文章编号: 1001-0920(2019)11-2303-07 DOI: 10.13195/j.kzyjc.2019.0215

DoS攻击下的信息物理系统事件触发预测控制设计

孙洪涛[1,2], 彭 晨[1†], 王志文[2]

(1. 上海大学 机电工程与自动化学院，上海 200444；2. 兰州理工大学 电气工程与信息工程学院，兰州 730050)

摘 要: 针对信息物理系统(CPS)安全控制设计问题,提出拒绝服务(DoS)攻击下具有任意有界丢包的事件触发预测控制(ETPC)方法. 首先,考虑DoS攻击能量的有限性及攻击行为的任意性,将DoS攻击描述为事件触发通信机制下的任意有界丢包;其次,在控制器端利用最近一次收到的状态信息进行控制器增益序列的预测设计以补偿DoS攻击造成的数据包丢失;随后,基于Lyapunov稳定性理论及切换系统分析方法考虑了DoS攻击下CPS的安全性并给出了控制序列设计方法. 所提出的ETPC设计方法只需利用最近时刻收到的状态信息,无需满足传统CPS稳定性对最大允许丢包数的约束,为大时滞CPS的稳定性分析及控制提供了有效的解决方案. 最后,通过仿真实例验证所提出的基于事件触发预测控制设计方法的有效性.

关键词: 信息物理系统；拒绝服务攻击；事件驱动；预测控制

中图分类号: TP273 **文献标志码:** A

Event-triggered predictive control of cyber-physical systems under DoS attacks

SUN Hong-tao[1,2], *PENG Chen*[1†], *WANG Zhi-wen*[2]

(1. School of Mechatronic Engineering and Automation，Shanghai University，Shanghai，200444，China；2. College of Electrical and Information Engineering，Lanzhou University of Technology，Lanzhou 730050，China)

Abstract: This paper investigates security control design of cyber-physical systems (CPS) under denial of service (DoS) attacks. The event-triggered predicative control (ETPC) strategy is proposed to deal with arbitrary bounded packet dropout under DoS attacks for CPS. Firstly, arbitrary bounded packet dropout in the event-triggered communication scheme is employed to describe the effect of DoS attacks by considering its energy-constraint and arbitrariness. Then, a control gain sequence derived by the latest received state is predicted to compensate the packet dropouts caused by DoS attacks at the controller side. In what follows, the security analysis and ETPC design are conducted by using Lyapunov stability theory and the switch system method. The proposed ETPC method only needs the latest received state and dose not need to satisfy with the constraint of maximum allowable packets dropouts bound in traditional stability analysis methods, which provides an effective solution for the analysis and control of CPS with large time delay. Finally the simulation results show the effectiveness of the proposed ETPC method.

Keywords: cyber physical systems；denial of service attacks；event-triggered；predictive control

0 引 言

随着信息系统与物理系统的不断融合,集通信、控制与计算于一体的信息物理系统(cyber-physical systems, CPS)及相关理论技术得到了迅速发展,推动了工业自动化、智慧交通及智能电网等领域关键技术的不断升级,引领新一轮产业变革,成为政府、企业和学术界重点关注的领域之一[1].

本质上,CPS中的计算单元与物理对象通过网络空间进行集成与交互,形成了开放式的网络化智能信息系统. 然而,开放网络环境下,信息安全的脆弱性凸显. 近年来,以Stuxnet为代表的信息安全事件表明:信息安全与物理安全可以相互转化、相互影响,进而影响CPS的综合服务性能[2-3]. 从CPS安全角度来说,现有的研究主要针对拒绝服务攻击和数据注入(欺骗)攻击两类[4]. DoS攻击能够阻塞网络信道使得CPS量测和控制信息无法正常更新,攻击方式简单、常见且最易实现[5],因此,如何在DoS 攻击下考虑系统的安全性是CPS安全控制研究中需要考虑的一个重要方面.

目前,DoS攻击下的CPS安全控制问题已得到了诸多学者的关注. 考虑CPS中不同的采样及控制方式,DoS攻击通常被建模为网络时延[6]或者丢

收稿日期: 2019-02-27；**修回日期:** 2019-08-30.

基金项目: 国家自然科学基金项目(61833011, 61673255, 61863026)；上海市优秀学术带头人项目(18XD1401600).

责任编委: 夏元清.

†通讯作者. E-mail: c.peng@shu.edu.cn.

包[7]. 在连续系统中,如果DoS攻击被建模为时延,则如何降低系统对时延的保守性是解决CPS安全控制问题的主要方法. 而当前CPS大多采用数字化的采样控制方式,因此,目前绝大多数的工作均将DoS建模为数据的随机或者有界丢包. 如文献[8-10]将DoS攻击造成的丢包假设为服从随机Bernoulli分布或者具有Markov跳变规律;文献[11-12]则在刻画丢包行为的基础上考虑了DoS攻击能量的有限性. 进而,基于切换系统、博弈论、随机及最优控制的分析与控制方法被用于解决DoS攻击下的CPS安全问题. 考虑CPS 的大规模特性和网络的脆弱性,一方面,网络可用资源日益缺乏;另一方面,从攻击者的角度来说,攻击行为除了能量限制外将不再服从特定的概率统计规律,具有一定的任意性. 因此,事件触发机制下考虑DoS攻击的CPS安全性分析与控制方法研究具有重要意义. 在事件触发机制下,文献[13]通过对DoS攻击频率及持续时间的刻画得出了系统的输入到状态稳定(input-to-state stability, ISS)的条件;文献[14]通过弹性事件触发参数的设计来处理网络化电力系统中的数据丢包问题,并给出了最大允许的丢包上界. 事实上,DoS攻击最终对CPS的影响体现在系统的性能上. 不同于对DoS攻击时间的刻画,文献[15]则通过在事件触发条件中引入与状态无关的性能损失参数来刻画DoS 攻击对系统性能的影响.

