DoS 攻击下的自适应事件触发数据驱动预测控制

任清爽，陈 珺†，闻继伟，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: 研究了未知信息物理系统在 DoS 攻击下的自适应事件触发数据驱动预测控制问题. 针对传统事件触发机制在 DoS 攻击下易丢失关键数据的缺陷, 提出引入动态补偿因子的自适应事件触发机制, 通过指数衰减特性量化攻击持续时间对触发阈值的影响, 实现资源开销和控制性能之间的平衡. 另外, 结合 Willems 基本引理, 利用离线数据直接构建预测控制器, 通过优化问题求解预测序列以补偿 DoS 攻击带来的影响. 在理论上, 证明了自适应事件触发机制下无终端约束的多步控制的迭代可行性, 并推导出系统稳定条件. 最后, 以开环不稳定反应器为例, 在 DoS 攻击和噪声干扰共存的环境下, 充分验证了所提方法的有效性与鲁棒性.

关键词: 不确定系统；DoS 攻击；自适应事件触发机制；数据驱动控制；预测控制

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2025.1232

引用格式: 任清爽, 陈珺, 闻继伟, 等. DoS 攻击下的自适应事件触发数据驱动预测控制 [J]. 控制与决策, xxxx, x(x): xxxx-xxxx.

Adaptive event-triggered data-driven predictive control under DoS attacks

REN Qing-shuang，*CHEN Jun*†，*WEN Ji-wei*，*LIU Fei*

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

Abstract: This paper investigates the problem of adaptive event-triggered data-driven predictive control for unknown cyber-physical systems subject to DoS attacks. To address the deficiency where traditional event-triggered mechanisms (ETM) are prone to losing critical data during DoS attacks, an adaptive ETM with a dynamic compensation factor is proposed. This mechanism quantifies the impact of attack duration on the triggering threshold via exponential decay characteristics, thereby achieving a balance between communication resource consumption and control performance. Furthermore, by combining Willems' fundamental lemma, a predictive controller is constructed directly using offline data. The prediction sequence is obtained by solving an optimization problem to actively compensate for the adverse effects of DoS attacks. Theoretically, the recursive feasibility of the multi-step control without terminal constraints under the proposed adaptive ETM is proven, and the sufficient conditions for system stability are derived. Finally, using an open-loop unstable reactor as a benchmark, the effectiveness and robustness of the proposed method are rigorously verified in an environment where DoS attacks and noise disturbances coexist.

Keywords: uncertain systems； DoS attacks； adaptive event-triggered mechanism； data-driven control； predictive control

0 引 言

信息物理系统 (Cyber-Physical Systems, CPS) 作为计算单元与物理过程深度集成的智能化载体, 正深刻变革工业自动化[1]、智能电网[2] 及无人系统[3] 等关键领域. 然而, CPS 的广泛应用也伴随着诸多的技术挑战. 首先是网络安全问题尤为突出, 由于 CPS 利用开放的网络进行通讯, 使得网络攻击 (如数据篡改、拒绝服务攻击 (Denial of service, DoS)、重放攻击) 不仅威胁信息保密性, 更能直接转化为对系统的实质性危害. 其次, 由于网络信道资源的受限, CPS 通常依赖大规模分布的传感器、执行器和控制器进行数据交换与协同工作. 有限的网络带宽以及不同

收稿日期: 2025-11-28；**录用日期:** 2026-03-03.
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

设备间的资源竞争, 严重制约了关键数据的实时性和可靠传输, 尤其在工业控制或自动驾驶等对时效性要求极高的场景下, 可能导致系统性能下降甚至引发安全事故[4]. 因此, 构建一个既高效又安全的CPS网络架构已成为当今研究的一个热点, 同时有效解决资源约束与网络安全的问题, 是保障CPS可靠运行和持续发展的关键.

关于网络安全方面, 本文主要讨论DoS攻击的影响. 相较于其他攻击, DoS无需侵入系统内部或破解加密机制, 仅凭海量无效信息即可对系统造成破坏, 具备低技术门槛与高攻击效率[5]. 在CPS环境中, DoS攻击会通过洪泛流量直接瘫痪网络信道, 瓦解CPS赖以运行的信息-物理实时交互闭环[6]. 因此, 在资源受限的CPS环境下, 如何有效抑制DoS攻击的影响并确保系统鲁棒性, 是当前亟待突破的目标. 文献 [7] 利用DoS攻击的频率和持续时间来建立DoS攻击模型, 并分析了闭环系统的输入状态稳定性. 文献 [8] 和文献 [9] 则利用模型预测控制 (MPC) 的预测时域特性, 在DoS攻击期间对系统进行补偿, 以减弱DoS攻击对系统造成的不利影响. 文献 [10] 则避免了MPC建模困难的缺点, 设计了一种弹性数据驱动预测控制方法, 且提出的数据驱动控制方法与基于模型的控制方法具有相近的弹性水平.

除此之外, 为了提高系统的效率和减少资源消耗, 事件触发控制 (Event-triggering mechanism, ETM) 被广泛的应用到CPS中. 传统的时间触发控制 (Time-triggered mechanism, TTM) 是固定周期执行, 会在系统状态平稳时产生大量冗余通信和无效计算, 导致资源浪费. 相比之下, ETM摒弃了固定的时间周期, 转而依据系统运行的实际状态来动态决定何时需要进行采样、传输或控制计算. 相较于TTM的固定周期调度, ETM通过抑制非必要操作, 显著降低通信负载和控制器计算开销, 同时维持闭环系统稳定性[11]. 通过ETM来减少资源消耗已经得到了广泛的研究[12-14], 文献 [12] 在传统的TTM和ETM之间取得平衡, 提出了一种周期性ETM. 文献 [13] 提出了一种基于记忆的ETM, 利用历史信号序列提升控制性能, 突破了传统ETM的设计范式. 文献 [14] 则提出了一种数据驱动的事件触发控制方案. 然而, ETM的高效性恰成其受DoS攻击时的致命弱点, 该机制本身滤除冗余信息, 而传输的均为相对有价值的数据. 一旦遭受DoS攻击, 关键事件信息丢失将导致系统迅速恶化, 此时资源节约优势反加剧安全风险. 因此, 在ETM框架下设计鲁棒的DoS防御策略, 已成为CPS安全的重要研究领域[15-17].

