中国科学: 信息科学 2021 年 第 51 卷 第 1 期: 89–103
SCIENTIA SINICA Informationis
论文

稀疏恶意攻击下的信息物理系统的 “PID” 型性能和安全控制

谢春华[1,2], 杨辉[1,2*], 李哲[3]

1. 华东交通大学电气与自动化工程学院, 南昌 330013
2. 江西省先进控制与优化重点实验室, 南昌 330013
3. 湖南大学电气与信息工程学院, 长沙 410082
* 通信作者. E-mail: yhshuo@ecjtu.edu.cn

收稿日期: 2020–03–07; 修回日期: 2020–05–06; 接受日期: 2020–06–29; 网络出版日期: 2020–12–14

国家自然科学基金 (批准号: 61903141, 61903132, 61733005)、中国博士后科学基金 (批准号: 2019M662260) 和江西省自然科学基金 (批准号: 20192BAB217008) 资助项目

摘要 针对遭受稀疏恶意攻击的离散时间线性系统, 本文研究其安全控制问题. 假设恶意攻击者受有限资源的约束, 仅能操控远程控制器和执行器之间的若干通信通道. 对于设计者来说, 并不知道哪些通道受到攻击, 哪些通道没有受到攻击. 本文提出了一种新的安全的远程控制方法, 它由控制律、切换函数和选择机制构成. 选择机制为控制律提供合适的反馈增益, 并产生一个切换函数, 用以阻止攻击信号进入被控对象. 理论分析表明, 在基本的和必要的假设条件下, 本文考虑的安全控制问题可转化为求解状态反馈镇定问题. 本文所提控制方法, 能保证闭环系统的稳定性且使其具有 “PID” 型性能的抗攻击能力. 最后, 通过对某无人地面车辆系统的仿真实验, 验证了理论结果的正确性.

关键词 安全控制, 信息物理系统, 稀疏恶意攻击, 切换策略, 抗攻击性能

1 引言

在过去 20 年里, 集成了物理过程、计算资源和通信能力的信息物理系统的研究得到了广泛关注. 然而, 因网络安全而导致的事故却显著增加 [1]. 从关键基础设施系统到高可靠性军事系统等众多领域均可能遭受网络攻击. 其中著名的网络攻击案例有: 德国钢厂受网络攻击 [2]、震网病毒攻击 [3]、“火焰” 网络病毒攻击 [4], 以及 RQ-170 哨兵无人机因网络原因遭劫持事件 [5]. 因此, 提高信息物理系统的安全性具有强烈的实际需求.

一般来说, 攻击可以通过影响信息物理系统的所有组件实现. 通信网络和计算节点均可能被攻击者入侵. 系统设备 (如传感器、控制器和执行器) 也可能被攻击者蓄意改变. 因此, 信息物理系统的安

引用格式: 谢春华, 杨辉, 李哲. 稀疏恶意攻击下的信息物理系统的 “PID” 型性能和安全控制. 中国科学: 信息科学, 2021, 51: 89–103, doi: 10.1360/SSI-2020-0212
Xie C-H, Yang H, Li Z. Secure control and proportional-integral-derivative performance of cyber-physical systems with sparse adversarial attacks (in Chinese). Sci Sin Inform, 2021, 51: 89–103, doi: 10.1360/SSI-2020-0212

全问题面临两个挑战: (i) 传统的信息安全技术 (如身份验证和加密机制) 可用于防止入侵, 但攻击者仍然可以通过系统设备非侵入式地影响系统; (ii) 针对访问内部网络的攻击, 虽然可以通过加密工具防护, 但是许多信息物理系统限于有限资源的约束, 无法部署大量安全技术 [1]. 鉴于这些原因, 有必要在控制律、估计算法、检测机制等设计层面考虑攻击, 并提供防护.

在控制律、估计算法、检测机制等设计层面, 针对信息物理系统的应用, 现有结果主要研究了传感器调度 [6]、安全状态估计 [7~9]、攻击检测 [10,11] 和安全控制 [12,13] 等子问题. 值得一提的是, 信息物理系统安全控制问题面临众多挑战 [12], 这也是本文要研究的核心问题. 近年来, 人们尝试解决安全控制问题, 并取得了大量的研究成果. 举例来说, 文献 [14] 针对稀疏传感器攻击的信息物理系统, 利用抗攻击状态观测器构造了一个基于安全观测器的控制器. 然而, 由于控制器并不能阻止执行器攻击进入被控对象中, 导致这种方法不能被用来处理执行器攻击的情况. 此外, 针对拒绝服务攻击 [15~19]、“状态 – 依赖” 型攻击 [20]、随机网络攻击 [21,22] 和恶意切换攻击 [23], 数种不同类型的安全控制器被提出. 不幸的是, 拒绝服务攻击、“状态 – 依赖” 型攻击、随机网络攻击、恶意切换攻击和稀疏攻击的本质区别, 使得这些方法不能被扩展到稀疏恶意攻击的情况. 除此之外, 有学者利用补偿器来处理攻击 [24~26], 但是需要对攻击做严格的假设, 如强稀疏可检测性. 当然, 还有一些其他的研究结果, 如文献 [27,28]. 然而, 就我们所知, 对于离散时间线性系统而言, 安全的远程控制设计仍然是一个活跃的且富有挑战性的问题. 对于远程控制器和执行器之间的通信通道可能遭受稀疏恶意攻击, 安全远程控制设计问题还没有得到很好的研究. 这是本文工作的研究动机.

另一方面, 由于互联网数据通信网络技术的飞速发展, 网络控制应用受到了广泛的关注 [29~31]. 这些实际应用包括远程移动机器人 [32]、电力系统 [33]、灌溉系统 [34]、工厂自动化等, 它们是通过系统设备之间的有线或无线连接构成的. 远程控制体系结构的主要优点有: (i) 控制系统设计易于维护和扩展; (ii) 系统操作员的安全 (如核工业) 可得到有效保障; (iii) 减少了系统携带的设备, 如无人地面车辆、航空航天器. 因此, 本文所研究的问题具有重要的实际意义.

本文研究带有干扰和稀疏恶意攻击的离散时间线性信息物理系统的安全远程控制问题, 主要贡献归纳如下.

(a) 本文提出了一种新的安全远程控制方法, 该方法由控制律、切换函数和选择机制构成, 可应用于存在外界干扰的系统.

(b) 本文将安全控制问题转化为求解状态反馈镇定问题. 此外, 所提控制器能保证闭环系统的稳定性且使其具有 “PID” 型性能的抗攻击能力. 值得注意的是, 虽然安全控制问题已有所研究 [13,26], 但信息物理系统的 “PID” 型性能并不能得到保证.

本文结构安排如下. 在第 2 节的问题描述之后, 第 3 节介绍了所提出方法的主要思想, 即安全控制器的设计. 第 4 节给出了某无人地面车辆系统的仿真实验. 最后第 5 节是结论部分.

符号说明. A^{T} 表示矩阵 A 的转置. 对于给定的 $p,q\in\mathbb{N}$ 且满足 $p\geqslant q$, C_p^q 表示 p 取 q 的组合数. $\mathrm{diag}\{s_1,s_2,\ldots,s_n\}$ 表示对角矩阵且主对角元素分别为 $s_1,s_2,\ldots,s_n$. 令 $\mathrm{card}(\mathbb{M})$ 和 $\mathrm{supp}(x)$ 分别表示集合 $\mathbb{M}$ 的基数和向量 x 的支撑集. I 表示适当维数的单位矩阵.