目前,多数的研究仍是在假设DoS攻击造成的数据丢包服从特定的概率分布条件下进行的,且对CPS稳定性的分析仍然被约束在传统保证系统稳定的最大允许时滞、丢包上界的框架下,具有一定的保守性. 本文讨论具有数据包传输机制的CPS安全控制问题,将DoS攻击下的事件触发CPS建模为一类控制器有界顺序切换系统;利用预测控制的基本思想及Lyapunov稳定性理论、线性矩阵不等式(linear matrix inequalities, LMIs)技术提出了相应的事件触发预测控制序列设计方法;最后,通过一个球杆实例验证所提出方法的有效性.

1 问题描述

考虑如图1所示的典型CPS控制结构. 所有控制功能组件通过网络连接,由于网络的开放性及脆弱性,易遭受网络攻击.

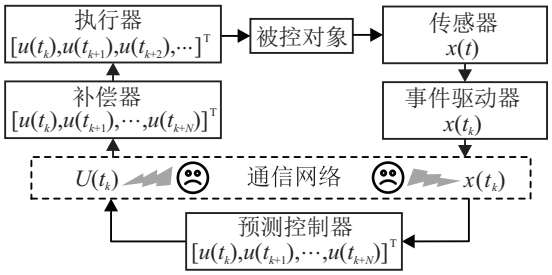

图1 DoS攻击下的CPS结构图

假设被控对象的动态演化规律可由如下线性时不变离散时间系统方程描述:

$$x(k+1)=Ax(k)+Bu(k). \tag{1}$$

其中:$x(k)\in R^n$ 和 $u(k)\in R^p$ 分别为状态向量和控制向量,A和B是具有适当维数的常数矩阵. 系统的初始条件为$x(0)=x_0$.

注1 式(1)是以固定采样周期h进行系统离散化的结果. 事实上,被控对象通过传感器采样实时状态$x(k)$,为与事件触发数据传输机制作比较,可记采样数据的集合为$\boldsymbol{S}_1=\{x(0),x(1),x(2),\cdots,x(k),\cdots\},k\in\boldsymbol{N}$为正数集合.

为了便于分析,首先对上述CPS进行如下假设.

假设1 (A,B)可控.

假设2 传感器采用时间驱动,控制器、执行器用事件驱动,补偿器采用时间与事件混合驱动方式.

假设3 数据传输采用单包方式传输并带有时间戳.

注2 在带有时间戳的数据包传输过程中,如果在规定的时间内补偿器收到了远程控制端传来的数据包,则采用事件驱动的方式将控制量传送至执行器;如果在规定的时间内未收到远程控制端传来的数据包,则从最后一次数据包中取出相应的控制分量按照时间触发的方式将数据包送至执行器.

注3 通常,对于一个控制系统来说,传统时滞系统分析方法可以得出一个使得系统稳定的最大允许的丢包,为边界$N_{\max}$,如果时滞或者丢包区间大于利用时滞系统分析方法所求出的最大允许时滞边界,则可能导致系统不再稳定. 而本文所提出的预测方法中,可以根据DoS攻击能量设计任意长度为N的预测控制序列以补偿丢包造成的控制信号缺失. 即预测控制序列的长度不必限定在系统最大允许丢包数$[0,N_{\max})$范围之内.

1.1 事件触发传输机制

为了减小数据包传送数量,在传感器侧通过设计一个事件触发器来判别传感器数据包是否需要被释放到控制器端. 假设最近一次数据发送的时刻为$x(k_r)$,则下一个事件触发的时刻可由下式确定:

$$k_{r+1}=k_r+\min_{k\in\boldsymbol{N},k>k_r}\{k|e(k)^{\mathrm{T}}\Phi e(k)\geqslant\delta x^{\mathrm{T}}(k_r)\Phi x(k_r)\}. \tag{2}$$

其中:$\delta>0$为给定的事件触发参数,Φ为适当维数的正定对称矩阵,而

$$e(k)=x(k)-x(k_r) \tag{3}$$

定义了当前采样时刻的状态$x(k)$和最近一次触发时刻的状态$x(k_r)$之间的误差.

采样数据通过事件触发器选择需要发送到远程

预测控制器端的状态数据$x(k_r)$,并记触发时刻的采样数据集合为$\boldsymbol{S}_2 = \{x(k_0), x(k_1), x(k_2), \cdots, x(k_r), \cdots\}$;显然有$\boldsymbol{S}_2 \subseteq \boldsymbol{S}_1$. 这样,并不是所有采样状态数据$x(kh)$均需被发送,而是通过事件触发器来判断是否满足触发条件.

假设4　相邻两次事件触发区间$[k_r, k_{r+1},)(i \in \{1,2,3,\cdots\})$是有界的,上界记为$M$,即$k_{r+1} - k_r \leqslant M$, M是一个正整数.

注4　事实上,数据包发送速率可通过调节事件触发参数δ实现. δ越大,数据传送的速率越低,对网络的占用越少;相反,δ越小,数据传送的速率越高,对网络的占用越多. 当$\delta = 0$时,上述事件触发机制将退化为传统的时间触发机制.

1.2　DoS攻击下的丢包

由于DoS攻击的存在,被触发的状态或者控制数据包均可能被攻击者劫持,导致触发数据丢包. 在执行器侧,如果记k_r为补偿器当前收到的最新数据包时刻,则由于DoS攻击,在接下来的$k_{r+1}, k_{r+2}, \cdots, k_{r+s}$时刻将会造成触发数据包丢失的现象. 进一步,记$s = 0,1,2, \sigma(k_r)$为DoS攻击造成的连续丢包数量,则可对DoS攻击能量作出如下假设.

