DoS 攻击下无终端成分的数据驱动弹性预测控制

任清爽，陈 珺†，刘 飞

(江南大学 轻工过程先进控制教育部重点实验室，江苏 无锡 214122)

摘 要: 针对一种 DoS 攻击下的未知线性时不变系统, 提出一种无终端成分的弹性数据驱动预测控制算法. 首先, 所提出算法与传统的模型预测控制相比, 通过分析系统输入输出数据来学习系统的行为模式, 并仅依靠系统历史输入输出数据来预测未来的输入输出. 当 DoS 攻击发生时, 该方案能够利用预测控制的特性补偿由 DoS 攻击造成丢失的数据, 从而减少 DoS 攻击对系统的负面影响. 然后, 在考虑有界网络诱导噪声和过程噪声的情况下, 证明该方案能够保证系统的鲁棒稳定性. 最后, 通过数值仿真结果验证该方案的有效性和可行性, 实验结果表明该方案具有更强的鲁棒性和抗 DoS 攻击能力.

关键词: 数据驱动；DoS 攻击；预测控制；鲁棒控制；稳定性分析

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2024.1488

引用格式: 任清爽, 陈珺, 刘飞. DoS 攻击下无终端成分的数据驱动弹性预测控制 [J]. 控制与决策, 2025, 40(10): 3190-3200.

Data-driven resilient predictive control without terminal components under DoS attacks

REN Qing-shuang，*CHEN Jun*†，*LIU Fei*

(Key Laboratory of Advanced Process Control for Light Industry of Ministry of Education，Jiangnan University，Wuxi 214122，China)

Abstract: A resilient data-driven predictive control algorithm without terminal components is proposed for an unknown linear time-invariant system under DoS attacks. Compared with the traditional model predictive control, this paper learns the behavior pattern of the system by analyzing the input and output data of the system, and predicts the future input and output, only relying on the historical input and output data of the system. When DoS attacks occur, the scheme can use the characteristics of predictive control to compensate for the lost data caused by the DoS attack, thereby reducing the negative impact of the DoS attack on the system. Then we prove that the proposed scheme can guarantee the robust stability of the system considering bounded network induced noise and process noise. Finally, the effectiveness and feasibility of the scheme are verified by numerical simulation results. The experimental results show that the scheme has stronger robustness and anti-DoS attack ability.

Keywords: data-driven；DoS attacks；predictive control；robust control；stability analysis

0 引 言

信息物理融合系统 (CPS) 是信息科学与物理科学交叉融合的新型系统, 近年来发展迅速, 在智能制造[1]、智能交通[2]、智慧医疗 [3] 等多个领域得到了广泛应用, 显著提高了生产效率, 降低了运营成本, 并推动了资源的优化配置和可持续利用. 然而, 随着 CPS 应用范围的扩大, 其面临的网络攻击风险也日益增加[4]. 在网络攻击方式中, DoS 攻击尤为常见, 因为相较于其他类型的网络攻击, DoS 攻击较容易发起[5]. 攻击者可利用相对简单的工具和少量的资源对目标发起攻击. 在系统遭受 DoS 攻击后, 系统可能会处于离线或脆弱状态, 从而易受到其他形式的攻击, 如数据泄露、恶意软件植入等. 因此, 加强 CPS 的网络安全防护, 确保其稳定运行, 已成为当前亟待解决的问题[6].

除考虑 DoS 攻击带来的影响, CPS 的控制策略还需要考虑各种约束, 如对物理过程施加物理约束, 以保障操作的安全性和避免执行器过载. 作为处理

收稿日期: 2024-12-25；**录用日期:** 2025-04-01.
基金项目: 国家自然科学基金项目 (62073154).
责任编委: 侯忠生.
†通信作者. E-mail: chenjun1860@126.com.

约束最有效的控制方法之一, 模型预测控制 (MPC) 已被广泛应用于 DoS 攻击下系统控制问题中[7-9]. 相较于传统控制算法, MPC 采用先预测再控制的策略, 能够处理多变量的复杂系统, 并采用滚动优化策略及时弥补不确定性, 具有较强的鲁棒性、稳定性和抗干扰能力[10]. 另外, 利用 MPC 的预测特性能够在 DoS 攻击造成数据丢失时实现数据补偿, 从而提高控制的稳定性和可靠性.

随着大数据技术的发展, 现在正逐步从传统模型预测控制向数据驱动预测控制过渡. 上述针对 DoS 攻击的 MPC 算法需要建立精确的被控对象模型, 但是, 在 CPS 控制问题中, 由于系统的高度复杂性和不确定性, 以及外部干扰和攻击的存在, 很难建立完全符合实际的数学模型. 而数据驱动预测控制不依赖于精确的数学模型, 而是利用丰富的历史数据和先进的算法来预测系统行为并优化控制策略. 这一转变带来了诸多优点, 包括更高的灵活性, 更强的自适应能力以及对未知和时变系统特性的更好处理, 从而显著提升了控制系统的性能和效率. 根据文献 [11], 数据驱动方法大致可分为间接法和直接法: 间接法通常依赖于系统辨识, 即首先利用输入输出数据建立系统的数学模型, 然后基于该模型设计控制器, 这类方法虽然受益于基于模型的保证, 但是这种方法对数据要求较高, 且对于建模错误很敏感[12]; 而直接法则是直接利用输入输出数据来设计控制器, 如基于神经网络的数据驱动算法[13-15] 和基于系统行为学理论的数据驱动算法[16-18] 等. 其中: 基于神经网络的数据驱动算法需要大量的数据来训练策略, 在训练阶段需要较高的计算资源, 同时理论保证较弱, 稳定性难以严格证明; 而基于系统行为学理论的数据驱动算法可直接利用可用数据来实现控制目标, 同时能够提供严格的数学保证, 确保系统的稳定性和收敛性, 因此得到更为广泛的研究[19-22]. 文献 [19] 中引入终端约束证明了数据驱动 MPC 的鲁棒稳定性; 文献 [20] 则在文献 [19] 的基础上对不含任何终端成分的数据驱动 MPC 进行了稳定性分析, 从而减少了算法复杂度; 另外, 文献 [21] 提出了一种无终端成分的切换数据驱动预测控制方案; 文献 [22] 从减少资源消耗的角度提出了数据驱动自触发预测控制. 此外, 基于系统行为学的数据驱动算法也被成功应用于无人机[23] 和自动驾驶[24] 等实际应用中. 在 CPS 的安全控制问题中, 文献 [25] 将该类数据驱动 MPC 方法应用于针对 DoS 攻击的算法中, 提出了一种数据驱动弹性预测控制, 但是, 该算法的抗 DoS 攻击能力与预测时域长度相关, 当 DoS 攻击持续时间较长时无法达到较好的控制效果.

本文研究的目标是仅通过一些离线实验获得的输入输出系统轨迹使得系统保持稳定, 并减少 DoS 攻击对系统造成的负面影响, 同时, 分析 DoS 攻击持续时间和噪声大小对于鲁棒稳定性的影响, 并给出稳定性条件. 相比于文献 [25], 本文依靠足够长的预测时域而非终端成分来稳定线性时不变 (LTI) 系统, 能够减少算法复杂度; 同时, 利用一种补偿方法来补偿由 DoS 攻击造成丢失的数据, 该补偿方法与预测时域长度无关, 且能够降低更高强度的 DoS 攻击对系统造成的影响. 最后, 通过一个仿真例子来验证所提出方案具有更强的抗 DoS 攻击能力和鲁棒性.

1　问题描述

1.1　系统模型

考虑一个带过程噪声的离散 LTI 系统, 如下所示:

$$\mathcal{S}:\begin{cases} x_{t+1}=Ax_t+Bu_t+w_t,\\ y_t=Cx_t+Du_t, \end{cases} \tag{1}$$

其中$x_t\in\mathbb{R}^{n_x}$、$u_t\in\mathbb{R}^{n_u}$、$y_t\in\mathbb{R}^{n_y}$和$w_t\in\mathbb{R}^{n_x}$分别为系统的状态、控制输入、输出和过程噪声. 关于系统$\mathcal{S}$的一些假设如下.

假设 1　假设系统$\mathcal{S}$是一个未知 LTI 系统, 仅系统的输入输出轨迹$\{u_t^d,y_t^d\}_{t=0}^{N-1}$能够被收集.

假设 2　假设 LTI 系统$\mathcal{S}$的(A,B)满足能控性判据, (A,C)满足能观性判据.

利用系统$\mathcal{S}$的可观性性质, 存在一个常数$\eta\geqslant n_x$, 使得$\mathrm{rank}(\mathcal{O}_\eta)=n_x$, 其中$\mathcal{O}$为可观性矩阵, 即

$$\mathcal{O}_\eta=\begin{bmatrix} C\\ CA\\ \vdots\\ CA^{\eta-1}\end{bmatrix}. \tag{2}$$

由系统$\mathcal{S}$所构成的 CPS 系统如图 1 所示. 假设控制器到执行器 (C-A) 通道是理想的, 传感器到控制器 (S-C) 通道存在网络诱导噪声且会受到 Dos 攻

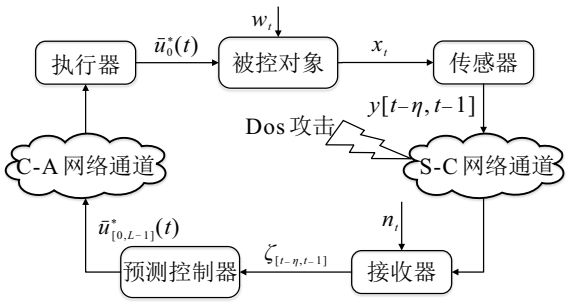


图1　网络控制系统结构

击. 在任一时刻t, 传感器会通过 S-C 通道发送包含前η时刻的输出测量值$y_{[t-\eta,t-1]}$, 在传输过程中, 数据会受到网络诱导噪声n_t的影响, 即当接收器接收到数据时, 有

$$\zeta_t = y_t + n_t. \tag{3}$$

假设 3 假设过程噪声w_t和网络诱导噪声n_t的边界是一个已知常数$\bar{v} := \max\{\|w_t\|, \|n_t\|\}, t \in \mathbb{N}_+$.

