$$

其中: $\bar{\omega}_k>0$是已知向量, 且$\underline{\omega}_k=-\bar{\omega}_k$.

假设 3 量测噪声υ_k满足

$$-\vartheta\mathbf{1}_p\leqslant\upsilon_k\leqslant\vartheta\mathbf{1}_p,\ \forall k\geqslant 0,$$

其中: $\vartheta>0$是已知常数, $\mathbf{1}_p$是元素皆为1的p维列向量.

注 1 假设1−3说明系统初始状态x_0、过程噪声ω_k和量测噪声υ_k均是有界的, 它们是区间观测器设计中的普遍性假设[16–19].

2.2 隐蔽式攻击

当系统的传感器遭受攻击时, 输出方程(2)变为

$$y_{\mathrm{a},k}=Cx_k+\upsilon_k+a_k, \tag{3}$$

其中: $y_{\mathrm{a},k}$表示系统受到攻击时的输出, $a_k\in\mathbb{R}^p$表示攻击信号. 给定初始状态$x_0\in\mathbb{R}^n$, 将系统在噪声$\omega_0,\cdots,\omega_{k-1},\upsilon_k$和攻击$a_k$的作用下$k$时刻的输出记为$y_{\mathrm{a}}(x_0,\omega_{0:\,k-1},\upsilon_k,a_k)=Cx(k,x_0,\omega_{0:\,k-1})+\upsilon_k+a_k$.

攻击者需要保证自身不被检测器检测到, 依据文献[12], 隐蔽式攻击的定义如下所示.

定义 1 如果存在初始状态x_0^1, $x_0^2\in[\underline{x}_0,\bar{x}_0]$, 过程噪声$\omega_{0:\,k-1}^1,\omega_{0:\,k-1}^2\in[\underline{\omega}_{0:\,k-1},\bar{\omega}_{0:\,k-1}]$和量测噪声$\upsilon_k^1,\upsilon_k^2\in[-\vartheta\mathbf{1}_p,\vartheta\mathbf{1}_p]$, 使得

$$y_{\mathrm{a}}(x_0^1,\omega_{0:\,k-1}^1,\upsilon_k^1,a_k)=y(x_0^2,\omega_{0:\,k-1}^2,\upsilon_k^2),\ \forall k\geqslant 0, \tag{4}$$

那么, 攻击a_k就可以称作是隐蔽的.

本文的目的是设计隐蔽式攻击下的系统(1)(3)的区间观测器.

3 主要结果

本节先给出隐蔽式攻击信号的上、下界估计方法, 并进一步设计两种区间观测器. 最后, 基于H_∞滤波理论计算出最优观测器增益矩阵.

3.1 隐蔽式攻击信号上、下界的估计

为了估计攻击信号a_k,下面给出需要的引理和假

设条件.

引理 1[22]　如果向量x, $\underline{x}$, $\bar{x} \in \mathbb{R}^n$满足$\underline{x} \leqslant x \leqslant \bar{x}$, 那么, 对于任意的常数矩阵$M \in \mathbb{R}^{m\times n}$都有

$$M^+\underline{x} - M^-\bar{x} \leqslant Mx \leqslant M^+\bar{x} - M^-\underline{x}. \tag{5}$$

假设 4　存在非奇异矩阵$U \in \mathbb{R}^{n\times n}$使$D = UA\cdot U^{-1}$是Schur且非负的.

注 2　当A可对角化时且特征值大于等于0小于1时, 假设4成立.

当系统遭受隐蔽式攻击时, 给出如下所示的区间观测器以估计a_k:

$$\begin{cases} \bar{a}_k = (CU^{-1})^+\bar{\epsilon}_k - (CU^{-1})^-\underline{\epsilon}_k + 2\vartheta\mathbf{1}_p,\\ \underline{a}_k = (CU^{-1})^+\underline{\epsilon}_k - (CU^{-1})^-\bar{\epsilon}_k - 2\vartheta\mathbf{1}_p,\\ \bar{\epsilon}_{k+1} = D\bar{\epsilon}_k + \tilde{U}(\bar{\omega}_k - \underline{\omega}_k),\\ \underline{\epsilon}_{k+1} = D\underline{\epsilon}_k - \tilde{U}(\bar{\omega}_k - \underline{\omega}_k),\\ \bar{\epsilon}_0 = \tilde{U}(\bar{x}_0 - \underline{x}_0),\\ \underline{\epsilon}_0 = -\tilde{U}(\bar{x}_0 - \underline{x}_0), \end{cases} \tag{6}$$

其中$\bar{a}_k, \underline{a}_k \in \mathbb{R}^p$分别是攻击信号$a_k$的上界和下界估计值.

