第 40 卷第 2 期
2023 年 2 月

控 制 理 论 与 应 用
Control Theory & Applications

Vol. 40 No. 2
Feb. 2023

拒绝服务攻击下网络化非线性系统的采样数据控制

赵　宁[1†], 刘永超[2]

(1. 哈尔滨工程大学 智能科学与工程学院, 黑龙江 哈尔滨 150001;

2. 青岛大学 复杂性科学研究所, 山东 青岛 266071)

摘要: 本文研究了在拒绝服务攻击下网络化非线性系统的采样数据输出反馈控制问题. 首先, 为了避免使用完整的状态信息, 在存在拒绝服务攻击的情况下设计了一种新颖的切换观测器. 其次, 同时考虑两个采样周期和拒绝服务攻击的影响, 建立了一个新的切换增广系统模型, 包括系统本身和误差系统. 利用该模型和分段Lyapunov-Krasovskii泛函方法推导出保证切换增广系统是指数稳定的充分条件. 进一步, 利用线性矩阵不等式的解给出了观测器和控制器增益的共同设计方案. 最后, 通过仿真验证所提出控制方法的有效性.

关键词: 网络化非线性系统; 采样数据控制; 拒绝服务攻击; 指数稳定

引用格式: 赵宁, 刘永超. 拒绝服务攻击下网络化非线性系统的采样数据控制. 控制理论与应用, 2023, 40(2): 240 – 247

DOI: 10.7641/CTA.2022.11302

Sampled-data control for networked nonlinear systems under denial-of-service attacks

ZHAO Ning[1†], LIU Yong-chao[2]

(1. College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin Heilongjiang 150001, China;
2. Institute of Complexity Science, Qingdao University, Qingdao Shandong 266071, China)

Abstract: This paper studies the sampled-data output feedback control problem for networked nonlinear systems under denial-of-service attacks. First, to avoid using full state information, a novel switched observer is developed in the presence of denial-of-service attacks. Second, a new switched augmented system model, including the considered system and the error system, is established by considering the effect of two sampling periods and denial-of-service attacks simultaneously. By virtue of this new model combined with a piecewise Lyapunov-Krasovskii functional method, the sufficient conditions are derived to guarantee exponential stability of the resulting switched system. Furthermore, the co-design method of observer and controller gains is given by a solution of linear matrix inequalities. Finally, simulation results are presented to verify the effectiveness of the developed control method.

Key words: networked nonlinear systems; sampled-data control; denial-of-service attacks; exponential stability

Citation: ZHAO Ning, LIU Yongchao. Sampled-data control for networked nonlinear systems under denial-of-service attacks. *Control Theory & Applications*, 2023, 40(2): 240 – 247

1　引言

近年来, 网络控制系统 (networked control system, NCS)的安全控制问题受到广泛关注[1–4]. 物理设备之间的通信网络容易受到蓄意攻击, 使系统间歇性地处于开环状态, 进而导致系统瘫痪. 此外, 一些攻击者对网络系统造成严重事故, 例如石油管道爆炸和电力系统故障[5]. 特别是拒绝服务(denial of service, DoS)攻击, 向网络通信通道发送大量数据, 减缓网络响应和阻断信号传输, 最终导致通信网络瘫痪, 这就给NCS带来极大的安全隐患[6]. 因此, 考虑网络攻击的影响, 研究NCS的安全控制问题具有重要的现实意义.

相比其他类型的攻击, 例如欺骗攻击和重放攻击, DoS攻击是黑客容易采用的攻击方式[7]. 因此, 如何设计防御策略来抵御DoS攻击的影响受到了广泛关注, 并取得了一些丰硕的成果[8–11]. 文献[8]提出了一种采样数据控制方案, 通过限制DoS攻击的频率和持续时间确保了NCS稳定性. 文献[9]将文献[8]中的结果推广到DoS攻击下的多个传输通道,并使用线性矩阵不

收稿日期: 2021–12–30; 录用日期: 2022–05–27.
†通信作者. E-mail: zhaoning_hrbeu@163.com.
本文责任编委: 龙离军.
国家自然科学基金项目(52171299)资助.
Supported by the National Natural Science Foundation of China (52171299).

等式技术来分析系统稳定性. 考虑到DoS攻击的影响和节省网络资源, 文献[10]研究了随机NCS的弹性事件触发控制问题.

随着无线数字通信的迅速发展, 实际系统的控制输入命令通常采用采样数据控制方式. 特别是, NCS的控制信号一般是通过网络媒介传输的. 传感器和/或控制器通过网络传输的信号只能是离散数字信号, 即采样数据信号. 这种控制方法在现有结果[12–15]中得到了广泛的讨论. 文献[12]提出分散输出反馈控制器, 通过调整增益和最大允许采样周期旨在保证系统全局稳定. 文献[13]在考虑随机故障和非周期性采样下, 研究了柔性航天器的有限时间模糊切换控制问题. 针对受限于执行器饱和下的一类非线性系统, 文献[14]研究了一种基于采样数据扩展状态观测器的自抗扰控制问题. 上述文献没有考虑到开放性网络所带来的安全问题. 同时, 考虑到系统的全状态信息一般是不可测的, 因此仅仅利用可测量的输出信息去设计控制器更加符合实际情况. 为此, 文献[15]提出了一种分散输出反馈采样数据控制策略去保证非线性系统在DoS攻击下是稳定的.

文献[15]中是在没有考虑时滞的影响下得出了结论. 然而时滞现象广泛地存在实际控制系统中. 受到文献[15]结果的启发, 本文提出了一种新颖而简单的方法来解决网络化非线性时滞系统的安全控制问题. 本文的主要贡献总结如下:

1) 提出了一种新的切换系统方法, 将非线性NCS, DoS攻击和采样数据控制策略集成到一个统一的框架中. 通过使用分段Lyapunov-Krasovskii泛函方法推导出了一些新的稳定性判据, 以保证生成的时滞切换系统是指数稳定的;

2) 与文献[15]的系统模型相比, 本文考虑了时滞因素对系统性能的影响, 这符合大部分物理系统中存在时延的情况. 利用线性矩阵不等式技术, 得到了时滞相关的稳定性条件;

3) 观察文献[15]中的定理1可知, 只有在控制增益和观测增益给定的前提下, 才能转化为标准的线性矩阵不等式用于求解. 本文提出了一种解耦方法, 并且给出了共同设计观测增益和控制增益的解决方案. 本文方法的优势在于给出了控制增益和观测增益的显式表达式, 避免了随机尝试去寻找合适的增益参数.