考虑系统$\mathcal{S}$在理想情况下的系统模型, 即无噪声情况下的状态空间表达为

$$\mathcal{S}_i : \begin{cases} \hat{x}_{t+1} = A\hat{x}_t + Bu_t, \\ \hat{y}_t = C\hat{x}_t + Du_t, \end{cases} \tag{4}$$

其中$\hat{x}_t$和$\hat{y}_t$记为不受过程噪音w_t干扰下的系统状态和系统输出. 定义如下 Hankel 矩阵:

$$H_L(z) := \begin{bmatrix} z_0 & z_1 & \cdots & z_{N-L} \\ z_1 & z_2 & \cdots & z_{N-L+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{L-1} & z_L & \cdots & z_{N-1} \end{bmatrix}.$$

定义 1[26] 对于一个序列$\{u_t\}_{t=0}^{N-1}$, $u_t \in \mathbb{R}^{n_u}$, 若$\mathrm{rank}(H_L(u)) = n_u L$, 则称$\{u_t\}_{t=0}^{N-1}$是$L$阶持续激励的.

引理 1[26] 假设$\{u_t^d, \hat{y}_t^d\}_{t=0}^{N-1}$为系统$\mathcal{S}_i$的一条输入输出轨迹, 且被测输入序列$\{u_t^d\}_{t=0}^{N-1}$是$L+n$阶持续激励的, 当且仅当存在实数向量$g \in \mathbb{R}^{N-L+1}$满足

$$\begin{bmatrix} H_L(u^d) \\ H_L(\hat{y}^d) \end{bmatrix} g = \begin{bmatrix} \bar{u}_t \\ \bar{y}_t \end{bmatrix}, \tag{5}$$

则轨迹$\{\bar{u}_t, \bar{y}_t\}_{t=0}^{L-1}$是该系统的一条轨迹.

1.2 DoS 攻击模型

DoS 攻击数学模型常用伯努利分布[27] 和马尔可夫链[28] 进行建模. 本文采用伯努利分布对 DoS 攻击建模, 通过调整伯努利分布的参数来模拟 DoS 攻击的不同强度和频率, 从而评估其对于系统的影响. 记$d_s(t)$为在t时刻是否发生 DoS 攻击的布尔型变量, 即

$$d_s(t) = \begin{cases} 1, \ \text{在}t\text{时刻发生DoS攻击;} \\ 0, \ \text{在}t\text{时刻未发生DoS攻击.} \end{cases} \tag{6}$$

其中$d_s(t)$服从伯努利分布, 满足

$$\mathbb{P}\{d_s(t) = 1\} = P_d, \tag{7}$$

$$\mathbb{P}\{d_s(t) = 0\} = 1 - P_d, \tag{8}$$

这里$P_d \in [0,1]$为发生 DoS 攻击的概率. 另外, 记上一次成功传输的时刻为t_s, 即$d_s(t_s) = 0$; 记$l := t - t_s$为 DoS 攻击直至当前时刻t的持续时间, $l \in \mathbb{N}$. 由于攻击者只能在网络通道上发起受有限能量限制的间歇性攻击, 给出如下假设.

假设 4 假设 DoS 攻击持续时间l最长不超过$\bar{l}$, 即$l \leqslant \bar{l}$, 其中$\bar{l} \in \mathbb{N}_+$.

2 控制器设计及稳定性分析

本节提出了一种 DoS 攻击下弹性数据驱动 MPC 方案, 并分析了噪声和 DoS 攻击持续时间对于系统鲁棒稳定性的影响.

2.1 弹性数据驱动 MPC

首先, 令L表示数据驱动 MPC 方案的预测时域步长. 控制器基于预先收集到的数据$\{u_t^d, y_t^d\}_{t=0}^{N-1}$和过去$\eta$步输入输出$\{u_{[t-\eta,t-1]}, \tilde{y}_{[-\eta,-1]}(t)\}$来预测未来$L$步的轨迹, 其中只有对$t$时刻的预测输入将作用于系统. 根据引理 1, 预先收集到的数据应满足持续激励条件, 为满足这一要求, 对预先收集到的数据作出如下假设.

假设 5 假设$\{u_N^d, y_N^d\} := \{u_t^d, y_t^d\}_{t=0}^{N-1}$是系统$\mathcal{S}$以初始条件为$x_0$的一条输入输出轨迹, 且控制输入序列$\{u_N^d\}$是$L + n_x + \eta$阶持续激励的, 系统输出序列$\{y_N^d\}$是离线收集无网络诱导噪声$n_t$的.

根据上述条件, 以预测时域步长为L的无终端约束弹性数据驱动 MPC 方案的优化问题表示为

$$J_L^*(u_{[t-\eta,t-1]}, \tilde{y}_{[-\eta,-1]}(t)) :=$$

$$\min_{g,\bar{u},\bar{y},\sigma} \sum_{k=0}^{L-1} l(\bar{u}_k(t), \bar{y}_k(t)) + \lambda_g \bar{v}\|g(t)\|^2 + \frac{\lambda_\sigma}{\bar{v}}\|\sigma(t)\|^2.$$

$$\text{s.t.} \ \begin{bmatrix} H_{L+\eta}(u_N^d) \\ H_{L+\eta}(y_N^d) \end{bmatrix} g(t) = \begin{bmatrix} \bar{u}(t) \\ \bar{y}(t) + \sigma(t) \end{bmatrix}; \tag{9a}$$

$$\begin{bmatrix} \bar{u}_{[-\eta,-1]}(t) \\ \bar{y}_{[-\eta,-1]}(t) \end{bmatrix} = \begin{bmatrix} u_{[t-\eta,t-1]} \\ \tilde{y}_{[-\eta,-1]}(t) \end{bmatrix}; \tag{9b}$$

$$\bar{u}_k(t) \in \mathbb{U}, \ k \in [0, L-1]. \tag{9c}$$

其中: $(\bar{u}, \bar{y})$的轨迹长度为$L+\eta$, 这里η步过去时域$\{\bar{u}_k(t), \bar{y}_k(t)\}_{k=-\eta}^{-1}$用于表示系统在$t$时刻的初始状态; $l(\bar{u}, \bar{y})$是一个关于人工平衡点(u^s, y^s)的二次惩罚项, 有

$$l(\bar{u}, \bar{y}) := \|\bar{u} - u^s\|_R^2 + \|\bar{y} - y^s\|_Q^2, \tag{10}$$

其中权重矩阵R、$Q \succ 0$; 根据文献 [19], 松弛变量$\sigma(t)$用于补偿噪声对预测输出带来的影响; 惩罚项$\|g(t)\|^2$用于减少 Hankel 矩阵中噪声的影响; $\lambda_g > 0$和$\lambda_\sigma > 0$分别为惩罚项$g(t)$和$\sigma(t)$的参数. 为了简化稳定性分析, 在优化问题 (9) 中只考虑输入约束, 且预先收集的数据只包含过程噪声w_t, 不包含网络诱导噪声n_t.

值得注意的是, 在优化问题 (9) 中不需要系统矩阵已知, 只需要通过离线实验从系统$\mathcal{S}$中收集一定长度的输入输出轨迹. 对于无弹性措施的数据驱动

MPC[20], 当系统遭受 DoS 攻击造成数据包丢失时, 即 $d_s(t)=1$, 此时控制器无法得知系统过去输出 $\zeta_{[t-\eta,t-1]}$, 导致优化问题 (9) 不能被及时地求解, 这可能会导致被控系统偏离稳定状态. 而所提出控制器能够存储接收到的过去η时刻的系统输出, 若在t时刻成功传输, 即$d_s(t)=0$时, 则控制器会更新并保存接收到的过去η时刻的输出, 然后对优化问题 (9) 进行求解; 而当 Dos 攻击造成丢包时, 即$d_s(t)=1$, 此时控制器会无法得知上一时刻的系统输出, 因此, 利用上一时刻的预测输出来补偿上一时刻系统实际输出, 即 $\tilde{y}_{-1}(t)=\bar{y}_0^*(t-1)$, 然后再对优化问题 (9) 进行求解, 即可实现弹性控制. 具体步骤如算法 1 所示.

算法 1　弹性数据驱动 MPC.

离线运行阶段:

step 1: 采集满足假设 5 的输入输出轨迹$\{u_N^d, y_N^d\}$;

step 2: 选择合适的参数$Q\succ 0$, $R\succ 0$, $\lambda_g>0$, $\lambda_\sigma>0$.

