文章编号: 1001-0920(2019)08-1681-07 DOI: 10.13195/j.kzyjc.2018.0024

DoS干扰攻击下的信息物理系统状态反馈稳定

汪慕峰, 胥布工†

(华南理工大学 自动化科学与工程学院, 广州 510640)

摘 要: 基于网络的工业控制系统作为信息物理系统(CPSs)的一种重要应用正迅猛发展. 然而,近年来针对工业控制系统的恶意网络攻击引起了人们对CPS安全问题的广泛关注. 拒绝服务(DoS)干扰攻击作为CPS中最容易发生的攻击方式得到了深入研究. 对此,提出一种能量受限的、周期的DoS干扰攻击模型,攻击的目的是增大无线信道发生数据包随机丢包的概率. 基于一类CPS简化模型,考虑CPS中传感器与控制器(S-C)之间无线信道同时存在DoS干扰攻击和固有随机数据包丢失的情况,采用状态反馈,基于随机Lyapunov函数和线性矩阵不等式方法得到可以保证系统稳定的充分条件,并利用系统稳定的充分条件和锥补线性化算法设计控制器. 最后,通过两个数值仿真例子验证所提出控制策略的有效性.

关键词: 信息物理系统; 拒绝服务干扰攻击; 能量受限; 周期; 数据包丢失; 状态反馈稳定

中图分类号: TP273 **文献标志码:** A

State feedback stabilization of cyber-physical system under DoS jamming attacks

WANG Mu-feng, XU Bu-gong†

(College of Automation Science and Technology, South China University of Technology, Guangzhou 510640, China)

Abstract: Industrial control systems based on the network have developed rapidly as an important application of the cyber-physical systems (CPSs). However, the malicious cyber attacks on the network of the industrial control system have aroused widespread concern about the security of CPSs in recent years. Denial-of-service (DoS) attack, which aims to jam the communication between system components, has been widely studied since this attack pattern is the most accomplishable. In this paper, an energy-constrained periodic DoS jamming attacker model is proposed to increase the probability of stochastic packet dropouts. We consider a class of CPSs with inherent stochastic packet dropouts under DoS jamming attack on the wireless channel between a sensor and a controller. A sufficient condition for the existence of the state feedback controller which guarantees the stochastic stability of the CPS is established based on stochastic Lyapunov function and linear matrix inequality approach. The design of the controller can be solved by the cone complementarity linearization algorithm. Finally, two numerical simulations illustrate the effectiveness of the proposed controller.

Keywords: cyber-physical systems (CPSs); DoS jamming attack; energy-constrained; periodic; packet dropouts; state feedback stabilization

0 引 言

随着计算技术、控制技术和通信技术的不断发展和深度融合,信息物理系统(cyber-physical systems, CPSs)[1]正在迅猛发展,并广泛地应用于航空航天、智能电网、智能交通、远程医疗等重要基础设施中[2-5]. 特别地,工业控制系统[6]作为CPS的重要应用,与人们的日常生产生活紧密相关. 近年来,随着工业生产规模的不断扩大,传感技术、计算技术和无线通信网络技术的不断发展,催生出网络环境下的新型工业控制系统. 无线网络的介入,特别是基于无线通信的各类传感器在工业控制系统中的大量部署,使得工业控制系统具有低成本、自组织、易部署、易维护等优点. 但是,无线网络中存在的恶意攻击、随机丢包等因素,也严重影响着工业控制系统的安全运行[7-8]. 2011年"震网"病毒利用工业控制系统漏洞入侵伊朗布尔什核电站[9],2012年"火焰"病毒入侵中东地区石油工业控制系统[10],这些事件表明,CPS一旦遭到恶意网络攻击,将会造成十分严重的经济损失和社会危害,对

收稿日期: 2018-01-04; **修回日期:** 2018-04-03.

基金项目: 国家自然科学基金-广东联合基金重点项目(U1401253); 国家自然科学基金项目(61573153); 广东省自然科学基金项目(2016A030313510).

责任编委: 王龙.

†通讯作者. E-mail: aubgxu@scut.edu.cn.

人们正常的生产生活造成极大的影响. 针对恶意网络攻击下的CPS安全问题,科学家们从不同角度展开了研究[11-13]. Cárdenas等[12]提出了CPS运行的安全目标:完整性、可用性、机密性. Teixeira等[13]总结了网络攻击的基本特征,将典型的攻击方式分为:拒绝服务攻击(denial-of-service, DoS)、数据重放攻击(replay data attack)和错误数据注入攻击(false data injection attack). 其中,DoS攻击作为CPS中最容易实现的攻击方式得到了广泛研究. 一个典型的DoS攻击者可以通过阻碍或干扰正常通信来降低信道传输质量,引起系统的不稳定[13-14]. 目前,DoS攻击下的CPS安全问题研究主要从以下3个角度进行:

1) 从攻击者的角度研究DoS攻击的最优攻击调度. Zhang等[15]研究了CPS中能量受限DoS干扰攻击者的最优攻击调度,由于攻击者能量受限,假设在有限时间范围内攻击者只能对无线信道发动有限数量的干扰攻击,并从理论上证明了攻击者的最优攻击策略为发动连续攻击;随后,Zhang等[16]研究了CPS中周期的、能量受限的DoS干扰攻击者的最优攻击调度,由于能量受限,攻击者只能在活跃期发动n次攻击,在非活跃期内存储能量,同时,从理论上证明了在活跃期内发动连续攻击为最优攻击策略;Peng等[17]研究了一类包含两个子系统的无线CPS中能量受限的、周期的DoS干扰攻击者的最优攻击调度,由于能量受限,攻击者只能在活跃期内有选择性地对一条信道发动有限数量的DoS干扰攻击,攻击将造成该时刻数据包的随机丢失.

2) 从受攻击系统的角度研究有效防御控制策略. Foroush等[18]基于输入-状态稳定性研究了一种周期的、能量受限的DoS干扰攻击下的CPS事件触发稳定策略;Persis等[19]建立了一般的DoS攻击模型,并研究了DoS攻击下的CPS稳定性,仅需限制该攻击者模型在一段时间内的攻击频率和攻击持续时间,便可以描述攻击者的周期性、能量受限等特性. 后来,基于文献[19]中的DoS攻击模型,Feng等[20]研究了DoS攻击下的网络控制系统弹性控制策略设计问题,Dolk等[21]研究了DoS攻击下基于输出事件触发的网络控制系统的弹性控制策略设计问题,Cetinkaya等[14]研究了DoS攻击和随机丢包下的网络线性动态系统的有效控制问题.

3) 从博弈论的角度研究攻击与防御的最优博弈策略. Li等[22]考虑攻击者和传感器均能量受限条件下,基于二人零和博弈,研究了DoS干扰攻击下的CPS远程状态估计. Yuan等[23]基于博弈论研究了CPS抵抗DoS攻击的弹性控制策略问题,考虑攻击者能量受限,定义了一个随机变量α_i^k表示攻击强度. Ding等[24]提出了一种能量受限的DoS攻击者模型,并定义信号干扰噪声比(SINR)来表示攻击造成的影响;考虑一个多信道的CPS,基于博弈论建立了传感器与攻击者之间的二人零和博弈决策过程. Zhao等[25]假设DoS攻击者和受攻击目标均能量受限,利用二人零和博弈研究了攻击者与防御者各自的最优决策.

另一方面,由于通信信道的固有因素,如:带宽资源受限、网络拥塞、网络缓冲溢出等,会出现数据包随机丢失的现象,并最终导致控制系统性能下降甚至不稳定[22,26-27],使得在研究CPS安全问题时考虑随机数据包丢失具有重要意义. 然而,现有的关于CPS安全问题的研究中,极少有同时考虑恶意攻击和固有数据包丢失的情况.

本文考虑一类由受控对象、传感器、控制器和执行器组成的CPS简化模型,该模型广泛地应用于工业生产中,研究DoS干扰攻击下CPS的状态反馈稳定性问题. 要研究DoS干扰攻击下的信息物理系统安全问题,关键是建立一种合理的DoS干扰攻击模型. 由上述研究可知,能量受限和周期性是DoS干扰攻击的主要特征,也是研究者在建立DoS攻击模型时考虑的主要因素. 本文建立一种新的能量受限的、周期的DoS干扰攻击模型. 攻击者在攻击期对无线信道发动连续攻击以降低无线信道的数据包传输成功率,同时,考虑无线信道固有的数据包随机丢失对CPS的影响. 基于Lyapunov函数和线性矩阵不等式方法,采用状态反馈控制,得到保持系统稳定的充分条件. 理论推导和数值仿真均验证了所提出控制策略的有效性.

综上,本文的主要贡献如下:

1) 提出一种新的能量受限的、周期的DoS干扰攻击模型,该模型具有固定的工作周期;

2) 同时考虑DoS干扰攻击和无线信道固有的数据包随机丢失对CPS的影响;

3) 采用状态反馈控制,得到实现DoS干扰攻击下CPS稳定的充分条件,该控制策略简单易行.

首先给出符号说明: $\boldsymbol{R}^n$ 和 $\boldsymbol{R}^{m\times n}$ 分别表示n维和$m\times n$维欧几里德空间; $\boldsymbol{Z}^+$ 表示正整数集; $A>0(A<0)$表示A是一个适当维数的正(负)定矩阵; I和0分别表示适当维数的单位矩阵和零矩阵; $[\cdot]^{\mathrm{T}}$表示矩阵的转置; $\lambda_{\max}(A)(\lambda_{\min}(A))$表示矩阵$A$的最大(最小)特征值; $\mathrm{Trace}(\cdot)$表示矩阵的迹; $\mathrm{Pr}[\cdot]$表示一个随机事件的概率; A^{T}表示矩阵A的转置; $\mathrm{E}[\cdot]$表示一

个随机事件的数学期望;矩阵中的符号$*$表示矩阵的对称部分.