论文的其余部分安排如下: 在第2节中, 描述了系统模型、DoS攻击模型、建立在DoS攻击下的观测器和基于观测器的控制器; 在第3节中, 导出了稳定性分析的主要结果以及控制器和观测器设计策略; 第4节展示了两个例子用于验证理论结果; 最后, 第5节给出了结论.

符号说明: 设$\mathbb{R}^{n\times m}$是所有$n\times m$实矩阵的集合; $\mathcal{T}>0$ $(\mathcal{T}\geqslant 0)$表示矩阵$\mathcal{T}$是实对称正定(半正定)的; $\mathrm{He}(\mathcal{T})$表示$\mathcal{T}+\mathcal{T}^{\mathrm{T}}$; $*$表示由对称块矩阵的对称项; $\mathrm{diag}\{\cdots\}$代表块对角线矩阵.

2 问题描述

2.1 系统描述

考虑一类网络化非线性时滞系统

$$\begin{cases}\dot{x}_k(t)=x_{k+1}(t)+f_k(x(t),x(t-\tau),u(t)),\\ \qquad k=1,\cdots,n-1,\\ \dot{x}_n(t)=u(t)+f_n(x(t),x(t-\tau),u(t)),\\ y(t)=x_1(t),\end{cases}\tag{1}$$

其中: $x(t)=[x_1(t)\ \cdots\ x_n(t)]^{\mathrm{T}}\in\mathbb{R}^n$是状态向量, $u(t)\in\mathbb{R}$是控制输入信号, $y(t)\in\mathbb{R}$是可测量的输出信号, 和$f_k(x(t),x(t),u(t))$是连续的非线性函数. 延迟状态$x(t)$表示为$x(t-\tau)=[x_1(t-\tau_1)\cdots\ x_n(t-\tau_n)]^{\mathrm{T}}$, 其中$\tau_i>0,\ i=1,\cdots,n$表示常数时滞. 系统的初始条件设置为$x(s)=\varphi(s),\ s\in[-\bar{\tau},0]$, 其中$\bar{\tau}=\max\{\tau_1,\cdots,\tau_n\}$. 针对系统中的非线性函数, 给出如下假设:

假设 1[16] 对于$k=1,\cdots,n$, 存在一些已知的常数$\alpha_{l,k}\geqslant 0$和$\beta_{l,k}\geqslant 0$, 使得

$$|f_k(x(t),x(t-\tau),u(t))|\leqslant \\ (\sum_{l=1}^{k}\alpha_{k,l}|x_l(t)|+\sum_{l=1}^{k}\beta_{k,l}|x_l(t-\tau_l)|).\tag{2}$$

系统(1)写成向量形式为

$$\begin{cases}\dot{x}(t)=Ax(t)+Bu(t)+f(x(t),x(t-\tau),u(t)),\\ y(t)=Cx(t),\end{cases}\tag{3}$$

其中:

$$A=\begin{bmatrix}0&1&&\\&\ddots&\ddots&\\&&0&1\\&&&0\end{bmatrix},B=\begin{bmatrix}0\\ \vdots\\0\\1\end{bmatrix},C=\begin{bmatrix}1\\ \vdots\\0\\0\end{bmatrix}^{\mathrm{T}}\text{ 和}$$

$$f(x(t),x(t-\tau),u(t))=\\ [f_1(x(t),x(t-\tau),u(t))\cdots f_n(x(t),x(t-\tau),u(t))].$$

引理 1 设非线性函数$f_k(x(t),x(t-\tau),u(t))$, $k=1,\cdots,n$, 满足假设1, 和给定矩阵$\bar{H}=\mathrm{diag}\{H^{n-1},\cdots,H,1\}$, 其中$H\geqslant 1$是标量参数. 则

$$||\bar{H}f(x(t),x(t-\tau),u(t))||^2\leqslant\\ c_1^2||\bar{H}x(t)||^2+c_2^2||\bar{H}x(t-\tau)||^2,$$

其中:

$$c_1^2=\max\{\sum_{k=1}^{n}\frac{k\alpha_{k,1}^2}{H^{2(k-1)}},\cdots,\sum_{k=n}^{n}\frac{k\alpha_{k,n}^2}{H^{2(k-n)}}\},\tag{4}$$

$$c_2^2=\max\{\sum_{k=1}^{n}\frac{k\beta_{k,1}^2}{H^{2(k-1)}},\cdots,\sum_{k=n}^{n}\frac{k\beta_{k,n}^2}{H^{2(k-n)}}\}.\tag{5}$$

证 对于$k=1\cdots n$, 由假设1可得

$$|f_k(x(t),x(t-\tau),u(t))|^2\leqslant$$
$$(2k\sum_{l=1}^{k}\alpha_{k,l}^2|x_l(t)|^2+2k\sum_{l=1}^{k}\beta_{k,l}^2|x_l(t-\tau_l)|^2).$$

基于上式, 可得

$$||Hf(x(t),x(t-\tau),u(t)))||^2=$$
$$\sum_{k=1}^{n}H^{2(n-k)}|f_k(x(t),x(t-\tau),u(t)|^2=$$
$$(\sum_{k=1}^{n}\frac{k\alpha_{k,1}^2}{H^{2(k-1)}})\,|H^{n-1}x_1(t)|^2+\cdots+$$
$$(\sum_{k=n}^{n}\frac{k\alpha_{k,n}^2}{H^{2(k-n)}})\,|H^0x_n(t)|^2+$$
$$(\sum_{k=1}^{n}\frac{k\beta_{k,1}^2}{H^{2(k-1)}})\,|H^{n-1}x_1(t-\tau_1)|^2+\cdots+$$
$$(\sum_{k=n}^{n}\frac{k\beta_{k,n}^2}{H^{2(k-n)}})\,|H^0x_n(t-\tau_n)|^2.$$

根据式(4)–(5), 可得出结论. 证毕.

2.2 DoS攻击

由于网络化控制系统的结构属性, 当信号通过网络媒介传输时容易受到攻击的蓄意破坏. 特别是DoS攻击的影响, 因为在控制系统中, 网络攻击更加容易发生的是DoS攻击[7]. 它的主要目的是阻断信号的正常传输, 使得系统在开环状态和闭环状态不定期的切换. 由于物理设备自带着防火墙和检测防御装置, 使得攻击不可能持续破坏. 另一方面, 攻击者为了防止攻击信息被检测到, 因此会间歇发送干扰信号, 使得防御者很难及时检测到. 基于整个时间轴, 设区间$D_{1,j}=[d_j,d_j+\ell_j)$表示为攻击静默时间, 区间$D_{2,j}=[d_j+\ell_j,d_{j+1}),j=0,1,\cdots,$表示为攻击活跃区间, 其中$d_0=0$, d_{j+1}表示每个攻击区间攻击开始发生时刻, $d_j+\ell_j$表示每个攻击区间攻击停止时刻. 基于上述分析, 攻击的频率和持续时间满足如下限制条件.

