

控制与决策

Control and Decision

多策略虚假数据注入攻击下切换系统滑模控制的安全设计

马娟, 赵海娟, 徐勤琪

引用本文:

马娟, 赵海娟, 徐勤琪. 多策略虚假数据注入攻击下切换系统滑模控制的安全设计[J]. *控制与决策*, 2024, 39(12): 4093-4098.

在线阅读 View online: <https://doi.org/10.13195/j.kzyjc.2023.1236>

您可能感兴趣的其他文章

Articles you may be interested in

磁悬浮开关磁阻电机的自适应终端滑模控制

Adaptive terminal sliding mode control of bearingless switched reluctance motor
控制与决策. 2021, 36(6): 1449-1456 <https://doi.org/10.13195/j.kzyjc.2019.1064>

输入饱和的充液航天器抗干扰有限时间滑模控制

Anti-disturbance finite-time sliding mode control for liquid-filled spacecraft with input saturation
控制与决策. 2021, 36(5): 1078-1086 <https://doi.org/10.13195/j.kzyjc.2019.0820>

基于模型依赖驻留时间的异步切换控制

Asynchronous switching control based on mode-dependent average dwell time
控制与决策. 2021, 36(3): 609-618 <https://doi.org/10.13195/j.kzyjc.2019.0645>

直线同步电动机磁悬浮系统的自适应模糊滑模控制

Adaptive fuzzy sliding mode control for magnetic suspension system of linear synchronous motor
控制与决策. 2021, 36(3): 693-698 <https://doi.org/10.13195/j.kzyjc.2019.0774>

基于反馈无源化的切换非线性系统 H_∞ 跟踪控制

Passification-based H_∞ tracking control for a class of switched nonlinear systems
控制与决策. 2021, 36(11): 2729-2734 <https://doi.org/10.13195/j.kzyjc.2020.0798>

多策略虚假数据注入攻击下切换系统滑模控制的安全设计

马娟¹, 赵海娟^{1,2†}, 徐勤琪¹

(1. 青岛理工大学 信息与控制工程学院, 山东 青岛 266520;

2. 安徽大学 信息材料与智能感知安徽省实验室, 合肥 230601)

摘要: 研究在多策略网络攻击下切换系统的滑模控制问题. 在传感器向控制器传输信息的通道中, 系统遭受到多策略的虚假数据注入 (false data injection, FDI) 攻击. 与传统的 FDI 攻击不同, 多策略 FDI 攻击会根据攻击时刻选择不同攻击策略. 多策略 FDI 攻击造成系统传输信息的损坏, 进而导致切换系统状态不稳定甚至发散. 为解决这一问题, 应用滑模控制方法保证切换系统的依概率输入-状态稳定性. 应用 Lyapunov 函数方法得到了闭环切换系统稳定性的充分条件. 另外, 建立了系统状态与受损状态信息之间的数学模型, 基于可用的受损状态, 设计滑模控制律, 所设计的滑模控制律保证了系统状态的可达性, 系统状态轨迹在有限时间内被驱动到指定滑模面内. 最后, 通过数值仿真验证了所提方法的有效性.

关键词: 切换系统; 滑模控制; 多策略; 虚假数据注入攻击; 依概率输入-状态稳定; Lyapunov 函数

中图分类号: TP273

文献标志码: A

DOI: 10.13195/j.kzyjc.2023.1236

引用格式: 马娟, 赵海娟, 徐勤琪. 多策略虚假数据注入攻击下切换系统滑模控制的安全设计 [J]. 控制与决策, 2024, 39(12): 4093-4098.

Secure sliding mode control of switched systems under multi-strategy false data injection attacks

MA Juan¹, ZHAO Hai-juan^{1,2†}, XU Qin-qi¹

(1. School of Information and Control Engineering, Qingdao University of Science and Technology, Qingdao 266520, China; 2. Information Materials and Intelligent Sensing Laboratory of Anhui Province, Anhui University, Hefei 230601, China)

Abstract: Different from the traditional false data injection (FDI) attack, the multi-strategy FDI attack selects different attack strategies according to the attacking moment. The multi-strategy FDI attack causes damage to system transmission information, which leads to an unstable state or even dispersion of the switching system. To solve this problem, this paper applies the sliding mode control method to ensure the probabilistic input-state stability performance of the switching system. A sufficient condition for the stability of the closed-loop switching system is obtained by applying the Lyapunov function method. In addition, a mathematical model between the system state and the damaged state information is established, and a sliding mode control law is designed based on the available damaged states. The designed sliding mode control law ensures the accessibility of the system state, and the system state trajectory is driven to the specified sliding mode surface within a finite time. Finally, numerical simulation verifies the effectiveness of the method.

