文章编号:1006-2467(2020)09-0910-06 DOI: 10.16183/j.cnki.jsjtu.2020.168

拒绝服务攻击下信息物理系统事件触发广义预测控制

王志文, 刘 伟
(兰州理工大学 电气工程与信息工程学院; 甘肃省工业过程先进控制重点实验室;
电气与控制工程国家级实验教学示范中心, 兰州 730050)

摘 要: 针对传感器到控制器通信信道上存在拒绝服务(DoS)攻击的信息物理系统的安全问题进行研究. 首先,基于系统的定周期采样策略,设计了事件触发的通信策略,以减少通信资源的占用. 同时,为降低 DoS 攻击给系统带来的不良影响,提出了一种基于预测控制的数据补偿方法,在控制器节点中,通过成功接收到的历史状态信息得到系统受攻击导致状态信息丢失情况下的状态预测值,并给出控制器反馈增益的表达式. 随后,提出了事件触发预测控制下的系统闭环模型,分析了系统闭环稳定的充分条件. 最后,通过仿真实例证明了该方法的有效性.

关键词: 信息物理系统;拒绝服务攻击(DoS);事件触发策略;广义预测控制
中图分类号: TP 273 **文献标志码**: A

Event-Triggered Generalized Predictive Control of Cyber-Physical Systems Under Denial-of-Service Attacks

WANG Zhiwen, *LIU Wei*
(College of Electrical and Information Engineering; Key Laboratory of Gansu Advanced Control for Industrial Processes; National Demonstration Center for Experimental Electrical and Control Engineering Education, Lanzhou University of Technology, Lanzhou 730050, China)

Abstract: A generalized predictive control strategy of cyber-physical systems under denial-of-service (DoS) attack is studied. First, an event-triggered communication strategy is designed to reduce the occupation of communication resources based on the periodic sampling strategy of the system. At the same time, in order to reduce the adverse effects of DoS attacks on the system, a data compensation method based on predictive control is proposed. The data of state information lost in system attacks are predicted by the successfully received historical state information in the controller nodes, and the expression of the controller feedback gain is proposed. Then, a closed-loop model of the system under event-triggered predictive control is proposed and sufficient conditions are analyzed. Finally, the effectiveness of the method is proved by the simulation example.

Key words: cyber-physical system; denial-of-service attack (DoS); event-triggered strategy; generalized predictive control

---

收稿日期:2020-01-10
基金项目:国家自然科学基金(61863026,61563031,61751315),甘肃省高等学校产业支撑引导(2019C-05),甘肃省工业过程先进控制重点实验室开放基金(2019KFJJ03)资助项目
作者简介:王志文(1976-),男,甘肃省武威市人,教授,现主要从事网络化控制系统的研究.
电话(Tel.):13893329300;E-mail:wwwangzhiwen@163.com.

随着计算机技术和数据通信技术的不断发展与融合，信息物理系统(CPS)技术应运而生. CPS 是由多维异构计算单元和物理系统在网络环境中高度集成与交互而构成的一类新型智能复杂系统[1]. 该系统将计算资源与物理资源紧密结合、协调分配，实现了系统对物理环境的实时感知和动态分布式控制. CPS 因具有结构灵活、低成本和高效性等诸多优点而被广泛应用于工业过程控制等领域，但是其设备智能化、通信网络化等特性，也使得 CPS 易成为网络攻击的目标. 拒绝服务(DoS)攻击出现的频率最高，也最难以防范，其本质是阻止物理系统量测或控制信号的实时传输，致使控制信号更新不及时以及不完整，进而导致控制品质下降甚至失稳. 随着网络规模的扩大，用户对系统安全性和稳定性的要求也随之上升，信息物理系统的安全问题受到学者的广泛关注.