假设5　如果连续触发数据包丢失的数量上界为N,则DoS攻击的单次攻击能量(最大持续时间)小于$N \times M \times h$,其中h是传感器的采样周期.

显然,$\overrightarrow{\sigma}(k_r) \in \mathcal{D} \triangleq \{0,1,2,\cdots,N\}$. 另外,$\overrightarrow{\sigma}(k_r)$可认为是一个具有有界顺序切换特征的时变切换信号,对应地形成内嵌式有界顺序切换系统[12].

注5　事件触发传输机制中,当存在DoS攻击时,丢失的数据包的个数为N,因此,在预测控制序列设计中,仅需根据触发包丢失的个数确定预测控制分量的个数,然后根据预先设定的控制执行规则进行数据包丢失的补偿. 结合假设4,本文可设定当执行器端执行上一时刻控制量后,如果在Mh时间间隔仍未收到触发数据包,则执行下一预测控制分量.

注6　本文所指的有界顺序切换系统指的是各个子系统之间只能按照特定的顺序进行切换,即在能量有限的DoS攻击中,用切换信号$\overrightarrow{\sigma}(k_r)$标识的子系统在执行器每次收到最近一次控制信号后,只能沿着$0 \to N$的方向进行切换,而不能向逆方向或者任意方向切换.

DoS攻击引起的触发数据包丢失将降低CPS(1)的性能,甚至失稳. 因此,需要设计必要的控制策略应对DoS引起的丢包.

1.3　事件触发机制下的DoS攻击丢包补偿

本文的主要思想是利用预测控制的思想对由DoS攻击引起的触发数据包的丢失进行相应的补偿. 基于收到的状态信号$x(k_r)$,控制器不仅要计算当前的控制信号$u(k_r)$,还要基于当前的状态信号进行事件触发机制下连续N步控制信号$u(k_{r+1})$, $u(k_{r+2}), \cdots, u(k_{r+N})$的预测,将预测控制序列发送到补偿器中以对数据包丢失起到补偿作用.

假设当前控制器最新接收到的最新更新时刻为k_r,对应的状态向量为$x(k_r)$. 在k_r时刻基于状态反馈的控制量及其预测控制量可表示为

$$u(k_{r+s}) = K_s x(k_r). \tag{4}$$

其中: K_s为对应的在切换信号$s \in \mathcal{D} \triangleq \{0,1,2,\cdots, N\}$下的控制器增益,且初始控制条件为$u(k_0) = K_0 x(0)$.

在基于数据包的网络传输机制中,当前k_r时刻及其连续N步基于事件触发的预测控制量将被打包在控制序列$U(k_r) = [u(k_r)^{\mathrm{T}}, u(k_{r+1})^{\mathrm{T}}, \cdots, u(k_{r+N})^{\mathrm{T}}]$中,并被传输以补偿DoS攻击造成的数据丢包.

1.4　安全性定义及重要引理

定义1　CPS(1)在DoS攻击下具有$\varepsilon \sim N$安全度,如果对于DoS攻击造成的最大丢包数量N,存在标量$c > 0, \varepsilon \in (0,1)$,使得下列不等式成立:

$$\|x(k)\| \leqslant c\varepsilon^k \|x(0)\|, \tag{5}$$

其中$x(0)$是系统的初始状态.

引理1[16]　对于任意矩阵$F \in \boldsymbol{R}^{n\times n}$与任意向量$x \in \boldsymbol{R}^n$,如下不等式成立:

$$\lambda_{\min}(F)\|x\| \leqslant \|Fx\| \leqslant \lambda_{\max}(F)\|x\|, \tag{6}$$

其中$\lambda_{\min}(F)$、$\lambda_{\max}(F)$分别代表矩阵F的最小与最大奇异值.

2　稳定性分析及安全控制器设计

2.1　基于事件触发的预测控制机制

本节将分析预测事件驱动机制下CPS(1)的动态演化规律. 由事件触发机制(2)及误差定义(3)可得如下关系.

情形1　无DoS攻击.

当$k \in [k_r, k_{r+1})$时,有

$$\begin{aligned} x(k+1) &= (A + BK_0)x(k) - BK_0 e(k) = \\ &\quad F_0 x(k) - BK_0 e(k) \end{aligned} \tag{7}$$

对所有$r \in \boldsymbol{N}$成立.

情形2　DoS攻击造成1步丢包.

当$k = k_{r+1}$时,为1步(预测)事件触发时刻, $e(k) = 0$,所以

$$x(k+1) = F_0 x(k). \tag{8}$$

当$k \in [k_{r+1}, k_{r+2})$时,有

$$\begin{aligned} x(k+1) &= AF_0 x(k) + BK_1 x(k_r) = \\ &\quad (AF_0 + BK_1)x(k) - BK_1 e(k) = \\ &\quad F_1 x(k) - BK_1 e(k). \end{aligned} \tag{9}$$

$$\vdots$$

情形N DoS攻击造成N步丢包.