2 问题描述

2.1 系统结构

恶意攻击下的安全控制系统架构如图 1 所示. 考虑到便于控制系统设计的维护/扩展, 确保系统操作员的安全, 减少系统携带设备等原因, 控制器被安装在远程端. 例如, 在铀浓缩工厂中, 监视控制

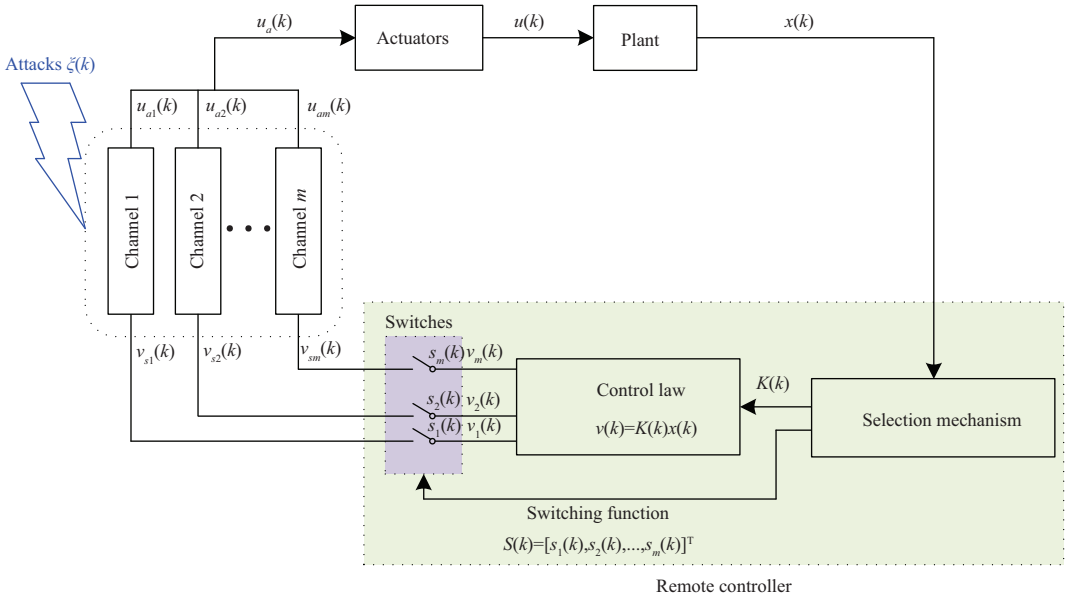

图 1 (网络版彩图) 恶意攻击下的安全控制体系结构

Figure 1 (Color online) Secure control architecture under malicious attacks

远离离心机, 以确保系统操作员的安全 [3]. 远程控制器通过通信网络将控制信号传送至执行器, 该方式常见于远程控制系统 [29,35,36]. 由于通信网络可能不完全可靠, 远程控制器和执行器之间交换的数据可能会出现异常. 比如, 攻击者试图拦截和修改传输数据, 这可能会降低系统控制性能. 本文假设攻击者受有限资源的约束, 只能操控若干通信通道 [7]. 针对每种攻击情况, 设计相应的反馈增益 $K(k)$, 以保证系统的稳定性和良好的性能. 在每一时刻, 如何选择反馈增益, 由第 3 节的算法 1 中的选择机制来确定. 切换函数 $S(k)=\{s_1(k),s_2(k),\ldots,s_m(k)\}$ 也由该机制决定, 用于帮助搜索未知的被攻击通信通道, 进而关闭被攻击的通信通道, 最终达到防止攻击信号进入被控对象中.

注释1 在图 1 中, 如果违反了 "PID" 型性能条件 $J_P(k)\leqslant H_P\left(k_0,k,\delta_\omega,x(k_0)\right)$, $J_I(k_0,k)\leqslant H_I\left(k_0,k,\delta_\omega,\ x(k_0)\right)$, $J_D(k)\leqslant H_D\left(k_0,k,\delta_\omega,x(k_0)\right)$ (详情请见算法 1), 选择机制将会通知控制律模块, 让其选择下一个候选反馈增益 $K(k)$, 并且通过重构切换函数 $S(k)$ 的值控制开关的 "开/关" 状态. 函数 $J_P(\cdot),J_I(\cdot),J_D(\cdot),H_P(\cdot),H_I(\cdot),H_D(\cdot)$ 的定义将在 (10)~(12), (18), (20) 和 (21) 中给出. 算法 1 将显示: 选择机制通知下一个模块更新增益的次数不会超过 $\sum_{j=0}^{a_{\max}}C_m^j-1$ 次. 值得指出的是, 本文采用的方法与去伪切换监督控制 [37,38] 有相似之处. 去伪监督控制的主要思想是构造候选控制器来控制不确定被控对象. 不同的是, 本文所提控制器针对的是网络通信不可靠的被控对象.

注释2 控制向量 $v(k)$ 的数据传输方式大致可分为两类: (a) 分别传输 $v(k)$ 的每个分量; (b) 打包传输所有分量. 注意, 恶意攻击者可能拥有有限的资源并操控若干通信通道 [7]. 因此, 为了提高系统抗稀疏攻击的能力, $v(k)$ 的各个分量将被分开传输, 这也是本文采用的数据传输方式. 此外, 执行器可以安装在不同的位置, 这也可能会导致 $v(k)$ 中的各个分量分开传输.

2.2 被控对象模型

考虑如下遭受恶意攻击的线性被控对象:

$$x(k+1)=Ax(k)+Bu(k)+B_\omega\omega(k), \tag{1}$$

其中 $k \in \mathbb{N}$ 表示时间, $x(k) \in \mathbb{R}^n$ 为状态向量, $u(k) \triangleq [u_1(k), u_2(k) \ldots, u_m(k)]^{\mathrm{T}} \in \mathbb{R}^m$ 是作用于被控对象的控制量, A, B 和 B_ω 为已知实数常矩阵. 此外, 向量 $\omega(k) \in \mathbb{R}^\omega$ 代表过程干扰.

假设1 $\omega(k)$ 是未知有界的 [39], 即存在某个常数 $\delta_\omega \geqslant 0$ 使得 $\|\omega(k)\| \leqslant \delta_\omega, \forall k \geqslant 0$.

2.3 切换函数

由图 1 中的开关 $S_1, S_2, \ldots, S_m$, 可得

$$v_{si}(k) = \begin{cases} v_i(k), & \text{如果第 } i \text{ 个开关 } S_i \text{ 是关闭的,} \\ \text{NULL}, & \text{如果第 } i \text{ 个开关 } S_i \text{ 是开启的,} \end{cases} \tag{2}$$

其中 “NULL” 表示没有数据在传输.

为了简洁起见, 采用 $s_i(k) \in \{0, 1\}$ 来描述开关 S_i 的 “开/关” 状态: (a) $s_i(k) = 0$ 表示开关 S_i 处于 “开” 位置; (b) $s_i(k) = 1$ 表示开关 S_i 处于 “ 关” 位置. 那么, 可以将 (2) 重新写成

$$v_{si}(k) = \begin{cases} v_i(k), & s_i(k) = 1, \\ \text{NULL}, & s_i(k) = 0. \end{cases} \tag{3}$$

2.4 攻击模型

假设攻击者能够截获并修改传输中的数据. 如果通信通道中没有数据在传输, 无数据可供攻击者截获, 在这种情况下假设攻击者不注入攻击信号. 具体来说, 攻击者将原始数据 $v_{si}(k)$ 更改为 $u_{ai}(k)$ 后发送给执行器 (请见图 1), 即

$$u_{ai}(k) = \begin{cases} v_{si}(k) + \xi_i(k), & s_i(k) = 1, \\ \text{NULL}, & s_i(k) = 0, \end{cases} \tag{4}$$

其中 $\xi_i(k)$ 表示由恶意攻击者注入到第 i 个通信通道上的攻击信号; $u_{ai}(k)$ 表示攻击者将 $v_{si}(k)$ 修改后形成的信号. 当第 i 个通道没有数据在传输时, 没有数据可供截获, 攻击者不注入攻击信号. 在现实中, 由于资源有限, 攻击者也许只能操控若干通信通道 [7]. 正是由于这一原因, 稀疏攻击被广泛研究, 比如文献 [7,8,10,13,14,24]. 根据上述实际情况, 本文假设攻击者最多操控 $a_{\max}$ 个远程控制器和执行器之间的通信通道, 并且设计者不知道哪些通道被攻击者攻击了, 其中整数 $a_{\max}$ 将在假设 2 中加以解释和说明. 换句话说, $\mathrm{card}(\mathbb{K}) \leqslant a_{\max}$, 其中 $\mathbb{K} \triangleq \mathrm{supp}(\xi(k))$, $\xi(k) \triangleq [\xi_1(k), \xi_2(k), \ldots, \xi_m(k)]^{\mathrm{T}}$. 假设 $\mathbb{K}$ 为未知时不变集合. 对于设计者来说, 并不知道 $\xi_i(k), i = 1, 2, \ldots, m$ 中哪些是非零的. 显然, $\mathbb{K}$ 也可以用来表示远程控制器和执行器之间的被攻击者操控的通信通道所组成的集合. 由于网络带宽的物理限制, 无法在传输的数据中注入无穷大的攻击信号. 为此, $\xi(k)$ 可被视为任意有界实值函数, 但不遵循任何特定模型.

