DoS攻击下基于切换Luenberger观测器的冗余控制

赖绍禹[1], 陈 博[1,2†], 俞 立[1,2]

(1. 浙江工业大学 信息工程学院, 浙江 杭州 310023; 2. 浙江工业大学 网络空间安全研究院, 浙江 杭州 310023)

摘要: 研究了DoS攻击下网络化控制系统基于观测器的控制器设计问题. 首先, 提出了一种具有多个增益的切换Luenberger观测器, 实现了无DoS攻击时系统状态的间歇性估计. 根据获得的估计值, 控制器同时计算了系统当前以及未来一段时域的控制信号, 并将其封装在一个数据包中发送给执行器, 保证了系统在有无DoS攻击时都有合适的控制输入更新. 其次, 利用构造的切换系统对DoS攻击下观测器与控制器的不同动态进行了统一的建模, 基于多Lyapunov函数方法推导了任意切换律下系统指数稳定的充分条件, 并给出了相应的观测器与控制器设计方法. 最后, 通过网络化倒立摆系统的实验验证了所提方法的有效性.

关键词: 拒绝服务攻击; 切换系统; Luenberger观测器; 输出反馈

引用格式: 赖绍禹, 陈博, 俞立. DoS攻击下基于切换Luenberger观测器的冗余控制. 控制理论与应用, 2020, 37(4): 758 – 766

DOI: 10.7641/CTA.2019.90326

Switching-Luenberger-observer-based redundant control under DoS attacks

LAI Shao-yu[1], CHEN Bo[1,2†], YU Li[1,2]

(1. College of Information Engineering, Zhejiang University of Technology, Hangzhou Zhejiang 310023, China;
2. Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou Zhejiang 310023, China)

Abstract: A observer-based redundant control method is proposed for networked control systems under denial-of-service (DoS) attacks. First, a switching Luenberger observer with multiple gains is designed such that the intermittent state estimation is achieved in the absence of DoS attacks. Based on the obtained state estimates, the current control input along with some future control inputs are calculated and sent to the actuators using a packet simultaneously, and then the actuators always have appropriate control inputs to be applied. In this case, the dynamics of the observer and controller under DoS attacks is modeled by a constructed switching system model. By resorting to the multiple Lyapunov functions, the exponentially stable conditions of the constructed switching system model are derived under arbitrary switching laws. Moreover, the corresponding observer and controller are also designed. Finally, an experiment on networked inverted pendulum system is used to show the effectiveness of the proposed method.

Key words: denial-of-service attack; switching system; Luenberger observer; output feedback

Citation: LAI Shaoyu, CHEN Bo, YU Li. Switching-Luenberger-observer-based redundant control under DoS attacks. *Control Theory & Applications*, 2020, 37(4): 758 – 766

1 引言

近年来, 以5G为代表的通信技术的快速发展极大地改变了传统控制系统的面貌. 通过使用专用或公共网络进行控制系统各个模块之间的通信, 使得控制技术与通信技术发生了深度的融合[1]. 与此同时, 网络化控制系统(networked control systems, NCSs)、信息物理系统(cyber-physical systems, CPSs)等概念也应运而生. 本质上讲, 无论是NCSs还是CPSs, 其都是控制系统在融合新一代的通信、感知、计算等技术后升级换代的产物[2–4]. 随着网络通信技术在控制系统中的大量运用, 网络化在给控制系统的部署、维护以及扩展带来了极大灵活性的同时也使控制系统暴露在了网络攻击的威胁之下. 近年来, 频繁发生的关于工业控制系统的安全事件也充分暴露了控制系统在网络环境下的巨大安全隐患. 2010年, 伊朗位于纳坦兹的铀浓缩工厂遭受了蠕虫病毒Stuxnet的攻击, 并导致

收稿日期: 2019−05−07; 录用日期: 2019−09−05.

†通信作者. E-mail: bchen@aliyun.com.

本文责任编委: 夏元清.

国家自然科学基金项目(61673351, 61973277)资助.

Supported by the National Natural Science Foundation of China (61673351, 61973277).

了近千台离心机损毁, 同时Stuxnet病毒也攻击了Bushehr核电站, 最终Bushehr核电站被迫关闭、伊朗核计划也被迫推迟[5]. 2012年, “火焰”病毒席卷中东地区, 对石油工业控制系统的安全运行造成了重大影响[6]. 2015年, 专门针对电力系统的Black-Energy3病毒攻击了乌克兰的电力部门, 导致7座110 kV和23座35 kV变电站长达3个小时的断电, 22万人的电力供应受到影响[7]. 由此可见, 控制系统在网络环境下面临的安全威胁十分严峻, 特别是关系到国民经济的重要工业控制系统, 一旦其受到攻击, 随之而来的人力、物力以及经济损失将可能是不可估量的[8]. 因此, 研究网络攻击下控制系统的安全问题具有重要的现实意义[9].

目前, 针对网络化控制系统的网络攻击可大致概括为拒绝服务(denial-of-service, DoS)攻击[10]、重放攻击[11]和虚假数据注入攻击[12]这3类. 其中, DoS攻击又是最容易实施且经济损失最重大的一种攻击[13]. 因此, 如何保证DoS攻击下控制系统的安全运行引起了学术界以及工业界的广泛关注. 从控制理论的视角出发, 有关DoS攻击下控制系统安全问题的研究主要集中在以下两个方面:

1) 基于估计(滤波)理论, 研究DoS攻击下控制系统的状态估计问题: 文献[14]基于多传感器信息冗余的优势, 提出了DoS攻击下分布式降维融合估计方法, 实现了DoS攻击下系统状态的有效估计. 文献[15]从攻击者的角度出发, 研究了有能量约束的DoS攻击者的攻击策略和系统状态的估计性能之间的关系, 并从理论上给出了攻击者在能量约束下使估计误差协方差最大的攻击策略. 文献[16]研究了有能量约束的DoS攻击者对远程两个无线传感器的DoS攻击调度问题, 其中两个传感器是通过不同的频带发送量测数据的, 并且攻击者一次只能攻击一个信道. 文献[17]基于博弈论研究了有能量约束的传感器节点向远程估计器发送量测值的策略和攻击者对通信链路发动DoS攻击策略之间的博弈问题, 并证明了最优状态估计策略是传感器节点和攻击者零和博弈的纳什平衡点.

2) 从系统控制的角度出发, 研究DoS攻击对系统性能的影响以及应对措施: 文献[18]从攻击频率和持续时间两个维度对DoS攻击行为进行了建模, 并导出了系统在DoS攻击下能够保持输入–状态稳定的充分条件. 文献[19]针对基于输出反馈的动态事件触发控制系统, 提出了一种能够容忍DoS攻击的控制器设计框架, 并实现了系统的控制性能与系统对DoS攻击的鲁棒性之间的平衡. 文献[20]研究了能量约束下DoS攻击攻击调度方式和系统控制性能之间的关系, 并从理论上导出了使得线性二次高斯控制器代价函数最大的最优攻击策略. 文献[21]将拒绝服务攻击和控制器视为博弈双方, 研究了它们之间的零和博弈问题, 并从理论上证明了攻击者和防御者之间的最优博弈策略为两者之间的鞍点平衡点. 文献[22]则根据控制器和DoS攻击者在不同情形下博弈结果的差异, 提出了一种基于博弈结果的切换控制策略. 文献[23]利用Markov随机博弈的方法研究了多通道传输框架下对信道的DoS攻击和量测数据传输策略之间的博弈问题, 并通过动态规划以及值迭代方法给出了DoS攻击下的最优控制策略.

