

欺骗攻击下 Markov 跳变系统的不匹配量化自适应安全控制

李雪林^{1,3}, 倪玉冰¹, 张 健¹, 顾 阳², 孙玉坤³

(1.江苏旅游职业学院信息工程学院,江苏 扬州 225001)

(2.南京工业大学机械与动力工程学院,江苏 南京 211816)

(3.江苏大学电气信息工程学院,江苏 镇江 212013)

[摘要] 本文研究了欺骗攻击下 Markov 跳变系统的不匹配量化自适应安全控制策略. 在控制器端设置了一个多通道结构的量化器,且每个通道具有随时间变化的不匹配度,设计了一个自适应更新率来估计网络攻击的未知界限. 接着,设计了一个由三部分组成的自适应安全控制器,基于 Lyapunov 理论和顶点分离技术,闭环系统随机有界稳定并满足所需的 H_∞ 性能指标. 最后,通过仿真实验验证了所提策略的有效性.

[关键词] 自适应安全控制,网络攻击,量化控制,Markov 跳变系统

[中图分类号] TP273 [文献标志码] A [文章编号] 1001-4616(2024)03-0104-08

Mismatched Quantized Adaptive Security Control for Markov Jump Systems Subject to Deception Attacks

Li Xuelin^{1,3}, Ni Yubing¹, Zhang Jian¹, Gu Yang², Sun Yukun³

(1.School of Information Engineering, Jiangsu Vocational College of Tourism, Yangzhou 225001, China)

(2.School of Mechanical and Power Engineering, Nanjing Tech University, Nanjing 211816, China)

(3.School of Electrical Information Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: This paper concerned with the mismatched quantized adaptive security control scheme of Markov jump systems under deception attacks. A quantizer with multi-channel structure is set up at the controller side and each channel has a time-varying mismatch degree. An adaptive update law is designed to estimate the unknown bounds of the cyber-attack. Subsequently, the adaptive security controller consists of three parts is designed. Based on Lyapunov theory and vertex separation technique, the closed-loop system is stochastically boundedness and satisfies the desired H_∞ performance. The effectiveness of the proposed scheme is verified by a simulation.

Key words: adaptive security control, cyber-attack, quantized control, Markov jump system

近几十年来,Markov 跳变系统作为一类随机系统,因其能够描述具有随机结构或参数的系统而备受关注^[1]. Markov 跳变系统由多个子系统或模态组成,可以随机地从一个子系统或模态跳变到另一个子系统或模态. 目前,这类随机系统已被应用于各个领域,包括化学过程^[2-3]、航空航天工业^[4]和工业制造^[5-6].

随着网络技术的迅速发展,网络控制系统的模式被越来越多的工业系统所采用. 在网络系统中,为了有效降低网络资源消耗,通常会采用量化控制^[7],并引入量化器对不同大小的数据进行分类和编码. 迄今为止,已有许多关于将量化控制应用于网络化 Markov 跳变系统的研究成果被报道. 文献[8]研究了离散时间模糊 Markov 跳变系统的异步动态量化耗散控制策略. 文献[9]研究了静态对数量化器下 T-S 模糊非均质 Markov 跳变系统的 H_∞ 和 l_2-l_∞ 滤波器设计问题. 值得注意的是,上述结果中量化器的灵敏度参数必须匹配. 然而,在实际应用中,由于硬件的不完善,实现这一点可能具有挑战性. 尽管存在一些结果研究了

收稿日期:2024-03-25.

基金项目:江苏省重点研发计划项目(BE2021094)、国家自然科学基金项目(51977103,51877101)、江苏高校优势学科建设工程(三期)项目(PAPD-2018-87).

通讯作者:李雪林,副教授,研究方向:智能控制,电工技术. E-mail:17189509@qq.com

存在非时变不匹配参数的情况,但存在多通道不匹配参数的情况少有提及^[10-11].

另一方面,网络控制系统难免会遭受恶意者的网络攻击^[12].一般来说,网络攻击分为拒绝服务攻击和欺骗攻击^[13].这两种攻击分别会影响数据的可用性和可信度^[14].因此,在对网络化 Markov 跳变系统进行稳定性分析时,应适当考虑它们的影响.文献[15]研究了欺骗攻击下 Markov 跳变系统的有限时间事件触发控制.但是假设了欺骗攻击的能量上界是已知的,这在实际中是不合理的.文献[16]中研究了拒绝服务攻击下不确定 Markov 跳变系统的事件触发 H_∞ 控制.需要特别指出的是,上述研究都没有考虑如何通过控制器主动补偿攻击的影响.

基于上述分析,本文致力于对欺骗攻击下 Markov 跳变系统的不匹配量化自适应安全控制的问题进行研究.设计了一个多通道结构的不匹配量化器,且每个通道具有随时间变化的不匹配度.对于网络攻击,设计了一个自适应更新率来在线估计其能量上界.接着,给出了自适应安全控制器的设计流程.借助于 Lyapunov 理论和顶点分离技术,得到了闭环系统随机有界稳定并满足所需的 H_∞ 性能指标的充分条件.最后,通过仿真实验验证了所提策略的有效性.

