DOI:10.13878/j.cnki.jnuist.2020.03.003

赵宁[1]　张会焱[2]　石碰[3]

# 拒绝服务攻击下网络化控制系统的基于观测器输出反馈控制

**摘要**

本文考虑了拒绝服务攻击下的网络化控制系统的$H_\infty$输出反馈控制问题.拒绝服务攻击的特征表现为能量有限和周期类型,它攻击无线网络通道进而退化系统性能.在系统状态部分未知的前提下,为了保证被控系统的稳定性和$H_\infty$性能指标,通过设计基于观测器输出反馈控制器,使得网络化控制系统在丢包和拒绝服务攻击下仍然保持稳定和预定性能.最后数值例子验证了所设计的控制器是有效的.

**关键词**

网络化控制系统;拒绝服务攻击;丢包;稳定性;$H_\infty$性能指标

**中图分类号** TP273

**文献标志码** A

## 0　引言

近几十年来,通信、控制和计算机技术的飞速发展对控制系统的结构产生了至关重要的影响.在传统的控制系统中,传感器、控制器和执行器之间的相互连接通常是由端口与端口之间布线来实现的.然而这将产生布线困难、维护困难和灵活性低等问题.由于被控对象复杂性的不断增加,许多自动化系统都出现了故障.在这种情况下,网络化控制系统越来越受到人们的关注.通过多用途共享网络将空间分布的元素连接起来,这样会产生灵活的体系结构并且通常可以降低安装和维护成本.如今,网路化控制系统已经广泛应用到实际系统中,例如汽车自动化[1]、智能建筑[2]、交通网络[3]、互联网上的触觉协作[4]和无人飞行器[5]等.

然而,网络化控制系统在给人们带来方便的同时,也存在着一些安全隐患.网络攻击所引发的安全事故并不少见,例如,“StuxNet”是一种针对工业控制系统操作的破坏性病毒.在2010年,该病毒非法侵入伊朗核设施并实施破坏,导致该国的布什尔核电站推迟启动[6].2011年大庆石化、西南管线广东调控中心、齐鲁石化和多个场站感染病毒,导致控制器通信中断.上述案例表明,网络易受到攻击,它所带来的影响不仅仅对个人产生严重的后果,甚至对社会和国家的安全带来威胁. 因此研究网络化控制系统的安全控制受到了国内外学者的广泛关注.

在网络化控制系统中,网络攻击的主要攻击类型有:拒绝服务攻击[7]、欺骗攻击[8]和重放攻击. 拒绝服务攻击主要是大量的通信量阻断信号的传输,使得网络资源被消耗殆尽,进而导致服务对象无法得到满足.欺骗攻击主要是实现对真实数据的篡改使其网络传输虚假数据,进而影响系统的性能.重放攻击主要是攻击者通过记录以前一段时间的传输数据,然后在某一时刻将这些记录的数据替换真实的数据.正如文献[7]中所言,在网络传输过程中,更有可能发生拒绝服务攻击,并且大量的研究成果已经被发表,见参考文献[7,8-14].文献[14]考虑了在周期类型的拒绝服务攻击和随机丢包下,基于观测器的输出反馈控制使得物理信息系统达到随机稳定和性能指标.然而在稳定性证明中,引入了大量的辅助矩阵进而造成计算量增加.为了改

**收稿日期** 2020-02-08

**资助项目** 国家自然科学基金(61773131);重庆市教委重大项目(KJZD-M201900801);重庆市教委青年项目(KJQN201900831)

**作者简介**

赵宁,男,博士生,研究方向为网络化控制系统.zhaoning@ hrbeu.edu.cn.com

石碰(通信作者),男,教授,博士生导师,研究方向智能控制、多机器人智能集群等.peng.shi@ adelaide.edu.au

1　哈尔滨工程大学　自动化学院,哈尔滨,150001

2　重庆工商大学　国家智能制造服务国际科技合作基地,重庆,400067

3　阿德莱德大学　电气与电子工程学院,阿德莱德SA,5005

善这一情况,因此触发了本文的研究.

