软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(6):1672−1680 [doi: 10.13328/j.cnki.jos.006000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

马尔可夫信息物理系统拒绝服务攻击安全控制*

马 超[1,2], 吴 伟[2]

[1](北京科技大学 自动化学院,北京 100083)

[2](复杂系统管理与控制国家重点实验室(中国科学院 自动化研究所),北京 100190)

通讯作者: 吴伟, E-mail: wei.wu@ia.ac.cn

摘 要: 研究了马尔可夫跳变信息物理系统(CPS)在模态依赖拒绝服务(DoS)攻击下的安全控制问题.提出了一种模态依赖事件触发策略来减少网络资源消耗.特别地,DoS 攻击被设置为依赖系统模态,从而更贴近实际的应用.基于 Lyapunov Krasovskii 泛函方法建立了闭环系统在 DoS 攻击下渐近一致有界的充分性条件.更进一步,根据矩阵技术设计了所需的安全控制器.最后,通过一个实例说明了该方法的有效性.

关键词: 安全控制;事件触发控制;马尔可夫跳变信息物理系统;拒绝服务攻击

中图法分类号: TP311

中文引用格式: 马超,吴伟.马尔可夫信息物理系统拒绝服务攻击安全控制.软件学报,2020,31(6):1672−1680. http://www.jos.org.cn/1000-9825/6000.htm

英文引用格式: Ma C, Wu W. Event-triggering secure control of Markov jump cyber-pysical systems under mode-dependent denial of service attacks. Ruan Jian Xue Bao/Journal of Software, 2020,31(6):1672−1680 (in Chinese). http://www.jos.org.cn/1000-9825/6000.htm

Event-triggering Secure Control of Markov Jump Cyber-Pysical Systems Under Mode-dependent Denial of Service Attacks

MA Chao[1,2], WU Wei[2]

[1](School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China)

[2](State Key Laboratory for Management and Control of Complex Systems (Institute of Automation, Chinese Academy of Sciences), Beijing 100190, China)

Abstract: This study investigates the secure control problem of Markov jump cyber-physical systems (CPS) under mode-dependent denial of service (DoS) attacks. A novel mode-dependent event-triggering strategy is adopted to reduce the network resource consumptions. In particular, the DoS attacks are supposed to be mode-dependent for more practical applications. The Lyapunov-Krasovskii functional method is utilized to establish the sufficient conditions such that the resulting closed-loop system can be uniformly ultimately bounded under DoS attacks. Furthermore, the desired secure controller can be designed in terms of matrix techniques. Finally, an illustrative example is presented to demonstrate the effectiveness of the theoretical method.

Key words: secure control; event-triggering control; Markov jump cyber-physical system; denial of service attack

近年来,伴随着信息与网络技术的飞速发展,信息物理系统成为了一个热门的研究领域[1,2].信息物理系统在实际应用中的例子包括智能电网[3]、智能运输系统[4]、智能工厂[5]等.特别是由于信息物理系统中通信网络组件的使用,信息物理系统的安全控制问题受到了研究学者的广泛关注.一般而言,当信息物理系统中的传感器

* 基金项目: 国家自然科学基金(61703038, 61627808, 9164820); 中央高校基本科研业务费专项资金(FRF-TP-18-034A2)

Foundation item: National Natural Science Foundation of China (61703038, 61627808, 9164820); Fundamental Research Funds for the Central Universities (FRF-TP-18-034A2)

本文由“信息物理系统软件设计自动化”专题特约编辑卜磊教授、陈铭松教授、朱祺教授、刘超教授推荐.

收稿时间: 2019-08-24; 修改时间: 2019-10-23; 采用时间: 2020-01-13; jos 在线出版时间: 2020-04-18

或者通信网络受到恶意攻击后,信息物理系统将无法按照正常系统状态进行控制,从而导致控制系统的性能下降甚至不稳定[6−8].常见的网络攻击类型主要有拒绝服务攻击[9]、重放攻击[10]以及欺骗攻击[11].近年来,拒绝服务攻击作为一种典型的恶意攻击手段被大量应用于网络系统,其主要方式为阻塞信息的正常通信.因此,针对拒绝服务攻击的特点,一些有效的安全控制及调度策略被提出,并且取得了良好的控制效果[12−14].此外,考虑到信息物理系统中存在的通信资源约束,基于事件触发的通信与控制策略被大量采用.与传统的基于时间触发策略不同,基于事件触发的策略可以按照给定的事件触发机制大量地减少信息传递的次数,从而提高通信资源的利用率[15−17].