2.5 执行器模型

假设执行器在接收到控制信号后, 输出其接收到的控制信号. 否则, 执行器输出为零, 例如, 如果第 i 个通信通道中没有数据传输, 那么第 i 执行器的输出为零. 执行器可描述为

$$u_i(k) = \begin{cases} u_{ai}(k), & s_i(k) = 1, \\ 0, & s_i(k) = 0. \end{cases} \tag{5}$$

于是, 结合式 (3)∼(5), 可以得到

$$u_i(k) = s_i(k)\left(v_i(k) + \xi_i(k)\right), \quad i = 1, 2, \ldots, m. \tag{6}$$

因此, 系统 (1) 可以进一步重写为如下系统:

$$x(k+1) = Ax(k) + BS(k)\left(v(k) + \xi(k)\right) + B_\omega \omega(k), \tag{7}$$

其中, $S(k) \triangleq \mathrm{diag}\{s_1(k), s_2(k), \ldots, s_m(k)\}$, $v(k) \triangleq [v_1(k), v_2(k), \ldots, v_m(k)]^{\mathrm{T}}$.

注释3 $\xi(k)$ 也可以用来描述通信通道故障或执行器故障 [40, 41], 且不会影响本文主要结果.

注释4 由于控制信号 $v(k)$ 在通信传输过程中可能会遭受恶意攻击, 有时可能需要传输冗余信息, 比如传输 $[v^{\mathrm{T}}(k), v^{\mathrm{T}}(k)]^{\mathrm{T}}$. 在这种情况下, 仍可以采用本文所提方法类推并加以解决, 故本文仅仅考虑传输 $v(k)$ 的情况.

2.6 远程控制器

由于远程控制器和执行器之间最多有 $a_{\max}$ 个通信通道遭受到攻击, 并且被攻击的通信通道对于设计者来说是未知的. 因此, 从设计者的角度来看, 有 $\sum_{j=0}^{a_{\max}} C_m^j$ 种可能的攻击情形. 很显然, 期望设计 $\sum_{j=0}^{a_{\max}} C_m^j$ 个反馈增益候选集合. 针对每一种攻击情形, 能从增益候选集中选择合适的反馈增益, 使得系统具有一个理想的行为. 需要注意的是, 由于攻击情形的不确定性, 需要建立一个选择机制来选择合适的反馈增益 $K(k)$ 和切换函数 $S(k)$.

具体来说, 根据 $\sum_{j=0}^{a_{\max}} C_m^j$ 种可能的攻击情形, 将设计 $\sum_{j=0}^{a_{\max}} C_m^j$ 个相应的反馈增益 $K_{\mathbb{J}}$, 其中集合 $\mathbb{J}$ 满足 $\mathbb{J} \subseteq \{1, \ldots, m\}$ 和 $\mathrm{card}(\mathbb{J}) \leqslant a_{\max}$. 为了便于记忆, 针对于集合 $\mathbb{J}$ 中的通信通道被恶意攻击者操控而 $\bar{\mathbb{J}}$ 中的通信通道没有受到攻击的情况, 令 $K_{\mathbb{J}}$ 为该情况下被设计的反馈增益, 其中 $\bar{\mathbb{J}} \triangleq \{1, 2, \ldots, m\} \setminus \mathbb{J}$.

基于攻击模型 (4), 远程控制律设计如下:

$$v(k) = K(k)x(k), \tag{8}$$

其中反馈增益 $K(k) \in \{K_{\mathbb{J}} | \mathbb{J} \subseteq \{1, 2, \ldots, m\}, \mathrm{card}(\mathbb{J}) \leqslant a_{\max}\}$.

由式 (7) 和 (8) 组成的闭环系统可以描述为

$$x(k+1) = \left(A + BS(k)K(k)\right)x(k) + BS(k)\xi(k) + B_\omega \omega(k). \tag{9}$$

2.7 设计目标

为了达到控制目标, 对系统 (1) 和攻击模型 (4) 做如下必要假设.

假设2 对于满足 $\mathbb{J} \subseteq \{1, 2, \ldots, m\}$ 和 $\mathrm{card}(\mathbb{J}) = a_{\max}$ 的任意集合 $\mathbb{J}$, 总存在一个状态反馈控制器, 能镇定由 $(A, B|_{\bar{\mathbb{J}}})$ 描述的系统. 此外, $(*)|_{\bar{\mathbb{J}}}$ 表示在矩阵 $*$ 中, 由列号在集合 $\bar{\mathbb{J}}$ 中的列所构成的新矩阵.

注释5 当远程控制器和执行器之间有 $a_{\max}$ 个通信通道遭受攻击时, $v(k)$ 中将有 $a_{\max}$ 个分量被篡改. 因此, 要求剩余的 $m - a_{\max}$ 个未被攻击的控制分量能镇定系统. 由此可见, 假设 2 是镇定系统的必要条件.

注释6 由假设 2 可知, $a_{\max}$ 取决于系统参数 (A, B), 反映着系统的固有特性, 故 $a_{\max}$ 可被视为系统操作员的一个设计参数 [7]. 显然, $a_{\max}$ 可以通过系统参数 (A, B) 事先加以确定. 因此, 当攻击

者在远程控制器和执行器之间最多操控 $a_{\max}$ 个通信通道时, 可以事先验证假设 2 是否满足. 此外, $a_{\max}$ 的值越大, 意味着系统在攻击下的安全控制能力越强, $a_{\max}$ 决定着系统抵御稀疏恶意攻击的能力. 基于上述原因, 本文假设攻击者的行为在系统的抵御能力范围内, 即满足假设 2. 类似的假设可见文献 [7,8,10,13,14,24].

注释7 从假设 2 可以看出, 同时遭受攻击的通信通道的最大个数是最大正整数 p, 使得系统 $(A, B|_{\bar{\mathbb{J}}})$ 对所有 $\bar{\mathbb{J}} \triangleq \{1,2,\ldots,m\}\setminus\mathbb{J}$ 是可镇定的, 其中 $\mathbb{J}\subseteq\{1,2,\ldots,m\}$, $\mathrm{card}(\mathbb{J})=p$. 令 p^* 为最大的正整数 p. 可以很容易地验证 $a_{\max}$ 可以从 $\{0,1,2,\ldots,p^*\}$ 中选择任意整数. 另外, 值得一提的是, 根据注释 6, 建议将 $a_{\max}$ 选定为 p^*, 以提高系统在攻击下的安全控制能力.

受 PID 控制的启发, 本文将考虑 “PID” 型性能, 旨在实现如下控制目标.

控制目标. 在假设 1 和 2 下, 设计反馈增益 $K(k)$ 和切换函数 $S(k)$, 使得闭环系统 (9) 是稳定的, 且具有一定的抗攻击性能. 具体地说, $\exists k_0\in\mathbb{N}$, 使得对于所有的 $k\geqslant k_0$, 性能指标 $J_{\mathrm{P}}(k), J_{\mathrm{I}}(k_0,k), J_{\mathrm{D}}(k)$ 的界不依赖于攻击, 其中 $J_{\mathrm{P}}(k), J_{\mathrm{I}}(k_0,k), J_{\mathrm{D}}(k)$ 的定义如下.