1 问题描述

考虑如下的连续时间 Markov 跳变系统:

$$\begin{cases} \dot{\mathbf{x}}(t) = \mathbf{A}(r(t))\mathbf{x}(t) + \mathbf{B}(r(t))\mathbf{Q}(\mathbf{u}(t)) + \mathbf{D}(r(t))\boldsymbol{\omega}(t), \\ \mathbf{z}(t) = \mathbf{E}(r(t))\mathbf{x}(t) + \mathbf{F}(r(t))\boldsymbol{\omega}(t) \end{cases} \quad (1)$$

式中, $\mathbf{x}(t) \in \mathcal{R}^n$, $\mathbf{u}(t) \in \mathcal{R}^m$ 和 $\mathbf{z}(t) \in \mathcal{R}^r$ 分别为系统状态向量,控制输入和调节输出; $\mathbf{Q}(\cdot)$ 表示不匹配量化器; $\boldsymbol{\omega}(t) \in \mathcal{R}^d$ 是范数有界型外部干扰且属于 $L_2[0, +\infty)$ 空间; $\mathbf{A}(r(t))$, $\mathbf{B}(r(t))$, $\mathbf{D}(r(t))$, $\mathbf{E}(r(t))$ 和 $\mathbf{F}(r(t))$ 是合适维度的系统矩阵.此外, $r(t)$ 是属于有限集合 $\mathbb{S} = \{1, 2, \dots, N\}$ 的右连续 Markov 过程,具有以下性质:

$$Pr\{r(t+\Delta)=j|r(t)=i\} = \begin{cases} \pi_{ij}\Delta + o(\Delta) & i \neq j \\ 1 + \pi_{ii}\Delta + o(\Delta) & i = j \end{cases} \quad (2)$$

式中, $\Delta > 0$ 且满足 $\lim_{\Delta \rightarrow 0} (o(\Delta)/\Delta) = 0$; π_{ij} 是在时间 t 时从模态 i 跳转到模态 j 的概率. π_{ij} 在时间 $t+\delta$ 时满足:

$$\begin{cases} \pi_{ij} \geq 0, & \forall i \neq j \in \mathbb{S} \\ \pi_{ii} = - \sum_{j=1, i \neq j}^N \pi_{ij}, & i = (1, \dots, N) \end{cases} \quad (3)$$

为了简化表示,当 $r(t)=i$ 时,系统矩阵 $\mathbf{A}(r(t))$ 简写为 \mathbf{A}_i ,其他矩阵同样简写.

在给出主要结果之前,引入以下引理 1.

引理 1^[17] 给定 H_∞ 性能水平 $\gamma (\gamma > 0)$,如果在零初始条件下,条件

$$\mathcal{E}\left\{\int_0^\infty \mathbf{z}^T(t)\mathbf{z}(t)dt\right\} < \gamma^2 \mathcal{E}\left\{\int_0^\infty \boldsymbol{\omega}^T(t)\boldsymbol{\omega}(t)dt\right\} \quad (4)$$

成立,那么系统就被称为具有 γ 水平的随机稳定性.

引理 2^[18] 如果存在一个对称矩阵 $\boldsymbol{\Theta}$ 具有以下结构:

$$\boldsymbol{\Theta} = \begin{bmatrix} \boldsymbol{\Theta}_{11} & \boldsymbol{\Theta}_{12} \\ \boldsymbol{\Theta}_{12}^T & \boldsymbol{\Theta}_{22} \end{bmatrix}, \quad (5)$$

式中, $\boldsymbol{\Theta}_{11}, \boldsymbol{\Theta}_{22} \in \mathbb{R}^{nm \times nm}$, $\boldsymbol{\Theta}_{12}$ 是维度合适的任意矩阵; $\boldsymbol{\Theta}_{22}^{kk} \in \mathbb{R}^{n \times n} (k=1, \dots, m)$ 是矩阵 $\boldsymbol{\Theta}_{22}$ 的第 (k, k) 块,且是负定矩阵.对于多面体不确定性 $\rho \in \Delta_\rho$,如果下面的条件成立:

$$\begin{cases} \boldsymbol{\Theta}_{11} + He(\Delta(\rho)\boldsymbol{\Theta}_{12}) + \Delta(\rho)\boldsymbol{\Theta}_{22}\Delta(\rho) \geq 0, \\ \begin{bmatrix} \mathbf{X} & \mathbf{Y} \\ \mathbf{Y}^T & 0 \end{bmatrix} + \mathbf{Z}^T \boldsymbol{\Theta} \mathbf{Z} < 0, \end{cases} \quad (6)$$

那么,可以得到:

$$J(\rho) = \mathbf{X} + \sum_k^m \rho_k \mathbf{Y}_k + \left(\sum_k^m \rho_k \mathbf{Y}_k \right)^T < 0, \quad (7)$$

式中, $\mathbf{X} = \mathbf{X}^T \in \mathbb{R}^{n \times n}$; 对所有 $\rho_k \in [\bar{\rho}_k, \bar{\rho}_k]$, 有 $\Delta_\rho = \{\rho = (\rho_1, \dots, \rho_m) : \rho_k \in \{\bar{\rho}_k, \bar{\rho}_k\} \text{ 和 } \Delta(\rho) = \text{diag}\{\rho_1 I, \dots,$

$$\rho_m I\}; \mathbf{Y} = [\mathbf{Y}_1 \mathbf{Y}_2 \cdots \mathbf{Y}_m] (\mathbf{Y}_k \in \mathbb{R}^{n \times n}); \mathbf{Z} = \begin{bmatrix} \mathbf{I}_{n \times n} & & \\ & \ddots & \\ & & \mathbf{I}_{n \times n} & 0 \\ 0 & & & \mathbf{I}_{nm \times nm} \end{bmatrix}.$$

本文的研究目的如下:

- (1) 开发了一种自适应估计与补偿方案, 以降低网络攻击对系统的影响.
- (2) 确保系统是随机有界稳定的并且满足所需的 H_∞ 性能指标 γ .