Keywords: switching systems; sliding mode control; multi-strategy; false data injection attacks; input-to-state stable in probability; Lyapunov function

0 引言

信息物理系统 (cyber-physical systems, CPSs) 实现了信息、通信与物理系统之间的高度融合, 构成多维的混杂系统. CPSs 的控制涉及物理进程, 系统状态通过传感器传递给控制器, 后者再将控制信号传

至执行器, 以维持系统所需状态. 然而, 在控制信号或系统状态通过网络通道传输时, 不可避免地会遭受一些网络攻击. 一般而言, 网络攻击可以分为 3 种常见类型: 拒绝服务 (denial of service, DoS) 攻击^[1]、重放攻击、虚假数据注入 (false data injection, FDI) 攻

收稿日期: 2023-08-30; 录用日期: 2024-03-05.

基金项目: 国家自然科学基金项目 (62103219); 安徽大学信息材料与智能感知安徽省实验室开放基金项目 (IMIS202115).

责任编委: 卢剑权.

†通讯作者. E-mail: zhj52108@163.com.

击^[2-4]. 这些攻击可能会破坏传输信息的完整性和可用性,导致控制性能下降. 最近,复杂系统的网络攻击问题取得了许多研究进展^[5-7]. 在实际应用中,系统参数的微小变化和未建模的动态变化是不可忽视的因素,往往被视为模型的不确定性. 此外,输入信号中的外部干扰也是无法避免的现象.

滑模控制(sliding mode control, SMC)是解决这些不确定因素^[8-9]和外部干扰的有效技术,具有响应速度快、设计过程简单、对参数的不确定性和匹配干扰有很强的鲁棒性等优点. 在文献[10],引入奇异扰动分析方法以解决未知上界干扰的自适应SMC问题,并构建了自适应二阶SMC律;在文献[11],考虑了动态事件触发后的触发数据量化和DoS攻击问题,创建了一个混合切换模糊系统,并提出了一种基于观测器的SMC方案. 目前,滑模控制方法已经被广泛应用于切换系统的研究,并取得了诸多重要的成果.

切换系统作为一类重要的混杂系统^[12],通常由一组子系统和切换规则组成. 切换系统不是单一的连续或者离散系统,无论子系统稳定与否,通过设计合适的切换信号,可以保证整个系统的稳定. 随着切换系统的发展,学者们进一步研究了驻留时间法,并将其发展为平均驻留时间^[13],在切换系统的综合研究中取得了许多建设性的成果^[14-15].

文献[16-17]研究了网络攻击下切换系统的滑模控制问题,其中考虑的网络攻击是单一的攻击策略. 与DoS攻击不同,FDI攻击不需要预先知道系统信息,因此更难以被检测和处理. FDI攻击利用系统数据检测漏洞,恶意篡改状态估计结果,严重威胁了系统的安全性和可靠性. 文献[18]研究了区间型2型(interval type-2, IT2)模糊系统的滑模控制问题,分析了FDI攻击对系统状态的影响,设计了一种安全滑模控制器,建立了系统状态与被攻击状态之间的关系. 在实际系统中,攻击者通常随机采取不同的方法和策略进行攻击,这种攻击方式既节省网络资源又提高了准确性. 因此,深入分析多策略攻击对系统性能的影响显得尤为重要. 本文主要通过设计滑模控制律的方法,旨在保证切换系统在多策略FDI攻击的影响下依然能够维持依概率输入-状态稳定(input-to-state stable in probability, ISSiP)性能. 目前,网络攻击下的切换系统的滑模控制问题仍然是一个具有挑战性的课题. 本文的主要贡献有: 1) 将已有的攻击模型应用到切换系统中,为一般的混杂系统提供更加简化的模型,同时提高了系统控制的效率. 2) 构造了切换系统状态与损坏状态之间的关系,在此基础上设计了滑模控制律驱动状态到达指定滑模面的邻域. 3) 应用

Lyapunov函数方法,分析了闭环切换系统依概率输入-状态稳定性ISSiP,保证了系统的状态轨迹和给定边界之间的收敛性.

符号使用说明. \otimes 是克罗内克乘积,克罗内克函数 $\delta(a - b)$ 是一个二元函数,如果 $a - b = 0$,则其输出值为1,否则为0. 函数 $\eta(r)$ 在定义域上连续且严格递增,并且 $\eta(0) = 0$,则函数 $\eta(r)$ 属于 \mathcal{K} 类函数. 连续函数 $\phi(r, k)$,对于每一个固定的 k , $\phi(r, k)$ 是 \mathcal{K} 类函数,对于每一个固定的 r ,函数 $\phi(r, \cdot)$ 是递减的,并且当 $\phi(r, k) \rightarrow 0$ 时, $k \rightarrow \infty$,那么函数 $\phi(r, k)$ 是 \mathcal{KL} 类函数. 数学上用 \sup 这个记号表示最小上界. 函数 $\text{sgn}(c)$ 是符号函数,定义为

$$\text{sgn}(c) = \begin{cases} 1, & c > 0; \\ 0, & c = 0; \\ -1, & c < 0. \end{cases}$$

1 问题提出

考虑下面一类不确定非线性切换系统:

$$\begin{cases} x(k+1) = (A_{\sigma(k)} + \Delta A_{\sigma(k)})x(k) + \\ \quad B_{\sigma(k)}(u(k) + f_{\sigma(k)}(x(k), k)), \\ y(k) = C_{\sigma(k)}x(k). \end{cases} \quad (1)$$