假设 2[8] [攻击频率] 对于$t\geqslant\bar t_1\geqslant0$, 存在一个标量$T_1>0$, 使得

$$N(t,\bar t_1)\leqslant\frac{t-\bar t_1}{T_1}.$$

假设 3[8] [攻击持续时间]对于$t\geqslant\bar t_1\geqslant0$, 存在一个标量$T_2>1$, 使得

$$\Pi(t,\bar t_1)\leqslant\frac{t-\bar t_1}{T_2}.$$

设攻击区间的采样器1的采样周期为h_1, 设无攻击区间的采样器2的采样周期为h_2, 无攻击区间采样时刻记为$t_i=ih_1,i=1,2,\cdots$. 这里假设存在一个正整数$\aleph$, 使得$h_1=\aleph h_2$. 这里采用两种采样周期主要是借助文献[8]中的的思想. 由于攻击可能发生在两个采样时刻之间, 这样难以采用一个采样周期分割区间去分析系统的稳定和控制器设计. 为此这里依据攻击区间和无攻击区间选取不同的采样周期, 将整个时间轴分成攻击影响区域和无攻击影响区域, 进而清晰的描述攻击对系统的影响. 以采样区间$[t_i,t_{i+1}]$和攻击区间$D_{2,j}$为例, 可以列举为3种情况说明攻击与采样周期之间的关系:

1) 当以采样周期为h_1进入到攻击区间, 并且攻击持续至少一个采样周期时间, 那么攻击真正影响信号传输的开始时刻为$\underline{n}_jh_2=t_i+h_1$. 相对应的攻击影响结束时刻为$\bar n_jh_2$, 其中$\bar n_j=\max\{\mu|\mu h_2\leqslant d_{j+1},\mu\in\mathbb{N}\}$;

2) 当以采样周期为h_2进入到攻击区间, 这就意味着攻击发生的两个区间距离很近, 那么攻击真正影响信号传输的开始时刻为$\underline{n}_jh_2$, 其中$\underline{n}_j=\min\{\mu|\mu h_2\geqslant d_j+\ell_j,\mu\in\mathbb{N}\}$. 相对应的攻击影响结束时刻仍旧为$\bar n_jh_2$;

3) 当攻击发生在采样周期为h_1的区间内, 那么攻击对系统的性能是没有影响的.

基于上述分析可知, 攻击有效的影响区间可以定义为: $\bar D_{1,j}=[\underline{n}_jh_2,(\bar n_j+1)h_2)$. 为了避免上述区间存在交集的情况, 受文献[8]启发, 下面给出严格的无交集的攻击有效影响区间. 设$\eta_0^1=\underline{n}_0h_2$, $\eta_{m+1}^1=\min\{\underline{n}_jh_2>\eta_m^1,\ d_j+\ell_j-t_i\leqslant h_1\}$, 和

$$\eta_m^2=\sum_{d_j\in[\eta_m^1,\eta_{m+1}^1)}|\bar D_{2,j}\backslash\bar D_{2,j+1}|.$$

对于任意时间区间$[\bar t_1,\bar t_2)$, 无交集的攻击区间定义为

$$\tilde D_{2,m}(\bar t_2,\bar t_1)=\bigcup_{m\in\mathbb{N}}G_{1,m}\cap[\bar t_1,\bar t_2),\tag{6}$$

其中$G_{1,m}=[\eta_m^1,\eta_m^1+\eta_m^2)$. 与之相对应的无攻击影响有效区域为

$$\tilde D_{1,m}(\bar t_2,\bar t_1)=\bigcup_{m\in\mathbb{N}}G_{2,m-1}\cap[\bar t_1,\bar t_2),\tag{7}$$

其中: $G_{2,-1}=[0,\eta_0^1]$, $G_{2,m}=[\eta_m^1+\eta_m^2,\eta_{m+1}^1)$. 那么, 显然有

$$|\tilde D_{1,m}(\bar t_2,\bar t_1)|=\bar t_2-\bar t_1-|\tilde D_{1,m}(\bar t_2,\bar t_1)|.$$

通过观察攻击区域$D_{2,j}$和有效攻击区域$\bar D_{2,j}$, 可知

$$|\bar D_{2,j}|\leqslant|D_{2,j}|+h_2,$$

这就意味着

$$|\tilde D_{1,m}(\bar t_2,\bar t_1)|\leqslant|\Pi(\bar t_2,\bar t_1)|+h_2N(\bar t_2,\bar t_1).\tag{8}$$

2.3 基于采样数据的输出反馈控制

在攻击有效区间和无效区间, 基于采样数据的观测器和控制器设计如下:

$$\dot{\hat x}(t)=\begin{cases}A\hat x(t)+Bu(t)+\\ L_1(y(t_i)-C\hat x(t_i)),t\in G_{1,m},\\ A\hat x(t)-L_2C\hat x(t_i),\ t\in G_{2,m},\end{cases}\tag{9}$$

和

$$u(t)=\begin{cases}-K\hat{x}(t_i),\ t\in G_{1,m},\\ 0,\qquad\quad\ t\in G_{2,m}.\end{cases}\tag{10}$$

设误差信号为$e(t)=x(t)-\hat{x}(t)$. 基于系统(3)和观测器(9), 可得

$$\dot{e}(t)=\begin{cases}Ae(t)-L_1Ce(t-d(t))+\\ f(x(t),x(t-\tau),u(t)),\ t\in G_{1,m},\\ Ae(t)+L_2C\hat{x}(t-d(t))+\\ f(x(t),x(t-\tau),u(t)),\ t\in G_{2,m},\end{cases}\tag{11}$$

设$\xi(t)=[x^{\mathrm T}(t)\ \mathrm{e}^{\mathrm T}(t)]^{\mathrm T}$, 整合观测器(9), 控制器(10)和误差系统(11)可得

$$\dot{\xi}(t)=\begin{cases}\bar{A}\xi(t)+\bar{L}_1\xi(t-d(t))+\\ \bar{f}(x(t),x(t-\tau),u(t)),\ t\in G_{1,m},\\ \bar{A}\xi(t)+\bar{L}_2\xi(t-d(t))+\\ \bar{f}(x(t),x(t-\tau),u(t)),\ t\in G_{2,m},\end{cases}\tag{12}$$

其中:

$d(t)=t-t_i$,

$\bar{A}=\begin{bmatrix}A & \mathbf{0}\\ \mathbf{0} & A\end{bmatrix}$, $\bar{L}_1=\begin{bmatrix}-BK & BK\\ \mathbf{0} & -L_1C\end{bmatrix}$, $\bar{L}_2=\begin{bmatrix}\mathbf{0} & \mathbf{0}\\ L_2C & \mathbf{0}\end{bmatrix}$,

$\bar{f}(x(t),x(t-\tau),u(t))=$

$[f^{\mathrm T}(x(t),x(t-\tau),u(t))\ \ f^{\mathrm T}(x(t),x(t-\tau),u(t))]^{\mathrm T}$.