2 主要结果

在本节中, 首先给出欺骗攻击的模型, 接着给出不匹配量化器的实现, 然后是不匹配量化自适应安全控制器的设计, 最后推导出一个充分条件, 以保证系统的随机有界稳定性.

2.1 欺骗攻击模型

由于网络安全设备或软件的应用、通信协议和网络条件(如网络负载、网络拥塞和网络传输速率)的不同, 攻击具有随机性. 对于这种随机性, 本文使用了一个服从给定伯努利分布的二进制变量 $\beta(t)$ 来描述这种攻击现象. 当控制器发送的控制信号 $\mathbf{u}(t)$ 被工厂成功接收时, $\beta(t) = 0$; 当 $\mathbf{u}(t)$ 在不可靠网络中丢失或被篡改时, $\beta(t) = 1$. 若控制信号被攻击者成功截获, 那么攻击者会释放攻击性信号 $\mathbf{h}(\mathbf{x}(t), t)$. 基于上述分析, 被攻击后的控制输入 $\mathbf{u}(t)$ 改写为^[19]:

$$\bar{\mathbf{u}}(t) = \beta(t) \mathbf{h}(\mathbf{x}(t), t) + (1 - \beta(t)) \mathbf{u}(t), \quad (8)$$

式中, $\beta(t)$ 的数学期望为 $\bar{\beta}$. 此外, 假设欺骗信号 $\mathbf{h}(\mathbf{x}(t), t)$ 的能量有限并满足 $\|\mathbf{h}(\mathbf{x}(t), t)\| \leq \kappa \|\mathbf{x}\|$, 且 κ 是未知的.

2.2 不匹配量化器

设 $\mathbf{B}_i = [b_1 \cdots b_k \cdots b_m]$, $\mathbf{B}_{ik} = [0 \cdots b_k \cdots 0]$ 和 $\mathbf{Q}(\mathbf{u}(t)) = [\mathbf{Q}(u_1(t)) \cdots \mathbf{Q}(u_k(t)) \cdots \mathbf{Q}(u_m(t))]^T$. 首先, 设定第 k 个编码器处理 $u_k(t)$. 然后, 经过处理的数据由理想网络传输到第 k 个解码器. 通过解码, 量化后的输入 $Q(u_k(t))$ 表示如下^[9]:

$$\mathbf{Q}(u_k(t)) = \phi_k^d(t) \text{round}\left(\frac{u_k(t)}{\phi_k^e(t)}\right) \triangleq \phi_k^d(t) q\left(\frac{u_k(t)}{\phi_k^e(t)}\right), \quad (9)$$

式中, $\text{round}(\cdot)$ 是将输入值四舍五入为最接近的整数; $\phi_k^e(t)$ 和 $\phi_k^d(t)$ 分别是第 k 个编码器/解码器的参数. 假定 $\phi_k^e(t)$ 和 $\phi_k^d(t)$ 的边界是已知的, 并且满足 $\phi_k^e(t) \in [\bar{\phi}_k^e, \bar{\phi}_k^e]$ 和 $\phi_k^d(t) \in [\bar{\phi}_k^d, \bar{\phi}_k^d]$.

设不匹配度 $\rho_k(t) = \phi_k^d(t)/\phi_k^e(t)$, 可以得到 $\rho_k(t) \in [\bar{\rho}_k, \bar{\rho}_k]$. 式中的 $Q(u_k(t))$ 可以表示如下:

$$\mathbf{Q}(u_k(t)) = \rho_k(t) \phi_k^e(t) q\left(\frac{u_k(t)}{\phi_k^e(t)}\right). \quad (10)$$

因此, $\mathbf{Q}(\mathbf{u}(t))$ 表示为:

$$\mathbf{Q}(\mathbf{u}(t)) = \boldsymbol{\rho}(t) \boldsymbol{\Phi}^e(t) q(\boldsymbol{\Phi}^{e^{-1}}(t) \mathbf{u}(t)), \quad (11)$$

式中, $\boldsymbol{\Phi}^d(t) = \text{diag}\{\phi_1^d(t), \dots, \phi_m^d(t)\}$, $\boldsymbol{\Phi}^e(t) = \text{diag}\{\phi_1^e(t), \dots, \phi_m^e(t)\}$ 和 $\boldsymbol{\rho}(t) = \text{diag}\{\rho_1(t), \dots, \rho_m(t)\}$.

为了便于下面的推导, $\rho_k(t)$ 的等价变换为下式:

$$\rho_k(t) = \hat{\rho}_k + \bar{\omega}_k(t), \quad (12)$$

式中, 标称部分 $\hat{\rho}_k = (\bar{\rho}_k + \bar{\rho}_k)/2$; 不确定部分 $\bar{\omega}_k(t) \in [\bar{\rho}_k - \hat{\rho}_k, \bar{\rho}_k - \hat{\rho}_k]$.

因此, 不匹配度 $\boldsymbol{\rho}(t)$ 可以改写为:

$$\boldsymbol{\rho}(t) = \hat{\boldsymbol{\rho}} + \bar{\boldsymbol{\omega}}(t), \quad (13)$$

式中, 标称部分 $\hat{\boldsymbol{\rho}} = \text{diag}\{\hat{\rho}_1, \dots, \hat{\rho}_{n_u}\}$; 不确定部分 $\bar{\boldsymbol{\omega}}(t) = \text{diag}\{\bar{\omega}_1(t), \dots, \bar{\omega}_m(t)\}$.