其中: $x(k) \in \mathbb{R}^n$ 表示系统状态, $u(k) \in \mathbb{R}^m$ 表示控制输入, $y(k) \in \mathbb{R}^p$ 表示测量输出,非线性函数 $f_{\sigma(k)}(x(k), k)$ 表示外部干扰,满足 $\|f_{\sigma(k)}(x(k), k)\| \leq d_{\sigma(k)} \|x(k)\|$,参数 $d_{\sigma(k)} > 0$ 是已知标量. $\{A_{\sigma(k)}, B_{\sigma(k)}, C_{\sigma(k)}, R_{\sigma(k)} : \sigma(k) \in \mathcal{I}\}$ 是一组已知矩阵, $\sigma(k)$ 是切换信号. 对于任意一个切换信号 $\sigma(k) = i$,相应的第 i 个子系统的系统矩阵可以表示为 $A_{\sigma(k)} \triangleq A_i, B_{\sigma(k)} \triangleq B_i, C_{\sigma(k)} \triangleq C_i$,不确定项 $\Delta A_{\sigma(k)} \triangleq \Delta A_i$ 满足 $\Delta A_i = E_i M_i(k) Z_i$. 其中: Z_i 和 E_i 是已知常数矩阵; $M_i(k)$ 是一个未知的变化矩阵,满足 $M_i^T(k) M_i(k) \leq I$. 矩阵 B_i 是列满秩矩阵,即 $\sigma(k) = i$ 时, $\text{rank}\{B_i\} = m$. 切换系统(1)可以重写为

$$\begin{cases} x(k+1) = \\ (A_i + \Delta A_i)x(k) + B_i(u(k) + f_i(x(k), k)), \\ y(k) = C_i x(k). \end{cases} \quad (2)$$

数据在传输过程中不可避免地会遭受网络攻击,这可能导致系统信息遭受破坏,从而影响系统的控制性能. 在本文中,多策略FDI攻击以随机方式发生在传感器到控制器通信通道上(图1所示). 在这种攻击中,不同的攻击策略会根据通信通道的不同进行选择,其显著特点在于攻击者无需预先获知系统信息,只需植入虚假信息来破坏有效信息的完整性.

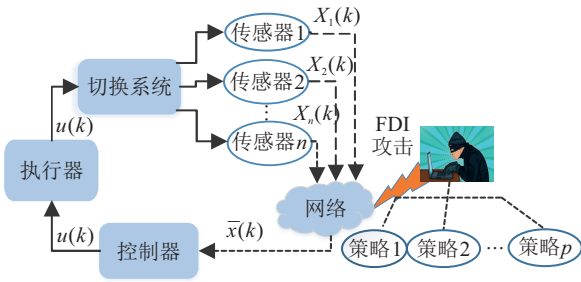


图1 多策略FDI攻击下的切换系统

在传感器到控制器的通信通道中,传感器节点被随机注入不同的攻击策略,造成控制器接收到的信息受损.鉴于攻击者能量受限,分析系统状态和受损状态之间的关系,构建了多策略FDI攻击数学模型,则控制器侧接收到的状态为

$$\bar{x}(k) = x(k) + \sum_{\lambda=1}^p \alpha_{\lambda}(k) j_{\lambda}(k). \quad (3)$$

其中: $\bar{x}(k)$ 是损坏的系统状态, $j_{\lambda}(k)$ ($\lambda = 1, 2, \dots, p$)是攻击策略,随机变量 $\alpha_{\lambda}(k) \in \{0, 1\}$ 服从伯努利分布.在每个时刻,攻击者只选择一种攻击策略,即 $\sum_{\lambda=1}^p \alpha_{\lambda}(k) = 1$,其中 $\alpha_{\lambda}(k) = 1$ 代表第 λ 个攻击策略发生.假设第 λ 个攻击策略发生的概率为

$$P\{\alpha_{\lambda}(k) = 1\} = \bar{\alpha}_{\lambda}, \lambda = 1, 2, \dots, p. \quad (4)$$

其中: $\bar{\alpha}_{\lambda}(k) \in [0, 1]$, $\sum_{\lambda=1}^p \bar{\alpha}_{\lambda}(k) = 1$.

第 λ 个攻击策略的形式如下:

$$j_{\lambda}(k) = H_{\lambda} \varphi(k), \lambda = 1, 2, \dots, p. \quad (5)$$

其中: $H_{\lambda} = \text{diag}\{\gamma_{\lambda_1}, \dots, \gamma_{\lambda_n}\}$ 是注入矩阵; $\varphi(k) = [\varphi_1(k), \dots, \varphi_n(k)]^T$ 是虚假数据; $\gamma_{\lambda_k} = 1$ 代表第 k 个传感器节点受到攻击,否则 $\gamma_{\lambda_k} = 0$.由于攻击者能量受限,注入的数据存在上限值,记为 $\bar{\varphi}_k$,即 $|\varphi_k(k)| \leq \bar{\varphi}_k$.另外,记 $\bar{\varphi} = [\bar{\varphi}_1, \dots, \bar{\varphi}_n]^T$.

