基于离散事件系统鲁棒监控的强制隐蔽综合

戴茵茵, 王　飞†, 罗继亮

(华侨大学 信息科学与工程学院, 福建 厦门 361021)

摘要: 当离散事件系统模型未知, 但属于某一集合时, 则需要使用一个模型集来表示该系统.为了防止模型集中任一系统的秘密信息泄露, 本文基于鲁棒监控方法研究了强制隐蔽性的监控综合问题. 首先, 通过构造上界自动机和包含所有可能秘密的完全秘密信息, 提出可以保证模型集中所有秘密隐蔽性的鲁棒监控器的存在性条件; 之后, 基于该存在条件, 提出了获取该鲁棒监控器的算法, 并从理论上证明该算法获得的鲁棒监控器是正确的; 最后, 以一个位置信息保护的实例, 说明算法的有效性.

关键词: 强制隐蔽性; 鲁棒监控器; 离散事件系统

引用格式: 戴茵茵, 王飞, 罗继亮. 基于离散事件系统鲁棒监控的强制隐蔽综合. 控制理论与应用, 2025, 42(4): 847 – 854

DOI: 10.7641/CTA.2025.30782

Opacity-enforcing synthesis on robust supervisory control of discrete event systems

DAI Yin-yin, WANG Fei†, LUO Ji-liang

(College of Information Science and Engineering, Huaqiao University, Xiamen Fujian 361021, China)

Abstract: When discrete event systems with model uncertainty belongs to a set, it is necessary to use the set of models to represent the given system. To prevent the leakage of secret for any system in the model set, the synthesis problem of opacity-enforcing on robust supervisory control is investigated in this paper. Firstly, by constructing an upper bound automaton and full secret information containing all secret of the model set, a condition for the existence of a robust supervisor is presented to keep all the secret's opacity in the model set. Afterwards, based on the exist condition, an algorithm is proposed to obtain the robust supervisor. And, by theoretically proof, it shows that the supervisor obtained from the algorithm is correct. Finally, an example of location information protection is used to show the effectiveness of the algorithm.

Key words: opacity-enforcing; robust supervisors; discrete event systems

Citation: DAI Yinyin, WANG Fei, LUO Jiliang. Opacity-enforcing synthesis on robust supervisory control of discrete event systems. *Control Theory & Applications*, 2025, 42(4): 847 – 854

1 引言

离散事件系统 (discrete event systems)[1–2] 是20世纪80年代兴起, 用来研究由事件驱动的一门科学. 其监控理论是通过设计反馈控制器来限制可能的状态转移序列来获取期望的行为, 该理论在制造系统、化工系统、智能电网、数据库管理、通讯协议、物流网络、计算机网络和信息安全等方面有广泛的应用.

本文基于自动机模型研究了信息流的一个重要性质—隐蔽性(opacity), 即通过分析对手能否探知系统的秘密行为, 来验证和保护可信信息或信息流的安全性. 2004年, 隐蔽性的概念[3]在计算机科学中首次被提出, 之后, 在离散事件系统领域的Petri网模型[4]和自动机模型[5]中引入了该概念来保证信息的安全. 文献[5]基于语言给出了强隐蔽、弱隐蔽和无隐蔽的定义; 文献[6–9]又基于状态给出了初始状态隐蔽[6,8]、k-步隐蔽[7]、无限步隐蔽[8]、当前状态隐蔽[9]和初始–结束状态隐蔽[9]的概念. 2019年, 文献[10]对于典型的隐蔽性的验证和综合给出了详细的综述性评价. 自2019年以来, 随着隐蔽性概念的推广, 众多学者又进一步深化了验证和综合问题. 如文献[11–14]虽均采

收稿日期: 2023−12−04; 录用日期: 2025−02−21.

†通信作者. E-mail: feiw545@163.com; Tel.: +86 13459227556.

本文责任编委: 李少远.

国家自然科学基金项目(61203040), 福建省自然科学基金项目(2022J01295), 泉州市科协项目资助.

Supported by the National Natural Science Foundation of China (61203040), the National Natural Science Foundation of Fujian Province (2022J-01295) and the Quanzhou Association for Science and Technology.

用了插入事件的方法来改变对手的观测函数, 进而保持隐蔽性, 但也有很明显的区别; 文献[11]引入虚拟事件插入, 文献[12]在插入函数中引入了约束条件, 文献[13]则考虑了删除事件的情形, 而文献[14]采用插入函数的方法来混淆秘密信息, 使系统无限步隐蔽与k-步隐蔽; 文献[15]推广了k-步隐蔽性概念, 并提出了验证强与弱k-步隐蔽的算法; 文献[16]对于有动态能观函数的系统解决了其无限步隐蔽的综合问题; 文献[17]通过引入识别器, 对于部分能观系统, 提出了无限步强隐蔽与k-步强隐蔽的验证方法, 并解决了两者强制隐蔽性的监控综合问题; 文献[18]通过引入动态信息释放模型, 利用一种新的观测器结构, 提出验证当前状态隐蔽性的有效算法; 文献[19]利用代数状态空间的思想, 解决了验证和综合部分能观系统当前状态隐蔽性的问题; 文献[20]引入了粗糙集作为知识提取工具来验证基于语言的隐蔽性; 文献[21]发展了文献[22]的方法, 通过在系统与其观测器的同步积中计算子观测器, 利用迭代算法获得强制隐蔽性的最大允许监控器; 文献[23]提出k-隐蔽的概念, 并给出综合k-隐蔽的最大允许监控器的方法.