另一方面,作为一类特殊的切换系统,马尔可夫跳变系统通常用来描述具有不同模态切换特性的实际物理系统[18].许多针对马尔可夫跳变系统的分析与综合方法被提出,用来解决稳定性问题[19]、状态估计问题[20]、同步问题[21]等.需要指出的是:大多数针对信息物理系统的建模通常基于系统参数及状态非跳变假设,相应的结果仍然具有一定的保守性.目前,对于马尔可夫跳变类型信息物理系统的研究尚处于起步阶段,例如文献[22]通过利用自适应滑模控制方法成功解决了马尔可夫跳变类型信息物理系统在对抗攻击下的安全控制问题等,然而在其他类型网络攻击下的安全控制问题仍然具有相当的挑战性[23,24].

针对以上不足,本文主要研究了一类马尔可夫跳变信息物理系统在拒绝服务攻击下的安全控制问题.与已有的文献相比较,本文的贡献主要包括以下 3 个方面.

(1) 考虑到马尔可夫跳变信息物理系统的跳变特性,建立了一种新的模态依赖安全控制模型,从而更好地模拟实际网络攻击的模式;

(2) 提出了一种新颖的模态依赖事件触发控制策略,用来解决网络攻击下的安全控制问题;

(3) 利用凸优化的方法建立了实现安全控制所需要的充分性条件,并且给出了相应的事件触发函数与安全控制器的设计过程.

本文第 1 节首先给出马尔可夫跳变信息物理系统的模型与安全控制问题的数学描述,并且设计了模态依赖的事件触发函数与控制器.第 2 节给出相应的充分性条件以及数学推导过程.第 3 节通过一个数值仿真的例子说明本文所提出设计方法的有效性与适用性.第 4 节对本文研究工作进行总结并给出未来研究工作的一些展望.

本文采用下列统一的数学符号:R^n 表示实数域 n 维向量空间,$R^{m\times n}$ 表示实数域 $m\times n$ 矩阵空间,$P>0$ 表示矩阵 P 是正定的,$\mathbb{E}\{\cdot\}$表示随机过程的数学期望,*表示对称矩阵中的对称部分.

1 预备知识与问题描述

1.1 马尔可夫跳变信息物理系统数学模型

固定概率空间为(Ω,F,P),考虑下列连续时间马尔可夫跳变信息物理系统,其动力学模型为

$$\dot{x}(t)=A(\sigma(t))x(t)+B(\sigma(t))u(t) \tag{1}$$

其中,$x(t)\in R^n$ 为系统的状态向量,$u(t)\in R^m$ 为系统的控制输入,$A(\sigma(t))$与 $B(\sigma(t))$均为模态$\sigma(t)$下的已知常量矩阵.不失一般性,假设系统的任意模态均为可检测的,并且系统的初始状态假定为:$x(0)=x_0$.

$\sigma(t)$表示连续时间离散状态的马尔可夫过程,其取值在一个有限的集合 $I=\{1,2,\ldots,N\}$内.相应的,其状态转移概率矩阵$\Pi=\{\pi_{ij}\},\forall i,j\in I$ 被描述为

$$\Pr(\sigma(t+\Delta t)=j:\sigma(t)=i)=\begin{cases}\pi_{ij}\Delta t+o(\Delta t), & \text{if } i\neq j\\ 1+\pi_{ii}\Delta t+o(\Delta t), & \text{if } i=j\end{cases} \tag{2}$$

其中,$\pi_{ij}\geqslant 0$ 表示从 t 时刻模态 i 跳变到从 $t+\Delta t$ 时刻模态 j 的转移概率, $\pi_{ii}=-\sum_{j=1,\,j\neq i}^{N}\pi_{ij}$,$\Delta t>0$,$o(\Delta t)$表示Δt 的高阶无穷小, $\lim_{t\to\infty}o(\Delta t)/\Delta t=0$.

