欺骗攻击下弹性自触发模型预测控制

贺　宁[1,2], 马　凯[1], 沈　超[2†], 徐中显[1], 钱　成[1]

(1. 西安建筑科技大学 机电工程学院, 陕西 西安 710055; 2. 西安交通大学 网络空间安全学院, 陕西 西安 710049)

摘要: 针对在欺骗攻击下自触发模型预测控制系统的安全控制问题, 本文提出一种基于关键数据保护的弹性自触发模型预测控制(MPC)策略. 对比现有的自触发MPC, 该方法仅需对少量关键控制样本进行保护, 则可保证闭环系统稳定运行, 从而有效节省系统资源. 首先, 基于自触发MPC和欺骗攻击的特征推导标称系统与被攻击系统状态之间的误差上界, 从而定量分析出欺骗攻击对系统的损害. 然后, 通过所获得误差上界和李雅普诺夫定理建立关键数据的选取条件并对其实施保护. 最后, 严格证明了在仅对关键控制样本实施保护后, 被控系统仍可在欺骗攻击下保持稳定. 此外, 基于移动机器人和弹簧小车系统对所提算法进行了仿真实验, 结果表明所提算法能够显著节省保护资源, 验证了算法的有效性.

关键词: 信息物理融合系统; 模型预测控制; 自触发机制; 弹性控制; 欺骗攻击

引用格式: 贺宁, 马凯, 沈超, 等. 欺骗攻击下弹性自触发模型预测控制. 控制理论与应用, 2023, 40(5): 865 – 873

DOI: 10.7641/CTA.2022.11129

Resilient self-triggered model predictive control under deception attacks

HE Ning[1,2], MA Kai[1], SHEN Chao[2†], XU Zhong-xian[1], QIAN Cheng[1]

(1. School of Mechanical and Electrical Engineering, Xi'an University of Architecture and Technology, Xi'an Shaanxi 710055, China;
2. School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an Shaanxi 710049, China)

Abstract: Aiming at solving the cyber security problem of self-triggered model predictive control (MPC) in cyber-physical systems under deception attacks, a resilient self-triggered MPC strategy based on the key data protection is proposed. Compared with the existing MPC methods, the proposed method only protects a small number of key control samples to ensure the stability of the system, thus effectively saving system resources. Firstly, the upper limit of the difference between the nominal and attacked states is analyzed based on the characteristics of self-triggered MPC and deception attacks, so as to quantitatively calculate the damages to the system caused by deception attacks. Then, the selection conditions of the key data are given based on the obtained upper limit of the state difference and Lyapunov stability theory. Finally, it is demonstrated that the controlled system can be operated stably under deception attacks when only key control samples are protected. Furthermore, the proposed algorithm is simulated based on the mobile robot and cart-damper-spring system, and the results show that the proposed algorithm can significantly save the protection resources, which verifies the effectiveness of the method.

Key words: cyber-physical system; model predictive control; self-triggered mechanism; resilient control; deception attacks

Citation: HE Ning, MA Kai, SHEN Chao, et al. Resilient self-triggered model predictive control under deception attacks. *Control Theory & Applications*, 2023, 40(5): 865 – 873

1　引言

近年来, 随着计算机技术和通信网络的发展, 信息物理融合系统(cyber-physical system, CPS)得到了学术界和工业界的广泛关注. CPS是涉及控制、通信和计算机等技术的复杂系统, 实现了全系统的自治与协作. 目前, CPS 已经成功应用于机器人、交通、医疗、智能建筑和智能家居等多个领域[1–2].

模型预测控制 (model predictive control, MPC)作为一种先进控制策略, 擅长处理带有复杂约束的多变量最优控制问题, 在带有复杂物理约束的CPS中得到了广泛应用[3–5]. 为了进一步拓宽MPC的应用场景, 降低系统能耗, 事件触发MPC已成为研究与应用的热

收稿日期: 2021−11−17; 录用日期: 2022−06−24.

†通信作者. E-mail: chaoshen@xjtu.edu.cn; Tel.: +86 18629439025.

本文责任编委: 倪茂林.

国家自然科学基金项目(61903291), 博士后面向基金项目(2019M660257)资助.

Supported by the National Natural Science Foundation of China (61903291) and the China Postdoctoral Science Foundation (2019M660257).

点. 文献[6]基于实际状态与最优状态的误差构造了事件触发MPC机制, 并给出了保证系统稳定性和可行性的充要条件. 文献[7]针对带有附加扰动的连续时间线性系统, 构造了一种微分型事件触发MPC框架, 更好地考虑了状态变化的动态特性对触发机制的影响. 需要强调的是, 不同于传统MPC在每个时刻都需要进行最优控制问题的求解和控制信号的传输, 自触发MPC在继承事件触发MPC仅在预设触发条件被满足时才进行控制问题求解的基础思想上, 通过预测未来触发时刻, 进一步降低了事件触发MPC监控成本[8]. 因此, 自触发MPC可以减少系统不必要的采样与更新, 从而显著降低其计算、通信和监控负担. 文献[9]通过分析系统的闭环理论特性, 设计了基于零阶保持器的自触发MPC, 文献[10]将该方法扩展至一阶保持的同时减小了采样保持控制信号与最优控制信号之间的偏差. 文献[11]提出了一种新颖的自触发机制和预测时域更新策略, 从降低求解优化问题的频率和每个优化问题的复杂度两方面节省了计算资源. 基于上述优势, 自触发MPC已被成功用于各类实际CPS系统, 如工业机械臂[12]、水下机器人[13]、高速列车[14]等.

然而, CPS在开放的网络环境进行信息交互时, 不可避免地会遭受到恶意的网络攻击, 最具有代表性的就是欺骗攻击. 欺骗攻击通过篡改网络层传输的数据使被控系统性能显著降低, 并且还具备一定的隐匿性[15]. 近年来, 关于欺骗攻击的研究主要聚焦于攻击的建模、检测与防御. 文献[16]通过分析欺骗攻击的实施条件, 设计出不依赖实时数据的攻击序列生成方法, 该方法对传统的χ^2检测器具有完全隐匿性. 文献[17] 提出了一种通过主动修改测量数据去检测通信网络中存在的隐匿攻击的方法. 为使CPS在遭受欺骗攻击时可以稳定运行, 一个有效的解决方案是建立基于保护方法或检测方法的弹性控制机制. 弹性控制是指系统能够在异常情况下(包含恶意攻击和灾难威胁)维持状态已知和可接受一定恢复程度的正常运行[18]. 文献[19]研究了基于MPC的多面体不确定模型在网络环境下的安全控制问题, 建立了包含概率欺骗攻击、多面体不确定性和有界干扰的系统模型. 此外, 作者从可实现鲁棒不变集、控制性能和安全需求等方面为具有欺骗攻击和有界扰动的线性变参数系统提供了一种有效的安全控制方法. 文献[20]提及的弹性记忆控制技术同时考虑了事件触发机制和欺骗攻击, 并基于李雅普诺夫泛函方法得到了渐进稳定性的充分条件. 文献[21]设计了一种同时考虑H_2和H_∞性能指标的弹性MPC算法, 该算法能够有效减弱干扰和欺骗攻击对CPS造成的损害.