本文的主要贡献如下:

1) 借助文献[13]中的方法,把网络化控制系统受到随机丢包的影响,将系统转换为马尔可夫跳变系统,进而研究系统的稳定性并进行性能分析.

2) 比较文献[13],我们考虑的问题更加复杂,系统本身受到外部干扰的影响.比较文献[14],我们方法的优势在于极大地减少了计算量.

3) 比较文献[15],在设计控制器中,系统参数矩阵 $\boldsymbol{B}$ 需要列满秩的条件被移除.

## 1 问题描述和预备知识

考虑如下离散系统:

$$\begin{aligned}&\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{u}(k)+\boldsymbol{B}_w\boldsymbol{w}(k),\\&\boldsymbol{y}(k)=\boldsymbol{C}\boldsymbol{x}(k),\\&\boldsymbol{z}(k)=\boldsymbol{D}\boldsymbol{x}(k),\end{aligned}\tag{1}$$

式中:$\boldsymbol{x}(k)\in\mathbf{R}^n$ 是系统的状态,$\boldsymbol{u}(k)\in\mathbf{R}^m$ 是系统的控制输入,$\boldsymbol{w}(k)\in\mathbf{R}^q$ 是干扰输入同时属于空间 $l_2[0,\infty)$,$\boldsymbol{y}(k)\in\mathbf{R}^p$ 是系统的可测量输出和 $\boldsymbol{z}(k)\in\mathbf{R}^z$ 是系统的实际输出.矩阵 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{B}_w,\boldsymbol{C},\boldsymbol{D}$ 是已知矩阵并且具有恰当维数.

如图 1 所示,在网络化控制系统中的网络层受到拒绝服务的蓄意攻击.本文中我们考虑能量有限的拒绝服务攻击,具体表现为如下周期循环类型的攻击策略:

$$k\in[(s-1)T+1,sT],$$

式中:$T$ 表示循环的持续时间,$s$ 表示周期数量.那么在该周期中显然包含着攻击的活跃时间和睡眠时间.为了刻画这一过程,我们引入如下表达式:

$$\sigma(k)=\begin{cases}1, & k\in[(s-1)T+1,(s-1)T+T_{\text{off}}],\\2, & k\in[(s-1)T+T_{\text{off}}+1,sT],\end{cases}$$

式中:$T_{\text{off}}(<T)$ 表示在一个周期内攻击的睡眠持续时间.$\sigma(k)=1$ 表示为网络传输信号正常,$\sigma(k)=2$ 表示为网络传输信号受到拒绝服务攻击.令 $\lambda(k,\sigma(k))\in\{0,1\}$,表示在 $k$ 时刻控制器是否成功接收到数据信号:

$$\lambda(k,\sigma(k))=\begin{cases}1, & \text{成功},\\0, & \text{失败}.\end{cases}$$

那么对于 $k$ 时刻控制器是否成功收到数据包的概率描述如下:

$$\begin{aligned}&\Pr[\lambda(k,\sigma(k))=1]=\alpha_{\sigma(k)},\\&\Pr[\lambda(k,\sigma(k))=0]=1-\alpha_{\sigma(k)},\end{aligned}\tag{2}$$

式中:$\alpha_{\sigma(k)}\in[0,1)$ 是已知的常数.由式(2)可得:

$$\begin{aligned}&\mathrm{E}[\lambda(k,\sigma(k))-\alpha_{\sigma(k)}]=0,\\&\mathrm{E}[(\lambda(k,\sigma(k))-\alpha_{\sigma(k)})^2]=\alpha_{\sigma(k)}(1-\alpha_{\sigma(k)}).\end{aligned}$$

在拒绝服务的攻击下,丢失的数据将被最近一次接收的数据所代替,它的表示式如下:

$$\begin{aligned}\bar{\boldsymbol{y}}(k)=&\lambda(k,\sigma(k))\boldsymbol{y}(k)+\\&(1-\lambda(k,\sigma(k)))\bar{\boldsymbol{y}}(k-1).\end{aligned}$$