1.2 模态依赖事件触发的安全控制器设计

在实际应用中,拒绝服务攻击通常难以预测.当攻击发生以后,安全控制器可以确保系统在一定的安全性能下稳定的运行.在事件触发策略下,假定系统的传感器按照时间序列采样传输的,其采样周期为 h,其采样序列为 $S_1=\{0,h,2h,3h,\dots,kh,(k+1)h,\dots\}$.不失一般性,当前控制信息成功更新时刻(事件触发时刻)定义为 t_kh,且下一个成功更新时刻定义为 $t_{k+1}h$,其更新序列为 $S_2=\{0,t_1h,t_2h,t_3h,\dots,t_kh,t_{k+1}h,\dots\}$.

此外,定义$\varepsilon(i_kh)$为拒绝服务攻击的发生:

$$\varepsilon(i_kh)=\begin{cases}0, & \text{拒绝服务攻击未发生}\\ 1, & \text{拒绝服务攻击发生}\end{cases},$$

其中,i_kh 为第 k 个控制信息成功更新间隔内的传感器采样时刻,即 $t_kh=i_kh<t_{k+1}h$.

更进一步,定义拒绝服务攻击的持续时间为

$$\Delta_{t_{k+1}h}^{DoS}=t_{t_{k+1}h}^{DoS}-t_{k+1}h, t_{t_{k+1}h}^{DoS}\geqslant t_{k+1}h,$$

其中,$t_{t_{k+1}h}^{DoS}$ 表示能量有限的拒绝服务攻击发生情况下的控制信息成功更新时刻.

此外,定义 i_kh 时刻拒绝服务攻击发生情况下的马尔可夫跳变信息物理系统状态误差为 $e(i_kh)=x(i_kh)-x(t_kh)$,从而可以设计下列模态依赖的事件触发策略:

$$t_{k+1}h=t_kh+\min(i_kh\mid \delta x^T(t_k)\Phi_1(\sigma(t))x(t_k)-e^T(i_kh)\Phi_2(\sigma(t))e(i_kh)+\varepsilon(i_kh)\Psi(\Delta_{t_{k+1}h}^{DoS})) \tag{3}$$

其中,

- δ为模态依赖的阈值参数;
- $\Phi_1(\sigma(t))$与$\Phi_2(\sigma(t))$为模态依赖的常量矩阵;
- $\Psi(\Delta_{t_{k+1}h}^{DoS})=(x(i_kh)-x(t_{k+1}h))^T\Phi(x(i_kh)-x(t_{k+1}h))$,$\Phi>0$ 表示由拒绝服务攻击引起的附加误差函数.

在此基础上,可以设计下面的模态依赖状态反馈控制器:

$$u(t)=K(\sigma(t))x(t_kh), t_kh\leqslant t<t_{k+1}h \tag{4}$$

其中,$K(\sigma(t))\in R^{m\times n}$ 为待求的模态依赖状态反馈增益矩阵.

将上述设计的状态反馈控制器带入信息物理系统,可以进一步得到闭环系统的状态方程为

$$\dot{x}(t)=A(\sigma(t))x(t)+B(\sigma(t))K(\sigma(t))x(t_kh), t_kh\leqslant t<t_{k+1}h \tag{5}$$

为了方便描述上述方程,采用下标 i 来描述$\sigma(t)$.因此,系统(5)可以进一步写成下面的形式:

$$\dot{x}(t)=A_ix(t)+B_iK_ix(t_kh), t_kh\leqslant t<t_{k+1}h \tag{6}$$

值得注意的是,本文中的事件触发控制机制考虑了模态变化对于事件触发函数以及控制器的影响,因此具有更加广泛的适用性.此外,考虑到拒绝服务攻击具有针对性地对于信息物理系统的不同模态进行不同的攻击方式,本文所提出的模态依赖拒绝服务攻击也具有更加实际的背景.

1.3 控制目标

根据上述结果,本文的控制目标是:当拒绝服务攻击发生时,马尔可夫跳变信息物理系统(1)可以确保具有均方意义下渐近一致有界,即确保零初始系统的控制性能损失在安全控制器的作用下满足一定的指标 J_{DoS},即 $\|x(t)\|\leqslant J_{DoS}$,其中,$\|x(t)\|$表示 x 的欧几里德范数.