关于 DoS 攻击引发的安全问题和 DoS 攻击建模问题已被广泛研究. 与一般的数据丢包问题不同，由 DoS 攻击带来的通信故障问题通常不服从某一类概率分布[4]，这给控制系统的分析和设计带来了新的挑战. 文献[2]研究了一类单输入系统下周期 DoS 攻击问题，并给出了应对已知攻击周期上界 DoS 攻击的极点配置方法. 进一步，文献[3]针对多输入连续控制系统下 DoS 攻击问题，给出了已知 DoS 攻击周期上界时系统的稳定性条件. 文献[4-6]研究了几类具有特定随机过程的 DoS 攻击下系统的安全控制问题：文献[4]研究了伯努利模型 DoS 攻击下离散系统的 LQG 最优控制问题；文献[5-6]则研究了马尔可夫模型 DoS 攻击下系统的风险敏感控制问题和弹性控制问题. 在实际情况下 DoS 攻击通常不会遵循某种特定的规律. 为了更简洁地描述 DoS 攻击的行为，文献[7-8]从攻击频率和持续时间对随机 DoS 攻击来进行约束：文献[7]提出了一种保证网络化控制系统输入状态稳定的弹性控制策略；文献[8]提出了一种动态的事件触发策略，并证明了其有效性. 在文献[9-10]中，作者从攻击者的角度研究 DoS 攻击，并描述了使得攻击收益最大化的 DoS 攻击调度策略. 为了进一步描述 DoS 攻击者与 CPS 控制策略的交互性，许多学者从博弈论的角度进行了相关研究：文献[11]中，二者的交互被看作零和博弈，考虑了二者的纳什均衡策略；文献[12]分别从攻击者和防御者两个角度分析了带有未知策略的不完全信息博弈均衡解，并比较完全信息情况，设计了基于卡尔曼滤波的预测控制器. 现有文献主要对特定攻击类型的 DoS 攻击进行了一定的研究，但对 CPS 自身特性和 DoS 攻击与控制策略交互性的研究存在一定的局限性.

综合上述文献中的相关研究成果和不足，本文建立了基于事件触发预测控制的离散时间线性网络控制系统. 对于表征 DoS 攻击信号的问题，现有研究中通常假设 DoS 攻击服从一类概率分布. 然而，在存在智能干扰器的情况下，DoS 攻击难以满足相应的统计特性，并且防御者也难以获取准确的统计信息. 为了缩短理论研究与工程应用之间的差距，本文选取随机 DoS 攻击模型，从能量受限的角度去设计 DoS 攻击模型，得到了攻击的最大步长. 在系统受到攻击时，为了避免因数据无法传输而造成的系统性能下降，设计了一种基于广义预测控制的数据补偿策略，并同时结合事件触发机制，减少网络信道上数据传输量，降低通信网络负荷. 在对受攻击的系统状态进行分析时，将系统描述为一个切换系统，并建立了系统闭环稳定性条件.

1　问题描述

如图 1 所示为离散时间线性不变系统，在其控制系统中，传感器到控制器之间的通信线路为网络通信线路，而网络攻击即发生在此网络信道中. 攻击发生时，网络通道上被视为系统状态信号完全无法传输.

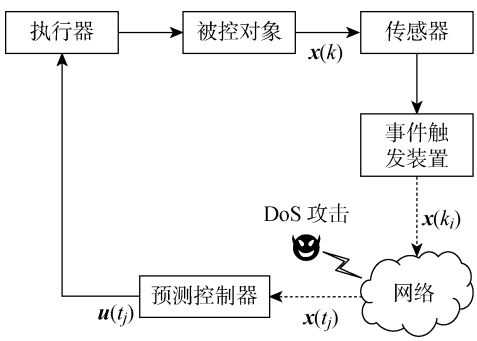

图 1　系统结构示意图

Fig. 1　Diagram of system structure

在系统传感器节点处采用定周期采样策略，结合事件触发机制来减少网络带宽的占用，并通过广义预测控制算法，在 DoS 攻击发生时，控制器基于历史状态信息来得出丢失状态信号的预测值，从而主动补偿网络攻击对系统造成的影响.

系统被控对象可被描述为：

$$\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{u}(k) \tag{1}$$

式中：$\boldsymbol{x}(k)\in\mathbf{R}^{n\times 1}$ 为控制系统的状态变量；$\boldsymbol{u}(k)\in\mathbf{R}^{m\times 1}$ 为系统的控制输入；$\boldsymbol{A}\in\mathbf{R}^{n\times n}$，$\boldsymbol{B}\in\mathbf{R}^{n\times m}$. 假定系统$(\boldsymbol{A},\boldsymbol{B})$ 可控，DoS 攻击最长步长为 d.