那么可以得到如下定理:

定理 1　当受攻击系统(1)(3)的参数满足假设1−4时, 隐蔽式攻击a_k满足

$$\underline{a}_k \leqslant a_k \leqslant \bar{a}_k,\ \forall k \geqslant 0.$$

证　根据定义1有

$$y(x_0^1, \omega_{0:\,k-1}^1, \upsilon_k^1) + a_k = y(x_0^2, \omega_{0:\,k-1}^2, \upsilon_k^2),\ \forall k \geqslant 0,$$

即

$$a_k = C\Delta_k + \upsilon_k^2 - \upsilon_k^1,$$

其中$\Delta_k = x(x_0^2, \omega_{0:\,k-1}^2) - x(x_0^1, \omega_{0:\,k-1}^1)$, 且满足

$$\Delta_{k+1} = A\Delta_k + \omega_k^2 - \omega_k^1.$$

令$\epsilon_k = U\Delta_k$, 有

$$\epsilon_{k+1} = D\epsilon_k + U(\omega_k^2 - \omega_k^1), \tag{7}$$

$$a_k = CU^{-1}\epsilon_k + \upsilon_k^2 - \upsilon_k^1. \tag{8}$$

利用假设2可以得到

$$\underline{\omega}_k - \bar{\omega}_k \leqslant \omega_k^2 - \omega_k^1 \leqslant \bar{\omega}_k - \underline{\omega}_k,\ \forall k \geqslant 0.$$

而依据假设1, 可知

$$\underline{\epsilon}_0 \leqslant \epsilon_0 \leqslant \bar{\epsilon}_0.$$

由式(7)和引理1可得$\underline{\epsilon}_k \leqslant \epsilon_k \leqslant \bar{\epsilon}_k,\ \forall k \geqslant 0$.

根据假设3, 易得

$$-2\vartheta\mathbf{1}_p \leqslant \upsilon_k^2 - \upsilon_k^1 \leqslant 2\vartheta\mathbf{1}_p,\ \forall k \geqslant 0.$$

由式(8)和引理1可得$\underline{a}_k \leqslant a_k \leqslant \bar{a}_k,\ \forall k \geqslant 0$.

证毕.

3.2　受攻击系统的原坐标系下的区间观测器设计

基于上述讨论, 由式(6)得到隐蔽式攻击信号的上界$\bar{a}_k$和下界$\underline{a}_k$. 接下来, 将利用上、下界的信息设计原坐标系下的区间观测器, 为此需要用到下面的假设.

假设 5[19]　存在增益矩阵L使得$A - LC$是非负且Schur的.

假设5是设计区间观测器的一个很重要的条件, 它具有很强的约束性, 在下一小节会进行放宽.

对于已知攻击信号上、下界$\bar{a}_k$, $\underline{a}_k$的受攻击系统(3), 设计如下所示的原坐标系下的区间观测器:

$$\begin{cases} \bar{x}_{k+1} = (A - LC)\bar{x}_k + Ly_{\mathrm{a},k} + \bar{\omega}_k + \\ \qquad L^*\vartheta - L^+\underline{a}_k + L^-\bar{a}_k,\\ \underline{x}_{k+1} = (A - LC)\underline{x}_k + Ly_{\mathrm{a},k} + \underline{\omega}_k - \\ \qquad L^*\vartheta - L^+\bar{a}_k + L^-\underline{a}_k, \end{cases} \tag{9}$$

其中: $\bar{x}_k \in \mathbb{R}^n$和$\underline{x}_k \in \mathbb{R}^n$分别是系统状态$x_k$的上界和下界估计值, $L^* = \tilde{L}\mathbf{1}_p$. 定义$\bar{e}_k = \bar{x}_k - x_k$和$\underline{e}_k = x_k - \underline{x}_k$为上、下界估计值与真实状态之间的差, 即上界误差和下界误差.

定理 2　若遭受隐蔽式攻击的系统(1)(3)的参数满足假设1−4, 且区间观测器(9)的增益L满足假设5, 则有

$$\underline{x}_k \leqslant x_k \leqslant \bar{x}_k,\ \forall k \geqslant 0.$$

证　由式(1)和式(9)得, 上界误差$\bar{e}_k$和下界误差$\underline{e}_k$分别满足

$$\begin{aligned} \bar{e}_{k+1} &= (A - LC)\bar{e}_k + L\upsilon_k + L^*\vartheta + \bar{\omega}_k - \\ &\qquad \omega_k + La_k - (L^+\underline{a}_k - L^-\bar{a}_k),\\ \underline{e}_{k+1} &= (A - LC)\underline{e}_k - L\upsilon_k + L^*\vartheta + \omega_k - \\ &\qquad \underline{\omega}_k - La_k + L^+\bar{a}_k - L^-\underline{a}_k. \end{aligned}$$

根据假设2, 可得$\bar{\omega}_k - \omega_k$和$\omega_k - \underline{\omega}_k$是非负的. 而依据假设3, $L\upsilon_k + L^*\vartheta$和$-L\upsilon_k + L^*\vartheta$是非负的. 由定理1和引理1可得$La_k - (L^+\underline{a}_k - L^-\bar{a}_k)$和$-La_k + L^+\bar{a}_k - L^-\underline{a}_k$是非负的. 另外, 可以从假设5和$\bar{e}_0 = \bar{x}_0 - x_0 \geqslant 0$, $\underline{e}_0 = x_0 - \underline{x}_0 \geqslant 0$得出$\bar{e}_k \geqslant 0$且$\underline{e}_k \geqslant 0$, $\forall k \geqslant 0$. 因此, $\underline{x}_k \leqslant x_k \leqslant \bar{x}_k,\ \forall k \geqslant 0$.