(P1) “比例” 型 (proportional-type, P 型) 性能指标:

$$J_{\mathrm{P}}(k)\triangleq\|x(k)\|. \tag{10}$$

(P2) “积分” 型 (integral-type, I 型) 性能指标:

$$J_{\mathrm{I}}(k_0,k)\triangleq\frac{1}{k-k_0+1}\sum_{\tau=k_0}^{k}x^{\mathrm{T}}(\tau)Qx(\tau), \tag{11}$$

其中 $Q>0$ 是给定的权矩阵.

(P3) “差分” 型 (derivative-type, D 型) 性能指标:

$$J_{\mathrm{D}}(k)\triangleq\|x(k)-x(k-1)\|. \tag{12}$$

注释8 由于攻击信号 $\xi(k)$ 是攻击者蓄意设计的, 它的值可能是大的, 变化快的. 在这种情况下, 传统的鲁棒控制器可能会导致系统状态不能收敛到原点的一个小邻域内, 从而导致不理想的稳态性能. 为了有效地应对上述情况, 有必要寻求针对恶意攻击的安全控制方法, 使闭环系统稳定并具有一定的抗攻击性能.

3 抗攻击控制器和选择机制设计

如 2.6 小节所述, 需要设计一组反馈控制增益 $K_{\mathbb{J}}$. 此外, $K_{\mathbb{J}}$ 是针对如下攻击情况进行设计的: 集合 $\mathbb{J}$ 中的通信通道被恶意攻击者操控, 而 $\bar{\mathbb{J}}$ 中的通信通道没有受到攻击. 在这种攻击情形下, 反馈增益 $K(k)$ 的理想值为 $K_{\mathbb{J}}$.

切换函数 $S(k)$ 将用于帮助搜索被攻击的通信通道, 并阻止攻击信号进入被控对象中. 例如, 考虑一种简单情景, 即远程控制器和执行器之间的第 i 个通信通道被攻击者操控, 因此, 可以从式 (6) 和 (7) 可知, 信号 $s_i(k)(v_i(k)+\xi_i(k))$ 将进入被控对象中. 在这种情况下, $s_i(k)$ 被期望设计为 $s_i(k)=0$, 使得 $s_i(k)\xi_i(k)=0$, 从而阻止攻击信号 $\xi_i(k)$ 进入被控对象中.

综上所述, 如果我们知道 $\mathbb{J}$ 中的通信通道被攻击者操控且 $\bar{\mathbb{J}}$ 中的通信通道未受到攻击, 则可以设计反馈增益 $K(k)$ 和切换函数 $S(k)$ 以遵守如下理想原则:

$$K(k)=K_{\mathbb{J}},\ s_i(k)=\begin{cases}1,\ i\in\bar{\mathbb{J}},\\ 0,\ i\in\mathbb{J}.\end{cases}\tag{13}$$

由式 (9) 和 (13) 可知, 在理想情况 (13) 下, 闭环系统可以写成

$$x(k+1)=(A+BS(k)K_{\mathbb{J}})\,x(k)+BS(k)\xi(k)+B_\omega\omega(k)=\left\{A+(B|_{\bar{\mathbb{J}}})\left((K_{\mathbb{J}})|^{\bar{\mathbb{J}}}\right)\right\}x(k)+B_\omega\omega(k),\tag{14}$$

其中 $(K_{\mathbb{J}})|^{\bar{\mathbb{J}}}$ 表示在矩阵 $K_{\mathbb{J}}$ 中, 由行号在集合 $\bar{\mathbb{J}}$ 中的行所构成的新矩阵. 另一方面, 可以很容易地证明假设 2 等价于: 对于所有满足 $\mathrm{card}(\mathbb{J})\leqslant a_{\max}$ 的 $\mathbb{J}$, 始终存在一个对应的状态反馈增益 $K(\mathbb{J})$ 使得 $A+(B|_{\bar{\mathbb{J}}})K(\mathbb{J})$ 是 Schur 的. 考虑到这一点, 反馈增益 $K_{\mathbb{J}}$ 可以很容易由 $(K_{\mathbb{J}})|^{\bar{\mathbb{J}}}=K(\mathbb{J})$ 加以确定. 在这样的反馈增益 $K_{\mathbb{J}}$ 控制下, 闭环系统 (14) 的稳定性将得到保证. 此外, 为了使得闭环系统 (14) 具有良好的控制性能, 可以基于 H_∞ 或 H_2 控制理论来设计 $K_{\mathbb{J}}$.

如前所述, 如果已知 $\mathbb{J}$ 中的通信通道被攻击者侵入而 $\bar{\mathbb{J}}$ 中的通道没有被攻击的话, 则反馈增益 $K_{\mathbb{J}}$ 可用于镇定系统, 并且切换函数 $S(k)$ 可防止攻击信号进入被控对象中. 在下面的定理中, 我们将分析在这种理想情况下的系统响应.

定理1 在假设 1 和 2 下, 考虑时间区间 $[k_0,k]$ 上闭环系统 (9). 如果 $\mathbb{K}\subseteq\mathbb{J}\subseteq\{1,2,\ldots,m\}$, 那么 $\forall\tau\in[k_0,k]$ 设计如下反馈增益 $K(k)$ 和切换函数 $S(k)$:

$$K(\tau)=K_{\mathbb{J}},\ s_i(\tau)=\begin{cases}1,\ i\in\bar{\mathbb{J}},\\ 0,\ i\in\mathbb{J},\end{cases}\tag{15}$$

其中 $K_{\mathbb{J}}$ 是按照假设 2 来设计的, 使得 $A+(B|_{\bar{\mathbb{J}}})((K_{\mathbb{J}})|^{\bar{\mathbb{J}}})$ 是 Schur 的. 那么, 闭环系统将具有 "PID" 型性能, 即满足式 (18), (20) 和 (21).

证明 由 $\mathbb{K}\subseteq\mathbb{J}\subseteq\{1,2,\ldots,m\}$ 和 (15), 可得 $S(\tau)\xi(\tau)=0$, $\forall\tau\in[k_0,k]$. 于是, 式 (9) 可推出式 (14), 即

$$x(\tau+1)=\underbrace{\left\{A+(B|_{\bar{\mathbb{J}}})\left((K_{\mathbb{J}})|^{\bar{\mathbb{J}}}\right)\right\}}_{\mathtt{A}}x(\tau)+B_\omega\omega(\tau).\tag{16}$$

容易得到

$$x(k)=\mathtt{A}^{k-k_0}x(k_0)+\sum_{\tau=k_0}^{k-1}\mathtt{A}^{k-\tau-1}B_\omega\omega(\tau).\tag{17}$$

通过简单的数学运算, 可知

$$J_{\mathrm{P}}(k)\leqslant\|\mathtt{A}^{k-k_0}x(k_0)\|+\delta_\omega\left\|\sum_{\tau=k_0}^{k-1}\mathtt{A}^{k-\tau-1}B_\omega\right\|\triangleq H_P\left(k_0,k,\delta_\omega,x(k_0)\right).\tag{18}$$

考虑 D 型性能指标 $J_{\mathrm{D}}(k)$, 容易得到

$$x(k)-x(k-1)=\mathtt{A}^{k-k_0}x(k_0)+\sum_{\tau=k_0}^{k-1}\mathtt{A}^{k-\tau-1}B_\omega\omega(\tau)$$

$$- \mathtt{A}^{k-k_0-1}x(k_0) - \sum_{\tau=k_0}^{k-2} \mathtt{A}^{k-\tau-2}B_\omega\omega(\tau), \tag{19}$$