在线运行阶段:

step 1: if $d_s(t)=0$ then

step 2:　$\tilde{y}_{[-\eta,-1]}(t)=\zeta_{[t-\eta,t-1]}$

step 3: else if $d_s(t)=1$ then

step 4:　$\tilde{y}_{[-\eta,-1]}(t)=[\tilde{y}_{[-\eta+1,-1]}(t-1);\bar{y}_0^*(t-1)]$

step 5: end if

step 6: 使用$\{u_{[t-\eta,t-1]},\tilde{y}_{[-\eta,-1]}(t)\}$求解问题 (9)

step 7: 对系统$\mathcal{S}$施加控制输入$u_t=\bar{u}_0^*(t)$

step 8: 令$t=t+1$, 返回至 step 1

由算法 1 可以看出, 控制器在每一时刻t均会进行一次优化问题求解, 在每次补偿数据时均是利用预测时域的首位元素, 即$\bar{y}_0^*(t)$, 即使 DoS 攻击持续时间大于预测时域, 系统仍然可通过预测机制来补偿丢失的数据, 不受预测时域长度的影响.

2.2　预测误差边界

若优化问题 (9) 在$t\in N_+$时刻是可行的, 则预测输出$\bar{y}_t$与系统实际输出y_t间的误差是存在一个上界的. 定义在t时刻优化求解的预测误差$e_q^y(t)=y_{t+q}-\bar{y}_q^*(t)$, 其中$\bar{y}^*(t)$为优化问题 (9) 在$t$时刻求得的最优预测输出.

定理 1　假设问题 (9) 在t时刻是可行的, 其中$t\geqslant t_s$, 且$J_L^*(\tilde{\xi})\leqslant\bar{J}$, 则预测误差$e_q^y(t)$满足

$$\|e_q^y(t)\|\leqslant\beta_l(\bar{v},q),\ q\in[0,L-1]. \tag{11}$$

这里: 对于每个固定的 DoS 攻击持续时间$l\in\mathbb{N}$; $\beta_l(\bar{v},q)\in\mathcal{KL}$, 其定义如下所示:

$$\beta_l(\bar{v},q):=\begin{cases}\alpha_1(q)\sqrt{\eta}\bar{v}+\alpha_2(\bar{v},q),\ l=0;\\ \alpha_1(q)\Big[\sqrt{\eta-l}\bar{v}+\displaystyle\sum_{j=0}^{l-1}\beta_j(\bar{v},0)\Big]+\\ \alpha_2(\bar{v},q),\ 1\leqslant l<\eta;\\ \alpha_1(q)\displaystyle\sum_{j=l-\eta}^{l-1}\beta_j(\bar{v},0)+\alpha_2(\bar{v},q),\ l\geqslant\eta.\end{cases} \tag{12}$$

证明　根据文献 [25], 预测误差$e_q^y(t)$的上界可表示为

$$\|e_q^y(t)\|\leqslant\alpha_1(q)\|y_{[t-\eta,t-1]}-\bar{y}_{[-\eta,-1]}^*(t)\|+\alpha_2(\bar{v},q). \tag{13}$$

其中

$$\alpha_1(q):=b_2\rho^{q+\eta};$$

$$\alpha_2(\bar{v},q):=$$

$$\alpha_1(q)\Big[\|\Upsilon_\eta(I)\|\sqrt{\frac{(N-L-\eta+1)\bar{J}\bar{v}}{\lambda_g}}+\sqrt{\eta}\bar{v}+\sqrt{\frac{\bar{J}\bar{v}}{\lambda_\sigma}}\Big]+b_1\sum_{j=0}^{q+\eta-1}\rho^j\bar{v}+\Big[2b_1\sum_{j=\eta}^{N-1}\rho^j+\|\Upsilon_{L+\eta}(I)\|\Big]\sqrt{\frac{(L+\eta)(N-L-\eta)\bar{J}\bar{v}}{\lambda_g}}+\sqrt{\frac{\bar{J}\bar{v}}{\lambda_\sigma}},$$

且$\alpha_2\in\mathcal{KL}$; 常数$b_1,b_2,b_3,\rho>0$且满足$\|CA^j\|\leqslant b_1\rho^j$, $\|CA^{j+\eta}\mathcal{O}^\dagger\|\leqslant b_2\rho^j$和$\|CA^{j+\eta}\mathcal{O}_\eta^\dagger\Upsilon_\eta(I)\|\leqslant b_3\rho^j$, 这里$\mathcal{O}^\dagger$为矩阵$\mathcal{O}$的左逆矩阵; $\Upsilon_n(I)$定义如下所示:

$$\Upsilon_n(I):=\begin{bmatrix}0&0&\cdots&0\\ C&0&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ CA^{n-2}&CA^{n-3}&\cdots&0\end{bmatrix}.$$

由式 (13) 可知, $\|e_q^y(t)\|$与$\bar{y}_{[-\eta,-1]}^*(t)$有关, 因此, 对 DoS 攻击持续时间$l$与过去时域$\eta$的关系分为$l=0$, $1\leqslant l<\eta$和$l\geqslant\eta$三种情况讨论.

1) 当$l=0$时, 有$\bar{y}_{[-\eta,-1]}^*(t)=\zeta_{[t-\eta,t-1]}$, 该情况与文献 [25] 所证明的相同, 可得到

$$\|e_q^y(t)\|\alpha_1(q)\sqrt{\eta}\bar{v}+\alpha_2(\bar{v},q)=:\beta_0(\bar{v},q).$$

2) 当$1\leqslant l<\eta$时, 根据算法 1, 有$\bar{y}_{[-\eta,-1]}^*(t)=[\zeta_{[t-\eta,t-l-1]};\bar{y}_0^*(t-l:t-1)]$, 其中$\bar{y}_0^*(t-l:t-1):=[\bar{y}_0^*(t-l);\ldots;\bar{y}_0^*(t-1)]$, 可得到

$$\|y_{[t-\eta,t-1]}-\bar{y}_{[-\eta,-1]}^*(t)\|\leqslant\|n_{[t-\eta,t-l-1]}\|+\|e_0^y(t-l:t-1)\|\leqslant\sqrt{\eta-l}\bar{v}+\sum_{j=0}^{l-1}\beta_j(\bar{v},0). \tag{14}$$

将式 (14) 代入 (13), 可得到

$$\|e_q^y(t)\| \leqslant$$
$$\alpha_1(q)\sqrt{\eta-l}\bar{v}+\sum_{j=0}^{l-1}\beta_j(\bar{v},0)+\alpha_2(\bar{v},q)=:\beta_l(\bar{v},q),$$
$$1\leqslant l<\eta.$$

3) 当$l\geqslant\eta$时, 根据算法 1, 有$\bar{y}^*_{[-\eta,-1]}(t)=\bar{y}^*_0(t-\eta:t-1)$, 同理, 可得到

$$\|e_q^y(t)\|\leqslant\sum_{j=l-\eta}^{l-1}\beta_j(\bar{v},0)+\alpha_2(\bar{v},q)=:\beta_l(\bar{v},q),$$
$$l\geqslant\eta.$$

综上, 定理 1 得证. □

根据定理 1 中的结果可得出预测误差$e_q^y(t)$边界会受 DoS 攻击持续时间l和噪声边界$\bar{v}$的影响, DoS 攻击持续时间l越长, 预测误差越大. 由于 DoS 攻击持续时间l存在一个上界, 即$l\leqslant\bar{l}$, 当$l=\bar{l}$时预测误差边界达到最大, 即对于任意时刻t均满足$\|e_q^y(t)\|\leqslant\beta_{\bar{l}}(\bar{v},q)$, 保证了预测误差的有界性. 当成功传输时, 即$l=0$时, 预测误差边界会重新恢复至无 DoS 攻击时的正常水平. 注意, 当噪声边界$\bar{v}=0$时, 对于任意的 DoS 攻击持续时间$l\geqslant0$, 预测误差$e_q^y(t)$始终为 0.

2.3 稳定性分析

首先, 定义系统$\mathcal{S}$的扩展状态为

$$\xi_t=\begin{bmatrix}u_{[t-\eta,t-1]}\\ y_{[t-\eta,t-1]}\end{bmatrix}. \tag{15}$$

记Γ_ξ为扩展状态ξ_t到状态x_t的线性变换矩阵, 即$x_t=\Gamma_\xi\xi_t$. 另外, 记$\tilde{\xi}_t:=[u_{[t-\eta,t-1]};\tilde{y}_{[-\eta,-1]}(t)]$. 然后, 构造如下李雅普诺夫函数:

$$V_L(\xi_t)=J_L^*(\tilde{\xi}_t)+W(\xi_t). \tag{16}$$

其中: $W(\xi_t):=\|\xi_t\|_P^2$, $P\succ0$, 且存在一个常数ϵ_0[29]满足

$$W(\xi_{t+1})\leqslant W(\xi_t)+\|u_t\|_R^2+\|y_t\|_Q^2-\epsilon_0\|\xi_t\|^2. \tag{17}$$

为证明李雅普诺夫函数的收敛性, 下面给出李雅普诺夫函数的类连续性[20]. 与文献 [20] 不同的是, 本文考虑了过程噪声和 DoS 攻击的影响.

引理 2 假设问题 (9) 在t时刻是可行的, u^d是$\eta+L+n_x$阶持续激励的, 且$V_L(\xi_t)\leqslant\bar{V}$, 则存在函数$\alpha_4(\bar{v},\bar{l})$, 使得

$$V_{L-1}(\xi_{t+1})\leqslant V_L(\xi_t)-\epsilon_0\|\xi_t\|^2+\alpha_4(\bar{v},\bar{l}), \tag{18}$$

其中: $\epsilon_0>0$; 对于每个固定的$\bar{l}\geqslant0$, $\alpha_4(\bar{v},\cdot)\in\mathcal{K}_\infty$.