本文考虑在实际CPS系统中被保护数据的数量通常与资源消耗有关[22], 同时结合自触发MPC在处理约束和降低系统能耗等方面的优势, 提出一种保护有限数据的弹性自触发控制策略. 本文的主要贡献包括3个方面:

1) 构建一种基于关键数据保护的弹性自触发MPC机制, 主要内容为: ① 在控制器侧对连续控制信号进行离散采样; ② 基于解析的误差上界表达式计算出被保护的控制样本并对其实施保护; ③ 在执行器侧通过采样保持方式应用通过网络通道接收到的控制样本;

2) 基于自触发MPC和欺骗攻击的特征分析出标称系统和被攻击系统之间的误差上界, 从而定量分析出欺骗攻击对系统造成的损害;

3) 结合李雅普诺夫稳定性理论证明了弹性自触发MPC算法的可行性和系统的闭环稳定性.

本文所使用的符号定义如下: $\mathbb{R}$, $\mathbb{R}^+$分别为实数集和非负实数集; $\mathbb{N}$为非负整数集, $\mathbb{N}^+$为正整数集. $\|n\|=\sqrt{n^{\mathrm{T}}n}$表示向量$n$的欧几里得范数, $\|n\|_P=\sqrt{n^{\mathrm{T}}Pn}$表示向量$n$的$P$范数. 给定两个不同的集合$\Omega_1$和$\Omega_2$, $\Omega_1\ominus\Omega_2=\{x|x\in\Omega_1, x\notin\Omega_2\}$. 如果一个连续函数$\alpha:[0,\ a)\to[0,\infty)$严格递增, 并且满足$\alpha(0)=0$, $\lim\limits_{r\to\infty}\alpha(r)=\infty$, 则称函数$\alpha$为$\mathcal{K}_\infty$函数.

2 问题描述

本节分别对非线性系统, 控制器结构以及欺骗攻击进行建模.

2.1 系统描述

考虑如下非线性系统模型:

$$\begin{cases} x(t)=\phi(x(t),\ u(t))=f(x)+g(x)u(t),\\ t\geqslant t_0,\ x(t_0)=x_0, \end{cases} \tag{1}$$

其中: $x(t)\in\mathbb{R}^n$, $u(t)\in\mathbb{R}^m$分别为系统状态和控制输入, t_0定义为初始时间. 控制输入u满足如下约束:

$$u(t)\in\mathcal{U}\subseteq\mathbb{R}^m,\ \forall t\geqslant t_0. \tag{2}$$

系统(1)满足如下假设:

假设 1 非线性方程$\phi(x,u):\mathbb{R}^n\times\mathbb{R}^m\to\mathbb{R}^n$满足$\phi(0,0)=0$, 并且存在常数$\mathcal{L}_\phi$使$\|\phi(x_1,u)-\phi(x_2,u)\|\leqslant\mathcal{L}_\phi\|x_1-x_2\|, x\in\mathbb{R}^n$成立. 此外, 存在正常数$\mathcal{L}_{\mathrm{g}}>0$满足$\|g(x)u\|\leqslant\mathcal{L}_{\mathrm{g}}\|u\|$.

系统(1)为带有约束连续型仿射系统, 通常采用MPC作为其控制策略去显性处理输入输出约束, 此外, 考虑图1中的网络控制系统, 将带有传感器和执行器系统的设备通过网络通道连接到至MPC. 为节省通信和计算资源, 本文在MPC控制器中引入自触发机制.

2.2 自触发MPC

在每一个触发瞬间$t_k, k\in\mathbb{N}^+$, 自触发MPC基于系统模型(1)和当前测量值$x(t_k)$通过求解最优控制问题$\mathcal{P}$获取最优控制序列$u^*(s), s\in[t_k, t_k+T_P]$, 并将

触发间隔$t_{k+1}-t_k$内控制序列作用于系统, t_{k+1}通过自触发机制获得, T_P为预测时域. $\mathcal{P}$定义为

$$\min_{u} J(x(t_k),\ u), \tag{3}$$

$$\text{s.t. } \dot{x}=\phi(x,\ u),\ s\in[t_k,\ t_k+T_P], \tag{4}$$

$$u(s)\in\mathcal{U}, \tag{5}$$

$$x(t_k+T_P)\in\Omega(\varepsilon_f). \tag{6}$$

代价函数J定义如下:

$$J(x(t_k),\ u)=\int_{t_k}^{t_k+T_P} F(x(s),\ u(s))\mathrm{d}s+V_f(x(t_k+T_P)), \tag{7}$$

$F(x(s),u(s))$和$V_f(x(t_k+T_P))$分别为阶段和终端代价函数, 给定$\varepsilon_f>0$, 终端约束集$\Omega(\varepsilon_f)$描述为

$$\Omega(\varepsilon_f)=\{x(s)\in\mathbb{R}^n: V_f(x(s))\leqslant\varepsilon_f\}. \tag{8}$$

为了推导系统闭环稳定性, 通常引入假设2.

假设 2　$\exists\varepsilon>\varepsilon_f>0$和终端反馈控制律$\kappa(x)$使

$$\frac{\partial V_f}{\partial x}(f(x)+g(x)\kappa(x))\leqslant -F(x,\ \kappa(x)),\ \forall x\in\Omega(\varepsilon_f) \tag{9}$$

成立, $\varepsilon=\alpha\varepsilon_f$, $\alpha\in(0,\ 1)$.

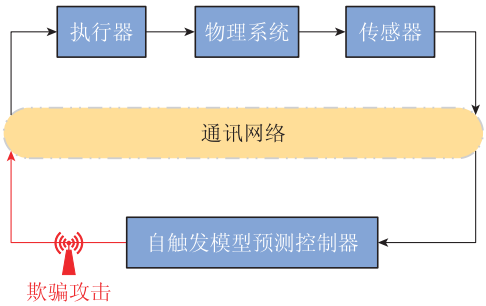

图 1　网络控制系统框架

Fig. 1　The framework of a networked control system

定义 1　控制器控制目标是使系统(1)在有限时间内进入终端约束集$\Omega(\varepsilon_f)$.

定义 2　定义一个MPC稳定区域$\Xi_V=\{x\in\mathbb{R}^n, J^*(x)\leqslant J_0\}$, $\Omega(\varepsilon_f)\in\Xi_V$. $J^*(x)$为求解最优控制问题$\mathcal{P}$获得的最优代价函数.

基于Ξ_V, 进一步假设$F(x,u)$和$V_f(x)$遵循假设3.

假设 3　$\exists\mathcal{K}_\infty$函数$\alpha_1$和$\alpha_2$满足$F(x(s),u(s))\geqslant\alpha_1, V_f(x(s))\leqslant\alpha_2$. 此外, $F(x,u)$和$V_f(x)$在$\forall x_1,x_2\in\Xi_V$上存在李普希兹常数$\mathcal{L}_F$和$\mathcal{L}_V$使

$$\|F(x_1,\ u)-F(x_2,\ u)\|\leqslant\mathcal{L}_F\|x_1-x_2\|, \tag{10}$$

$$\|V_f(x_1,\ u)-V_f(x_2,\ u)\|\leqslant\mathcal{L}_V\|x_1-x_2\| \tag{11}$$

成立.

如果假设1–3成立, 则最优代价函数$J^*(x)$在$x\in\Xi_V$上存在李普希兹常数$\mathcal{L}_J$满足$\|J^*(x_1)-J^*(x_2)\|\leqslant\mathcal{L}_J\|x_1-x_2\|$.