综合上述文献的内容, 隐蔽性的研究都是基于模型已知的情形下做出的, 而对于模型未知的系统, 研究相对较少. 最开始关于模型未知的研究, 来自于文献[24]提出的鲁棒监控器的设计方法, 之后该鲁棒性的框架中逐渐应用到完全能观系统的非阻塞[25]、部分能观系统的非阻塞[26]、网络离散事件系统控制[27]等方面. 近些年, 模型未知问题的研究又从控制的角度扩展到了确定系统的故障诊断[28–29], 确定系统的故障预测[29–30]和随机系统的故障诊断与预测[31–32]等方面. 故障诊断与预测作为隐蔽性验证的特例, 文献[28](或文献[30])是将鲁棒诊断器(或预测器)的存在性转化成每个可能系统的鲁棒可诊断性(或可预测性)的判别, 并将每个系统的鲁棒可诊断性(或可预测性)的判别和对于每个可能系统设计测试自动机联系起来. 文献[29]通过将多个可能的模型集的故障诊断或预测问题转化为任意两个可能模型集的故障诊断或预测问题, 降低了验证的复杂性, 改善了文献[28]和文献[30]的结果. 文献[31]将文献[28]中的模型未知的故障诊断的框架应用到概率自动机中, 同时也考虑了误诊断概率的情况. 类似地, 文献[32]也在文献[30]的框架中引入了状态转移概率, 并讨论了误预测的概率问题. 本文关于隐蔽性的研究, 是在模型集合已知, 但精确模型未知的情形下, 利用监控理论约束任意可能的受控系统的行为, 讨论如何保证所有可能的秘密信息的信息安全的问题. 相较于隐蔽性问题研究, 本文针对的是模型未知的情况, 扩展了隐蔽性验证与综合问题的应用对象; 而相较于前述的故障诊断与故障预测的问题(即隐蔽性验证的特例), 本文是通过设计鲁棒监控器的方法来保证受控系统的隐蔽性, 属于隐蔽性的综合问题研究而非验证问题研究. 这一问题的研究不仅促进了隐蔽性相关内容的发展, 具有重要的理论价值, 同时在工业和生活中也具有广泛的应用. 例如, 在柔性制造系统中, 为了保证产品的多样化以及每种产品的核心工序不被外泄, 则需根据不同加工工序建立一组模型集, 通过设计强制秘密隐蔽性的鲁棒监控器的方法保证核心工序的隐蔽性, 增强产品在市场的竞争力. 本文针对模型未知的系统, 用模型集来表示该系统, 在系统完全能观的条件下, 提出并解决了保证模型集中任一系统的秘密信息不泄露的综合问题.

2 预备知识

2.1 离散事件系统的监控理论

给定离散事件系统为一自动机模型$G=(Q,\Sigma,\delta,q_0,Q_{\rm m})$, 其中: Q为状态集, Σ为事件集, $\delta:Q\times\Sigma\to Q$为状态转移函数, q_0为初始状态, $Q_{\rm m}$为标识状态集. 自动机的生成语言记为$L(G)=\{s\in\Sigma^*|\delta(q_0,s)!\}$, 其中!表示有定义, 标识语言为$L_{\rm m}(G)=\{s\in\Sigma^*|\delta(q_0,s)\in Q_{\rm m}\}$. 为了限制系统的行为, 事件被分为能控事件与不能控事件, 其集合分别记为$\Sigma_{\rm c}$和$\Sigma_{\rm u}$. 记$\Gamma=\{\gamma|\Sigma_{\rm u}\subseteq\gamma\subseteq\Sigma\}$为控制模式集, 称映射$f:L(G)\to\Gamma$为系统$G$的监控器, 在监控器$f$的控制下, 闭环系统$L(f/G)$可按如下递推方式获得:

$$\begin{cases}\varepsilon\in L(f/G),\\ s\sigma\in L(f/G)\Leftrightarrow s\in L(f/G),\ s\sigma\in L(G),\ \sigma\in f(s).\end{cases}$$

对于语言$L\subseteq L(G)$, 记$\bar{L}$为串$s\in L$的所有前缀的集合, 如果$\bar{L}=L$, 则称L是闭(前缀闭)的. 如果语言L满足$\bar{L}\Sigma_{\rm u}\cap L(G)\subseteq\bar{L}$, 则称$L$是能控的.

文献[1]对于系统G提出了监控器存在条件如下:

定理 1 给定非空语言$L\subseteq L(G)$, 则存在监控器f使得$L(f/G)=L$的充要条件是L是能控、闭的.

2.2 离散事件系统的鲁棒监控

在研究离散事件系统的监控综合问题时, 一般需要知道其精确的数学模型. 如果系统模型未知时, 文献[24]提出了鲁棒监控器的概念, 用来控制所有可能的系统.

如果系统模型未知, 但知道其属于某一个特定的模型集, 则用指定的某一自动机已经不足以控制该系统, 文献[24]假设系统的模型属于某一模型集$\{G_i|i\in I\}$, 对于该模型集中的任意模型, 如果能设计监控器来获取系统的期望行为, 则称该监控器为鲁棒监控器, 具体定义如下.

定义 1 给定一组自动机模型$\{G_i|i\in I\}$, 对于任意的一个系统$G\in\{G_i|i\in I\}$, 如果均能综合一监控器f, 则称f是模型集$\{G_i|i\in I\}$的鲁棒监控器.

在文献 [24] 中, 为了控制未知系统$G\in\{G_i|i\in I\}$, 则分别构造G的下界自动机F和上界自动机H,

使其生成语言分别为$L(F)=\underset{i\in I}{\cap}L(G_i)$和$L(H)=\underset{i\in I}{\cap}L(G_i)$, 并且满足$L(F)\subseteq L(G)\subseteq L(H)$.

在系统完全能观的条件下, 文献[24]给出了关于鲁棒监控器的存在条件如下.

定理 2　给定非空语言$L\subseteq L(F)$, 对于系统$G\in\{G_i|i\in I\}$, 则存在监控器f使得$L(f/G)=L$的充要条件是L是关于$L(H)$的能控、闭语言.

2.3　离散事件系统的隐蔽性

为了研究系统的信息安全, 假设外部机构(或对手, 或黑客)完全了解系统的结构, 但仅能观测到部分的系统信息. 定义$\theta:\Sigma^*\to\Sigma_{\rm a}^*$为外部机构的观测函数, 其中$\Sigma_{\rm a}\subseteq\Sigma$为该外部机构能"看到"的事件集. 外部机构根据观测到的信息, 可构筑系统的估计行为. 如果外部机构的估计行为不能推断出系统的秘密, 则称该秘密是隐蔽的, 具体定义[5,22]如下.

定义 2　给定非空语言$K\subseteq L(G)$, 对于任意的$s\in L(G)$, 如果存在$s'\in L(G)-K$使得$\theta(s)=\theta(s')$成立, 则称K关于$L(G)$与$\Sigma_{\rm a}$是(强)隐蔽的(opaque), 简称K是(强)隐蔽的.

如果$K\not\subseteq L(G)$, 则上述定义可简化如下.

定义 3　给定非空语言K, 对于任意的$s\in K\cap L(G)$, 如果存在$s'\in L(G)-K\cap L(G)$使得$\theta(s)=\theta(s')$成立, 则称K关于$L(G)$与$\Sigma_{\rm a}$是隐蔽的, 简称K是隐蔽的.