2.3 自适应补偿策略

为应对欺骗攻击, 提出了一种自适应安全控制器, 其结构如下:

$$\begin{cases} \mathbf{u}(t) = \mathbf{u}_l(t) + \mathbf{u}_c(t) + \mathbf{u}_n(t) \\ \mathbf{u}_l(t) = \mathbf{K}_i \mathbf{x}(t) \\ \mathbf{u}_c(t) = -\frac{\eta \rho_{\max} \hat{\delta}(t) \mathbf{B}_i^T \mathbf{P}_i \mathbf{x}(t)}{2(1-\bar{\beta})\rho_{\min}} \\ \mathbf{u}_n(t) = -\frac{\theta}{2} \text{sign}(\mathbf{B}_i^T \mathbf{P}_i \mathbf{x}(t)) \end{cases} \quad (14)$$

式中, \mathbf{K}_i 表示控制器增益; \mathbf{P}_i 是一个正定对称矩阵; η 是给定的正常数; $\theta = \max \{\bar{\phi}_k^e\}$; $\text{sign}(\cdot)$ 表示取输入值的符号; $\rho_{\min} = \min \{\bar{\rho}_k\}$; $\rho_{\max} = \max \{\bar{\rho}_k\}$; $\hat{\delta}(t)$ 是 $\delta(\delta = \kappa^2)$ 的估计值且由下式更新:

$$\dot{\hat{\delta}}(t) = -\zeta \sigma(t) \hat{\delta}(t) + \zeta \eta \rho_{\max} \|\mathbf{B}_i^T \mathbf{P}_i \mathbf{x}(t)\|^2, \quad (15)$$

式中, $\hat{\delta}(t) = \delta + \bar{\delta}(t)$; ζ 是给定的正常数; $\sigma(t)$ 是正标量参数且满足 $\lim_{t \rightarrow \infty} \int_{t_0}^t v(s) ds \leq \bar{v} < \infty$.

至此, 给出闭环系统的状态空间表达式:

$$\begin{cases} \dot{\mathbf{x}}(t) = \mathbf{A}_i \mathbf{x}(t) + \mathbf{B}_i \beta(t) \boldsymbol{\phi}^d(t) \mathbf{h}(\mathbf{x}(t), t) + \mathbf{D}_i \boldsymbol{\omega}(t) + \mathbf{B}_i(1-\beta(t)) \boldsymbol{\rho}(t) (\mathbf{u}(t) + \mathbf{e}_q(t)), \\ \mathbf{z}(t) = \mathbf{E}_i \mathbf{x}(t) + \mathbf{F}_i \boldsymbol{\omega}(t) \end{cases} \quad (16)$$

式中, $\mathbf{e}_q(t) = \boldsymbol{\phi}^e(t) q(\mathbf{u}(t)/\boldsymbol{\phi}^e(t)) - \mathbf{u}(t)$ 且满足 $\|\mathbf{e}_q(t)\|_{\infty} \leq \theta/2$.

2.4 稳定性分析

定理 1 给定性能指标 γ , 如果存在对称正定矩阵 $\mathbf{X}_i = \mathbf{P}_i^{-1}$, 矩阵 $\mathbf{Y}_i = \mathbf{K}_i \mathbf{X}_i$, 使得下面两个线性矩阵不等式

$$\begin{bmatrix} \mathbf{I} \\ \boldsymbol{\Delta}(\rho) \end{bmatrix}^T \boldsymbol{\Theta} \begin{bmatrix} \mathbf{I} \\ \boldsymbol{\Delta}(\rho) \end{bmatrix} \geq 0, \quad (17)$$

$$\boldsymbol{\Xi}_i + \boldsymbol{\Psi}_i \boldsymbol{\Gamma}_i^{-1} \boldsymbol{\Psi}_i^T + \mathbf{Z}^T \boldsymbol{\Theta} \mathbf{Z} < 0, \quad (18)$$

$$\boldsymbol{\Xi}_i = \begin{bmatrix} \boldsymbol{\Xi}_i^1 & \mathbf{B}_{i1}(1-\bar{\beta})\mathbf{Y}_i & \cdots & \mathbf{B}_{ik}(1-\bar{\beta})\mathbf{Y}_i \\ * & 0 & \cdots & 0 \\ * & * & \ddots & \vdots \\ * & * & * & 0 \end{bmatrix}$$

$$\boldsymbol{\Psi}_i = \begin{bmatrix} \mathbf{D}_i & \mathbf{X}_i \mathbf{E}_i^T & [\mathbf{X}_i, \cdots, \mathbf{X}_i, \cdots, \mathbf{X}_i] & \mathbf{X}_i \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\boldsymbol{\Gamma}_i = \begin{bmatrix} -\gamma^2 \mathbf{I} & \mathbf{F}_i^T & 0 & 0 \\ * & -\mathbf{I} & 0 & 0 \\ * & * & \text{diag}\{-\pi_{ij}^{-1} \mathbf{X}_j\} & 0 \\ * & * & * & \frac{-\eta}{\beta^2 \theta^2 \rho_{\max}} \mathbf{I} \end{bmatrix}$$

$$\boldsymbol{\Xi}_i^1 = \text{Sym}(\mathbf{A}_i \mathbf{X}_i + \mathbf{B}_i(1-\bar{\beta}) \hat{\boldsymbol{\rho}} \mathbf{Y}_i) + \pi_{ii} \mathbf{X}_i$$

成立, 那么闭环系统 (18) 在控制器 (14) 下是随机有界稳定的并满足所需的 H_{∞} 性能指标 γ .