2 离散时间事件触发通信策略

为了减少控制信号在网络信道上的传输量，从而降低通信网络负荷，状态信号只有在满足特定的事件触发条件时才被传输. 假定事件触发时刻为 k_i $(i=0,1,2,\cdots)$，当系统状态 $\boldsymbol{x}(k_i)$ 在事件触发时刻 k_i 被传输时，下一事件触发时刻 k_{i+1} 由以下方程确定[13]：

$$\begin{aligned} k_{i+1} = k_i + \min_r \{ r \mid [\hat{\boldsymbol{x}}(k_i+r) - \boldsymbol{x}(k_i)]^{\mathrm{T}} \\ \boldsymbol{\Phi}[\hat{\boldsymbol{x}}(k_i+r) - \boldsymbol{x}(k_i)] > \\ \mu \hat{\boldsymbol{x}}^{\mathrm{T}}(k_i+r)\boldsymbol{\Phi}\hat{\boldsymbol{x}}(k_i+r)\} \\ r \in \mathbf{N}_+, \quad \mu \in (0,1) \end{aligned} \tag{2}$$

式中：$\hat{\boldsymbol{x}}(k_i+r)$ 为 k_i+r 时刻系统的预测状态；μ 为给定参数；$\boldsymbol{\Phi}$ 为正定对称矩阵.

网络信道中存在 DoS 攻击，可能造成部分通信数据未能成功传输的情况. 综合事件触发机制和 DoS 攻击对系统造成的影响，将不同情况下的系统状态进行划分. 系统中状态数据的传输示意图如图 2 所示.

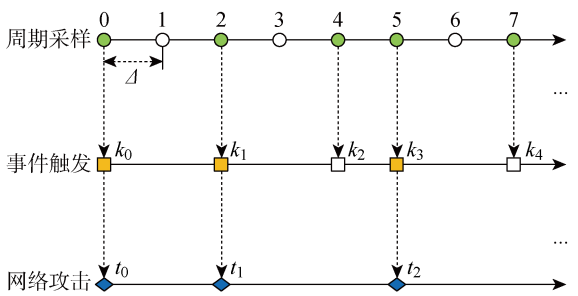

图 2 数据传输状态示意图

Fig. 2 Status of data during transmission

将系统事件触发时刻记为 k_i. k_i 时刻时，如果系统未受到 DoS 攻击，则状态 $\boldsymbol{x}(k_i)$ 被成功传输，将该时刻记为 $t_j(j=0,1,2,\cdots)$ 可得 $\{t_0,t_1,t_2,\cdots\} \subset \{k_0,k_1,k_2,\cdots\} \subset \{0,1,2,\cdots\}$. Δ 则为系统采样周期.

3 DoS 攻击下的广义预测控制策略

一般在网络系统的预测控制方案中，状态数据 $\boldsymbol{x}(k)$ 在每个采样周期均被发送，并且周期性地更新控制律. 然而，在事件触发控制策略下，只有当满足事件触发条件式(2)时才将状态信息发送到控制器，减少信道资源占用. 此外，对于由 DoS 攻击所造成的数据传输失败从而导致系统性能降低甚至失稳的情况，将介绍一种预测控制算法，对传输失败的数据进行补偿.

3.1 预测控制反馈增益

当 t_j 时刻时，数据被成功传输，预测控制的最优性能指标为[14]

$$\begin{aligned} \min \boldsymbol{J}(t_j) = \sum_{l=1}^{N_p} \boldsymbol{x}^{\mathrm{T}}(t_j+l \mid t_j)\boldsymbol{Q}\boldsymbol{x}(t_j+l \mid t_j) + \\ \sum_{l=0}^{N_u-1} \boldsymbol{u}^{\mathrm{T}}(t_j+l \mid t_j)\boldsymbol{R}\boldsymbol{u}(t_j+l \mid t_j) \end{aligned} \tag{3}$$

式中：$\boldsymbol{Q}$ 和 $\boldsymbol{R}$ 为正定对称的加权矩阵；N_p 和 N_u 分别为预测范和控制范围，$N_p \geqslant N_u \geqslant d$；$\boldsymbol{x}(t_j+l|t_j)$ 和 $\boldsymbol{u}(t_j+l|t_j)$ 分别为基于 t_j 时刻的状态变量和控制输入的测量值而得出的 t_j+l 时刻的状态变量和控制输入的预测值.