上述研究大多依赖明确的模型参数. 然而对于复杂系统, 精确建模十分困难, 数据采集则相对容易. 针对模型未知的控制问题, 现在主流的方法有无模型自适应控制 (MFAC)[18] 和基于学习的MPC[19] 等. MFAC利用动态线性化技术处理非线性系统, 机器学习的方法则擅长处理高维复杂映射. 然而, 与上述方法相比, 最近提出的一种基于Willems基本引理的数据驱动控制方法具有独特的理论优势[20-22], 它无需在线估计参数或进行大规模训练, 而是利用离线数据直接构建预测控制器. 这使得该方法天然契合MPC框架. 尽管如此, 现有的数据驱动MPC研究大多只关注单一目标, 要么仅考虑抗DoS攻击的安全性, 要么仅通过ETM节约资源. 针对模型未知CPS, 目前很少有研究能同时解决网络安全威胁和信道资源受限这两个问题.

本文研究的目标是设计一种DoS攻击下的自适应事件触发数据驱动预测控制, 主要贡献如下: (1) 提出了一种引入动态补偿因子的DoS攻击下自适应事件触发机制 (AETM), 能够在DoS攻击发生时动态调整事件触发阈值. (2) 在考虑测量噪声和过程噪声下仅利用系统的输入输出数据构建事件触发预测控制器, 并通过优化问题求解预测序列以补偿DoS攻击影响. (3) 证明了引入AETM的多步控制迭代可行性和稳定性, 并给出了稳定性条件.

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

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

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. 矩阵A、B、C和D是具有适当维度的常数矩阵, 这些矩阵被假定是未知的, 但离线收集的输入输出轨迹$\{u_t^d,\tilde{y}_t^d\}_{t=0}^{N-1}$能够被收集, 其中$\tilde{y}_t^d:=y_t^d+n_t$, n_t为测量噪声. 关于系统$\mathcal{S}$有如下假设:

假设 1 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.

假设 2 假设过程噪声w_t和测量噪声n_t是有界的, 即满足$\bar{v}:=max\{\|w_t\|,\|n_t\|\},t\in\mathbb{N}_+$, 其中$\bar{v}$是一个常数.

假设系统$\mathcal{S}$通过网络进行控制, 并且DoS攻击会影响传感器-控制器 (S/C) 通道, 且认为攻击发生时, S/C通道完全阻塞. 在任一时刻t, 传感器会采集当前时刻的输出测量值$\tilde{y}_t$并传输到事件触发器; 事

件触发器会存储前n_x时刻的测量值, 即$\tilde{y}_{[t-n_x,t-1]}$, 当事件触发器的触发条件成立时, 事件触发器会通过 S/C 通道发送$\tilde{y}_{[t-n_x,t-1]}$到控制器, 所构成的系统框图如图 1 所示.

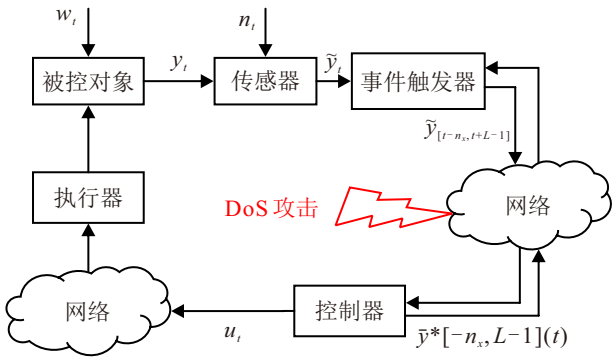


图1　网络控制系统框图

注 1　本文重点讨论 S/C 通道的 DoS 攻击问题. 在实际 CPS 中, 传感器节点通常因分布广泛而更易受攻击. 此外, 针对 C/A 通道的 DoS 攻击可被建模为控制输入数据的丢失, 其补偿机制与 S/C 通道的数据丢失处理在理论上具有相似性. 为简便起见, 本文主要针对 S/C 通道受攻击情况进行分析, 该框架可推广至双通道受攻击的场景.

为了利用离线收集的数据直接建立控制器, 接下来引入 Willems 基本引理. 定义 Hankel 矩阵如下:

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

定义 1　[23] 对于一个序列$\{u_t\}_{t=0}^{N-1}$, $u_t \in \mathbb{R}^{n_u}$, 如果$rank(H_L(u)) = n_u L$, 则称$\{u_t\}_{t=0}^{N-1}$是L阶持续激励的.

引理 1　[23] 假设$\{u_t^d, y_t^d\}_{k=0}^{N-1}$是 LTI 系统的一条输入输出轨迹, 且被测输入序列$\{u_t^d\}_{k=0}^{N-1}$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

$$\begin{bmatrix} H_L(u^d) \\ H_L(y^d) \end{bmatrix} g = \begin{bmatrix} \bar{u}_t \\ \bar{y}_t \end{bmatrix}. \tag{2}$$

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

在本文的研究情境中, 当 DoS 攻击发生时, 通信资源将被完全占用, 此时 S/C 通信链路彻底中断, 无法进行任何信息传输. 为了更精确地对 DoS 攻击进行建模和分析, 本文利用攻击频率和持续时间这两个关键参数来描述 DoS 攻击行为[7,10]. 定义布尔变量l_t表示在t时刻是否发生 DoS 攻击, 即

$$l_t = \begin{cases} 1, & \text{在}t\text{时刻发生DoS攻击}, \\ 0, & \text{在}t\text{时刻未发生DoS攻击}. \end{cases} \tag{3}$$

基于此, DoS 攻击在$[t_1, t_2)$时间内的持续时间可以描述为$\Phi_d(t_1,t_2) := \sum_{t=t_1}^{t_2-1} l_t$. 为了进一描述 DoS 攻击的频率特征, 定义布尔变量d_t如下

$$d_t = \begin{cases} 1, & l_t = 1\text{且}l_{t-1} = 0, \\ 0, & \text{其他}. \end{cases} \tag{4}$$

由此 DoS 攻击在$[t_1, t_2)$时间内的发生频率可以描述为$\Phi_f(t_1,t_2) := \sum_{t=t_1}^{t_2-1} d_t$. 从实际应用场景出发, 攻击者的能量资源并非无穷无尽, 这就意味着连续 DoS 攻击的次数必然存在上限.

假设 3　假设连续 DoS 攻击的持续时间ℓ最长不超过$\bar{\ell}$, 即$\ell \leqslant \bar{\ell}$, 其中$\bar{\ell} \in \mathbb{N}_+$.

2　控制器设计及稳定性分析

在本节中, 首先设计了 DoS 攻击下的 AETM. 然后, 利用 Willmes 的基本引理和预先收集的数据, 直接构造基于 AETM 的数据驱动预测控制器. 最后, 证明了该控制器的迭代可行性和稳定性, 并给出了稳定性条件.