证明 首先, 用$(\bar{u}^*(t),\bar{y}^*(t),g^*(t),\sigma^*(t))$表示优化问题 (9) 在$t$时刻的最优解, 用$(\bar{u}(t),\bar{y}(t),\bar{g}(t),\bar{\sigma}(t))$表示优化问题 (9) 在$t$时刻的可行解. 然后, 选择一个在$t+1$时刻预测时域为$L-1$的可行解. 记系统$\mathcal{S}$以$(u_{[t-\eta,t-1]},y_{[-\eta,-1]}(t))$为初始条件在控制输入$\bar{u}^*(t)$的作用下输出轨迹为$y_{[t,t+L-1]}$. 令$\bar{u}$为$\bar{u}_{[-\eta,L-2]}(t+1)=\bar{u}^*_{[-\eta+1,L-1]}(t)$, 令$\bar{y}$的过去时域序列为$\bar{y}_{[-\eta,-1]}(t+1)=\tilde{y}_{[-\eta,-1]}(t+1)$, 预测时域序列为$\bar{y}_{[0,L-2]}(t+1)=y_{[t+1,t+L-1]}$, 则$\bar{g}(t+1)$可选择为

$$\bar{g}(t+1)=H_{ux}^{\ddagger}\begin{bmatrix}\bar{u}_{[-\eta,L-2]}(t+1)\\ x_{t+1-\eta}\end{bmatrix}. \tag{19}$$

其中: $H_{ux}:=[H_{L+\eta}(u_N^d)^{\mathrm{T}},H_1(\hat{x}^d_{N-L-\eta+1})^{\mathrm{T}}]^{\mathrm{T}}$, $H_{ux}^{\ddagger}$为矩阵H_{ux}的右逆矩阵, $\{\hat{x}_N^d\}$为系统$\mathcal{S}_i$预先收集数据$\{u_N^d,\hat{y}_N^d\}$所对应的状态轨迹. 接着, 对$\bar{\sigma}(t+1)$进行构造, 由于$\bar{\sigma}(t+1)$与 DoS 攻击持续时间有关, 类似定理 1 的证明, 需要对l进行分类讨论, 限于篇幅, 本文余下部分只对$\eta\leqslant l\leqslant\bar{l}$的情况进行讨论.

考虑在$t+1$时刻 DoS 攻击持续时间为$\eta<l+1\leqslant\bar{l}$, 为满足约束 (9a) 和 (9b), $\bar{\sigma}(t+1)$可选择

$$\bar{\sigma}_{[-\eta,-1]}(t+1)=$$
$$[I,0]\Phi^w\bar{g}(t+1)-\Upsilon_\eta(I)w_{[t+1-\eta,t]}+e_0^y(t+1-\eta:t), \tag{20}$$

$$\bar{\sigma}_{[0,L-2]}(t+1)=$$
$$[0,I]\Phi^w\bar{g}(t+1)-\Upsilon_{L-1}(I)w_{[t+1,t+L-1]}. \tag{21}$$

其中

$$\Phi^w:=\mathcal{O}_{L+\eta}W^d+\Upsilon_{L+\eta}(I)H_{L+\eta}(w_N^d),$$
$$W^d:=\Big[0,w_0^d,\dots,\sum_{i=0}^{N-L-\eta-1}A^iw^d_{N-L-\eta-1-i}\Big].$$

由于$\bar{y}_{[0,L-2]}(t+1)=y_{[t+1,t+L-1]}$, 根据定理 1, 可得到

$$\|\bar{y}_q(t+1)-\bar{y}^*_{q+1}(t)\|_Q\leqslant\sqrt{\bar{\lambda}(Q)}\beta_l(\bar{v},q), \tag{22}$$

$$\|\bar{y}_q(t+1)-\bar{y}^*_{q+1}(t)\|_Q^2\leqslant\bar{\lambda}(Q)\beta_l^2(\bar{v},q). \tag{23}$$

这里: $q\in[0,L-2]$, $\bar{\lambda}(Q)$为矩阵Q的最大奇异值. 利用系统$\mathcal{S}$的滞后性, 有

$$x_{t+1-\eta}=\left[\mathcal{M}_1\mathcal{O}_\eta^\dagger\right]\xi_{t+1}-\mathcal{O}_\eta^\dagger\Upsilon_\eta(I)w_{[t+1-\eta,t]}, \tag{24}$$

其中$\mathcal{M}_1$由系统矩阵A、B、C、D构成. 然后, 由系统$\mathcal{S}$的动态过程, 可得到

$$x_{t+1-\eta}=[\mathcal{M}_1\quad\mathcal{O}_\eta^\dagger](\tilde{A}\xi_t+\tilde{B}\bar{u}_0^*(t)+\tilde{E}w_{t+1})-$$
$$\mathcal{O}_\eta^\dagger\Upsilon_\eta(I)w_{[t+1-\eta,t]}, \tag{25}$$

这里$\tilde{A}$、$\tilde{B}$和$\tilde{E}$为系统$\mathcal{S}$以ξ_t为状态的系统矩阵. 根据$\underline{\lambda}(P)\|\xi_t\|^2\leqslant W(\xi_t)\leqslant V_L(\xi_t)\leqslant\bar{V}$, 可得到

$$\|\xi_t\|^2\leqslant\frac{\bar{V}}{\underline{\lambda}(P)}, \tag{26}$$

$$\|\bar{u}^*_{[-\eta,L-1]}(t)\|^2 \leqslant \frac{\bar{V}}{\underline{\lambda}(R)}, \tag{27}$$

其中$\underline{\lambda}(P)$为矩阵P的最小奇异值. 接下来, 可利用式 (26) 和 (27) 推导出$\|x_{t+1-\eta}\|^2$的上界为

$$\begin{aligned}&\|x_{t+1-\eta}\|^2 \leqslant\\ &2c_\xi\Big(2\|\tilde{A}\|^2\frac{\bar{V}}{\underline{\lambda}(P)}+2\|\tilde{B}\|^2\frac{\bar{V}}{\underline{\lambda}(R)}+2\|\tilde{E}\|^2\bar{v}^2\Big)+\\ &2\|\mathcal{O}_\eta^\dagger\Upsilon_\eta(I)\|^2(\eta-1)\bar{v}^2=:b_x(\bar{v}),\end{aligned} \tag{28}$$

这里$c_\xi:=\|[\mathcal{M}_1\quad \mathcal{O}_l^\dagger]\|^2$. 由式 (19), 可得到$\|\bar{g}(t+1)\|^2$的上界为

$$\begin{aligned}&\|\bar{g}(t+1)\|^2 \leqslant\\ &\|H^\ddagger_{ux}\|^2(\|\bar{u}^*_{[-\eta+1,L-1]}(t)\|^2+\|x_{t+1-\eta}\|^2)\overset{(28)}{\leqslant}\\ &\|H^\ddagger_{ux}\|^2\Big(\frac{\bar{V}}{\underline{\lambda}(R)}+b_x(\bar{v})\Big)=:b_g(\bar{v}).\end{aligned} \tag{29}$$

同理, 由式 (20) 和 (21), 可得到$\|\bar{\sigma}(t+1)\|^2$的上界为

$$\begin{aligned}&\|\bar{\sigma}(t+1)\|^2 \leqslant\\ &2\sum_{j=l+1-\eta}^{l}\beta_j^2(\bar{v},0)+2\|\Upsilon_\eta(I)\|^2\eta\bar{v}^2+\\ &\Big[4\Big(b_1\sum_{j=L+\eta}^{N-1}\rho^j\Big)^2(L+\eta)(N-L-\eta)\bar{v}^2+\\ &4\|\Upsilon_{L+\eta}(I)\|^2(L+\eta)(N-L-\eta+1)\bar{v}^2\Big]b_g(\bar{v})+\\ &2\|\Upsilon_{L-1}(I)\|^2(L-1)\bar{v}^2=:b_\sigma(\bar{v},l).\end{aligned} \tag{30}$$

最后, 可得到目标函数$J^*_{L-1}(\tilde{\xi}_{t+1})$的上界为

$$\begin{aligned}&J^*_{L-1}(\tilde{\xi}_{t+1}) \leqslant\\ &\sum_{k=0}^{L-2}\|\bar{u}_k(t+1)\|_R^2+\|\bar{y}_k(t+1)\|_Q^2+\\ &\lambda_g\bar{v}\|\bar{g}(t+1)\|^2+\frac{\lambda_\sigma}{\bar{v}}\|\bar{\sigma}(t+1)\|^2 \leqslant\\ &\sum_{k=0}^{L-2}\|\bar{u}_k(t+1)\|_R^2+\|\bar{y}_k(t+1)-\bar{y}^*_{k+1}(t)+\\ &\bar{y}^*_{k+1}(t)\|_Q^2+\lambda_g\bar{v}b_g(\bar{v})+\frac{\lambda_\sigma}{\bar{v}}b_\sigma(\bar{v},l) \leqslant\\ &J^*_L(\tilde{\xi}_t)-l(\bar{u}^*_0(t),\bar{y}^*_0(t))+\alpha_3(\bar{v},l).\end{aligned} \tag{31}$$

其中

$$\begin{aligned}&\alpha_3(\bar{v},l):=\\ &2\sqrt{\bar{\lambda}(Q)\bar{V}}\sum_{k=0}^{L-2}\beta_l(\bar{v},k)+\bar{\lambda}(Q)\sum_{k=0}^{L-2}\beta_l^2(\bar{v},k)+\\ &\lambda_g\bar{v}b_g(\bar{v})+\frac{\lambda_\sigma}{\bar{v}}b_\sigma(\bar{v},l).\end{aligned} \tag{32}$$