为了方便后续分析, 下面给出系统(12)的指数稳定性定义:

定义 1 [17] 对于任意的初始条件, 存在两个标量$\alpha\geqslant 1$和$\beta>0$, 使得系统的解满足如下不等式:

$$||x(t)||\leqslant\alpha\mathrm{e}^{-\beta t}||\varphi||_{\bar\tau},\ t\geqslant 0,$$

其中$||\varphi||_{\bar\tau}=\sup\limits_{s\in[-\bar\tau,0]}||\varphi(s)||$, 则称系统(12)是指数稳定的.

本文的目标是设计一个基于观测器的采样数据控制器, 使得系统(12)在DoS攻击下是指数稳定的.

3 稳定性分析和控制器设计

本节将给出在DoS攻击下系统(12)指数稳定的充分条件.

定理 1 设增益矩阵K, L_1和L_2是已知的. 对于给定的常数$\tau_i, i=1,\cdots,n, \delta_\sigma, h_\sigma, T_\sigma, \gamma_\sigma, \kappa_\sigma, \sigma=1,2$, 满足

$$\lambda=:\gamma_1-(\gamma_1+\gamma_2)(\frac{\bar{h}_1+h_2}{T_1}+\frac{1}{T_2})-\frac{\ln(\kappa_1\kappa_2)}{T_1}>0,\tag{13}$$

其中$\bar{h}_1=\max\{h_1,\bar\tau\}$. 如果存在正定矩阵$P_\sigma$, Q_σ, R_σ, 任意矩阵X_σ, 和正的标量参数$\rho_{\sigma i}, \sigma=1,2, i=1,\cdots,n$, 使得如下不等式成立:

$$c_2^2-\rho_{\sigma i}^2\mathrm{e}^{-(2-\sigma)\gamma_\sigma\tau_i}\leqslant 0,\tag{14}$$

$$\begin{bmatrix}R_\sigma & X_\sigma\\ * & R_\sigma\end{bmatrix}>0,\tag{15}$$

$$P_1\leqslant\kappa_2P_2,\ P_2\leqslant\kappa_1\mathrm{e}^{(\gamma_1+\gamma_2)\bar{h}_1}P_1,\tag{16}$$

$$Q_\sigma\leqslant\kappa_{3-\sigma}Q_{3-\sigma},\ R_\sigma\leqslant\kappa_{3-\sigma}R_{3-\sigma},\tag{17}$$

$$\rho_{\sigma i}^2\leqslant\kappa_{3-\sigma}\rho_{(3-\sigma)i}^2,\tag{18}$$

$$\begin{bmatrix}\varGamma_{11}^\sigma & \varGamma_{12}^\sigma & \varGamma_{13}^\sigma & P_\sigma & h_1\bar{A}^{\mathrm T}P_\sigma\\ * & \varGamma_{22}^\sigma & \varGamma_{23}^\sigma & \mathbf{0} & h_1\bar{L}_\sigma^{\mathrm T}P_\sigma\\ * & * & \varGamma_{33}^\sigma & \mathbf{0} & \mathbf{0}\\ * & * & * & \varGamma_{44}^\sigma & h_1P_\sigma\\ * & * & * & * & \varGamma_{55}^\sigma\end{bmatrix}<0,\tag{19}$$

其中:

$\varGamma_{11}^1=\mathrm{He}\{P_1\bar{A}\}+\gamma_1P_1+Q_1-\mathrm{e}^{-\gamma_1h_1}R_1+\varUpsilon_1$,

$\varUpsilon_1=I_1^{\mathrm T}\bar{H}^{\mathrm T}(\bar\rho_1^{\mathrm T}\bar\rho_1+c_1^2I_{2n})\bar{H}I_1,\ I_1^{\mathrm T}=[I_n\ 0_n]$,

$\varGamma_{12}^1=P_1\bar{L}_1+\mathrm{e}^{-\gamma_1h_1}(R_1-X_1),\ \varGamma_{13}=\mathrm{e}^{-\gamma_1h_1}X_1$,

$\varGamma_{22}^1=-\mathrm{e}^{-\gamma_1h_1}(2R_1-\mathrm{He}\{X_1\})$,

$\varGamma_{23}^1=\mathrm{e}^{-\gamma_1h_1}(R_1-X_1)$,

$\varGamma_{33}^1=-\mathrm{e}^{-\gamma_1h_1}(Q_1+R_1)$,

$\varGamma_{11}^2=\mathrm{He}\{P_2\bar{A}\}-\gamma_2P_2+Q_2-R_2+\varUpsilon_2$,

$\varUpsilon_2=I_1^{\mathrm T}\bar{H}^{\mathrm T}(\bar\rho_2^{\mathrm T}\bar\rho_2+c_1^2I_{2n})\bar{H}I_1$,

$\varGamma_{12}^2=P_2\bar{L}_2+R_2-X_2,\ \varGamma_{23}=X_2$,

$\varGamma_{22}^2=-(2R_2-\mathrm{He}\{X_2\})$,

$\varGamma_{23}^2=R_2-X_2,\ \varGamma_{33}^2=Q_2+R_2$,

$\varGamma_{44}^\sigma=-\mathrm{diag}\{\bar{H}^{\mathrm T}\bar{H},\bar{H}^{\mathrm T}\bar{H}\}$,

$\varGamma_{55}^\sigma=\delta_\sigma^2R_\sigma-2\delta_\sigma P_\sigma$,

$\bar\rho_\sigma=\mathrm{diag}\{\rho_{\sigma1},\cdots,\rho_{\sigma n}\}$.

那么, 系统(12)在DoS攻击下是指数稳定的.

