DOI: 10.7641/CTA.2015.40510

部分可观Petri网结构信息在故障诊断中的应用

叶丹丹, 罗继亮†

(华侨大学 信息科学与工程学院, 福建 厦门 361021)

摘要: 针对离散事件系统的故障诊断问题, 本文提出了一种基于部分可观Petri网结构信息的诊断方法. 它包括两个部分, 第1部分利用故障变迁的可诊断子网确定故障变迁的可诊断性. 第2部分在故障可诊断的基础上提出一种在线故障诊断方法: 首先, 利用Petri网的几种基本子网来分析故障变迁的可诊断子网的结构信息; 其次, 根据给定的可观测变迁序列和可诊断子网的结构特征来描述子网内部托肯的流动形式; 最后, 定义故障函数, 并结合具体实例来描述故障变迁的发生情况. 该故障诊断的方法基于部分可观Petri网结构信息, 无需遍历系统状态空间, 免去多项式级的计算复杂性, 能够满足实时性的要求.

关键词: 离散事件系统; 故障诊断; Petri网; 故障函数

中图分类号: TP273　　**文献标识码**: A

Application of structural information of partially observed Petri net in fault diagnosis

YE Dan-dan, LUO Ji-liang†

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

Abstract: For fault diagnosis problems in discrete event systems, we propose an approach based on the structural information of partially observed Petri nets. This work consists two parts. In the first part, the diagnosable subnet is used to determine the diagnosability of the fault transition. In the second part, a method is proposed to online diagnose the fault if it is diagnosable. First, several basic subnets are used to analyze the structural information of the diagnosable subnet of the fault transition. Then, the flow of tokens in the diagnosable subnet is described by the sequence of observable transitions and the structural characteristics of the diagnosable subnet. Finally, by defining the failure function and giving an example, we described the fault. With the structural information of partially observed Petri nets, it is not necessary to traverse all states of the system. Because this approach is with the computational complexity of polynomials only, it meets with the real time requirements.

Key words: discrete event system; fault diagnosis; Petri net; failure function

1 引言(Introduction)

在计算机、通信以及传感器技术的推动下, 离散事件系统(DES)迅速发展起来, 比如网络通讯系统、智能交通系统等等, 通常呈现为复杂大规模系统, 状态空间随单元数指数级增长, 该复杂性使得系统容易发生故障, 任何故障都可能造成严重损失, 因此需要对故障进行及时诊断和控制. 离散事件系统的故障诊断问题一直以来获得了广泛的关注和研究[1−4]. 在近几年中, 故障诊断问题较多利用Petri网进行分析, 主要是因为同其他离散事件的分析工具, 比如自动机相比, Petri网具有不需要穷举空间内所有的状态, 建模效率高的优点, 同时其内在的分布式特性可以降低故障诊断问题中计算复杂性.

针对完全可观的Petri网模型, 国内外已给出相应的研究方法. Lefebvre和Delherm[5]通过最小诊断器的方法来立即检测和隔离故障. 郑永煌、田锋和李人厚等人[6]通过时间Petri网模型来判断一个液体火箭发动机启动过程中是否存在故障. Cabasino, Giua和Seatzu

收稿日期: 2014−06−03; 录用日期: 2014−12−02.

†通信作者. E-mail: jlluo@hqu.edu.cn; Tel.: +86 13110595996.

国家青年科学基金(61203040), 福建省自然科学基金项目(2014J01339), 福建省高等学校新世纪优秀人才支持计划项目(11FJRC01), 福建省高校杰出青年科研人才培育计划项目(JA10004)资助.

Supported by National Science Foundation for Distinguished Young Scholars of China (61203040), Natural Science Foundation of Fujian Province (2014J01339), Program for New Century Excellent Talents in Fujian Province (11FJRC01) and Fujian Youth College Outstanding Research Talents Cultivation Plan (JA10004).

等人[7]利用带标签的Petri网构建了ABS (anti-lock braking system)系统模型从而检测出该系统中存在的故障问题. Hashizume, Kuwashita等[8]提出了利用普通Petri网中的库所不变量的方法来寻找系统的故障.