尽管DoS攻击下控制系统安全问题研究取得了不错的进展, 但是目前的研究大多局限了只考虑DoS攻击下的状态估计问题或控制问题, DoS攻击下状态估计器与控制器的联合设计问题仍然缺乏足够的关注. 为此, 本文研究了DoS攻击下控制系统的观测器与控制器的联合设计问题. 针对有能量约束的DoS攻击造成通信链路阻塞的情形, 首先提出了一种具有多个增益的切换Luenberger观测器, 实现了对系统状态的间歇性估计. 通过将文献[24]中DoS攻击下基于状态反馈的冗余控制思想进行扩展, 在未发生DoS攻击的时刻, 观测器基于系统输出首先计算出当前时刻的状态估计值, 然后控制器基于状态估计值计算出当前以及未来一段时域内冗余的控制信号, 并将其封装在一个数据包中发送给执行器. 执行器则根据DoS攻击发生的情况选择适当数量的控制信号用于执行, 从而保证了执行器在有无DoS攻击的情况下都有合适的控制输入. 该方法能够有效地克服执行器在DoS攻击下采用保持输入或零输入策略的盲目性, 使系统在DoS攻击下也能实现良好的控制性能. 其次, 通过引入一个同时包含观测器和系统状态的增广变量, 用切换系统对不同持续时间DoS攻击下的观测器和系统状态的动态特性进行了统一的描述, 并基于多Lyapunov函数方法推导了保证切换系统在任意切换律下指数稳定的充分条件, 同时给出了基于观测器的控制器设计方法. 最后, 通过网络化控制倒立摆的实验验证了所提方法的有效性.

说明: $\mathbb{R}^n$和$\mathbb{R}^{m\times n}$分别表示n维和$m\times n$维实欧几里得空间; $\mathbb{N}$表示非负整数集; $\mathbb{N}_{[c1,c2]}$表示整数集$\{t\in\mathbb{N}|c1\leqslant t\leqslant c2\}$; $A>0$表示A是一个具有适当维数的正定矩阵; $\|x\|$表示向量x的2范数; $\sigma_{\max}(A)$和$\sigma_{\min}(A)$分别表示矩阵A的最大奇异值和最小奇异值; I和0分别表示具有适当维数的单位阵和零矩阵; A^{T}表示矩阵A的转置; 矩阵中的符号$*$表示矩阵的对称块; $\{\cdot\}$表示包含元素$\cdot$的集合; $\cup$表示集合的并操作运算符.

2　问题描述

考虑如图1所示的由传感器、观测器、控制器和执行器组成的网络化控制系统.

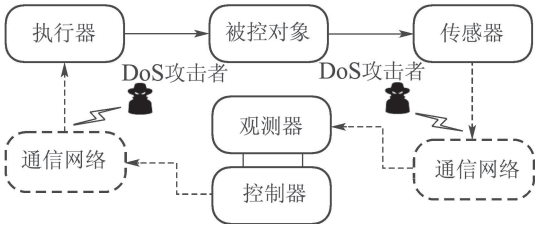

图 1 DoS攻击下的网络化控制系统

Fig. 1 The networked control system under DoS attacks

在图1所示的网络化控制系统中, 传感器通过网络将获取的量测数据发送给观测器, 观测器则根据传感器的量测值以及系统的输入给出系统的状态估计, 并通过内部网络发送给执行器. 控制器则根据观测器的状态估计值计算出对应的控制信号并通过网络发送给执行器. 外部环境中存在的攻击者可对传感器到观测器或控制器到执行器的通信链路发动DoS攻击进而阻断数据的传输. 其中, 被控对象的动态特性可以由如下的离散时间线性状态空间模型描述:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k), \\ y(k) = Cx(k) + Du(k), \end{cases} \tag{1}$$

其中: $x(k) \in \mathbb{R}^n$是系统状态, $u(k) \in \mathbb{R}^m$是控制输入, $y(k) \in \mathbb{R}^p$是量测输出; A, B, C和D为已知的具有适当维数的常系数矩阵.

在进一步讨论DoS攻击情形之前, 首先本文对DoS攻击行为做出如下假设.

假设 1 由于能量约束, DoS攻击者能够连续中断的最大通信次数为N.

为了对DoS攻击下系统的状态进行估计, 本文引入图2所示的切换Luenberger观测器.

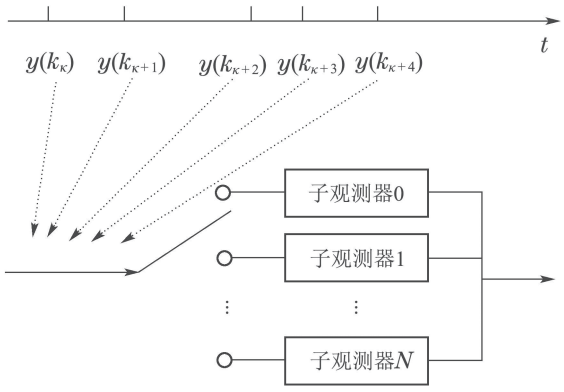

图 2 切换Luenberger观测器示意图

Fig. 2 The schematic of switching Luenberger observer

图2中, 每个子观测器的动态特性可以由如下的方程进行描述:

$$\begin{cases} \hat{x}(k_{\kappa+1}) = F_{\sigma(k_\kappa)}\hat{x}(k_\kappa) + \bar{u}_{\sigma(k_\kappa)}(k_\kappa) + \\ \qquad\qquad L_{\sigma(k_\kappa)}(y(k_\kappa) - \hat{y}(k_\kappa)), \\ \hat{y}(k_\kappa) = C\hat{x}(k_\kappa) + Du(k_\kappa), \end{cases} \tag{2}$$

其中$k_\kappa (k_\kappa \in \mathbb{N}, \kappa \in \mathbb{N})$表示切换Luenberger观测器的切换点, 即传感器到观测器以及控制器到执行器的网络都没有发生DoS攻击的采样时刻.

$$\sigma(k_\kappa) : \mathbb{N} \to M \triangleq \{0, 1, \cdots, N\}$$

是一个依赖于DoS攻击行为的切换信号. $\sigma(k_\kappa)$的取值表示在时刻k_κ之后数据传输被DoS攻击连续中断的次数, 即从时刻$k_\kappa + 1$起有连续$\sigma(k_\kappa)$次的数据传输被DoS攻击中断(若$\sigma(k_\kappa) = 0$则表示在采样时刻$k_\kappa + 1$没有DoS攻击发生). $\hat{x}(k_\kappa)$为系统状态的估计值, $y(k_\kappa)$为量测的系统输出, $\hat{y}(k_\kappa)$为估计的系统输出, $L_{\sigma(k_\kappa)}$为需要设计的观测器增益, $F_{\sigma(k_\kappa)}$定义为

$$F_{\sigma(k_\kappa)} \triangleq A^i (i = \sigma(k_\kappa)),$$

$\bar{u}_{\sigma(k_\kappa)}$为时刻$k_\kappa$到$k_{\kappa+1}$之间系统的输入对系统状态$x(k_{\kappa+1})$叠加量的总和. 很明显, 切换Luenberger观测器中相邻的两个切换点k_κ和$k_{\kappa+1}$满足

$$k_{\kappa+1} = k_\kappa + \sigma(k_\kappa) + 1, \tag{3}$$

其中$k_0 = 0$.

