DOI: 10.13382/j.jemi.B1902497

事件触发网络化控制系统在攻击下的稳定性分析*

申玉斌[1] 费敏锐[2]
(1.河南牧业经济学院 信息工程学院 郑州 450044; 2.上海大学 机电工程与自动化学院 上海 200444)

摘 要:以存在网络延迟的 NCSs 为研究对象,结合事件触发机制,研究遭受拒绝服务攻击(DoS)的 NCSs 稳定性问题。在 DoS 攻击过程中,NCSs 的传感器无法接收测量信息或者执行器无法获取控制信息,会存在不稳定的子系统。为了提高 NCSs 的稳定性,首先,把存在网络时延和 DoS 攻击的 NCSs 系统建模成包含稳定子系统和不稳定子系统的闭环切换系统模型;接着,基于切换系统分析方法,得到该系统指数稳定的充分条件;进一步,分析 DoS 攻击的时间比率,只要 DoS 攻击时间比例在有效范围,不论 DoS 攻击如何作用于系统,总能保证该系统的指数稳定性。实验结果表明,当 $0<\delta<3$ 时,网络控制系统能获得相应的指数稳定性,验证了此方法在 DoS 攻击下,具有事件触发机制 NCSs 稳定的有效性。

关键词: DoS 攻击;网络化控制系统;事件触发;安全性;指数稳定性;Wirtinger 不等式
中图分类号: TP273.3 **文献标识码**:A **国家标准学科分类代码**: 510.8010

Stability analysis of event-triggered networked control systems under attack

Shen Yubin[1] Fei Minrui[2]
(1.School of Information Engineering, Henan University of Animal Husbandry and Economy, Zhengzhou 450044, China;
2.School of Mechatronics Engineering and Automation, Shanghai University, Shanghai 200444, China)

Abstract: This paper takes networked control systems (NCSs) with network-induced delay as the research object, combined with the event-triggered mechanism, which studies the stability of NCSs under denial of service (DoS) attacks. In the process of DoS attacks, the sensor of NCSs cannot receive the measurement information in time, or the actuator cannot get the control information, then there will be unstable subsystems. In order to improve the stability of NCSs, firstly, NCSs is modeled as a closed-loop switched system with both stable subsystems and unstable subsystems. The model can handle of network-induced delay and DoS attacks uniformly. Then, based on the analysis method of the switched system, a sufficient condition is derived from the concerned NCSs to be exponentially stable. Furthermore, the time ratio of the DoS attack is also analyzed, the concerned NCSs is always guaranteed to be exponentially stable, as long as the occurring probability of DoS attacks is in the effective range. Finally, the experimental results show that NCSs can obtain the corresponding exponential stability for $0<\delta<3$; the stability of NCSs with event-triggered mechanism under the DoS attack is given to show the effectiveness of the proposed result.

Keywords: denial of service (DoS) attacks; networked control systems (NCSs); event-triggered; security; exponential stability; Wirtinger-based inequality

0 引 言

网络化控制系统的安全性在近年来受到了广泛的关注。尽管网络化控制系统[1-4]的开放通信连接对聚集远程系统信息和本地信息更加便利,但是当网络攻击成为一种常见的网络问题时,实际的物理通信通道在数据传输时将会变得不太可靠,无论从理论上还是工程实践的角度上,网络化控制系统中的安全性逐渐成为亟待解决的重要问题。网络化控制系统安全性的威胁主要来自于

收稿日期: 2019-08-22 Received Date: 2019-08-22
*基金项目:国家自然科学基金(61633016)资助项目

一些恶意的对手或者团体。破坏安全性的 3 种攻击行为比较常见,分别是拒绝服务攻击(denial of service, DoS)、数据入侵攻击和欺骗攻击。而对于数据包传递危害最严重的攻击之一就是 DoS 攻击。恶意 DoS 攻击能发送大量的虚假信息,形成一个数据洪流发往网络化控制系统中的目标节点,进而大量消耗连接目标节点的网络带宽资源,从而形成网络中断[5]。在 DoS 攻击的情况下,网络设备很难传送满足事件触发策略的采样数据包[6-10]。

最近几年各国学者的研究发现[11-13],恶意的 DoS 攻击会使网络化控制系统越来越脆弱。为了提高网络化控制系统的稳定性,通过事件触发控制方法[14-16]以及优化控制方法[17]能进一步保证系统的稳定性。文献[18-19]攻击者和数据传输者之间使用随机博弈论的方法,对 DoS 攻击提出一种优化防御机制,但忽略了 DoS 攻击与控制系统性能之间的权衡问题;文献[20]当控制系统的采样数据被随机攻击时,通过测量传输方法和有限维动态系统控制策略的优化得到最优测量数据,但容易误将网络中突发数据流当作攻击进行处理;文献[21-22]当控制和测量数据包通过网络传输被恶意攻击时,可以使用安全约束优化控制,但需要数据采样速率与包传输速率相匹配;文献[23-24]系统地描述低比率 DoS 攻击对于反馈控制系统的影响,并提出新的控制机制,但忽略了 DoS 攻击给系统建模带来的影响;文献[25]提出一种 DoS 攻击的防御技术,针对分布式 DoS 攻击洪流给网络化控制系统提供有效保护,但是忽略了 DoS 攻击的效能分析。