由式(1)可得

$$\begin{aligned} \boldsymbol{x}(t_j+l+1 \mid t_j) = \boldsymbol{A}\boldsymbol{x}(t_j+l \mid t_j) + \\ \boldsymbol{B}\boldsymbol{u}(t_j+l \mid t_j) \end{aligned} \tag{4}$$

则系统的预测控制方程可写为

$$\boldsymbol{X}(t_j+1) = \boldsymbol{A}_p\boldsymbol{x}(t_j) + \boldsymbol{B}_p\boldsymbol{U}(t_j) \tag{5}$$

式中：

$$\boldsymbol{X}(t_j+1) = \begin{bmatrix} \boldsymbol{x}^{\mathrm{T}}(t_j+1 \mid t_j) & \cdots & \boldsymbol{x}^{\mathrm{T}}(t_j+N_p \mid t_j) \end{bmatrix}^{\mathrm{T}}$$

$$\boldsymbol{U}(t_j) = \begin{bmatrix} \boldsymbol{u}^{\mathrm{T}}(t_j \mid t_j) & \cdots & \boldsymbol{u}^{\mathrm{T}}(t_j+N_u-1 \mid t_j) \end{bmatrix}^{\mathrm{T}}$$

$$\boldsymbol{A}_p = \begin{bmatrix} \boldsymbol{A}^{\mathrm{T}} & (\boldsymbol{A}^2)^{\mathrm{T}} & \cdots & (\boldsymbol{A}^{N_p})^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}}$$

$$\boldsymbol{B}_p = \begin{bmatrix} \boldsymbol{B} & \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{A}\boldsymbol{B} & \boldsymbol{B} & \cdots & \boldsymbol{0} & \boldsymbol{0} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \boldsymbol{A}^{N_u-1}\boldsymbol{B} & \boldsymbol{A}^{N_u-2}\boldsymbol{B} & \cdots & \boldsymbol{A}\boldsymbol{B} & \boldsymbol{B} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \boldsymbol{A}^{N_p-1}\boldsymbol{B} & \boldsymbol{A}^{N_p-2}\boldsymbol{B} & \cdots & \boldsymbol{A}^{N_p-N_u+1}\boldsymbol{B} & \boldsymbol{A}^{N_p-N_u}\boldsymbol{B} \end{bmatrix}$$

进一步，系统的性能指标函数式(3)可化为

$$\begin{aligned} \boldsymbol{J}(t_j) = \boldsymbol{X}^{\mathrm{T}}(t_j+1)\overline{\boldsymbol{Q}}\boldsymbol{X}(t_j+1) + \\ \boldsymbol{U}^{\mathrm{T}}(t_j)\boldsymbol{R}\boldsymbol{U}(t_j) \end{aligned} \tag{6}$$

式中：

$$\overline{\boldsymbol{Q}} = \mathrm{diag}\,(\boldsymbol{Q},\cdots,\boldsymbol{Q})$$

$$\overline{\boldsymbol{R}} = \mathrm{diag}\,(\boldsymbol{R},\cdots,\boldsymbol{R})$$

系统的预测控制优化问题可以根据式(3)和(4)化为

$$\min_{\boldsymbol{U}(t_j)} \boldsymbol{J}(t_j) \tag{7}$$

$\partial \boldsymbol{J}(t_j)/\partial \boldsymbol{U}(t_j)=0$ 时，最优控制输入解为

$$\boldsymbol{U}^*(t_j) = -(\boldsymbol{B}_p^{\mathrm{T}}\overline{\boldsymbol{Q}}\boldsymbol{B}_p + \overline{\boldsymbol{R}})^{-1}\boldsymbol{B}_p^{\mathrm{T}}\overline{\boldsymbol{Q}}\boldsymbol{A}_p\boldsymbol{x}(t_j) \tag{8}$$

从而，在事件触发时刻 t_j 的控制输入为

$$\boldsymbol{u}(t_j) = \boldsymbol{u}(t_j \mid t_j) = \boldsymbol{F}\boldsymbol{x}(t_j) \tag{9}$$