基于上述分析,我们构造如下形式的观测器:

$$\begin{aligned}&\hat{\boldsymbol{x}}(k+1)=\boldsymbol{A}\hat{\boldsymbol{x}}(k)+\boldsymbol{B}\boldsymbol{u}(k)+\boldsymbol{L}(\bar{\boldsymbol{y}}(k)-\boldsymbol{C}\hat{\boldsymbol{x}}(k)),\\&\boldsymbol{u}(k)=\boldsymbol{K}\hat{\boldsymbol{x}}(k),\end{aligned}$$

式中:$\hat{\boldsymbol{x}}(k)\in\mathbf{R}^n$ 是观测器状态,矩阵 $\boldsymbol{K},\boldsymbol{L}$ 是待设计的增益矩阵.定义估计误差为 $\boldsymbol{e}(k)=\boldsymbol{x}(k)-\hat{\boldsymbol{x}}(k)$,进而得到如下的误差系统方程:

$$\begin{aligned}\boldsymbol{e}(k+1)=&(\boldsymbol{A}-\boldsymbol{L}\boldsymbol{C})\boldsymbol{e}(k)-\\&(1-\lambda(k,\sigma(k)))\boldsymbol{L}(\bar{\boldsymbol{y}}(k-1)-\boldsymbol{C}\boldsymbol{x}(k))+\boldsymbol{B}_w\boldsymbol{w}(k).\end{aligned}$$

令 $\boldsymbol{\eta}(k)=[\boldsymbol{x}^{\mathrm{T}}(k)\quad\boldsymbol{e}^{\mathrm{T}}(k)\quad\bar{\boldsymbol{y}}^{\mathrm{T}}(k-1)]^{\mathrm{T}}$,我们可以得到如下增广系统:

$$\boldsymbol{\eta}(k+1)=\boldsymbol{\Phi}_{r(k)}\boldsymbol{\eta}(k)+\bar{\boldsymbol{B}}_w\boldsymbol{w}(k),\tag{3}$$

式中:$r(k)$ 是马尔可夫链,

$$\boldsymbol{\Phi}_{r(k)}=\begin{bmatrix}\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K} & -\boldsymbol{B}\boldsymbol{K} & \boldsymbol{0}\\(1-\lambda(k,\sigma(k)))\boldsymbol{L}\boldsymbol{C} & \boldsymbol{A}-\boldsymbol{L}\boldsymbol{C} & -(1-\lambda(k,\sigma(k)))\boldsymbol{L}\\\lambda(k,\sigma(k))\boldsymbol{C} & \boldsymbol{0} & (1-\lambda(k,\sigma(k)))\boldsymbol{I}\end{bmatrix},$$

$$\bar{\boldsymbol{B}}_w=\begin{bmatrix}\boldsymbol{B}_w\\\boldsymbol{B}_w\\\boldsymbol{0}\end{bmatrix}.$$

因此闭环系统(3)带有两个模态的马尔可夫线性系统:

1) 没有丢包现象:

$$r(k)=1,\boldsymbol{\Phi}_{r(k)}=\begin{bmatrix}\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K} & -\boldsymbol{B}\boldsymbol{K} & \boldsymbol{0}\\\boldsymbol{0} & \boldsymbol{A}-\boldsymbol{L}\boldsymbol{C} & \boldsymbol{0}\\\boldsymbol{C} & \boldsymbol{0} & \boldsymbol{0}\end{bmatrix}.$$

2) 发生丢包现象:

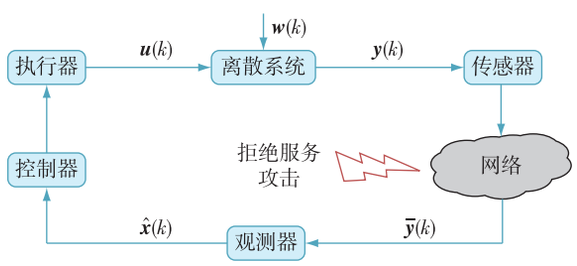


图 1 拒绝服务攻击下的网络化控制系统框架

Fig. 1 Structure of networked control system under denial-of-service attacks

$$r(k)=0,\boldsymbol{\Phi}_{r(k)}=\begin{bmatrix}\boldsymbol{A}+\boldsymbol{BK} & -\boldsymbol{BK} & \boldsymbol{0}\\ \boldsymbol{LC} & \boldsymbol{A}-\boldsymbol{LC} & \boldsymbol{L}\\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}\end{bmatrix}.$$

接下来引入系统(3)是随机稳定的且满足 $H_\infty$ 性能指标的定义.

**定义 1**

1) 若对于任意的初始条件 $\boldsymbol{\eta}_0$ 和初始模态 $\boldsymbol{r}_0$,系统(3)的解满足下述条件:

$$\sum_{k=0}^{\infty}\mathrm{E}\{\|\boldsymbol{x}(k)\|^2\mid\boldsymbol{x}_0,\boldsymbol{r}_0\}<\infty,$$

则称系统(3)是随机稳定的.

2) 在零初始条件下,存在一个正数 $\gamma$,对于任意的非零干扰 $\boldsymbol{w}(k)\in l_2[0,\infty)$,有如下不等式成立:

$$\mathrm{E}\Big\{\sum_{k=0}^{\infty}\|z(k)\|^2\Big\}<\gamma^2E\Big\{\sum_{k=0}^{\infty}\|\boldsymbol{w}(k)\|^2\Big\}.$$

本文的目的在于通过设计基于观测器的输出反馈控制器使得系统(1)在拒绝服务攻击和随机丢包下是随机稳定的且满足预先设定的 $H_\infty$ 性能指标.

## 2 稳定性和 $H_\infty$ 性能分析

本节将给出系统(3)随机稳定和 $H_\infty$ 性能指标的充分条件.为了后续分析,我们令 $\boldsymbol{\pi}=\{\pi_{ij}\}$ 为马尔可夫链 $r(k)$ 的概率转移矩阵,其中

$$\pi_{ij}=\Pr\{\boldsymbol{\eta}(k+1)=j\mid\boldsymbol{\eta}(k)=i\},$$

$$\pi_{ij}\geqslant 0(i,j=1,2),\sum_{j=1}^{2}\pi_{ij}=1.$$

**定理 1** 对于给定的常数 $\alpha_1,\alpha_2,\gamma$,和增益矩阵 $\boldsymbol{K}$ 和 $\boldsymbol{L}$,若存在正定矩阵 $\boldsymbol{P}_i(i=1,2)$,使得下面不等式成立:

$$\boldsymbol{\Psi}_i=\begin{bmatrix}\sum_{j=1}^{2}\boldsymbol{\Phi}_i^{\mathrm{T}}\pi_{ij}\boldsymbol{P}_j\boldsymbol{\Phi}_i-\boldsymbol{P}_i+\boldsymbol{QD}^{\mathrm{T}}\boldsymbol{DQ}^{\mathrm{T}} & \sum_{j=1}^{2}\boldsymbol{\Phi}_i^{\mathrm{T}}\pi_{ij}\boldsymbol{P}_j\boldsymbol{B}_w\\ * & \sum_{j=1}^{2}\boldsymbol{B}_w^{\mathrm{T}}\pi_{ij}\boldsymbol{P}_j\boldsymbol{B}_w-\gamma^2\boldsymbol{I}\end{bmatrix}<0, \tag{4}$$

其中 $\pi_{i1}=\alpha_{\sigma(k)},\pi_{i2}=1-\alpha_{\sigma(k)},\boldsymbol{Q}=[\boldsymbol{I}\quad\boldsymbol{0}\quad\boldsymbol{0}]^{\mathrm{T}}$,则闭环系统(3)是随机稳定的且满足 $H_\infty$ 性能指标.