注意到式(2)给出的切换Luenberger观测器实际上是一种间歇性观测器, 即它只在无DoS攻击的时刻工作并给出系统当前的状态估计. 为了实现这样的工作模式, 关键点是观测器需要在每个采样时刻确定此时传感器到观测器或控制器到执行器的通信链路是否被DoS攻击中断. 在每个采样时刻, 观测器可以根据是否能接收传感器的量测数据来判断传感器到观测器的通信链路是否被DoS攻击中断. 为了使观测器在每个采样时刻能够判断控制器到执行器的通信链路是否被DoS攻击中断, 一个简单可行的方法是执行器在收到控制信号之后立即向控制器发送一个应答信号(ACK信号)来确认数据是否传输成功. 如果控制器收到ACK信号, 则说明控制器到执行器的通信链路没有被DoS攻击中断, 执行器成功收到控制信号, 根据式(3), 此时系统切换到下一个子系统.

引入的切换Luenberger观测器给出了被控对象在没有DoS攻击时刻的状态估计值. 结合文献[24]中在DoS攻击下基于状态反馈的冗余控制思想, 本文将根据Luenberger观测器的状态估计值设计一种冗余的控制律使得执行器在有无DoS攻击的情况下都有合适的控制信号. 本文的核心思想如下: 在没有DoS攻击的时刻k_κ, 控制器根据Luenberger观测器给出的状态估计$\hat{x}(k_\kappa)$计算出当前以及部分未来时域的控制输入, 并将它们封装在一个数据包中同时发送给执行器. 执行器则根据DoS攻击的发生情况选择执行部分或全部的控制信号. 基于这一思想, 本文给出如下的冗余控制律:

$$u(k_\kappa + s) = K_s \hat{x}(k_\kappa), \tag{4}$$

其中: $s = 0, 1, \cdots, \sigma(k_\kappa)$, $\sigma(k_\kappa)$是与式(2)给出的切换Luenberger观测器中$\sigma(k_\kappa)$相一致的切换信号. $u(k_\kappa)$,

$u(k_\kappa+1),\cdots,u(k_\kappa+s)$分别表示执行器在离散时间时刻$k_\kappa, k_\kappa+1,\cdots,k_\kappa+s$的控制输入. $K_0, K_1, \cdots, K_N$是需要进行设计的控制器增益. 控制律(4)的具体实施过程如下: 控制器在每个没有发生DoS攻击的离散时间时刻k_κ根据观测器对当前状态的估计值$\hat{x}(k_\kappa)$计算出$N+1$个控制输入

$$U(k_\kappa)=[u^{\mathrm{T}}(k_\kappa)\ \ u^{\mathrm{T}}(k_\kappa+1)\ \ \cdots\ \ u^{\mathrm{T}}(k_\kappa+N)]^{\mathrm{T}},$$

并将其封装在一个数据包中同时发送给执行器. 若在$k_\kappa+1$时刻有新的数据包到达执行器, 则执行器只执行$U(k_\kappa)$中的第1个控制输入$u(k_\kappa)$. 否则, 执行器在执行完控制信号$u(k_\kappa)$后, 将会依次执行$u(k_\kappa+1), \cdots, u(k_\kappa+s)$直到下一个新的数据包到达. 当新的数据包到达时, 执行器便会丢弃原有的数据包并立即去执行新的数据包中的控制输入. 这里控制律的冗余性体现在不是每次计算的所有控制信号都会被执行器执行.

于是, 根据DoS攻击连续中断通信次数的差异, 被控对象在相邻两个DoS攻击未发生的时刻(即切换点)间的动态特性可以表示为

$$\begin{aligned}&x(k_{\kappa+1})=\\&x(k_\kappa+i+1)=\\&(A^iBK_0+A^{i-1}BK_1+\cdots+A^0BK_i)\times\\&\hat{x}(k_\kappa)+A^{i+1}x(k_\kappa),\end{aligned}\tag{5}$$

其中$i=\sigma(k_\kappa)$. 根据$\bar{u}_{\sigma(k_\kappa)}(k_\kappa)$的定义, 式(5)表明

$$\begin{aligned}\bar{u}_{\sigma(k_\kappa)}(k_\kappa)=&(A^iBK_0+A^{i-1}BK_1+\cdots+\\&A^0BK_i)\hat{x}(k_\kappa),\ i=\sigma(k_\kappa).\end{aligned}$$

定义估计误差

$$e(k_\kappa)\triangleq\hat{x}(k_\kappa)-x(k_\kappa),\ z(k_\kappa)\triangleq[x^{\mathrm{T}}(k_\kappa)\ \ e^{\mathrm{T}}(k_\kappa)]^{\mathrm{T}}.$$

结合式(2)以及式(5), 本文引入如下的切换系统模型来对观测器和被控对象的动态进行统一的描述:

$$z(k_{\kappa+1})\triangleq H_{\sigma(k_\kappa)}z(k_\kappa),\tag{6}$$

其中:

$$H_{\sigma(k_\kappa)}\triangleq\begin{bmatrix}F_{\sigma(k_\kappa)}+B_{\sigma(k_\kappa)} & B_{\sigma(k_\kappa)}\\ 0 & F_{\sigma(k_\kappa)}-L_{\sigma(k_\kappa)}C\end{bmatrix},$$

$$B_{\sigma(k_\kappa)}=A^iBK_0+A^{i-1}BK_1+\cdots+A^0BK_i,$$

$$F_{\sigma(k_\kappa)}\triangleq A^i,\ i=\sigma(k_\kappa).$$

注 1　这里的控制方法的可行性得益于网络中数据包的封装特性. 以链路层的Ethernet封装为例, 每个以太网帧的数据字段长度有一个最小46字节的要求[25–26]. 这意味着, 在除去以太网帧中封装的上层数据包的头部情况下发送1个字节或几个字节之间的数据将会消耗相同的网络资源. 通常, 本文需要数据封装不会超过以太网帧数据字段的最小字节要求. 因此, 本文提出的控制方法不会增加额外的网络负载.

注 2　这里的控制方法同样可以处理NCSs的丢包问题. 然而, DoS攻击诱导的丢包现象和网络中固有的丢包现象的重要区别在于: DoS攻击造成的丢包率会远远大于网络中本身存在的丢包率并且网络中本身存在的丢包过程往往是一个随机过程, 而DoS攻击造成丢包现象则往往不满足某一特定的概率分布[13,27]. 因此, 这里的控制方法更具有一般性.