式中：预测控制反馈增益为

$$\boldsymbol{F}=-[\boldsymbol{I}\quad\boldsymbol{0}\quad\cdots\quad\boldsymbol{0}](\boldsymbol{B}_p^{\mathrm{T}}\overline{\boldsymbol{Q}}\boldsymbol{B}_p+\overline{\boldsymbol{R}})^{-1}\boldsymbol{B}_p^{\mathrm{T}}\overline{\boldsymbol{Q}}\boldsymbol{A}_p$$

3.2　事件触发机制下数据补偿策略

假设在事件触发时刻 k_i，状态 $\boldsymbol{x}(k_i)$ 被成功传输，则有 $k_i=t_j$，如图 3 所示，在区间 $[t_j,t_{j+1})$ 内，控制反馈增益为 $\boldsymbol{F}$，即在事件触发时刻 k_{i+s}（$s=1,2,\cdots,d$），有

$$\boldsymbol{u}(k_{i+s})=\boldsymbol{F}\hat{\boldsymbol{x}}(k_{i+s}) \tag{10}$$

并且在区间 $[k_{i+s},k_{i+s+1})$ 内，控制律保持不变.

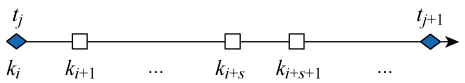

图 3　相邻成功传输时刻间数据传输状态示意图

Fig. 3　Data status between two successfully transmitted moments

t_j 和 t_{j+1} 为两次相邻的数据信号成功传输时刻，事件触发时刻 k_{i+1} 等则由于 DoS 攻击的存在而使信号无法传输. 在两次相邻的成功传输时刻 $[t_j,t_{j+1})$ 之间，基于上一次成功传输的状态信息，对未能传输成功的状态进行预测：

$$\boldsymbol{x}(k_i)=\boldsymbol{x}(t_j) \tag{11}$$

$$\hat{\boldsymbol{x}}(k_i+1)=\boldsymbol{A}\boldsymbol{x}(k_i)+\boldsymbol{B}\boldsymbol{F}\boldsymbol{x}(k_i) \tag{12}$$

$$\hat{\boldsymbol{x}}(k_i+j+1)=\boldsymbol{A}\hat{\boldsymbol{x}}(k_i+j)+\boldsymbol{B}\boldsymbol{F}\boldsymbol{x}(k_i) \tag{13}$$

$$j=1,2,\cdots,k_{i+1}-k_i-1$$

$$\hat{\boldsymbol{x}}(k_{i+s}+j+1)=\boldsymbol{A}\hat{\boldsymbol{x}}(k_{i+s}+j)+\boldsymbol{B}\boldsymbol{F}\hat{\boldsymbol{x}}(k_{i+s}) \tag{14}$$

$$j=0,1,2,\cdots,k_{i+s+1}-k_{i+s}-1$$

3.3　DoS 攻击下事件触发预测控制的闭环控制系统

在反馈控制律式(10)的作用下，控制系统(1)可写为

$$\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{u}(k_{i+s})=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{F}\hat{\boldsymbol{x}}(k_{i+s}) \tag{15}$$

根据式(11)～(14)对预测状态的推导，可得

$$\hat{\boldsymbol{x}}(k_{i+s})=\left(\boldsymbol{A}^{k_{i+s}-k_i}+\sum_{j=1}^{k_{i+s}-k_i}\boldsymbol{A}^{k_{i+s}-k_i-j}\boldsymbol{B}\boldsymbol{F}\right)\boldsymbol{x}(k_i) \tag{16}$$

因此，闭环控制系统的方程可以写为

$$\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{F}\left(\boldsymbol{A}^{k_{i+s}-k_i}+\sum_{j=1}^{k_{i+s}-k_i}\boldsymbol{A}^{k_{i+s}-k_i-j}\boldsymbol{B}\boldsymbol{F}\right)\boldsymbol{x}(k_i) \tag{17}$$

定义状态误差 $\boldsymbol{e}(k)=\hat{\boldsymbol{x}}(k)-\boldsymbol{x}(k_i)$，则闭环控制系统可以描述为如下形式：

$$\boldsymbol{x}(k+1)=\boldsymbol{\Pi}_{\sigma_s}\boldsymbol{x}(k)-\boldsymbol{\Xi}_{\sigma_s}\boldsymbol{e}(k) \tag{18}$$