**证明** 构造如下形式的 Lyapunov 函数

$$V(k)=\boldsymbol{\eta}^{\mathrm{T}}(k)\boldsymbol{P}_{r(k)}\boldsymbol{\eta}(k).$$

它沿着系统(3)的解对时间的差分为

$$\mathrm{E}\{\Delta V(k)\}+\mathrm{E}\{z^{\mathrm{T}}(k)z(k)-\gamma^2\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{w}(k)\}=$$
$$\mathrm{E}\{\boldsymbol{\eta}^{\mathrm{T}}(k+1)\boldsymbol{P}_{r(k+1)}\boldsymbol{\eta}(k+1)\mid V(k)\}-$$
$$\boldsymbol{\eta}^{\mathrm{T}}(k)\boldsymbol{P}_{r(k)}\boldsymbol{\eta}(k)+\mathrm{E}\{\boldsymbol{\eta}^{\mathrm{T}}(k)\boldsymbol{QD}^{\mathrm{T}}\boldsymbol{DQ}^{\mathrm{T}}\boldsymbol{\eta}(k)-$$
$$\gamma^2\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{w}(k)\}=\begin{bmatrix}\boldsymbol{\eta}^{\mathrm{T}}(k)\\ \boldsymbol{w}^{\mathrm{T}}(k)\end{bmatrix}^{\mathrm{T}}\boldsymbol{\Psi}_i\begin{bmatrix}\boldsymbol{\eta}^{\mathrm{T}}(k)\\ \boldsymbol{w}^{\mathrm{T}}(k)\end{bmatrix}. \tag{5}$$

当 $\boldsymbol{w}^{\mathrm{T}}(k)=\boldsymbol{0}$,结合(4)和(5)可得:

$$\mathrm{E}\{\Delta V(k)\}+\mathrm{E}\{z^{\mathrm{T}}(k)z(k)-\gamma^2\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{w}(k)\}\leqslant$$
$$-\beta\boldsymbol{\eta}^{\mathrm{T}}(k)\boldsymbol{\eta}(k),$$

其中,$\beta=\lambda_{\min}(-\boldsymbol{\Psi}_i)$.对于任意整数 $t>1$,有

$$\mathrm{E}\{V(\boldsymbol{\eta}(t+1))\}-\mathrm{E}\{V(\boldsymbol{\eta}(0))\}\leqslant$$
$$-\beta\mathrm{E}\Big\{\sum_{k=0}^{t}\|\boldsymbol{\eta}(k)\|^2\Big\},$$

于是就有

$$\mathrm{E}\Big\{\sum_{k=0}^{t}\|\boldsymbol{\eta}(k)\|^2\Big\}\leqslant\frac{1}{\beta}\boldsymbol{\eta}^{\mathrm{T}}(0)\boldsymbol{P}_{r(0)}\boldsymbol{\eta}(0).$$

上述等式关于 $t$ 两边取极限可得:

$$\mathrm{E}\Big\{\sum_{k=0}^{\infty}\|\boldsymbol{\eta}(k)\|^2\Big\}<\infty.$$

因此,根据定义 1 可知在拒绝服务攻击和随机丢包下,闭环系统(3)是随机稳定的.

当 $\boldsymbol{w}^{\mathrm{T}}(k)\neq\boldsymbol{0}$,结合式(4)和(5)可得:

$$\mathrm{E}\{\Delta V(k)\}+\mathrm{E}\{z^{\mathrm{T}}(k)z(k)-\gamma^2\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{w}(k)\}\leqslant 0.$$

上述等式关于 $k$ 两边取极限可得:

$$\mathrm{E}\Big\{\sum_{k=0}^{\infty}\|z(k)\|^2\Big\}<\gamma^2\mathrm{E}\Big\{\sum_{k=0}^{\infty}\|\boldsymbol{w}(k)\|^2\Big\}.$$

那么闭环系统(3)满足预先设定 $H_\infty$ 性能指标 $\gamma$.