引入随机变量 $\rho(k) \in \{1, \dots, p\}$ 来描述多策略FDI攻击的发生,当 $P\{\rho(k) = 1\}$ 时,攻击一定发生,从式(4)很容易知道, $P\{\rho(k) = 1\} = P\{\alpha_{\lambda}(k) = 1\} = \bar{\alpha}_{\lambda}$.因此,式(3)中的受损状态可以进一步改写为

$$\bar{x}(k) = x(k) + \Psi_{\rho(k)} J(k). \quad (6)$$

其中: $\Psi_{\rho(k)} = [\delta(\rho(k)-1), \dots, \delta(\rho(k)-p)] \otimes I$, $\delta(a-b)$ 是克罗内克函数, $J(k) = [j_1^T(k), \dots, j_p^T(k)]^T$.

2 设计滑模控制律

基于矩阵加权方法设计一个公共线性滑模函数

$$s(k) = Gx(k). \quad (7)$$

其中:矩阵 $G \triangleq \sum_{i=1}^N \omega_i B_i^T$,选择合适的参数 ω_i 使得 GB_i 非奇异.基于可用的状态信息,设计滑模控制器

$$u(k) = K_i \bar{x}(k) - d_i \|\bar{x}(k)\| \text{sgn}(\bar{s}(k)). \quad (8)$$

控制增益矩阵 K_i 将在后面设计.可以注意到,与以往的设计不同,选择了 $\bar{s}(k)$ 作为滑动变量,因此系统状态选择了损坏的系统状态来设计控制器.将滑模控制律(8)代入到切换系统(2)后,结合式(6)可以得到以下闭环切换系统,即

$$\begin{cases} x(k+1) = \\ \bar{A}_i x(k) + B_i K_i \Psi_{\rho(k)} J(k) + B_i \bar{d}(k), \\ y(k) = C_i x(k). \end{cases} \quad (9)$$

其中

$$\bar{A}_i \triangleq A_i + \Delta A_i + B_i K_i,$$

$$\bar{d}(k) \triangleq f_i(x(k), k) - d_i \|\bar{x}(k)\| \text{sgn}(\bar{s}(k)).$$

从闭环切换系统(9)可以看出系统中只有一个随机变量,这种处理方式简化了问题的复杂程度.为了分析FDI攻击下切换系统滑模控制的稳定性,下面给出闭环切换系统的ISSiP定义.

定义1 如果对于任意 $\varpi \in (0, 1)$,存在函数 $\phi(\cdot, \cdot) \in \mathcal{KL}$ 和 $\eta(\cdot) \in \mathcal{K}$ 使得 $x(k)$ 满足条件

$$P\{\|x(k)\| < \phi(\|x(0)\|, k) + \eta(\sup_{0 \leq s \leq k} \|x(s)\|)\} \geq 1 - \varpi, \quad (10)$$

则称闭环切换系统(9)是ISSiP.

3 稳定性和可达性分析

在本节中,应用Lyapunov函数方法得到闭环切换系统(9)ISSiP的充分条件.所设计的滑模控制律可以保证系统状态的可达性,系统状态轨迹在有限时间内被驱动到指定滑模面 $s(k) = 0$ 周围的小邻域 Θ 内.

定理1 给定标量 $0 < \beta_i < 1$,如果存在参数 $\xi_i > 0$ 和 $\iota_i > 0$,以及矩阵 $P_i > 0$ 和 K_i ,满足不等式条件

$$B_i^T P_i B_i - \xi_i I \leq 0, \quad (11)$$

$$\Pi_1 \triangleq -\beta_i P_i + 3\bar{A}_i^T P_i \bar{A}_i + 6(\xi_i + \iota_i) d_i^2 I < 0, \quad (12)$$

$$P_i \leq \mu P_j, \quad (13)$$

同时,平均驻留时间满足

$$\tau_a > \tau_a^* = -\frac{\ln \mu}{\ln \beta_i}, \quad (14)$$

则闭环切换系统(9)为ISSiP.

证明 选择Lyapunov函数为

$$V_1(k) \triangleq x^T(k) P_i x(k), \quad (15)$$

由期望值定律可以得到

$$\begin{aligned} E\{x^T(k+1) P_i x(k+1) | x(k), \rho(k) = \lambda\} \leq \\ 3[A_i x(k)]^T P_i A_i^T x(k) + 3\bar{d}^T(k) B_i^T P_i B_i \bar{d}(k) + \\ 3\Psi_{\lambda} J(k)^T P_i \Psi_{\lambda} J(k), \end{aligned} \quad (16)$$

由不等式条件(11),可以得到

$$\begin{aligned} & \bar{d}^T(k)B_i^T P_i B_i \bar{d}^T(k) \leq \\ & 4d_i^2 \xi_i x^T(k)x(k) + 2d_i^2 \xi_i j_\lambda^T(k)j_\lambda(k). \end{aligned} \quad (17)$$