对于部分可观的离散事件系统, 其故障诊断问题将会变得非常复杂, 因为系统状态是各单元状态的排列组合n个单元, 会有2^n个系统状态数的存在因此不可观测的状态空间随着系统规模呈现指数级增长, 面临空间爆炸的危险, 由于故障诊断实际是在庞大的状态空间内预测故障行为, 这使得部分可观的离散事件系统的故障诊断变得异常困难. Ru和Hadjicostis[9]提出了将给定的部分可观的Petri网转化为等价的有标签的Petri网, 通过给Petri网中库所和变迁加观测器的方法, 计算出故障变迁发生的置信度. 这种方法利用Petri网结构信息来转化网的结构, 诊断效率提高, 但是当系统复杂性增大时, 与可观标签序列相对应的结点的可达图的构建复杂性会呈现指数级增长, 增加了搜索故障的难度. Cabasino, Giua和Seatzu[10]提出了关于部分可观Petri网的方法故障诊断的, 其中给出了基础标识和故障函数的概念, 并利用基础标识可达图给出了故障诊断方法, 该方法从搜索系统各个状态的角度进行故障诊断, 故障定位清晰, 但是当系统复杂度增加时, 该方法面临空间爆炸和诊断不确定性的问题. 紧接着 Cabasino, Giua 和 Seatzu 等人[11]同样基于基础标识的思想, 对不同的Petri网结构作出了改进, 提出针对带标签的 Petri 网的分散式诊断的方法. 后来Cabasino, Giua和Seatzu[12]将基础可达树扩展到改进的基础可达图, 通过构建基础可达诊断器, 来对有界的Petri网进行诊断. Giua, Cabasino等[13]又提出了针对无界Petri网的诊断方法, 通过构建可覆盖树来解决无界的Petri网的故障诊断问题, 这种方法将应用范围扩展到无界Petri网, 但是当系统的状态数增多时, 验证网的构建复杂性呈指数级增长, 故障诊断行为变得非常困难. Cabasino, Giua和Pocci等[14]针对一个制造业系统, 对比了利用基础可达诊断器进行诊断的方法和利用可达树进行故障诊断的方法, 验证了基础可达诊断器方法具有更低的计算复杂性. 最后Cabasino, Giua和Seatzu等[15]在文献[10–11]的基础上, 利用基础标识的方法, 将故障变迁推广到带有相同标签的不可分辨的可观变迁, 拓宽了基础标识方法的应用范围. 基础标识的方法从可达图出发, 仅仅利用变迁之间的关系与标识中蕴含的信息, 诊断效率大大降低.

针对现有方法中存在的诊断效率低、故障函数分类模糊以及对Petri网结构信息的利用率低等缺点, 提出了一种针对部分可观Petri网系统的故障诊断方法. 该诊断方法主要关注Petri网的结构信息, 借助Petri网内部托肯的演化情况, 利用可观变迁序列中所蕴含的故障信息来分析和判断故障发生情况. 首先需要确定故障变迁的可诊断性, 通过定义故障变迁的可诊断子网的概念, 以及引入Petri网中路径的相关概念来界定其可诊断的范围. 在可诊断性的基础上, 针对故障变迁的可诊断子网进行故障诊断: 首先定义Petri网的几种基本网结构, 在这几种基本网结构的基础上, 对可诊断子网结构进行分析, 根据观测到的可观变迁的信息, 提取子网的结构信息; 根据可观变迁的激发次数, 基于子网结构特征, 得到子网内部托肯的流动情况; 最后根据故障变迁的输入库所或输出库所内的最大滞留托肯数以及故障函数的含义等, 可以得到该故障变迁的发生情况. 本文给出了一个针对部分可观Petri网故障诊断的方法, 该方法在满足故障变迁的上游子网中不存在分流子网, 下游子网中不存在逆分流子网的约束条件下, 通过对Petri网本身的结构信息的分析和利用, 无需遍历系统的所有状态, 大大减少了计算的复杂度, 属于多项式级计算复杂度, 对于可观信息的提取和处理, 提高了诊断效率, 同时很大程度上解决了基础标识方法中Petri网结构信息利用率低的缺点.