1　问题建立

考虑一类DoS攻击下的CPS如图1所示. 其中:传感器、控制器和执行器均为时间驱动;控制器中有缓存器,用来存储最近一次成功收到的数据包. 传感器-控制器(S-C)之间通过无线信道传递数据,其他系统组件之间通过可靠的有线信道传递数据,且无线信道存在随机数据包丢失现象. 由于无线信道开放、广播、共享等特性,使DoS干扰攻击更容易在无线信道中发动[28-29]. 假设攻击者有能力对S-C之间的无线信道发动DoS干扰攻击.

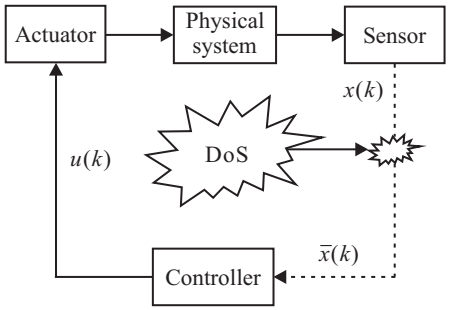

图1　DoS干扰攻击下的信息物理系统

注1　在工业控制系统中,传感器与控制器之间采用无线连接已经得到广泛应用,具有低成本、低功耗、易部署、易维护等优点.

注2　文献[14]所研究的问题与本文类似,但是本文将提出一种新的DoS攻击模型来模拟攻击对系统造成的影响.

1.1　DoS干扰攻击者模型

DoS干扰攻击最典型的实现方式是通过干扰系统元件之间的正常通信来降低无线信道的数据包传输成功率[22]. 本文建立一种新的能量受限的、周期的DoS干扰攻击模型. 攻击者的工作周期可表示为

$$k \in [(n-1)T+1, nT].$$

其中:T为常数,表示攻击者任意一个工作周期的持续时间;$n(n \in \boldsymbol{Z}^+)$表示攻击者的第$n$个工作周期.

令常数$t_{\rm off}(t_{\rm off} \in \boldsymbol{Z}^+, t_{\rm off} \leqslant T)$表示攻击者在任意一个工作周期内的休眠期持续时间.

定义$\sigma(k) \in \{1,2\}$表示攻击者的不同时期,有

$$\sigma(k) = \begin{cases} 1,\ k \in [(n-1)T+1, (n-1)T+t_{\rm off}]; \\ 2,\ k \in [(n-1)T+t_{\rm off}+1, nT]. \end{cases} \tag{1}$$

其中:$\sigma(k)=1$表示攻击者处于第n个工作周期的休眠期,$\sigma(k)=2$表示攻击者处于第n个工作周期的攻击期. 攻击者任意工作周期示意如图2所示.

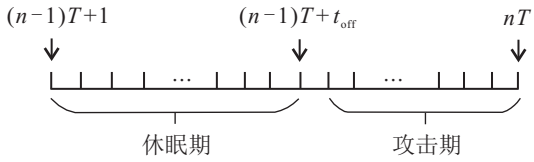

图2　DoS干扰攻击工作周期示意

由于能量受限,攻击者必须在每个工作周期内先进入休眠期,为即将发生的攻击期补充能量,并在攻击期对无线信道发动连续的DoS干扰攻击. 具体描述如下:

1) 在休眠期,攻击者为攻击期积累能量,不发动攻击. 然而,由于无线信道的固有特性,会发生随机数据包丢失现象[26-27].

2) 在攻击期,攻击者对无线信道发动连续DoS干扰攻击. 攻击使得信道的数据包传输成功率降低[15,30].

注3　显然,当$t_{\rm off} = T$时,攻击者将一直处于休眠状态,不会对无线信道发动干扰攻击.

注4　由文献[15-16,18]中建立的合理的、被广为接受的DoS攻击者模型可知,能量受限和周期性是DoS干扰攻击的主要特征. 特别地,攻击者由于能量受限而采用周期攻击形式是易于实现的[18]. 此外,能量受限条件下,DoS干扰攻击者的最优攻击策略为发动连续攻击[15-16]. 因此,本文提出一种能量受限、周期的DoS干扰攻击模型. 与已有的DoS攻击模型不同[14-17,19-25],该模型有具体的周期结构,且在攻击期内发动连续攻击.

结合式(1),定义$\theta(\sigma(k),k) \in \{0,1\}$表示存在周期攻击的情况下,$k$时刻的数据包是否传输成功,即

$$\theta(\sigma(k),k) = \begin{cases} 1,\ \text{Transmission success}; \\ 0,\ \text{Transmission failure}. \end{cases} \tag{2}$$

假设1　假设数据包在休眠期和攻击期的成功传输率均服从Bernoulli概率分布,这与文献[31]和文献[22]中的假设相同. 结合式(1)和(2),可得

$$\begin{cases} \Pr[\theta(\sigma(k),k)=1] = \alpha_{\sigma(k)}, \\ \Pr[\theta(\sigma(k),k)=0] = 1-\alpha_{\sigma(k)}. \end{cases} \tag{3}$$

注5　值得注意的是,无攻击情况下无线信道的数据包传输成功率会比有攻击情况下的高[23],即$\alpha_1 > \alpha_2$. 另外,如果$\alpha_1 = \alpha_2$,则说明攻击对系统没有造成影响. 此时仅需考虑存在随机数据包丢失,该类问题已得到了广泛研究[26-27,31-32].