式中：

$$\sigma_s\in S=\{\sigma_0,\sigma_1,\cdots,\sigma_d\}$$

$$\boldsymbol{\Pi}_{\sigma_s}=\boldsymbol{A}+\boldsymbol{B}\boldsymbol{F}\left(\boldsymbol{A}^{\sigma_s}+\sum_{j=1}^{\sigma_s}\boldsymbol{A}^{\sigma_s-j}\boldsymbol{B}\boldsymbol{F}\right)$$

$$\boldsymbol{\Xi}_{\sigma_s}=\boldsymbol{B}\boldsymbol{F}\left(\boldsymbol{A}^{\sigma_s}+\sum_{j=1}^{\sigma_s}\boldsymbol{A}^{\sigma_s-j}\boldsymbol{B}\boldsymbol{F}\right)$$

$$\sigma_s=k_{i+s}-k_i$$

4　系统稳定性分析

本节在闭环系统式(18)的基础上，讨论了事件触发器参数 $\boldsymbol{\Phi}$ 的设计，并分析了系统的李雅普诺夫(Lyapunov)稳定性，给出了系统稳定性条件.

定理 1　考虑上文所给出的事件触发预测控制系统，对于给定的系统矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$，常数参数 $\mu\in(0,1)$，预测控制反馈增益 $\boldsymbol{F}$，如果存在适当维数的矩阵 $\boldsymbol{P}>0$ 和 $\boldsymbol{\Phi}>0$，使得对于所有 $\sigma_s\in S$，都有如下矩阵不等式成立：

$$\begin{bmatrix}-\boldsymbol{P}+\mu\boldsymbol{\Phi} & * & *\\ \boldsymbol{0} & -\boldsymbol{\Phi} & *\\ \boldsymbol{P}\boldsymbol{\Pi}_{\sigma_s} & -\boldsymbol{P}\boldsymbol{\Xi}_{\sigma_s} & -\boldsymbol{P}\end{bmatrix}<0 \tag{19}$$

则闭环系统式(18)是渐进稳定的. 式中：“$*$”为矩阵对称项的省略.

证明　选取闭环系统的 Lyapunov 方程为

$$\boldsymbol{V}(x)=\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{P}\boldsymbol{x}(k) \tag{20}$$

式中：矩阵 $\boldsymbol{P}$ 为对称正定矩阵. 根据事件触发条件式(2)可得，在没有发生事件触发的时间段内，有

$$\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{e}(k)\leqslant\mu\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{x}(k) \tag{21}$$

结合式(20)和(21)，可得

$$\begin{aligned}\Delta V=&\boldsymbol{V}(\boldsymbol{x}(k+1))-\boldsymbol{V}(\boldsymbol{x}(k))=\\&\boldsymbol{x}^{\mathrm{T}}(k+1)\boldsymbol{P}\boldsymbol{x}(k+1)-\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{P}\boldsymbol{x}(k)\leqslant\\&\boldsymbol{x}^{\mathrm{T}}(k+1)\boldsymbol{P}\boldsymbol{x}(k+1)-\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{P}\boldsymbol{x}(k)-\\&\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{e}(k)+\mu\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{x}(k)=\\&[\boldsymbol{\Pi}_{\sigma_s}\boldsymbol{x}(k)-\boldsymbol{\Xi}_{\sigma_s}\boldsymbol{e}(k)]^{\mathrm{T}}\\&\boldsymbol{P}[\boldsymbol{\Pi}_{\sigma_s}\boldsymbol{x}(k)-\boldsymbol{\Xi}_{\sigma_s}\boldsymbol{e}(k)]-\\&\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{P}\boldsymbol{x}(k)-\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{e}(k)+\\&\mu\boldsymbol{x}^{\mathrm{T}}(k)\boldsymbol{\Phi}\boldsymbol{x}(k)=\\&\begin{bmatrix}\boldsymbol{x}(k)\\ \boldsymbol{e}(k)\end{bmatrix}^{\mathrm{T}}\boldsymbol{\Omega}\begin{bmatrix}\boldsymbol{x}(k)\\ \boldsymbol{e}(k)\end{bmatrix}\end{aligned} \tag{22}$$