2 控制算法设计

在本节中,首先通过建立合适的 Lyapunov-Krasovskii 泛函给出了实现安全控制性能的充分性条件,进而通过矩阵变换的方法求解模态依赖安全控制器的有效增益.

定理 1. 给定信息物理系统(1)与相应的事件触发安全控制器增益(4),如果存在模态依赖矩阵 $P_i>0$,矩阵 $R>0$,当满足下列线性矩阵不等式条件$\Xi_i<0$ 时,系统可以在拒绝服务攻击发生时控制性能损失满足指标:

$$J_{DoS}=\frac{\varepsilon(i_k h)\Psi(\Delta_{i_{k+1}h}^{DoS})}{\kappa\lambda_{\min}(P_i)},$$

其中,

$$\Xi_i=\begin{bmatrix}\Xi_{1i} & \Xi_{2i}\\ * & \Xi_{3i}\end{bmatrix},$$

$$\Xi_{1i}=2P_iA_i+2P_iB_iK_i+\delta\Phi_{1i}+\sum_{i=1}^{N}\pi_{ij}P_j,$$

$$\Xi_{2i}=[-P_iB_iK_i-\delta\Phi_{1i}\quad -P_iB_iK_i-\delta\Phi_{1i}\quad hA_i^TR+hK_i^TB_i^TR],$$

$$\Xi_{3i}=\begin{bmatrix}-R+\delta\Phi_{1i} & \delta\Phi_{1i} & -hK_i^TB_i^TR\\ * & -\Phi_{2i}+\delta\Phi_{1i} & -hK_i^TB_i^TR\\ * & * & -R\end{bmatrix}.$$

证明:对于闭环系统(6),采用虚拟时滞方法[25]可以得到:

$$\dot{x}(t)=A_ix(t)+B_iK_i(x(t-d(t))-e(i_kh)),t_kh\leqslant t<t_{k+1}h \tag{7}$$

其中,$d(t)=t-i_kh$ 为虚拟时滞并且满足条件:$0\leqslant d(t)<h$.

对应给定的模态$\sigma(t)=i$,构造下列模态依赖 Lyapunov-Krasovskii 泛函:

$$V(t)=\sum_{k=1}^{2}V_k(t),$$

其中,

$$V_1(t)=x^T(t)P_ix(t),$$

$$V_2(t)=h\int_{-h}^{0}\int_{t+\theta}^{t}\dot{x}^T(s)R\dot{x}(s)\mathrm{d}s\mathrm{d}\theta.$$

此外,定义弱无穷小算子为

$$\mathcal{L}V(t)=\lim_{\Delta t\to\infty}\frac{1}{\Delta t}\mathbb{E}\{V(t+\Delta t,i)\,|\,t-V(t)\}.$$

对系统(6)进行计算可以得到:

$$\begin{aligned}\mathcal{L}V_1(t)&=\dot{x}^T(t)P_ix(t)+x^T(t)P_i\dot{x}(t)+\sum_{i=1}^{N}\pi_{ij}x^T(t)P_jx(t)\\&=2x^T(t)P_i\dot{x}(t)+\sum_{i=1}^{N}\pi_{ij}x^T(t)P_jx(t)\\&=2x^T(t)P_iA_ix(t)+2x^T(t)P_iB_iK_ix(t)-2x^T(t)P_iB_iK_i\int_{t-d(t)}^{t}\dot{x}^T(s)\mathrm{d}s\\&\quad-2x^T(t)P_iB_iK_ie(i_kh))+\sum_{i=1}^{N}\pi_{ij}x^{\tau}(t)P_jx(t),\end{aligned}$$

$$\begin{aligned}\mathcal{L}V_2(t)&=h^2\dot{x}^T(t)R\dot{x}(t)-h\int_{t-h}^{t}\dot{x}^T(s)R\dot{x}(s)\mathrm{d}s\\&\leqslant h^2\dot{x}^T(t)R\dot{x}(t)-h\int_{t-h}^{t}\dot{x}^T(s)\mathrm{d}sR\int_{t-h}^{t}\dot{x}(s)\mathrm{d}s\\&\leqslant h^2\dot{x}^T(t)R\dot{x}(t)-h\int_{t-d(t)}^{t}\dot{x}^T(s)\mathrm{d}sR\int_{t-d(t)}^{t}\dot{x}(s)\mathrm{d}s.\end{aligned}$$