注 1　本文所提出方法可适用于目前主流MPC使用的二次型代价函数, 即$J(x(t_k),\ u)=\int_{t_k}^{t_k+T_P}\|x(s)\|_Q^2+\|u(s)\|_R^2\mathrm{d}s+\|x(t_k+T_P)\|_Z^2$, 这里$Q$, R, Z为权重矩阵. 此外, 对包含非二次型代价函数的MPC系统, 如果系统模型满足式(1)且MPC阶段和终端函数满足假设3中的性质与要求, 本方法仍可被使用以保证系统在欺骗攻击下的可行性、稳定性. 假设1–3为设计非线性MPC的一般性假设, 上述提到的各种集合和参数计算方法可以在文献[9]及其参考文献中找到. 由于假设2中给出了终端控制律$\kappa(x)$, 所以为了节省通信和计算资源, MPC通常采用“双模控制”, 即系统状态x一旦进入$\Omega(\varepsilon)$, 控制输入$u(t)$将通过$\kappa(x)$获得, 不再求解$\mathcal{P}$[23]. 此外, $\kappa(x)$通常被布置于系统侧, 因此$\kappa(x)$不需要被传输.

注意, 通过求解$\mathcal{P}$获得的最优控制输入$u^*(s),\ s\in[t_k,t_k+T_P]$是一个连续的输入信号, 但是在图1所示的网络控制系统中, 控制器在有限的传输带宽下只能发送有限数量的控制样本. 为解决这一问题, 工业应用中通常将$u^*(s)$离散化为$N(N\in\mathbb{N}^+)$个控制样本, 即数据包$\boldsymbol{U}^*(t_k)$:

$$\boldsymbol{U}^*(t_k)=\{u^*(t_k),u^*(t_k+\delta_1),\cdots,u^*(t_k+\sum_{i=1}^{N}\delta_i)\}, \tag{12}$$

这里$t_k+\sum_{i=1}^{N}\delta_i$满足$t_k+\sum_{i=1}^{N}\delta_i=t_{k+1}-t_k=\Delta_N$. 在触发瞬间$t_k$, $\boldsymbol{U}^*(t_k)$通过网络信道发送至执行器, 执行器通过采样保持方式应用$\boldsymbol{U}^*(t_k)$获得实际系统状态$x(s)$. 基于上述设置, 一个典型的自触发MPC算法描述如下:

1) 求解$\mathcal{P}$获得$u^*(s),x^*(s),\ s\in[t_k,t_k+T_P]$;

2) 基于闭环系统稳定性分析设计自触发条件, 并通过设计控制样本$\boldsymbol{U}^*(t_k)$, 获得最大化触发间隔的下一个触发时刻t_{k+1}[9,24];

3) 执行器在Δ_N内采用采样保持方式应用$\boldsymbol{U}^*(t_k)$, 并在t_{k+1}将实际系统状态x_{k+1}传回控制器.

由于网络存在安全漏洞, 控制样本$\boldsymbol{U}^*(t_k)$可能被攻击者恶意篡改, 导致系统不稳定, 即系统会受到欺骗攻击的威胁.

2.3　欺骗攻击

自触发MPC执行非周期采样, 即控制输入和测量值仅在触发瞬间t_k被传输; 同时, 相比反馈通道(执行器至控制器), 前向网络通道(控制器至执行器)包含更多信息(不仅控制样本, 而且相应的执行时间)[9], 它可能更易于遭到恶意攻击. 所以本文所考虑的欺骗攻击发生在前向通道. 定义被攻击之后的控制输入为$u_{\mathrm{a}}(\cdot)$, 相应系统状态为$x_{\mathrm{a}}(\cdot)$.

为了提高欺骗攻击的隐匿性, 假设$\boldsymbol{U}^*(t_k)$中的第1个控制样本未被篡改, 并且每个被篡改的控制样

本都设置为$\boldsymbol{U}^*(t_k)$中已经存在的值. 由于攻击资源消耗和被篡改的数据量呈正相关[25], 攻击者在发动欺骗攻击时可以考虑两种不同的攻击场景, 即: 通过篡改一个控制样本来节省攻击资源, 或者通过篡改多个控制样本实现最大化破坏. 定义攻击者篡改的第 1 个控制样本为$u^*(t_k+\Delta_l), 0<l<N$, 并且令$M(1\leqslant M<N)$为被篡改控制样本数量, $\delta_q,\cdots,\delta_o,\delta_l$为被攻击控制样本间隔. 则被篡改之后数据包可以表示如下:

1) 篡改1个控制样本(参考图2).

$$\begin{aligned}\boldsymbol{U}_1(t_k)=\{&u^*(t_k),\cdots,u^*(t_k+\Delta_{l-2}),\\&u^*(t_k+\Delta_{l-2}),\cdots,u^*(t_k+\Delta_N)\},\end{aligned}\tag{13}$$

2) 篡改M个控制样本(参考图3).

$$\begin{aligned}&\boldsymbol{U}_M(t_k)=\\&\{u^*(t_k),\cdots,u^*(t_k+\Delta_{l-2}),\\&\underbrace{u^*(t_k+\Delta_{l-2}),\cdots,u^*(t_k+\Delta_{l-2})}_{c_1},\cdots,\\&\underbrace{u^*(t_k+\Delta_{o-c_2-1}),\cdots,u^*(t_k+\Delta_{o-c_2-1})}_{c_2},\cdots,\\&\underbrace{u^*(t_k+\Delta_{q-c_i-1}),\cdots,u^*(t_k+\Delta_{q-c_i-1})}_{c_i},\cdots,\\&u^*(t_k+\Delta_N)\},\end{aligned}\tag{14}$$

其中: $c_i(1<c_i<M)$为连续攻击控制样本数, c_i满足$c_1+c_2+\cdots+c_i=M$, 且$N\geqslant q>\cdots>o>\cdots>l$.

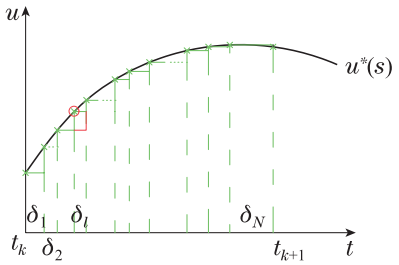

图 2 欺骗攻击篡改1个控制样本示意图

Fig. 2 Schematic diagram of the deception attack tampering a single control sample

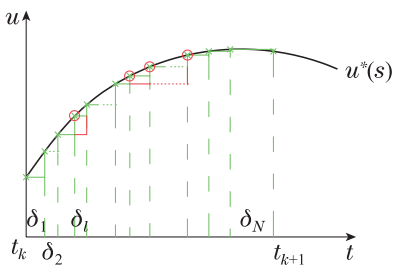

图 3 欺骗攻击篡改M个控制样本示意图

Fig. 3 Schematic diagram of the deception attack tampering M control samples

图2–3为所考虑的攻击模式提供了两个示例. 给定在t_k处获得的最优输入序列(实线"$u^*(s)$"), 自触发控制器从获得的输入序列中选择N个控制样本(叉号)通过网络发送. 同时, 攻击者在传输的控制样本(叉号)中篡改有限数量的样本(圆圈)来实现网络攻击.

注意, 如果将上述数据包$\boldsymbol{U}^*(t_k)$直接应用于执行器, 则系统稳定性将无法被保证, 甚至直接导致系统失稳. 为了确保系统性能, 通常考虑将整个$\boldsymbol{U}^*(t_k)$进行保护. 但是, 如果采用整体保护机制不仅会增加计算资源的消耗同时会占用大量网络带宽资源, 所以为了解决资源消耗和数据安全这一实际矛盾[22], 有必要提出一种只需要保护少量控制样本, 但仍能保证系统稳定的弹性自触发MPC.