注6　函数$\theta(\sigma(k),k)$与$\sigma(k)$相关,表示有(无)攻击下数据包的传输成功(失败). 与已有研究[26-27,31]相比更加复杂.

1.2 系统模型

图1中的被控对象描述如下:

$$x(k+1)=Ax(k)+Bu(k). \tag{4}$$

其中: $x(k)\in \boldsymbol{R}^n$ 为系统状态向量, $u(k)\in \boldsymbol{R}^m$ 为控制输入, A 和 B 为已知的适当维数常系数矩阵.

为保证上述CPS的稳定运行,采用如下形式的状态反馈控制器:

$$u(k)=K\bar{x}(k). \tag{5}$$

其中: $\bar{x}(k)$ 为控制器的输入, K 为待设计的反馈增益矩阵.

当 k 时刻数据包 $x(k)$ 传输失败时,采用最近一个时刻的数据 $\bar{x}(k-1)$ 代替. 因此,控制器接收到的系统状态为

$$\bar{x}(k)=\theta(\sigma(k),k)x(k)+(1-\theta(\sigma(k),k))\bar{x}(k-1). \tag{6}$$

应用控制器(5)到系统(4),被控对象表示为

$$\begin{aligned}x(k+1)=Ax(k)+BK[&\theta(\sigma(k),k)x(k)+\\&(1-\theta(\sigma(k),k))\bar{x}(k-1)].\end{aligned} \tag{7}$$

令 $z(k)=[x^{\mathrm{T}}(k)\quad \bar{x}^{\mathrm{T}}(k-1)]^{\mathrm{T}}$, $\xi(k)\in\{1,2\}$,并结合式(2)~(7),闭环系统可表示为

$$z(k+1)=\Phi_{\xi(k)}z(k), \tag{8}$$

其中

$$\Phi_{\xi(k)}=\begin{bmatrix}A+\theta(\sigma(k),k)BK & (1-\theta(\sigma(k),k))BK\\ \theta(\sigma(k),k)I & (1-\theta(\sigma(k),k))I\end{bmatrix}.$$

Dos干扰攻击下的闭环系统(8)可由下面两个子系统表示:

1) 当数据包传输成功时, $\theta(\sigma(k),k)=1$,有

$$\Phi_1=\begin{bmatrix}A+BK & 0\\ I & 0\end{bmatrix}; \tag{9}$$

2) 当数据包传输失败时, $\theta(\sigma(k),k)=0$,有

$$\Phi_2=\begin{bmatrix}A & BK\\ 0 & I\end{bmatrix}. \tag{10}$$

令 $\xi(k)=i,\xi(k+1)=j$,于是在 k 时刻为子系统 $\Phi_{\xi(k)}$ 的概率为 $\pi_{ij}=\Pr[\xi(k+1)=j|\xi(k)=i]$,其中 $\pi_{ij}\geqslant 0,\forall i,j\in\{1,2\},\sum\limits_{i=1}^{2}\pi_{ij}=1$. 由式(3)得 $\pi_{i1}=\alpha_{\sigma(k)},\pi_{i2}=1-\alpha_{\sigma(k)}$.

注7 闭环系统(8)是一个Markov跳变系统. 由于含有函数 $\theta(\sigma(k),k)$,必须要考虑攻击者的周期,使得系统的切换更加复杂.

引理1 对于给定的对称矩阵 $S=\begin{bmatrix}S_{11} & S_{12}\\ S_{21} & S_{22}\end{bmatrix}$,其中 $S_{11}\in R^{r\times r}$,以下3个条件等价:

1) $S<0$;

2) $S_{11}<0, S_{22}-S_{12}^{\mathrm{T}}S_{11}^{-1}S_{12}<0$;

3) $S_{22}<0, S_{11}-S_{12}S_{11}^{-1}S_{12}^{\mathrm{T}}<0$.

2 随机稳定性分析

本节将建立实现闭环系统(8)随机稳定的充分条件.