证 对于$t\geqslant 0$, 构造如下形式的Lyapunov-Krasovskii泛函:

$$V(t)=\begin{cases}V_1(t),\ t\in G_{1,m},\\ V_2(t),\ t\in G_{2,m},\end{cases}\tag{20}$$

其中

$V_\sigma(t)=$

$\xi^{\mathrm T}(t)P_\sigma\xi(t)+\int_{t-h_1}^t\mathrm{e}^{(-1)^\sigma\gamma_\sigma(t-s)}\xi^{\mathrm T}(s)Q_\sigma\xi(s)\mathrm{d}s+$

$\sum\limits_{i=1}^n\int_{t-\tau_i}^t\mathrm{e}^{(-1)^\sigma\gamma_\sigma(t-s)}\rho_{\sigma i}^2H^{2(n-i)}x_i^2(s)\mathrm{d}s+$

$h_1\int_{-h_1}^0\int_{t+s}^t\mathrm{e}^{(-1)^\sigma\gamma_\sigma(t-\theta)}\dot\xi^{\mathrm T}(\theta)R_\sigma\dot\xi(\theta)\mathrm{d}\theta\mathrm{d}s$.

当$t\in G_{1,m}$, 泛函沿着系统(12)的轨迹对时间的导数为

$\dot{V}_1(t)\leqslant$

$$\xi^{\mathrm{T}}(t)\mathrm{He}\{P_1\bar{A}\}\xi(t)+2\xi^{\mathrm{T}}(t)P_1\bar{L}_1\xi(t-d(t))+\\2\xi^{\mathrm{T}}(t)P_1\bar{f}(x(t),x(t-\tau),u(t))+\\\xi^{\mathrm{T}}(t)Q_1\xi(t)-\mathrm{e}^{-\gamma_1h_1}\xi^{\mathrm{T}}(t-h_1)Q_1\xi(t-h_1)+\\\sum_{i=1}^{n}\rho_i^2H^{2(n-i)}x_i^2(t)+h_1^2\dot{\xi}^{\mathrm{T}}(t)R_1\dot{\xi}(t)-\\\sum_{i=1}^{n}\rho_i^2\mathrm{e}^{-\gamma_1\tau_i}H^{2(n-i)}x_i^2(t-\tau_i)-\\\mathrm{e}^{-\gamma_1h_1}h_1\int_{-h_1}^{0}\dot{\xi}^{\mathrm{T}}(\theta)R_1\dot{\xi}(\theta)\mathrm{d}\theta. \tag{21}$$

通过利用Jenson不等式和倒凸组合技术, 根据条件不等式(15), 式$-h_1\int_{-h_1}^{0}\dot{\xi}^{\mathrm{T}}(\theta)R_1\dot{\xi}(\theta)\mathrm{d}\theta$ 可放缩为

$$-h_1\int_{-h_1}^{0}\dot{\xi}^{\mathrm{T}}(\theta)R_1\dot{\xi}(\theta)\mathrm{d}\theta\leqslant\\-\begin{bmatrix}\chi_1(t)\\\chi_2(t)\end{bmatrix}^{\mathrm{T}}\begin{bmatrix}R_1&X_1\\*&R_1\end{bmatrix}\begin{bmatrix}\chi_1(t)\\\chi_2(t)\end{bmatrix}, \tag{22}$$

其中: $\chi_1(t)=\xi(t)-\xi(t-d(t))$, $\chi_2(t)=\xi(t-d(t))-\xi(t-h_1)$.

对于任意选取的常数$\delta_1>0$, 显然有$(P_1R_1^{-\frac{1}{2}}-\delta_1R^{\frac{1}{2}})^{\mathrm{T}}(P_1R_1^{-\frac{1}{2}}-\delta_1R^{\frac{1}{2}})\geqslant0$, 这就意味着

$$-P_1R_1^{-1}P_1\leqslant\delta_1^2R_1-2\delta_1P_1. \tag{23}$$

那么, 整合不等式(21)–(23), 利用引理1和定理条件(14)(19), 可得

$$\dot{V}_1(t)+\gamma_1V_1(t)\leqslant0,\ t\in G_{1,m}. \tag{24}$$

当$t\in G_{2,m}$, 计算过程类似于$t\in G_{1,m}$, 因此详细过程省略. 由此可以得到

$$\dot{V}_2(t)-\gamma_2V_2(t)\leqslant0,\ t\in G_{2,m}. \tag{25}$$

那么, 整合式(24)–(25), 可得

$$\dot{V}(t)=\begin{cases}\mathrm{e}^{-\gamma_1(t-\eta_m^1)}V_1(\eta_m^1), & t\in G_{1,m},\\\mathrm{e}^{\gamma_2(t-\eta_m^1-\eta_m^2)}V_2(\eta_m^1+\eta_m^2), & t\in G_{2,m}.\end{cases}$$

余下的证明可以在文献[10]的帮助下完成. 因此, 这里不再详细描述. 证毕.

通过观察可知, 定理1中是在给定控制增益和观测增益下给出系统稳定判据. 因此, 如下定理将基于定理1的结果设计控制增益和观测增益, 并且在此增益下能够保证系统是稳定的.

定理 2 对于给定的常数$\tau_i, i=1,\cdots,n$, $\delta_\sigma, h_\sigma, T_\sigma, \gamma_\sigma, \kappa_\sigma, \sigma=1,2$, 满足式(13). 如果存在对称正定矩阵$P_\sigma=\mathrm{diag}\{P_{\sigma1},P_{\sigma2}\}>0$, Q_σ, R_σ, 任意矩阵$\bar{K}$, Y, Z_σ, X_σ, $\sigma=1,2$, 和正的标量参数ε和$\rho_{\sigma i}$, $i=1,\cdots,n$, 使得式(14)–(18)和下面不等式成立:

$$\begin{bmatrix}-\varepsilon I&(P_{11}B-BY)^{\mathrm{T}}\\*&-I\end{bmatrix}<0, \tag{26}$$

$$\begin{bmatrix}\mathit{\Gamma}_{11}^\sigma&\mathit{\Gamma}_{12}^\sigma&\mathit{\Gamma}_{13}^\sigma&P_\sigma&h_1\bar{A}^{\mathrm{T}}P_\sigma\\*&\mathit{\Gamma}_{22}^\sigma&\mathit{\Gamma}_{23}^\sigma&\mathbf{0}&h_1\hat{L}_\sigma^{\mathrm{T}}\\*&*&\mathit{\Gamma}_{33}^\sigma&\mathbf{0}&\mathbf{0}\\*&*&*&\mathit{\Gamma}_{44}^\sigma&h_1P_\sigma\\*&*&*&*&\mathit{\Gamma}_{55}^\sigma\end{bmatrix}<0, \tag{27}$$