3 弹性自触发MPC

本节提供一种弹性控制方法, 利用保护较少的控制样本的方式减弱欺骗攻击的不利影响, 进而在保证系统稳定前提下降低资源消耗. 具体来说, 将原始连续输入信号离散为$\boldsymbol{U}^*(t_k)$后, 提出的自适应保护机制去确定若干关键控制样本; 然后, 对这些控制样本在传输时给予保护; 最后, 执行器采用采样保持机制应用数据包$\boldsymbol{U}_M(t_k)$.

由于防御者目标是去减弱欺骗攻击对系统性能的影响, 所以在建立有效防御机制之前需要对欺骗攻击产生的影响进行定量分析, 因此首先利用引理1和引理2对不同攻击情形下系统状态误差上界进行解析计算. 定义$\mathcal{E}_1^l$为$\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|$的上界, $\mathcal{E}_{(\cdot)}^{(\cdot)}$的上标为被攻击的控制样本的位置, 下标为被攻击样本个数.

引理 1 假设第l个控制样本被攻击, 则$\mathcal{E}_1^l$可以通过下式计算:

$$\begin{aligned}&\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|\leqslant\\&\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-2})-u^*(t_k+\Delta_{l-1})\|\times\\&\delta_l{\rm e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{l-1})}=\mathcal{E}_1^l,\end{aligned}\tag{15}$$

其中$l=2,3\cdots,N-1,N$.

证 从式(13)建模可知, 欺骗攻击产生的破坏起始于$t_k+\Delta_{l-1}$, 即

$$x(t_k+\Delta_{l-1})=x_{\rm a}(t_k+\Delta_{l-1}).$$

在$t_k+\Delta_N$系统被攻击前后的输出可以表示为

$$\begin{aligned}&x(t_k+\Delta_N)=\\&x(t_k+\Delta_{l-1})+\\&\int_{t_k+\Delta_{l-1}}^{t_k+\Delta_l}\phi(x(s),u^*(t_k+\Delta_{l-1}))\mathrm{d}s+\\&\cdots\int_{t_k+\Delta_{N-1}}^{t_k+\Delta_N}\phi(x(s),\ u^*(t_k+\Delta_{N-1}))\mathrm{d}s,\\&x_{\rm a}(t_k+\Delta_N)=\\&x_{\rm a}(t_k+\Delta_{l-1})+\end{aligned}$$

$$\int_{t_k+\Delta_{l-1}}^{t_k+\Delta_l}\phi(x_{\rm a}(s),u^*(t_k+\Delta_{l-2}))\mathrm{d}s+$$
$$\cdots\int_{t_k+\Delta_{N-1}}^{t_k+\Delta_N}\phi(x_{\rm a}(s),u^*(t_k+\Delta_{N-1}))\mathrm{d}s.$$

则, 在$t_k+\Delta_l$误差上界为

$$\|x(t_k+\Delta_{l-1})-x_{\rm a}(t_k+\Delta_{l-1})\|=$$
$$\int_{t_k+\Delta_{l-1}}^{t_k+\Delta_l}\phi(x(s),u^*(t_k+\Delta_{l-1}))\mathrm{d}s-$$
$$\int_{t_k+\Delta_{l-1}}^{t_k+\Delta_l}\phi(x_{\rm a}(s),u^*(t_k+\Delta_{l-2}))\mathrm{d}s\leqslant$$
$$\int_{t_k+\Delta_{N-1}}^{t_k+\Delta_l}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-1})-u^*(t_k+\Delta_{l-2})\|\delta_l\leqslant$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-1})-u^*(t_k+\Delta_{l-2})\|\delta_l\mathrm{e}^{\mathcal{L}_\phi\delta_l},$$

上式可以通过Gronwall-bellman不等式获得. 在$t_k+\Delta_{l+1}$时刻的误差上界可以表示为

$$\|x(t_k+\Delta_{l+1})-x_{\rm a}(t_k+\Delta_{l+1})\|\leqslant$$
$$\|x(t_k+\Delta_l)-x_{\rm a}(t_k+\Delta_l)\|+$$
$$\int_{t_k+\Delta_l}^{t_k+\Delta_{l+1}}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s\leqslant$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-1})-u^*(t_k+\Delta_{l-2})\|\delta_l\mathrm{e}^{\mathcal{L}_\phi(\delta_l+\delta_{l+1})},$$

通过递推进一步可以确定

$$\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|\leqslant$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-1})-u^*(t_k+\Delta_{l-2})\|\delta_l\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{l-1})}.$$

令

$$\mathcal{E}_1^l=\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-2})-u^*(t_k+\Delta_{l-1})\|\delta_l\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{l-1})}.$$

证毕.

由于仅攻击单个控制样本对系统的破坏相对有限, 所以攻击者在攻击资源充足的情况下可能会对多个控制样本进行篡改, 以达到较大的破坏效果. 所以有必要分析同时篡改多个控制样本对系统造成的影响.

引理 2　假设从第l个控制样本开始, 攻击者对M个控制样本进行篡改, 则$\mathcal{E}_M^{l,\cdots,o,q}$可以通过下式计算:

$$\begin{cases}\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|\leqslant\mathcal{E}_M^{l,\cdots,o,q},\\ \mathcal{E}_M^{l,\cdots,o,q}=\mathcal{E}_{M-1}^{l,\cdots,o}\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_o)}+\\ \qquad\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{l-1})-\\ \qquad u^*(t_k+\Delta_{l-1-g})\|\delta_q\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{q-1})},\end{cases}\tag{16}$$

这里$\delta_q,\cdots,\delta_o,\delta_l$为被攻击控制样本间隔, 并且满足$l<\cdots<o<q\leqslant N$.

证　在$t_k+\Delta_N$, 误差上界$\mathcal{E}_M^{l,\cdots,o,q}$为

$$\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|\leqslant$$
$$\|x(t_k+\Delta_q)-x_{\rm a}(t_k+\Delta_l)\|+$$
$$\int_{t_k+\Delta_q}^{t_k+\Delta_{q+1}}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s+\cdots+$$
$$\int_{t_k+\Delta_{N-1}}^{t_k+\Delta_N}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s\leqslant$$
$$\|x(t_k+\Delta_q)-x_{\rm a}(t_k+\Delta_l)\|\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_q)}=\mathcal{E}_M^{l,\cdots,o,q}.$$

当$q=o+1$时, 假设攻击者以第$q+1-g$个控制样本起始, 连续篡改$g(g\geqslant 2)$个控制样本, 则

$$\|x(t_k+\Delta_q)-x_{\rm a}(t_k+\Delta_q)\|=$$
$$\|x(t_k+\Delta_{q-1})-x_{\rm a}(t_k+\Delta_{q-1})\|+$$
$$\int_{t_k+\Delta_q}^{t_k+\Delta_{q+1}}\phi(x(s),u^*(t_k+\Delta_{q-1}))\mathrm{d}s-$$
$$\int_{t_k+\Delta_q}^{t_k+\Delta_{q+1}}\phi(x_{\rm a}(s),u^*(t_k+\Delta_{q-g-1}))\mathrm{d}s\leqslant$$
$$\|x(t_k+\Delta_{q-1})-x_{\rm a}(t_k+\Delta_{q-1})\|\mathrm{e}^{\mathcal{L}_\phi\delta_q}+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{q-1})-u^*(t_k+\Delta_{q-g-1})\|\delta_q\mathrm{e}^{\mathcal{L}_\phi\delta_q},$$