结合式 (17) 和 (31), 可得到

$$\begin{aligned}V_{L-1}(\xi_{t+1}) \leqslant\ & V_L(\xi_t)+\|y_t\|_Q^2-\|\bar{y}^*_0(t)\|_Q^2-\\ &\epsilon_0\|\xi_t\|^2+\alpha_3(\bar{v},l).\end{aligned} \tag{33}$$

另有

$$\begin{aligned}&\|y_t\|_Q^2-\|\bar{y}^*_0(t)\|_Q^2=\\ &\|y_t-\bar{y}^*_0(t)+\bar{y}^*_0(t)\|_Q^2-\|\bar{y}^*_0(t)\|_Q^2 \leqslant\\ &\|y_t-\bar{y}^*_0(t)\|_Q^2+2\|y_t-\bar{y}^*_0(t)\|_Q\|\bar{y}^*_0(t)\|_Q \leqslant\\ &\bar{\lambda}(Q)\beta_l^2(\bar{v},0)+2\bar{\lambda}(Q)\sqrt{\bar{V}}\beta_l(\bar{v},0).\end{aligned} \tag{34}$$

将式 (34) 代入 (33), 可得到

$$V_{L-1}(\xi_{t+1}) \leqslant V_L(\xi_t)-\epsilon_0\|\xi_t\|^2+\alpha_4(\bar{v},l), \tag{35}$$

这里

$$\begin{aligned}\alpha_4(\bar{v},l):=\ &\alpha_3(\bar{v},l)+\bar{\lambda}(Q)\beta_l^2(\bar{v},0)+\\ &2\bar{\lambda}(Q)\sqrt{\bar{V}}\beta_l(\bar{v},0).\end{aligned} \tag{36}$$

又由于对于任意固定的$\bar{v}\geqslant 0$, $\alpha_4(\cdot,l)$是单调不减的, 有$\alpha_4(\cdot,l)\leqslant\alpha_4(\cdot,\bar{l})$. □

下面为算法 1 的闭环稳定性结果.

定理 2　假设u^d是$\eta+L+n_x$阶持续激励的且$V_L(\xi_t)\leqslant\bar{V}$, 则存在常数$\underline{L},\bar{v}_L,\bar{l}_L\geqslant 0$对于任意的预测时域$L$和噪声边界$\bar{v}\geqslant 0$以及 Dos 攻击最长持续时间$\bar{l}\geqslant 0$满足$L>\underline{L},\bar{v}\leqslant\bar{v}_L$和$\bar{l}\leqslant\bar{l}_L$, 使得问题 (9) 在任意时刻$t\geqslant 0$是可行的, 闭环输入$u_t$满足约束$u_t\in\mathbb{U}$, 且李雅普诺夫函数$V_L(\xi_t)$满足

$$\underline{\lambda}(P)\|\xi_t\|^2\leqslant V_L(\xi_t)\leqslant\bar{\gamma}\|\xi_t\|^2+\alpha_6(\bar{v},\bar{l}), \tag{37}$$

$$V_L(\xi_{t+1})\leqslant\alpha_L V_L(\xi_t)+\alpha_{13}(\bar{v},\bar{l}). \tag{38}$$

其中: $\bar{\gamma}$为一个常数; 且$0<\alpha_L<1$; 对于每个固定的$\bar{l}>0$, $\alpha_6,\alpha_{13}\in\mathcal{K}_\infty$.

证明　首先, 证明式 (37) 表明李雅普诺夫函数$V_L(\xi_t)$是有界的. 由$V_L(\xi_t)\geqslant W(\xi_t)\geqslant\underline{\lambda}(P)\|\xi_t\|^2$, 即可得到$V_L(\xi_t)$的下界. 然后, 求$V_L(\xi_t)$的上界. 构造问题 (9) 在$t$时刻的一组可行解为$(\bar{g}(t),\bar{\sigma}(t),\bar{u}_{[-\eta,L-1]}(t),\bar{y}_{[-\eta,L-1]}(t))$. 由式 (9b), 有$\bar{u}_{[-\eta,L-1]}(t)=u_{[t-\eta,t-1]}$和$\bar{y}_{[-\eta,-1]}(t)=\tilde{y}_{[-\eta,-1]}(t)$. 对于理想系统$\mathcal{S}_i$而言, 利用系统的可控性, 存在一个常数$\delta>0$和一个输入序列$u_{[t,t+L-1]}\in\mathbb{U}^L$, 对于所有的$x_t$均满足$\|x_t\|/\gamma_\xi\leqslant\|\xi_t\|\leqslant\delta$, 其中$\gamma_\xi:=\|\Gamma_\xi\|$, 输入序列能够使得状态$x_{[t,t+L-1]}$和相应的输出$\hat{y}_{[t,t+L-1]}$在$L$步内到达原点附近, 则存在一个常数$\gamma_{uy}$满足

$$\left\|\begin{bmatrix}u_{[t,t+L-1]}\\ \hat{y}_{[t,t+L-1]}\end{bmatrix}\right\|^2\leqslant\gamma_{uy}^2\|x_t\|^2. \tag{39}$$

因此, 对于$\|\xi_t\|^2\leqslant\delta^2$的情况下, 可选择$\bar{u}_{[0,L-1]}(t)=u_{[t,t+L-1]}$以及$\bar{y}_{[0,L-1]}(t)=\hat{y}_{[t,t+L-1]}$. 根据上述对$(\bar{u}_{[-\eta,L-1]}(t),\bar{y}_{[-\eta,L-1]}(t))$的构造, 由文献 [25], 可得到$V_L(\xi_t)$的上界为

$$\begin{aligned}&V_L(\xi_t)\leqslant\\ &\bar{\lambda}(Q,R)\gamma_{uy}^2\gamma_\xi^2\|\xi_t\|^2+\bar{\lambda}(P)\|\xi_t\|^2+\end{aligned}$$

$$\lambda_g\bar{v}(\gamma_1\|\xi_t\|^2+\gamma_2\bar{v}^2)+(\lambda_\sigma/\bar{v})(\alpha_5(\bar{v})\gamma_1\|\xi_t\|^2+\alpha_5(\bar{v})\gamma_2\bar{v}^2+2\|\Upsilon_\eta(I)\|^2\eta\bar{v}^2+2\|y_{[t-\eta,t-1]}-\bar{y}^*_{[-\eta,-1]}(t)\|). \tag{40}$$

其中

$$\alpha_5(\bar{v}):=2\Big[2\Big(b_1\sum_{j=L+\eta}^{N-1}\rho^j\Big)^2(L+\eta)(N-L-\eta)+2\|\Upsilon_{L+\eta}\|^2(L+\eta)(N-L-\eta+1)\Big]\bar{v}^2,$$

$$\gamma_1:=\|H^\ddagger_{ux}\|^2(\gamma^2_{uy}\gamma^2_\xi+2\|\Psi^\dagger_\eta\|^2),$$

$$\gamma_2:=2\|H^\ddagger_{ux}\|^2\|\mathcal{O}^\dagger_\eta\Upsilon_\eta(I)\|^2\eta,$$

Ψ_η的定义如下所示:

$$\Psi_\eta:=\begin{bmatrix}I & 0\\ \Upsilon_\eta(B) & \mathcal{O}_\eta\end{bmatrix}. \tag{41}$$

类似于定理 1, 对于$l\geqslant\eta$, 有$\bar{y}^*_{[-\eta,-1]}(t)=\bar{y}^*_0(t-\eta:t-1)$, 由式 (40), 可得到

$$V_L(\xi_t)\leqslant\bar{\lambda}(Q,R)\gamma^2_{uy}\gamma^2_\xi\|\xi_t\|^2+\bar{\lambda}(P)\|\xi_t\|^2+\lambda_g\bar{v}(\gamma_1\|\xi_t\|^2+\gamma_2\bar{v}^2)+(\lambda_\sigma/\bar{v})\Big(\alpha_5(\bar{v})\gamma_1\|\xi_t\|^2+\alpha_5(\bar{v})\gamma_2\bar{v}^2+2\|\Upsilon_\eta(I)\|^2\eta\bar{v}^2+2\sum_{j=l-\eta}^{l-1}\beta^2_j(\bar{v},0)\Big)=\gamma_3\|\xi_t\|^2+\alpha_6(\bar{v},l). \tag{42}$$

其中

$$\gamma_3:=\bar{\lambda}\gamma^2_{uy}\gamma^2_\xi+\bar{\lambda}(P)+\lambda_g\bar{v}\gamma_1+(\lambda_\sigma/\bar{v})\alpha_5(\bar{v})\gamma_1,$$

$$\alpha_6(\bar{v},l):=\lambda_g\gamma_2\bar{v}^3+(\lambda_\sigma/\bar{v})\Big(\alpha_5(\bar{v})\gamma_2\bar{v}^2+2\|\Upsilon_\eta(I)\|^2\eta\bar{v}^2+2\sum_{j=l-\eta}^{l-1}\beta^2_j(\bar{v},0)\Big).$$

对于每个固定的$l\leqslant 0$, $\alpha_6(\cdot,l)$是单调不减的, 因此, 有$\alpha_6(\cdot,l)\leqslant\alpha_6(\cdot,\bar{l})$. 然后对于满足$V_L(\xi_t)\leqslant\bar{V}$的任意$\xi_t$可以扩大$V_L(\xi_t)$的上界为

$$V_L(\xi_t)\leqslant\bar{\gamma}\|\xi_t\|^2+\alpha_6(\bar{v},\bar{l}), \tag{43}$$

这里$\bar{\gamma}:=\max\Big\{\gamma_3,\dfrac{\bar{V}-\alpha_6(\bar{v},\bar{l})}{\delta^2}\Big\}$.