定义1 对于任意的初始条件 $\varphi(0)$,如果存在一个矩阵 $\Gamma>0$ 满足如下不等式,则闭环系统(8)是随机稳定的:

$$\sum_{k=0}^{\infty}\mathrm{E}\{\|z(k)\|^2|\varphi(0)\}\leqslant z(0)^{\mathrm{T}}\Gamma z(0). \tag{11}$$

定理1 结合式(1),给定控制器增益矩阵 K,如果存在适当维数的矩阵 $P_i>0,\forall i\in\{1,2\}$,满足下面的矩阵不等式,则闭环系统(8)是随机稳定的:

$$\Omega_i=\sum_{j=1}^{2}\Phi_i^{\mathrm{T}}\pi_{ij}P_j\Phi_i-P_i<0. \tag{12}$$

其中

$$\pi_{i1}=\alpha_{\sigma(k)},\ \pi_{i2}=1-\alpha_{\sigma(k)},$$

$$\Phi_1=\begin{bmatrix}A+BK & 0\\ I & 0\end{bmatrix},\ \Phi_2=\begin{bmatrix}A & BK\\ 0 & I\end{bmatrix}.$$

证明 构建闭环系统(8)的Lyapunov函数如下:

$$V(k)=z^{\mathrm{T}}(k)P_{\xi(k)}z(k).$$

沿着闭环系统(8)求解,可得

$$\begin{aligned}&\mathrm{E}[\Delta V(k)]=\\&\mathrm{E}[V(k+1,\xi(k+1))]-V(k,\xi(k))=\\&\mathrm{E}[z^{\mathrm{T}}(k+1)P_{\xi(k+1)}z(k+1)]-\\&z^{\mathrm{T}}(k)P_{\xi(k)}z(k)=\\&\mathrm{E}[z^{\mathrm{T}}(k)\Phi_{\xi(k)}^{\mathrm{T}}P_{\xi(k+1)}\Phi_{\xi(k)}z(k)]-\\&z^{\mathrm{T}}(k)P_{\xi(k)}z(k)=\\&z^{\mathrm{T}}(k)\Big(\sum_{j=1}^{2}\Phi_i^{\mathrm{T}}\pi_{ij}P_j\Phi_i-P_i\Big)z(k)=\\&z^{\mathrm{T}}(k)\Omega_i z(k).\end{aligned} \tag{13}$$

结合式(12),由(13)可得

$$\mathrm{E}[\Delta V(k)]\leqslant-\lambda_{\min}(-\Omega_i)z^{\mathrm{T}}(k)z(k)\leqslant\eta\|z(k)\|^2. \tag{14}$$

其中: $\eta=\inf\{\lambda_{\min}(-\Omega_i)\}$, $\lambda_{\min}(-\Omega_i)$ 表示矩阵 $-\Omega_i$ 的最小特征值. 由式(14)可知,对于任意的 $T>0$,有

$$\mathrm{E}[V(z(T+1))]-\mathrm{E}[V(z(0))]\leqslant-\eta\sum_{k=0}^{T}\mathrm{E}[\|z(k)\|^2]. \tag{15}$$

令 $T\to\infty$, 由式(15)可得

$$\sum_{k=0}^{\infty}\mathrm{E}[\|z(k)\|^2]\leqslant\frac{1}{\eta}\mathrm{E}[V(z(0))]<\infty. \tag{16}$$

根据定义1, 闭环系统(8)是随机稳定的. □

3　控制器设计

本节将根据定理1, 提出控制器的设计方法.

利用引理1, 不等式(12)可以表示成如下形式:

$$\begin{bmatrix}\Xi_1 & \Xi_2\\ * & \Xi_3\end{bmatrix}<0. \tag{17}$$

其中

$$\Xi_1=-\mathrm{diag}\{P_1^{-1},P_2^{-1}\},$$
$$\Xi_2=[\sqrt{\pi_{i1}}\Phi_1^{\mathrm{T}}\quad\sqrt{\pi_{i2}}\Phi_2^{\mathrm{T}}]^{\mathrm{T}},$$
$$\Xi_3=-P_i,$$
$$\pi_{i1}=\alpha_{\sigma(k)},\ \pi_{i2}=1-\alpha_{\sigma(k)},$$
$$\Phi_1=\begin{bmatrix}A+BK & 0\\ I & 0\end{bmatrix},\ \Phi_2=\begin{bmatrix}A & BK\\ 0 & I\end{bmatrix}.$$

显然, 矩阵不等式(17)中含有非线性项 P_1^{-1},P_2^{-1}. 因此, 首先引入新的矩阵变量 $X_i(i\in\{1,2\})$, 令 $X_i=P_i^{-1}$; 然后, 用 $X_1P_1=I, X_2P_2=I$ 代替矩阵不等式(17)中的非线性项 P_1^{-1} 和 P_2^{-1}; 最后, 利用锥补线性化(CCL)方法[33], 通过求解如下具有线性矩阵不等式约束的最小化问题, 得到状态反馈控制器:

$$\min_{X_i,P_i}\mathrm{Trace}\Big(\sum_{i=1}^{2}P_iX_i\Big); \tag{18}$$

$$\text{s.t.}\ \begin{bmatrix}\Xi_4 & \Xi_5\\ * & \Xi_6\end{bmatrix}<0,\ \begin{bmatrix}P_i & I\\ I & X_i\end{bmatrix}>0. \tag{19}$$