上式蕴含着

$$\begin{aligned} J_{\mathrm{D}}(k) &= \|x(k)-x(k-1)\| \\ &\leqslant \left\|\left((\mathtt{A}-I)\mathtt{A}^{k-k_0-1}\right)x(k_0)\right\| + \delta_\omega\left\{\left\|(\mathtt{A}-I)\sum_{\tau=k_0}^{k-2}\mathtt{A}^{k-\tau-2}B_\omega\right\| + \|B\|\right\} \\ &\triangleq H_D\left(k_0,k,\delta_\omega,x(k_0)\right). \end{aligned} \tag{20}$$

接下来, 考虑 I 型性能指标 $J_{\mathrm{I}}(k_0,k)=\frac{1}{k-k_0+1}\sum_{h=k_0}^{k}x^{\mathrm{T}}(h)Qx(h)$. 借助式 (17) 和一些数学运算, 可得

$$\begin{aligned} J_{\mathrm{I}}(k_0,k) \leqslant{}& \frac{1}{k-k_0+1}\sum_{h=k_0}^{k}\left\|x^{\mathrm{T}}(k_0)\left(\mathtt{A}^{h-k_0}\right)^{\mathrm{T}}Q\mathtt{A}^{h-k_0}x(k_0)\right\| \\ &+ \frac{\delta_\omega^2}{k-k_0+1}\sum_{h=k_0}^{k}\sum_{\tau_2=k_0}^{h-1}\sum_{\tau_1=k_0}^{h-1}\left\|\left(\mathtt{A}^{h-\tau_1-1}B_\omega\right)^{\mathrm{T}}Q\mathtt{A}^{h-\tau_2-1}B_\omega\right\| \\ &+ \frac{2\delta_\omega}{k-k_0+1}\sum_{h=k_0}^{k}\sum_{\tau=k_0}^{h-1}\left\|\left(\mathtt{A}^{h-\tau-1}B_\omega\right)^{\mathrm{T}}Q\mathtt{A}^{h-k_0}x(k_0)\right\| \\ \triangleq{}& H_I\left(k_0,k,\delta_\omega,x(k_0)\right). \end{aligned} \tag{21}$$

注释9 因为 $H_P\left(k_0,k,\delta_\omega,x(k_0)\right)$, $H_I\left(k_0,k,\delta_\omega,x(k_0)\right)$ 和 $H_D\left(k_0,k,\delta_\omega,x(k_0)\right)$ 没有依赖攻击信号 $\xi(k)$, 所以 “PID” 型性能 (18), (20) 和 (21) 是抗攻击的. 此外, 在定理 1 中, 根据 $\mathtt{A}$ 是 Schur 的, 容易证明 $H_P\left(k_0,k,\delta_\omega,x(k_0)\right), H_I\left(k_0,k,\delta_\omega,x(k_0)\right)$ 和 $H_D\left(k_0,k,\delta_\omega,x(k_0)\right)$ 的有界性.

依照定理 1 可知, 如果可以设计 $K(k)$ 和 $S(k)$ 阻止攻击信号进入被控对象中, 则 “PID” 型性能将满足 (18), (20), (21), 并且性能指标的界与攻击信号无关. 不幸的是, 对于设计者来说, 不知道哪些通信通道受到攻击, 哪些没有受到攻击. 因此, 定理 1 还不足以让设计者处理由攻击引起的控制问题. 那么, 当攻击通信通道未知时, 又如何设计 $K(k)$ 和 $S(k)$? 由定理 1, 很自然地联想到其反问题: 可否使用 (18), (20), (21) 作为标准, 来决定是否需要重新配置 $K(k)$ 和 $S(k)$? 幸运的是, 答案是肯定的, 并将在本文后续部分给出证明.

接下来, 将展示如何在每一时刻更新反馈增益 $K(k)$ 和切换函数 $S(k)$. 首先, 构造这样一个长度为 $\sum_{j=0}^{a_{\max}}C_m^j$ 的序列 $\mathbb{J}_1\mathbb{J}_2\mathbb{J}_3\cdots\mathbb{J}_{\sum_{j=0}^{a_{\max}}C_m^j}$ 以满足如下 3 个规则:

(i) $\mathbb{J}_i\neq\mathbb{J}_j, \forall i\neq j$ 且 $i,j\in\{1,2,\ldots,\sum_{j=0}^{a_{\max}}C_m^j\}$;

(ii) $\mathbb{J}_i$ 是 $\{1,2,\ldots,m\}$ 的子集且满足 $i\in\{1,2,\ldots,\sum_{j=0}^{a_{\max}}C_m^j\}$ 和 $\mathrm{card}\left(\mathbb{J}_i\right)\leqslant a_{\max}$;

(iii) $\mathrm{card}(\mathbb{J}_1)\leqslant\mathrm{card}(\mathbb{J}_2)\leqslant\cdots\leqslant\mathrm{card}(\mathbb{J}_{\sum_{j=0}^{a_{\max}}C_m^j})$,

其中, $\mathbb{J}_i$ 表示远程控制器和执行器之间可能的被攻击通信通道集合. 该序列中的元素根据被攻击的通信通道数目由少到多进行排序.

借助于序列 $\mathbb{J}_1\mathbb{J}_2\mathbb{J}_3\cdots\mathbb{J}_{\sum_{j=0}^{a_{\max}}C_m^j}$, 提出算法 1, 用以选择并更新 $K(k)$ 和 $S(k)$.

注释10 在算法 1 中, 候选的反馈增益总数是一个组合数, 这可能会导致切换搜索过程时间长, 从而在一定程度上限制了所提方法的可推广性. 为了降低计算复杂度, 可使用集合覆盖方法 [42] 来有效地减少候选增益数.

算法 1 Secure control with selection mechanism

Require: Closed-loop system (9) under Assumptions 1 and 2; Given sequence $\mathbb{J}_1\mathbb{J}_2\mathbb{J}_3\cdots\mathbb{J}_{\sum_{j=0}^{a_{\max}} C_m^j}$.

Initialization: $k_0=0$; $k=0$; $\ell(0)=1$.

while $k\geqslant 0$ **do**

Let $\mathbb{J}(k)=\mathbb{J}_{\ell(k)}$.

Select the feedback gain for the system (9):

$$K(k)=K_{\mathbb{J}(k)}. \tag{22}$$

Design the switching function $S(k)$:

$$s_i(k)=\begin{cases}1,\ i\in\bar{\mathbb{J}}(k),\\ 0,\ i\in\mathbb{J}(k).\end{cases} \tag{23}$$

if "PID" performance satisfies

$$\begin{cases}J_P(k)\leqslant H_P\left(k_0,k,\delta_\omega,x(k_0)\right),\\ J_I(k_0,k)\leqslant H_I\left(k_0,k,\delta_\omega,x(k_0)\right),\\ J_D(k)\leqslant H_D\left(k_0,k,\delta_\omega,x(k_0)\right).\end{cases} \tag{24}$$

then

$\ell(k+1)=\ell(k)$.

else

$\ell(k+1)=\ell(k)+1, k_0=k+1$; % Prepare the reselection for $K(k+1)$ and $S(k+1)$.

end if

$k\leftarrow k+1$.

end while

定理2 在假设 1 和 2 下, 考虑闭环系统 (9). 如果反馈增益 $K(k)$ 和切换函数 $S(k)$ 由算法 1 确定, 那么存在一个有限常数 $k^*\in\mathbb{N}$ 使得对于所有的 $k\geqslant k^*$, 性能指标 $J_{\rm P}(k)$, $J_{\rm I}(k^*,k)$, $J_{\rm D}(k)$ 具有如下特征:

$$\begin{cases}J_{\rm P}(k)\leqslant H_P\left(k^*,k,\delta_\omega,x(k^*)\right),\\ J_{\rm I}(k^*,k)\leqslant H_I\left(k^*,k,\delta_\omega,x(k^*)\right),\\ J_{\rm D}(k)\leqslant H_D\left(k^*,k,\delta_\omega,x(k^*)\right).\end{cases} \tag{25}$$

证明 根据集合 $\mathbb{K}$ 和 $\mathbb{J}_i$ 的定义, 可知 $\mathbb{K}$ 在序列 $\mathbb{J}_1\mathbb{J}_2\cdots\mathbb{J}_{\sum_{j=0}^{a_{\max}} C_m^j}$ 中. 不失一般性, 可假设序列的第 $\hbar$ 个元素是 $\mathbb{K}$, 即, $\mathbb{J}_\hbar=\mathbb{K}$, 其中 $1\leqslant\hbar\leqslant\sum_{j=0}^{a_{\max}} C_m^j$.