上述隐蔽性的定义表明, 如果外部机构不能通过观测函数分辨秘密信息和非秘密信息, 则该系统就是隐蔽的, 秘密不会被泄露.

3　基于鲁棒监控的强制隐蔽性综合

之前在研究隐蔽性的时候, 都是假设系统模型是已知的. 但如果系统模型未知时, 则相应的秘密信息也是未知的, 此时如何保持未知系统的隐蔽性, 是本文研究的主要内容.

类似于文献[24], 假设受控系统模型虽然不知道, 但知道其模型属于某一个模型集(即模型集中任一模型都可能是该受控系统), 并且该模型集中的任一模型均有各自的秘密信息. 为了方便, 下文称这类系统为未知系统. 对于这类系统, 本文做如下假设.

假设外部机构了解所有可能模型(即模型集中的任一模型)的结构信息, 知道监控器的任意监控策略, 并可以通过一系列的观测手段"看到"系统的部分操作.

对于未知系统G, 记其所属的系统集为$\{G_i|i\in I\}$, 而对于集合中每个可能的系统$G_i=(Q_i,\Sigma_i,\delta_i,q_{i0})$, 假设其秘密为$K_i\subseteq L(G_i)$, 类似于文献[22], 设其是正则语言, 并且在G_i中均存在标识状态集$Q_{{\rm m}i}$可以辨识K_i, 即$K_i=L_{\rm m}(G_i)$表示G_i中的标识语言.

在上述假设和完全能观的条件下, 本文提出如下综合问题.

基于鲁棒监控的强制隐蔽性综合问题: 给定系统$G\in\{G_i|i\in I\}$, 寻找一个鲁棒监控器f使得任意的K_i关于$L(f/G)$和$\Sigma_{\rm a}$均是隐蔽的, 其中K_i为某一系统G_i中的秘密信息, 并且$i\in I$.

类似于文献[24], 构造未知系统G的上界自动机H和下界自动机F, 使得生成语言$L(H)=\underset{i\in I}{\cup}L(G_i)$与$L(F)=\underset{i\in I}{\cap}L(G_i)$成立. 而对于秘密集$\{K_i\subseteq L(G_i)|i\in I\}$, 构造完全秘密信息$K=\underset{i\in I}{\cup}K_i$, 表示所有可能的秘密信息的上界, 显然有$K_i\subseteq K\subseteq L(H)$成立. 再由文献[33]可知, K是正则语言. 显然, K可以被H中的某一状态子集辨识, 记该状态子集为H中的标识状态集$Q_{{\rm m}H}$, 则有$K=L_{\rm m}(H)$. 基于系统集$\{G_i|i\in I\}$和上界自动机H的关系, 可知$\underset{i\in I}{\cup}Q_{{\rm m}i}=Q_{{\rm m}H}$.

根据构造的上界自动机H和下界自动机F, 如下定理提出了未知系统防止秘密泄漏的鲁棒监控器的存在条件.

定理 3　设未知系统$G\in\{G_i|i\in I\}$, 每个系统G_i的秘密$K_i\subseteq L(G_i)$. 对于上界自动机H、下界自动机F和完全秘密信息K, 如果存在监控器g使得K关于$L(g/H)(\subseteq L(F))$和$\Sigma_{\rm a}$是隐蔽的, 则对于未知系统G, 必存在一个鲁棒监控器f, 使得任意秘密K_i关于$L(f/G)$和$\Sigma_{\rm a}$是隐蔽的, 其中$i\in I$.

证　先证鲁棒监控器的存在性.

对于上界自动机H和下界自动机F, 由定理的条件可知,

存在监控器g使得$L(g/H)\subseteq L(F)\Rightarrow$

$L(g/H)$关于$L(H)$是能控、闭的$\Rightarrow$

对于系统$G\in\{G_i|i\in I\}$均存在一个监控器f,

使得$L(f/G)=L(g/H)\subseteq L(F)$成立$\Rightarrow$

f是$\{G_i|i\in I\}$的鲁棒监控器.

再证对于上述鲁棒监控器f, K_i关于$L(f/G)$和$\Sigma_{\rm a}$是隐蔽的, 其中$i\in I$.

$\forall s\in K_i\cap L(f/G)\Rightarrow$

$s\in K\cap L(g/H)\Rightarrow$

$\exists s'\in L(g/H)-K$, s.t. $\theta(s)=\theta(s')$成立$\Rightarrow$

$s'\in L(f/G)-K_i$, s.t. $\theta(s)=\theta(s')$成立, 其中$i\in I\Rightarrow$

K_i关于$L(f/G)$与$\Sigma_{\rm a}$是隐蔽的, 其中$i\in I$.

由前述证明可知, 如果存在监控器g使得K关于$L(g/H)(\subseteq L(F))$和$\Sigma_{\rm a}$是隐蔽的, 则对于系统G, 均存在一个鲁棒监控器f使得秘密K_i关于$L(f/G)$和$\Sigma_{\rm a}$是隐蔽的, 其中$i\in I$.　证毕.

基于上述定理的证明过程, 易得如下推论.

推论 1 设未知系统$G \in \{G_i|i \in I\}$, 且G_i的秘密$K_i \subseteq L(G_i)$. 对于上界自动机H、下界自动机F和完全秘密信息K, 如果存在监控器g使得K关于$L(g/H)(\subseteq L(F))$和$\Sigma_{\rm a}$是隐蔽的, 而对于未知系统G, 也存在一个鲁棒监控器f, 使得$L(f/G) = L(g/H)$成立, 则秘密K_i关于$L(f/G)$和$\Sigma_{\rm a}$是隐蔽的, 其中$i \in I$.

4 算法与实例

由第3节的定理3可知, 利用系统集构造的上界自动机H和下界自动机F的生成语言$L(H)$与$L(F)$, 如果能保证完全秘密信息关于受控闭环行为是隐蔽的, 则也存在一个鲁棒监控器, 能保证模型集中所有秘密信息都是隐蔽的. 定理3仅提供了鲁棒监控器的存在条件, 并未给出鲁棒监控器的构造方法. 而基于定理3的证明过程, 推论1提出了一种获得鲁棒监控器的方法. 具体算法见表1.

表 1 算法1: 鲁棒监控器f的实现算法

Table 1 Algorithm 1: The implementation algorithm of the robust supervisor f

输入: 系统集$\{G_i|i \in I\}$, 秘密$K_i = L_{\rm m}(G_i)$.