2.1　自适应事件触发机制

虽然 ETM 能够显著降低网络和控制器资源消耗, 但数据传输触发瞬间可能会遭受 DoS 攻击, 导致传输的数据丢失, 如图 2 所示. 记t_k为事件触发器第k次触发的时刻, r_k表示事件触发器第k次触发和第$k+1$次触发的时间间隔, 即$r_k := t_{k+1} - t_k$. 同理记t_p为控制器第p次调度的时刻, 相应的h_p表示控制器第p次调度和第$p+1$次调度的时间间隔即, $h_p := t_{p+1} - t_p$, 其中$k, p \in \mathbb{N}_+$. 由于控制器需接收数据后执行调度, 因此有$\{t_p\}_{p=1}^{\infty} \subseteq \{t_k\}_{k=1}^{\infty}$. 令$t_p = t_k$, 记$\ell_p$表示在$[t_p, t_{p+1})$时间内 DoS 攻击的持续时间, 即$\ell_p := \Phi_d(t_p, t_{p+1})$.

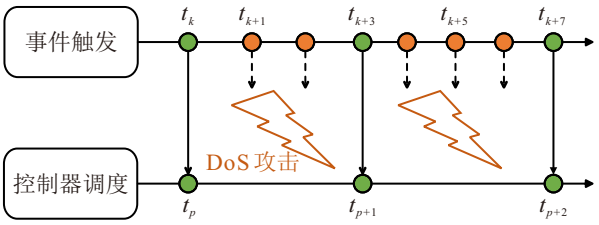


图2　DoS 攻击下数据传输时序图

本文在文献 [14] 的基础上, 引入动态因子$\eta(r)$, $\eta(r)$可以将 DoS 攻击对系统输出的累积影响量化为触发条件下的权重系数, 以此实现自适应调节事件触发阈值. 本文构造的 AETM 如下

$$t_{k+1}=t_k+r_k,$$
$$r_k=\min\{r\in\mathbb{N}_{[1,M]}|\|\tilde{y}_{[t_k,t_k+r-1]}\|^2-\|\bar{y}^*_{[0,r-1]}(t_k)\|^2\geqslant\eta(r)(c_1\bar{v}^2+c_2\|\bar{y}^*_{r-1}(t_k)\|^2)-2\sqrt{r}\bar{v}\|\tilde{y}_{[t_k,t_k+r-1]}\|\}. \quad (5)$$

其中$\bar{y}^*(t)$表示预测控制器产生的预测序列, $M\in\mathbb{N}_+$表示事件触发器的最长触发间隔, $c_1,c_2>0$, $\eta(r)$定义如下

$$\eta(r):=\eta_0+(\eta_1-\eta_0)e^{-c_3\|\tilde{y}_{[t_k,t_k+r-1]}-\bar{y}^*_{[0,r-1]}(t_k)\|}.$$

其中$0\leqslant\eta_0\leqslant\eta_1<1, c_3>0$.

根据图 2 的示意, 结合公式 (5) 的 AETM 和假设 3, 能够得知控制器相邻调度时刻的间隔满足$1\leqslant h_p\leqslant M+\bar{\ell}$.

2.2 控制器设计

考虑从系统$\mathcal{S}$采集的 I/O 轨迹$\{u_N^d,\tilde{y}_N^d\}:=\{u_t^d,\tilde{y}_t^d\}_{t=0}^{N-1}$, 其中输入序列$u_N^d$具有$L+2n_x$阶持续激励性. 结合 AETM, 给定历史窗口$u_{[t_p-n_x,t_p-1]}$, $\tilde{y}_{[t_p-n_x,t_p-1]}$, 以预测时域$L$构建的优化问题为:

$$J_L^*(u_{[t_p-n_x,t_p-1]},\tilde{y}_{[t_p-n_x,t_p-1]}):=\min_{g,\bar{u},\bar{y},\sigma}\sum_{j=0}^{L-1}l(\bar{u}_j(t_p),\bar{y}_j(t_p))+\lambda_g\bar{v}\|g(t_p)\|^2+\frac{\lambda_\sigma}{\bar{v}}\|\sigma(t_p)\|^2$$

$$\text{s.t.}\ \begin{bmatrix}H_{L+n_x}(u_N^d)\\H_{L+n_x}(\tilde{y}_N^d)\end{bmatrix}g(t_p)=\begin{bmatrix}\bar{u}(t_p)\\\bar{y}(t_p)+\sigma(t_p)\end{bmatrix} \quad (6a)$$

$$\begin{bmatrix}\bar{u}_{[-n_x,-1]}(t_p)\\\bar{y}_{[-n_x,-1]}(t_p)\end{bmatrix}=\begin{bmatrix}u_{[t_p-n_x,t_p-1]}\\\tilde{y}_{[t_p-n_x,t_p-1]}\end{bmatrix} \quad (6b)$$

$$\bar{u}_j(t_p)\in\mathbb{U},\ k\in[0,L-1]. \quad (6c)$$

其中$p\in\mathbb{N}_+$, $(\bar{u},\bar{y})$为$L+n_x$步预测轨迹, 其中前n_x步$\{\bar{u}_{[-n_x,-1]}(t_p),\bar{y}_{[-n_x,-1]}(t_p)\}$表示系统在$t_p$时刻的初始状态. 另外$l(\bar{u},\bar{y})$是一个关于人工平衡点$(u^s,y^s)$的二次惩罚项, 有

$$l(\bar{u},\bar{y}):=\|\bar{u}-u^s\|_R^2+\|\bar{y}-y^s\|_Q^2. \quad (7)$$

其中权重矩阵R、$Q\succ0$. 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. 另外在无事件触发间隔内或 DoS 攻击持续期间内, 控制器将利用上一次触发得到的预测输入序列$\bar{u}_{t-t_p}(t_p)$来进行输出, 即

$$u_t=\begin{cases}\bar{u}_0^*(t_p),\ t\in\{t_p\}_{p=0}^\infty,\\\bar{u}^*_{t-t_p}(t_p),\ t\notin\{t_p\}_{p=0}^\infty,\end{cases} \quad (8)$$

其中$\bar{u}^*(t_p)$表示t_p时刻优化问题的最优. 为了简化稳定性分析, 在优化问题 (6) 中只考虑输入约束.