接下来证明式 (38) 表明李雅普诺夫函数会收敛至一个球域中, 考虑在$t+1$时刻 DoS 攻击持续时间为$l+1\leqslant\bar{l}$, 通过式 (17) 迭代, 可得到

$$W(\xi_{t+L})-W(\xi_{t+1})\leqslant\sum_{k=0}^{L-2}-\epsilon_0\|\xi_{t+1+k}\|^2+l(\bar{u}_k(t+1),\bar{y}_k(t+1))\leqslant\sum_{k=0}^{L-2}-\epsilon_0\|\xi_{t+1+k}\|^2+l(\bar{u}^*_k(t+1),\bar{y}^*_k(t+1))+\alpha_7(\bar{v},l)\leqslant\sum_{k=0}^{L-2}-\epsilon_0\|\xi_{t+1+k}\|^2+J^*_{L-1}(\tilde{\xi}_{t+1})+\alpha_7(\bar{v},l), \tag{44}$$

其中

$$\alpha_7(\bar{v},l):=\bar{\lambda}(Q)\sum_{k=0}^{L-2}\beta^2_l(\bar{v},k)+2\bar{\lambda}(Q)\sqrt{\bar{V}}\sum_{k=0}^{L-2}\beta_l(\bar{v},k). \tag{45}$$

由α_7的表达式可见, 对于任意给定的$\bar{v}$, $\alpha_7(\cdot,l)$是单调不减的, 因此, 有$\alpha_7(\bar{v},l)\leqslant\alpha_7(\bar{v},\bar{l})$. 由于$W(\xi_t)\geqslant 0$, 利用引理 2, 可推出

$$\epsilon_0\sum_{k=0}^{L-2}\|\xi_{t+1+k}\|^2\leqslant J^*_{L-1}(\tilde{\xi}_{t+1})+W(\xi_{t+1})+\alpha_7(\bar{v},\bar{l})\overset{(18)}{\leqslant}V_L(\xi_t)-\epsilon_0\|\xi_t\|^2+\alpha_8(\bar{v},\bar{l}), \tag{46}$$

这里$\alpha_8(\bar{v},\bar{l}):=\alpha_4(\bar{v},\bar{l})+\alpha_7(\bar{v},\bar{l})$. 因此, 存在一个常数$k_x\in\mathbb{I}_{[0,L-2]}$满足

$$\|\xi_{t+1+k_x}\|^2\leqslant\frac{V_L(\xi_t)+\alpha_8(\bar{v},\bar{l})}{\epsilon_0(L-1)}. \tag{47}$$

给定一个常数C满足

$$\alpha_8(\bar{v},\bar{l})\leqslant C. \tag{48}$$

由式 (47) , 可得到

$$\|\xi_{t+1+k_x}\|^2\leqslant\frac{\bar{V}+C}{\epsilon_0(L-1)}. \tag{49}$$

因此, 当预测时域$L>\underline{L}_0:=1+\dfrac{\bar{V}+C}{\epsilon_0\delta^2}$时, 可得到$\|\xi_{t+1+k_x}\|^2\leqslant\delta^2$.

根据上述条件, 当$q\in[k_x,L-1]$时, 有$\|\xi_{t+1+k_x}\|\leqslant\delta$, 类似式 (39), 存在一个输入轨迹$\bar{u}_{[k_x,L-1]}(t+1)$使得对应的输出$\hat{y}$趋近于原点, 即满足

$$\left\|\begin{bmatrix}\bar{u}_{[k_x,L-1]}(t+1)\\ \hat{y}_{[t+1+k_x,t+L]}\end{bmatrix}\right\|^2\leqslant\gamma^2_{uy}\|x_{t+1+k_x}\|^2. \tag{50}$$

因此, 可构造如下可行的输入轨迹:

$$\bar{u}_{[-\eta,L-1]}(t+1)=\begin{bmatrix}\bar{u}^*_{[-\eta+1,k_x]}(t)\\ \bar{u}_{[k_x,L-1]}(t+1)\end{bmatrix}. \tag{51}$$

同时, 相对应的输出轨迹$\bar{y}(t+1)$为

$$\bar{y}_{[-\eta,L-1]}(t+1)=\begin{bmatrix}\tilde{y}_{[-\eta,-1]}(t+1)\\ y_{[t+1,t+k_x]}\\ \hat{y}_{[t+1+k_x,t+L]}\end{bmatrix}. \tag{52}$$

根据上述条件, 可行输入输出$(\bar{u}(t+1),\bar{y}(t+1))$在问题 (9) 中相对应的$\bar{g}(t+1)$可选择为

$$\bar{g}(t+1)=H^\ddagger_{ux}\begin{bmatrix}\bar{u}_{[-\eta,L-1]}(t+1)\\ x_{t+1-\eta}\end{bmatrix}. \tag{53}$$

另外, 对于$l\geqslant\eta$时, $\bar{\sigma}(t+1)$可选择为

$$\bar{\sigma}_{[-\eta,-1]}(t+1)=\\ -\Upsilon_{\eta}(I)w_{[t+1-\eta,t]}+e_0^y(t-\eta:t)+[I,0]\Phi^w\bar{g}(t+1), \tag{54}$$

$$\bar{\sigma}_{[0,k_x-1]}(t+1)=\\ -\Upsilon_{k_x}(I)w_{[t+1,t+k_x]}+[0,I,0]\Phi^w\bar{g}(t+1), \tag{55}$$

$$\bar{\sigma}_{[k_x,L-1]}(t+1)=\\ \mathcal{O}_{L-k_x}\sum_{j=0}^{k_x+\eta-1}A^jw_{t+k_x-j}+[0,I]\Phi^w\bar{g}(t+1). \tag{56}$$

根据构造的可行解, 可利用式 (37)、(47) 和 (50) 得到后k_x步的目标函数满足

$$\sum_{k=k_x}^{L-1}\|\bar{u}_k(t+1)\|_R^2+\|\bar{y}_k(t+1)\|_Q^2\leqslant\\ \bar{\lambda}(R,Q)\sum_{k=k_x}^{L-1}\|\bar{u}_k(t+1)\|^2+\|\bar{y}_k(t+1)\|^2\overset{(50)}{\leqslant}\\ \bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\|\xi_{t+1+k_x}\|^2\overset{(47)}{\leqslant}\\ \frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2(V_L(\xi_t)+\alpha_8(\bar{v},\bar{l}))}{\epsilon_0(L-1)}\overset{(37)}{\leqslant}\\ \frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0(L-1)}\|\xi_t\|^2+\alpha_9(\bar{v},\bar{l}), \tag{57}$$

其中

$$\alpha_9(\bar{v},\bar{l}):=\frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2(\alpha_6(\bar{v},\bar{l})+\alpha_8(\bar{v},\bar{l}))}{\epsilon_0(L-1)}.$$

接下来, 类似式 (31), 可得到前k_x步的目标函数满足

$$\sum_{k=0}^{k_x-1}\|\bar{u}_{k+1}^*(t)\|_R^2+\|\bar{y}_k(t+1)\|_Q^2\leqslant\\ J_L^*(\tilde{\xi}_t)-\|\bar{u}_0^*(t)\|_R^2-\|\bar{y}_0^*(t)\|_Q^2+\alpha_{10}(\bar{v},\bar{l}), \tag{58}$$

这里

$$\alpha_{10}(\bar{v},\bar{l}):=2\bar{\lambda}(Q)\sqrt{\bar{V}}\sum_{k=0}^{k_x-1}\beta_{\bar{l}}(\bar{v},k)+\\ \bar{\lambda}(Q)\sum_{k=0}^{k_x-1}\beta_{\bar{l}}^2(\bar{v},k). \tag{59}$$

由式 (51) 可知, 可行输入被分为$\bar{u}_{[-\eta+1,k_x]}^*(t)$和$\bar{u}_{[k_x,L-1]}(t+1)$两段, 因此, 可得到这两段序列的上界分别为

$$\|\bar{u}_{[\eta+1,k_x]}^*(t)\|^2\leqslant\frac{\bar{V}}{\underline{\lambda}(R)}, \tag{60}$$

$$\|\bar{u}_{[k_x,L-1]}(t+1)\|^2\leqslant\gamma_{uy}^2\gamma_{\xi}^2\delta^2. \tag{61}$$

另外, 由式 (28), 有

$$\|x_{t+1-\eta}\|^2\leqslant b_x(\bar{v}). \tag{62}$$

根据上述条件可求得$\|\bar{g}(t+1)\|^2$的上界为

$$\|\bar{g}(t+1)\|^2\overset{(53)}{\leqslant}\\ \|H_{ux}^{\ddagger}\|^2(\|\bar{u}_{[-\eta,L-1]}(t+1)\|^2+\|x_{t+1-\eta}\|^2)\overset{(60),(61),(62)}{\leqslant}\\ \|H_{ux}^{\ddagger}\|^2\Big(\frac{\bar{V}}{\underline{\lambda}(R)}+\gamma_{uy}^2\gamma_{\xi}^2\delta^2+b_x(\bar{v})\Big)=:\bar{b}_g(\bar{v}). \tag{63}$$