2　基本概念(Basic concepts)

Petri网的结构表示为$N = (P, T, \mathrm{Pre}, \mathrm{Post})$, 其中: P是库所的集合: $P = \{p_1, p_2, \cdots, p_n\}$; T是变迁的集合: $T = \{t_1, t_2, \cdots, t_m\}$; $\mathrm{Pre}: P \times T \to \{0, 1, \cdots\}$是前向关联矩阵, 其定义了从库所到变迁的有向弧的权值; $\mathrm{Post}: T \times P \to \{0, 1, \cdots\}$是后向关联矩阵, 其定义了从变迁到库所的有向弧的权值.

$N' = (P', T', \mathrm{Pre}', \mathrm{Post}')$, $P' \subseteq P$, $T' \subseteq T$, N'称为N的子网, Pre'和 Post'为Pre和Post分别在$P' \times T'$上的投影.

由有向弧连接着交替的库所和变迁组成的序列称为路径. 针对一个子网, 若一条路径中的任意一个结点不属于该子网, 则称该路径在子网外. ${}^\bullet p$和$p^\bullet$分别表示库所p的输入变迁集合和输出变迁集合, 在本文中表示库所p的一个输入变迁和输出变迁. ${}^\bullet t$和$t^\bullet$分别表示变迁t的输入库所集合和输出库所集合. 标识是n维的列向量$\boldsymbol{m}$, 其第$i \in \mathbb{Z}$维表示对应库所内的托肯数, 初始标识表示为$\boldsymbol{m}_0$. 当且仅当$\boldsymbol{m} \geqslant \mathrm{Pre}(\cdot, t)$, 变迁$t$在标识$\boldsymbol{m}$下是使能的, 记做$\boldsymbol{m}[t\rangle$. 只有使能的变迁才能激发. 如果$\boldsymbol{m}[t\rangle$, 变迁$t$激发后系统到达新的标识$\boldsymbol{m}' = \boldsymbol{m} + D \cdot \boldsymbol{\delta}(t)$, 其中$\boldsymbol{\delta}(t)$是一个$m$维的(激发)列向量, 其$t$对应的维为1, 其余为0, $D = \mathrm{Post} - \mathrm{Pre}$, 是 Petri 网的关联矩阵. Petri网中所有变迁序列构成的集合称作序列集, 记做T^*. 如果变迁序列$\sigma \in T^*$且在$\boldsymbol{m}$下是使能的, 记做$\boldsymbol{m}[\sigma\rangle$, 激发后系统到达标识$\boldsymbol{m}'$, 记做$\boldsymbol{m}[\sigma\rangle\boldsymbol{m}'$.

变迁集$T = T_\mathrm{o} \cup T_\mathrm{u}$, 其中$T_\mathrm{o}$为可观变迁集合, 可观变迁用$t$表示, T_u为不可观变迁集合, 不可观变迁用ε表示. 不可观变迁集T_u分为两个子集, 即$T_\mathrm{u} = T_{\mathrm{u,f}} \cup T_{\mathrm{u,reg}}$, 其中$T_{\mathrm{u,f}}$是故障变迁集合, $T_{\mathrm{u,reg}}$是非故障不可观变迁集合.

定义 1 设R是一个非空的变迁集合, σ是一个变迁序列, 仅保留序列σ中属于集合R的变迁, 形成一个新的序列, 称序列σ在集合R上的投影, 记做$\rho(\sigma, R)$.

3 故障诊断(Fault diagnosis)

3.1 故障的可诊断性(Fault diagnosability)

在对故障进行诊断之前, 先要确定故障的可诊断性.

定义 2 在Petri网中存在一条路径, 若该路径满足:

1) 路径中所有的变迁均为不可观变迁;

2) 路径中不存在环状结构;

则该路径称为一条不可观路径.

定义 3 在Petri网中存在一条包含库所p的路径, 它的起始结点和终止结点为可观变迁, 其余变迁均为不可观变迁, 则这条路径称作库所p的可观路径.

定义 4 在一个Petri网中, 若通过可观测到的变迁信息, 判断某一故障变迁一定发生、可能发生或者不会发生, 则该故障变迁称作是可诊断的.

定义 5 给定Petri网中的一个故障变迁, 由其输入库所和输出库所的可观路径组成的子网, 称作该变迁的故障子网, 若该故障子网满足:

1) 子网内任何库所p不是子网外任何不可观路径中的结点;

2) 子网内任何变迁不是子网外任何库所的输出;

则该故障子网称作该变迁的可诊断子网.