其中:

$$\hat{L}_1=\begin{bmatrix}-B\bar{K}&B\bar{K}\\\mathbf{0}&-Z_1C\end{bmatrix},\ \hat{L}_2=\begin{bmatrix}\mathbf{0}&\mathbf{0}\\Z_2C&\mathbf{0}\end{bmatrix}.$$

那么, 系统(12)在DoS攻击下是指数稳定的. 而且, 观测增益和控制增益的显式表达式为

$$L_1=P_{12}^{-1}Z_1,\ L_2=P_{22}^{-1}Z_2,\ K=Y^{-1}\bar{K}.$$

证 从系统(3)可知, 矩阵B是列满秩的. 那么就存在一个矩阵Y, 使得$P_{11}B=BY$. 它等价于$\mathrm{tr}\{(P_{11}B-BY)^{\mathrm{T}}(P_{11}B-BY)\}=0$成立. 通过利用Schur引理, 这个条件可以等价转化为优化问题(26). 设$Z_1=P_{12}L_1$, $Z_2=P_{22}L_2$ 和$K=Y\bar{K}$. 如果条件(27)成立, 那么定理1中的条件(19)成立. 这就保证了系统的稳定性.

证毕.

注 1 定理2的条件与采样周期$h_1(h_2)$密切相关. 对于较大的$h_1(h_2)$, 定理2中线性矩阵不等式的条件可能无解, 那么就无法设计控制器. 另一方面, 较小的$h_1(h_2)$通常会导致所考虑的最终系统的性能更好, 但是会增加网络负载. 因此应该选择一个相对小的采样周期$h_1(h_2)$去采集数据, 从而实现所需的系统的性能指标.

注 2 根据不等式(13), 衰减率为

$$\frac{\lambda}{2}=\gamma_1(1-\frac{\bar{h}_1+h_2}{T_1}-\frac{1}{T_2})-\\\gamma_2(\frac{\bar{h}_1+h_2}{T_1}+\frac{1}{T_2})-\frac{\ln(\kappa_1\kappa_2)}{T_1}. \tag{28}$$

从不等式(28)可以看出当所有其他参数固定时, 衰减率相对于参数$T_1(T_2)$而言, 随着$T_1(T_2)$的值增加, 攻击频率降低(攻击持续时间变短), 控制输入损失相对较少, 这意味着系统将以更大的衰减率达到稳定. 此外, 从不等式(28)可以看出, 当所有其他参数固定时, 衰减率是参数$\gamma_2(\gamma_1)$的单调递减(增)函数. 这意味着通过选取小的T_1, T_2, γ_2和尽可能大的γ_1以获得更大的衰减率同时保证定理2中的其他不等式成立, 从而保证系统快速地达到稳定.

注 3 相比于文献[15]中提出的控制策略, 本文的优势在于:

1) 文献[15]仅仅考虑了攻击影响传感器和控制器的网络通道, 而本文考虑了攻击同时影响双边网络通道. 在攻击破坏更加恶劣的情况下, 提出了安全控制器依然能够保证系统的稳定性;

2) 本文提出的采样控制策略可以弹性抵制攻击. 文献[15]仅仅采用了一种采样方案, 如果攻击停止时刻不是采样时刻, 这会间接延长攻击的不利影响. 而本文中通过利用切换采样方案, 保证攻击停止时刻控制器立刻更新去抵制攻击

的影响.

4 数值仿真

本节将分别采用数值例子和实际例子去说明结果的有效性.

例 1 考虑一个带有时滞的二阶非线性系统

$$\begin{cases}\dot{x}_1(t)=x_2(t)+0.5x_1(t)\sin(x_2^2(t)),\\ \dot{x}_2(t)=u(t)-0.4x_2(t-0.2)\cos(x_1^2(t)).\end{cases}\tag{29}$$

通过系统(29)可知$|0.5x_1(t)\sin(x_2^2(t))|\leqslant 0.5|x_1(t)|$, $|0.4x_2(t-0.2)\cos(x_1^2(t))|\leqslant 0.4|x_2(t-0.2)|$, $\tau_1=0$, 和$\tau_2=0.2$. 令参数$H=1.2$, 根据引理1可得$c_1^2=0.25$和$c_2^2=0.32$. 为了求解定理2中的线性矩阵不等式和仿真需要, 参数选取为$h_1=h_2=0.02$, $\kappa_1=\kappa_2=1.01$, $T_1=5$, $T_2=3$, $\gamma_1=1$, $\gamma_2=1.6$, $\varepsilon=0.0001$, $\delta_1=0.1$ $\delta_2=0.2$, $\rho_{11}=\rho_{12}=\rho_{21}=\rho_{22}=1.32$. 根据这些参数, 可得$\lambda=0.015>0$, $c_2^2-\rho_{\sigma 1}^2\mathrm{e}^{-(2-\sigma)\gamma_\sigma\tau_1}=-1<0$, $c_2^2-\rho_{12}^2\mathrm{e}^{-\gamma_1\tau_2}=-0.7607<0$, 这就意味着不等式(13)–(14)成立. 同理, 可知式(18)成立.

接下来, 基于定理2的线性矩阵不等式条件, 利用计算软件可以求得观测增益和控制增益为

$$L_1=[11.3041\ \ 2.2778]^{\mathrm{T}},$$
$$L_2=[-0.0309\ \ -0.0346]^{\mathrm{T}},$$
$$K=[1.4525\ \ 3.4242].$$

初始条件选取为$x(0)=[1\ 2]^{\mathrm{T}}$,和$\hat{x}(0)=[1\ 0]^{\mathrm{T}}$. 为了说明选取的数值例子是非平凡的, 当系统处于开环状态时, 通过图1可知, 系统是不稳定的. 在DoS 攻击下, 利用设计的控制增益和观测增益, 可得仿真给出系统的状态曲线图, 误差轨迹图和控制输入, 如图2–4所示. 图中, 灰色阴影部分表示攻击的发生区间, 不难计算可以得出在40 s之内攻击发生的频次是7次和持续时间为10.21 s. 经过验证可知限制攻击频率和攻击持续时间的假设1和假设2满足. 另一方面, 从图2和图3知系统和误差系统是稳定的, 这就验证了所提出基于观测器的控制策略能够有效地抵制攻击的影响, 同时保证了系统的稳定性.