定理 1 在增益矩阵已知的前提下,给出了闭环系统(3)随机稳定和满足性能指标的充分条件.下面在增益矩阵未知的情况下给出系统综合分析的充分条件.

**定理 2** 对于给定的常数 $\alpha_1,\alpha_2,\gamma,\phi$,若存在正定矩阵 $\boldsymbol{P}_i$,使得下面不等式成立:

$$\begin{bmatrix}\boldsymbol{\Gamma}_{11} & \boldsymbol{\Gamma}_{12} & \boldsymbol{\Gamma}_{13}\\ * & \boldsymbol{\Gamma}_{22} & \boldsymbol{\Gamma}_{23}\\ * & * & \boldsymbol{\Gamma}_{33}\end{bmatrix}<0, \tag{6}$$

式中 $\boldsymbol{\Gamma}_{11}=-\boldsymbol{P}_i+\boldsymbol{QD}^{\mathrm{T}}\boldsymbol{DQ}^{\mathrm{T}},\boldsymbol{\Gamma}_{12}=\boldsymbol{0},\boldsymbol{\Gamma}_{13}=\boldsymbol{\Phi}_i^{\mathrm{T}}$,

$\boldsymbol{\Gamma}_{22}=-\gamma^2\boldsymbol{I},\boldsymbol{\Gamma}_{23}=\bar{\boldsymbol{B}}_w^{\mathrm{T}}$,

$\boldsymbol{\Gamma}_{33}=-2\phi\boldsymbol{I}+\phi^2(\alpha_{\sigma(k)}\boldsymbol{P}_1+(1-\alpha_{\sigma(k)})\boldsymbol{P}_2)$,

则闭环系统(3)是随机稳定的且满足 $H_\infty$ 性能指标.

**证明** 由于

$$-(\alpha_{\sigma(k)}\boldsymbol{P}_1+(1-\alpha_{\sigma(k)})\boldsymbol{P}_2)^{-1}\leqslant$$
$$-2\phi\boldsymbol{I}+\phi^2(\alpha_{\sigma(k)}\boldsymbol{P}_1+(1-\alpha_{\sigma(k)})\boldsymbol{P}_2),$$

因此 $\boldsymbol{\Gamma}_{33}<0$,显然有 $-(\alpha_{\sigma(k)}\boldsymbol{P}_1+(1-\alpha_{\sigma(k)})\boldsymbol{P}_2)^{-1}<0$.再根据 Schur 引理,式(6)能够保证式(4)成立,因此,闭环系统(3)是随机稳定的且满足 $H_\infty$ 性能指标.

## 3 仿真结果与性能比较

本节中,在拒绝服务攻击和随机丢包发生的情况下,一个网络化控制系统的例子来验证所提出控制方法的有效性.

**例 1** 我们选取如下系统(1)相应的系数矩阵:

$$\boldsymbol{A}=\begin{bmatrix}0 & 1\\ 0 & -0.8\end{bmatrix},\quad \boldsymbol{B}=\begin{bmatrix}0\\ 1.25\end{bmatrix},$$

$$\boldsymbol{B}_w=\begin{bmatrix}0.1\\ 0.1\end{bmatrix},\quad \boldsymbol{C}=[1\quad 0],\quad \boldsymbol{D}=0.5.$$

其他参数选取为:$\alpha_1=0.9,\alpha_2=0.65,\gamma=2,\phi=0.1$.