当$q=o+w,\ w>1$时, 为得到统一表达式, 令$g=1$, 即以第q个控制样本起始, 连续篡改1个控制样本, 则

$$\|x(t_k+\Delta_q)-x_{\rm a}(t_k+\Delta_q)\|\leqslant$$
$$\|x(t_k+\Delta_o)-x_{\rm a}(t_k+\Delta_o)\|+$$
$$\sum_{v=1}^{w}\int_{t_k+\Delta_o}^{t_k+\Delta_{o+v}}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s+$$
$$\int_{t_k+\Delta_{q-1}}^{t_k+\Delta_q}\mathcal{L}_\phi\|x(s)-x_{\rm a}(s)\|\mathrm{d}s+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{q-1})-u^*(t_k+\Delta_{q-g-1})\|\delta_q\leqslant$$
$$\|x(t_k+\Delta_o)-x_{\rm a}(t_k+\Delta_o)\|\mathrm{e}^{\mathcal{L}_\phi(\Delta_{o+v}-\Delta_o)}+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{q-1})-u^*(t_k+\Delta_{q-g-1})\|\delta_q\mathrm{e}^{\mathcal{L}_\phi\Delta_q},$$

相似于引理1, 可以获得

$$\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|\leqslant$$
$$\|x(t_k+\Delta_o)-x_{\rm a}(t_k+\Delta_o)\|\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_o)}+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{q-g-1})-u^*(t_k+\Delta_{q-1})\|\times$$
$$\delta_q\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{q-1})}\leqslant$$
$$\mathcal{E}_{M-1}^{l,\cdots,o}\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_o)}+$$
$$\mathcal{L}_{\rm g}\|u^*(t_k+\Delta_{q-g-1})-u^*(t_k+\Delta_{q-1})\|\times$$
$$\delta_q\mathrm{e}^{\mathcal{L}_\phi(\Delta_N-\Delta_{q-1})}=\mathcal{E}_M^{l,\cdots,o,q}.$$

证毕.

注 2　对被攻击状态误差进行理论分析的目的是获得欺骗攻击对系统状态造成的偏差量$\|x(t_k+\Delta_N)-x_{\rm a}(t_k+\Delta_N)\|$的上界, 以保证所设计的弹性控制器可以应对最恶劣的攻击结果. 然而, 在实际系统中, 由于攻击资源等的限制, 攻击者对系统的破坏可能会低于这一程度, 基于此, 本方法的理论分析可能存在一定的保守性. 为降低这一保守性以提升控制器性能, 在状态误差分析中针对可能存在的不同攻击场景进行了分类讨论, 即攻击资源匮乏环境下的单个控制样本攻击(引理1)和攻击资源充裕环境下的多个控制样本攻击(引

理2), 并进一步将相关结果考虑到了弹性控制优化问题(17)中, 以有效提升理论分析的准确性.

假定被保护控制样本的数量P, 其所对应的控制样本位置集合为Θ_P, 则攻击者可选取$\Theta_M=\boldsymbol{U}^*(t_k)\ominus\Theta_P$中的控制样本进行攻击, 并假设通过引理1–2获得误差上界最大值$\max\mathcal{E}_M^{\Theta_M}$. 则$\Theta_P$可通过式(17)进行确定.

$$\Theta_P=\arg\min P(\Theta_P), \tag{17}$$

$$\text{s.t. } P=N-M, \tag{17a}$$

$$\Theta_M=\boldsymbol{U}^*(t_k)\ominus\Theta_P, \tag{17b}$$

$$\eta=\frac{\mu}{\mathcal{L}_J}\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s, \tag{17c}$$

$$\max\mathcal{E}_M^{\Theta_M}+E(\Delta_N)-\eta<0, \tag{17d}$$

式中: $E(\Delta_N)$为$\|x^*(t_k+\Delta_N)-x(t_k+\Delta_N)\|$的上界, 可由文献[9]中引理1获得, $\mu\in(0,\ 1)$. 优化问题(17)表示求解能够满足攻击样本数、李雅普诺夫稳定性等约束前提下, 被保护控制样本数$P(\Theta_p)$最小时的保护控制样本集合Θ_p. 约束(17a)–(17b)体现了被保护控制样本和最大攻击控制样本数的相互关系, 即二者之和为整个自触发控制序列样本数N. 约束(17c)为包含性能参数的阶段代价函数, 在实际使用中可通过调节μ的大小控制系统性能. 约束(17d)是基于李雅普诺夫定理的稳定性约束. 具体的讲, 当约束(17d)满足时, $J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x_{\mathrm{a}}(t_k))<0$成立, 由于代价函数$J^*(\cdot)$满足李雅普诺夫函数性质[9], 因此当约束(17d)满足时, 系统李雅普诺夫函数递减, 从而保证了系统的稳定性. 基于式(17)提出以下弹性自触发MPC算法保证在资源受限情况下被控系统可弹性地抵御欺骗攻击, 见表1.

表 1 算法1: 弹性自触发MPC

Table 1 Algorithm 1: Resilient self-triggered MPC

1 **while** $x(t_k)\notin\Omega(\varepsilon)$ **do**
2 通过自触发MPC机制获得$\boldsymbol{U}^*(t_k)$;
3 通过式(17)获得被保护的样本集合Θ_P;
4 对Θ_P实施保护, 并将数据包$\boldsymbol{U}^*(t_k)$发送至执行器;
5 执行器采用采样保持方式应用$\boldsymbol{U}_M(t_k)$;
6 传输$x(t_{k+1})$至控制器;
7 $k=k+1$
8 **end while**
9 应用终端控制律$u(t)=\kappa x(t)$.

算法1关键步骤解释如下: 第2步: 当系统状态$x\notin\Omega(\varepsilon)$且满足预设的自触发条件时, 求解$\mathcal{P}$并获得控制样本集$\boldsymbol{U}^*(t_k)$和下一个触发时刻$t_{k+1}$; 第3步: 基于$\boldsymbol{U}^*(t_k)$通过求解优化问题(17) 获得被保护样本集合$\Theta_P$; 第9步: 当$x\in\Omega(\varepsilon)$时通过终端控制律$\kappa(x)$稳定系统, 并在此后不再求解最优控制问题$\mathcal{P}$, 其中终端控制律$\kappa(x)$可通过线性二次调节器(linear quadratic regulator, LQR)方法获得[26].

注意, 算法1的计算量主要来源于第2步通过自触发MPC机制获取$\boldsymbol{U}^*(t_k)$和第3步通过式(17)获得被保护的样本集合Θ_P. 首先, 由于自触发机制的引入, 算法1的第2步相较于传统MPC显著的降低了求解$\mathcal{P}$的次数, 节省了计算资源的消耗; 其次, 由于第3步的计算量主要源自优化问题(17)的求解, 而其所需的阶段代价函数$F(x^*(s),u^*(s))$值在第2步求解$\mathcal{P}$之后就可获得, 误差上界$\max\mathcal{E}_M^{\Theta_M}+E(\Delta_N)$在引理1和引理2中也推导了解析解, 因此优化问题(17)的计算量也相对有限. 综上, 算法1拥有较为理想的在线计算量.

4 性能分析

本节将从理论上论证算法1的可行性和系统闭环稳定性.

定理 1 如果初始自触发MPC可行且稳定, 则算法1所提的弹性自触发MPC也是可行的.