结合 AETM 和 DoS 攻击补偿措施, 本文提出针对 DoS 攻击的自适应事件触发数据驱动 MPC 算法如下:

算法 1 自适应事件触发数据驱动 MPC

离线运行阶段:

step 1: 采集满足持续激励条件的输入输出轨迹$\{u_N^d,y_N^d\}$;

step 2: 选择合适的参数M, c_1, c_2, $c_3>0$, Q, $R\succ0$, $\lambda_g>0$, $\lambda_\sigma>0$;

在线运行阶段:

step 1: if $t\in\{t_p\}_{p=0}^\infty$ then

step 2: 使用$\{u_{[t-n_x,t-1]},\tilde{y}_{[t-n_x,t-1]}\}$求解优化问题 (6), 令$u_t=\bar{u}_0^*(t)$

step 3: else if $t\notin\{t_p\}_{p=0}^\infty$ then

step 4: 令$u_t=\bar{u}^*_{t-t_p}(t_p)$

step 5: end if

step 6: 令$t=t+1$, 回到 step1

2.3 稳定性证明

首先定义系统$\mathcal{S}$的扩展状态为

$$\xi_t=\begin{bmatrix}u_{[t-n_x,t-1]}\\y_{[t-n_x,t-1]}\end{bmatrix}. \quad (9)$$

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$\tilde{\xi}_t:=[u_{[t-n_x,t-1]};\tilde{y}_{[t-n_x,t-1]}]$. 接下来构造李雅普诺夫函数如下

$$V_L(\xi_t)=J_L^*(\tilde{\xi}_t)+W(\xi_t). \quad (10)$$

其中$W(\xi_t):=\|\xi_t\|_P^2$是一个 IOSS 李雅普诺夫函数[21], $P\succ0$, 且存在一个常数ϵ_0满足

$$W(\xi_{t+1})\leqslant W(\xi_t)+\|u_t\|_R^2+\|y_t\|_Q^2-\epsilon_0\|\xi_t\|^2. \quad (11)$$

引理 2 [10] 考虑具有算法 1 中的控制器的系统$\mathcal{S}$, 如果优化问题 (6) 在t_p时刻是可行的, 且$J_L^*(\tilde{\xi})\leqslant\bar{J}$, 则预测误差$e_q^y(t_p)=y_{t_p+q}-\bar{y}_q^*(t_p)$满足:

$$\|e_q^y(t_p)\|^2\leqslant\beta(\bar{v},q),q\in N_{[0,L-1]}, \quad (12)$$

其中$\beta(\bar{v},q)\in\mathcal{KL}$.

引理 3 假设问题 (6) 在t_p时刻是可行的, $p\in\mathbb{N}$, u_N^d是$L+2n_x$阶持续激励的, 且$V_L(\xi_{t_p})\leqslant\bar{V}$, 则存在函数$\alpha_1(\bar{v})$和$\alpha_2(\bar{v})$使得

$$V_{L-h_p}(\xi_{t_{p+1}})\leqslant V_L(\xi_{t_p})-\epsilon_0\|\xi_{t_p}\|^2+\alpha_1(\bar{v}), \quad (13)$$

$$\underline{\lambda}(P)\|\xi_{t_p}\|^2\leqslant V_L(\xi_{t_p})\leqslant\bar{\gamma}\|\xi_{t_p}\|^2+\alpha_2(\bar{v}), \quad (14)$$

其中$h_p:=t_{p+1}-t_p$, $\epsilon_0>0$, $\alpha_1(\bar{v}),\alpha_2(\bar{v})\in\mathcal{K}_\infty$, $\bar{\gamma}$是一个常数, $\underline{\lambda}(P)$表示矩阵P的最小奇异值.

证明 该引理是文献 [21] 的引理 3 的一种多步扩展, 本文考虑了过程噪声w_t, 同时将文献 [21] 引

理 3 扩展成为n步, 证明步骤与其类似, 主要区别在于构造可行解有所不同, 而构造可行解的思路与定理 1 的证明思路类似, 因此该定理的证明过程省略.

定理 1　假设u_N^d是$L+2n_x$阶持续激励的且$V_L(\xi_{t_p})\leqslant\bar{V}$, 那么存在常数$\underline{L},\bar{v}_L\geqslant 0$对于任意的预测时域$L>\underline{L}$和噪声边界$\bar{v}_L\geqslant\bar{v}\geqslant 0$, 如果问题 (6) 在$t_0$时刻是可行的, 那么在任意时刻$t_p\geqslant 0$都是可行的, $p\in\mathbb{N}_+$, 且李雅普诺夫函数$V_L(\xi_{t_p})$满足:

$$V_L(\xi_{t_{p+1}})\leqslant\alpha_L V_L(\xi_{t_p})+\alpha_3(\bar{v}). \tag{15}$$

其中$0<\alpha_L<1$, $\alpha_3(\bar{v})$关于$\bar{v}$单调递增.

证明　令x_N^d,w_N^d,n_N^d为与采集轨迹$(u_N^d,\tilde{y}_N^d)$对应的状态及噪声序列. 记$(\bar{u}^*,\bar{y}^*,\bar{g}^*,\bar{\sigma}^*)$与$(\bar{u},\bar{y},\bar{g},\bar{\sigma})$分别为优化问题$J_{L-h_p}(\tilde{\xi}_{t_{p+1}})$的最优解与可行解. 结合公式 (6a) 和 (6b), 定义优化问题$J_{L-h_p}(\tilde{\xi}_{t_{p+1}})$不含测量噪声的初始条件为

$$\xi_0(t_{p+1})=\begin{bmatrix}\bar{u}^*_{[-n_x,-1]}(t_{p+1})\\ \tilde{y}_{[t_{p+1}-n_x,t_{p+1}-1]}\end{bmatrix}+\begin{bmatrix}0\\ \bar{\sigma}^*_{[-n_x,-1]}(t_{p+1})\end{bmatrix}-\begin{bmatrix}0\\ H_{L+n_x-h_p}(n^d_{N-h_p})\bar{g}^*(t_{p+1})\end{bmatrix}. \tag{16}$$

根据公式 (1) 的扩展, 考虑在输入序列$\bar{u}_j=\bar{u}_j^*$作用下, 将实际系统输出作为可行解$\bar{y}_j(t_{p+1})$有

$$\bar{y}_j(t_{p+1})=\tilde{C}\tilde{A}^j\xi_{t_{p+1}}+\tilde{C}\sum_{i=0}^{j-1}(\tilde{A}^i\tilde{B}\bar{u}_{j-i-1}(t_{p+1})+\tilde{A}^i\tilde{E}w_{t_{p+1}+j-i-1})+\tilde{D}\bar{u}_j(t_{p+1}). \tag{17}$$