此外,可以根据事件触发函数进一步得到:

$$e^T(i_kh)\Phi_{2i}(\sigma(t))e(i_kh)\leqslant\delta(\sigma(t))x^T(t_k)\Phi_{1i}(\sigma(t))x(t_k)+\varepsilon(i_kh)\Psi(\Delta_{t_{k+1}h}^{DoS}).$$

从而有:

$$\mathcal{L}V(t)\leqslant\eta^T(t)\Xi\eta(t)+\varepsilon(i_kh)\Psi(\Delta_{t_{k+1}h}^{DoS}),$$

其中,$\eta(t)=\left[x^T(t),\int_{t-d(t)}^{t}\dot{x}^T(s)\mathrm{d}s,e^T(i_kh)\right]^T$,$\Xi_i$ 在定理 1 中给定.

由上式可知存在一个参数κ>0,从而可以得到:

$$\mathcal{L}V(t) \leqslant -\kappa V(t) + \varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS}).$$

从而有:

$$x^T(t)P_i x(t) \leqslant V(t) \leqslant V(0) + \frac{\varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS})}{\kappa}.$$

最终可以得到:

$$\| x(t) \| \leqslant \sqrt{\frac{V(0) + \dfrac{\varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS})}{\kappa}}{\lambda_{\min}(P_i)}}.$$

综上所述,可以发现性能损失主要与 $\dfrac{\varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS})}{\kappa\lambda_{\min}(P_i)}$ 有关,从而得到:

$$J_{DoS} = \frac{\varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS})}{\kappa\lambda_{\min}(P_i)}.$$

证明完毕. □

在定理 1 得到结果的基础上,下面的定理将给出模态依赖安全控制器增益的设计过程.

定理 2. 给定信息物理系统(1)与相应的事件触发安全控制器(4),如果存在模态依赖矩阵 $\bar{P}_i > 0$,S_i,矩阵 $\bar{R} > 0$,当满足下列线性矩阵不等式条件 $\bar{\Xi}_i < 0$ 时,系统可以在拒绝服务攻击发生时控制性能损失满足指标:

$$J_{DoS} = \frac{\varepsilon(i_k h)\Psi(\Delta_{t_{k+1}h}^{DoS})}{\kappa\lambda_{\min}(P_i)},$$

其中,

$$\bar{\Xi}_i = \begin{bmatrix} \bar{\Xi}_{1i} & \bar{\Xi}_{2i} \\ * & \bar{\Xi}_{3i} \end{bmatrix},$$

$$\bar{\Xi}_{1i} = \begin{bmatrix} 2A_i\bar{P}_i + 2B_iS_i + \delta\bar{\Phi}_{1i} + \pi_{ii}\bar{P}_i & -B_iS_i - \delta\bar{\Phi}_{1i} & -B_iS_i - \delta\bar{\Phi}_{1i} \\ * & -\bar{R} + \delta\bar{\Phi}_{1i} & \delta\bar{\Phi}_{1i} \\ * & * & -\bar{\Phi}_{2i} + \delta\bar{\Phi}_{1i} \end{bmatrix},$$

$$\bar{\Xi}_{2i} = \begin{bmatrix} h\bar{P}_iA_i^T + hS_i^TB_i^T & \sqrt{\pi_{i1}}\bar{P}_i & \cdots & \sqrt{\pi_{iN}}\bar{P}_i \\ -hS_i^TB_i^T & 0 & \cdots & 0 \\ -hS_i^TB_i^T & \vdots & \ddots & \vdots \end{bmatrix},$$

$$\bar{\Xi}_{3i} = \begin{bmatrix} \bar{R} - 2\bar{P}_i & 0 & \ddots & 0 \\ * & -\bar{P}_1 & \ddots & 0 \\ * & * & \ddots & 0 \\ * & * & * & -\bar{P}_N \end{bmatrix}.$$

当上述条件满足时,事件触发安全控制器(4)的模态依赖增益可以根据以下计算求解:

$$K_i = S_i\bar{P}_i^{-1}.$$

证明:针对矩阵Ξ_i<0 进行全等变换,令 $\bar{P}_i = P_i^{-1}$,$\bar{R} = P_i^{-1}RP_i^{-1}$,$\bar{\Phi}_{1i} = P_i^{-1}\Phi_{1i}P_i^{-1}$,$\bar{\Phi}_{2i} = P_i^{-1}\Phi_{2i}P_i^{-1}$,并且有 $K_i\bar{P}_i^{-1} = S_i$,则可以根据定理 1 的证明得到上述结果. □

3 仿真验证

本节通过一个仿真例子来验证所设计控制算法的有效性,需要指出的是,本文提出的算法对于线性马尔可夫信息物理系统具有一定的通用性与适用性.