将 $\sum_{\lambda=1}^P \bar{\alpha}_\lambda = 1$ 和 $j_\lambda(k) = H_\lambda \varphi(k)$ 代入式(17),任意给定满足不等式关系 $0 < \beta_i < 1$ 的参数 β_i ,可得

$$\begin{aligned} & E\{V_1(k+1)|\} - \beta_i V_1(k) \leq \\ & x^T(k)\Pi_1 x(k) + \chi \|\varphi(k)\|^2. \end{aligned} \quad (18)$$

其中

$$\Pi_1 \triangleq -\beta_i P_i + 3\bar{A}_i^T P_i \bar{A}_i + 6(\xi_i + \iota_i)d_i^2 I,$$

$$\begin{aligned} \chi \triangleq \max \left\{ \lambda_{\max} \left(\sum_{\lambda=1}^P \bar{\alpha}_\lambda H_\lambda^T [3(B_i K_i)^T G^T Q_i G B_i K_i + \right. \right. \\ \left. \left. 3(B_i K_i)^T P_i B_i K_i + 6d_i^2 \xi_i I] H_\lambda \right) \right\}. \end{aligned}$$

若条件(12)成立,则根据式(18)可以得到

$$E\{V_1(k+1)|x(k)\} \leq \beta_i V_1(k) + \chi \|\varphi(k)\|^2, \quad (19)$$

对式(19)应用迭代方法可得

$$\begin{aligned} E\{V_1(k)\} & \leq \mu^{N_{\sigma(k)}(0,k)} \beta_i^k V_1(0) + \\ & \sum_{s=0}^{k-1} \mu^{N_{\sigma(k)}(s,k)} \beta_i^{k-s-1} \chi \|\varphi(s)\|^2. \end{aligned} \quad (20)$$

此外,由式(15)中的 Lyapunov 函数可知

$$E\{V_1(k)\} \geq a E\{\|x(k)\|^2\}, \quad (21)$$

$$V_1(0) \leq b \|x(0)\|^2. \quad (22)$$

其中: $a = \lambda_{\min}(P_i)$, $b = \lambda_{\max}(P_i)$. 从式(20)~(22)可以推断出

$$\begin{aligned} E\{\|x(k)\|\} & \leq \sqrt{\frac{b}{a} (\beta_i \mu^{\frac{1}{\tau_a}})^k} \|x(0)\| + \\ & \sqrt{\frac{\chi}{a(1-\beta_i)}} \mu^N \sup_{0 \leq s \leq k} \|\varphi(s)\| = \\ & \phi(\|x(0)\|, k) + \eta \left(\sup_{0 \leq s \leq k} \|\varphi(s)\| \right). \end{aligned} \quad (23)$$

其中: $\eta \left(\sup_{0 \leq s \leq k} \|\varphi(s)\| \right) = \sqrt{\frac{\chi}{a(1-\beta_i)}} \mu^N \sup_{0 \leq s \leq k} \|\varphi(s)\|$, 是严格递增的, 并且 $\eta \left(\sup_{0 \leq s \leq k} \|\varphi(s)\| \right) \rightarrow 0$, 则函数 $\eta \left(\sup_{0 \leq s \leq k} \|\varphi(s)\| \right)$ 属于 \mathcal{K} 类函数. $\phi(\|x(0)\|, k) = \sqrt{\frac{b}{a} (\beta_i \mu^{\frac{1}{\tau_a}})^k} \|x(0)\|$, 对于每一个固定的 k , $\phi(\cdot, k)$ 是 \mathcal{K} 类函数. 对于每一个固定的 $\|x(0)\|$, 函数 $\phi(\|x(0)\|, \cdot)$ 是递减的, 并且 $\phi(\|x(0)\|, k) \rightarrow 0$ 时, $k \rightarrow \infty$. 综上, 函数 $\phi(\|x(0)\|, k)$ 是 \mathcal{KL} 类函数.

通过马尔科夫不等式,对于任意 $\varpi \in (0, 1)$,可得

$$\begin{aligned} & P \left\{ \|x(k)\| \leq \frac{1}{\varpi} \phi(\|x(0)\|, k) + \right. \\ & \left. \eta \left(\sup_{0 \leq s \leq k} \|\varphi(s)\| \right) \right\} \geq 1 - \varpi. \end{aligned} \quad (24)$$

因此,从式(24)可以得出结论,根据定义1,闭环切换系统(9)的ISSiP得到保证. □

下面定理将给出保证闭环切换系统状态轨迹到达指定滑模面 $s(k) = 0$ 附近的 Θ 域的充分条件.