通过求解定理 2 中的条件(6),可以得到控制器和观测器的增益矩阵如下:

$$\boldsymbol{K}=[-0.317\ 0\quad 0.090\ 5],$$

$$\boldsymbol{L}=[-0.584\ 3\quad 0.460\ 9].$$

接下来选取外部干扰信号的表达式如下:

$$w(k)=\begin{cases}\mathrm{e}^{-0.03k}\sin\left(\dfrac{\pi k}{2}\right), & 1\leqslant k\leqslant 20,\\ 0, & \text{其他}.\end{cases}$$

对于拒绝服务攻击,我们假设循环周期 $T=20$,攻击的睡眠周期为 $T_{\mathrm{off}}=10$,总共执行时间为 60 s.基于上面的数据,我们可以仿真得到在总时间 60 s 中,图 2 记录了丢包时刻,其中蓝线表示系统在无攻击区间内发生的丢包时刻,相对应的红色为有攻击区间内发生的丢包时刻.图 3 为闭环系统(1)的状态曲线.图 4 为误差方程的状态曲线.通过图 3 和图 4 可以知道闭环系统(1)和误差系统是稳定的.

此外考虑系统的 $H_\infty$ 性能指标.经过计算得到:

$$\sqrt{\mathrm{E}\Big\{\sum_{k=0}^{\infty}\|z(k)\|^2\Big\}/\mathrm{E}\Big\{\sum_{k=0}^{0}\|w(k)\|^2\Big\}}=1.648\ 0<\gamma=2.$$

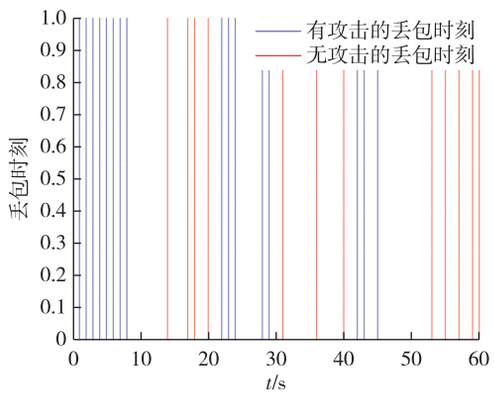


图 2 丢包时刻

Fig. 2 Moments of packet loss

这就说明了本文提出的控制器的设计方案是有效的.

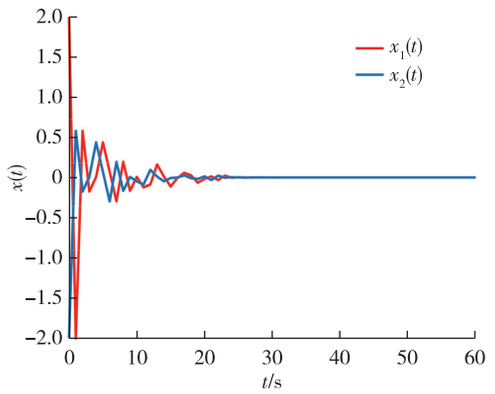


图 3 闭环系统(3)的状态响应曲线

Fig. 3 State response curve of the closed-loop system (3)

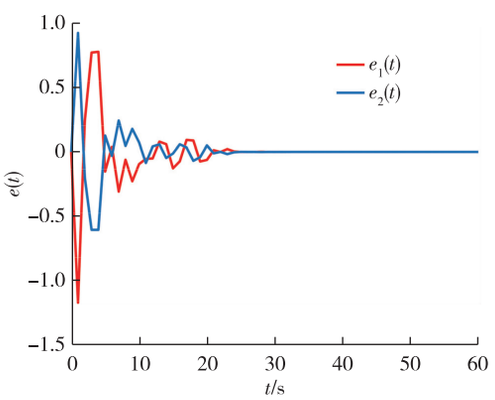


图 4 误差系统的状态响应曲线

Fig. 4 State response curve of the error system

## 4 结束语

本文针对网络化控制系统中网络层遭到拒绝服务攻击和诱导随机丢包现象,提出了基于观测器的控制器设计方案.该方案结合了马尔可夫链得到了随机意义下的系统的稳定性和满足 $H_\infty$ 性能指标.仿真结果表明,本文所提出的控制方案可以应用到具体的数值例子中,且易于计算.