针对恶意 DoS 攻击如何设计最大容忍程度参数,使网络化控制系统的性能在 DoS 攻击影响中辨识出来,将成为一个需要解决的问题,如何对存在网络时变延迟和 DoS 攻击的网络环境中保证网络化控制系统的指数稳定性非常重要。在本文中,假设当发生 DoS 攻击时,意味着攻击时段内网络中断,并且系统得不到更新的控制信息将失去稳定性。存在网络时变延迟的网络化控制系统中保证指数稳定性,需要考虑 DoS 攻击时间区间与无攻击系统运行时间区间比率关系。基于以上分析,本文在 DoS 攻击下,首先将事件触发网络化控制系统转换为一类时变延迟切换系统;之后,根据延迟系统属性构造了特殊的 Lyapunov-Krasovskii 函数,用于 DoS 攻击下事件触发闭环网络化控制系统的指数稳定性的判定,通过分析适当的攻击时间比例关系,获得较好的稳定性效果。通过 DoS 攻击下网络化控制系统的示例,说明以上方法的有效性。

1 问题阐述

网络化控制系统结构示意如图 1 所示。

网络化控制系统模型如下:

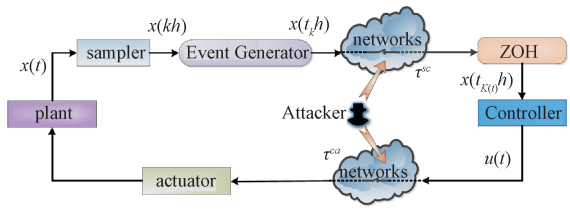


图 1 DoS 攻击下事件触发的闭环系统框架

Fig.1 The framework of the closed-loop system with event-triggered sampling under DoS attacks

$$\begin{aligned}\dot{\boldsymbol{x}}(t)&=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t)+\boldsymbol{B}_{\omega}\boldsymbol{\omega}(t)\\ \boldsymbol{z}(t)&=\boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{D}\boldsymbol{u}(t)\end{aligned}\tag{1}$$

式中:$\boldsymbol{x}(t)\in\boldsymbol{R}^n$ 是系统状态向量;$u(t)\in\boldsymbol{R}^m$ 是控制输入向量;$\boldsymbol{\omega}(t)\in L_2[0,\infty)$ 是外部干扰输入向量;$\boldsymbol{z}(t)\in\boldsymbol{R}^p$ 是控制输出向量。$x(0)\in\boldsymbol{R}^n$ 是初始状态,$\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{B}_{\omega}$、$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 是已知具有适当维数的固定矩阵。

1.1 事件触发数据传输协议

本文系统模型(1)中状态反馈控制具有的形式为 $\boldsymbol{u}(t)=\boldsymbol{K}\boldsymbol{x}(t)$,$\boldsymbol{K}$ 是控制器增益。由事件触发策略决定的数据包在没有 DoS 攻击的情况下,通过网络发送到 ZOH 中,然后传递给控制器。考虑网络诱导延时 τ_{t_k} 的影响,ZOH 输出可看做为 $\bar{\boldsymbol{x}}(t)=\boldsymbol{x}(t_kh)$,控制器在时刻 $t_kh+\tau_{t_k}$ 收到状态数据 $\bar{\boldsymbol{x}}(t)$。此外,ZOH 将一直保持信号 $\bar{\boldsymbol{x}}(t)$,直到下一个更新数据到达。

$$\boldsymbol{u}(t)=\boldsymbol{K}\boldsymbol{x}(t)=\boldsymbol{K}\bar{\boldsymbol{x}}(t),t_kh\leqslant t<t_{k+1}h,k\in N\tag{2}$$

对于 $\tau_m=min_{t_k\in N}\{\tau_{t_k}\}>0$ 和 $\tau_M=max_{t_k\in N}\{\tau_{t_k}\}$,以下不等式成立,$\tau_{t_k}$ 是有界的,且有 $\tau_{t_k}=\tau_{t_k}^{sc}+\tau_{t_k}^{ca}$,$\tau_m\leqslant\tau_{t_k}\leqslant\tau_M$。$t_k$ 之后下一个释放采样数据的时刻根据如下通信策略来决定:

$$\begin{aligned}t_{k+1}h=\min\{&t_kh+ih\mid i\in N,(\boldsymbol{x}(t_kh+ih)-\\&\boldsymbol{x}(t_kh))^{\mathrm{T}}\boldsymbol{\Phi}(x(t_kh+ih)-\boldsymbol{x}(t_kh)))>\\&\sigma\boldsymbol{x}(t_kh+ih)^{\mathrm{T}}\boldsymbol{\Phi}\boldsymbol{x}(t_kh+ih)\}\end{aligned}\tag{3}$$

对于 $\boldsymbol{e}_k(t)=\boldsymbol{x}(t_kh)-\boldsymbol{x}(t_kh+ih)$ 是最后成功传输时刻与当前实时采样时刻的状态误差。能得到如下的事件触发策略描述:

$$\boldsymbol{e}_k^{\mathrm{T}}(t)\boldsymbol{\Phi}\boldsymbol{e}_k(t)\leqslant\sigma\boldsymbol{x}^{\mathrm{T}}(t_kh+ih)\boldsymbol{\Phi}\boldsymbol{x}(t_kh+ih)\tag{4}$$

当状态误差值满足条件(4)时,采样数据不发送,当不满足条件(4)时,即需要发送数据。传感器到控制器的传输通道由网络来实现,在没有受到 DoS 攻击的情况下,当事件触发条件(4)不成立时会存在这样的时间序列 $\{t_k\}_{k\in N_0}=\{t_0,t_1,\cdots\}$,说明这些时刻的采样数据需要通过网络发送给控制器。同时,假设事件触发的周期是 T,则有 $t_{k+1}h-t_kh=\mathrm{T}$,$k\in N_0$。因此在此系统中不会出现芝诺现象,因为当使用 $h\in N_{>0}$,由于时间标准化的措施,下一个事件触发的时刻为 $t_{k+1}h=t_kh+ih$,则 $T\geqslant h>0$。