输出: 鲁棒监控器f的生成语言$L(f/G)$.

1 基于系统集$\{G_i|i \in I\}$, 构造上界自动机H使得$L(H) = \mathop{\cup}\limits_{i\in I} L(G_i)$, 下界自动机$F$使得$L(F) = \mathop{\cap}\limits_{i\in I} L(G_i)$;

2 构造完全秘密信息$K = \mathop{\cup}\limits_{i\in I} K_i \subseteq L(H)$, 并且$K$可以被上界自动机$H$辨识, 记为$K = L_{\rm m}(H)$;

3 **if** $L(F)$关于$L(H)$是能控的**then**

4 令自动机$M = F$;

5 **else**

6 基于$L(H)$, 寻找$L(F)$的能控子语言L;

7 构造自动机M使得$L(M) = L$;

8 **end if**

9 **if** K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的**then**

10 对于未知系统$G \in \{G_i|i \in I\}$, 设计监控器f, 使得$L(f/G) = L(M)$;

11 **else**

12 令$K' = K \cap L(M) \subseteq L(F)$;

13 利用文献[21]的方法, 基于自动机M构造监控器g_1使得K'关于$L(g_1/M)$和$\Sigma_{\rm a}$是隐蔽的;

14 对于未知系统$G \in \{G_i|i \in I\}$, 设计监控器f[24], 使得$L(f/G) = L(g_1/M)$;

15 **end if**

对于上述算法1获得的闭环系统行为$L(f/G)$, 其监控器f满足如下性质.

定理 4 算法1获得的监控器f具有如下性质:

1) 监控器f是关于未知系统$G \in \{G_i|i \in I\}$的鲁棒监控器;

2) 任意秘密信息K_i关于$L(f/G)$以及$\Sigma_{\rm a}$是隐蔽的, 其中$i \in I$.

证 先证明结论1).

由定理2知, 需证算法获得的闭环系统行为$L(f/G) \subseteq L(F)$, 并且$L(f/G)$关于$L(H)$是能控的闭语言.

算法1的第3–8行可知, 构造的M的生成语言$L(M) \subseteq L(F)$, 且$L(M)$关于$L(H)$是能控的. 再由M的构造知, $L(M) = \bar{L}(M)$, 即$L(M)$是闭的. 故$L(M) \subseteq L(F)$关于$L(H)$是能控、闭的. 下面考虑两种情形.

情形 1 如果K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的, 则

K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的 $\Rightarrow$

对于未知系统$G \in \{G_i|i \in I\}$,

算法1获得的监控器f使得$L(f/G) = L(M)$成立 $\Rightarrow$

$L(f/G) \subseteq L(F)$关于$L(H)$是能控、闭的.

情形 2 如果K不是关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的, 则由算法的第12–14行可知, 算法获得的监控器g_1使得$L(g_1/M) \subseteq L(M) \subseteq L(F)$成立, 并且$L(g_1/M)$关于$L(M)$是能控、闭的.

$$\forall s \in L(g_1/M),\ \sigma \in \Sigma_{\rm u},\ s\sigma \in L(H) \Rightarrow$$
$$s \in L(M),\ \sigma \in \Sigma_{\rm u},\ s\sigma \in L(H) \Rightarrow$$
$$s\sigma \in L(M) \Rightarrow$$
$$s\sigma \in L(g_1/M) \Rightarrow$$
$$s\sigma \in L(f/G).$$

综上, 由定理2可知, 算法1所得的监控器f是关于未知系统$G \in \{G_i|i \in I\}$的鲁棒监控器.

再证明结论2, 即证明K_i关于$L(f/G)$以及$\Sigma_{\rm a}$是隐蔽的, 其中f是算法1获得的监控器, $i \in I$.

由算法的第3–8行可知, 对于自动机M, 总存在监控器g使得$L(g/H) = L(M) \subseteq L(F)$成立. 下面也考虑两种情形.

情形 1 如果K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的, 则

K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的 $\Rightarrow$

K关于$L(g/H)$和$\Sigma_{\rm a}$是隐蔽的 $\Rightarrow$

K_i关于$L(f/G)$以及$\Sigma_{\rm a}$是隐蔽的,

其中f为算法第10行获得的监控器, $i \in I$.

情形 2 如果K不是关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的, 下面分两步证明闭环系统行为$L(f/G)$的隐蔽性.

第1步 首先证K关于$L(g_1/M)$和$\Sigma_{\rm a}$是隐蔽的, 即$\forall s \in K \cap L(g_1/M)$, 需证$\exists s' \in L(g_1/M)$–$L(g_1/M) \cap K$使得$\theta(s) = \theta(s')$, 其中$L(g_1/M)$为算法第13行获得用来保证$K'$满足隐蔽性的闭环系统行为.

$$\forall s \in K \cap L(g_1/M) \Rightarrow$$
$$s \in K \cap L(M) \Rightarrow$$
$$s \in K' \Rightarrow$$
$$s \in K' \cap L(g_1/M) \Rightarrow$$

$\exists s' \in L(g_1/M) - K'$使得$\theta(s) = \theta(s')$成立 $\Rightarrow$

$s' \in L(g_1/M) - K \cap L(M) \Rightarrow$

$s' \in L(g_1/M) - K \cap L(M) \cap L(g_1/M) \Rightarrow$

$s' \in L(g_1/M) - K \cap L(g_1/M) \Rightarrow$

K关于$L(g_1/M)$和Σ_{a}是隐蔽的.

第2步　由K关于$L(g_1/M)$与Σ_{a}是隐蔽的, 证明K_i关于$L(f/G)$以及Σ_{a}是隐蔽的, 其中$i \in I$.

K关于$L(g_1/M)$与Σ_{a}是隐蔽的 $\Rightarrow$

K关于$L(f/G)$与Σ_{a}是隐蔽的 $\Rightarrow$

K关于$L(g/H)$和Σ_{a}是隐蔽的 $\Rightarrow$

K_i关于$L(f/G)$和Σ_{a}是隐蔽的, 其中$i \in I$.

证毕.

由上述证明过程知, 算法1中获得的鲁棒监控器f能使任意系统的秘密信息K_i关于$L(f/G)$以及Σ_{a}是隐蔽的, 其中$i \in I$.

为了说明算法1的可行性, 下面基于一个位置防护的实例, 构造一个能强制所有秘密隐蔽的鲁棒监控器, 具体实例与计算过程如下.