其中$j\in\mathbb{N}_{[0,L-h_p-1]}$, 矩阵$\tilde{A},\tilde{B},\tilde{C},\tilde{D},\tilde{E}$表示系统$\mathcal{S}$以$\xi_t$为扩展状态的系统矩阵. 然后利用公式 (6a), 最优解$\bar{y}_j^*(t_{p+1})$可以表示为

$$\bar{y}_j^*(t_{p+1})=\tilde{C}\tilde{A}^j\xi_0(t_{p+1})+\tilde{C}\sum_{i=0}^{j-1}\tilde{A}^i\tilde{B}\bar{u}^*_{j-i-1}(t_{p+1})+\tilde{D}\bar{u}_j^*(t_{p+1})-\bar{\sigma}_j^*(t_{p+1})+H_{L+n_x-h_p}(n^d_{N-h_p})\bar{g}^*(t_{p+1}). \tag{18}$$

结合公式 (13) 和公式 (14) 可得$J_{L-\gamma_p}(\tilde{\xi}_{t_{p+1}})\leqslant\bar{V}+\alpha_1(\bar{v})$, 因此可以得到$\|\bar{g}^*(t_{p+1})\|$和$\|\bar{\sigma}^*(t_{p+1})\|$的上界为

$$\|\bar{\sigma}^*(t_{p+1})\|\leqslant\sqrt{\bar{v}(\bar{V}+\alpha_1(\bar{v}))/\lambda_\sigma}:=\delta^\sigma(\bar{v}), \tag{19}$$

$$\|\bar{g}^*(t_{p+1})\|\leqslant\sqrt{(\bar{V}+\alpha_1(\bar{v}))/\bar{v}\lambda_g}:=\delta^g(\bar{v}). \tag{20}$$

然后将上述公式代入到 (16) 中有

$$\|\xi_{t_{p+1}}-\xi_0(t_{p+1})\|\leqslant\delta^\xi(\bar{v}), \tag{21}$$

其中

$$\delta^\xi(\bar{v}):=\bar{v}\sqrt{n_x}+\sqrt{(N-L-n_x+h_p+1)n_x}\bar{v}\delta^g(\bar{v})+\delta^\sigma(\bar{v}).$$

利用可行解 (17) 减去最优解 (18), 并结合 (19)、(20) 和 (21), 可以得到

$$\|\bar{y}_j(t_{p+1})-\bar{y}_j^*(t_{p+1})\|_Q\leqslant\sqrt{\bar{\lambda}(Q)}(c(j)\delta^\xi(\bar{v})+\sqrt{(N-L-n_x+h_p+1)n_x}\bar{v}\delta^g(\bar{v})+\delta^\sigma(\bar{v})+\sum_{i=0}^{j-1}c(i)\|\tilde{E}\|\bar{v})=:\delta_j^y(\bar{v}), \tag{22}$$

其中$c(j):=\|\tilde{C}\tilde{A}^j\|,\delta_j^y(\bar{v})\in\mathcal{K}_\infty$. 接下来根据公式 (11) 迭代, 利用不等式$\|a+b\|^2\leqslant\|a\|^2+\|b\|^2+2\|a\|\|b\|$可得

$$W(\xi_{t_{p+1}+L-h_p})-W(\xi_{t_{p+1}})\leqslant-\epsilon_0\sum_{j=0}^{L-h_p-1}\|\xi_{t_{p+1}+j}\|^2+J^*_{L-h_p}(\tilde{\xi}_{t_{p+1}})+\alpha_4(\bar{v}), \tag{23}$$

其中$\alpha_4(\bar{v}):=\sum_{j=0}^{L-h_p-1}\delta_j^y(\bar{v})^2+2\delta_j^y(\bar{v})\sqrt{\bar{V}+\alpha_1(\bar{v})}$. 由于$W(\xi)>0$, 结合 (13) 可以得到

$$\epsilon_0\sum_{j=0}^{L-h_p-1}\|\xi_{t_{p+1}+j}\|^2\leqslant V_{L-h_p}(\xi_{t_{p+1}})+\alpha_4(\bar{v})\leqslant V_L(\xi_{t_p})-\epsilon_0\|\xi_{t_p}\|^2+\alpha_5(\bar{v}), \tag{24}$$

其中$\alpha_5(\bar{v}):=\alpha_4(\bar{v})+\alpha_1(\bar{v})$. 根据上式可得, 存在一个常数$j_x\in N_{[0,L-h_p-1]}$, 满足如下

$$\|\xi_{t_{p+1}+j_x}\|^2\leqslant\frac{V_L(\xi_{t_p})+\alpha_5(\bar{v})}{\epsilon_0(L-h_p)}\leqslant\frac{\bar{V}+C_\alpha}{\epsilon_0(L-\bar{\ell}-M)}, \tag{25}$$

其中C_α是一个常数, 满足$\alpha_5(\bar{v})\leqslant C_\alpha$. 根据上述公式可得, 只要预测时域长度$L$满足

$$L>\underline{L}_1:=\bar{\ell}+M+\frac{\bar{V}+C_\alpha}{\epsilon_0\delta^2} \tag{26}$$

则有$\|\xi_{t_{p+1}+j_x}\|^2\leq\delta^2$, 这意味着系统状态在有限步内收敛至目标集.

接下来证明李雅普诺夫函数$V(\xi)$的收敛性. 考虑到$j\in[j_x,L-1]$时$\|\xi_{t_{p+1}+j}\|\leqslant\delta$, 存在局部镇定控制器使得状态收敛, 且其产生的输入输出轨迹满足$\|(u,y)\|\leqslant\gamma_\xi\|\xi\|$. 因此, 可在$t_{p+1}$时刻构造如下候选输入序列

$$\bar{u}_{[-n_x,L-1]}(t_{p+1})=\begin{bmatrix}\bar{u}^*_{[-n_x+h_p,h_p+j_x-1]}(t_p)\\ u_{[t_{p+1}+j_x,t_{p+1}+L-1]}\end{bmatrix}. \tag{27}$$

相应的输出序列$\bar{y}$则由实际测量值与名义预测值拼接而成.