由式 (54) ∼ (56), 可得到$\|\bar{\sigma}(t+1)\|^2$的上界为

$$\|\bar{\sigma}(t+1)\|^2\leqslant\\ 2\sum_{j=l-\eta}^{l-1}\beta_j^2(\bar{v},0)+2\|\Upsilon_{\eta}\|^2\eta\bar{v}^2+\\ \alpha_5(\bar{v})\bar{b}_g(\bar{v})+2\|\Upsilon_{k_x}\|^2k_x\bar{v}^2+\\ 2\Big\|\mathcal{O}_{L-k_x}\sum_{j=0}^{k_x+\eta-1}A^j\Big\|^2\bar{v}^2=:\bar{b}_{\sigma}(\bar{v},l), \tag{64}$$

其中对于每个固定的$\bar{v}$, $\bar{b}_{\sigma}(\cdot,l)$是单调不减的, 因此, 有$\bar{b}_{\sigma}(\bar{v},l)\leqslant\bar{b}_{\sigma}(\bar{v},\bar{l})$, 满足

$$\|\bar{\sigma}(t+1)\|^2\leqslant\bar{b}_{\sigma}(\bar{v},\bar{l}). \tag{65}$$

然后, 结合式 (57)、(58)、(63) 和 (65), 可得到

$$J_L^*(\tilde{\xi}_{t+1})\leqslant J_L^*(\tilde{\xi}_t)-\|\bar{u}_0^*(t)\|_R^2-\|\bar{y}_0^*(t)\|_Q^2+\\ \frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0(L-1)}\|\xi_t\|^2+\alpha_{11}(\bar{v},\bar{l}), \tag{66}$$

这里

$$\alpha_{11}(\bar{v},\bar{l}):=\\ \alpha_9(\bar{v},\bar{l})+\alpha_{10}(\bar{v},\bar{l})+\lambda_g\bar{v}\bar{b}_g(\bar{v})+\frac{\lambda_{\sigma}}{\bar{v}}\bar{b}_{\sigma}(\bar{v},\bar{l}).$$

接着, 结合式 (17) 和 (66), 有

$$V_L(\xi_{t+1})\leqslant\\ V_L(\xi_t)+\|y_t\|_Q^2-\|\bar{y}_0^*(t)\|_Q^2+\\ \alpha_{11}(\bar{v},\bar{l})\Big(\frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0(L-1)}-\epsilon_0\Big)\|\xi_t\|^2\leqslant\\ V_L(\xi_t)+\alpha_{12}(\bar{v},\bar{l})+\Big(\frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0(L-1)}-\epsilon_0\Big)\|\xi_t\|^2, \tag{67}$$

其中

$$\alpha_{12}(\bar{v},\bar{l}):=\\ \alpha_{11}(\bar{v},\bar{l})+\bar{\lambda}(Q)\beta_{\bar{l}}^2(\bar{v},0)+2\bar{\lambda}(Q)\sqrt{\bar{V}}\beta_{\bar{l}}(\bar{v},0),$$

推导过程同式 (34). 最后, 将式 (37) 代入 (67), 可得到

$$V_L(\xi_{t+1})\leqslant\alpha_LV_L(\xi_t)+\alpha_{13}(\bar{v},\bar{l}). \tag{68}$$

这里

$$\alpha_L:=1-\frac{\epsilon_0}{\bar{\gamma}}\Big(1-\frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0^2(L-1)}\Big), \tag{69}$$

$$\alpha_{13}(\bar{v},\bar{l}):=\frac{\epsilon_0}{\bar{\gamma}}\Big(1-\frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0^2(L-1)}\Big)\alpha_6(\bar{v},\bar{l})+$$

$$\alpha_{12}(\bar{v},\bar{l}). \tag{70}$$

为确保李雅普诺夫函数的非递增性质, 预测时域要足够长以满足

$$L > \underline{L}_1 := 1 + \frac{\bar{\lambda}(R,Q)\gamma_{uy}^2\gamma_{\xi}^2\bar{\gamma}}{\epsilon_0^2}. \tag{71}$$

综上, 预测时域L应满足

$$L > \underline{L} := \max\{\underline{L}_0, \underline{L}_1\}. \tag{72}$$

同时, 为确保$V(\xi_t) \leqslant \bar{V}$在迭代过程中成立, 要使得$\alpha_{13} \leqslant (1-\alpha_L)\bar{V}$成立, 则噪声边界$\bar{v}$和最长 DoS 攻击持续时间$\bar{l}$需要满足$\bar{v} \leqslant \bar{v}_L, \bar{l} \leqslant \bar{l}_L$, 其中$\bar{v}_L, \bar{l}_L$为

$$(\bar{v}_L, \bar{l}_L) = \min\{\alpha_{13}^{-1}((1-\alpha_L)\bar{V}), \alpha_8^{-1}(C)\}. \tag{73}$$

满足上述条件则可使得系统稳定. □

3 仿真分析

为验证算法 1 的有效性, 本节进行数值仿真测试. 考虑一个间歇式反应器实例[25], 该系统是开环不稳定的, 其连续系统的系统矩阵如下所示:

$$A = \begin{bmatrix} 1.38 & -0.207\,7 & 6.715 & -5.676 \\ -0.581\,4 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix},$$

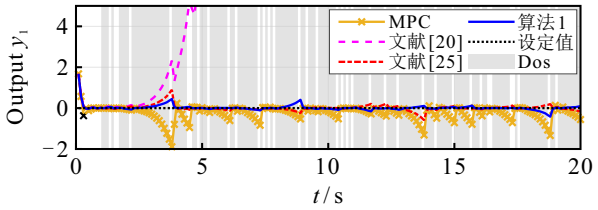
$$B = \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix}, \ C = \begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$D = 0.$$

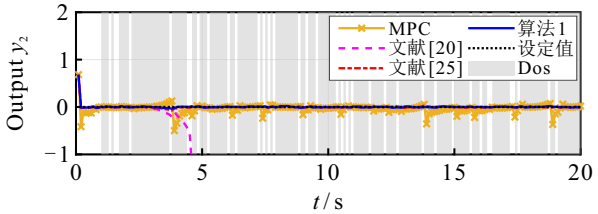
该系统的可观性指数为$\eta = 2$.

对上述系统的控制目标是在满足输入约束$u_t \in \mathbb{U} = [-5, 5]$的同时将系统输出控制到设定点$y^s = [0, 0]^{\mathrm{T}}$. 在控制器的设计过程中, 上述系统矩阵是不可用的. 首先, 以采样周期$T = 0.1$ s离线采集一条长度 $N = 100$的输入输出轨迹$\{u_t^d, y_t^d\}_{t=0}^{N-1}$, 其中$\{u_t^d\}_{t=0}^{N-1}$满足$L+\eta+n_x$阶持续激励性. 另外, 根据算法 1, 选择预测时域$L = 30$, $Q = 0.1I$, $R = 10^{-4}I$, $\lambda_g = 0.1$, $\lambda_h = 100$. 为了对 DoS 攻击进行仿真, 以概率$P_d = 0.8$产生一条服从伯努利分布的随机 DoS 攻击序列.

为表明所提出算法的控制性能, 利用文献 [25] 算法的无终端约束形式与文献 [20] 中的数据驱动 MPC 方案进行对比, 其中文献 [20] 中的算法在 DoS 攻击期间的控制输入$u = 0$. 另外, 为了更好地表明所提出数据驱动方法的优势, 利用基于模型的 MPC 与所提出算法进行对比, 其中基于模型的 MPC 算法采用的数学模型是基于相同的数据集通过系统辨识工具得到的, 而在弹性策略上, 依然采用算法 1 中的补偿方法. 图 2 ∼ 图 4 比较了各算法在不同噪声边界和 DoS 攻击最大持续时间下的性能. 首先, 由图 2 观察得到: 当噪声边界和 DoS 攻击最大持续时间均处于较低水平时, 即$\bar{v} = 0.01$和$\bar{l} = 15$时, 所提出算法与文献 [25] 提出的算法性能相当, 能够快速收敛至设定点y^s. 基于模型的 MPC 算法由于采用的数学模型精度不高, 在 DoS 攻击期间出现较大的偏差,

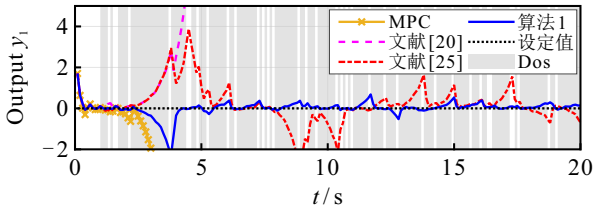


(a) y_1输出曲线

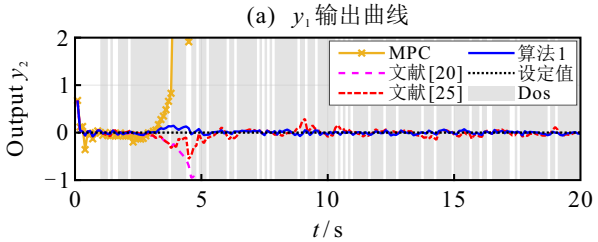


(b) y_2输出曲线

图2 DoS 攻击下系统输出: $\bar{v} = 0.01, \bar{l} = 15$

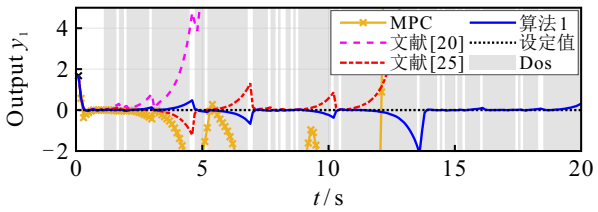


(a) y_1输出曲线

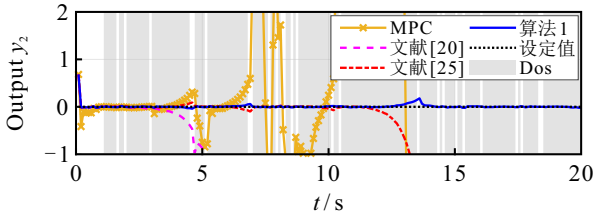


(b) y_2输出曲线

图3 DoS 攻击下系统输出: $\bar{v} = 0.05, \bar{l} = 15$



(a) y_1输出曲线



(b) y_2输出曲线

图4 DoS 攻击下系统输出: $\bar{v} = 0.01, \bar{l} = 30$

另外, 由于文献 [20] 的算法无弹性措施, DoS 攻击对系统造成的影响较大以至于系统输出在 DoS 攻击期间发散.