例 2 考虑如下化学反应釜系统模型[18]:

$$\begin{cases}\dot{x}_1(t)=x_2(t)-2(x_1(t)+x_1(t-\tau))-\\ \qquad x_1(t)+1.5x_1(t-\tau),\\ \dot{x}_2(t)=u(t)-3x_2(t)+x_1(t-\tau)+x_2(t-\tau)-\\ \qquad 0.5x_2(t-\tau)\cos(x_1(t)).\end{cases}\tag{30}$$

所需的一些参数与例子1相同, 其他参数选取为$\delta_1=\delta_2=0.01$, $\rho_{11}=\rho_{21}=\rho_{22}=4.6$ 和$\rho_{12}=7.5$. 通过计算可得$c_1^2=15.25$和$c_2^2=4.5$. 经过验证可得不等式(13)–(14)成立. 利用软件可以求得观测增益和控制增益为

$$L_1=[17.6346\ \ 2.3364]^{\mathrm{T}},$$
$$L_2=[0.0006\ \ 0.0243]^{\mathrm{T}},$$
$$K=[1.2109\ \ 5.5705].$$

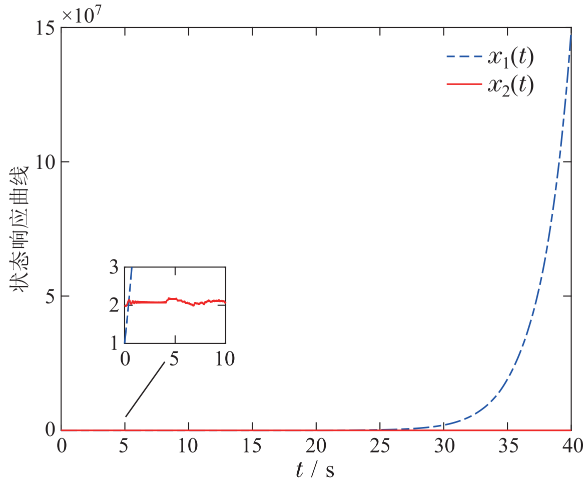

图 1 开环系统(29)状态

Fig. 1 The states of the open system (29)

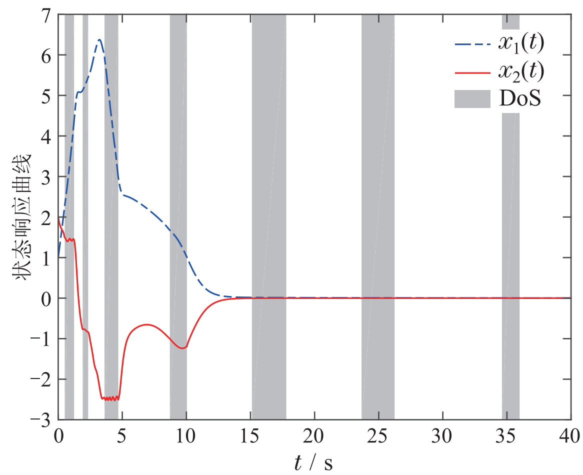

图 2 在DoS攻击下系统(29)的状态

Fig. 2 The states of system (29) under DoS attacks

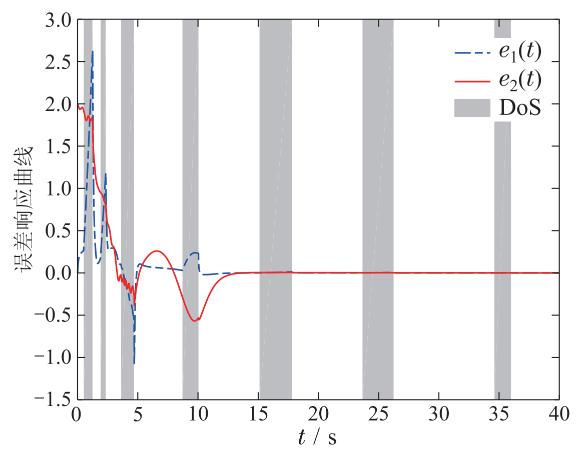

图 3 在DoS攻击下误差系统的状态

Fig. 3 The states of the error system under DoS attacks

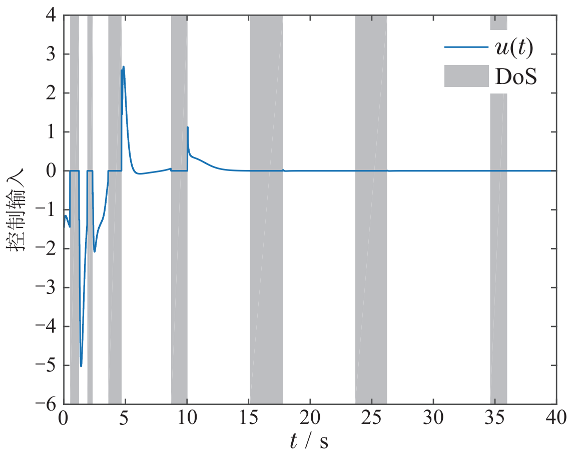

图 4 在DoS攻击下系统的控制输入

Fig. 4 The control input of system (29) under DoS attacks

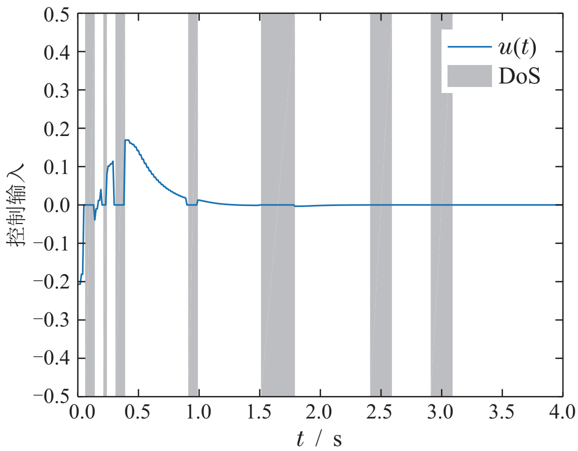

图 7 在DoS攻击下系统的控制输入

Fig. 7 The control input of system (30) under DoS attacks

初始条件选取为$x(0) = [0.6 \quad -0.5]^{\mathrm{T}}$, $\hat{x}(0) = [0.6 \quad 0]^{\mathrm{T}}$. 由图7知, 在DoS攻击发生区间, 控制输入为零. 通过观察图5–6知, 即使在部分区间攻击阻断控制输入, 系统和误差系统仍旧是稳定的, 这就验证了所提出基于观测器的控制策略能够有效地抵制攻击的影响, 同时保证系统的稳态.