考虑下列负载根据马尔可夫链变化的 RLC 电路模型,如图 1 所示.

$$\frac{dI_L(t)}{dt}=\frac{u-u_c(t)-I_L(t)}{L_i},\frac{du_c(t)}{dt}=\frac{I_L(t)}{C_i}.$$

令 $x(t)=[u_c(t),I_L(t)]^T$,则有:

$$A_i=\begin{bmatrix}0 & \frac{1}{C_i}\\ -\frac{1}{L_i} & -\frac{R}{L_i}\end{bmatrix},B_i=\begin{bmatrix}0\\ \frac{1}{L_i}\end{bmatrix}.$$

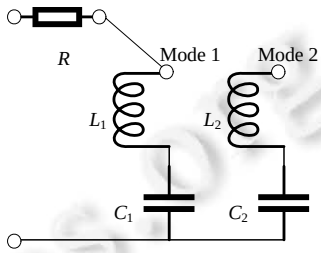

Fig.1 RLC circuit

图 1 RLC 电路

在仿真实验中,假设上述 RLC 电路具有两个不同模态,即两种不同的负载满足马尔可夫链变化,这里使用下列参数:

$$A_1=\begin{bmatrix}0 & \frac{1}{0.5}\\ -\frac{1}{4} & -\frac{0.01}{4}\end{bmatrix},A_2=\begin{bmatrix}0 & \frac{1}{0.8}\\ -\frac{1}{8} & -\frac{0.01}{8}\end{bmatrix},B_1=\begin{bmatrix}0\\ \frac{1}{4}\end{bmatrix},B_2=\begin{bmatrix}0\\ \frac{1}{8}\end{bmatrix},\Pi=\begin{bmatrix}-0.5 & 0.5\\ 0.3 & -0.3\end{bmatrix}.$$

系统的采样周期设定为 h=0.05s,事件触发参数设置为δ=0.1.根据上述参数设置,根据定理 2 的算法可以得到相应的模态依赖安全控制器增益为

$$\kappa_1=[-0.8125\ -0.9496],\kappa_2=[-1.4783\ -1.2428].$$

根据得到的安全控制器参数,并且假设 $\Psi\left(\Delta_{t_{k+1}h}^{DoS}\right)$=10,$\kappa$=0.2,图 2~图 4 分别展示了拒绝服务攻击发生概率为 0.02 时,事件触发间隔示意图与对应的马尔可夫跳变信息物理系统的闭环状态轨迹图.