其中

$$\Xi_4=-\mathrm{diag}\{X_1,X_2\},$$
$$\Xi_5=[\Psi_1^{\mathrm{T}}\quad\Psi_2^{\mathrm{T}}]^{\mathrm{T}},$$
$$\Xi_6=-P_i,$$
$$\Psi_1=\sqrt{\pi_{i1}}(A_1+\bar{B}KH_1),$$
$$\Psi_2=\sqrt{\pi_{i2}}(A_2+\bar{B}KH_2),$$
$$\pi_{i1}=\alpha_{\sigma(k)},\ \pi_{i2}=1-\alpha_{\sigma(k)},$$
$$A_1=\begin{bmatrix}A & 0\\ I & 0\end{bmatrix},\ A_2=\begin{bmatrix}A & 0\\ 0 & I\end{bmatrix},\ \bar{B}=[B^{\mathrm{T}}\quad 0]^{\mathrm{T}},$$
$$H_1=[I\quad 0],\ H_2=[0\quad I].$$

上述具有线性矩阵不等式约束的最小化问题可通过迭代算法1计算求解.

算法1

Step 1: 令 $k=0, k_{\max}=100$, 找到一组可行解 P_i^0, X_i^0, K^0.

Step 2: 求解如下具有线性矩阵不等式约束的最小化问题:

$$(\tilde{P}_i,\tilde{X}_i,\tilde{K})=\min\mathrm{Trace}\sum_{i=1}^{2}(P_i^kX_i+P_iX_i^k),$$

s.t. 式(19).

令 $P_i^{k+1}=\tilde{P}_i, X_i^{k+1}=\tilde{X}_i, K^{k+1}=\tilde{K}$.

Step 3: 如果满足式(19), 则退出循环; 否则, 令 $k=k+1$, 返回 Step 2.

4　数值仿真

本节利用数值仿真来验证所设计控制策略的有效性.

假设攻击者一个工作周期持续时间为 $T=20$, 休眠持续时间为 $t_{\mathrm{off}}=10$, 总的运行时间为 $t=200$, 即运行周期为 $n\in\{1,2,\cdots,10\}$.

在休眠期内, 攻击者不发动攻击, 仅考虑无线信道的固有数据包随机丢失. 在攻击期内, 攻击者发动连续攻击, 使无线信道的数据包成功传输率下降. 假设系统处于攻击者休眠期时无线信道的数据包成功传输率为 $\alpha_1=0.9$, 处于攻击者攻击期时无线信道的数据包成功传输率下降为 $\alpha_2=0.55$.

例1　考虑文献[18]中的二维线性离散系统

$$A=\begin{bmatrix}0 & 1\\ 1.5 & -1\end{bmatrix},\ B=\begin{bmatrix}0\\ 1\end{bmatrix}.$$

选择系统初始值为 $x(0)=[2\quad -2]^{\mathrm{T}}$. 由式(18)可得矩阵 A_1、A_2、$\bar{B}$、H_1、H_2. 利用算法1得到控制增益矩阵为

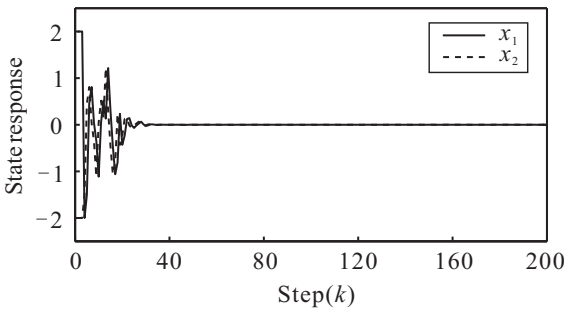

图 3　例1系统的状态轨迹

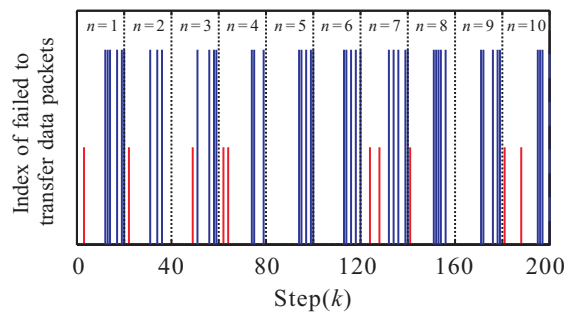

图 4　例1各周期内数据包丢失情况

$$K=[-1.6500\quad 1.1000].$$

仿真结果如图3和图4所示.