如图1所示, 变迁$t_{\rm f}$的输入库所p_1, p_3, p_4和输出库所p_5, p_7的可观路径构成故障子网, 如图2所示, 由于p_2,p_6不满足定义5中的条件(1), 因此只有输入库所p_1, p_4和输出库所p_7的可观路径构成$t_{\rm f}$的可诊断子网.

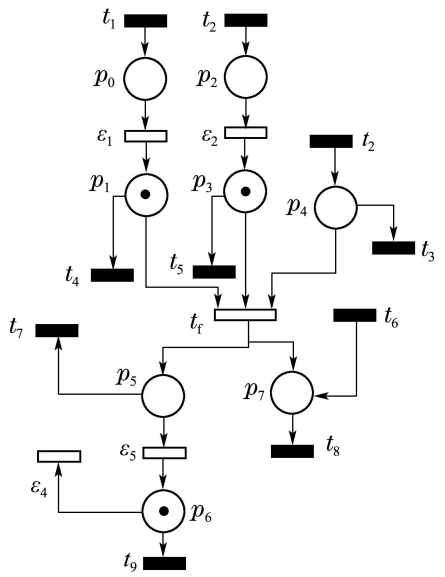

图 1 故障子网模型

Fig. 1 The fault subnet model

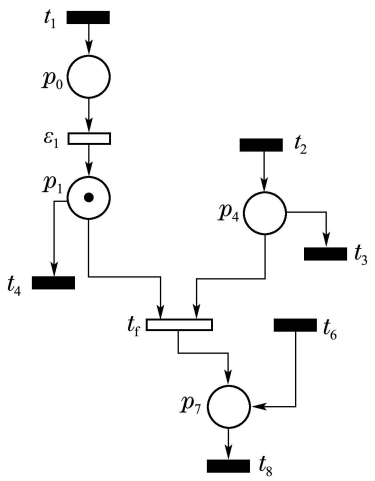

图 2 可诊断子网模型

Fig. 2 The diagnosable subnet model

引理 1 变迁$t_{\rm f}$的故障子网是可诊断子网时, 故障变迁是可诊断的.

证 设$p \in {}^{\cdot}t_{\rm f}$, $p' \in t_{\rm f}^{\cdot}$. 在$t_{\rm f}$的故障子网中, 设π_1是从库所p的可观路径的起始结点到库所p的一条路径, 该路径中任何库所不是子网外任何不可观路径中的结点, 该路径中的变迁不是子网外任何库所的输出, 这样在已知路径π_1中可观变迁的激发次数的情况下, 可以保证托肯只在路径π_1中流动, 因此可以推断出输入库所p内最多流入多少托肯; 同理, 设π_2是从库所p到其可观路径(出去包含$t_{\rm f}$的可观路径外)的汇变迁的一条路径, 可以推断出输入库所p至少流出多少托肯. 这样库所p中最终存留的托肯可以推算出来. 同理, 留在库所p'中的托肯也可以求得. 根据这两个条件, 可以检测到故障变迁$t_{\rm f}$的发生, 即故障变迁$t_{\rm f}$是可诊断的.

3.2 基于结构信息的故障诊断(Fault diagnosis based on structure information)

在给出故障变迁的诊断方法之前, 需要确定其可诊断性, 当变迁的故障子网为可诊断子网时, 故障变迁是可诊断的, 下面给出故障变迁的故障诊断方法.

定义 6 给定Petri网中的一个结点, 以该结点为终止结点的所有路径构成的子网, 称作该结点的上游子网; 以该结点为起始结点的所有路径构成的子网, 称作该结点的下游子网.

定义 7 给定Petri网中的两个变迁t_1和t_2, 若t_1的输出库所是t_2的输入, 则t_1称作t_2的直接上游变迁, t_2称作t_1的直接下游变迁.

定义 8 一个库所p的可观路径中, 由可观变迁指向库所p的路径中所有变迁组成的集合称为库所p的上游变迁集, 记做$T(p)$, 由库所p指向可观变迁的路径中所有变迁组成的集合称为库所p的下游变迁

集, 记做$T'(p)$.