1.2　DoS 攻击的实际活动

DoS 攻击作为一种攻击现象，能分别影响测量和控制通道的信号传输，在 DoS 攻击出现时，满足发送条件的采样数据既不能发送也不能接收。通过图 2 所示可知，DoS 攻击的目的是阻止有效数据信息的传输。

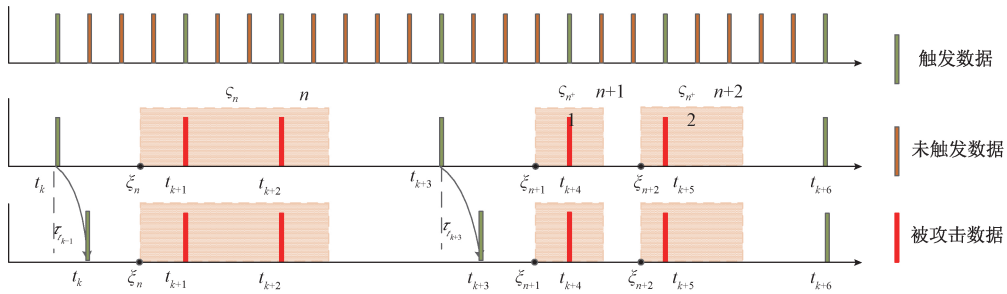


图 2　给定 DoS 攻击模式的示例

Fig.2　Exemplifies for a given DoS pattern

在 DoS 攻击情况下，由控制器根据最近一次成功接收的传输数据产生控制信号，实现对系统的控制操作。第 n 个 DoS 攻击时间区间可以表示为 $D_n = \{\xi_n\} \cup [\xi_n, \xi_n + \zeta_n]$。$\xi_n$ 是网络传输环境中第 n 个 DoS 攻击出现的时刻，ζ_n 是第 n 个 DoS 攻击时间区间的持续时间长度。如果 $\zeta_n = \infty$，则网络不能实现传输，即网络化控制系统将成为开环系统。当 $\zeta_n = 0$，则第 n 个 DoS 攻击在时刻 ξ_n 形成了单脉冲。

可以将整个系统运行时间看做 $\aleph(t_0,t)$，同时将其划分为 $\aleph_S(t_0,t)$ 和 $\aleph_D(t_0,t)$ 两部分，$\aleph_S(t_0,t)$ 表示网络可以通信的时间区间集合，$\aleph_D(t_0,t)$ 表示不能通信的时间区间集合，则有 $\aleph(t_0,t) = \aleph_S(t_0,t) \cup \aleph_D(t_0,t)$。

给定 $t_0, t \in N_0$，要求有 $t \geqslant t_0$，从而可知不能通信时间区间为 $\aleph_D(t_0,t) = \bigcup_{n\in N} D_n \cap [t_0,t]$，可以通信的时间区间为 $\aleph_S(t_0,t) = \aleph(t_0,t) \setminus \aleph_D(t_0,t)$。在系统整个运行时间 $[t_0,t)$ 中，没有 DoS 攻击的时间区间总长度的值设为 $|\aleph_S(t_0,t)|$，对于存在 DoS 攻击的时间总长度的值设为 $|\aleph_D(t_0,t)|$。因此有：$|\aleph_S(t_0,t)| + |\aleph_D(t_0,t)| = t - t_0$。

网络化控制系统中，存在 DoS 攻击时，当前时刻 t 之前可能会随机出现多个时长不定的 DoS 攻击，设置 $n(t)$ 作为当前时间 t 之前 DoS 攻击次数：

$$n(t) = \begin{cases} -1, t < h_0 \\ \sup\{n \in N \mid \xi_n < t\}, \text{其他} \end{cases} \tag{5}$$

因此，在整个系统运行时间 $[t_0,t)$ 中，DoS 攻击时间区间可得：

$$\aleph_D(t_0,t) = \{\bigcup_{n=0}^{n(t)-1} D_n\} \cup [\xi_{n(t)}, \min\{\xi_{n(t)} + \zeta_{n(t)}, t\}] \tag{6}$$

同时，为了后续的定理使用，需要如下的定义。

定义 1　存在定值 $\delta \geqslant 0$，用于表示以下不等式关系：

$$\frac{|\aleph_D(t_0,t)|}{|\aleph_S(t_0,t)|} \leqslant \delta, \forall t \in N_{\geqslant 0} \tag{7}$$

定义 2　存在定值 $\vartheta \in N_{\geqslant 0}$ 和 $\tau_D \in N_{\geqslant T}$，有以下不等式成立：

$$n(t_0,t) \leqslant \vartheta + \frac{t - t_0}{\tau_D} \tag{8}$$

对于所有的 $t_0, t \in N_{\geqslant 0}$，同时，$t \geqslant t_0$。

定义 3　系统(1)的初始值可使系统指数稳定，如果这里存在 $\theta > 0$ 和 $M \geqslant 0$，对于任何初始数据值 $x_{t_0} = \phi$，有：

$$\| \boldsymbol{x}(t,t_0,\phi) \| \leqslant M \| \phi \|_{\iota} e^{-\theta(t-t_0)} \tag{9}$$