进而根据约束 (6a) 和 (6b), 对应的$\bar{g}(t_{p+1})$和$\bar{\sigma}(t_{p+1})$可唯一确定. 由于$\bar{g}$和$\bar{\sigma}$的构造过程与文献 [24] 的定理 2 类似, 可证该候选解满足所有约束条件, 故优化问题在t_{p+1}时刻递归可行. 基于上述可行

解, 并利用最优性原理$J^*(\xi_{t_{p+1}}) \leqslant \bar{J}(\xi_{t_{p+1}})$, 可推导出李雅普诺夫函数满足

$$V_L(\xi_{t_{p+1}}) \leqslant V_L(\xi_{t_p}) + \sum_{j=0}^{h_p-1}(\|y_{t_p+j}\|_Q^2 - \|\bar{y}_j^*(t_p)\|_Q^2) + (\frac{\bar{\lambda}(R,Q)\gamma_\xi^2\bar{\gamma}}{\epsilon_0(L-h_p)} - \epsilon_0)\|\xi_{t_p}\|^2 + \alpha_6(\bar{v}), \tag{28}$$

其中$\alpha_6(\bar{v}) \in \mathcal{K}_\infty$, $\bar{\lambda}(R,Q)$表示矩阵Q和R中最大奇异值.

接下来根据$t_{p+1}-1$时刻是否存在 DoS 攻击分两种情况进行讨论:

情况 1: $l_{t_{p+1}-1}=0$

当$t_{p+1}-1$时刻无 DoS 攻击发生时, 说明t_{p+1}时刻触发条件 (5) 成立, 但$t_{p+1}-1$时刻时触发条件 (5) 是违背的, 则有

$$\|\tilde{y}_{[t_p,t_p+h_p-2]}\|^2 - \|\bar{y}^*_{[0,h_p-2]}(t_p)\|^2 \leqslant \eta(h_p-1)(c_1\bar{v}^2 + c_2\|\bar{y}^*_{h_p-2}(t_p)\|^2) - 2\sqrt{h_p-1}\bar{v}\|\tilde{y}_{[t_p,t_p+h_p-2]}\|. \tag{29}$$

根据上述公式, 由于$\tilde{y}_t = y_t + n_t$, 利用三角不等式$\|a+b\|^2 \geqslant \|a\|^2 + \|b\|^2 - 2\|a\|\|b\|$和$\eta(r) \leqslant \eta_1$, 则有

$$\|y_{[t_p,t_p+h_p-2]}\|^2 - \|\bar{y}^*_{[0,h_p-2]}(t_p)\|^2 \leqslant \eta_1 c_2\bar{V}/\underline{\lambda}(Q) + (\eta_1 c_1 + h_p - 1)\bar{v}^2. \tag{30}$$

另外根据引理 2 有

$$\|y_{t_p+h_p-1}\|^2 - \|\bar{y}^*_{h_p-1}(t_p)\|^2 \leqslant \beta^2(\bar{v}, h_p-1) + 2\beta(\bar{v}, h_p-1)\sqrt{\bar{V}/\underline{\lambda}(Q)}. \tag{31}$$

结合公式 (30) 和 (31) 可以得到

$$\|y_{[t_p,t_p+h_p-1]}\|^2 - \|\bar{y}^*_{[0,h_p-1]}(t_p)\|^2 \leqslant \alpha_7(\bar{v}). \tag{32}$$

情况 2: $l_{t_{p+1}-1}=1$

当$t_{p+1}-1$时刻存在 DoS 攻击时, 假设此次 DoS 攻击的持续时间为ℓ, 即此次 DoS 攻击连续发生在$[t_{p+1}-\ell, t_{p+1}-1]$时间内, 则说明在$t_{p+1}-\ell-1$时刻触发条件 (5) 依然违背, 则类似情况 1 的推导可得

$$\|y_{[t_p,t_p+h_p-1]}\|^2 - \|\bar{y}^*_{[0,h_p-1]}(t_p)\|^2 \leqslant \alpha_8(\bar{v}). \tag{33}$$

将公式 (32) 和 (33) 代入到 (28) 有

$$V_L(\xi_{t_{p+1}}) \leqslant V_L(\xi_{t_p}) + (\frac{\bar{\lambda}(R,Q)\gamma_\xi^2\bar{\gamma}}{\epsilon_0(L-h_p)} - \epsilon_0)\|\xi_{t_p}\|^2 + \alpha_9(\bar{v}), \tag{34}$$

其中$\alpha_9(\bar{v}) := \max\{\alpha_8(\bar{v}), \alpha_7(\bar{v})\} + \alpha_6(\bar{v})$. 最后将公式 (14) 代入到上式中可以得到

$$V_L(\xi_{t_{p+1}}) \leqslant \alpha_L V_L(\xi_{t_p}) + \alpha_3(\bar{v}), \tag{35}$$

其中

$$\alpha_L := 1 - \frac{\epsilon_0}{\bar{\gamma}}(1 - \frac{\bar{\lambda}(R,Q)\gamma_\xi^2\bar{\gamma}}{\epsilon_0^2(L-\bar{\ell}-M)}), \tag{36}$$

$$\alpha_3(\bar{v}) := \frac{\epsilon_0}{\bar{\gamma}}(1 - \frac{\bar{\lambda}(R,Q)\gamma_\xi^2\bar{\gamma}}{\epsilon_0^2(L-\bar{\ell}-M)})\alpha_2(\bar{v}) + \alpha_9(\bar{v}). \tag{37}$$

为了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

$$L > \underline{L}_1 := \bar{\ell} + M + \frac{\bar{\lambda}(R,Q)\gamma_\xi^2\bar{\gamma}}{\epsilon_0^2}. \tag{38}$$

综上预测时域L应当满足

$$L > \underline{L} := max\{\underline{L}_0, \underline{L}_1\}. \tag{39}$$

同时为了确保$V(\xi_{t_p}) \leq \bar{V}$在迭代过程中成立, 因此要使$\alpha_3 \leqslant (1-\alpha_L)\bar{V}$成立, 则噪声边界$\bar{v}$需要满足$\bar{v} \leqslant \bar{v}_L$, 其中$\bar{v}_L$为

$$\bar{v}_L = min\{\alpha_3^{-1}((1-\alpha_L)\bar{V}), \alpha_5^{-1}(C_\alpha)\}. \tag{40}$$

满足上述条件则可以使系统稳定, 定理 1 得证. □

注 2 基于定理 1 的理论分析, 证明了保证闭环系统稳定性所需的预测时域下界$\underline{L}$的存在性. 该下界与噪声水平$\bar{v}$呈正相关关系, 即噪声水平越高, 所需的预测时域越长. 虽然该下界还依赖于系统矩阵的范数, 但这些范数可以基于采集的数据集进行粗略估计[25]. 由于稳定性证明过程存在保守放缩, 因此算法对估计精度的要求较为宽松, 可以为控制器的参数整定提供定性指导.