当$k=k_{r+1}$时,为1步(预测)事件触发时刻,$e(k)=0$,所以

$$x(k+1)=F_0x(k). \tag{10}$$

当$k=k_{r+2}$时,为2步(预测)事件触发时刻,$e(k)=0$,所以

$$x(k+1)=F_1x(k). \tag{11}$$

$$\vdots$$

当$k=k_{r+N-1}$时,为N步(预测)事件触发时刻,$e(k)=0$,所以

$$x(k+1)=F_Nx(k). \tag{12}$$

当$k\in[k_{r+N},k_{r+N+1})$时,有

$$\begin{aligned}x(k+1)=&AF_Nx(k)+BK_Nx(k_r)=\\&(AF_N+BK_N)x(k)-BK_Ne(k)=\\&F_Nx(k)-BK_Ne(k).\end{aligned} \tag{13}$$

由式(7)$\sim$(13)中不难看出,具有N步DoS丢包的CPS系统本质上可建模为包含事件触发机制(2)的有界顺序切换系统

$$x(k+1)=F_{\vec{\sigma}(k_r)}x(k)-BK_{\vec{\sigma}(k_r)}e(k), \tag{14}$$

其中$\vec{\sigma}(k_r)\in\{0,1,2,\cdots,N\}$标称了DoS攻击下的子系统在$k_r$时刻的触发数据包的丢失数量.

注7 事实上,当DoS攻击丢包发生时,系统所能得到的准确的信息只有最近一次收到的反馈状态$x(k_r)$. 基于此,本文所提出的预测控制方法仅需通过收到的最近一次状态信息$x(k_r)$来预测未来多步控制器增益,与传统基于模型的预测方法相比,无需通过预测的状态作为下一步递推的依据. 因此,所提出的预测控制设计方法更加适用于DoS攻击造成的反馈信息缺失的情况,增加了预测控制设计的灵活度.

2.2 安全性分析

定理1 对于$\forall i\in\mathcal{D}$和给定的正定标量$0<c_i<1,\mu>0$,如果存在正定对称矩阵P_i,Φ使得如下线性矩阵不等式组成立:

$$\begin{bmatrix}\Xi_{i11}&\Xi_{i12}&\Xi_{i13}\\*&\Xi_{i22}&\Xi_{i23}\\*&*&\Xi_{i33}\end{bmatrix}<0; \tag{15}$$

$$P_a<\mu P_b,\ \forall a,b\in\mathcal{D}; \tag{16}$$

$$\varepsilon=\mu\bar{c}. \tag{17}$$

则CPS(1)在最大攻击能量为NM的DoS攻击下具有$\frac{1}{2MN}\sqrt{\mu\bar{c}}\sim N$安全度. 这里,$M$为事件触发间隔上界. 其中

$$\begin{aligned}&\Xi_{i11}=-c_i+\delta\Phi,\ \Xi_{i12}=-\delta\Phi,\ \Xi_{i13}=P_iF_i^{\mathrm{T}},\\&\Xi_{i22}=-\Phi+\delta\Phi,\ \Xi_{i23}=-P_i(BK_i)^{\mathrm{T}},\\&\Xi_{i33}=-P_i,\ \bar{c}=\max\{i\in\mathcal{D}|c_i\}.\end{aligned}$$

证明 基于上述DoS攻击下CPS的切换系统模型(14),选取分段Lyapunov泛函

$$V_{\vec{\sigma}(k_r)}(k)=x^{\mathrm{T}}(k)P_{\vec{\sigma}(k_r)}x(k), \tag{18}$$

$$V_{\vec{\sigma}(k_r)}(k+1)=x^{\mathrm{T}}(k+1)P_{\vec{\sigma}(k_r)}x(k+1). \tag{19}$$

沿着系统(7)对$V_{\vec{\sigma}(k_r)}(k)$计算差分,并考虑事件触发条件(2),可得

$$\begin{aligned}\nabla V_{\vec{\sigma}(k_r)}(k)=&V_{\vec{\sigma}(k_r)}(k+1)-V_{\vec{\sigma}(k_r)}(k)=\\&[AF_{\vec{\sigma}(k_r)}-BK_{\vec{\sigma}(k_r)}e(k)]^{\mathrm{T}}P_{\vec{\sigma}(k_r)}\times\\&[AF_{\vec{\sigma}(k_r)}-BK_{\vec{\sigma}(k_r)}e(k)]-\\&c_{\vec{\sigma}(k_r)}x(k)^{\mathrm{T}}P_{\vec{\sigma}(k_r)}x(k)-\\&e(k)^{\mathrm{T}}\Phi e(k)+\delta x^{\mathrm{T}}(k_r)\Phi x(k_r)=\\&[x(k)\quad e(k)]\widetilde{\Xi}\begin{bmatrix}x(k)\\e(k)\end{bmatrix}.\end{aligned} \tag{20}$$

其中

$$\widetilde{\Xi}=\begin{bmatrix}\widetilde{\Xi}_{11}&\widetilde{\Xi}_{12}\\*&\widetilde{\Xi}_{22}\end{bmatrix}; \tag{21}$$

$$\begin{aligned}&\widetilde{\Xi}_{11}=F_{\vec{\sigma}(k_r)}^{\mathrm{T}}P_{\vec{\sigma}(k_r)}F_{\vec{\sigma}(k_r)}-c_{\vec{\sigma}(k_r)}P_{\vec{\sigma}(k_r)}+\delta\Phi,\\&\widetilde{\Xi}_{12}=F_{\vec{\sigma}(k_r)}P_{\vec{\sigma}(k_r)}BK_{\vec{\sigma}(k_r)}-\delta\Phi,\\&\widetilde{\Xi}_{22}=(BK_{\vec{\sigma}(k_r)})^{\mathrm{T}}P_{\vec{\sigma}(k_r)}BK_{\vec{\sigma}(k_r)}-\Phi+\delta\Phi.\end{aligned}$$