式中：

$$\boldsymbol{\Omega}=\begin{bmatrix}\boldsymbol{\Pi}_{\sigma_s}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{\Pi}_{\sigma_s}-\boldsymbol{P}+\mu\boldsymbol{\Phi} & *\\ -\boldsymbol{\Xi}_{\sigma_s}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{\Pi}_{\sigma_s} & \boldsymbol{\Xi}_{\sigma_s}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{\Xi}_{\sigma_s}-\boldsymbol{\Phi}\end{bmatrix}=$$

$$\begin{bmatrix}-\boldsymbol{P}+\mu\boldsymbol{\Phi} & *\\ \boldsymbol{0} & -\boldsymbol{\Phi}\end{bmatrix}-$$

$$\begin{bmatrix}\boldsymbol{\Pi}_{\sigma_s}^{\mathrm{T}}\boldsymbol{P}\\ -\boldsymbol{\Xi}_{\sigma_s}^{\mathrm{T}}\boldsymbol{P}\end{bmatrix}(-\boldsymbol{P})^{-1}[\boldsymbol{P}\boldsymbol{\Pi}_{\sigma_s}\quad-\boldsymbol{P}\boldsymbol{\Xi}_{\sigma_s}]$$

根据舒尔(Schur)补定理，如果 $\boldsymbol{\Omega}<0$，则线性矩

阵不等式(19)成立,同时有 $\Delta \boldsymbol{V}<0$. 根据 Lyapunov 稳定性定理,闭环系统是渐进稳定的.

5 数值仿真分析

考虑如下的离散时间控制系统:

$$\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{u}(k)$$

其中:$\boldsymbol{A}=\begin{bmatrix}0 & 1\\ -2 & -3\end{bmatrix}$,$\boldsymbol{B}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$;系统初始状态为 $\boldsymbol{x}_0=\begin{bmatrix}20\\ -20\end{bmatrix}$. 选择 $\boldsymbol{Q}=\boldsymbol{I}_{2\times 2}$,$\boldsymbol{R}=\boldsymbol{I}_{2\times 2}$,$N_p=4$,$N_u=3$,事件触发条件式(2)中 $\mu=0.1$,DoS 攻击步长 $d=3$,则预测控制反馈增益

$$\boldsymbol{F}=\begin{bmatrix}0.342\,2 & -0.147\,8\\ 1.600\,8 & 2.230\,1\end{bmatrix}$$

通过 LMI 工具箱求解线性矩阵不等式(19)可得

$$\boldsymbol{P}=\begin{bmatrix}2.550\,9 & 2.079\,3\\ 2.079\,3 & 2.617\,7\end{bmatrix}$$

$$\boldsymbol{\Phi}=\begin{bmatrix}13.543\,8 & 12.086\,4\\ 12.086\,4 & 14.216\,4\end{bmatrix}$$

则在 DoS 攻击下,具有事件触发预测控制的系统仿真结果如图 4 所示. 红色曲线 x' 为无预测控制下系统受 DoS 攻击时的状态曲线,在该情况下系统受到 DoS 攻击时,系统状态信号视为丢失. 蓝色曲线 x 为具有预测控制的控制系统受 DoS 攻击时的状态曲线,该情况下系统受到攻击时,则采用预测控制信号实施控制作用. 阴影部分表示系统受到 DoS 攻击的时间段. 在给定的 DoS 攻击下,未采用控制算法的系统已经处于失稳状态. 而预测控制算法能明显改善系统状态,使之能抵御一定强度的 DoS 攻击,增强系统安全性能.