定理2 给定标量 $0 < \beta_i < 1$,如果存在参数 $\xi_i > 0, \iota_i > 0, \varsigma_i > 0$ 和矩阵 $P_i > 0, Q_i > 0, K_i$,满足矩阵不等式条件

$$B_i^T G^T Q_i G B_i \leq \varsigma_i I, \quad (25)$$

$$\Pi_2 \triangleq 3\bar{A}_i^T (G^T Q_i G) \bar{A}_i + \Pi_1 < 0, \quad (26)$$

$$Q_i \leq \mu Q_j, \quad (27)$$

则系统状态 $x(k)$ 将被驱动到 Θ 域中,围绕指定的滑动面 $s(k) = 0$,并有

$$\Theta = \left\{ s(k) \mid \|s(k)\| \leq \sqrt{\frac{\Upsilon(k)}{\lambda_{\min}(Q_i)}} \right\}, \quad (28)$$

其中

$$\begin{aligned} \Upsilon(k) & = 12\varsigma_i d_i^2 \|x(k)\|^2 + \\ & \max \left\{ \left\| \sum_{\lambda=1}^P \bar{\alpha}_\lambda H_\lambda^T [3(B_i K_i)^T P_i B_i K_i + \right. \right. \\ & \left. \left. 6d_i^2 (\xi_i + \iota_i) I] H_\lambda \right\| \|\varphi(k)\|^2 \right\}. \end{aligned}$$

证明 从线性滑模函数(7)和闭环切换系统(9)

可以得到

$$\begin{aligned} s(k+1) & = G(A_i + \Delta A_i)x(k) + G B_i (K_i(\bar{x}(k) + \\ & \Psi_{\rho(k)} J(k)) - d_i \|\bar{x}(k)\| \text{sgn}(\bar{s}(k))). \end{aligned} \quad (29)$$

选择候选 Lyapunov 函数为

$$V_2(k) \triangleq V_1(k) + s^T(k)Q_i s(k), \quad (30)$$

将滑模控制律(8)和(29)代入(30),类似定理1的证明,

当 $\|s(k)\| > \sqrt{\frac{\Upsilon(k)}{\lambda_{\min}(Q_i)}}$ 时,可得

$$E\{V_2(k+1)\} \leq \beta_i V_2(k), \quad (31)$$

其中 $0 < \beta_i < 1$. 因此,系统状态轨迹在有限时间内到达滑模面 $s(k) = 0$ 附近的 Θ 域. □

注1 由定理1的式(12)和定理2的式(26)可知,式(26)包含式(12),同时,式子中存在未知参数的耦合项,因此定理1和定理2中的不等式条件是非线性的. 后续,应用 Schur 补引理,将得到定理3中可求解控制增益的线性矩阵不等式条件.

4 求解控制增益 K_i

从定理1和定理2可以看出,如果条件(11)、(12)、(28)和(29)成立,就可以保证指定滑动面的可达性和闭环切换系统的ISSiP. 下面应用 Schur 补方法提供一组满足定理1和定理2的线性矩阵不等式条件.

定理3 给定标量 $0 < \beta_i < 1$,如果存在参数 ξ_i 、

ς_i 和矩阵 $\mathcal{P}_i > 0, \mathcal{Q}_i > 0, G$ 和 \mathcal{L}_i 满足以下条件:

$$\begin{bmatrix} -\bar{\xi}_i I & \bar{\xi}_i B_i^T \\ * & \mathcal{P}_i \end{bmatrix} \leq 0, \quad (32)$$

$$\begin{bmatrix} -\varsigma_i I & B_i^T G^T \\ * & -\mathcal{Q}_i \end{bmatrix} \leq 0, \quad (33)$$

$$\begin{bmatrix} -\beta_i \mathcal{P}_i & \bar{A} & \bar{A} G_i^T & \sqrt{6d_i^2} \mathcal{P}_i \\ * & -\frac{1}{3} \mathcal{P}_i & 0 & 0 \\ * & * & -\frac{1}{3} \mathcal{Q}_i & 0 \\ * & * & * & -\bar{\xi} \end{bmatrix} < 0, \quad (34)$$

$$\mathcal{P}_i \leq \mu \mathcal{P}_j, \mathcal{Q}_i \leq \mu \mathcal{Q}_j. \quad (35)$$

其中

$$\mathcal{P}_i = P_i^{-1}, \mathcal{Q}_i = Q_i^{-1}, \bar{\xi}_i = (\xi_i + \varsigma_i)^{-1},$$

$$\bar{A} = \mathcal{P}_i(A_i + \Delta A_i)^T + \mathcal{L}_i B_i^T.$$

同时,平均驻留时间满足

$$\tau_a > \tau_a^* = -\frac{\ln \mu}{\ln \beta_i}, \quad (36)$$

则保证了指定滑模面的可达性和闭环切换系统的(2)的ISSiP.此外,滑模控制增益 $K_i = \mathcal{L}_i^T \mathcal{P}_i^{-1}$.