例2 考虑现实中的一些系统的矩阵维数较高,采用文献[32]中的四维线性离散系统进一步仿真验证. 该线性离散系统可描述为

$$A=\begin{bmatrix}1 & 1/5 & 0 & 0\\ 0 & 11/4 & 0 & 1/5\\ 1 & 1/5 & 1/3 & 3/4\\ 0 & -1 & 0 & 1/4\end{bmatrix},\ B=\begin{bmatrix}1 & 0\\ 0 & 1\\ 0 & 1\\ 1 & 0\end{bmatrix}.$$

选择系统初始值为$x(0)=[2\quad 1\quad -1\quad -2]^{\mathrm{T}}$. 由式(18)可得矩阵$A_1$、$A_2$、$\bar{B}$、$H_1$、$H_2$. 利用算法1得到控制增益矩阵为

$$K=\begin{bmatrix}-0.5700 & 0.4560 & 0.1000 & -0.1425\\ -0.5700 & -1.6815 & -0.1900 & -0.5415\end{bmatrix}.$$

仿真结果如图5和图6所示.

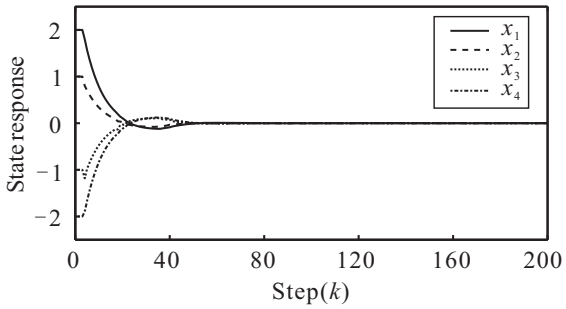

图5 例2系统的状态轨迹

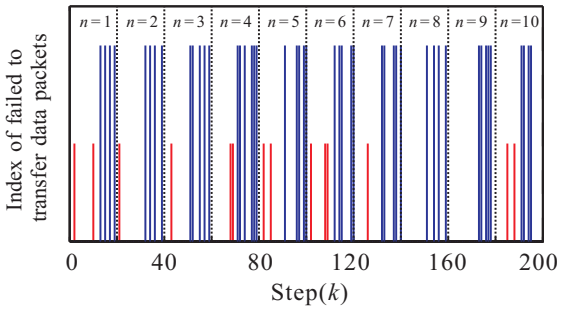

图6 例2各周期内数据包丢失情况

图3和图5所示为相应系统的状态轨迹. 考虑无线信道固有随机丢包,在DoS干扰攻击下,利用本文提出的控制策略,系统可以很快地实现稳定. 说明所提出的控制策略不仅有效,而且同样能解决高维系统的稳定问题,具有一定的广泛性.

图4和图6显示了处于攻击者不同工作周期内数据包随机丢失的情况. 其中,n表示所处的周期情况,短竖线表示处于攻击者休眠期内发生数据包丢失的时刻,长竖线表示处于攻击者攻击期内发生数据包丢失的时刻. 显然,由于受到攻击者在攻击期的连续攻击,使发生数据包丢失的时刻明显增多,数据包传输成功率有所下降.

5 结 论

本文针对一类无线信道存在数据包随机丢失的CPSs,采用状态反馈控制,研究CPSs遭受DoS干扰攻击情况下的稳定问题,提出了一种能量受限的、周期的DoS干扰攻击模型. 该模型有明确的周期结构,并在攻击期发动连续DoS干扰攻击,目的是降低无线信道的数据包传输成功率. 基于随机Lyapunov函数、线性矩阵不等式方法和锥补线性化方法,得到了实现CPS稳定的充分条件和控制器的设计方法. 数值仿真验证了该控制策略不仅有效,而且适用于高维矩阵系统.

由于恶意攻击对CPSs的正常运行造成很大影响,在未来的研究中,将主要解决以下3个问题:

1)改进本文提出的DoS干扰攻击模型;

2)考虑事件触发机制,在节约网络资源的条件下,实现DoS干扰攻击下的CPS稳定;

3)考虑多种攻击同时存在的情况,建立多种攻击的统一模型,实现多种恶意攻击下的CPS稳定.

参考文献(References)

[1] Derler P, Lee E A, Vincentelli A S. Modeling cyber-physical systems[J]. Proc of the IEEE, 2012, 100(1): 13-28.

[2] Sampigethaya K, Poovendran R. Aviation cyber-physical systems: Foundations for future aircraft and air transport[J]. Proc of the IEEE, 2013, 101(8): 1834-1855.

[3] Mo Y L, Kim T H, Brancik K, et al. Cyber-physical security of a smart gird infrastructure[J]. Proc of the IEEE, 2012, 100(99): 1-15.

[4] Liu Y G, Xu B G, Ding Y H. Convergence analysis of cooperative breaking control for interconnected vehicle systems[J]. IEEE Trans on Intelligence Transport Systems, 2017, 18(7): 1894-1906.

[5] Lee I, Sokolsky O, Chen S J, et al. Challenges and research directions in medical cyber-physical systems[J]. Proc of the IEEE, 2012, 100(1): 75-90.

[6] Jazdi N. Cyber physical system in the context of industry 4.0[C]. Proc of the IEEE Int Conf on Automation, Quality and Testing, Robotics. Cluj-Napoca, 2014: 1-4.