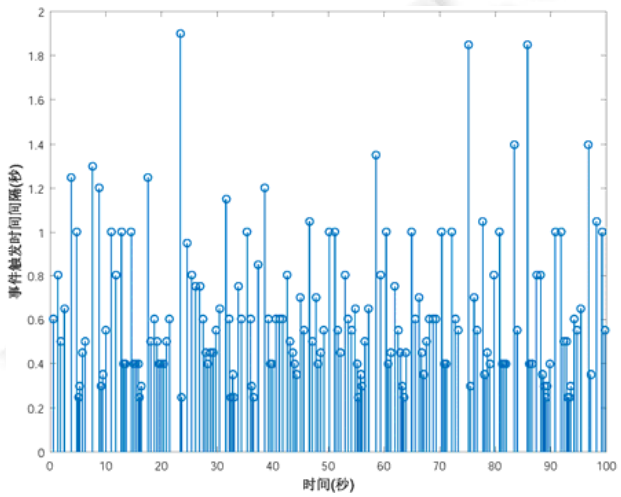

Fig.2 Release intervals of the event-triggered control

图 2 事件触发释放间隔

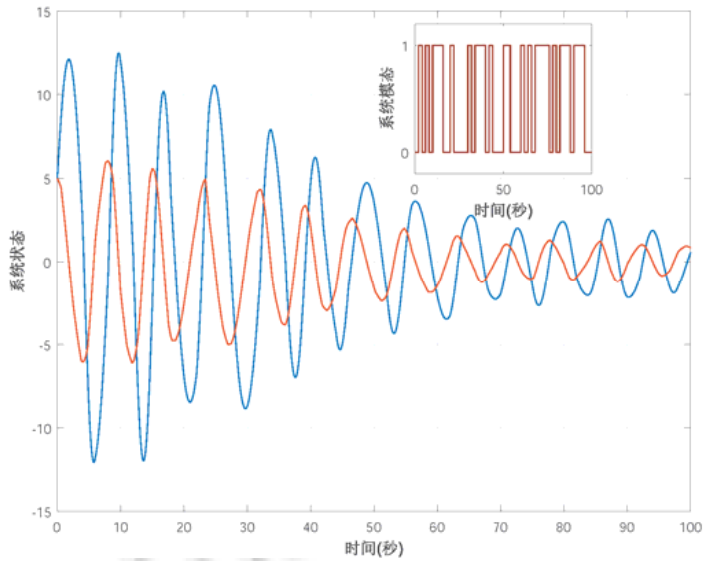

Fig.3 State response of the closed-loop Markov jump cyber-pysical system

图 3 马尔可夫跳变信息物理系统闭环状态轨迹

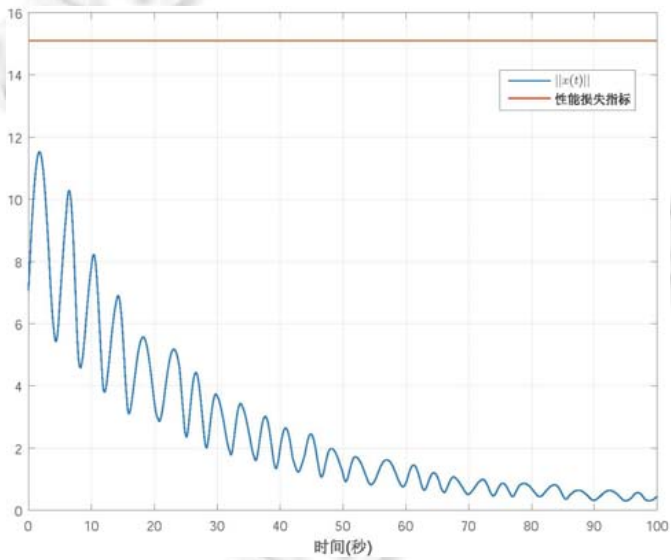

Fig.4 Performance response of the closed-loop Markov jump cyber-pysical system

图 4 马尔可夫跳变信息物理系统性能轨迹

从图 2 可以看出,采用事件触发策略可以降低控制器的更新间隔从而减轻网络负载.同时,从图 3、图 4 可以看到:马尔可夫跳变 RLC 电路在闭环控制作用下最终的系统状态可以收敛在一定范围区间内,即满足第 1.3 节中的控制目标$\|x(t)\|\leqslant J_{DoS}$.综上所述,不难发现:系统可以在安全控制器的作用下有效的满足性能指标,仿真结果支持了理论计算的有效性.

4 结 论

本文研究了一类马尔可夫跳变信息物理系统在拒绝服务攻击下的安全控制问题.特别地,提出了一种新颖

的模态依赖安全控制器设计方法用来应对模态依赖拒绝服务攻击的影响.通过使用凸优化的方法,给出了确保系统的控制性能损失指标的充分性条件.在此基础上,利用矩阵方法设计了模态依赖安全控制器.最后,通过一个 RLC 电路的例子验证了本文所得到理论结果的有效性.未来研究工作将进一步研究通信带宽约束对于信息物理系统安全控制的影响.

References:

[1] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans. on Automatic Control, 2013,58(11): 2715−2729.

[2] Humayed A, Lin J, Li F, *et al*. Cyber-Physical systems security—A survey. IEEE Internet of Things Journal, 2017,4(6):1802−1831.

[3] Chen TM, Sanchez-Aarnoutse JC, Buford J. Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans. on Smart Grid, 2011,2(4):741−749.