其中，$(t_0,\phi) \in N^+ \times PC([-\iota,0], N^n)$，$\theta$ 是指数收敛率。

1.3　闭环网络化控制系统模型

从图 2 可以发现，时间轴被划分为多个区间，在这些时间区间中由事件触发策略(4)决定的数据可以被发送到控制器，但是由于 DoS 攻击的存在，其中一些数据虽然由事件触发策略决定，但是却不能发送到控制器。闭环动态系统根据系统所处时间区间的不同被分为稳定与不稳定的切换系统模式。

基于以上的分析，控制系统的实际控制输入可表述为 $\boldsymbol{u}(t) = K\boldsymbol{x}(t_{k(t)}h)$。本文 $t_{k(t)}$ 做为系统最近成功更新的时刻，其中：

$$k(t) = \sup\{k \in N \mid t_k \notin \aleph_D(t_0,t)\}$$

当 $k(0) = -1$ 时，表示控制输入这个时刻不能通过通信通道作用于系统的起始时刻，因此 $\boldsymbol{x}(t_{-1}) := 0$。闭环控制系统(1)可以重写为：

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}K\boldsymbol{x}(t_{k(t)}h) + \boldsymbol{B}_\omega\boldsymbol{\omega}(t) \\ \boldsymbol{z}(t) &= \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{D}K\boldsymbol{x}(t_{k(t)}h) \end{aligned} \tag{10}$$

2 主要结果

使用平均驻留时间方法对网络化控制系统的指数稳定性条件进行分析。

定理 对于系统(10),给定定值 $a_1 > 0, a_2 > 0$, $\tau_D > 0, \eta_1 > 0$ 和 $\eta_2 > 0$,以及任意值 ϑ,如果存在矩阵 $\boldsymbol{P}_i$、$\boldsymbol{Q}_j$、$\boldsymbol{R}_j$ 和 $\boldsymbol{Z}_k (i = 1,2; j = 1,2,3,4; k = 1,2,3,4,5,6)$,对于以下线性矩阵不等式成立。

$$\boldsymbol{\Pi}_1 = \begin{bmatrix} \overline{\Psi} & * & * & * \\ \eta_1 R_1 \Gamma_1 & -R_1 & * & * \\ (\eta_2 - \eta_1) R_2 \Gamma_1 & 0 & -R_2 & * \\ \eta_2 Z_1 \Gamma_1 & 0 & 0 & -Z_1 \end{bmatrix} < 0,$$

$$\boldsymbol{\Pi}_2 = \begin{bmatrix} \widehat{\Psi} & * & * & * \\ \eta_1 R_3 \Gamma_2 & -R_3 & * & * \\ (\eta_2 - \eta_1) R_4 \Gamma_2 & 0 & -R_4 & * \\ \eta_2 Z_4 \Gamma_2 & 0 & 0 & -Z_4 \end{bmatrix} < 0$$

系统(10)是指数稳定并且有不等式成立 $\| \boldsymbol{x}(t) \| \leqslant H \| \boldsymbol{x}(t_0) \| e^{-G(t-t_0)}$, 存在 $H = \left(\frac{\beta}{\alpha}\rho^{\vartheta}\right)^{\frac{1}{2}}$, $G = \frac{1}{2}\left[\frac{(2a_1 - 2a_2\delta)}{1+\delta} - \frac{\ln\rho}{\tau_D}\right]$, $\alpha = \lambda_{\min\limits_{i=1,2}}(\boldsymbol{P}_i)$, $\beta = \lambda_{\max}(P_1) + \eta_1[\lambda_{\max}(Q_1) - \lambda_{\max}(Q_2)] + \eta_2[\lambda_{\max}(Q_2) + \frac{\pi^2}{4}\lambda_{\max}(Z_2) + \lambda_{\max}(Z_3)] + \frac{\eta_1^2}{2}\lambda_{\max}(R_1) + \frac{(\eta_2 - \eta_1)^2(\eta_2 + \eta_1)}{2} \cdot \lambda_{\max}(R_2) + \eta_2^3\lambda_{\max}(Z_1)$。

对于 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的比值 δ,满足以下的条件:$\delta < \frac{2a_1\tau_D - \ln\rho}{2a_2\tau_D + \ln\rho}$,其中,$\rho \geqslant 1$,同时有 $\boldsymbol{P}_i \leqslant \rho\boldsymbol{P}_j$, $\boldsymbol{Q}_m \leqslant \rho\boldsymbol{Q}_n, \boldsymbol{R}_m \leqslant \rho\boldsymbol{R}_n, \boldsymbol{Z}_p \leqslant \rho\boldsymbol{Z}_q, (i,j = 1,2; m,n = 1,2,3,4; p,q = 1,2,3,4,5,6)$。