进一步, 作者将相邻两个切换点的系统状态$z(k_\kappa)$和$z(k_{\kappa+1})$(即没有DoS攻击时刻的状态)之间的系统状态记为$z(k_{j,\kappa})$, 系统状态$z(k_{j,\kappa})$中的下标$j\in\mathbb{N}_{[1,N]}$表示系统状态$z(k_{j,\kappa})$是系统状态$z(k_\kappa)$后的第j个受到DoS攻击时的状态, 即

$$x(k_\kappa+j)=x(k_{j,\kappa}),\ k_\kappa<k_{j,\kappa}<k_{\kappa+1}.$$

根据以上系统状态的定义, 可知$z(k)$, $z(k_\kappa)$ 和$z(k_{j,\kappa})$满足$\{z(k)\}=\{z(k_\kappa)\}\cup\{z(k_{j,\kappa})\}$.

3　稳定性分析与观测器、控制器设计

在本节中, 作者将推导出使切换系统模型(6)在任意切换律下指数稳定的充分条件以及对应的观测器、控制器设计方案. 在给出主要的结论之前, 需要引入以下的定义及引理:

定义 1　对于切换系统模型(6), 若存在正整数c和$\lambda<1$使得如下的不等式

$$\|z(k)\|\leqslant c\lambda^k\|z(0)\|$$

成立, 则系统(6)是指数稳定的.

引理 1　对于任意一个矩阵$F\in\mathbb{R}^{n\times n}$以及任意一个向量$x\in\mathbb{R}^n$, 如下的不等式成立:

$$\alpha_2\|x\|\leqslant\|Fx\|\leqslant\alpha_1\|x\|,$$

其中α_1, α_2分别是F的最大奇异值和最小奇异值[28].

引理 2(Schur补引理[29])　假设一个对称矩阵S能够划分为以下4个部分:

$$S=\begin{bmatrix}S_{11} & S_{12}\\ S_{12}^{\mathrm{T}} & S_{22}\end{bmatrix}.$$

那么以下3个条件是等价的:

1) $S<0$;

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

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

3.1　稳定性分析

定理 1　对于切换系统(6), 若存在常数$0<\lambda_i<1$, $u>0$以及适当维数的矩阵$P_i>0$, $i\in M$使得以下的矩阵不等式

$$-\lambda_iP_i+H_i^{\mathrm{T}}P_iH_i<0,\tag{7}$$

$$P_\alpha<\mu P_\beta,\ \forall\alpha,\ \beta\in M,\tag{8}$$

$$\rho\triangleq\max\{\lambda_i\mu|i\in M\}<1\tag{9}$$

成立, 则系统(6)将会是指数稳定的.

证 为式(6)表示的切换系统模型中的每个子系统选择如下的分段Lyapunov函数:

$$V_{\sigma(k_\kappa)}(k_\kappa)=z^{\mathrm{T}}(k_\kappa)P_{\sigma(k_\kappa)}z(k_\kappa), \tag{10}$$

$$V_{\sigma(k_\kappa)}(k_{\kappa+1})=z^{\mathrm{T}}(k_{\kappa+1})P_{\sigma(k_\kappa)}z(k_{\kappa+1}), \tag{11}$$

其中下标$\sigma(k_\kappa)$表明式(10)–(11)中的Lyapunov函数对应位于切换点k_κ和$k_{\kappa+1}$之间的子系统$\sigma(k_\kappa)=i,\ i\in M$. 分别用$z^{\mathrm{T}}(k_\kappa)$和$z(k_\kappa)$左乘和右乘不等式(7)可以得到

$$[F_{\sigma(k_\kappa)}\ \ z(k_\kappa)]^{\mathrm{T}}P_{\sigma(k_\kappa)}[F_{\sigma(k_\kappa)}\ \ z(k_\kappa)]-\lambda_{\sigma(k_\kappa)}z^{\mathrm{T}}(k_\kappa)P_{\sigma(k_\kappa)}z(k_\kappa)<0, \tag{12}$$

其中$\lambda_{\sigma(k_\kappa)}$和$F_{\sigma(k_\kappa)}$对应位于切换点$k_\kappa$和$k_{\kappa+1}$之间的子系统$\sigma(k_\kappa)=i,\ i\in M$. 根据式(10)–(11), 有

$$V_{\sigma(k_\kappa)}(k_{\kappa+1})<\lambda_{\sigma(k_\kappa)}V_{\sigma(k_\kappa)}(k_\kappa). \tag{13}$$

类似地, 可以得到

$$V_{\sigma(k_{\kappa+1})}(k_{\kappa+2})<\lambda_{\sigma(k_{\kappa+1})}V_{\sigma(k_{\kappa+1})}(k_{\kappa+1}). \tag{14}$$

注意到如下的事实:

$$\begin{cases}V_{\sigma(k_{\kappa+1})}(k_{\kappa+1})=z^{\mathrm{T}}(k_{\kappa+1})P_{\sigma(k_{\kappa+1})}z(k_{\kappa+1}),\\ V_{\sigma(k_\kappa)}(k_{\kappa+1})=z^{\mathrm{T}}(k_{\kappa+1})P_{\sigma(k_\kappa)}z(k_{\kappa+1}),\end{cases} \tag{15}$$

以及条件(8), 可以得到

$$V_{\sigma(k_{\kappa+1})}(x_{\kappa+1})<\mu V_{\sigma(k_\kappa)}(k_{\kappa+1})<\mu\lambda_{\sigma(k_\kappa)}V(k_\kappa), \tag{16}$$

进一步, 通过归纳可以得到如下的递推关系:

$$V_{\sigma(k_{\kappa+2})}(k_{\kappa+2})<\rho V_{\sigma(k_{\kappa+1})}(k_{\kappa+1})<\cdots<\rho^{\kappa+1}V_{\sigma(k_1)}(k_1)<\rho^{\kappa+2}V_{\sigma(k_0)}(k_0), \tag{17}$$

其中$\rho\triangleq\max\{\lambda_i\mu|i\in M\}$. 由式(9)知$\rho<1$, 所以当$\kappa\to\infty$时, $V_{\sigma(k_\kappa)}(k_\kappa)$将收敛到0. 由$V_{\sigma(k_\kappa)}(k_\kappa)$的正定性, 本文可以进一步得出结论: 当$\kappa\to\infty$时, 状态序列$\{\mathrm{z}(k_\kappa)\}$也必将收敛到0. 进一步, 根据引理1, 对于每个$z(k_{j,\kappa})$, 如下的不等式成立:

$$\|z(k_{j,\kappa})\|\leqslant\varepsilon\|z(k_\kappa)\|, \tag{18}$$

其中: $\varepsilon\triangleq\max\{\sigma_{\max}(H_i)\},\ i=0,1,\cdots,N$. 不等式(18)表明每一个$\|z(k_{j,\kappa})\|$都不大于$\|z(k_\kappa)\|$的$\varepsilon$倍. 因此当$\kappa\to\infty$时, 状态序列$z(k_{j,\kappa})$也必然将会收敛到0. 又因为$\{z(k)\}=\{z(k_\kappa)\}\cup\{z(k_{j,\kappa})\}$, 所以在当$k\to\infty$时$z(k)$会收敛到0, 所以系统(6)是稳定的. 另一方面, 由式(17)可以得到

$$\beta_1\|z(k_{\kappa+2})\|^2\leqslant V_{\sigma(k_{\kappa+2})}(k_{\kappa+2})<\cdots<\rho^{\kappa+2}V_{\sigma(0)}(0)\leqslant\rho^{\kappa+2}\beta_2\|z(0)\|^2, \tag{19}$$