当噪声边界增加, DoS 攻击最大持续时间不变时, 由图 2 与图 3 的对比可以看出: 由于噪声水平的增加, 文献 [25] 提出的算法在 DoS 攻击期间出现较大偏差, 且在成功传输数据时也无法快速收敛至设定点; 同时, 基于模型的 MPC 算法由于数学模型的不精确最终导致系统输出发散; 而所提出算法在 DoS 攻击期间相较于其他算法拥有更强的鲁棒性, 系统输出也不会过多地偏离设定点, 仍然能够保持系统稳定. 当噪声边界不变, DoS 攻击最大持续时间增加时, 由图 2 与图 4 的对比可见: 在 DoS 攻击持续时间较长期间, 文献 [25] 提出的算法的输出偏差逐渐提升, 最终导致系统输出发散, 即使成功传输时也无法收敛; 而所提出算法依然能够在较长的 DoS 攻击期间保持良好的控制性能. 因此, 可以看出所提出算法具有更强的抗 DoS 攻击能力和鲁棒性, 且在成功传输数据时具有更快的收敛速度.

4 结 论

本文探讨了在 DoS 攻击下未知 LTI 系统的控制问题, 提出了一种无终端约束的数据驱动弹性预测控制方案. 该算法不依赖系统矩阵, 而是通过分析系统输入输出数据来学习系统的行为模式, 并仅依靠系统历史输入输出数据来建立预测模型, 通过预测时域对 DoS 攻击造成丢失的数据进行补偿, 降低 DoS 攻击对系统造成的影响. 然后, 通过数学分析验证了有限噪声边界和 DoS 攻击时长对于系统鲁棒稳定性的影响, 并给出了系统稳定条件. 最后, 通过实验表明: 所提出方案在过程噪声以及网络诱导噪声的影响下, 能够保证系统的稳定性, 并在系统遭受 DoS 攻击时, 能够最大程度地保证系统有效运行.

参考文献 (References)

[1] Monostori L, Kádár B, Bauernhansl T, et al. Cyber-physical systems in manufacturing[J]. CIRP Annals, 2016, 65(2): 621-641.

[2] 黄帅, 孙棣华, 赵敏. T-CPS 下考虑人驾车行为影响的混行车辆协同控制[J]. 控制与决策, 2024, 39(5): 1424-1432.
(Huang S, Sun D H, Zhao M. Cooperative control of mixed vehicles considering influence of human-driven vehicles behavior under T-CPS[J]. Control and Decision, 2024, 39(5): 1424-1432.)

[3] Priyadarshini I, Kumar R, Tuan L M, et al. A new enhanced cyber security framework for medical cyber physical systems[J]. SICS Software-Intensive Cyber — Physical Systems, 2021, 35(3): 159-183.

[4] 叶丹, 靳凯净, 张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252.
(Ye D, Jin K J, Zhang T Y. A survey on security of cyber-physical systems under network attacks[J]. Control and Decision, 2023, 38(8): 2243-2252.)

[5] Mahmoud M S, Hamdan M M, Baroudi U A. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges[J]. Neurocomputing, 2019, 338: 101-115.

[6] Kim S, Park K J, Lu C Y. A survey on network security for cyber-physical systems: From threats to resilient design[J]. IEEE Communications Surveys & Tutorials, 2022, 24(3): 1534-1573.

[7] 孙洪涛, 彭晨, 王志文. DoS 攻击下的信息物理系统事件触发预测控制设计[J]. 控制与决策, 2019, 34(11): 2303-2309.
(Sun H T, Peng C, Wang Z W. Event-triggered predictive control of cyber-physical systems under DoS attacks[J]. Control and Decision, 2019, 34(11): 2303-2309.)

[8] Zhang L J, Chen Y, Li M. Resilient predictive control for cyber-physical systems under denial-of-service attacks[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(1): 144-148.

[9] Yang H J, Xu H, Xia Y Q, et al. Stability analysis on networked control systems under double attacks with predictive control[J]. International Journal of Robust and Nonlinear Control, 2020, 30(4): 1549-1563.

[10] Kouvaritakis B, Cannon M. Model predictive control[J]. Springer International Publishing, 2016, 38: 13-56.

[11] Hou Z S, Wang Z. From model-based control to data-driven control: Survey, classification and perspective[J]. Information Sciences, 2013, 235: 3-35.

[12] Verheijen P C N, Breschi V, Lazar M. Handbook of linear data-driven predictive control: Theory, implementation and design[J]. Annual Reviews in Control, 2023, 56: 100914.

[13] Liu S L, Niu B, Zong G D, et al. Data-driven-based event-triggered optimal control of unknown nonlinear systems with input constraints[J]. Nonlinear Dynamics, 2022, 109(2): 891-909.

[14] Brüggemann S, Possieri C. On the use of difference of log-sum-exp neural networks to solve data-driven model predictive control tracking problems[J]. IEEE Control Systems Letters, 2021, 5(4): 1267-1272.

[15] 李耀华, 赵承辉, 周逸凡, 等. 基于数据驱动的永磁同步电机深度神经网络控制[J]. 电机与控制学报, 2022, 26(1): 115-125.
(Li Y H, Zhao C H, Zhou Y F, et al. Deep neural network control for PMSM based on data drive[J]. Electric Machines and Control, 2022, 26(1): 115-125.)

[16] Favoreel W, de Moor B, Gevers M. SPC: Subspace predictive control[J]. IFAC Proceedings Volumes, 1999, 32(2): 4004-4009.

[17] Coulson J, Lygeros J, Dörfler F. Data-enabled predictive control: In the shallows of the DeePC[C]. Proceedings of

the 18th European Control Conference. Naples, 2019: 307-312.

[18] Lazar M, Verheijen P C N. Generalized data-driven predictive control: Merging subspace and Hankel predictors[J]. Mathematics, 2023, 11(9): 2216.

[19] Berberich J, Köhler J, Müller M A, et al. Data-driven model predictive control with stability and robustness guarantees[J]. IEEE Transactions on Automatic Control, 2021, 66(4): 1702-1717.

[20] Bongard J, Berberich J, Köhler J, et al. Robust stability analysis of a simple data-driven model predictive control approach[J]. IEEE Transactions on Automatic Control, 2023, 68(5): 2625-2637.

[21] Wang Z M, Liu K Z, Wen S X, et al. Data-driven switched model predictive control without terminal ingredients[J]. IEEE Transactions on Automation Science and Engineering, 2024, 21(3): 4247-4260.

[22] Liu W J, Sun J, Wang G, et al. Data-driven self-triggered control via trajectory prediction[J]. IEEE Transactions on Automatic Control, 2023, 68(11): 6951-6958.

[23] Elokda E, Coulson J, Beuchat P N, et al. Data-enabled predictive control for quadcopters[J]. International Journal of Robust and Nonlinear Control, 2021, 31(18): 8916-8936.

[24] Wang J W, Zheng Y, Li K Q, et al. DeeP-LCC: Data-enabled predictive leading cruise control in mixed traffic flow[J]. IEEE Transactions on Control Systems Technology, 2023, 31(6): 2760-2776.

[25] Liu W J, Sun J, Wang G, et al. Data-driven resilient predictive control under denial-of-service[J]. IEEE Transactions on Automatic Control, 2023, 68(8): 4722-4737.

[26] Willems J C, Rapisarda P, Markovsky I, et al. A note on persistency of excitation[J]. Systems & Control Letters, 2005, 54(4): 325-329.

[27] Yang H J, Li Y, Dai L, et al. MPC-based defense strategy for distributed networked control systems under DoS attacks[J]. Systems & Control Letters, 2019, 128: 9-18.

[28] Befekadu G K, Gupta V, Antsaklis P J. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies[J]. IEEE Transactions on Automatic Control, 2015, 60(12): 3299-3304.

[29] Cai C H, Teel A R. Input-output-to-state stability for discrete-time systems[J]. Automatica, 2008, 44(2): 326-336.

作者简介

任清爽 (2001−), 男, 硕士生, 主要研究方向为模型预测控制、数据驱动控制理论及应用, E-mail: renqingshuang@yeah.net;

陈珺 (1980−), 女, 副教授, 博士, 主要研究方向为模糊控制理论及应用、复杂系统建模及应用, E-mail: chenjun1860@126.com;

刘飞 (1965−), 男, 教授, 博士, 主要研究方向为过程控制、智能装备与控制系统, E-mail: fliu@jiangnan.edu.cn.