证明 选择如下的候选 Lyapunov 函数:

$$V(t) = \mathbf{x}^T(t) \mathbf{P}_i \mathbf{x}(t) + \frac{1}{2} \zeta^{-1} \hat{\delta}^2(t). \quad (19)$$

接着, 在不考虑干扰的情况下对 $V(t)$ 求导, 可得:

$$E\{V(t)\} = E\{\mathbf{x}^T(t) (\mathbf{P}_i \mathbf{A}_i + \mathbf{A}_i^T \mathbf{P}_i \mathbf{P} + \sum_{l=1}^N \pi_{il} \mathbf{P}_l) \mathbf{x}(t) + 2\mathbf{x}^T(t) \mathbf{P}_i \mathbf{B}_i \bar{\beta} \boldsymbol{\phi}^d(t) \mathbf{h}(\mathbf{x}(t), t) +$$

$$2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)(\mathbf{u}(t)+\mathbf{e}_q(t))+\zeta^{-1}\bar{\delta}(t)\dot{\hat{\delta}}(t)\}. \quad (20)$$

将控制器(14)代入式(22),可得:

$$\begin{aligned} E\{V(t)\} \leq & E\{\mathbf{x}^T(t)(\text{Sym}\{\mathbf{P}_i(\mathbf{A}_i+\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)\mathbf{K}_i)\} + \sum_{l=1}^N \pi_{il}\mathbf{P}_l)\mathbf{x}(t) + 2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)(\mathbf{u}_n(t) + \\ & \mathbf{e}_q(t)) + 2\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\|\bar{\beta}\|\boldsymbol{\phi}^d(t)/\boldsymbol{\phi}^e(t)\|\|\boldsymbol{\phi}^e(t)\|\|\mathbf{h}(\mathbf{x}(t),t)\| + \\ & 2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)\mathbf{u}_c(t) + \zeta^{-1}\bar{\delta}(t)\dot{\hat{\delta}}(t)\}. \end{aligned} \quad (21)$$

考虑非线性部分 $\mathbf{u}_n(t)$ 可得:

$$\begin{aligned} 2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)(\mathbf{u}_n(t)+\mathbf{e}_q(t)) \leq & -\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)\theta\text{sign}(\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t)) + \\ & 2(1-\bar{\beta})\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\boldsymbol{\rho}(t)\|_1\|\mathbf{e}_q(t)\|_\infty \leq -\theta(1-\bar{\beta})\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\boldsymbol{\rho}(t)\|_1 + \\ & \theta(1-\bar{\beta})\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\boldsymbol{\rho}(t)\|_1 = 0. \end{aligned} \quad (22)$$

另一方面,把自适应更新率(16)代入可得:

$$\begin{aligned} 2\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\|\bar{\beta}\|\boldsymbol{\phi}^d(t)/\boldsymbol{\phi}^e(t)\|\|\boldsymbol{\phi}^e(t)\|\|\mathbf{h}(\mathbf{x}(t),t)\| + 2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)\mathbf{u}_c(t) - \sigma(t)\bar{\delta}(t)\dot{\hat{\delta}}(t) + \\ \eta\rho_{\max}\bar{\delta}(t)\|\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t)\|^2 \leq 2\bar{\beta}\rho_{\max}\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\|\theta\kappa\|\mathbf{x}(t)\| - \eta\rho_{\max}\bar{\delta}(t)\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\frac{\boldsymbol{\rho}(t)}{\rho_{\min}}\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t) + \\ \eta\rho_{\max}\bar{\delta}(t)\|\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t)\|^2 - \sigma(t)\bar{\delta}(t)\dot{\hat{\delta}}(t) \leq \eta\rho_{\max}\kappa^2\|\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\|^2 + \rho_{\max}\bar{\beta}^2\theta^2\|\mathbf{x}(t)\|^2 - \\ \eta\rho_{\max}\bar{\delta}(t)\mathbf{x}^T(t)\mathbf{P}_i\mathbf{B}_i\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t) + \eta\rho_{\max}\bar{\delta}(t)\|\mathbf{B}_i^T\mathbf{P}_i\mathbf{x}(t)\|^2 - \sigma(t)\bar{\delta}(t)\dot{\hat{\delta}}(t) = \\ \rho_{\max}\bar{\beta}^2\theta^2\|\mathbf{x}(t)\|^2 - \sigma(t)\bar{\delta}(t)\dot{\hat{\delta}}(t) \leq \rho_{\max}\bar{\beta}^2\theta^2\|\mathbf{x}(t)\|^2 + \frac{1}{4}\sigma(t)\delta^2. \end{aligned} \quad (23)$$

结合式(24)和式(25),可得:

$$E\{V(t)\} \leq E\{\mathbf{x}^T(t)(\text{Sym}\{\mathbf{P}_i(\mathbf{A}_i+\mathbf{B}_i(1-\bar{\beta})\boldsymbol{\rho}(t)\mathbf{K}_i)\} + \sum_{l=1}^N \pi_{il}\mathbf{P}_l + \rho_{\max}\bar{\beta}^2\theta^2\mathbf{I})\mathbf{x}(t) + \frac{1}{4}\sigma(t)\delta^2\}. \quad (24)$$