5 数值仿真

考虑具有两个子系统的切换系统,每个子系统的矩阵信息如下:

$$A_1 = \begin{bmatrix} 0.5 & -0.9 \\ 0.5 & -0.6 \end{bmatrix}, B_1 = \begin{bmatrix} 2 & -1 \\ -2 & 3 \end{bmatrix}, E_1 = \begin{bmatrix} 0.2 \\ 0.2 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} -0.2 & 0.5 \\ -0.5 & 0.8 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & 2 \\ 1 & -4 \end{bmatrix}, E_2 = \begin{bmatrix} 0.2 \\ 0.4 \end{bmatrix},$$

$$Z_1 = [0.1 \ 0.1], Z_2 = [-0.2 \ 0.2],$$

$$M_1 = \sin k, M_2 = \cos k,$$

$$f_1(x(k), k) = 0.2 \sqrt{x_1^2 + x_2^2}.$$

假设 $\omega_1 = \omega_2 = 1/2$,滑动矩阵为 $G = \omega_1 B_1 + \omega_2 B_2$,可知 GB_i 是列满秩矩阵.另外,选取参数 $\mu = 2, \beta = 0.6, \bar{d} = 1.5$.

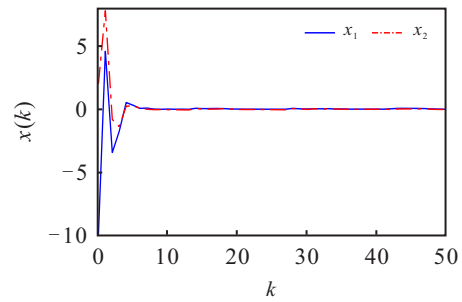
假设有3种类型的FDI攻击策略,使用注入式 $H_1 = \text{diag}\{1, 0\}, H_2 = \text{diag}\{0, 1\}, H_3 = \text{diag}\{1, 1\}$;发生的概率为 $\bar{\alpha}_1 = 0.4, \bar{\alpha}_2 = 0.5, \bar{\alpha}_3 = 0.1$;虚假数据为 $\bar{\varphi}_1 = \bar{\varphi}_2 = \bar{\varphi}_3 = 0.1$.令 $x(0) = [-10 \ 2]^T$,通过定理3中的LMIs条件求解,可得控制器增益

$$K_1 = \begin{bmatrix} 0.3810 & -0.3505 \\ 0.3238 & -0.3831 \end{bmatrix},$$

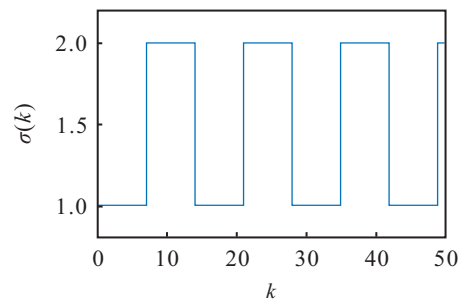
$$K_2 = \begin{bmatrix} 0.0822 & -0.1065 \\ -0.0229 & 0.1937 \end{bmatrix}.$$

图2显示了平均驻留时间 $\tau_a = 7$ 的切换信号和闭环切换系统的状态轨迹;服从伯努利序列取值为0

或1的随机变量 $\alpha(k)$ 显示在图3中;滑动变量 $s(k)$ 和实际执行器信号 $u(k)$ 的响应在图4和图5中显示.



(a) 状态轨迹



(b) 切换信号

图2 系统状态响应

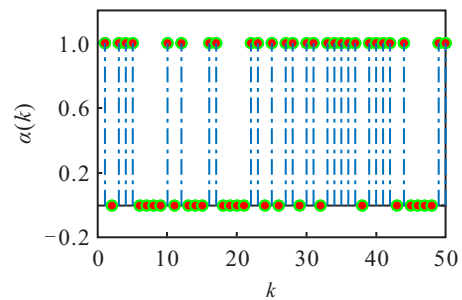


图3 攻击事件发生

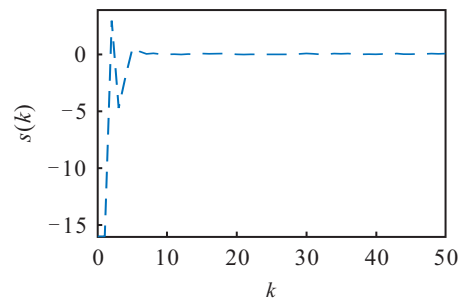


图4 滑动变量

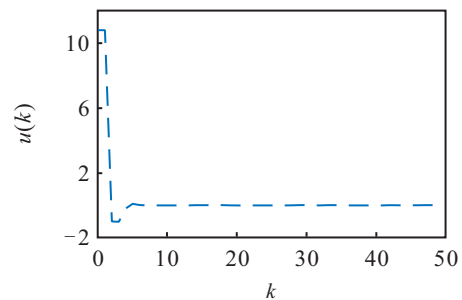


图5 实际执行器信号

6 结论

本文研究了多策略FDI攻击下一类非线性切换系统的滑模控制问题. 在传感器到控制器的通信通道中, 系统在任意时刻可能会遭受随机的虚假数据注入攻击, 导致控制器接收到的信息受到破坏. 为此, 本文分析了受损状态与系统状态之间的关系, 并建立了多策略FDI攻击的数学模型; 基于多策略FDI攻击模型, 构建了相应的滑模控制器和滑模面; 应用多Lyapunov函数方法, 得到了闭环切换系统ISSiP的充分条件. 最后, 通过数值仿真验证了所提出方法的有效性.