证明:对于系统(10),当系统运行时间 $t \in \aleph(t_0,t)$,由于存在 $\aleph_S(t_0,t)$ 和 $\aleph_D(t_0,t)$ 区间集合,系统状态会在不同的时间区间集合中发生切换,设不同区间对应的 Lyapunov-Krasovskii 函数满足式(11)和式(12)。

$$V_1(t) = \boldsymbol{x}^{\mathrm{T}}(t)P_1\boldsymbol{x}(t) + \int_{t-\eta_1}^{t} e^{2a_1(v-t)}\boldsymbol{x}^{\mathrm{T}}(v)Q_1\boldsymbol{x}(v)\mathrm{d}v + \int_{t-\eta_2}^{t-\eta_1} e^{2a_1(v-t)}\boldsymbol{x}^{\mathrm{T}}(v)Q_2\boldsymbol{x}(v)\mathrm{d}v + \int_{t_{k(t)}h}^{t} e^{2a_1(v-t)}\boldsymbol{x}^{\mathrm{T}}(v)Z_3\boldsymbol{x}(v)\mathrm{d}v + (\eta_2 - \eta_1)\int_{-\eta_2}^{-\eta_1}\int_{t+u}^{t} e^{2a_1(v-t)}\dot{\boldsymbol{x}}^{\mathrm{T}}(v)R_2\dot{\boldsymbol{x}}(v)\mathrm{d}v\mathrm{d}u - \frac{\pi^2}{4}\int_{t_{k(t)}h}^{t} e^{2a_1(v-t)}[\boldsymbol{x}(v) - \boldsymbol{x}(t_{k(t)}h)]^{\mathrm{T}}Z_2[\boldsymbol{x}(v) - \boldsymbol{x}(t_{k(t)}h)]\mathrm{d}v + \eta_2^2\int_{t_{k(t)}h}^{t} e^{2a_1(v-t)}\dot{\boldsymbol{x}}^{\mathrm{T}}(v)Z_1\dot{x}(v)\mathrm{d}v + \int_{-\eta_1}^{0}\int_{t+u}^{t} e^{2a_1(v-t)}\dot{\boldsymbol{x}}^{\mathrm{T}}(v)R_1\dot{\boldsymbol{x}}(v)\mathrm{d}v\mathrm{d}u \tag{11}$$

$$V_2(t) = \boldsymbol{x}^{\mathrm{T}}(t)P_2\boldsymbol{x}(t) + \int_{t-\eta_1}^{t} e^{2a_2(t-v)}\boldsymbol{x}^{\mathrm{T}}(v)Q_3x(v)\mathrm{d}v + \int_{t-\eta_2}^{t-\eta_1} e^{2a_2(t-v)}\boldsymbol{x}^{\mathrm{T}}(v)Q_4\boldsymbol{x}(v)\mathrm{d}v + \int_{t_{k(t)}h}^{t} e^{2a_2(t-v)}\boldsymbol{x}^{\mathrm{T}}(v)Z_6\boldsymbol{x}(v)\mathrm{d}v + \eta_1\int_{-\eta_1}^{0}\int_{t+u}^{t} e^{2a_2(t-v)}\dot{\boldsymbol{x}}^{\mathrm{T}}(v)R_3\dot{\boldsymbol{x}}(v)\mathrm{d}v\mathrm{d}u + (\eta_2 - \eta_1)\int_{-\eta_2}^{-\eta_1}\int_{t+u}^{t} e^{2a_2(t-v)}\dot{\boldsymbol{x}}^{\mathrm{T}}(v)R_4\dot{x}(v)\mathrm{d}v\mathrm{d}u + \eta_2^2\int_{t_{k(t)}h}^{t} e^{2a_2(t-v)}\dot{\boldsymbol{x}}^{T}(v)Z_4\dot{\boldsymbol{x}}(v)\mathrm{d}v - \frac{\pi^2}{4}\int_{t_{k(t)}h}^{t} e^{2a_2(t-v)}[\boldsymbol{x}(v) - \boldsymbol{x}(t_{k(t)}h)]^{\mathrm{T}}Z_5[\boldsymbol{x}(v) - \boldsymbol{x}(t_{k(t)}h)]\mathrm{d}v \tag{12}$$

其中,$V_1(t) \leqslant \rho V_2(t)$,在 $t \in \aleph(t_0,t)$ 条件中,可得:

$$V(t) \leqslant \rho^{n(t_0,t)} e^{-2a_1|\aleph_S(t_0,t)| + 2a_2|\aleph_D(t_0,t)|} V_1(t_0) \tag{13}$$

根据定义 1 可知,$|\aleph_D(t_0,t)| \leqslant \delta|\aleph_S(t_0,t)|$,由于 $|\aleph_S(t_0,t)| + |\aleph_D(t_0,t)| = t - t_0$,则有 $t - t_0 \leqslant (1+\delta)|\aleph_S(t_0,t)|$。可得 $|\aleph_S(t_0,t)| \geqslant \frac{t-t_0}{1+\delta}$,由式(13),根据指数稳定性的要求,则有:

$$-2a_1|\aleph_S(t_0,t)| + 2a_2|\aleph_D(t_0,t)| \leqslant -\frac{(2a_1 - 2a_2\delta)}{1+\delta}(t - t_0) \tag{14}$$

结合(8)和式(13),可知:

$$V(t) \leqslant \rho^{\vartheta + \frac{t-t_0}{\tau_D}} e^{-\frac{(2a_1 - 2a_2\delta)}{1+\delta}(t-t_0)} V_1(t_0) = \rho^{\vartheta} e^{-\left[\frac{(2a_1 - 2a_2\delta)}{1+\delta} - \frac{\ln\rho}{\tau_D}\right](t-t_0)} V_1(t_0) \tag{15}$$

基于指数稳定性的要求,可得 $\frac{(2a_1 - 2a_2\delta)}{1+\delta} - \frac{\ln\rho}{\tau_D} > 0$,则有 $\delta < \frac{2a_1\tau_D - \ln\rho}{2a_2\tau_D + \ln\rho}$。