回顾式(13),式(26)等价于

$$\begin{aligned} E\{V(t)\} \leq & E\{\mathbf{x}^T(t)(\text{Sym}\{\mathbf{P}_i(\mathbf{A}_i+\mathbf{B}_i(1-\bar{\beta})\hat{\boldsymbol{\rho}}(t)\mathbf{K}_i)\} + \sum_{l=1}^N \pi_{il}\mathbf{P}_l + \rho_{\max}\bar{\beta}^2\theta^2\mathbf{I})\mathbf{x}(t) + \\ & \frac{1}{4}\sigma(t)\delta^2 + \mathbf{x}^T(t)(\text{Sym}\{\mathbf{P}_i\mathbf{B}_i(1-\bar{\beta})\tilde{\boldsymbol{\omega}}(t)\mathbf{K}_i\})\mathbf{x}(t)\}. \end{aligned} \quad (25)$$

应用引理 2, $E\{V(t)\} \leq 0.25\sigma(t)\delta^2$ 等价于:

$$\begin{bmatrix} \mathbf{I} \\ \boldsymbol{\Delta}(\rho) \end{bmatrix}^T \boldsymbol{\Theta} \begin{bmatrix} \mathbf{I} \\ \boldsymbol{\Delta}(\rho) \end{bmatrix} \geq 0, \quad (26)$$

$$\tilde{\Xi}_i + \mathbf{Z}^T \boldsymbol{\Theta} \mathbf{Z} < 0, \quad (27)$$

$$\tilde{\Xi}_i = \begin{bmatrix} \tilde{\Xi}_i^1 & \mathbf{P}_i\mathbf{B}_{i1}(1-\bar{\beta})\mathbf{K}_i & \cdots & \mathbf{P}_i\mathbf{B}_{ik}(1-\bar{\beta})\mathbf{K}_i \\ * & 0 & \cdots & 0 \\ * & * & \ddots & \vdots \\ * & * & * & 0 \end{bmatrix},$$

$$\tilde{\Xi}_i^1 = \text{Sym}\{\mathbf{P}_i(\mathbf{A}_i+\mathbf{B}_i(1-\bar{\beta})\hat{\boldsymbol{\rho}}(t)\mathbf{K}_i)\} + \sum_{l=1}^N \pi_{il}\mathbf{P}_l + \rho_{\max}\bar{\beta}^2\theta^2\mathbf{I}.$$

至此,如果式(28)和式(29)满足,那么系统是随机有界稳定的. 接着,设 $\boldsymbol{\psi}(t) = [\mathbf{x}^T(t), \boldsymbol{\omega}^T(t)]^T$ 并把干扰和 H_∞ 性能纳入考虑:

$$\begin{aligned} E\{V(t)\} = & E\{\mathbf{x}^T(t)(\tilde{\Xi}_i + \mathbf{Z}^T \boldsymbol{\Theta} \mathbf{Z})\mathbf{x}(t) + \frac{1}{4}\sigma(t)\delta^2 + 2\mathbf{x}^T(t)\mathbf{P}_i\mathbf{D}_i\boldsymbol{\omega}(t) + \mathbf{z}^T(t)\mathbf{z}(t) - \gamma^2\boldsymbol{\omega}^T(t)\boldsymbol{\omega}(t)\} = \\ & E\{\boldsymbol{\psi}^T(t)(\tilde{\Xi}_i + \tilde{\Psi}_i\tilde{\Gamma}_i^{-1}\tilde{\Psi}_i + \mathbf{Z}^T \boldsymbol{\Theta} \mathbf{Z})\boldsymbol{\psi}(t) + \frac{1}{4}\sigma(t)\delta^2\}, \end{aligned} \quad (28)$$

$$\text{式中, } \tilde{\Psi}_i = \begin{bmatrix} \mathbf{P}_i\mathbf{D}_i & \mathbf{E}_i^T \\ 0 & 0 \end{bmatrix}, \tilde{\Gamma}_i = \begin{bmatrix} -\gamma^2\mathbf{I} & \mathbf{F}_i^T \\ * & -\mathbf{I} \end{bmatrix}.$$

接着,如果要想实现系统的随机有界稳定,则下列条件必须得到满足:

$$\tilde{\Xi}_i + \tilde{\Psi}_i \tilde{\Gamma}_i^{-1} \tilde{\Psi}_i + Z^T \Theta Z < 0. \quad (30)$$

对线性矩阵不等式应用舒尔补引理并左乘右乘 $\text{diag}\{X_i; I; \dots; I; I\}$, 就可以得到定理 1 中的式 (19) 和式 (20). 证毕.

注 1 对于多面体不确定性 $\tilde{\omega}(t)$, 传统的鲁棒方法需要建立 2^m 个线性矩阵不等式来覆盖所有情况. 而与前者相比, 引理 2 (顶点分离技术) 通过引入结构化顶点分离器 Θ , 将线性矩阵不等式的数量减少到 $2m$ 个. 在求解定理 1 时, $\Delta(\rho)$ 将替换为 $\tilde{\omega}_k (k=1, \dots, m)$ 的上界 $\bar{\rho}_k - \hat{\rho}_k$ 与下界 $\bar{\rho}_k - \hat{\rho}_k$.