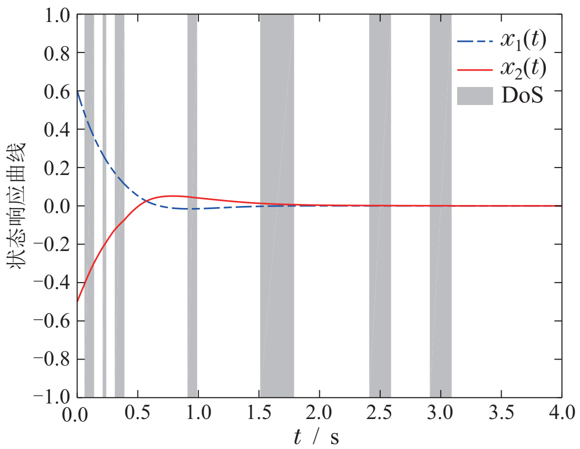

图 5 在DoS攻击下系统(30)的状态

Fig. 5 The states of system (30) under DoS attacks

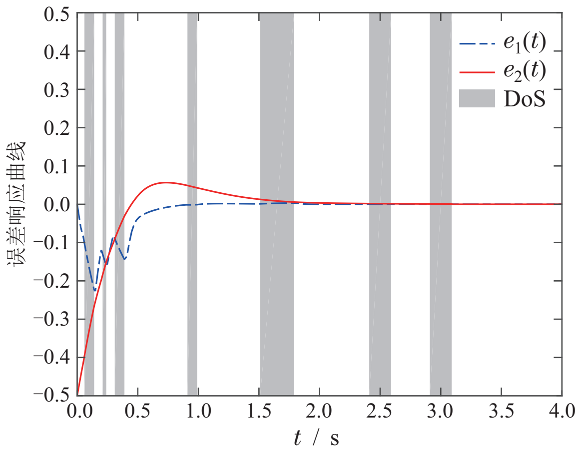

图 6 在DoS攻击下误差系统的状态

Fig. 6 The states of the error system under DoS attacks

5 结论

本文研究了非周期性DoS攻击下网络化时滞非线性系统的基于观测器的采样数据安全控制. 利用系统的间歇输出采样信息, 设计了依赖于攻击模式的观测器和控制器. 基于Lyapunov稳定定理, 给出了充分条件以确保在DoS攻击下系统是指数稳定的. 同时, 利用简单的矩阵变换, 给出了控制增益和观测增益共同设计的解决方案. 最后, 一个非平凡的数值例子和实际例子说明了所提出方法的有效性.

参考文献:

[1] LIU Shan, LI Shanbin, XU Bugong. Finite horizon H_∞ control for time-varying cyber-physical system under hybrid attacks. *Control Theory & Applications*, 2020, 37(2): 331 – 339.
(刘珊, 黎善斌, 胥布工. 混合攻击下时变信息物理系统的有限时域H_∞控制. 控制理论与应用, 2020, 37(2): 331 – 339.)

[2] HUANG Ling, GUO Jing, ZHANG Hengyan. Observer-based dynamic event triggering control for networked systems with periodic denial-of-service attack. *Control Theory & Applications*, 2021, 38(6): 851 – 861.
(黄玲, 郭婧, 张恒艳. 基于观测器的周期拒绝服务攻击网络化系统动态事件触发控制. 控制理论与应用, 2021, 38(6): 851 – 861.)

[3] AMIN S, SCHWART G A, SASTRY S S. Security of interdependent and identical networked control systems. *Automatica*, 2013, 49(1): 186 – 192.

[4] SANDBERG H, AMIN S, JOHANSSON K H. Cyber-physical security in networked control systems: an introduction to the issue, *IEEE Control Systems Magazine*, 2015, 35(1): 20 – 23.

[5] AOUFI S, DERNHAB A, GUERROUMI M. Survey of false data injection in smart power grid: attacks, countermeasures and challenges. *Journal of Information Security and Applications*, 2020, 54: 102518.

[6] AMIN S, CARDENAS A A, SASTRY S S. Safe and secure networked control systems under denial-of-service attacks. *International Workshop on Hybrid Systems: Computation and Control*. Berlin, Heidelberg, Springer, 2009.

[7] FOROUSH H S, MARTINEZ S. On triggering control of single-input linear systems under pulse-width modulated DoS signals. *SIAM Journal on Control and Optimization*, 2016, 54(6): 3084 – 3105.

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

[9] LU A Y, YANG G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. *IEEE Transaction on Automatic Control*, 2018, 63(6): 1813 – 1820.

[10] ZHAO N, SHI P, XING W, et al. Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks. *IEEE Transactions on Control of Network Systems*, 2020, 8(1): 158 – 167.

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

[12] QIAN C, DU H. Global output feedback stabilization of a class of nonlinear systems via linear sampled-data control. *IEEE Transactions on Automatic Control*, 2012, 57(11): 2934 – 2939.

[13] SUN G, XU S, LI Z. Finite-time fuzzy sampled-data control for nonlinear flexible spacecraft with stochastic actuator failures. *IEEE Transactions on Industrial Electronics*, 2017, 64(5): 3851 – 3861.

[14] YUAN Y, YU Y, WANG Z, et al. A sampled-data approach to nonlinear ESO-based active disturbance rejection control for pneumatic muscle actuator systems with actuator saturations. *IEEE Transactions on Industrial Electronics*, 2019, 66(6): 4608 – 4617.

[15] LI S, AHN C K, XIANG Z R. Decentralized sampled-data control for cyber-physical systems subject to DoS attacks. *IEEE Systems Journal*, 2021, 15(4): 5126 – 5134.

[16] ZHANG X, CHENG Z. Global stabilization of a class of time-delay nonlinear systems. *International Journal of Systems Science*, 2005, 36(8): 461 – 468.

[17] BENABDALLAH A, ECHI N. Global exponential stabilisation of a class of nonlinear time-delay systems. *International Journal of Systems Science*, 2016, 47(16): 3857 – 3863.

[18] ZHAI J. Dynamic output-feedback control for nonlinear time-delay systems and applications to chemical reactor systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2019, 66(11): 1845 – 1849.

作者简介:

赵　宁　博士研究生, 目前研究方向为网络化系统的安全控制, E-mail: zhaoning_hrbeu@163.com;

刘永超　讲师, 目前研究方向为非线性系统自适应控制, E-mail: sdliuyc@163.com.