由于 $\alpha \| \boldsymbol{x}(t) \|^2 \leqslant V(t), V_1(t_0) \leqslant \beta \| \boldsymbol{x}(t_0) \|^2$,结合式(15)可得:

$$\| \boldsymbol{x}(t) \|^2 \leqslant \frac{\beta}{\alpha}\rho^{\vartheta} e^{-\left[\frac{(2a_1 - 2a_2\beta)}{1+\delta} - \frac{\ln\rho}{\tau_D}\right](t-t_0)} \| x(t_0) \|^2$$

即定理的条件所得。根据定义 3,可知系统(10)是指数稳定的,完成证明。

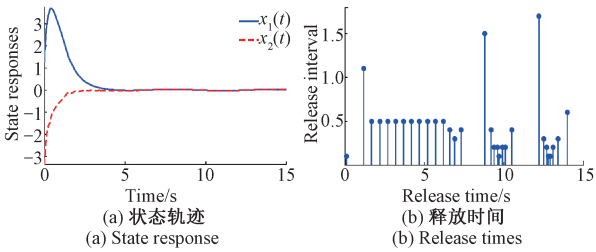
3 示例与仿真结果

在这一节,提供了数值示例,说明以上方法的有效性。对于网络化控制系统(1),给定如下参数:

$$\boldsymbol{A} = \begin{bmatrix} -1.8 & -5.8 \\ -2 & -5.6 \end{bmatrix}, \boldsymbol{B} = \begin{bmatrix} 1.5 \\ -8.6 \end{bmatrix}, \boldsymbol{B}_{\omega} = \begin{bmatrix} 0.2 \\ 0.2 \end{bmatrix},$$

$\boldsymbol{C}=[-1.4\quad -0.12]$，$\boldsymbol{D}=-0.054$，$w(t)=\begin{cases}sgn(sin(t)),t\in[0,15]\\0,\text{其他}\end{cases}$。同时给定的 $\eta_1=0.01$，$\eta_2=0.283$，采样周期 $h=0.1$ s，事件触发条件参数 $\sigma=0.25$ 和 $\boldsymbol{\Phi}=\begin{bmatrix}17.4944 & -17.3456\\-17.3456 & 17.3455\end{bmatrix}$，$H_\infty$ 参数 $\gamma=0.5$。

选择控制器增益 $\boldsymbol{K}=[-0.0769\quad 0.0763]$，根据初始值 $\boldsymbol{x}_0=[1.26\quad -3.53]^{\mathrm{T}}$ 来获得系统状态运行轨迹。从图 3(a)所示可以看到，在没有 DoS 攻击的时候，系统在事件触发策略(4)的作用下，通过有限采样数据的使用能够使系统在短时间内达到指数稳定性。

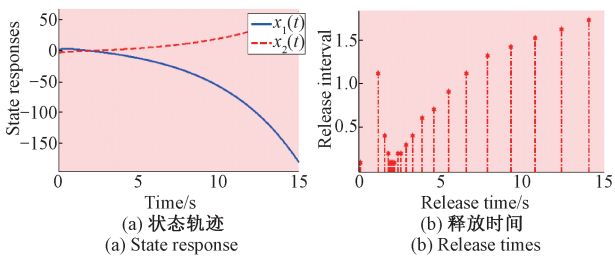


(a) 状态轨迹 (a) State response　(b) 释放时间 (b) Release times

图 3　没有 DoS 攻击时状态反映以及采样数据释放时间

Fig.3　The absence DoS of state response and release times of sample data

在图 4(a)所示可以看到，背景为淡红色的时间区域中，是 DoS 攻击活动的作用时间区间，系统状态运行曲线处于发散的状态，因为整个运行时间被 DoS 攻击的话，意味着网络化控制系统处于开环状态运行。从图 4(b)所示可以看到，红头虚线说明满足由事件触发策略决定的采样数据在 DoS 攻击的作用下不能通过网络发送到控制器。

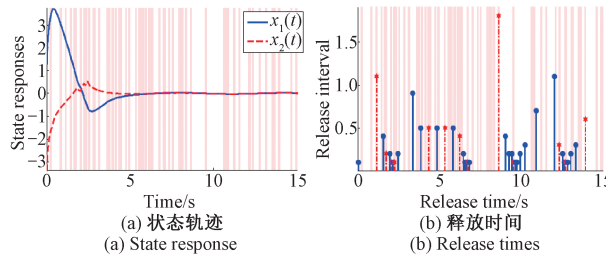


(a) 状态轨迹 (a) State response　(b) 释放时间 (b) Release times

图 4　DoS 攻击作用于整个运行时间

Fig.4　The presence of DoS with all time

根据定理 3 可知，当参数 $\delta\leqslant 0.5$ 时，意味着 DoS 攻击的时间长度 $|\aleph_D(t_0,t)|$ 不超过系统总运行时间长度 $|\aleph(t_0,t)|$ 的 $\frac{1}{3}$。系统(1)在此情况下存在着随机的恶意攻击，垂直淡红色条纹表示 DoS 攻击的活动时间区间。从图 5(b)所示可以看到，一些用虚线表示的无效事件触发数据，无法传输到控制器，但图 5(a)所示的系统运行状态依然保持指数稳定，这是因为有足够的有效事件触发数据能够通过网络成功传输到控制器，使系统达到稳定状态。

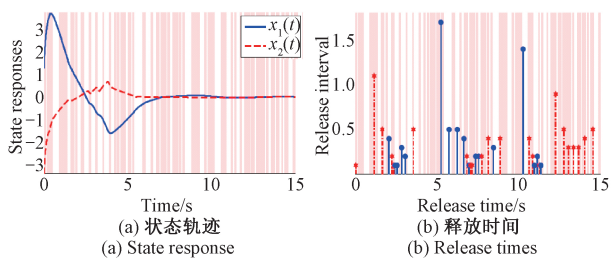


(a) 状态轨迹 (a) State response　(b) 释放时间 (b) Release times

图 5　DoS 攻击作用下 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的比值 $\leqslant 0.5$ 时状态和释放时间图