其中: $\beta_1=\min\limits_{\forall i\in M}(\sigma_{\min}(P_i)),\ \beta_2=\max\limits_{\forall i\in M}(\sigma_{\max}(P_i))$. 进一步, 可以得到

$$\|z(k_{\kappa+2})\|<(\sqrt{\rho})^{\kappa+2}\sqrt{\frac{\beta_2}{\beta_1}}\|z(0)\|. \tag{20}$$

结合不等式(18), 类似地, 可以得到

$$\|x(k_{j,\kappa+2})\|<\varepsilon(\sqrt{\rho})^{\kappa+2}\sqrt{\frac{\beta_2}{\beta_1}}\|x(0)\|. \tag{21}$$

注意到$k_{\kappa+2}$, $k_{j,\kappa+2}$和κ有如下的关系:

$$k_{\kappa+2}\leqslant(N+1)(\kappa+2), \tag{22}$$

当$\kappa+2\geqslant N$,

$$k_{j,\kappa+2}\leqslant(N+1)(\kappa+2)+N\leqslant(N+2)(\kappa+2). \tag{23}$$

综合式(20)–(23)以及$\rho<1$, 可以推出

$$\|z(k_{\kappa+2})\|<\left(\sqrt[2(N+1)]{\rho}\right)^{k_{\kappa+2}}\sqrt{\frac{\beta_2}{\beta_1}}\|z(0)\|, \tag{24}$$

当$\kappa+2\geqslant N$时,

$$\|z(k_{j,\kappa+2})\|<\varepsilon\left(\sqrt[2(N+2)]{\rho}\right)^{k_{j,\kappa+2}}\sqrt{\frac{\beta_2}{\beta_1}}\|z(0)\|. \tag{25}$$

比较式(24)–(25), 可以发现在N个切换点之后的$z(k)$都满足如下的不等式:

$$\|z(k)\|<\varepsilon\left(\sqrt[2(N+2)]{\rho}\right)^{k}\sqrt{\frac{\beta_2}{\beta_1}}\|z(0)\|. \tag{26}$$

由于这里的切换点指的是没有DoS攻击的时刻, 所以本文总是可以在$N(N+1)$个时间步内找到这N个切换点, 于是结合定义1可以得出结论: 系统(6)将会是指数稳定的. 证毕.

3.2 观测器与控制器设计

在本节中, 将根据定理1的结论给出对应的基于观测器的输出反馈控制器设计方案.

将式(6)中的$H_i(i\in M)$写成如下的形式:

$$H_i=A_{0i}+B_{0i}WT, \tag{27}$$

其中A_{0i}, B_{0i}, W, T分别为

$$A_{0i}=\begin{bmatrix}A^{i+1}&0\\0&A^{i+1}\end{bmatrix},$$

$$B_{0i}=\begin{bmatrix}\underbrace{A^iB\ \ A^{i-1}B\ \ \cdots\ \ A^0B\ 0\cdots0}_{\text{共}2(N+1)\text{项}}\\ \underbrace{0\ \ \cdots\ \ I\cdots0}_{\text{共}2(N+1)\text{项,第}N+2+i\text{项为单位阵}}\end{bmatrix},$$

$$W=\begin{bmatrix}K_0^{\mathrm{T}}&K_1^{\mathrm{T}}&\cdots&K_N^{\mathrm{T}}&0&0&\cdots&0\\0&0&\cdots&0&L_0^{\mathrm{T}}&L_1^{\mathrm{T}}&\cdots&L_N^{\mathrm{T}}\end{bmatrix}^{\mathrm{T}},$$

$$T=\begin{bmatrix}I&I\\0&-C\end{bmatrix}.$$

由Schur补引理, 矩阵不等式(7)等价于

$$\begin{bmatrix}-\lambda_iP_i&H_i^{\mathrm{T}}\\*&-P_i^{-1}\end{bmatrix}<0. \tag{28}$$

将式(27)代入到式(28)中, 可以得到

$$\begin{bmatrix} -\lambda_i P_i & A_{0i}^{\mathrm{T}} + T^{\mathrm{T}} W^{\mathrm{T}} B_{0i}^{\mathrm{T}} \\ * & -P_i^{-1} \end{bmatrix} < 0. \tag{29}$$

引入新的矩阵变量$Q_i (i \in M)$, 将式(29)重新写为

$$\begin{cases} \begin{bmatrix} -\lambda_i P_i & A_{0i}^{\mathrm{T}} + T^{\mathrm{T}} W^{\mathrm{T}} B_{0i}^{\mathrm{T}} \\ * & -Q_i \end{bmatrix} < 0, \\ Q_i = P_i^{-1},\ i \in M. \end{cases} \tag{30}$$

由于式(30)中含有矩阵的逆, 属于非线性项, 无法直接使用MATLAB的LMI工具箱进行求解, 因此需要对其进行进一步的转化. 应用文献[30]提出的锥补线性化算法, 不等式(8)–(9)和式(30)约束下的可行性问题可转化为如下的问题进行求解:

$$\min \mathrm{tr}(\sum_{i=0}^{N} P_i Q_i), \tag{31}$$

s.t. 式(8)–(9),

$$\begin{bmatrix} -\lambda_i P_i & A_{0i}^{\mathrm{T}} + T^{\mathrm{T}} W^{\mathrm{T}} B_{0i}^{\mathrm{T}} \\ * & -Q_i \end{bmatrix} < 0, \tag{32}$$

$$\begin{bmatrix} P_i & I \\ I & Q_i \end{bmatrix} \geqslant 0,\ i \in M, \tag{33}$$

其中, 式(31)中的极小化问题可用如下的迭代算法进行求解.

算法 1　基于观测器的输出反馈控制器求解算法.

步骤 1　选取一组使不等式(8)–(9)和式(32)–(33)成立的$0 < \lambda_N < \cdots < \lambda_1 < \lambda_0 < 1, \mu < \dfrac{1}{\lambda_0}$.

步骤 2　求得使不等式(8)–(9)和式(32)–(33)成立的一组可行解, 记为$(P_i^0, Q_i^0, K_i^0, L_i^0, i \in M)$, 并设置$l = 0, V_i^l = P_i^l,\ W_i^l = Q_i^l$.