某小区有两套双层楼房, 外楼梯连接上下两层, 具体结构见图1. 两栋楼房的一楼均包含一个客厅, 一个卫生间和一个卧室, 外面有花园, 客厅与卧室都存在阳台门进出花园; 而二楼则仅有客厅与卧室, 具体的平面布局见图2与图3. 为了方便建立模型, 设状态1表示处于一楼; 状态2表示处于一楼客厅; 状态3表示处于一楼卧室; 状态4表示处于花园; 状态10表示处于一楼卫生间; 状态11表示处于二楼; 状态7表示处于二楼客厅; 状态8表示处于二楼卧室. 事件a表示开门进入; c表示无门直接进入; d_1表示打开客厅阳台门进入; d_2表示打开卧室阳台门进入; e表示爬楼梯.

例 1　**情形** 1　假设两栋楼的卫生间位置不同, 第1栋的卫生间位于一楼客厅(见图2), 第2栋的卫生间位于一楼卧室(见图4), 二楼结构相同(见图3). 假设被监控者进入房间后可以自由出入各房间和花园, 但不能离开楼栋, 根据被监控者的所有可能运动位置, 建立自动机模型G_1与G_2, 分别如图5与图6所示. 设两系统的能控事件集为$\Sigma_{\mathrm{c}} = \{a, d_1, d_2, e\}$, 不能控事件集为$\Sigma_{\mathrm{u}} = \{c\}$, 其表示开门进入和上楼的行为是能控的, 但进入无门的房间是不能控的. 再假设黑客通过摄像头获取两栋楼房中的部分被监控者的活动信息, 记黑客能观测的事件集(或活动集)为$\Sigma_{\mathrm{a}} = \{a, c, d_1, d_2\}$, 其表示房间的不同功能区域间的摄像头的信息可被黑客获取, 但外楼梯未安装摄像头或摄像头损坏. 为了保护被监控者的隐私, 假设一楼卧室、卫生间以及室外花园属于被监控者隐私区域, 不适合被外人感知, 则在每个系统$G_i (i = 1, 2)$中均以秘密语言K_i表示被监控者运动到该区域的运动轨迹. 根据隐私区域的设定, 秘密(或标识)状态记为$\{3, 4, 10\}$, 则两个系统中的秘密语言$K_1 = L_{\mathrm{m}}(G_1) = \{s | \delta_1(1, s) \in \{3, 4, 10\}\}$和$K_2 = L_{\mathrm{m}}(G_2) = \{s | \delta_2(1, s) \in \{3, 4, 10\}\}$分别被状态集$\{3, 4, 10\}$辨识, 具体如图5与图6所示.

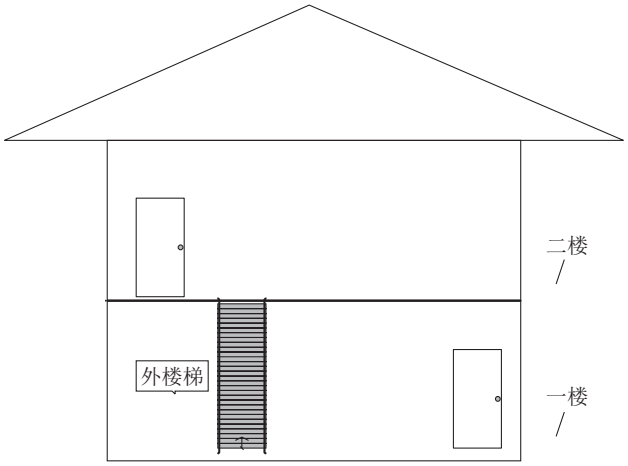

图 1　双层楼房示意图

Fig. 1　Schematic diagram of a two-story building

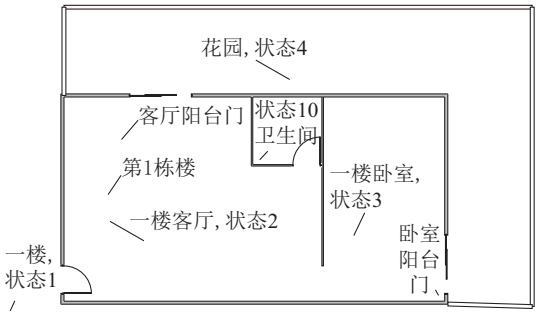

图 2　第1栋楼房一楼布局

Fig. 2　First-floor layout of building 1

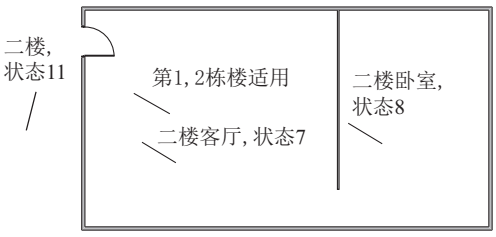

图 3　第1栋与第2栋楼房二楼布局

Fig. 3　Second-floor layout of building 1 and building 2

由于黑客不能判别被监控者在哪一栋楼房内, 故为了保护私人位置信息, 根据算法1可以构造一个同时适合于G_1与G_2的鲁棒监控器f, 使得闭环系统不会泄漏K_1与K_2的信息. 具体过程如下:

1) 基于系统G_1与G_2, 构造上界自动机H, 下界自动机F和完全秘密信息K, 分别如图7和图8所示, 其中完全秘密信息K在H中可被其中标识状态集辨识.

2) 易验证$L(F)$关于$L(H)$是能控的, 并且K关于$L(M)$不是隐蔽的, 其中$M = F$. 基于算法1第13行, 在自动机M中构造秘密语言K', 使得K'可被M的标

识状态集辨识(见图8). 在算法1的第13行中, 利用文献[21]的方法, 构造监控器 g_1, 使得 K' 关于 $L(g_1/M)$ (如图9 所示)和$\Sigma_{\rm a}$是隐蔽的. 再由第14行可得鲁棒监控器f的闭环系统行为$L(f/G)$, 如图9所示.