由式(21)可得

$$\begin{aligned}&\begin{bmatrix}-c_{\vec{\sigma}(k_r)}P_{\vec{\sigma}(k_r)}+\delta\Phi&-\delta\Phi\\*&-\Phi+\delta\Phi\end{bmatrix}+\\&\begin{bmatrix}F_{\vec{\sigma}(k_r)}^{\mathrm{T}}P_{\vec{\sigma}(k_r)}\\-(BK_{\vec{\sigma}(k_r)}^{\mathrm{T}})P_{\vec{\sigma}(k_r)}\end{bmatrix}P_{\vec{\sigma}(k_r)}^{-1}\times\\&[P_{\vec{\sigma}(k_r)}F_{\vec{\sigma}(k_r)}\quad-P_{\vec{\sigma}(k_r)}(BK_{\vec{\sigma}(k_r)})]<0.\end{aligned} \tag{22}$$

对式(22)应用Schur补引理可得:若

$$\begin{aligned}&\begin{bmatrix}-c_{\vec{\sigma}(k_r)}P_{\vec{\sigma}(k_r)}+\delta\Phi&-\delta\Phi\\*&-\Phi+\delta\Phi\\*&*\end{bmatrix}\rightarrow\\&\leftarrow\begin{bmatrix}F_{\vec{\sigma}(k_r)}^{\mathrm{T}}P_{\vec{\sigma}(k_r)}\\-(BK_{\vec{\sigma}(k_r)})^{\mathrm{T}}P_{\vec{\sigma}(k_r)}\\-P_{\vec{\sigma}(k_r)}\end{bmatrix}<0,\end{aligned} \tag{23}$$

则对于$k\in[k_r,k_{r+\vec{\sigma}(k_r)})$,可以保证在事件触发机制(2)下$V_{\vec{\sigma}(k_r)}(k+1)<c_{\vec{\sigma}(k_r)}V_{\vec{\sigma}(k_r)}(k)$成立.

进一步考虑其内部预测切换行为,可得

$$\begin{aligned}&V_{\vec{\sigma}(k_r)}(k)<c_{\vec{\sigma}(k_r)}V_{\vec{\sigma}(k_r)}(k_{\vec{\sigma}(k_r)})<\\&c_{\vec{\sigma}(k_r)}c_{\vec{\sigma}(k_r)-1}V_{\vec{\sigma}(k_r)}(k_{\vec{\sigma}(k_r)-1})<\cdots<\\&\mu c_{\vec{\sigma}(k_r)}\cdots c_0V_{\vec{\sigma}(k_r)}(k_r)<\\&\mu c_{\vec{\sigma}(k_{r-1})}\cdots c_0V_{\vec{\sigma}(k_{r-1})}(k_{r-1})<\cdots<\\&\mu^2c_{\vec{\sigma}(k_r)}\cdots c_0c_{\vec{\sigma}(k_{r-1})}\cdots c_0V_{\vec{\sigma}_{r-2}(0)}(k_{r-2})<\cdots<\\&\mu^{k_r}c_{\vec{\sigma}(k_r)}\cdots c_0\cdots c_{\vec{\sigma}(k_0)}\cdots c_0V_{\vec{\sigma}(k_0)}(k_0).\end{aligned} \tag{24}$$

事实上,对于所有$r\in\boldsymbol{N}$,因为$\vec{\sigma}(k_r)=i\in\mathcal{D}$,所以,$c_{\vec{\sigma}(k_r)}$的解是有限的且可由式(23)给出. 因此,令

$\bar{c}=\max\{\overrightarrow{\sigma}(k_r)\in\mathcal{D}|c_{\overrightarrow{\sigma}(k_r)}\}$. 对于所有$r\in\boldsymbol{N}$的内部有界顺序切换,有

$$c_{\overrightarrow{\sigma}(k_r)}\cdots c_0\leqslant\bar{c},\tag{25}$$

并且

$$V_{\overrightarrow{\sigma}_r(i)}(k)<(\mu\bar{c})^{k_r}V_{\overrightarrow{\sigma}_0(0)}(k_0),\tag{26}$$

其中$\mu\bar{c}<1$.

由引理1可得,对于所有$\overrightarrow{\sigma}(k_r)\in\mathcal{D}$,可取

$$\widetilde{c}=\max\{\overrightarrow{\sigma}(k_r)\in\mathcal{D}|\lambda_{\max}(F_{\overrightarrow{\sigma}(k_r)})\},$$
$$\widetilde{d}=\min\{\overrightarrow{\sigma}(k_r)\in\mathcal{D}|\lambda_{\min}(P_{\overrightarrow{\sigma}(k_r)})\},$$
$$\overline{d}=\max\{\overrightarrow{\sigma}(k_r)\in\mathcal{D}|\lambda_{\max}(P_{\overrightarrow{\sigma}(k_r)})\}.$$

因此:

1) 当$k=k_r$,即当前控制器采用实际接收到的状态时刻的数据时,有

$$||x(k_r)||<\sqrt{\frac{\overline{d}}{\widetilde{d}}}(\sqrt{\mu\bar{c}})^{k_r}||x(0)||;\tag{27}$$

2) 当$k=k_{r+\overrightarrow{\sigma}(k_r)}$,即当前控制器采用预测时刻的数据时,有

$$||x(k_{r+\overrightarrow{\sigma}(k_r)})||<\widetilde{c}\sqrt{\frac{\overline{d}}{\widetilde{d}}}(\sqrt{\mu\bar{c}})^{k_r}||x(0)||,\tag{28}$$

同时

$$k\leqslant k_rNM,$$
$$k\leqslant k_{r+\overrightarrow{\sigma}(k_r)}NM\leqslant k_{r+\overrightarrow{\sigma}(k_r)+1}NM.\tag{29}$$