证毕.

3.3　受攻击系统的坐标变换下的区间观测器设计

在上一小节, 基于假设5本文设计了原坐标系下的区间观测器(9), 但在某些情况下, 不存在增益L使矩阵$A - LC$是非负的. 一种可行的处理方法是通过引入坐标变换矩阵R, 使矩阵$R(A - LC)R^{-1}$是非负的. 因此, 将基于以下假设设计区间观测器.

假设 6[19]　存在矩阵L和非奇异矩阵R, 使得矩阵$A - LC$是Schur的, 且矩阵$R(A - LC)R^{-1}$是非负的.

定义中间变量$\hat{x}_{k+1}^+$和$\hat{x}_{k+1}^-$满足

$$\begin{cases}\hat{x}_{k+1}^{+}=(A-LC)\hat{x}_k^{+}+Ly_{\mathrm{a},k}+R^{-1}\tilde{R}\bar{\omega}_k+\\ \qquad L^*\vartheta-L^{+}\underline{a}_k+L^{-}\bar{a}_k,\\ \hat{x}_{k+1}^{-}=(A-LC)\hat{x}_k^{-}+Ly_{\mathrm{a},k}+R^{-1}\tilde{R}\underline{\omega}_k-\\ \qquad L^*\vartheta-L^{+}\bar{a}_k+L^{-}\underline{a}_k,\end{cases}\tag{10}$$

相应的初始条件为

$$\begin{cases}\hat{x}_0^{+}=S(R^{+}\bar{x}_0-R^{-}\underline{x}_0),\\ \hat{x}_0^{-}=S(R^{+}\underline{x}_0-R^{-}\bar{x}_0),\end{cases}\tag{11}$$

其中$S=R^{-1}$.

定理 3 若遭受隐蔽式攻击的系统(1)(3)的参数满足假设1−4, 且区间观测器的增益矩阵L满足假设6, 那么

$$\begin{cases}\bar{x}_k=S^{+}R\hat{x}_k^{+}-S^{-}R\hat{x}_k^{-},\\ \underline{x}_k=S^{+}R\hat{x}_k^{-}-S^{-}R\hat{x}_k^{+}\end{cases}\tag{12}$$

是可以满足$\underline{x}_k\leqslant x_k\leqslant\bar{x}_k$, $\forall k\geqslant 0$的一种区间观测器.

证 首先, 定义误差

$$E_k^{+}=R\hat{x}_k^{+}-Rx_k,$$
$$E_k^{-}=Rx_k-R\hat{x}_k^{-}.$$

由式(1)和式(10)可得

$$E_{k+1}^{+}=$$
$$R(A-LC)R^{-1}E_k^{+}+\tilde{R}\bar{\omega}_k-R\omega_k+RL^*\vartheta+$$
$$RL\upsilon_k+RLa_k-RL^{+}\underline{a}_k+RL^{-}\bar{a}_k,$$
$$E_{k+1}^{-}=$$
$$R(A-LC)R^{-1}E_k^{-}-\tilde{R}\underline{\omega}_k+R\omega_k+RL^*\vartheta-$$
$$RL\upsilon_k-RLa_k+RL^{+}\bar{a}_k-RL^{-}\underline{a}_k.$$

根据假设2有$\bar{\omega}_k+\underline{\omega}_k=0$, $\forall k\geqslant 0$. 又由引理1可知

$$-R^{+}\bar{\omega}_k-R^{-}\bar{\omega}_k\leqslant R\omega_k\leqslant R^{+}\bar{\omega}_k+R^{-}\bar{\omega}_k.\tag{13}$$

由不等式(13)得

$$\tilde{R}\bar{\omega}_k-R\omega_k\geqslant 0,$$
$$-\tilde{R}\underline{\omega}_k+R\omega_k=\tilde{R}\bar{\omega}_k+R\omega_k\geqslant 0.$$

此外, 已知

$$RL^*\vartheta+RL\upsilon_k\geqslant 0,$$
$$RLa_k-RL^{+}\underline{a}_k+RL^{-}\bar{a}_k\geqslant 0,$$
$$RL^*\vartheta-RL\upsilon_k\geqslant 0,$$
$$-RLa_k+RL^{+}\bar{a}_k-RL^{-}\underline{a}_k\geqslant 0.$$