[7] Gungor V C, Hancke G P. Industrial wireless sensor networks: Challenges, design principles, and technical approaches[J]. IEEE Trans on Industrial Electronics, 2009, 56(10): 4258-4265.

[8] Cao X H, Chen J M, Xiao Y, et al. Building-Environment control with wireless sensor and actuator networks: centralized versus distributed[J]. IEEE Trans on Industrial Electronics, 2010, 57(11): 3596-3605.

[9] Frawell J P, Rohozinski R. Stuxnet and the future of cyber war[J]. Survival, 2011, 53(1): 23-40.

[10] Iasiello E. Cyber attack: A dull tool to shape foreign policy[C]. Int Conf on Cyber Conflict. Tallinn, 2013: 1-18.

[11] Sundaram S, Hadjicosyis R. Distributed function calculation via linear iterative strategies in the presence of malicious agents[J]. IEEE Trans on Automatic Control, 2011, 56(7): 1495-1508.

[12] Cárdenas A A, Amin S, Sastry S. Secure control: Towards survivable cyber-physical systems[C]. Proc of the 28th Conf on Distributed Computing Systems Workshops. Beijing, 2008: 495-500.

[13] Teixeira A, Perez D, Sandberg H, et al. Attack models and scenarios for networked control systems[C]. Proc of 1st Int Conf on High Confidence Networked Systems. Beijing, 2012: 55-64.

[14] Cetinkaya A, Ishii H, Hayakawa T. Networked control under random and malicious packet losses[J]. IEEE Trans on Automatic Control, 2017, 62(5): 2434-2449.

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

[16] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack scheduling in wireless networked control system[J]. IEEE Trans on Control System Technology, 2016, 24(3): 843-852.

[17] Peng L H, Cao X H, Sun C Y, et al. Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems[J]. Neurocomputing, 2018, 272: 571-583.

[18] Foroush H S, Martínez S. On event-triggered control of linear systems under periodic denial of service attacks[C]. Proc of IEEE 51st Annual Conf on Decision and Control. Maui, 2012: 2551-2556.

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

[20] Feng S, Tesi P. Resilient control under denial-of-service: Robust design[J]. Automatica, 2017, 79: 42-51.

[21] Dolk V S, Tesi P. Event-triggered control systems under denial-of-service attacks[J]. IEEE Trans on Control Network Systems, 2017, 4(1): 93-104.

[22] 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 Trans on Automatic Control, 2015, 60(10): 2831-2836.

[23] Yuan Y, Yuan H H, Guo L, et al. Resilient control of networked control system under DoS attacks: A unified game approach[J]. IEEE Trans on Industrial Informatics, 2016, 12(5): 1786-1794.

[24] Ding K M, Li Y Z, Quevedo D E, et al. Multi-channel transmission schedule for remote state estimation under DoS attacks[J]. Automatica, 2017, 78: 194-201.

[25] Zhao Y H, He X, Zhou D H. Optimal joint control and triggering strategies against denial of service attacks: A zero-sum game[J]. IET Control Theory Applications, 2017,11(4): 2352-2360.

[26] Wu J, Chen T W. Design of networked control systems with packet dropouts[J]. IEEE Trans on Automatic Control, 2007, 52(7): 1314-1319.

[27] Wang Z D, Ho D W C, Liu Y R, et al. Robust H_∞ control for a class of nonlinear discrete time-delay stochastic systems with missing measurements[J], Automatica, 2009, 45: 684-691.

[28] Xu W Y, Trappe W, Zhang Y Y, et al. The feasibility of launching and detecting jamming attacks in wireless networks[C]. Proc of the 6th ACM Int Symposium on Mobile Ad Hoc Networking and computing. Urbana-Champaign, 2005: 46-57.

[29] Xu W Y, Ma K, Trappe W, et al. Jamming sensor networks: Attack and defense strategies[J]. IEEE Network, 2006, 20(3): 41-47.

[30] Richard P. Modern communications jamming: Principles and techniques[M]. Norwood: Artech House, 2011: 504-508.

[31] Wang Z D, Ho D W C, Liu Y R, et al. Variance-constrained filtering for uncertain stochastic systems with missing measurements[J]. IEEE Trans on Automatic Control, 2003, 48(7): 1254-1258.

[32] Zhang W A, Yu L. Output feedback stabilization of networked control systems with packet dropouts[J]. IEEE Trans on Automatic Control, 2007, 52(9): 1705-1710.

[33] Chaomel L E, Oustry F, Aitrami M. A cone complementarity linearization algorithm for static output feedback and related problems[J]. IEEE Trans on Automatic Control, 1997, 42(8): 1171-1176.

作者简介

汪慕峰(1990−), 男, 博士生, 从事信息物理系统安全理论与技术的研究, E-mail: 201610102003@mail.scut.edu.cn;

胥布工(1956−), 男, 教授, 博士生导师, 从事信息物理系统安全、无线传感器与执行器网络等研究, E-mail: aubgxu@scut.edu.cn.

(责任编辑: 李君玲)