注 3 由定理 1 可知, 预测时域L的选取依赖于 DoS 攻击的最大持续时间上界$\bar{l}$, 该参数通常可以基于网络入侵检测系统 (IDS) 的历史流量日志分析获得. 考虑到极端恶劣情况下攻击时长可能超出预测时域L的风险, 为防止系统失控并确保物理安全, 可以在执行器端引入故障安全机制, 超出预算时域的部分可以采取零输入$u_t=0$或零阶保持 (ZOH), 直至通信恢复.

3 仿真实验

在本节, 本文将自适应事件触发数据驱动预测控制算法应用到一个反应器示例[10] 中. 该示例是开环不稳定的, 其连续系统的系统矩阵如下

$$A = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix}$$

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

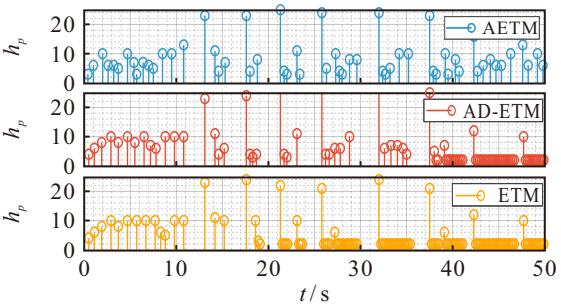
$$D = 0$$

对上述系统的控制目标是在满足输入约束$u_t \in \mathbb{U} = [-20, 20]$的同时将系统输出控制到设定点$y^s = [0, 0]^T$. 在控制器的设计过程中, 上述系统矩阵是不可用的. 以采样周期$T = 0.1s$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$L + 2n_x$阶持续激励性. 另外根据算法1, 选择预测时域$L = 30$, $Q = I$, $R = 10^{-4}I$, $\lambda_g = 0.1$, $\lambda_\sigma = 120$.

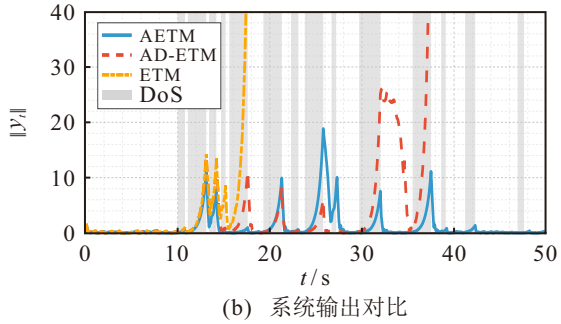
本文设计的 AETM 采用$\eta_0 = 0.2$、$\eta_1 = 0.6$、$c_1 = 10^3$、$c_2 = 50$、$c_3 = 1$. 在同样强度的 DoS 攻击和噪声环境下, 将基于攻击检测的 ETM(AD-ETM)[17] 与一般的 ETM[14] 进行比较, 以展示所提出算法的效率.

根据图 3 中的结果可见, 传统 ETM 在高频 DoS 攻击下因数据丢失而发散. AD-ETM 虽然引入了攻击强度识别机制, 但其本质依赖于对历史 DoS 攻击特性的估计, 不可避免地引入了检测时滞, 另外其动态因子不会反映由噪声引起的内部状态偏差, 导致在攻击突发初期无法及时下调触发阈值, 因此系统输出仍表现出显著的超调量. 相比之下, 本文提出的 AETM 利用预测误差驱动的指数衰减律动态调整阈值, 具备对系统状态恶化的瞬时响应能力. 实验结果证实, AETM 无需对 DoS 攻击参数进行显式估计即可迅速补偿攻击影响, 在确保稳定性的前提下, 实现了比 AD-ETM 更优的控制性能与通信资源的权衡.

图 4 揭示了参数c_3在资源消耗与控制性能间的权衡机制. 由图 4(a) 可知, 减小c_3会降低触发阈值对状态变化的敏感度, 虽有效减少了计算开销, 但也延缓了 DoS 攻击后的系统恢复响应. 相反, 图 4(b) 表明增大c_3能显著增强系统的抗扰能力与稳态性能. 综上, c_3的选取需在鲁棒性与资源效率间进行折中, 较大的c_3虽能提升抗攻击能力, 却增加了资源消耗. 此外, 受$\eta(r)$指数衰减特性的制约, 当c_3超过一定阈值后, 其带来的性能增益将趋于饱和.

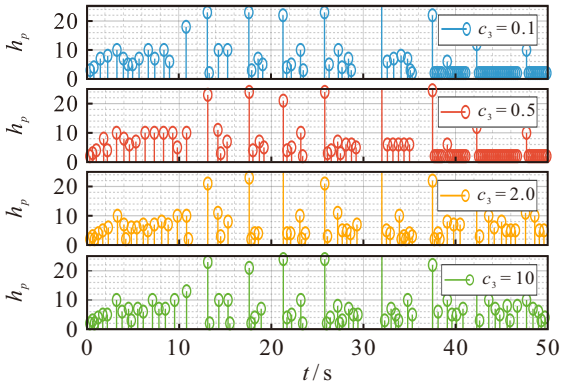


(a) 优化问题执行间隔对比

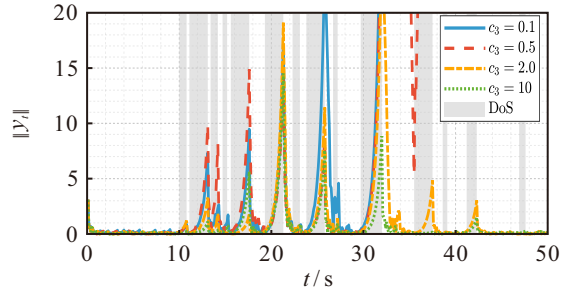


(b) 系统输出对比

图3 相同 DoS 攻击和噪声水平环境下系统资源消耗和系统性能对比: $\bar{v} = 0.025$, $\bar{\ell}_p = 20$, $\Phi_f = 14$, $\Phi_d = 180$.



(a) 优化问题执行间隔对比



(b) 系统输出对比

图4 不同c_3下系统资源消耗和系统性能对比: $\bar{v} = 0.025$, $\bar{\ell}_p = 20$, $\Phi_f = 14$, $\Phi_d = 180$

另外图 5 揭示了噪声水平$\bar{v}$与预测时域L之间的关系. 实验结果有力地证明了本文提出的基于 AETM 的数据驱动算法具有良好的鲁棒性. 面对更大的噪声水平$\bar{v}$, 算法可以通过适度增加预测时域长度来抵消噪声对预测精度的负面影响. 只要满足理论推导的稳定性约束条件$L > \underline{L}$, 即便在强噪声和高频 DoS 攻击的恶劣工况下, 所提方法依然能保证系统的有效性与鲁棒性.