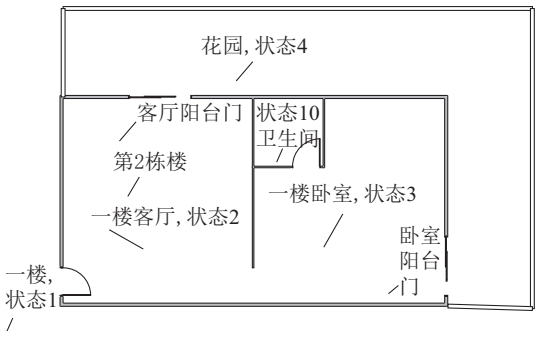

图 4 第2栋楼房一楼布局

Fig. 4 First-floor layout of building 2

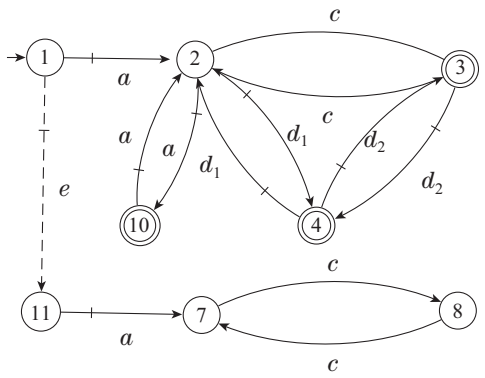

图 5 系统G_1和秘密K_1

Fig. 5 System G_1 and secret K_1

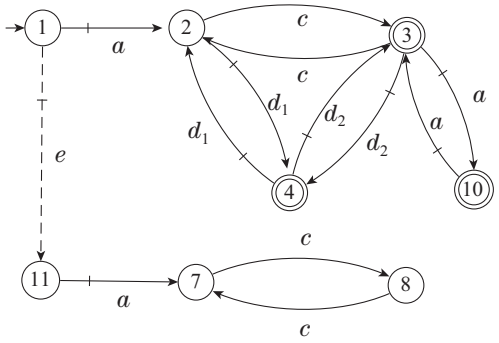

图 6 系统G_2和秘密K_2

Fig. 6 System G_2 and secret K_2

例 2 **情形** 2 (例1的续) 假设第1栋楼的花园与外界联通(见图 10), 且禁止从此处进入花园, 则系统G_1的模型可修改为G_1', 秘密K_1修改为K_1', 并且能辨识K_1'的标识状态集也是$\{3,4,10\}$(如图11); 系统G_2与秘密K_2保持不变(如图6). 此时未知系统的模型集为G_1'和G_2, 为了保护被监控者位置信息, 根据算法1, 构造鲁棒监控器f过程如下:

1) 构造上界自动机H、下界自动机F和完全秘密信息K, 分别如图12和图8所示, 其中K在H中为标识语言.

2) 显然$L(F)$关于$L(H)$是不能控的, 基于算法第6–7行, 在$L(F)$中寻找其关于$L(H)$的能控子语言L, 并构造自动机M使得$L(M)=L$, 如图9所示.

3) 易验证K关于$L(M)$和$\Sigma_{\rm a}$是隐蔽的, 故由算法1第10行可得鲁棒监控器f使得$L(f/G)=L(M)$, 如图9所示.

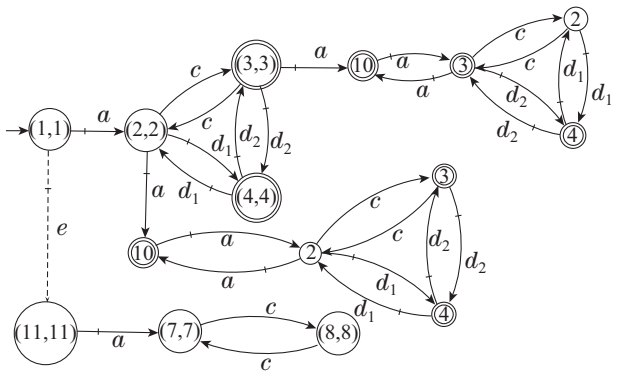

图 7 例1的上界自动机H和秘密K

Fig. 7 Upper bound automaton H and secret K in Example 1

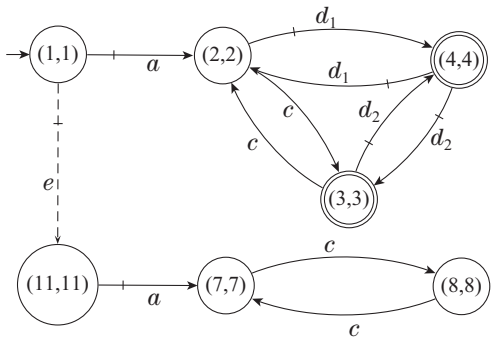

图 8 例1的下界自动机F和例1的自动机M和秘密K', 或例2的下界自动机F, 或例3的下界自动机F

Fig. 8 Lower bound automaton F, automaton M and secret K' in Example 1, or lower bound automaton F in Example 2 or Example 3

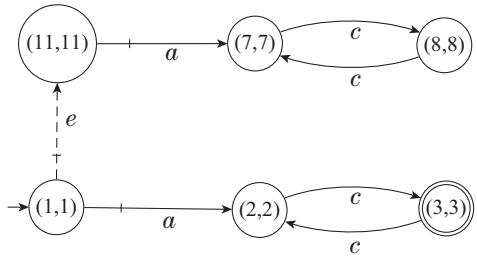

图 9 例1与例3的闭环系统行为$L(g1/M)$和$L(f/G)$, 或例3的自动机M和秘密K', 或例2的自动机M与$L(f/G)$

Fig. 9 Closed-loop behaviors $L(g1/M)$ and $L(f/G)$ in Example 1 and Example 3 are, or automaton M and secret K' in Example 3, or automaton M and closed-loop behavior $L(f/G)$ in Example 2

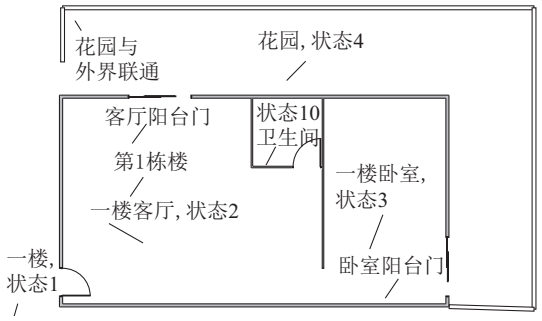

图 10 花园与外界联通时的一楼布局

Fig. 10 First-floor layout for the garden connected to the outside

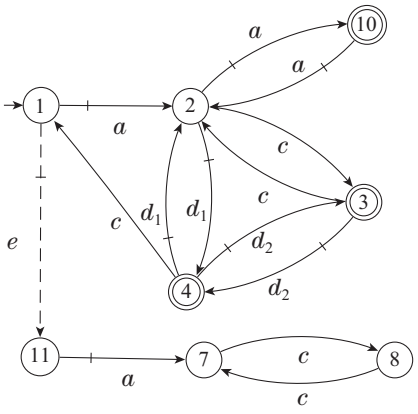

图 11 系统G_1'和秘密K_1'