与此同时, 有$\underline{x}_0\leqslant x_0\leqslant\bar{x}_0$, 因而$E_0^{+}=R^{+}\bar{x}_0-R^{-}\underline{x}_0-Rx_0$和$E_0^{-}=Rx_0-(R^{+}\underline{x}_0-R^{-}\bar{x}_0)$是非负的. 依据假设6, $R(A-LC)R^{-1}$也是非负的, 由此可以得到: $E_k^{+}\geqslant 0$且$E_k^{-}\geqslant 0$, $\forall k\geqslant 0$. 因此

$$R\hat{x}_k^{-}\leqslant Rx_k\leqslant R\hat{x}_k^{+}.\tag{14}$$

结合式(12)和式(14), 很容易证明

$$\underline{x}_k\leqslant x_k\leqslant\bar{x}_k.\tag{15}$$

证毕.

注 3 假设6放宽了假设5的条件. 事实上, 由于变换矩阵的存在, 式(10)中的L仅需保证$A-LC$是Schur的, 而不必像式(9)中那样需同时保证$A-LC$是Schur且非负的.

3.4 基于$\mathbf{H}_\infty$滤波理论的最优观测器增益

本节将给出计算原坐标系下的和坐标变换下的区间观测器(9)和(12)增益L的一种方法. 为此, 针对两种情况分别给出如下定义.

1) 原坐标系下的区间观测器(9): 定义估计误差$e_k=\bar{x}_k-\underline{x}_k$. 那么, 易得

$$e_{k+1}=$$
$$(A-LC)e_k+\bar{\omega}_k-\underline{\omega}_k+2L^*\vartheta+\tilde{L}\bar{a}_k-\tilde{L}\underline{a}_k=$$
$$(A-LC)e_k+F\delta_{1,k},\tag{16}$$

其中:

$$\delta_{1,k}=[\bar{\omega}_k^{\mathrm{T}}\ \ (\mathbf{1}_p\vartheta)^{\mathrm{T}}\ \ (\bar{a}_k-\underline{a}_k)^{\mathrm{T}}]^{\mathrm{T}},$$
$$F=[2I_n\ \ 2\tilde{L}\ \ \tilde{L}].$$

2) 坐标变换下的区间观测器(12): 定义估计误差$e_k=R^{-1}\tilde{S}^{-1}(\bar{x}_k-\underline{x}_k)$. 那么, 由式(12)可以得到

$$e_{k+1}=$$
$$R^{-1}\tilde{S}^{-1}(S^{+}R+S^{-}R)(\hat{x}_{k+1}^{+}-\hat{x}_{k+1}^{-})=$$
$$R^{-1}\tilde{S}^{-1}\tilde{S}R(\hat{x}_{k+1}^{+}-\hat{x}_{k+1}^{-})=$$
$$\hat{x}_{k+1}^{+}-\hat{x}_{k+1}^{-}=$$
$$R^{-1}(E_{k+1}^{+}+E_{k+1}^{-})=$$
$$(A-LC)R^{-1}(E_k^{+}+E_k^{-})+2L^*\vartheta+$$
$$R^{-1}\tilde{R}(\bar{\omega}_k-\underline{\omega}_k)+\tilde{L}\bar{a}_k-\tilde{L}\underline{a}_k=$$
$$(A-LC)e_k+F\delta_{2,k},\tag{17}$$

其中

$$\delta_{2,k}=[(R^{-1}\tilde{R}\bar{\omega}_k)^{\mathrm{T}}\ \ (\mathbf{1}_p\vartheta)^{\mathrm{T}}\ \ (\bar{a}_k-\underline{a}_k)^{\mathrm{T}}]^{\mathrm{T}}.$$

在上述两种情况下, 估计误差均有以下形式:

$$e_{k+1} = (A - LC)e_k + F\delta_{i,k},\ i = 1, 2. \quad (18)$$

为了获得准确的区间估计, 可以利用H_∞滤波理论设计区间观测器增益L使得估计误差e_k对有界不确定项$\delta_{i,k}$具有良好的鲁棒性, 从而尽可能地缩小区间宽度. 因此, 给出下述H_∞性能指标表达式:

$$\|e_k\|_2^2 \leqslant \gamma^2 \|\delta_{i,k}\|_2^2, \quad (19)$$

其中常数$\gamma > 0$.

利用有界实引理[23], 若以下不等式成立:

$$e_{k+1}^{\mathrm{T}} P e_{k+1} - e_k^{\mathrm{T}} P e_k + e_k^{\mathrm{T}} e_k \leqslant \gamma^2 \delta_{i,k}^{\mathrm{T}} \delta_{i,k}, \quad (20)$$

其中: $i = 1, 2,\ 0 \prec P \in \mathbb{R}^{n\times n}$, 则式(19)成立.

接下来, 由式(20)可以得到以下定理.