证 首先, 由于MPC在t_k时刻可行, 因此$x_{\mathrm{a}}(t_k)=x(t_k)=x^*(t_k)\in\Xi_V$和$J^*(x_{\mathrm{a}}(t_k))=J^*(x^*(t_k))<J_0$成立, 故当未受攻击时算法1在$t_{k+1}$时刻是可行的. 此外, 由于系统(1)在自触发MPC控制下是稳定的, 所以根据文献[27]引理1可知

$$\begin{aligned}&J^*(x^*(t_k+\Delta_N))-J^*(x(t_k))\leqslant\\&-\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s,\end{aligned} \tag{18}$$

这里$J^*(\cdot)$被视为李雅普诺夫候选函数. 基于$x^*(t_k)=x(t_k)=x_{\mathrm{a}}(t_k)$可得

$$\begin{aligned}&J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x_{\mathrm{a}}(t_k))\leqslant\\&J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x^*(t_k+\Delta_N))-\\&\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s,\end{aligned} \tag{19}$$

进一步可知

$$\begin{aligned}&J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x_{\mathrm{a}}(t_k))\leqslant\\&J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x(t_k+\Delta_N))+\\&J^*(x(t_k+\Delta_N))-J^*(x^*(t_k+\Delta_N))-\\&\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s.\end{aligned} \tag{20}$$

此外, 由式(17)可得

$$\max\mathcal{E}_M^{\Theta_M}+E(\Delta_N)<\frac{\mu}{\mathcal{L}_J}\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s. \tag{21}$$

所以式(20)可以重写为

$$\begin{aligned}&J^*(x_{\mathrm{a}}(t_k+\Delta_N))-J^*(x_{\mathrm{a}}(t_k))\leqslant\\&\mathcal{L}_J\|x_{\mathrm{a}}(t_k+\Delta_N)-x(t_k+\Delta_N)\|+\end{aligned}$$

$$\mathcal{L}_J\|x(t_k+\Delta_N)-x^*(t_k+\Delta_N)\|-\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s\leqslant\mathcal{L}_J(\max\mathcal{E}_{\theta_M}^M+E(\Delta_N))-\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s<(\mu-1)\int_{t_k}^{t_{k+1}}F(x^*(s),u^*(s))\mathrm{d}s<0. \quad (22)$$

所以$J^*(x_\mathrm{a}(t_k+\Delta_N))-J^*(x_\mathrm{a}(t_k))<0$, 即$J^*(x_\mathrm{a}(t_k+\Delta_N))\in\Xi_V$. 因此算法1在$t_{k+1}$时刻也是可行的.

证毕.

定理 2　假设1–3成立, 并且通过第2.2节设计的自触发MPC可使系统(1)稳定. 考虑系统(1)遭受到第2.3节所述的欺骗攻击, 则算法1可以确保状态x在有限时间内进入$\Omega(\varepsilon_f)$.

证　本文通过反证法证明被控系统可以在有限时间进入$\Omega(\varepsilon_f)$. 首先假设如果初始位置满足$x(t_0)\in\Xi_V\ominus\Omega(\varepsilon_f)$, 则系统(1)将一直处于终端约束集$\Omega(\varepsilon_f)$外部. 因为$x(s)\in\Xi_V\ominus\Omega(\varepsilon_f)$, 所以依据假设3和式(8)可以获得

$$F(x^*(s),u^*(s))\geqslant\alpha_1(\|x(s)\|)\geqslant\alpha_1(\alpha_2^{-1}(\varepsilon_f))>0, \quad (23)$$

其中$s\in[t_{k-1},\ t_k]$. 将式(23)代入式(22)可得

$$J^*(x_\mathrm{a}(t_k+\Delta_N))-J^*(x_\mathrm{a}(t_k))<-(1-\mu)\alpha_1(\alpha_2^{-1}(\varepsilon_f))\Delta_N\triangleq-\xi<0. \quad (24)$$

因此,

$$\begin{aligned}&J^*(x_\mathrm{a}(t_k))-J^*(x_\mathrm{a}(t_{k-1}))<-\xi,\\&J^*(x_\mathrm{a}(t_{k-1}))-J^*(x_\mathrm{a}(t_{k-2}))<-\xi,\\&\quad\vdots\\&J^*(x_\mathrm{a}(t_1))-J^*(x_\mathrm{a}(t_0))<-\xi\end{aligned} \quad (25)$$

成立. 对式(25)左右两项同时求和可得

$$J^*(x_\mathrm{a}(t_k))<-k\xi+J^*(x_\mathrm{a}(t_0))<-k\xi+J_0. \quad (26)$$

所以当$k\to+\infty$时$J^*(x_\mathrm{a}(t_k))\to-\infty$, 但是$J^*(\cdot)$事实上是恒大于0的, 所以上述假设系统(1)一直处于$\Omega(\varepsilon_f)$外不成立, 即$x_\mathrm{a}(s)$会在有限时间内进入终端约束集$\Omega(\varepsilon_f)$.　证毕.

注意, 在双模自触发MPC中系统状态进入$\Omega(\varepsilon)$时, 双模机制中的反馈控制器$\kappa(x)$将作用于系统. 因此, 系统(1)在弹性自触发MPC算法控制下是渐进稳定的, 即$t\to\infty$时$x(t)\to0$.

5　仿真验证

在本节中通过两个不同的非线性系统验证了算法1的有效性. 首先考虑一个移动机器人的位置调节问题. 它的系统模型描述如下:

$$\begin{bmatrix}\dot{x}(t)\\\dot{y}(t)\\\dot{\theta}(t)\end{bmatrix}=\begin{bmatrix}\cos(\theta(t))&0\\\sin(\theta(t))&0\\0&1\end{bmatrix}\begin{bmatrix}v(t)\\\omega(t)\end{bmatrix}, \quad (27)$$

式中: x, y和θ是系统的3个状态, v和ω分别表示线速度和角速度的控制输入. 因此, 系统可以重新定义为$\dot{\chi}(t)=\phi(\chi(t),u(t))$, 其中$\chi=[x;\ y;\ \theta]$, $u=[v;\omega]$, 并设初始位置状态$\chi(t_0)=[1.5;\ 1.5;\ 0]$, 约束条件为$\|v\|\leqslant\bar{v}=2.5$, $\|\omega\|\leqslant\bar{\omega}=7$. 根据文献[11]论述, 本文只考虑机器人位置调节问题而不考虑方向. 机器人位置调节采用文献[9]中的自触发MPC方案, 阶段和终端代价函数分别为$F=\chi^\mathrm{T}Q\chi+u^\mathrm{T}Ru$, $V_f=\chi^\mathrm{T}\chi$; 权重矩阵$Q=0.1I_3$, $R=0.05I_2$; 预测时域$T_P=1.1$ s. 其他参数为$\varepsilon=0.1078$, $\varepsilon_f=0.02$, $N=6$, $\mu=0.99$, 终端控制律$\kappa(x)$为

$$\begin{cases}v(t)=0.6[-x(t)\cos(\theta(t))-y(t)\sin(\theta(t))],\\\omega(t)=0.6[x(t)\sin(\theta(t))-y(t)\cos(\theta(t))].\end{cases} \quad (28)$$

在仿真中, 欺骗攻击将对所有未被保护的控制样本发起攻击. 图4–6展示了弹性自触发MPC抵抗欺骗攻击的效果.