## 参考文献

References

[1] Johansson K H, Törngren M, Nielsen L. Vehicle applications of controller area network[M]// Handbook of Networked and Embedded Control Systems. Boston, MA: Birkhäuser Boston, 2005: 741-765

[2] Wong J K W, Li H, Wang S W. Intelligent building research: a review[J]. Automation in Construction, 2005, 14(1): 143-159

[3] Papadimitratos P,La Fortelle A,Evenssen K,et al.Vehicular communication systems:enabling technologies,applications,and future outlook on intelligent transportation [J].IEEE Communications Magazine,2009,47(11):84-95
[4] Anderson R J,Spong M W.Bilateral control of teleoperators with time delay[J].IEEE Transactions on Automatic Control,1989,34(5):494-501
[5] Eun Y,Bang H.Cooperative control of multiple unmanned aerial vehicles using the potential field theory[J].Journal of Aircraft,2006,43(6):1805-1814
[6] Farwell J P,Rohozinski R.Stuxnet and the future of cyber war[J].Survival,2011,53(1):23-40
[7] Shisheh Foroush H,Martínez S.On triggering control of single-input linear systems under pulse-width modulated DoS signals[J].SIAM Journal on Control and Optimization,2016,54(6):3084-3105
[8] 王誉达,查利娟,刘金良,等.基于事件触发和欺骗攻击的多智能体一致性控制[J].南京信息工程大学学报(自然科学版),2019,11(4):380-389
WANG Yuda,ZHA Lijuan,LIU Jinliang,et al.Event-based consensus of multi-agent systems with deception attacks[J].Journal of Nanjing University of Information Science & Technology (Natural Science Edition),2019,11(4):380-389
[9] 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
[10] Feng S,Tesi P.Resilient control under denial-of-service:robust design[J].Automatica,2017,79:42-51
[11] 王江宁,严怀成,李郅辰,等.具有 DoS 攻击的网络控制系统事件触发安全控制[J].南京信息工程大学学报(自然科学版),2018,10(6):716-722
WANG Jiangning,YAN Huaicheng,LI Zhichen,et al.Event-based security control for networked control systems with DoS attacks [J].Journal of Nanjing University of Information Science & Technology (Natural Science Edition),2018,10(6):716-722
[12] Ma R J,Shi P,Wang Z H,et al.Resilient filtering for cyber-physical systems under denial-of-service attacks[J].International Journal of Robust and Nonlinear Control,2020,30(5):1754-1769
[13] Wang M F,Xu B G.Guaranteed cost control of cyber-physical systems with packet dropouts under dos jamming attacks [J].Asian Journal of Control,2019.DOI:10.1002/asjc.2130
[14] Su L,Ye D.Observer-based output feedback $H_\infty$ control for cyber-physical systems under randomly occurring packet dropout and periodic DoS attacks[J].ISA Transactions,2019,95:58-67
[15] Zhong Z X,Zhu Y Z.Observer-based output-feedback control of large-scale networked fuzzy systems with two-channel event-triggering[J].Journal of the Franklin Institute,2017,354(13):5398-5420

# Observer-based output feedback control for networked control systems under denial-of-service attacks

ZHAO Ning[1] ZHANG Huiyan[2] SHI Peng[3]
1 College of Automation,Harbin Engineering University,Harbin 150001
2 National Research Base of Intelligent Manufacturing Service,Chongqing Technology and Business University,Chongqing 400067
3 School of Electrical and Electronic Engineering,University of Adelaide,Adelaide,SA 5005

**Abstract** This paper is concerned with $H_\infty$ output feedback control problem of networked control systems under denial-of-service attacks. Denial-of-service attacks are characterized by energy constraint jamming signal with periodic strategy,which attack wireless network channels and degrade system performance.Under the premise that the state of the system is partly unknown,by designing the observer-based output feedback controller,networked control systems under packet loss and denial-of-service attacks can maintain stable and pre-specified performance level.Finally,a numerical example is presented to verify the effectiveness of the designed controller.

**Key words** networked control systems;denial-of-service attacks;packet loss;stability;$H_\infty$ performance level