综合式(27)和(28)可得

$$\|x(k_r)\|<\sqrt{\frac{\overline{d}}{\widetilde{d}}}(\sqrt{\mu\bar{c}})^{\frac{k}{NM}}\|x(0)\|,$$

$$\|x(k_{r+\overrightarrow{\sigma}(k_r)})\|<\widetilde{c}\sqrt{\frac{\overline{d}}{\widetilde{d}}}(\sqrt{\mu\bar{c}})^{\frac{k}{NM}}\|x(0)\|.\tag{30}$$

进一步,由于(预测)事件触发通信间隔内,所有$k\in[k_r,k_{r+\overrightarrow{\sigma}(k_r)})$均满足不等式(20),对于$\forall k$有

$$\|x(k)\|<\widetilde{c}\sqrt{\frac{\overline{d}}{\widetilde{d}}}(\sqrt[\frac{1}{2MN}]{\mu\bar{c}})^{k}\|x(0)\|.\tag{31}$$

取$\varepsilon=\sqrt[\frac{1}{2MN}]{\mu\bar{c}}$,由定义(1)可知,CPS(1)具有$\sqrt[\frac{1}{2MN}]{\mu\bar{c}}\sim N$安全度. 由$\overrightarrow{\sigma}(k_r)\in\mathcal{D}$可知,定理1得证. □

2.3　安全预测控制序列设计

基于定理1中的不等式(15)可得如下控制器设计方法.

定理2　对于$\forall i\in\mathcal{D}$和给定的正定标量$0<c_i<1,\mu>0$,如果存在正定对称矩阵$\overline{P}_i$和$\overline{\Phi}$使得如下线性矩阵不等式成立:

$$\begin{bmatrix}\overline{\Xi}_{i11}&\overline{\Xi}_{i12}&\overline{\Xi}_{i13}\\*&\overline{\Xi}_{i22}&\overline{\Xi}_{i23}\\*&*&\overline{\Xi}_{i33}\end{bmatrix}<0,\tag{32}$$

则CPS(1)在最大触发包丢失数为N的DoS攻击下具有$\sqrt[\frac{1}{2MN}]{\mu\bar{c}}\sim N$安全度的事件驱动预测控制增益序列为

$$U(k_r)=[(Y_0\overline{P}_0^{-1})^{\mathrm{T}}\quad(Y_1\overline{P}_1^{-1})^{\mathrm{T}}\quad\cdots\quad(Y_N\overline{P}_N^{-1})^{\mathrm{T}}]^{\mathrm{T}}.$$

其中

$$\overline{\Xi}_{i11}=-c_i\overline{P}_i+\delta\overline{\Phi},\ \overline{\Xi}_{i12}=-\delta\overline{\Phi},$$
$$\overline{\Xi}_{i13}=\overline{P}_i^{\mathrm{T}}\overline{A}_i^{\mathrm{T}}+Y_i^{\mathrm{T}}B^{\mathrm{T}},\ \overline{\Xi}_{i22}=-\overline{\Phi}+\delta\overline{\Phi},$$
$$\overline{\Xi}_{i23}=-Y_i^{\mathrm{T}}B^{\mathrm{T}},\ \overline{\Xi}_{i33}=-\overline{P}_i,$$
$$\overline{A}_i=A^{i+1}+\cdots+ABK_i,$$
$$\varepsilon=\mu\bar{c},\ \bar{c}=\max\{i\in\mathcal{D}|c_i\}.$$

证明　令$\overline{P}_i=P_i^{-1},\overline{\Phi}=\overline{P}_i^{\mathrm{T}}\Phi\overline{P}_i,Y_i=K_i\overline{P}_i$,考虑按照顺序定义的参数$\overrightarrow{\sigma}_r(i)\in\mathcal{D}$,对不等式(15)两边分别左乘和右乘对角阵$\mathrm{diag}[P^{-1},P^{-1},P^{-1}]$,可得定理2成立. □

注8　上述控制器设计体现了该切换系统的有界顺序特征,因为只有在前次控制器增益矩阵已知的情况下,才能对当前新的控制器增益进行设计;否则,当$i\geqslant1$时,将导致线性矩阵不等式(32)存在非线性项而无法求解的情况.

注9　事实上,在采用本文所给的安全预测控制序列作用下,系统的收敛指数$\sqrt[\frac{1}{2MN}]{\mu\bar{c}}$是一个与DoS攻击造成的丢包数$N$相关的函数,这正是DoS攻击下安全度的一个关键衡量指标.

3　仿真实例

本节采用传感器、控制器与执行器通过网络连接的网络化的球杆控制系统进行上述理论结果的验证[17-18]. 该系统的模型可由如下动态方程描述:

$$\begin{cases}0=\left(\dfrac{J_b}{R}+m\right)\ddot{\gamma}+mg\sin\theta-m\gamma\dot{\theta}^2,\\ \tau=(m\gamma^2+J+J_b)\ddot{\theta}+2m\gamma\dot{\gamma}\dot{\theta}+mg\gamma\cos\theta.\end{cases}$$