接下来, 我们将通过反证法证明 $\sup_{k\in\mathbb{N}}\ell(k)\leqslant\sum_{j=0}^{a_{\max}} C_m^j$. 依照反证法思路, 假设 $\sup_{k\in\mathbb{N}}\ell(k)>\sum_{j=0}^{a_{\max}} C_m^j$. 由算法 1 易知, $\ell(k)$ 在 $\ell(0)=1$ 的初始条件下, 按照 $\ell(k+1)=\ell(k)$ 或 $\ell(k+1)=\ell(k)+1$ 进行更新, 故 $\ell(k)$ 是递增的. 显然, 如果 $\sup_{k\in\mathbb{N}}\ell(k)>\sum_{j=0}^{a_{\max}} C_m^j$, 那么一定存在一个常数 $k_{\rm exist}\in\mathbb{N}$ 使得 $\ell(k_{\rm exist})=\hbar$ 和 $\ell(i)<\hbar,\forall i<k_{\rm exist}$. 由于 $\ell(k_{\rm exist})=\hbar$ 和 $\mathbb{J}_{\ell(k_{\rm exist})}=\mathbb{K}$, 且根据定理 1, 可得出式 (18), (20), (21) 在时间区间 $[k_{\rm exist},k_{\rm exist}+1]$ 上总是成立的. 进而根据算法 1 可得 $\ell(k_{\rm exist}+1)=\hbar$ 和 $\mathbb{J}_{\ell(k_{\rm exist}+1)}=\mathbb{K}$. 由数学归纳法, 可证明 $\ell(i)=\hbar,\forall i\geqslant k_{\rm exist}$. 从上述分析可知 $\ell(k)\leqslant\hbar\leqslant\sum_{j=0}^{a_{\max}} C_m^j,\forall k\in\mathbb{N}$, 这与假设 $\sup_{k\in\mathbb{N}}\ell(k)>\sum_{j=0}^{a_{\max}} C_m^j$ 相矛盾. 于是, $\sup_{k\in\mathbb{N}}\ell(k)\leqslant\sum_{j=0}^{a_{\max}} C_m^j$, 并且易知 $\ell(k)$ 不会超过序列元素总数.

由于 $\ell(k)$ 递增且有界, 所以 $\ell(k)$ 是收敛的. 那么, 一定存在一个常数 $k^*\in\mathbb{N}$ 使得 $\|\ell(k)-\ell^*\|<$

$1, \forall k \geqslant k^*$, 其中 $\ell^* \triangleq \lim_{k\to\infty} \ell(k)$. 另一方面, 从 $\ell(k)$ 的定义可知 $\ell(k) \in \mathbb{N}$ 和 $\ell^* \in \mathbb{N}$. 于是可知 $\ell(k) = \ell^*, \forall k \geqslant k^*$. 从算法 1 容易得出如下结论: $\ell(k) = \ell^*, \forall k \geqslant k^*$ 当且仅当式 (24) 对于所有的 $k \geqslant k^*$ 均成立.

注释11 在定理 1 中, 性能指标 $J_{\rm P}(k), J_{\rm I}(k_0, k)$ 和 $J_{\rm D}(k)$ 的上限已尽可能最小化. 这样做可使切换机制对攻击更加敏感, 因此可以更快地选择到合适的 $K(k)$ 和 $S(k)$ 以防止攻击信号进入被控对象.

注释12 对于未受攻击的正常系统来说, 式 (24) 总是成立的. 但是, 对于受到攻击的系统来说, 攻击信号 $\xi(k)$ 将影响闭环系统的 “PID” 型性能 (10)∼(12), 可能使得式 (24) 不再成立. 同样, 如果违反了条件 (24), 则系统必定异常/遭受攻击, 且应当重新选择反馈增益和切换函数. 根据以上分析, 可以使用式 (10)∼(12) 来判断控制性能是否足够好. 此外, 值得一提的是, 这种思想常见于去伪切换监督控制方法 [37, 38].

注释13 应当注意的是, 该序列将影响闭环系统的性能. 一般来说, $\mathbb{K}$ 在序列中的位置对性能有很大影响 (请参见仿真). 此外, 攻击信号 $\xi(k)$ 的值越大, 变化越快, 式 (24) 越不容易成立, 越能更早地阻止攻击信号进入被控对象中.

注释14 在算法 1 中, 参数 $\ell(k)$ 将最多更新 $\sum_{j=0}^{a_{\max}} C_m^j - 1$ 次便会收敛, 这与传统切换系统 [43, 44] 中的切换机制是不一样的. 在传统的切换系统中, 切换机制将被无限次切换.

4 数值仿真

考虑来自文献 [9] 中的不稳定无人地面车辆系统, 其采样时间为 0.1 s. 系统离散化后可写成

$$\begin{aligned}\begin{bmatrix} x(k+1) \\ v(k+1) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & {\rm e}^{1/10} \\ 1 & {\rm e}^{-B_m/10M} \end{bmatrix}}_{A} \begin{bmatrix} x(k) \\ v(k) \end{bmatrix} + \underbrace{\begin{bmatrix} ({\rm e}^{1/10}-1)/M & ({\rm e}^{1/10}-1)/M \\ \frac{1-{\rm e}^{-B_m/(10M)}}{B_m} & \frac{1-{\rm e}^{-B_m/(10M)}}{B_m} \end{bmatrix}}_{B} \underbrace{F(k)}_{u_a(k)} \\ + \underbrace{\begin{bmatrix} 1/10 & {\rm e}^{1/10}-1 \\ 1/10 & -M({\rm e}^{-B_m}/10M-1)/B_m \end{bmatrix}}_{B_\omega} \omega(k), \end{aligned} \tag{26}$$

其中 B_m 代表平动摩擦系数, F 是无人地面车辆系统的输入. 无人地面车辆中安装了 GPS 传感器以测量位置. 其他物理参数详见文献 [9]. 与文献 [9] 类似, 令 $M = 0.8$ kg 和 $B_m = 1$. 通过验证可知, 假设 2 在 $a_{\max} = 1$ 的条件下总是成立的. 这意味着当攻击远程控制器和执行器之间的通信通道不超过一个时, 可设计控制器以达到控制目标.

为了实现良好的控制性能, 根据 H_∞ 理论设计增益 $K_{\mathbb{J}}$: $K_\emptyset = [-4.0103, -3.9983; -4.0103, -3.9983]$, $K_{\{1\}} = [0, 0; -8.0203, -7.9965]$ 和 $K_{\{2\}} = [-8.0203, -7.9965; 0, 0]$. 其他仿真参数如下: $Q = I$,$\delta_\omega = 0.15\sqrt{2}$, $x(0) = [0.5; 0.5]$, $\omega(k) = [0.15\sin(0.1k); 0.15\cos(0.5k)]$. 在仿真例子中, 将通过 5 组测试验证所提安全控制方法的有效性. 在这 5 组测试中, 序列都被选定为 $\mathbb{J}_1\mathbb{J}_2\mathbb{J}_3$, 其中 $\mathbb{J}_1 = \emptyset, \mathbb{J}_2 = \{1\}, \mathbb{J}_3 = \{2\}$. 测试 1 对应于无攻击情况, 测试 2 和 4 均为第 1 个通信通道受到攻击的情况, 测试 3 和 5 是第 2 个通道受到攻击的情况. 在测试 2 和 3 中, 攻击信号值在区间 $[-0.1, 0.1]$ 上随机产生. 在测试 4 和 5 中, 攻击信号值在区间 $[-0.25, 0.25]$ 上随机产生.