定理 4　针对遭受隐蔽式攻击的系统(3), 给定常数$\gamma > 0$, 如果假设1–4满足, 并且存在矩阵$P \succ 0$, 使得如下线性矩阵不等式成立:

$$\begin{bmatrix} -P + I_n & 0 & A^{\mathrm{T}}P - C^{\mathrm{T}}D^{\mathrm{T}} \\ \star & -\gamma^2 I_n & F^{\mathrm{T}}P \\ \star & \star & -P \end{bmatrix} \preccurlyeq 0, \quad (21)$$

其中$D = PL$, 则有:

1) 如果区间观测器(9)的参数满足假设5, 那么式(9)是满足性能指标(19)的原坐标系下的区间观测器.

2) 如果区间观测器(12)的参数满足假设6, 那么(12)是满足性能指标(19)的坐标变换下的区间观测器.

与此同时, 通过求解以下优化问题:

$$\begin{aligned} &\min_{P,D}\ \gamma^2, \\ &\text{s.t. 式(21)},\ \gamma > 0, \end{aligned} \quad (22)$$

计算得出最优观测器增益矩阵

$$L = P^{-1}D. \quad (23)$$

证　结合式(18)和式(20)可以得到

$$[(A - LC)e_k + F\delta_{i,k}]^{\mathrm{T}} P[(A - LC)e_k + F\delta_{i,k}] - e_k^{\mathrm{T}} P e_k + e_k^{\mathrm{T}} e_k \leqslant \gamma^2 \delta_{i,k}^{\mathrm{T}} \delta_{i,k},\ i = 1, 2. \quad (24)$$

当且仅当存在$P \succ 0$和$\gamma > 0$使得

$$\begin{bmatrix} (A\text{–}LC)^{\mathrm{T}}P(A\text{–}LC)\text{–}P\text{+}I_n & (A\text{–}LC)^{\mathrm{T}}PF \\ \star & F^{\mathrm{T}}PF\text{–}\gamma^2 I_n \end{bmatrix} \preccurlyeq 0 \quad (25)$$

时, 不等式(24)成立.

式(25)可以进一步表示成以下形式:

$$\begin{bmatrix} -P + I_n & 0 \\ 0 & -\gamma^2 I_n \end{bmatrix} + \begin{bmatrix} (A - LC)^{\mathrm{T}}P \\ F^{\mathrm{T}}P \end{bmatrix} \times P^{-1}[P(A - LC)\ \ PF] \preccurlyeq 0. \quad (26)$$

最后, 由Schur补引理[24]可以得到

$$\begin{bmatrix} -P + I_n & 0 & A^{\mathrm{T}}P - C^{\mathrm{T}}L^{\mathrm{T}}P \\ \star & -\gamma^2 I_n & F^{\mathrm{T}}P \\ \star & \star & -P \end{bmatrix} \preccurlyeq 0, \quad (27)$$

显然, 式(27)可以写成式(21).

综上所述, 定理4得证.　　证毕.

注 4　定理4给出了通过求解优化问题(22)得到的观测增益L能否作为原坐标系或坐标变换下区间观测器增益的条件, 即假设5或6是否满足. 在保证(9)或(12)是区间观测器的条件下, 若要求解最优区间观测器增益L, 需要把假设5或6的条件作为约束加入到优化问题(22).

4　仿真

考虑遭受隐蔽式攻击的离散线性系统(1)(3), 给定矩阵A和C如下:

$$A = \begin{bmatrix} 0.5 & -1.1 \\ 0 & 0.16 \end{bmatrix},\ C = [0.1\ \ 1].$$

此外, 假设有界过程噪声为$\omega_k = 0.1\begin{bmatrix} \sin(0.5k) \\ \cos(0.5k) \end{bmatrix}$, 有界量测噪声为$\upsilon_k = 0.1\sin k$. 那么, 假设2和3中噪声边界为$\bar{\omega}_k = -\underline{\omega}_k = \begin{bmatrix} 0.1 \\ 0.1 \end{bmatrix}$和$\vartheta = 0.1$. 根据注2, 显然$A$符合假设4. 根据式(6)给出的攻击信号的上界$\bar{a}_k$和下界$\underline{a}_k$的表达式, 选择隐蔽式攻击信号$a_k = \dfrac{\bar{a}_k + \underline{a}_k}{2}$. 系统的初始状态和观测器的初始值选择如下:

$$x_0 = \begin{bmatrix} 1 \\ 2 \end{bmatrix},\ \underline{x}_0 = \begin{bmatrix} 0.5 \\ 1.5 \end{bmatrix},\ \bar{x}_0 = \begin{bmatrix} 1.5 \\ 2.5 \end{bmatrix}.$$

求解优化问题(22), 可计算出$\gamma_{\min} = 6.2$, 得到的增益矩阵L如下:

$$L = \begin{bmatrix} -0.9599 \\ 0.1532 \end{bmatrix}.$$

根据增益矩阵L, 容易计算出$A-LC$是Schur的但不是非负的, 即原坐标系下的区间观测器不可用. 因此, 需要利用坐标变换的方法设计区间观测器.