3 仿真实验

借用文献[20]中的 F-404 飞行器模型来验证所提出的控制策略. 则具体模型参数如下:

模式 1:

$$A_1 = \begin{bmatrix} -1.46 & 0 & 2.428 & 0 \\ 0.364 & 3 & -0.2 & -0.378 \\ 0.310 & 7 & 0 & -2.23 \end{bmatrix}, B_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, D_1 = \begin{bmatrix} 0.5 \\ 0.2 \\ 0 \end{bmatrix}, E_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, F_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

模式 2:

$$A_2 = \begin{bmatrix} -1.46 & 0 & 2.428 \\ 0.264 & 3 & -0.378 \\ 0.310 & 7 & 0 & -2.23 \end{bmatrix}, B_1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, D_1 = \begin{bmatrix} 0.5 \\ 0 \\ 0 \end{bmatrix}, E_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, F_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\text{转移概率矩阵为: } \begin{bmatrix} -0.3 & 0.3 \\ 0.4 & -0.4 \end{bmatrix}.$$

设置系统初值 $x(0) = [-4; 2.5; 3]$; 编码器参数 $\phi_1^e(0) \in [0.01, 0.012]$, $\phi_2^e(0) \in [0.015, 0.018]$; 解码器参数 $\phi_1^d(0) \in [0.008, 0.01]$, $\phi_2^d(0) \in [0.018, 0.025]$; $\bar{\beta} = 0.3$; $\eta = 1$. 接着, 可以得到 $\tilde{\omega}_1(t) \in [2/3, 1]$, $\tilde{\omega}_2(t) \in [1, 5/3]$. 利用上述参数求解定理 1 可得:

$$K_1 = \begin{bmatrix} -2.06 & -13.2 & 0.92 \\ -3.45 & -0.80 & -6.78 \end{bmatrix},$$

$$K_2 = \begin{bmatrix} -1.27 & -13.9 & 1.47 \\ -3.15 & -0.06 & -6.07 \end{bmatrix}.$$

选择 $\phi_1^e(0) = 0.01$, $\phi_2^e(0) = 0.018$, $\phi_1^d(0) = 0.09$, $\phi_2^d(0) = 0.02$, $\zeta = 1$, $\sigma(t) = \exp(-1.3t)$, $\omega(t) = 0.1 \text{rand}(1)$, 所产生的动态曲线如图 1-5 所示.