Fig. 11 System G_1' and secret K_1'

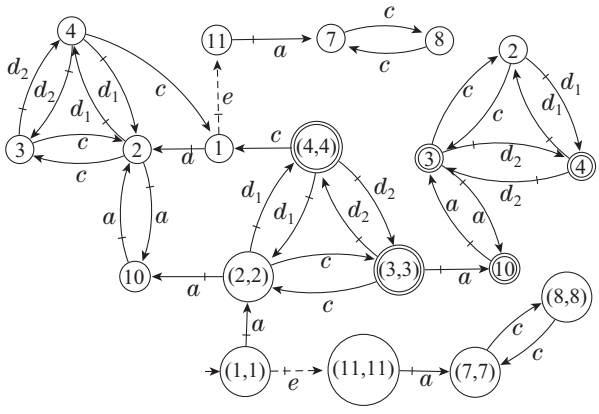

图 12 例2的上界自动机H和秘密K

Fig. 12 Upper bound automaton H and secret K in example 2

例 3　**情形** 3 (例1的再续)　假设第1栋楼的花园与外界联通(见图10), 第2栋楼一楼的洗手间同时连接客厅与卧室(见图 13), 建立系统模型G_1'和秘密信息K_1'以及G_2'和秘密信息K_2', 分别如图11和图14所示, 其中a_1表示打开客厅中卫生间的门进入, a_2表示打开卧室中卫生间的门进入, 并且假设事件a_1, a_2即是可控的, 又是能被黑客观测的. 此时未知系统的模型集为G_1'和G_2'. 为了保护被监控者位置信息, 根据算法1, 构造鲁棒监控器f如下:

1) 构造上界自动机H和完全秘密信息K(如图15)和下界自动机F(如图8);

2) 易验证$L(F)$关于$L(H)$是不能控的, 故构造自动机M(如图9), 使得$L(M)=L\subseteq L(F)$是关于$L(H)$的能控语言;

3) 在自动机M中, 获得$K'=K\cap L(M)$, 可被图9中的标识状态集辨识;

4) 在算法1的第13行中, 利用文献[21]的方法, 构造监控器g_1, 使得K'关于$L(g_1/M)$(如图9所示)和$\Sigma_{\rm a}$是隐蔽的. 再由第14行可得鲁棒监控器f的闭环系统行为$L(f/G)=L(g_1/M)$, 如图9所示.

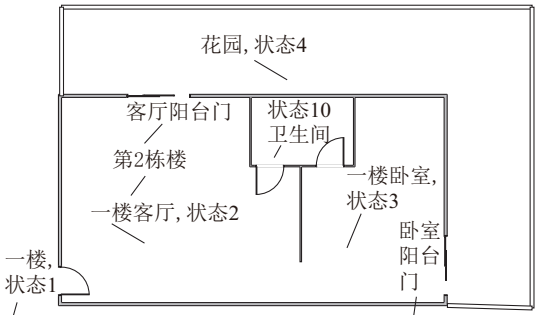

图 13 洗手间连接客厅与卧室的一楼布局

Fig. 13 First-floor layout for the bathroom connecting the living room and bedroom

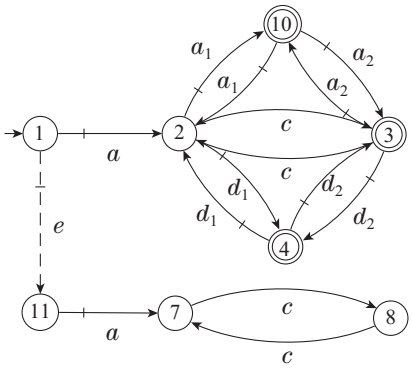

图 14 系统G_2'和秘密K_2'

Fig. 14 System G_2' and secret K_2'

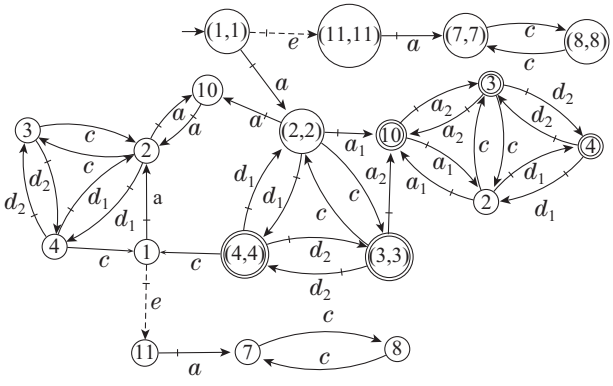

图 15 例3的上界自动机H和秘密K

Fig. 15 Upper bound automaton H and secret K in Example 3

综合以上保护被监控者位置信息的3种情形, 结合其闭环结构(如图9所示)可知, 在这3种情形下, 被监控者只要不打开卫生间的门, 不打开阳台与卧室到花园的门, 保持呆在卧室, 就可以保证自己的位置信息不会泄露.

5 结论

本文主要研究了在系统模型未知时, 利用鲁棒监控方法, 保持秘密行为安全性的综合问题. 利用可能的模型集构造上界自动机、下界自动机和需保护的所有可能秘密的“并”行为(即完全秘密信息), 给出了构造鲁棒监控器的方法来实现所有可能秘密的隐蔽性, 并从定理、算法和实例3个方面说明鲁棒监控器构造的合理性.

后期将考虑结合模型不确定和观测函数不确定[34–35], 一起研究信息物理系统在受到攻击时的信息安全问题.

参考文献:

[1] CASSANDRAS C, LAFORTUNE S. *Introduction to Discrete Event Systems*. Springer: Berlin/Heidelberg, Germany, 2008.

[2] WONHAM W, CAI K, RUDIE K. Supervisory control of discrete event systems: A brief history. *Annual Reviews in Control*, 2018, 45: 250 – 256.

[3] MAZARE L. Using unification for opacity properties. *The Workshop on Information Technology & Systems*. Las Vegas, LV, USA: ACM(Association for Computing Machinery), 2004: 165 – 176.

[4] BRYANS J, KOUTNY M, RYAN P. Modelling opacity using Petri net. *Electronic Notes in Theoretical Computer Science*, 2005, 121: 101 – 115.