为了使$R(A-LC)R^{-1}$非负, 选取变换矩阵

$$R=\begin{bmatrix}0.9942 & -0.2350\\ 0.0264 & 1.0213\end{bmatrix}.$$

坐标变换下的区间观测器的仿真结果如图1−6所示.

从图1和图2可以看出, 在无噪声和攻击时, 上、下区间观测值$\bar{x}_k$和$\underline{x}_k$逐渐收敛到真实状态.

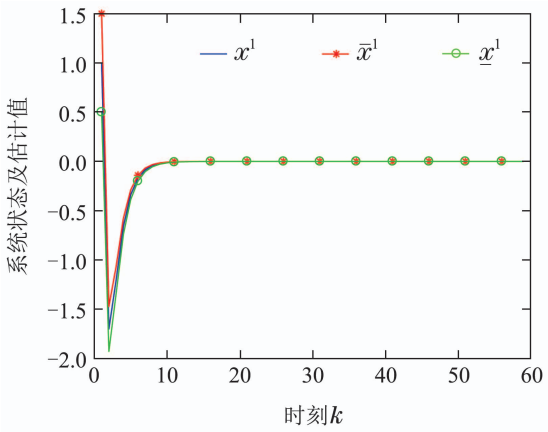

图 1 无噪声且无攻击时系统状态x^1及其区间估计值$\bar{x}^1$, $\underline{x}^1$

Fig. 1 State x^1 and its estimation $\bar{x}^1$, $\underline{x}^1$ without noise and attack

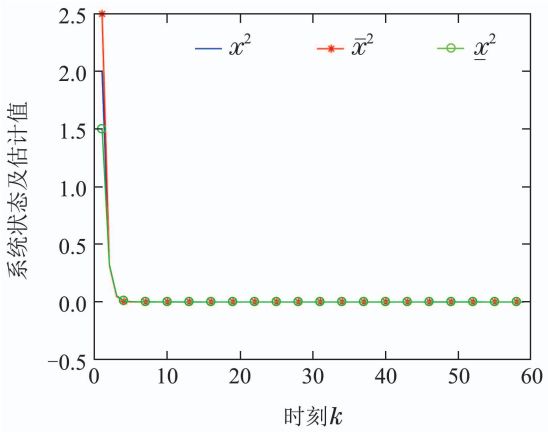

图 2 无噪声且无攻击时系统状态x^2及其区间估计值$\bar{x}^2$, $\underline{x}^2$

Fig. 2 State x^2 and its estimation $\bar{x}^2$, $\underline{x}^2$ without noise and attack

图3和图4表明, 在系统受到过程噪声、量测噪声和隐蔽式攻击影响的情况下, 设计的坐标变换下的区间观测器仍能有效地估计系统状态, 估计误差$\bar{x}_k^1-\underline{x}_k^1$和$\bar{x}_k^2-\underline{x}_k^2$分别收敛到4.3259和0.5920.

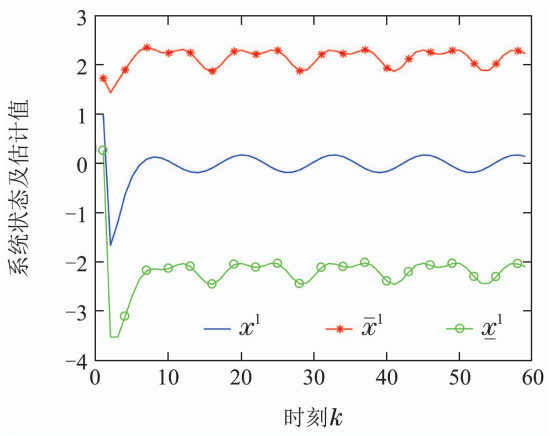

图 3 有噪声且有攻击时系统状态x^1及其区间估计值$\bar{x}^1$, $\underline{x}^1$

Fig. 3 State x^1 and its estimation $\bar{x}^1$, $\underline{x}^1$ with noise and attack

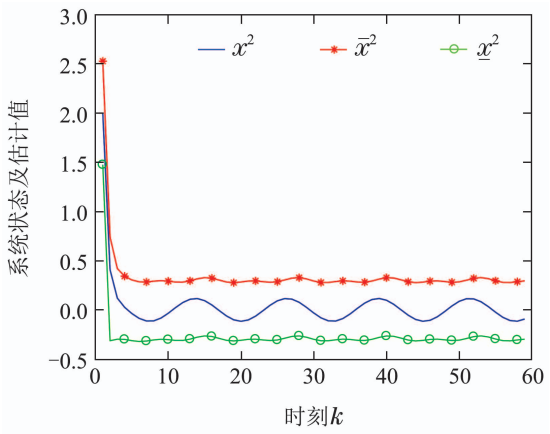

图 4 有噪声且有攻击时系统状态x^2及其区间估计值$\bar{x}^2$, $\underline{x}^2$

Fig. 4 State x^2 and its estimation $\bar{x}^2$, $\underline{x}^2$ with noise and attack

仅受噪声影响的情况如图5和图6所示, 估计误差$\bar{x}_k^1-\underline{x}_k^1$和$\bar{x}_k^2-\underline{x}_k^2$分别收敛到1.1292和0.2678, 比系统受到攻击的情况要小.