Fig.5　The presence of DoS with the rate of $\leqslant 0.5$ between $|\aleph_D(t_0,t)|$ and $|\aleph_S(t_0,t)|$

如果选择参数 $\delta=1$，即 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的时间值是相等的，从图 6(b)所示可以看出，会有采样数据虽然由事件触发策略(4)决定需要通过网络发送到控制器端，但是在 DoS 攻击的作用下被阻止。但是尽管阻止发送触发数据的时间与成功发送触发数据的时间相同，使用本文的设计方法，图 6(a)所示的系统状态仍然能在相对较短的时间内保持指数稳定性。



(a) 状态轨迹 (a) State response　(b) 释放时间 (b) Release times

图 6　DoS 攻击作用下 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的比值为 1 时状态和释放时间图

Fig.6　The presence of DoS with the rate of 1 between $|\aleph_D(t_0,t)|$ and $|\aleph_S(t_0,t)|$

当参数 $\delta\leqslant 2.45$ 时，存在更多的事件触发数据落在了时间区间集合 $\aleph_D(t_0,t)$ 中，在此区间的事件触发数据无法传输到控制器。从图 7(b)所示可以看到，如果在时间区间集合 $\aleph_S(t_0,t)$ 中控制器收到了适量的事件触发数据，产生相应的控制信号，图 7(a)所示的系统状态在发生一段时间波动后，能够保持指数稳定状态。

当选择的参数比值 $\delta\leqslant 3$ 时，从图 8(b)所示可以看到，落在了时间区间集合 $\aleph_D(t_0,t)$ 中事件触发策略(4)决定的采样数据更多，控制器收到的有效数据将会大大减少，以至于不能产生更多的有效控制信号作用于系统，

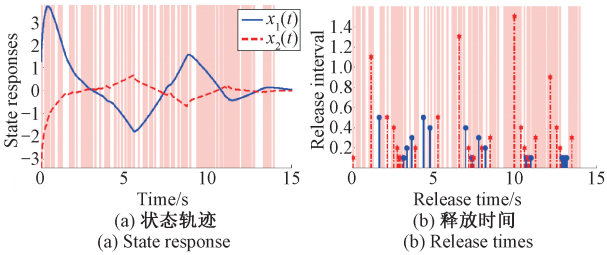


图 7 DoS 攻击作用下 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的比值≤2.45 时状态和释放时间图

Fig.7 The presence of DoS with the rate of ≤2.45 between $|\aleph_D(t_0,t)|$ and $|\aleph_S(t_0,t)|$

从图 8(a)所示可以看出,系统状态因此会失去稳定性。

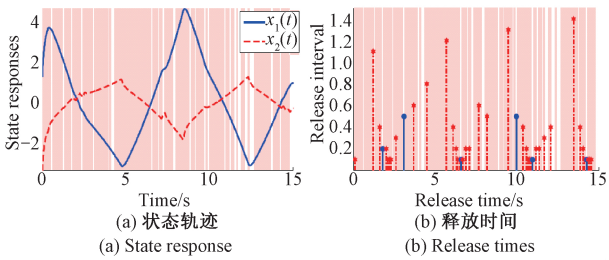


图 8 DoS 攻击作用下 $|\aleph_D(t_0,t)|$ 和 $|\aleph_S(t_0,t)|$ 的比值≤3 状态和释放时间图

Fig.8 The presence of DoS with the rate of ≤3 between $|\aleph_D(t_0,t)|$ and $|\aleph_S(t_0,t)|$

在本文设计的系统控制框架下,整个系统运行时间区间 $[t_0,t)$,对于随时可能发生的 DoS 攻击起始时刻和其有效时间区间 $\aleph_D(t_0,t)$ 可以是任意的,控制器不需要获得所有的事件触发策略(4)决定的采样数据,只要 DoS 攻击持续时间总长度值与没有攻击的总时间长度值满足一定的比例关系,即可以确保系统的指数稳定性。

4 结 论

在分析 DoS 攻击对事件触发网络化控制系统稳定性影响的基础上,考虑网络诱导延迟固有特性,利用切换系统理论与 Lyapunov 稳定性分析方法,得到网络化控制系统指数稳定性判定条件,并进一步分析恶意 DoS 攻击时间比例关系对系统稳定性的影响。通过仿真实验说明发生 DoS 攻击的网络化控制环境下本文方法的有效性。

参考文献

[1] ZHANG L, GAO H, KAYNAK O. Network-induced constraints in networked control systems: A survey[J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 403-416.

[2] YUAN Y, SUN F. Data fusion-based resilient control system under DoS attacks: A game theoretic approach [J]. International Journal of Control, Automation, and Systems, 2015, 13(3): 513-520.

[3] 张浩, 彭晨, 孙洪涛. 多路径的无线网络化控制系统镇定性研究[J]. 电子测量与仪器学报, 2016, 30(11): 1627-1634.
ZHANG H, PENG CH, SUN H T. Stabilization analysis of wireless networked control system with multi-path channels[J]. Journal of Electronic Measurement and Instrumentation, 2016, 30(11): 1627-1634.