步骤 3　求解以下的极小化问题:

$$\min\ \ \mathrm{tr}(\sum_{i=0}^{N} (V_i^l Q_i + W_i^l P_i),$$

s.t. 式(8)–(9)(32)–(33).

得到一组新的解$(P_i, Q_i, K_i, L_i, i \in M)$. 检验条件(7)是否满足, 若满足则退出计算, 否则设置$l = l+1$, $V_i^l = P_i,\ W_i^l = Q_i$, 并返回步骤3.

注 3　式(7)中的$\lambda_i (i \in M)$是和系统衰减率相关的一个参数. 当μ给定时, λ_i越小, λ_i所对应的子系统也就衰减得越快. 由于每个离散时间子系统的状态转移矩阵$H_i (i \in M)$所对应的状态转移过程的时间跨度是不同的, 算法1中选择的参数$0 < \lambda_N < \cdots < \lambda_1 < \lambda_0 < 1$(在$\mu$给定的情况下)表明子系统状态转移过程的时间跨度越大, 其衰减率也将会越大. 这里仅仅给出了设计参数的定性分配方案, 如何定量地确定设计参数的最优分配方案将是作者进一步的研究方向.

注 4　在系统建模过程中, 通过状态变量的增广, 用矩阵$H_{\sigma(k_\kappa)}$对观测器与被控对象的动态特性进行了统一的描述. 因此, 以上算法求出的观测器与控制器具有近似的收敛速度. 在实际的工程应用中, 为了获得更好的控制性能, 往往需要观测器的收敛速度大于控制器的收敛速度. 注意到矩阵$H_{\sigma(k_\kappa)}$中的$(F_{\sigma(k_\kappa)} - L_{\sigma(k_\kappa)} C)$是唯一一个和切换Luenberger观测器的衰减率相关的一项. 因此, 在实际应用中可根据需要在矩阵$(F_{\sigma(k_\kappa)} - L_{\sigma(k_\kappa)} C)$前乘以一个大于1的系数$\theta_i (i = \sigma(k_\kappa))$后再应用以上算法进行求解, 使求得的观测器相对于控制器有较大的收敛速度.

4　实验

考虑图3中的Googol公司的直线一级倒立摆系统.

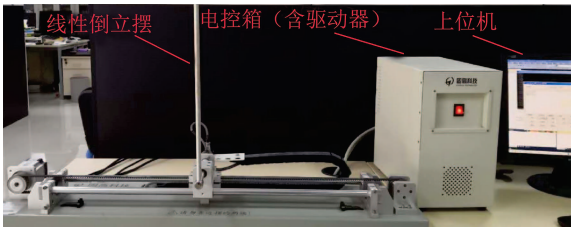

图 3　网络化控制的倒立摆系统

Fig. 3　The networked inverted pendulum system

该倒立摆系统主要包含倒立摆机构、电控箱、上位机3部分, 其中上位机上同时运行有通过UPD协议进行相互通信的客户端以及服务器端程序. 通过在客户端和服务器端之间人为地对量测信号和控制信号进行拦截可以模拟DoS攻击. 使用牛顿–欧拉方法以及小偏差线性化理论对图3所示的倒立摆系统进行建模可以得到如下的连续时间状态空间模型:

$$\begin{bmatrix} \dot{x} \\ \ddot{x} \\ \dot{\phi} \\ \ddot{\phi} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \dfrac{3\mathrm{g}}{4l} & 0 \end{bmatrix} \begin{bmatrix} x \\ \dot{x} \\ \phi \\ \dot{\phi} \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ \dfrac{3\mathrm{g}}{4l} \end{bmatrix} \ddot{x}, \tag{34}$$

$$y = \begin{bmatrix} x \\ \phi \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ \dot{x} \\ \phi \\ \dot{\phi} \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} \ddot{x}, \tag{35}$$

其中: x是倒立摆滑块的位置, $\dot{x}$是滑块的速度, 滑块的加速度$\ddot{x}$用作系统的输入, ϕ是摆杆与竖直方向的夹角, $\dot{\phi}$是摆杆的角速度, $l = 0.25$ m是摆杆转动轴心到其质心的长度, 9.8 m/s^{2}是重力加速度, y是系统的量测输出. 这里的倒立摆系统中只有滑块的位置和摆杆的角度是可直接测量的. 本文设置系统的采用周期为10 ms, 将系统的连续时间状态空间模型离散化后可以得到如下的对应于式(1)中的参数:

$$A = \begin{bmatrix} 1 & 0.01 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1.0015 & 0.0100 \\ 0 & 0 & 0.2941 & 1.0015 \end{bmatrix},\ B = \begin{bmatrix} 0.0001 \\ 0.0100 \\ 0.0002 \\ 0.0300 \end{bmatrix}, \tag{36}$$

$$C=\begin{bmatrix}1&0&0&0\\0&0&1&0\end{bmatrix},\ D=\begin{bmatrix}0\\0\end{bmatrix}. \tag{37}$$

本文假设DoS攻击者最多能连续阻塞至少一个通道的次数为5(即$N=5$), 这就意味着本文需要6个子系统来对DoS攻击下系统的所有可能的动态特性进行描述. 根据式(36)–(37)给出的离散时间系统参数, 取每个子系统的设计参数$\lambda_0, \lambda_1, \cdots, \lambda_5, \mu$的值分别为$0.985, 0.984, 0.983, 0.982, 0.981, 0.980, \dfrac{1}{0.99}$, 应用提出的设计算法, 使用MATLAB的LMI工具箱可以得到如下的控制器及观测器设计参数:

$$\begin{aligned}
K_0&=[10.2372\ \ 11.9624\ \ -64.5360\ \ -16.6246],\\
K_1&=[-0.7542\ \ -0.9617\ \ -7.9616\ \ 0.6835],\\
K_2&=[-0.9384\ \ -1.1256\ \ -6.8209\ \ 0.6045],\\
K_3&=[-0.9575\ \ -1.1597\ \ -6.4694\ \ 0.5141],\\
K_4&=[-0.8527\ \ -1.1075\ \ -6.6329\ \ 0.4661],\\
K_5&=[-0.7236\ \ -1.0622\ \ -6.8862\ \ 0.5278].
\end{aligned}$$

$L_0, L_1, L_2, L_3, L_4, L_5$的值分别为

$$L_0=\begin{bmatrix}0.9724&0.0442\\1.0351&0.4893\\-0.2221&1.2225\\-0.2398&1.9482\end{bmatrix},\ L_1=\begin{bmatrix}0.9852&0.0555\\1.0364&0.5214\\-0.2275&1.3070\\-0.2471&2.3388\end{bmatrix}, \tag{38}$$

$$L_2=\begin{bmatrix}0.9975&0.0686\\1.0372&0.5545\\-0.2322&1.3996\\-0.2535&2.7425\end{bmatrix},\ L_3=\begin{bmatrix}1.0093&0.0840\\1.0358&0.5956\\-0.2391&1.5101\\-0.2631&3.1734\end{bmatrix}, \tag{39}$$

$$L_4=\begin{bmatrix}1.0205&0.1024\\1.0320&0.6477\\-0.2502&1.6451\\-0.2784&3.6416\end{bmatrix},\ L_5=\begin{bmatrix}1.0308&0.1242\\1.0251&0.7130\\-0.2673&1.8098\\-0.3017&4.1546\end{bmatrix}. \tag{40}$$