[4] Jia D, Lu K, Wang J, *et al*. A survey on platoon-based vehicular cyber-physical systems. IEEE Communications Surveys & Tutorials, 2016,18(1):263−284.

[5] Wang L, Törngren M, Onori M. Current status and advancement of cyber-physical systems in manufacturing. Journal of Manufacturing Systems, 2015,37:517−527.

[6] Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. on Automatic Control, 2014,59(6):1454−1467.

[7] Li Y, Shi L, Cheng P, *et al*. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. IEEE Trans. on Automatic Control, 2015,60(10):2831−2836.

[8] Cao R, Cheng L. Secure control of Euler-Lagrange systems under denial-of-service attacks. Aerospace Control and Application, 2018,44(5):76−80 (in Chinese with English abstract).

[9] Chen B, Ho DW C, Zhang WA, *et al*. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. IEEE Trans. on Systems, Man, and Cybernetics: Systems, 2019,49(2):455−468.

[10] Chen B, Ho DWC, Hu G, *et al*. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. IEEE Trans. on Cybernetics, 2018,48(6):1862−1876.

[11] Miao F, Zhu Q, Pajic M, *et al*. Coding schemes for securing cyber-physical systems against stealthy data injection attacks. IEEE Trans. on Control of Network Systems, 2017,4(1):106−117.

[12] Han S, Xie M, Chen HH, *et al*. Intrusion detection in cyber-physical systems: Techniques and challenges. IEEE Systems Journal, 2014,8(4):1049−1059.

[13] Ding D, Han QL, Xiang Y, *et al*. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 2018,275:1674−1683.

[14] Wells LJ, Camelio JA, Williams CB, *et al*. Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2014,2(2):74−77.

[15] Lu AY, Yang GH. Event-Triggered secure observer-based control for cyber-physical systems under adversarial attacks. Information Sciences, 2017,420:96−109.

[16] Wang D, Wang Z, Shen B, *et al*. Recent advances on filtering and control for cyber-physical systems under security and resource constraints. Journal of the Franklin Institute, 2016,353(11):2451−2466.

[17] Shoukry Y, Tabuada P. Event-Triggered state observers for sparse sensor noise/attacks. IEEE Trans. on Automatic Control, 2016, 61(8):2079−2091.

[18] Shi P, Li F. A survey on Markovian jump systems: Modeling and design. Int'l Journal of Control, Automation and Systems, 2015, 13(1):1−16.

[19] De Farias DP, Geromel JC, Do Val JBR, *et al*. Output feedback control of Markov jump linear systems in continuous-time. IEEE Trans. on Automatic Control, 2000,45(5):944−949.

[20] Shen H, Zhu Y, Zhang L, *et al*. Extended dissipative state estimation for Markov jump neural networks with unreliable links. IEEE Trans. on Neural Networks and Learning Systems, 2017,28(2):346−358.

[21] Yang X, Cao J, Lu J. Synchronization of randomly coupled neural networks with Markovian jumping and time-delay. IEEE Trans. on Circuits and Systems I: Regular Papers, 2013,60(2):363−376.

[22] Chen, B, Niu, Y, Zou, Y. Security control for Markov jump system with adversarial attacks and unknown transition rates via adaptive sliding mode technique. Journal of the Franklin Institute, 2019,356(6):3333−3352.

[23] Yang, K, Wang, R, Jiang, Y, *et al*. Enhanced resilient sensor attack detection using fusion interval and measurement history. In: Proc. of the Int'l Conf. on Hardware/Software Codesign and System Synthesis. IEEE, 2018. 1−3.

[24] Yang K, Wang R, Jiang Y, *et al*. Sensor attack detection using history based pairwise inconsistency. Future Generation Computer Systems, 2018,86:392−402.

[25] Fridman E, Seuret A, Richard JP. Robust sampled-data stabilization of linear systems: an input delay approach. Automatica, 2004, 40(8):1441−1446.

附中文参考文献:

[8] 曹然,程龙.拒绝服务攻击下的 Euler-Lagrange 系统的安全控制.空间控制技术与应用,2018,44(5):76−80.

马超(1985－),男,辽宁辽阳人,博士,讲师,主要研究领域为智能系统,混杂系统.

吴伟(1979－),男,博士,副研究员,主要研究领域为智能机器人.