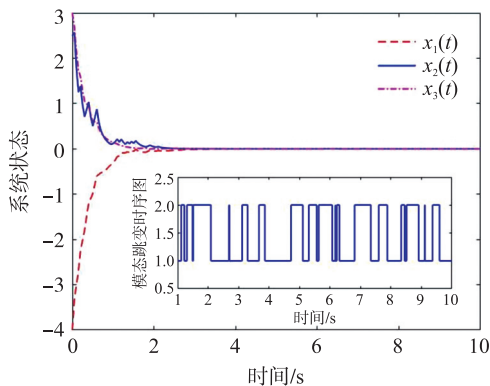


图 2 系统状态 $x(t)$

Fig. 2 System state $x(t)$

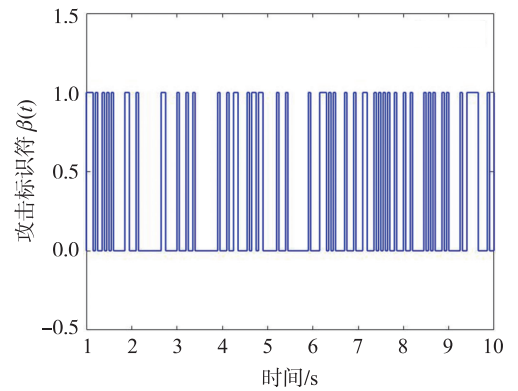


图 1 攻击标识符 $\beta(t)$

Fig. 1 Attack flag $\beta(t)$

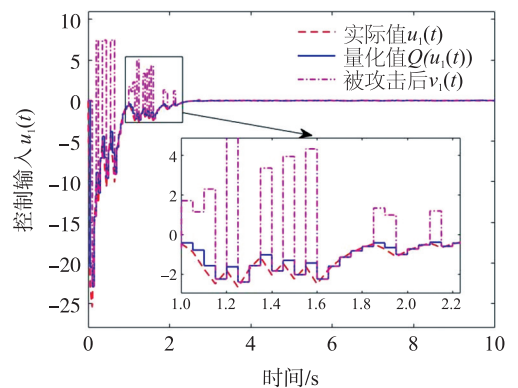


图 3 控制输入 $u_1(t)$

Fig. 3 Control input $u_1(t)$

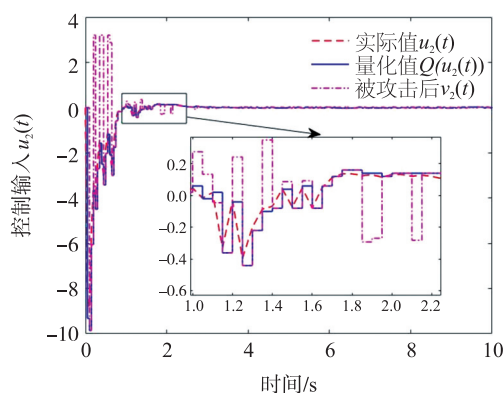


图 4 控制输入 $u_2(t)$

Fig. 4 Control input $u_2(t)$

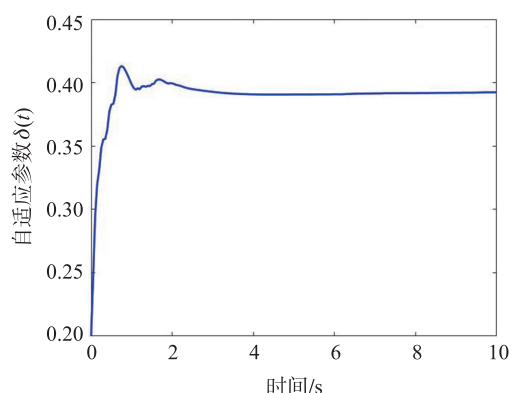


图 5 自适应参数 $\hat{\delta}(t)$

Fig. 5 Adaptive parameter $\hat{\delta}(t)$

图 1 展示了攻击者攻击成功与否的时序图. 从图 2 中可以得出, 本文所提出的自适应安全控制方法成功地保证了受攻击系统的稳定性. 从图 3 和图 4 可以看出, 攻击者的欺骗攻击使得控制输入偏离实际值很远. 但是, 依靠自适应补偿策略, 在攻击未成功时, 所提控制策略能够快速纠正偏差. 图 5 展示了自适应参数的在线估计曲线. 因此, 本文所提出的不匹配量化自适应安全控制策略是有效的.

4 结论

本文研究了欺骗攻击下 Markov 跳变系统的不匹配量化自适应安全控制策略. 设计了一个多通道结构的不匹配量化器, 且每个通道具有随时间变化的编码/解码参数. 设计了一个在线自适应更新率来估计网络攻击的能量上界. 接着, 给出了由三部分组成的自适应安全控制器的设计流程. 最后, 仿真实验证明了所提策略的有效性.

[参考文献]

- [1] 于之训, 陈辉堂, 王月娟. 基于 Markov 延迟特性的闭环网络控制系统研究[J]. 控制理论与应用, 2002(2): 263-267.
- [2] RASHID M M, YU J. Hidden Markov model based adaptive independent component analysis approach for complex chemical process monitoring and fault detection[J]. Industrial & engineering chemistry research, 2012, 51(15): 5506-5514.
- [3] 李雪林, 孙玉坤. 基于改进果蝇算法优化的最小二乘支持向量机动力电池荷电状态预测[J]. 南京工业大学学报(自然科学版), 2023, 45(6): 676-681.
- [4] 王青, 王昭磊, 祁成东, 等. 具有多通道数据传输的飞行器网络控制系统故障检测[J]. 控制与决策, 2014, 29(8): 1401-1407.
- [5] LI L, SUN Z. Dynamic energy control for energy efficiency improvement of sustainable manufacturing systems using Markov decision process[J]. IEEE transactions on systems, man, and cybernetics: systems, 2013, 43(5): 1195-1205.
- [6] 仇鑫, 尤晶晶, 叶鹏达, 等. 一种可重构 Stewart 型并联机器人的静刚度分析[J]. 南京师大学报(自然科学版), 2022, 45(3): 132-140.
- [7] 苏永彬, 洪瑞康, 刘瞰东. 基于前馈隐马尔可夫模型的机器人演示轨迹精准重构方法研究[J]. 仪器仪表学报, 2023, 44(12): 199-207.
- [8] ZHOU J, XU S. Asynchronous dissipative control of discrete-time fuzzy Markov jump systems with dynamic state and input quantization[J]. IEEE transactions on fuzzy systems, 2023, 31(11): 3906-3920.
- [9] HUA M, QIAN Y, DENG F, et al. Filtering for discrete-time Takagi-Sugeno fuzzy nonhomogeneous Markov jump systems with quantization effects[J]. IEEE transactions on cybernetics, 2020, 52(2): 982-995.
- [10] 开诚治, 刘天顺, 马青玉, 等. 基于轨道角动量谱分解的多通道水声通信及系统实现[J]. 南京师大学报(自然科学版), 2024, 47(1): 103-110.
- [11] SHEN M, NGUANG S K, AHN C K, et al. Robust H_2 control of linear systems with mismatched quantization[J]. IEEE transactions on automatic control, 2018, 64(4): 1702-1709.
- [12] SU Q, WANG H, SUN C, et al. Cyber-attacks against cyber-physical power systems security: state estimation, attacks

- reconstruction and defense strategy[J]. Applied mathematics and computation,2022,413:126639.
- [13] 崔北亮,岳阳. IPv6 中邻居发现协议剖析及攻防探索[J]. 南京工业大学学报(自然科学版),2021,43(6):746-754.
- [14] AMINI A, ASIF A, MOHAMMADI A, et al. Sampled-data dynamic event-triggering control for networked systems subject to DoS attacks[J]. IEEE transactions on network science and engineering,2021,8(3):1978-1990.
- [15] 谭天,高金凤,王锦霞,等. 网络攻击下的 Markov 跳变系统有限时间控制[J]. 信息安全研究,2021,7(2):145-154.
- [16] ZENG P, DENG F, LIU X, et al. Event-triggered H_∞ control for network-based uncertain Markov jump systems under DoS attacks[J]. Journal of the Franklin institute,2021,358(6):2895-2914.
- [17] SHI P, NGUANG S K. Robust H_∞ control for linear Markovian jump systems with unknown nonlinearities[J]. Journal of mathematical analysis and applications,2003,282(1):241-255.
- [18] YANG G H, CHE W W. Non-fragile H_∞ filter design for linear continuous-time systems[J]. Automatica,2008,44(11):2849-2856.
- [19] GU Y, SUN Z, LI L W, et al. Event-triggered security adaptive control of uncertain multi-area power systems with cyber attacks[J]. Applied mathematics and computation,2022,432:127344.
- [20] WANG Z, LIU Y, LIU X. Exponential stabilization of a class of stochastic system with Markovian jump parameters and mode-dependent mixed time-delays[J]. IEEE transactions on automatic control,2010,55(7):1656-1662.

[责任编辑:陆炳新]