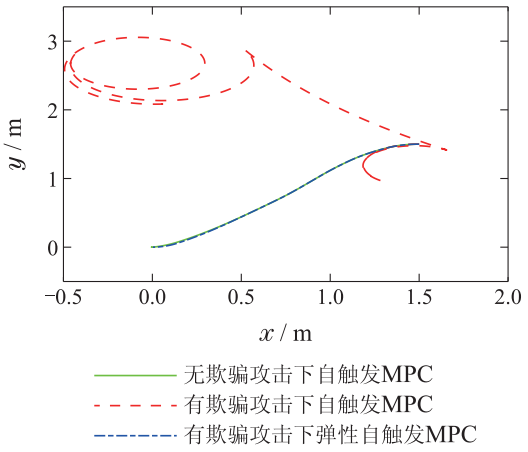

图 4　移动机器人位置调节图

Fig. 4　Diagram of mobile robot position adjustment

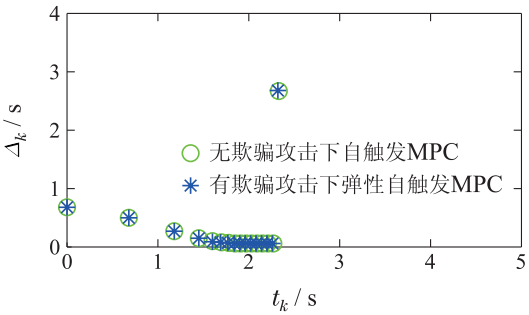

图 5　触发间隔对比

Fig. 5　Comparison of triggered interval

图4中虚线为自触发MPC受欺骗攻击的位置轨迹, 点划线为算法1受欺骗攻击后的状态轨迹, 实线为未

受欺骗攻击的最优位置轨迹. 从图4可以发现弹性自触发MPC在欺骗攻击下可以稳定运行至目标点, 并且运行轨迹与未遭受欺骗攻击时的自触发MPC一致, 但是如果不对控制样本进行保护, 欺骗攻击将对自触发系统产生严重破坏, 致使其失稳. 图5中展示了自触发MPC和受欺骗攻击下弹性自触发MPC的触发间隔, 分别用圆圈和星型标记. 图6横坐标代表每一个被传输的数据包$\boldsymbol{U}^*(t_k)$, 纵坐标对应$\boldsymbol{U}^*(t_k)$中6个控制样本, 其中被保护的控制样本使用阴影进行填充. 结合图4–6可以看出算法1在保证系统性能前提下仅对96个控制样本中的59个进行保护, 节省了38.5%的保护资源.

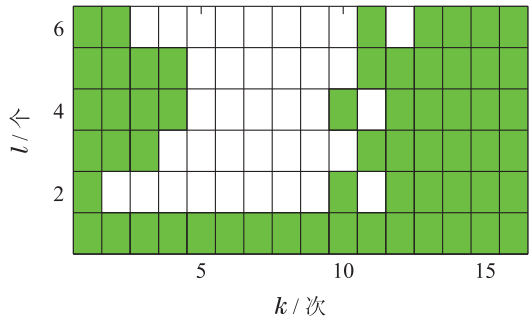

图 6 被保护控制样本

Fig. 6 Protected control samples

为进一步说明算法的有效性, 考虑弹簧小车系统的控制问题, 该系统模型描述如下:

$$\begin{cases} \dot{x}_1(t) = x_2(t), \\ \dot{x}_2(t) = -\dfrac{\tau}{M_{\rm c}}{\rm e}^{-x_1(t)}x_1(t) - \dfrac{h_{\rm d}}{M_{\rm c}}x_2(t) + \dfrac{v(t)}{M_{\rm c}}, \end{cases} \tag{29}$$

其中: $x_1(t)$和$x_2(t)$分别为小车位置和速度, $v(t)$为输入矩阵. 系统中涉及到的参数分别为$M_{\rm c} = 1.25$ kg, $\tau = 0.9$ N/m, $h_{\rm d} = 0.42$ N · s/m并且输入约束为$v(t) \in [-1.8, 1.8]$. 阶段和终端代价函数分别为$F = \chi^{\rm T}Q\chi + u^{\rm T}Ru$, $V_f = \chi^{\rm T}Z\chi$, 相关权重矩阵选择为

$$Q = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix},\ R = [0.1],\ Z = \begin{bmatrix} 0.1692 & 0.0572 \\ 0.0572 & 0.1391 \end{bmatrix}.$$

终端控制律$\kappa(x) = [-0.4454 \quad -1.0932]$, 其设计参数$\varepsilon = 0.1078$.

给定初始状态$x_0 = [1.4 \ \ 1.2]$, 分别将传统自触发MPC[9]和算法1应用于该系统, 图7–8分别展示了弹簧小车在不同情况下的位移对比和速度对比, 图9标记了采用算法1时所需保护的控制样本. 图7–9显示算法1在确保系统稳定的前提下在54个控制样本中只需保护30个(节省44.4%资源), 而系统在不采取任何保护措施时已明显处于发散状态, 说明了算法1的有效性.

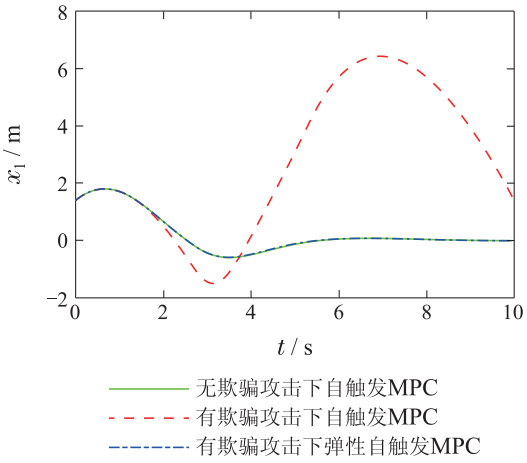

图 7 弹簧小车位移比较

Fig. 7 Comparison of displacements of cart-damper-spring

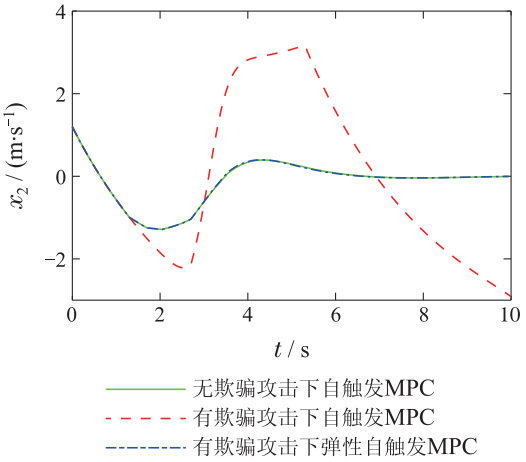

图 8 弹簧小车速度比较

Fig. 8 Comparison of velocities of cart-damper-spring

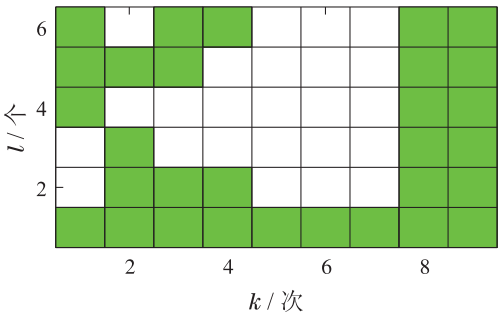

图 9 被保护控制样本

Fig. 9 Protected control samples

6 总结

针对受欺骗攻击的CPS系统, 本文提出了一种弹性自触发MPC算法. 首先, 基于自触发MPC特性和欺骗攻击模型计算出了标称状态与被攻击状态的误差上界; 然后, 依据李雅普诺夫稳定性理论设计了需要被保护控制样本的选取方式, 并对系统的稳定性和可行性进行了理论证明; 最后, 基于机器人和弹簧小车系统进行了仿真实验. 实验结果表明算法1能够保证

系统在遭受欺骗攻击时仍然可以稳定运行, 同时与传统整体保护机制相比, 算法1可以显著地节省保护资源, 因此算法1在自动控制系统中具有广泛的应用价值.