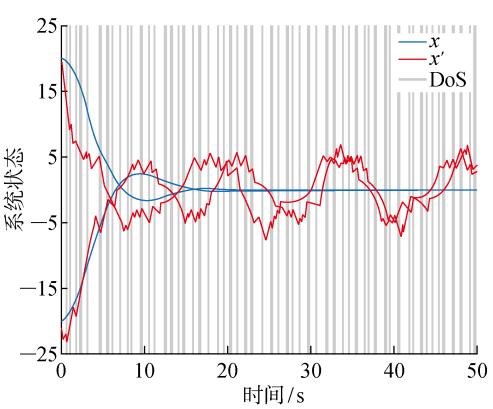

图 4 系统状态响应曲线

Fig. 4 Simulation result of response of system status

系统受攻击状态下的时间触发示意图如图 5 所示,其中:数值 1 为事件触发状态,数值 0 为事件未

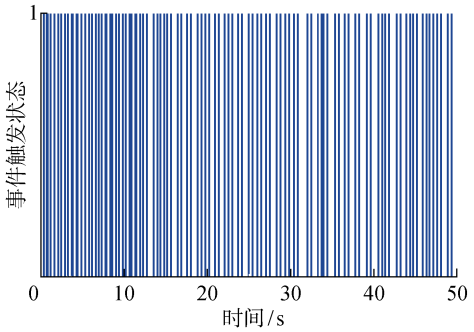

图 5 事件触发状态示意图

Fig. 5 Status of event-triggered generator

触发状态. 结合图 4 可得,在系统状态变化较快的时间段内,事件触发次数也明显较多,从而使系统能够迅速恢复稳定状态,而在系统状态较为平缓的时间段内,事件触发次数较少,从而减少了通信信道上的数据传输量,降低了网络系统的负荷,增加了系统的安全裕度.

根据仿真结果可以看出,在系统受到有限强度 DoS 攻击的情况下,文中所设计的预测控制算法对系统状态有良好的优化作用,能在一定程度上实现对系统的安全控制.

6 结语

本文针对 CPS 在传感器到控制器的网络线路上受到 DoS 攻击时如何确保系统性能的安全问题,并结合已有相关建模方式及实际情况,设计了一种事件触发广义预测控制算法,使得在减少网络信道数据传输量的同时,基于历史状态信息得到了缺失状态数据的预测值,从而补偿了丢失的状态信号,降低了攻击对系统造成的不良影响,并分析了系统的稳定性. 最后,本文通过一个 CPS 仿真实例验证了该方法的有效性.

参考文献:

[1] 张云贵. 信息物理融合的网络控制系统安全技术研究[D]. 哈尔滨:哈尔滨工业大学,2015.
ZHANG Yungui. Research on security technology of network control system based on cyber-physical concept[D]. Harbin: Harbin Institute of Technology, 2015.

[2] FOROUSH H S, MARTÍNEZ S. On single-input controllable linear systems under periodic DoS jamming attacks[J]. **Mathematics**, 2012(3): 1-12.

[3] FOROUSH H, MARTÍNEZ S. On multi-input controllable linear systems under unknown periodic DoS jamming attacks[C]// **Proceedings of the Conference**

on Control and its Applications. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2013: 222-229.

[4] AMIN S, CÁRDENAS A A, SASTRY S S. Safe and secure networked control systems under denial-of-service attacks[C]// **International Workshop on Hybrid Systems: Computation and Control**. San Francisco, CA, USA: 2009: 31-45.

[5] BEFEKADU G, GUPTA V, ANTSAKLIS P J. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies[J]. **IEEE Transactions on Automatic Control**, 2015, 60(12): 3299-3304.

[6] 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.

[7] 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.

[8] SENEJOHNNY D, TESI P, DE PERSIS C. Self-triggered coordination over a shared network under denial-of-service[C]// **IEEE Conference on Decision and Control (CDC)**. Osaka, Japan: IEEE, 2015: 3469-3474.

[9] ZHANG H, CHENG P, SHI L, *et al*. Optimal DoS attack scheduling in wireless networked control system[J]. **IEEE Transactions on Control Systems Technology**, 2016, 24(3): 843-852.

[10] 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.

[11] LI Y Z, SHI L, CHENG P, *et al*. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach[J]. **IEEE Transactions on Automatic Control**, 2015, 60(10): 2831-2836.

[12] 杨洪玖，徐豪，张金会. 不完全信息拒绝服务攻击下基于预测控制的信息物理系统稳定性分析[J]. **信息与控制**，2018，47(1)：75-80.
YANG Hongjiu, XU Hao, ZHANG Jinhui. Stability analysis of cyber-physical systems based on predictive control under denial of service attacks with incomplete information[J]. **Information and Control**, 2018, 47(1): 75-80.

[13] PENG C, YANG T C. Event-triggered communication and H∞ control co-design for networked control systems[J]. **Automatica**, 2013, 49(5): 1326-1332.

[14] 刘安东，季鹏. 随机时延网络化系统的模型预测控制[J]. **浙江工业大学学报**，2018，46(1)：67-71.
LIU Andong, JI Peng. Model predictive control for network-based system with random delay[J]. **Journal of Zhejiang University of Technology**, 2018, 46(1): 67-71.

（本文编辑：黄伟）