[5] LIN F. Opacity of discrete event systems and its applications. *Automatica*, 2011, 47(3): 496 – 503.

[6] SABOORI A, HADJICOSTIS C. Verification of initial-state opacity in security applications of DES. *The 9th International Workshop on Discrete Event Systems*. Gothenburg: Sweden, IEEE, 2008: 328 – 333.

[7] SABOORI A, HADJICOSTIS C. Verification of k-step opacity and analysis of its complexity. *IEEE Transactions Automation Science and Engineering*, 2011, 8(3): 549 – 559.

[8] SABOORI A, HADJICOSTIS C. Opacity-enforcing supervisory strategies via state estimator constructions. *IEEE Transactions on Automatic Control*, 2012, 57(5): 1155 – 1165.

[9] WU Y, LAFORTUNE S. Comparative analysis of related notions of opacity in centralized and coordinated architectures. *Discrete Event Dynamic Systems*, 2013, 23(3): 307 – 339.

[10] GUO Y, JIANG X, GUO C, et al. Overview of opacity in discrete event systems. *IEEE Access*, 2020, 8: 48731 – 48741.

[11] JI Y, WU Y, LAFORTUNE S. Enforcement of opacity by public and private insertion functions. *Automatica*, 2018, 93: 369 – 378.

[12] JI Y, YIN X, LAFORTUNE S. Enforcing opacity by insertion functions under multiple energy constraints. *Automatica*, 2019, 108: 108476.

[13] JI Y, YIN X, LAFORTUNE S. Opacity enforcement using nondeterministic publicly-known edit functions. *IEEE Transactions on Automatic Control*, 2019, 64(10): 4369 – 4376.

[14] LIU R, LU J. Enforcement for infinite-step opacity and K-step opacity via insertion mechanism. *Automatica*, 2022, 140: 110212.

[15] BALUN J, MASOPUST T. Verifying weak and strong k-step opacity in discrete-event systems. *Automatica*, 2023, 155: 111153.

[16] YIN X, LI S. Synthesis of dynamic masks for infinite-step opacity. *IEEE Transactions on Automatic Control*, 2020, 65(4): 1429 – 1441.

[17] MA Z, YIN X, LI Z. Verification and enforcement of strong infinite- and k-step opacity using state recognizers. *Automatica*, 2021, 133: 109838.

[18] HOU J, YIN X, LI S. A framework for current-state opacity under dynamic information release mechanism. *Automatica*, 2022, 140: 110238.

[19] ZHOU Y, CHEN Z, LIU Z. Verification and enforcement of current-state opacity based on a state space approach. *European Journal of Control*, 2023, 71: 100795.

[20] LIU Fuchun, ZHAO Yipeng, ZHAO Rui. Verification algorithm for opacity of discrete-event systems with rough set theory. *Control Theory & Applications*, 2019, 36(8): 1259 – 1264.
(刘富春, 赵毅澎, 赵锐. 基于粗糙集理论的离散事件系统不透明性的验证算法. 控制理论与应用, 2019, 36(8): 1259 – 1264.)

[21] MOULTON R, HAMGINI B, KHOUZANI Z, et al. Using subobservers to synthesize opacity enforcing supervisors. *Discrete Event Dynamic Systems*, 2022, 32(4): 611 – 640.

[22] DUBREIL J, DARONDEAU P, MARCHAND H. Supervisory control for opacity. *IEEE Transactions on Automatic Control*, 2010, 55(5): 1089 – 1100.

[23] WANG Fei, DAI Yinyin, JIN Fujiang. Supervisory control on opacity-margin of discrete event systems. *Control Theory and Applications*, 2025, 42(3): 618 – 626.
(王飞, 戴茵茵, 金福江. 基于隐蔽性裕度的离散事件系统监控. 控制理论与应用, 2025, 42(3): 618 – 626.)

[24] LIN F. Robust and adaptive supervisory control of discrete event systems. *IEEE Transactions on Automatic Control*, 1993, 38(12): 1848 – 1852.

[25] BOURDON S, LAWFORD M, WONHAM W. Robust nonblocking supervisory control of discrete-event systems. *IEEE Transactions on Automatic Control*, 2005, 50(12): 2015 – 2021.

[26] SABOORI A, ZAD S. Robust nonblocking supervisory control of discrete-event systems under partial observation. *Systems & Control Letters*, 2006, 55(10): 839 – 848.

[27] WANG F, SHU S, LIN F. Robust networked control of discrete event systems. *IEEE Transactions Automation Science and Engineering*, 2016, 13(4): 1528 – 1540.

[28] TAKAI S. Verification of robust diagnosability for partially observed discrete event systems. *Automatica*, 2012, 48(8): 1913 – 1919.

[29] YIN X, LI S. Robust diagnosability and robust prognosability of discrete-event systems revisited. *The 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems*. Tianjin: IEEE, 2018: 302 – 307.

[30] TAKAI S. Robust prognosability for a set of partially observed discrete event systems. *Automatica*, 2015, 51(12): 123 – 130.

[31] YIN X, CHEN J, LI Z, et al. Robust fault diagnosis of stochastic discrete event systems. *IEEE Transactions on Automatic Control*, 2019, 64(10): 4237 – 4244.

[32] LIAO H, LIU F, WU N. Robust predictability of stochastic discrete-event systems and a polynomial-time verification. *Automatica*, 2022, 144: 110477.

[33] HOPCROFT J, MOTWANI R. *Introduction to Automata Theory, Languages, and Computation*. 3rd Edition. Boston, MA, USA: Addison Wesley, 2007.

[34] ALVES M, BARCELOS R, CARVALHO L, et al. Robust decentralized diagnosability of networked discrete event systems against DoS and deception attacks. *Nonlinear Analysis: Hybrid Systems*, 2022, 44: 101162.

[35] XIAO C, LIU F. Robust fault prognosis of discrete-event systems against loss of observations. *IEEE Transactions Automation Science And Engineering*, 2022, 19(2): 1083 – 1094.

作者简介:

戴茵茵 讲师, 博士研究生, 目前研究方向为离散事件系统控制, E-mail: crystle@hqu.edu.cn;

王 飞 副教授, 博士, 目前研究方向为离散事件系统的监控理论, E-mail: feiw545@163.com;

罗继亮 教授, 博士, 主要研究方向为离散事件系统的监控理论、Petri网, E-mail: jlluo@hqu.edu.cn.