参考文献:

[1] CHEN J C, SHI Y. Stochastic model predictive control framework for resilient cyber-physical systems: Review and perspectives. *Philosophical Transactions of the Royal Society A*, 2021, 379(2207): 20200371.

[2] CHEN Siyun, LIU Ting, SHEN Chao, et al. Smart home energy optimization based on cognition of wearable devices sensor data. *Journal of Computer Research and Development*, 2016, 53(3): 704 – 715.
(陈思运, 刘烃, 沈超, 等. 基于可穿戴设备感知的智能家居能源优化. 计算机研究与发展, 2016, 53(3): 704 – 715.)

[3] KARAMANAKOS P, LIEGMANN E, GEYER T, et al. Model predictive control of power electronic systems: Methods, results, and challenges. *IEEE Open Journal of Industry Applications*, 2020, 1: 95 – 114.

[4] YE B L, WU W M, RUAN K Y, et al. A survey of model predictive control methods for traffic signal control. *IEEE/CAA Journal of Automatica Sinica*, 2019, 6(3): 623 – 640.

[5] YAN Fei, LI Pu, XU Xinying. Traffic signal hybrid control method based on iterative learning and model predictive control. *Control Theory & Applications*, 2021, 38(3): 339 – 348.
(闫飞, 李浦. 续欣莹. 基于迭代学习与模型预测控制的交通信号混合控制方法. 控制理论与应用, 2021, 38(3): 339 – 348.)

[6] LI H P, SHI Y. Event-triggered robust model predictive control of continuous-time nonlinear systems. *Automatica*, 2014, 50(5): 1507 – 1513.

[7] XU Z X, HE L L, HE N, et al. A quasi-differential type event-triggered model predictive control for perturbed continuous linear systems with constraints. *IET Control Theory & Applications*, 2021, 15(18): 2334 – 2343.

[8] CUI D, LI H. Dual self-triggered model-predictive control for nonlinear cyber-physical systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2021, 52(6): 3442 – 3452.

[9] HASHIMOTO K, ADACHI S, DIMAROGONAS D V. Self-triggered model predictive control for nonlinear input-affine dynamical systems via adaptive control samples selection. *IEEE Transactions on Automatic Control*, 2016, 62(1): 177 – 189.

[10] HE N, SHI D W, CHEN T W. Self-triggered model predictive control for networked control systems based on first-order hold. *International Journal of Robust and Nonlinear Control*, 2018, 28(4): 1303 – 1318.

[11] SUN Z Q, DAI L, LIU K, et al. Robust self-triggered MPC with adaptive prediction horizon for perturbed nonlinear systems. *IEEE Transactions on Automatic Control*, 2019, 64(11): 4780 – 4787.

[12] MI X, ZOU Y, LI S, et al. Self-triggered DMPC design for cooperative multiagent systems. *IEEE Transactions on Industrial Electronics*, 2019, 67(1): 512 – 520.

[13] HESHMATI-ALAMDARI S, EQTAMI A, KARRAS G C, et al. A self-triggered position based visual servoing model predictive control scheme for underwater robotic vehicles. *Machines*, 2020, 8(2): 33.

[14] XUN J, YIN J, LIU R, et al. Cooperative control of high-speed trains for headway regulation: A self-triggered model predictive control based approach. *Transportation Research Part C: Emerging Technologies*, 2019, 102: 106 – 120.

[15] LIU J L, YANG M, XIE X P, et al. Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2019, 67(3): 1021 – 1034.

[16] ZHANG T Y, YE D. False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach. *Automatica*, 2020, 120: 109177.

[17] PANG Z H, FAN L Z, SUN J, et al. Detection of stealthy false data injection attacks against networked control systems via active data modification. *Information Sciences*, 2021, 546: 192 – 205.

[18] MA Jing, YE Yong, JIA Qiusheng. Review of resilient control. *Information and Control*, 2015, 44(1): 67 – 75.
(马静, 叶泳, 贾秋生. 弹性控制综述. 信息与控制, 2015, 44(1): 67 – 75.)

[19] WANG J, DING B C, HU J C. Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach. *IEEE Transactions on Automatic Control*, 2020, 66(2): 760 – 767.

[20] WANG K Y, TIAN E G, LIU J L, et al. Resilient control of networked control systems under deception attacks: A memory-event-triggered communication scheme. *International Journal of Robust and Nonlinear Control*, 2020, 30(4): 1534 – 1548.

[21] LIU Y Z, CHEN Y, LI M, et al. MPC for the cyber-physical system with deception attacks. *The 32nd Chinese Control and Decision Conference*. Hefei: IEEE, 2020: 3847 – 3852.

[22] WANG Chenxu, LI Jinghu, YU Mingyan, et al. Power analysis security evaluation on Piccolo based on FPGA platform. *Journal of Electronics & Information Technology*, 2014, 36(1): 101 – 107.
(王晨旭, 李景虎, 喻明艳, 等. 基于FPGA平台的Piccolo功耗分析安全性评估. 电子与信息学报, 2014, 36(1): 101 – 107.)

[23] MAYNE D Q, RAWLINGS J B, RAO C V, et al. Constrained model predictive control: Stability and optimality. *Automatica*, 2000, 36(6): 789 – 814.

[24] CUI D, LI H. Self-triggered model predictive control with adaptive selection of sampling number. *IEEE International Conference on Industrial Cyber Physical Systems.* Taipei: IEEE, 2019: 802 – 807.

[25] WU G G, SUN J, CHEN J. Optimal data injection attacks in cyber-physical systems. *IEEE Transactions on Cybernetics*, 2018, 48(12): 3302 – 3312.

[26] SUN Y C, YANG G H. Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. *International Journal of Robust and Nonlinear Control*, 2019, 29(14): 4797 – 4811.

[27] CHEN H, ALLGÖWER F. A quasi-infinite horizon nonlinear model predictive control scheme with guaranteed stability. *Automatica*, 1998, 34(10): 1205 – 1217.

作者简介:

贺　宁　博士, 教授, 博士生导师, 主要研究方向为鲁棒模型预测控制、基于事件的控制及其在机器人系统中的应用, E-mail: hening@xauat.edu.cn;

马　凯　硕士研究生, 主要研究方向为信息物理系统安全、模型预测控制、自触发控制, E-mail: makai@xauat.edu.cn;

沈　超　博士, 教授, 博士生导师, 主要研究方向为网络物理系统优化与安全、网络与系统安全、人工智能安全, E-mail: chaoshen@xjtu.edu.cn;

徐中显　博士研究生, 主要研究方向为事件触发控制、模型预测控制与网络化控制, E-mail: zhongxianxu@xauat.edu.cn;

钱　成　硕士研究生, 主要研究方向为电力系统状态监测与健康状态估计, E-mail: qiancheng@xauat.edu.cn.