其中:τ是杆的力矩,J是杆的转动惯量,J_b是球的转动惯量,m是球的质量,R是球的半径,L是杆的长度,θ是杆的水平夹角,g是万有引力常量. 设定系统参数为$m=0.11\,\mathrm{kg},R=0.015\,\mathrm{m},J_b=9.9\times10^{-6}\,\mathrm{kg\cdot m^2},g=9.81\,\mathrm{m/s^2}$,并令控制输入为$u=\ddot{\theta}$,状态变量为$x=[\gamma\quad\dot{\gamma}\quad\theta\quad\dot{\theta}]^{\mathrm{T}}$. 对系统中的非线性项作线性化处理并以采样时间$T=0.02\,\mathrm{s}$离散化可得如下离散状态空间方程:

$$x(k+1)=Ax(k)+Bu(k).$$

其中

$$A=\begin{bmatrix}1.000\,0&0.020\,0&-0.001\,4&0\\0&1.000\,0&-0.140\,1&-0.001\,4\\0&0&1.000\,0&0.020\,0\\0&0&0&1.000\,0\end{bmatrix},$$

$$B=[0\quad 0\quad 0.0002\quad 0.0200]^{\mathrm{T}}.$$

假设DoS攻击能够造成的最大触发包丢失的数量为$N=3$,并且设定触发参数$\delta=0.05, c_0=c_1=c_2=c_3=0.9, \mu=1$,则$\bar{c}=0.9$. 根据定理2并利用Matlab求解可得如下(预测)控制器增益矩阵序列:

$$K_0=$$
$$[835.3566\quad 467.6408\quad -675.2308\quad -57.2989],$$
$$K_1=[-96.6799\quad -50.1269\quad 62.5480\quad 2.5352],$$
$$K_2=[4.4394\quad 2.1968\quad -2.4241\quad -0.0987],$$
$$K_3=[-73.1498\quad -37.8382\quad 46.2698\quad 1.0832].$$

仿真实验将通过3次实验结果的对比来说明本文所提出ETPC方法的有效性.

情况1 对于上述所设计的控制器增益序列,如果不存在DoS攻击,则只需利用控制器增益K_0对闭环系统进行控制. 系统的状态响应及触发间隔如图2和图3所示.

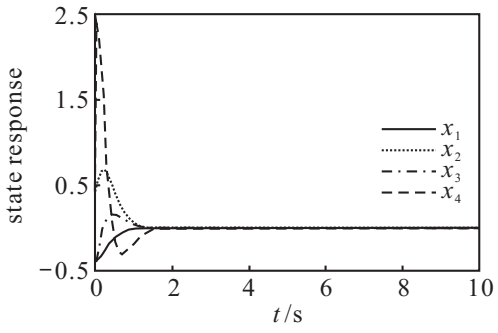

图2 无DoS攻击时系统的状态响应

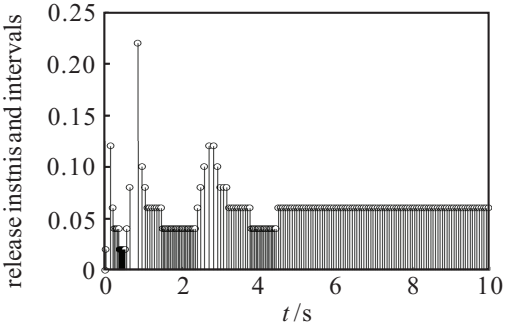

图3 无DoS攻击时事件触发间隔

如图2和图3所示,系统是稳定的,且在1 000次采样内只有177次采样时刻被传输,平均传输间隔为0.056 s,达到了节约网络资源的目的.

情况2 假如CPS遭受DoS攻击且攻击造成的最大丢包数为$N=3$,攻击信号序列如图4所示. 如果仍然采用不带预测补偿机制的控制器增益K_0,则系统将不再稳定,对应的状态响应由图5给出.

情况3 当存在DoS攻击时,为使系统稳定,采用本文提出的预测控制补偿增益序列K_1, K_2, K_3. 其状态响应及触发间隔如图6和图7所示.

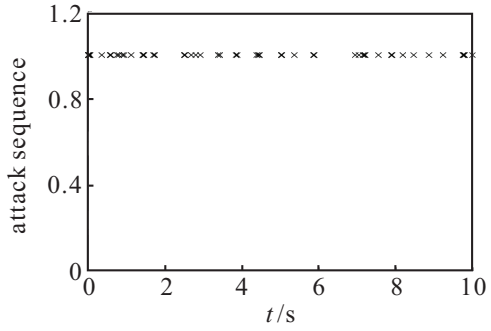

图4 DoS攻击序列信号(0—无攻击,1—有攻击)

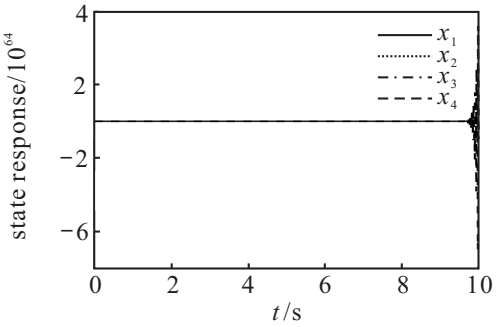

图5 存在DoS攻击且无补偿策略时系统的状态响应

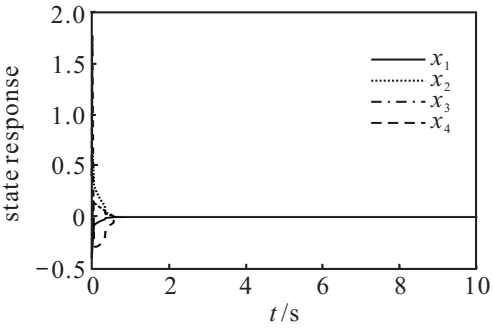

图6 存在DoS攻击并采用补偿策略时的系统状态响应

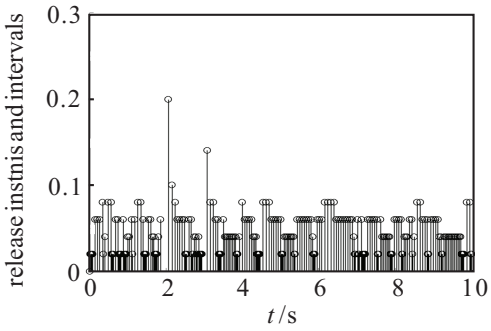

图7 存在DoS攻击时的事件触发间隔

显然,在预测补偿控制机制下系统是稳定的,且共有266个数据被应用于控制,平均传输间隔为0.038 s.