为了评估本文提出的控制方法, 本文选择一组理想的状态反馈控制作为对照. 由于倒立摆上没有直接测量速度以及角速度的传感器, 这里状态反馈控制中所需的倒立摆速度以及角速度是由下式

$$\dot{x}(k)=\frac{x(k)-x(k-1)}{t_{\rm s}},\ \dot{\theta}(k)=\frac{\theta(k)-\theta(k-1)}{t_{\rm s}}$$

计算的. 其中$t_{\rm s}$为倒立摆的采样间隔. 设置连续时间系统(34)的期望极点为[–2 -3 $-4+3{\rm i}$ $-4-3{\rm i}$], 解得状态反馈增益为

$$K=[5.0505\ \ 5.8249\ \ -35.2502\ \ -6.2750].$$

通过实验(这里的控制器是采用零阶保持策略的离散控制器), 可以得到如图4–5所示的关于倒立摆的位置以及角度的实验数据.

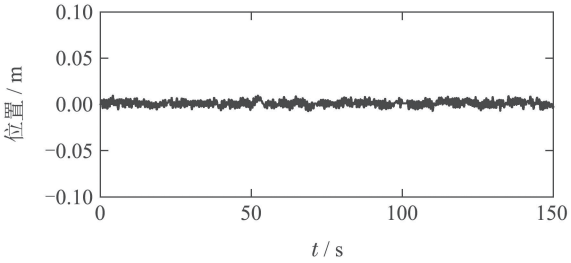

图 4 状态反馈控制下倒立摆滑块的位置

Fig. 4 The position of the slider under state feedback control

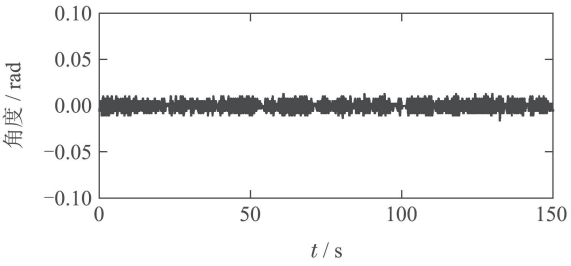

图 5 状态反馈控制下倒立摆摆杆的角度

Fig. 5 The angle of the pendulum rod under state feedback control

现考虑图6所示的DoS攻击(1表示有DoS攻击, 0表示无DoS攻击), 当周期地持续地施加图6所示的DoS攻击时, 状态反馈控制器无法对倒立摆进行有效的控制. 这表明所设计的状态反馈控制律虽然能够保证倒立摆在良好工况下的稳定运行, 但其对网络中发生的DoS攻击还是十分脆弱的.

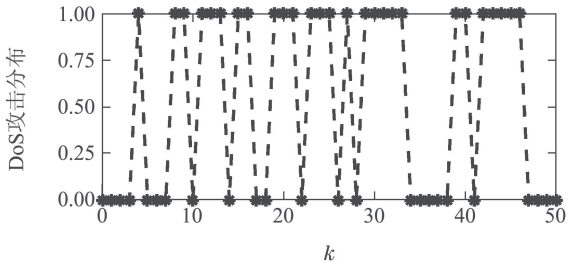

图 6 DoS攻击分布

Fig. 6 The distribution of DoS attack

下面应用本文提出的控制方法进行实验, 可以得到在有无DoS攻击下的实验结果图7–10(施加的持续性周期DoS攻击同样服从图6所示的DoS攻击分布).

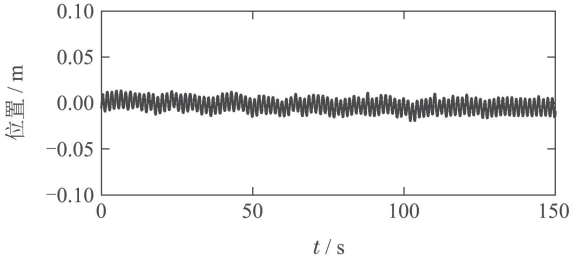

图 7 无DoS攻击时倒立摆滑块的位置

Fig. 7 The position of the slider in the absence of DoS attack

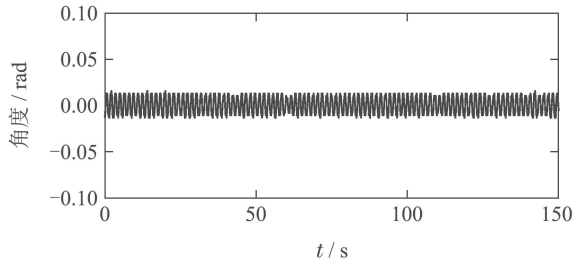

图 8 无DoS攻击时倒立摆摆杆的角度

Fig. 8 The angle of the pendulum rod in the absence of DoS attack

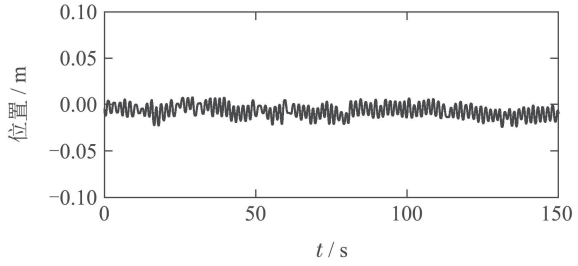

图 9 发生DoS攻击时倒立摆滑块的位置

Fig. 9 The position of the slider under DoS attack

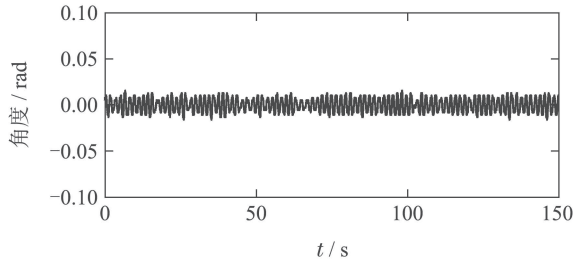

图 10 发生DoS攻击时倒立摆摆杆的角度

Fig. 10 The angle of the pendulum rod under DoS attack

以上的实验结果表明: 所提出的控制方法在有无DoS攻击的情况下都能对倒立摆进行有效的控制. 相比于状态反馈控制方法, 这里的基于Luenberger观测器的冗余控制方法对DoS攻击具有较强的鲁棒性但控制效果要稍微差一些. 观测器的引入会额外增加更多的不确定性, 相比于直接的状态反馈控制, 基于状态观测值的控制会不可避免地损失一定的控制性能. 当DoS攻击发生时, 系统的实际采样间隔会相应地增加, 这会降低相邻两个切换点之间的外部干扰、非线性因素对基于前一个切换点状态估计值计算的控制输入的有效性, 从而增加了DoS攻击下的倒立摆对外部干扰等影响的敏感性. 这一事实在图9上表现为倒立摆的位置出现了较大的波动. 进一步地, 通过在倒立摆摆杆的顶端施加一个水平方向的外部扰动, 可以发现DoS攻击下的倒立摆更容易失去原有的稳定性. 这是因为DoS攻击增加了倒立摆的实际采样间隔, 而采样间隔的增加使得系统对外部的干扰不能进行及时的反馈校正. 因此, 如何使网络化控制系统在有无DoS攻击的情况下拥有一致的控制性能将是作者下一步的研究方向.