[4] 方辉, 程权成. 离散系统量化 H_∞ 控制器设计[J]. 国外电子测量技术, 2016, 35(10):12-15,20.
FANG H, CHENG Q CH. Design of H_∞ controller for discrete system with quantized measurements[J]. Foreign Electronic Measurement Technology, 2016, 35(10): 12-15,20.

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

[6] WANG Y, LU J, LI Z. Mixed H_2/H_∞ control for a class of nonlinear networked control systems[J]. International Journal of Control, Automation, and Systems, 2016, 14(3): 655-665.

[7] AHMADI A A, SALMASI F R. Observer-based reliable control for lipschitz nonlinear networked control systems with quadratic protocol [J]. International Journal of Control, Automation, and Systems, 2015, 13(3): 753-763.

[8] ZHOU L, WEI Y. Stability analysis of networked control systems based on Lp properties[J]. International Journal of Control, Automation, and Systems, 2015, 13(2): 390-397.

[9] 陈珍萍, 李德权, 黄友锐,等. 无线传感器网络混合触发一致性时间同步[J]. 仪器仪表学报, 2015, 36(10): 2193-2199.
CHEN ZH P, LI D Q, HUANG Y R, et al. Mixed-triggered consensus time synchronization for wireless sensor networks [J]. Chinese Journal of Scientific Instrument, 2015, 36(10): 2193-2199.

[10] 吴杰, 付敬奇. 网络化控制系统的事件触发与量化控制协同设计[J]. 电子测量技术, 2017, 40(5): 80-86.
WU J, FU J Q. Co-design of event-triggered scheme and quantization control in networked control system [J]. Electronic Measurement Technology, 2017, 40(5):

80-86.
[11] AMIN S, SCHWARTZ G A, SASTRY S S. Security of interdependent and identical networked control systems [J]. Automatica, 2013, 49(1): 186-192.
[12] WEERAKKODY S, SINOPOLI B. Detecting integrity attacks on control systems using a moving target approach[C]. IEEE Conference on Decision and Control, 2015: 5820-5826.
[13] TEIXEIRA A, SHAMES I, SANDBERG H. A secure control framework for resource-limited adversaries [J]. Automatica, 2015, 51(1): 135-148.
[14] CETINKAYA A, ISHII H, HAYAKAWA T. Event-triggered control over unreliable networks subject to jamming attacks[C]. IEEE Conference on Decision and Control, 2015: 4818-4823.
[15] SHISHEH H F, MARTINEZ S. On event-triggered control of linear systems under periodic denial-of-service jamming attacks[C]. IEEE Conference on Decision and Control, 2012: 2551-2556.
[16] SARKER J H, MOUFTAH H T. A self-stabilized random access protocol against denial of service attack in wireless networks [J]. Security & Communication Networks, 2011, 4(9): 1075-1087.
[17] SHOUKRY Y, TABUADA P. Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks [C]. IEEE Conference on Decision and Control, 2014: 3548-3522.
[18] LIU S, LIU P X, SADDIK A, et al. A stochastic game approach to the security issue of networked control systems under jamming attacks [J]. Journal of the Franklin Institute, 2014, 351(9): 4570-4583.
[19] CHEN L, LENEUTRE J. Fight jamming with jamming: A game theoretic analysis of jamming attack in wireless networks and defense strategy[J]. Computer Networks, 2011, 55(9): 2259-2270.
[20] BEFEKADU G V G, ANTSAKLIS P. Risk-sensitive control under a class of denial-of-service attack models [C]. Proceedings of the 2011 American Control Conference. IEEE, 2011: 643-648.
[21] CETINKAYA A, ISHII H, HAYAKAWA T. Networked control under random and malicious packet losses [J]. IEEE Transactions on Automatic Control, 2017, 62(5): 2434-2449.
[22] HAN G J, SHEN W, DUONG T Q. A proposed security scheme against denial of service attacks in cluster-based wireless sensor networks[J]. Security & Communication Networks, 2014, 7(12): 2542-2554.
[23] TANG Y, LUO X, HUI Q. Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 339-353.
[24] MANSOURI D, MOKDDAD L, BEN-OTHMAN J, et al. Preventing denial of service attacks in wireless sensor networks [C]. IEEE International Conference on Communications, 2015: 3014-3019.
[25] BEITOLLAHI H, DECONINCK G. A dependable architecture to mitigate distributed denial-of-service attacks in network-based control systems[J]. Journal of Critical Infrastructure Protection, 2011, 4(3): 107-123.

作者简介

申玉斌,2005 年于西南科技大学获得硕士学位,2018 年于上海大学获得博士学位,现为河南牧业经济学院讲师,主要研究方向为网络化控制系统、鲁棒控制、智能控制。
E-mail:shenyb616@ 163.com

Shen Yubin received his M. Sc. degree from Southwest University of Science and Technology in 2005, Ph.D. degree from Shanghai University in 2018. Now he is a lecturer at Henan University of Animal Husbandry and Economy. His main research interests include networked control system, robust control, intelligent control.

费敏锐,分别在 1984 年和 1992 年于上海工业大学获得学士学位与硕士学位,1997 年于上海大学获得博士学位。现为上海大学教授,博士生导师,主要研究方向为智能控制、复杂系统建模,网络化控制系统和现场控制系统。
E-mail:mrfei@ staff.shu.edu.cn

Fei Minrui received B. Sc. and M. Sc. from Shanghai University of Technology in 1984 and 1992, and Ph. D. from Shanghai University in 1997, respectively. Now he is a professor and Ph. D. supervisor at Shanghai University. His main research interests include intelligent control, complex system modeling, networked control systems, and field control systems.