从图 2 中可以看出, 对于受到恶意攻击和干扰的系统, 依然可以实现令人满意的控制效果. 如图 3 所示, 在经过一定时间后, 控制输入很小, 有利于节能. 此外, 在图 4 中给出了 $\ell(k)$ 的更新曲线, 用以

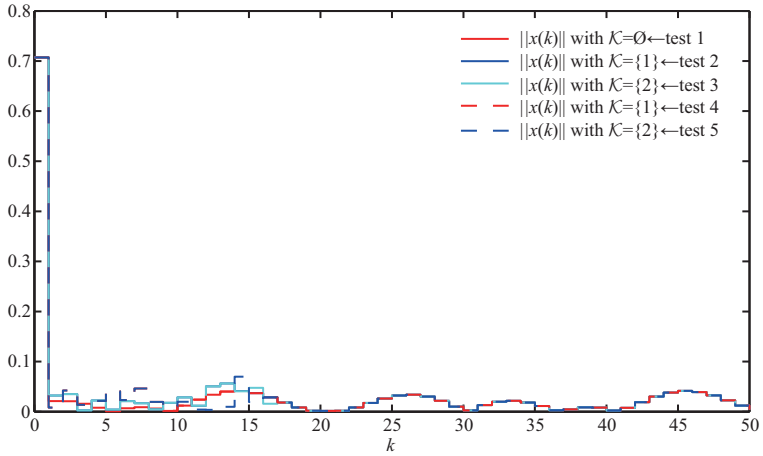

图 2　(网络版彩图) 闭环系统状态

Figure 2　(Color online) Closed-loop system states

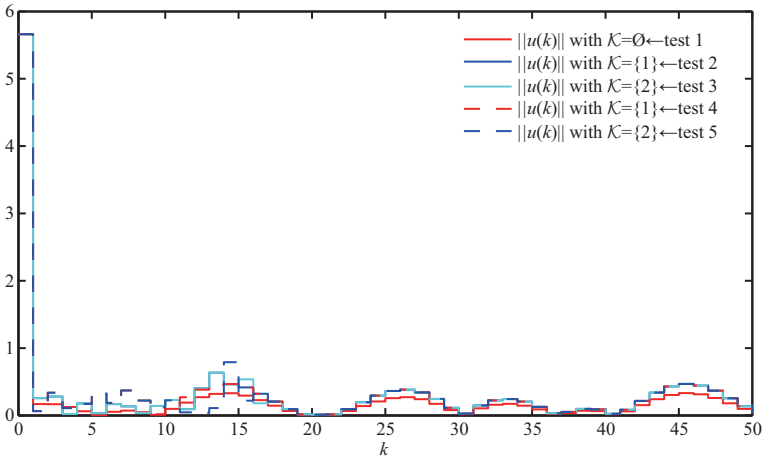

图 3　(网络版彩图) 控制输入

Figure 3　(Color online) Control inputs

显示反馈增益 $K(k)$ 和切换函数 $S(k)$ 的选择过程. 从图 4 可知, 所提出的选择机制可以选择正确的反馈增益 $K(k)$ 和切换函数 $S(k)$, 从而可以正确地防止攻击信号进入被控对象中. 一旦选择了正确的 $K(k)$, $S(k)$ (5 组测试分别对应于 $k = 0, 13, 16, 8, 15$), 不管攻击信号的幅值如何变化, 图 2 中所示的系统状态均迅速收敛到原点附近的小邻域内. 特别地, 所提方法中的选择机制对攻击信号具有较高灵敏度. 在测试 2 和 3 中, $\sup_k \|\xi(k)\| = 0.4714 \sup_k \|\omega(k)\| = 0.1$, 虽然攻击信号几乎是干扰的一半, 但是选择机制仍然可以选择出正确的 $K(k)$ 和 $S(k)$.

5　总结

本文针对遭受稀疏恶意攻击的线性系统, 提出了一种新的安全控制体系结构, 由控制律、切换函数和选择机制构成. 理论分析表明, 可以将安全控制问题转化为求解状态反馈镇定问题. 本文所提控

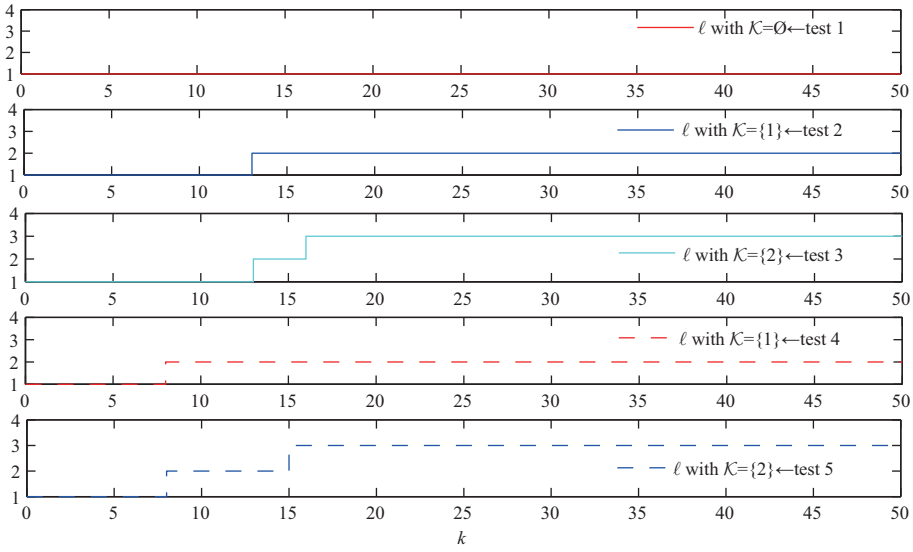

图 4 (网络版彩图) 选择过程

Figure 4 (Color online) Selection process

制方法能保证闭环系统是稳定的且使其具有 “PID” 型性能. 最后, 提供了无人地面车辆系统的仿真示例. 此外, 几乎所有的实际系统都受到输入幅度约束的限制且非线性在许多实际系统中广泛存在. 鉴于此, 我们未来的工作将研究具有输入饱和的非线性系统的安全控制问题.

参考文献

1 Pajic M, Weimer J, Bezzo N, et al. Design and implementation of attack-resilient cyberphysical systems: with a focus on attack-resilient state estimators. IEEE Control Syst, 2017, 37: 66–81

2 Lee R M, Assante M J, Conway T. German steel mill cyber attack. Ind Control Syst, 2014, 30: 62

3 Chen T M. Stuxnet, the real start of cyber warfare? IEEE Network, 2010, 24: 2–3

4 Lee D. Flame: massive cyber-attack discovered, researchers say. BBC News, 2012, 5: 2012

5 Peterson S, Faramarzi P. Iran hijacked us drone, says iranian engineer. Christian Sci Monitor, 2011, 15

6 Ding K, Li Y, Quevedo D E, et al. A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica, 2017, 78: 194–201

7 Mo Y, Sinopoli B. Secure estimation in the presence of integrity attacks. IEEE Trans Automat Contr, 2015, 60: 1145–1151

8 An L, Yang G H. Secure state estimation against sparse sensor attacks with adaptive switching mechanism. IEEE Trans Automat Contr, 2018, 63: 2596–2603

9 Shoukry Y, Nuzzo P, Puggelli A, et al. Secure state estimation for cyber-physical systems under sensor attacks: a satisfiability modulo theory approach. IEEE Trans Automat Contr, 2017, 62: 4917–4932

10 Mo Y, Hespanha J P, Sinopoli B. Resilient detection in the presence of integrity attacks. IEEE Trans Signal Process, 2014, 62: 31–43

11 Ye D, Zhang T Y. Summation detector for false data-injection attack in cyber-physical systems. IEEE Trans Cybern, 2020, 50: 2338–2345

12 Cardenas A A, Amin S, Sastry S. Secure control: towards survivable cyber-physical systems. In: Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, 2008. 495–500

13 Xie C H, Yang G H. Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators. Int J Robust Nonlin Control, 2018, 35: 4382–4403

14 Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks.