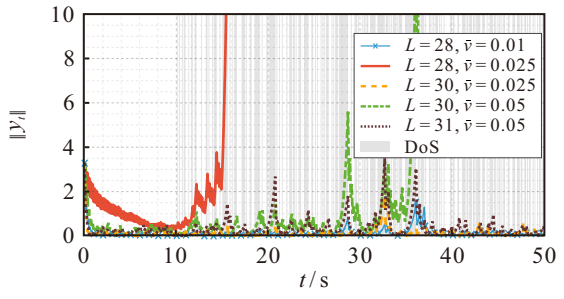


图5 不同噪声水平与预测时域下的系统鲁棒性分析: $\bar{\ell}_p = 12$, $\Phi_f = 98$, $\Phi_d = 220$

4 总 结

针对资源受限 CPS 在 DoS 攻击下的安全控制问题, 本文提出一种基于预测误差驱动的自适应事件触发数据驱动预测控制方法. 该方法结合 Willems 基本引理, 利用离线数据直接构建预测控制器以主动补偿攻击影响. 理论上证明了闭环系统的迭代可行性与稳定性, 并推导了预测时域L与系统噪声水平及攻击持续时间之间的定量依赖关系. 仿真结果证实, 提出的 AETM 机制在高频攻击下较传统机制具有更优的动态响应速度与抗扰鲁棒性, 且验证了通过适当增加L可有效抵消高强度噪声对预测精度的负面影响. 未来的工作将致力于该方法在非线性系统中的扩展, 可以通过引入 Hankel 矩阵在线更新策略或非线性基本引理以适应系统动态变化, 从而解决工业过程中的本质非线性问题.

参考文献 (References)

[1] Ghobakhloo M. Industry 4.0, digitization, and opportunities for sustainability[J]. Journal of Cleaner Production, 2020, 252: 119869.

[2] Dileep G. A survey on smart grid technologies and applications[J]. Renewable Energy, 2020, 146: 2589-2625.

[3] 张健, 朱延正, 苏春翌, 等. 一类无人艇的重复学习复合抗扰容错控制[J]. 控制与决策, 2025, 40(1): 261-270.
(Zhang J, Zhu Y Z, Su C Y, et al. Repetitive learning composite anti-disturbance fault-tolerant control for unmanned marine vehicles[J]. Control and Decision, 2025, 40(1): 261-270.)

[4] Liu S S, Liu L K, Tang J, et al. Edge computing for autonomous driving: Opportunities and challenges[J]. Proceedings of the IEEE, 2019, 107(8): 1697-1716.

[5] Pelechrinis K, Iliofotou M, Krishnamurthy S V. Denial of service attacks in wireless networks: The case of jammers[J]. IEEE Communications Surveys & Tutorials, 2011, 13(2): 245-257.

[6] Duo W L, Zhou M C, Abusorrah A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges[J]. CAA Journal of Automatica Sinica, 2022, 9(5): 784-800.

[7] 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.

[8] Sun Q, Zhang K W, Shi Y. Resilient model predictive control of cyber–physical systems under DoS attacks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(7): 4920-4927.

[9] Sun Q, Chen J C, Shi Y. Event-triggered robust MPC of nonlinear cyber-physical systems against DoS attacks[J]. Science China Information Sciences, 2021, 65(1): 110202.

[10] 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.

[11] Peng C, Li F Q. A survey on recent advances in event-triggered communication and control[J]. Information Sciences: An International Journal, 2018, 457(C): 113-125.

[12] Heemels W P M H, Donkers M C F, Teel A R. Periodic event-triggered control for linear systems[J]. IEEE Transactions on Automatic Control, 2013, 58(4): 847-861.

[13] Tian E G, Peng C. Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(11): 4610-4618.

[14] Yang Y, Shi D W, Yu H, et al. Event-triggered data-driven predictive control for multirate systems: Theoretic analysis and experimental results[J]. ASME Transactions on Mechatronics, 2025, 30(4): 2450-2460.

[15] Deng Y R, Yin X X, Hu S L. Event-triggered predictive control for networked control systems with DoS attacks[J]. Information Sciences, 2021, 542: 71-91.

[16] 赵颖, 郭世旭, 黄进. DoS 攻击下质量切换无人艇动态记忆事件触发动力定位控制[J]. 控制与决策, 2025, 40(1): 292-299.
(Zhao Y, Guo S X, Huang J. Dynamic memory event-triggered dynamic positioning for mass-switched unmanned marine vehicles under DoS attacks[J]. Control and Decision, 2025, 40(1): 292-299.)

[17] Sun H T, Peng C, Shen Y T. Attack-detection-based event-triggered transmission scheme for stabilizing cyber-physical systems under denial of service attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024, 2: 176-184.

[18] Hou Z S, Xiong S S. On model-free adaptive control and its stability analysis[J]. IEEE Transactions on Automatic Control, 2019, 64(11): 4555-4569.

[19] Hewing L, Wabersich K P, Menner M, et al. Learning-based model predictive control: Toward safe learning in control[J]. Annual Review of Control, Robotics, and Autonomous Systems, 2020, 3: 269-296.

[20] Berberich J, Kohler J, Muller 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.

[21] 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.

[22] Coulson J, Lygeros J, Dorfler F. Data-enabled predictive control: In the shallows of the DeePC[C]. 2019 18th

European Control Conference. Naples, 2019: 307-312.

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

[24] 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.
(Ren Q S, Chen J, Liu F. Data-driven resilient predictive control without terminal components under DoS attacks[J]. Control and Decision, 2025, 40(10): 3190-3200.)

[25] Rotulo M, De Persis C, Tesi P. Online learning of data-driven controllers for unknown switched linear systems[J]. Automatica, 2022, 145: 110519.

作者简介

任清爽 (2001−), 男, 硕士生, 主要研究方向为网络控制系统、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, 主要研究方向为为模糊控制理论及应用、复杂系统建模及应用, E-mail: chenjun1860@126.com;

闻继伟 (1981−), 男, 副教授, 博士, 主要研究方向为复杂系统性能分析, E-mail: wjw8143@jiangnan.edu.cn;

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.