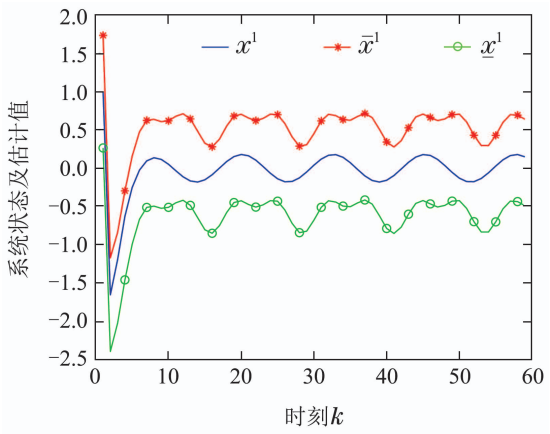

图 5 有噪声且无攻击时系统状态x^1及其区间估计值$\bar{x}^1$, $\underline{x}^1$

Fig. 5 State x^1 and its estimation $\bar{x}^1$, $\underline{x}^1$ with noise and without attack

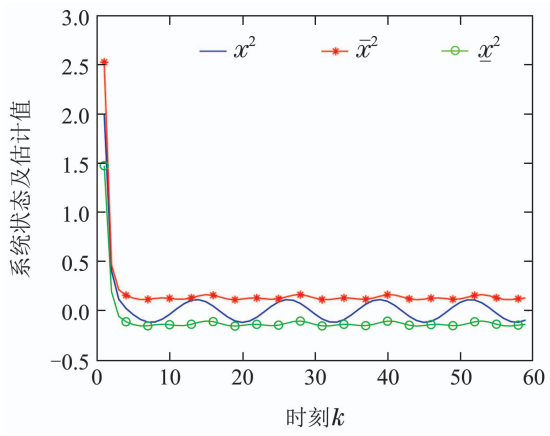

图 6 有噪声且无攻击时系统状态x^2及其区间估计值$\bar{x}^2$, $\underline{x}^2$

Fig. 6 State x^2 and its estimation $\bar{x}^2$, $\underline{x}^2$ with noise and without attack

5 结论

本文研究了隐蔽式攻击下的NCS安全问题. 首先, 在存在未知有界噪声的情况下, 依据攻击者可以保持隐蔽的条件, 给出了攻击信号的上、下界. 其次, 基于边界信息, 本文用两种方法设计了区间观测器: 其一是基于原坐标系的区间观测器设计方法, 直接构造增益矩阵; 其二是通过坐标变换对区间观测器的设计条件进行放宽处理, 这种方法更容易获得满足设计条件的增益矩阵. 然后, 基于H_∞滤波理论给出了可以获得最优观测器增益的线性矩阵不等式条件. 最后, 通过仿真实例验证了所提方法的有效性. 未来研究工作可以考虑把本文成果扩展到多传感器NCS[25]或云控制系统[26].

参考文献:

[1] GUPTA R A, CHOW M Y. Networked control system: Overview and research trends. *IEEE Transactions on Industrial Electronics*, 2010, 57(7): 2527 – 2535.

[2] LIU K, SELIVANOV A, FRIDMAN E. Survey on time-delay approach to networked control. *Annual Reviews in Control*, 2019, 48: 57 – 79.

[3] ZHAN Xisheng, WU Jie, GUAN Zhihong, et al. Stability analysis of networked system based on packet dropouts and bandwidth constraints. *Control Theory & Applications*, 2014, 31(8): 1111 – 1115.
(詹习生, 吴杰, 关治洪, 等. 基于丢包和带宽限制网络化系统稳定性分析. 控制理论与应用, 2014, 31(8): 1111 – 1115.)

[4] TEIXEIRA A, SOU K C, SANDBERG H, et al. Secure control systems: a quantitative risk management approach. *IEEE Control Systems Magazine*, 2015, 35(1): 24 – 45.

[5] DING D R, HAN Q L, XIANG Y, et al. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 2018, 275(1): 1674 – 1683.

[6] WU Yiming, DING Jiajun, HE Xiongxiong, et al. Secure consensus control for multi-agent systems under communication delay. *Control Theory & Applications*, 2016, 33(8): 1039 – 1045.
(伍益明, 丁佳骏, 何熊熊, 等. 通信时延下多智能体系统的安全一致性控制. 控制理论与应用, 2016, 33(8): 1039 – 1045.)