综合上述仿真结果,所提出的事件触发预测控制补偿方法是有效的;同时,相比于在模型预测机制下的丢包补偿方法,本文所提出的预测控制设计方法将大大减少数据包传输,节约了通信资源. 另外,通过对比图3和图7可知:在DoS攻击下,数据传输包的传输数量变多. 值得注意的是,由于预测控制器的引入改

变了原有控制器K_0下的事件触发行为,加上当前触发包的丢失会造成后续所有触发行为随之改变,因此,有可能导致数据传输量变大,但这并不影响触发包丢失情况下系统的稳定性.

4 结　论

针对DoS攻击下的CPS安全控制设计问题,本文提出了基于事件触发策略的预测补偿控制方法. 考虑DoS攻击的任意性及能量有界性,将事件触发机制下的DoS攻击丢包建模为一类具有任意有界顺序切换规律的切换系统模型,进而利用Lyapunov方法并结合LMIs技术给出了控制序列的求解方法. 所提出的ETPC设计方法只需利用最近时刻收到的状态信息,无需满足传统CPS稳定性对最大时滞、丢包的约束,为大时滞CPS的控制提供了有效的解决方案. 最后,通过仿真实验验证了所提出方法的有效性.

参考文献(References)

[1] 管晓宏, 关新平, 郭戈. 信息物理融合系统理论与应用专刊序言 [J]. 自动化学报, 2019, 45(1): 1-4.
(Guan X H, Guan X P, Guo G. Preface of the special issue on theory and applications of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 1-4.)

[2] Sandberg H, Amin S, Johansson K H. Cyberphysical security in networked control systems: An introduction to the issue[J]. IEEE Control Systems Magazine, 2015, 35(1): 20-23.

[3] Peng C, Sun H T, Yang M J, et al. A survey on security communication and control for smart grids under malicious cyber attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, DOI: 10.1109/TSMC.2018.2884952.

[4] 邬晶, 李依宁, 李少远. 分布式电网CPS系统数据攻击下的状态估计 [J]. 控制与决策, 2016, 31(2): 331-336.
(Wu J, Li Y N, Li S Y. State estimation for distributed cyber-physical power systems under data attacks[J]. Journal of Control and Decision, 2016,31(2): 331-336.)

[5] 文坤, 杨家海, 张宾. 低速率拒绝服务攻击研究与进展综述 [J]. 软件学报, 2014, 25(3): 591-605.
(Wen K, Yang J H, Zhang B. Survey on research and progress of low-rate denial of service attacks[J]. Journal of Software, 2014, 25(3): 591-605.)

[6] Cao R, Wu J, Long C, et al. Stability analysis for networked control systems under denial-of-service attacks[C]. Proc of the 54th IEEE Conference on Decision and Control. Osaka, 2015: 7476-7481.

[7] Long M, Wu C H, Hung J. Y. Denial of service attacks on network-based control systems: Impact and mitigation[J]. IEEE Transactions on Industrial Informatics, 2005, 1(2): 85-96.

[8] Ding D R, Wang Z D, Wei G L, et al. Event-based security control for discrete-time stochastic systems[J]. IET Control Theory & Applications, 2016, 10(15): 1808-1815.

[9] Yang H J, Shi M, Xia Y Q, et al. Security research on wireless networked control systems subject to jamming attacks[J]. IEEE Transactions on Cybernetics, 2018, DOI: 10.1109/TCYB.2018.2817249.

[10] Sun H T, Peng C, Yang T C, et al. Resilient control of networked control systems with stochastic denial of service attacks[J]. Neurocomputing, 2017, 270: 170-177.

[11] Zhang H, Cheng P, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint[J]. IEEE Transactions on Automatic Control, 2015, 60(11): 3023-3028.

[12] Lai S Y, Chen B, Li T X, et al. Packet-based state feedback control under DoS Attacks in cyber-physical systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, DOI: 10.1109/TCSII.2018.2881984.

[13] De Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service[J]. IEEE Transactions on Automatic Control, 2015, 60(11): 2930-2944.

[14] Peng C, Li J C, Fei M R. Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks[J]. IEEE Transactions on Power Systems, 2017, 32(5): 4110-4118.

[15] Sun H T, Peng C, Zhang W D, et al. Security-based resilient event-triggered control of networked control systems under denial of service attacks[J]. Journal of the Franklin Institute, 2018, DOI:10.1016/j.jfranklin.2018.04.001.

[16] Leon, Steve, Pearson. Linear algebra with applications: Pearson new international edition[M]. Pearson Higher Ed, 2013: 150-164.

[17] Yin X X, Yue D, Hu S L. Event-triggered predictive control for networked systems with communication delays compensation[J]. International Journal of Robust & Nonlinear Control, 2016, 25(18): 3572-3595.

[18] Zhang J H, Xia Y Q, Shi P. Design and stability analysis of networked predictive control systems[J]. IEEE Transactions on Control Systems Technology, 2013, 21(4): 1495-1501.

作者简介

孙洪涛(1987−), 男, 博士, 从事网络化系统安全控制的研究, E-mail: sht371322@163.com;

彭晨(1972−), 男, 教授, 博士生导师, 从事网络控制系统、模糊控制等研究, E-mail: c.peng@shu.edu.cn;

王志文(1976−), 男, 教授, 博士生导师, 从事信息物理系统、工业过程先进控制理论与应用等研究, E-mail: wwwangzhiwen@163.com.

(责任编辑：孙艺红)