参考文献(References)

- [1] Jhaveri R H, Patel S J, Jinwala D C. DoS attacks in mobile ad hoc networks: A survey[C]. 2012 Second International Conference on Advanced Computing & Communication Technologies. Rohtak, 2012: 535-541.
- [2] Liang G Q, Zhao J H, Luo F J, et al. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1630-1638.
- [3] Musleh A S, Chen G, Dong Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2218-2234.
- [4] Pang Z H, Fan L Z, Dong Z, et al. False data injection attacks against partial sensor measurements of networked control systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(1): 149-153.
- [5] Tan Y S, Xiong M H, Zhang B Y, et al. Adaptive event-triggered nonfragile state estimation for fractional-order complex networked systems with cyber attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(4): 2121-2133.
- [6] Chen B, Niu Y. Sliding mode switched control for markovian jumping systems subject to intermittent DoS attacks[J]. International Journal of Robust and Nonlinear Control, 2022, 32(3): 1545-1560.
- [7] Ding D R, Liu H Y, Dong H L, et al. Resilient filtering of nonlinear complex dynamical networks under randomly occurring faults and hybrid cyber-attacks[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(4): 2341-2352.
- [8] 巩敦卫, 张建化, 郭一楠. 一类不确定性网络控制系统的滑模控制器设计[J]. 控制与决策, 2006, 21(10): 1197-1200.
(Gong D W, Zhang J H, Guo Y N. Design of sliding mode controller for a class of networked control systems with uncertainties[J]. Control and Decision, 2006, 21(10): 1197-1200.)
- [9] 沙磊, 王树波, 刘逸坚. 基于扩张状态观测器的二质量系统非奇异快速终端滑模控制[J]. 控制与决策, 2023, 38(3): 850-856.
(Sha L, Wang S B, Liu Y J. Nonsingular fast terminal sliding mode control based on extended state observer for two mass systems[J]. Control and Decision, 2023, 38(3): 850-856.)
- [10] Ding S, Mei K, Yu X. Adaptive second-order sliding mode control: A lyapunov approach[J]. IEEE Transactions on Automatic Control, 2022, 67(10): 5392-5399.
- [11] Ye Z H, Zhang D, Cheng J, et al. Event-triggering and quantized sliding mode control of UMV systems under DoS attack[J]. IEEE Transactions on Vehicular Technology, 2022, 71(8): 8199-8211.
- [12] 林相泽, 田玉平. 切换系统的不变性原理与不变集的状态反馈镇定[J]. 控制与决策, 2005, 20(2): 127-131.
(Lin X Z, Tian Y P. Invariance principle and state feedback stabilization of invariant sets of switched systems[J]. Control and Decision, 2005, 20(2): 127-131.)
- [13] Zhang L, Shi P. Stability, l_2 -gain and asynchronous H_∞ control of discrete-time switched systems with average dwell time[J]. IEEE Transactions on Automatic Control, 2009, 54(9): 2192-2199.
- [14] 宋秀兰, 俞立. 一类不受控离散事件驱动不确定线性切换系统优化控制[J]. 控制与决策, 2016, 31(8): 1407-1412.
(Song X L, Yu L. Optimization control of a class of switched linear uncertain systems driven by uncontrollable discrete-events[J]. Control and Decision, 2016, 31(8): 1407-1412.)
- [15] 杨柳, 费中阳, 史爽, 等. 基于周期动态事件触发的网络化切换系统的分析与控制[J]. 控制与决策, 2021, 36(10): 2467-2474.
(Yang L, Fei Z Y, Shi S, et al. The analysis and control for networked switched systems based on periodic event-trigger[J]. Control and Decision, 2021, 36(10): 2467-2474.)
- [16] Zhao H, Niu Y, Jia T. Security control of cyber-physical switched systems under round-robin protocol: Input-to-state stability in probability[J]. Information Sciences: An International Journal, 2020: 121-134.
- [17] Jiao S Y, Xu S Y, Yuan D M, et al. Sliding mode control for networked control systems under DoS attacks via an event-triggered scheme[J]. Journal of the Franklin Institute, 2023, 360(4): 2931-2954.
- [18] Yang Y K, Niu Y G, Lam J. Security interval type-2 fuzzy sliding mode control under multi-strategy injection attack: Design, analysis, and optimization[J]. IEEE Transactions on Fuzzy Systems, 2023, 31(9): 2943-2955.

作者简介

马娟(1997-), 女, 硕士生, 主要研究方向为切换系统滑模控制网络攻击, E-mail: majuan_405@163.com;

赵海娟(1990-), 女, 副教授, 硕士生导师, 主要研究方向为滑模控制、切换系统和网络控制系统, E-mail: zhj52108@163.com;

徐勤琪(1999-), 男, 硕士生, 主要研究方向为切换系统滑模控制网络传输, E-mail: xqqi0525@163.com.