[7] GIRALDO J, URBINA D, CARDENAS A, et al. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys (CSUR)*, 2018, 51(4): 76.

[8] MOUSAVINEJAD E, YANG F, HAN Q L, et al. A novel cyber attack detection method in networked control systems. *IEEE Transactions on Cybernetics*, 2018, 48(11): 3254 – 3264.

[9] LU Genghong, FENG Dongqin. Industrial control system network security situation awareness modeling and algorithm implementation. *Control Theory & Applications*, 2016, 33(8): 1054 – 1060.
(陆耿虹, 冯冬芹. 工控网络安全态势感知算法实现. 控制理论与应用, 2016, 33(8): 1054 – 1060.)

[10] MO Y L, SINOPOLI B. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Transactions on Automatic Control*, 2016, 61(9): 2618 – 2624.

[11] CHEN Y, KAR S, MOURA J M F. Optimal attack strategies subject to detection constraints against cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 2018, 5(3): 1157 – 1168.

[12] PASQUALETTI F, DÖRFLER F, BULLO F. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2013, 58(11): 2715 – 2729.

[13] CHEN Y, KAR S, MOURA J M F. Dynamic attack detection in cyber-physical systems with side initial state information. *IEEE Transactions on Automatic Control*, 2017, 62(9): 4618 – 4624.

[14] BAI C Z, GUPTA V, PASQUALETTI F. On Kalman filtering with compromised sensors: attack stealthiness and performance bounds. *IEEE Transactions on Automatic Control*, 2017, 62(12): 6641 – 6648.

[15] ZHANG Q R, LIU K, XIA Y Q, et al. Optimal stealthy deception attack against cyber-physical systems. *IEEE Transactions on Cybernetics*, 2019, doi: 10.1109/TCYB.2019.2912622.

[16] WANG Y, BEVLY D M, RAJAMANI R. Interval observer design for LPV systems with parametric uncertainty. *Automatica*, 2015, 60(10): 79 – 85.

[17] EFIMOV D, RAÏSSI T, CHEBOTAREV S, et al. Interval state observer for nonlinear time varying systems. *Automatica*, 2013, 49(1): 200 – 205.

[18] WANG Z, LIM C C, SHEN Y. Interval observer design for uncertain discrete-time linear systems. *Systems & Control Letters*, 2018, 116(6): 41 – 46.

[19] EFIMOV D, PERRUQUETTI W, RAÏSSI T, et al. Interval observers for time-varying discrete-time systems. *IEEE Transactions on Automatic Control*, 2013, 58(12): 3218 – 32.

[20] ZHANG X, ZHU F, GUO S. Actuator fault detection for uncertain systems based on the combination of the interval observer and asymptotical reduced-order observer. *International Journal of Control*, 2019, doi: 10.1080/00207179.2019.1620329.

[21] XU F, TAN J, WANG X, et al. Conservatism comparison of set-based robust fault detection methods: Set-theoretic UIO and interval observer cases. *Automatica*, 2019, 105(7) : 307 – 313.

[22] EFIMOV D, FRIDMAN L, RAÏSSI T, et al. Interval estimation for LPV systems applying high order sliding mode techniques. *Automatica*, 2012, 48(9): 2365 – 2371.

[23] XU S, LAM J. *Robust Control and Filtering of Singular Systems*. Berlin, Germany: Springer, 2006.

[24] BOYD S, EL GHAOUI L, FERON E, et al. *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, USA: SIAM, 1994.

[25] LIU K, GUO H, ZHANG Q R, et al. Distributed secure filtering for discrete-time systems under Round-Robin protocol and deception attacks. *IEEE Transactions on Cybernetics*, 2019, doi: 10.1109/TCYB.2019.2897366.

[26] XIA Yuanqing. Cloud control systems and their challenges. *Acta Automatica Sinica*, 2016, 42(1): 1 – 12.
(夏元清. 云控制系统及其面临的挑战. 自动化学报, 2016, 42(1): 1 – 12.)

作者简介:

刘 坤 研究员, 目前研究方向为网络化控制理论与应用、复杂网络控制与安全等, E-mail: kunliubit@bit.edu.cn;

张淇瑞 博士研究生, 目前研究方向为信息物理系统的安全控制、最优化控制等, E-mail: qiruizhang@bit.edu.cn;

郭 航 硕士研究生, 目前研究方向为网络化控制系统的安全控制与滤波, E-mail: hangguo1994@gmail.com;

刘 涛 讲师, 目前研究方向为网络安全、离散时间系统等, E-mail: liutao19832001@163.com;

夏元清 教授, 目前研究方向为网络化信息处理与控制、云控制、空天地网络化协同控制等, E-mail: xia_yuanqing@bit.edu.cn.