IEEE Trans Automat Contr, 2014, 59: 1454–1467
15 Amin S, Schwartz G A, Sastry S S. Security of interdependent and identical networked control systems. Automatica, 2013, 49: 186–192
16 de Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Automat Contr, 2015, 60: 2930–2944
17 Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Automat Contr, 2018, 63: 1813–1820
18 Tang Y, Zhang D, Ho D W C, et al. Event-based tracking control of mobile robot with denial-of-service attacks. IEEE Trans Syst Man Cybern Syst, 2020, 50: 3300–3310
19 Chen X L, Wang Y G. Event-triggered attack-tolerant tracking control design for networked nonlinear control systems under DoS jamming attacks. Sci China Inf Sci, 2020, 63: 150207
20 Jin X, Haddad W M, Yucelen T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. IEEE Trans Automat Contr, 2017, 62: 6058–6064
21 Liu J, Gu Y, Xie X, et al. Hybrid-driven-based $\mathcal{H}_\infty$ control for networked cascade control systems with actuator saturations and stochastic cyber attacks. IEEE Trans Syst Man Cybern Syst, 2019, 49: 2452–2463
22 Liu J, Wu Z G, Yue D, et al. Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks. IEEE Trans Syst Man Cybern Syst, 2019. doi: 10.1109/TSMC.2018.2888633
23 Hu J, Shen J, Lee D. Resilient stabilization of switched linear control systems against adversarial switching. IEEE Trans Automat Contr, 2017, 62: 3820–3834
24 Lu A Y, Yang G H. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks. Inf Sci, 2017, 420: 96–109
25 Mustafa A, Modares H. Attack analysis and resilient control design for discrete-time distributed multi-agent systems. IEEE Robot Autom Lett, 2020, 5: 369–376
26 An L, Yang G H. LQ secure control for cyber-physical systems against sparse sensor and actuator attacks. IEEE Trans Control Netw Syst, 2019, 6: 833–841
27 D'Innocenzo A, Smarra F, Di Benedetto M D. Resilient stabilization of multi-hop control networks subject to malicious attacks. Automatica, 2016, 71: 1–9
28 Ding D, Wang Z, Han Q L, et al. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. IEEE Trans Syst Man Cybern Syst, 2018, 48: 779–789
29 Lai C-L, Hsu P-L. Design the remote control system with the time-delay estimator and the adaptive smith predictor. IEEE Trans Ind Inf, 2010, 6: 73–80
30 Chang X H, Huang R, Park J H. Robust guaranteed cost control under digital communication channels. IEEE Trans Ind Inf, 2020, 16: 319–327
31 Chang X H, Huang R, Wang H, et al. Robust design strategy of quantized feedback control. IEEE Trans Circ Syst II, 2020, 67: 730–734
32 Sayers C. Remote Control Robotics. Berlin: Springer, 1998
33 Buse D P, Wu Q H. Mobile agents for remote control of distributed systems. IEEE Trans Ind Electron, 2004, 51: 1142–1149
34 Kim Y, Evans R G, Iversen W M. Remote sensing and control of an irrigation system using a distributed wireless sensor network. IEEE Trans Instrum Meas, 2008, 57: 1379–1387
35 Pan Y J, Marquez H J, Chen T. Stabilization of remote control systems with unknown time varying delays by LMI techniques. Int J Control, 2006, 79: 752–763
36 Potter J J, Adams C J, Singhose W. A planar experimental remote-controlled helicopter with a suspended load. IEEE/ASME Trans Mechatron, 2015, 20: 2496–2503
37 Baldi S, Battistelli G, Mosca E, et al. Multi-model unfalsified adaptive switching supervisory control. Automatica, 2010, 46: 249–259
38 Battistelli G, Mosca E, Safonov M G, et al. Stability of unfalsified adaptive switching control in noisy environments. IEEE Trans Automat Contr, 2010, 55: 2424–2429
39 Mousavinejad E, Yang F, Han Q L, et al. A novel cyber attack detection method in networked control systems. IEEE Trans Cybern, 2018, 48: 3254–3264

40 Xie C-H, Yang H, Wang D H, et al. Asymptotic state estimation for linear systems with sensor and actuator faults. Sci China Inf Sci, 2019, 62: 212202
41 Li Y X, Yang G H. Robust adaptive fault-tolerant control for a class of uncertain nonlinear time delay systems. IEEE Trans Syst Man Cybern Syst, 2017, 47: 1554–1563
42 Lu A Y, Yang G H. Secure switched observers for cyber-physical systems under sparse sensor attacks: a set cover approach. IEEE Trans Automat Contr, 2019, 64: 3949–3955
43 Yin Y, Zhao X, Zheng X. New stability and stabilization conditions of switched systems with mode-dependent average dwell time. Circ Syst Signal Process, 2017, 36: 82–98
44 Zhao X, Yin Y, Zheng X. State-dependent switching control of switched positive fractional-order systems. ISA Trans, 2016, 62: 103–108

Secure control and proportional-integral-derivative performance of cyber-physical systems with sparse adversarial attacks

Chun-Hua XIE[1,2], Hui YANG[1,2*] & Zhe LI[3]

1. *School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang* 330013*, China*;
2. *Key Laboratory of Advanced Control & Optimization of Jiangxi Province, Nanchang* 330013*, China*;
3. *College of Electrical and Information Engineering, Hunan University, Changsha* 410082*, China*
* Corresponding author. E-mail: yhshuo@ecjtu.edu.cn

Abstract This study investigates the secure control problem for discrete-time linear systems with sparse adversarial attacks. The adversarial attacker is assumed to have limited resources and the capability of manipulating a certain number of communication channels between the remote controller and the actuators. For the designer, which channels are attacked and which are not are unknown. A novel secure remote control method is established in this study. This method consists of a control law, a switching function, and a selection mechanism. The selection mechanism is designed to help select a proper feedback gain for the control law and to produce a switching function that prevents attack signals from entering the plant. Under basic and necessary assumptions, the theoretical analysis shows that the secure control problem can be transformed into a state feedback stabilization problem and that the resulting closed-loop system is stable and resilient to proportional-integral-derivative attacks. Simulation on an unmanned ground vehicle system is performed to verify the theoretical results.

Keywords secure control, cyber-physical systems, sparse adversarial attacks, switching strategy, attack-resilient performance

Chun-Hua XIE was born in 1987. He received his B.S. degree in detection, guidance and control technology from the North University of China, Taiyuan, China, in 2012, and his M.S. and Ph.D. degrees from Northeastern University, Shenyang, China, in 2014 and 2018, respectively. He is now working as a lecturer in the School of Electrical and Automation Engineering of East China Jiaotong University, Nanchang, China. His current research interests include adaptive robust control, cyber-physical systems, fault-tolerant control, and fault diagnosis.

Zhe LI was born in 1988. He received his B.S., M.S., and Ph.D. degrees from Northeastern University, Shenyang, China, in 2011, 2013, and 2018, respectively. He is now working as an assistant professor in the College of Electrical & Information Engineering, Hunan University, Changsha, China. He is also a member of the National Engineering Laboratory of Robotic Vision & Control Technology, Hunan University, China. His current research interests include data-driven control, intelligent manufacturing, and industrial fault detection.

Hui YANG was born in 1965. He received his M.S. and Ph.D. degrees from Northeastern University, Shenyang, China, in 1988 and 2004, respectively. He is a professor in the School of Electrical and Automation Engineering of East China Jiaotong University, Nanchang, China. His current research interests are intelligent transportation system control, complex system modeling, control and optimization, and process industry integrated automation technology and applications.