5 结论

本文针对DoS攻击下网络化控制系统的安全控制问题, 提出了一种具有多个增益的切换Luenberger观测器, 实现了DoS攻击下系统状态值的间歇性观测. 根据获得的状态估计值设计了包含当前以及未来一段时域控制输入的冗余控制律, 保证了被控系统在有无DoS攻击的情况下都有合适控制输入更新, 克服了零输入策略和保持输入策略的盲目性. 进一步, 通过构造一个切换系统模型导出了控制系统在DoS攻击下指数稳定的充分条件以及获得所需的控制器增益和观测器增益的设计算法, 并基于构造的切换系统模型的结构特征定性地给出了设计参数的分配原则. 最后, 网络化倒立摆控制系统的实验验证了所提出的方法的有效性.

参考文献:

[1] SONG Hongbo, LIU Guoping. Networked predictive control for systems with multiple communication channels. *Control Theory & Applications*, 2015, 32(7): 912 – 917.
(宋洪波, 刘国平. 具有多传输通道系统的网络化预测控制. 控制理论与应用, 2015, 32(7): 912 – 917.)

[2] COLOMBO A W, KARNOUSKOS S, KAYNAK O, et al. Industrial cyber-physical systems: A backbone of the fourth industrial revolution. *IEEE Industrial Electronics Magazine*, 2017, 11(1): 6 – 16.

[3] ZHANG Heng. *Research on security theory for cyber-physical systems*. Hangzhou: Zhejiang University, 2015.
(张恒. 信息物理系统安全理论研究. 杭州: 浙江大学, 2015.)

[4] YUAN Yuan. *Analysis and design of networked control systems under DoS attacks*. Beijing: Tsinghua University, 2014.
(袁源. DoS攻击下网络化控制系统的分析与设计. 北京: 清华大学, 2014.)

[5] FARWELL J P, ROHOZINSKI R. Stuxnet and the future of cyber war. *Survival*, 2011, 53(1): 23 – 40.

[6] EMILIO I. Cyber attack: A dull tool to shape foreign plicy. *The 5th International Conference on Cyber Conflict*. Tallinn: IEEE, 2013: 1 – 18.

[7] TANG Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attacks against cyber physical power system. *Automation of Electric Power Systems*, 2016, 40(17): 59 – 69.
(汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述. 电力系统自动化, 2016, 40(17): 59 – 69.)

[8] LIU Ting, TIAN Jue, WANG Jiazhou, et al. Integrated security threats and defense of cyber-physical systems. *Acta Automatica Sinica*, 2019, 45(1): 7 – 26.
(刘烃, 田决, 王嫁舟, 等. 信息物理融合系统综合安全威胁与防御研究. 自动化学报, 2019, 45(1): 7 – 26.)

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

[10] YUAN Y, SUN F, LIU H. Resilient control of cyber-physical systems against intelligent attacker: A hierarchal stackelberg game approach. *International Journal of Systems Science*, 2016, 47(9): 2067 – 2077.

[11] ZHU M, SONIA M. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control*, 2013, 59(3): 804 – 808.

[12] DENG R, XIAO G, LU R, et al. False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, 2017, 13(2): 411 – 423.

[13] YUAN Y, YUAN H H, GUO L, et al. Resilient control of networked control system under DoS attacks: A unified game approach. *IEEE Transactions on Industrial Informatics*, 2016, 12(5): 1786 – 1794.

[14] CHEN B, HO W C D, ZHANG W A, et al. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. *IEEE Transactions on System, Man, and Cybernetics: Systems*, 2019, 49(2): 455 – 468.

[15] ZHANG H, CHENG P, SHI L, et al. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Transactions on Automatic Control*, 2015, 60(11): 3023 – 3028.

[16] PENG L, CAO X, SHI H, et al. Optimal jamming attack schedule for remote state estimation with two sensors. *Journal of the Franklin Institute*, 2018, 355(14): 6859 – 6876.

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

[18] PERSIS C D, TESI P. Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 2015, 60(11): 2930 – 2944.

[19] CETINKAYA A, ISHII H, HAYAKAWA T. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 2017, 62(5): 2434 – 2449.

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

[21] GUPTA A, LANGBORT C, BAŞAR T. Optimal control in the presence of an intelligent jammer with limited actions. *Proceedings of the 49th IEEE Conference on Decision and Control*. Atlanta: IEEE, 2010: 1096 – 1101.

[22] YUAN Y, SUN F, ZHU Q. Resilient control in the presence of DoS attack: Switched system approach. *International Journal of Control, Automation and Systems*, 2015, 13(6): 1423 – 1435.

[23] YUAN H H, XIA Y Q. Resilient strategy design for cyber-physical system underDoSattack over a multi-channel framework. *Information Sciences*, 2018, 454/455: 312 – 327.

[24] LAI S Y, CHEN B, LI T X, et al. Packet-based state feedback control under DoS attacks in cyber-physical systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2018, DOI 10.1109/TCSI-I.2018.2881984.

[25] FALL K R, STEVENS W R. *TCP/IP Illustrated, Volume 1: The Protocols*. Boston, United States: Addison-Wesley, 2011.

[26] ZHAO Y B, LIU G P, REES D. Design of a packet-based control framework for networked control systems. *IEEE Transactions on Control Systems Technology*, 2009, 17(4): 859 – 865.

[27] MA Jing, SUN Shuli. Linear optimal full-order estimators for discrete-time stochastic uncertain systems with packet losses. *Control Theory & Applications*, 2014, 31(6): 764 – 772.
(马静, 孙书利. 具有数据包丢失的离散随机不确定系统的线性最优满阶估值器. 控制理论与应用, 2014, 31(6): 764 – 772.)

[28] LEON S J. *Linear Algebra with Applications*. New York: Pearson, 2009.

[29] YU LI. *Robust Control: LMIs*. Beijing: Tsinghua University Press, 2002.
(俞立. 鲁棒控制: 线性矩阵不等式处理方法. 北京: 清华大学出版社, 2002.)

[30] EI GHAOUI L, OUSTRY F, AITRAMI M. A cone complementarity linearization algorithm for static output-feedback and related problems. *IEEE Transactions on Automatic Control*, 1997, 42(8): 1171 – 1176.

作者简介:

赖绍禹 硕士研究生, 目前研究方向为信息物理系统的安全控制, E-mail: zjutzjuy@gmail.com;

陈 博 教授, 目前研究方向为信息融合、安全估计与控制和信息物理系统, E-mail: bchen@aliyun.com;

俞 立 教授, 目前研究方向为网络化控制、信息融合和信息物理系统, E-mail: lyu@zjut.edu.cn.