定义 9　给定Petri网N中的一个故障变迁$t_{\rm f}$, 用库所p表示$t_{\rm f}$的一个输入库所或输出库所, 在$t_{\rm f}$的可诊断子网中, $t_{\rm f}$的上游级号函数是从集合$T(p)$到非负整数集合的映射, 即$K:T(p)\to\{0,1,2,\cdots\}$, 其中$\forall t\in T(p)$,

$$K(t)=\begin{cases}0, & t\in T_{\rm o},\\ K(t')+1,\ t\in T_{\rm u},\ t'\in T(p), & \end{cases}\tag{1}$$

其中t'是t的直接上游变迁.

定义 10　给定Petri网中的一个故障变迁$t_{\rm f}$, 用p表示$t_{\rm f}$的某个输入库所或输出库所, 在$t_{\rm f}$的可诊断子网中, $t_{\rm f}$的下游级号函数是从$T'(p)$到非负整数集合的映射, 即$H:T'(p)\to\{0,1,2,\cdots,t\}$, 其中$\forall t\in T'(p)$,

$$H(t)=\begin{cases}0, & t\in T_{\rm o},\\ H(t')+1,\ t\in T_{\rm u},\ t'\in {\rm T}'(p), & \end{cases}\tag{2}$$

其中t'是t的直接下游变迁.

根据定义8和定义9, 可以得到故障变迁$t_{\rm f}$的可诊断子网内每个变迁的级号值, 将相同级号值的变迁归为一类, 这样就可以对整个子网内的变迁进行分类.

定义 11　给定一个Petri网的初始标识$\boldsymbol{m}_0$和可观变迁序列ω, 定义集合$M_{\omega}=\left\{\boldsymbol{m}|\boldsymbol{m}_0[\sigma\rangle\boldsymbol{m},\rho(\sigma,T_{\rm o})=\omega,\sigma\in T^*\right\}$, M_{ω}称作ω的伴随标识集.

定义 12　给定Petri网中的一个库所p、初始标识$\boldsymbol{m}_0$和一个可观变迁序列ω, 若存在一个可观序列$\omega_1=\rho(\omega,T(p))$, 则$\theta(p,\omega)=\max\limits_{\boldsymbol{m}\in{\rm M}_{\omega_1}}[\boldsymbol{m}(p)-\boldsymbol{m}_0(p)]$称作库所$p$在$\omega$下的最大流入托肯数.

为了计算$\theta(p,\omega)$, 下面给出算法1.

算法 1　计算$t_{\rm f}$输入库所或输出库所p的$\theta(p,\omega)$.

输入: $t_{\rm f}$的可诊断子网N, 可观变迁序列ω, 初始标识$\boldsymbol{m}_0$.

输出: $\theta(p,\omega)$.

Step 1　在N中, $\forall t\in T(p)$, 利用式(1)计算$K(t)$;

Step 2　令$i=0$, $\boldsymbol{m}=\boldsymbol{m}_0$;

Step 3　得到同一级号的变迁组成的变迁集$T_i=\{t\in T(p)|K(t)=i\}$;

Step 4　令$T=T_i$;

Step 5　若$T\neq\phi$, 转Step 6; 否则转Step 9;

Step 6　判断在标识$\boldsymbol{m}$下, 变迁t是否使能, 是, 转Step 7; 否, 转Step 8;

Step 7　令$\boldsymbol{m}=\boldsymbol{m}+D\cdot\boldsymbol{\delta}(t)$, 转Step 6;

Step 8　令$T=T-\{t\}$, 转Step 5;

Step 9　$i=i+1$, 若$i\leqslant K(\dot{}p)$, 转Step 3; 否则转Step 10;

Step 10　$\theta(p,\omega)=\boldsymbol{m}(p)-\boldsymbol{m}_0(p)$, 退出算法.

算法1是基于Petri网结构特征提出的. 在算法1中首先得到故障变迁输入库所或输出库所的可观路径中所有变迁的级号函数值. 可观上游路径中的可观变迁激发, 即有托肯流入子网中, 更新标识, 级号加1, 让新级号值的使能变迁在新标识下全部激发后, 标识再次更新, 级号再次加1, 再次激发当前标识下的使能变迁, 直到托肯到达输入库所或输出库所时, 停止更新标识. 此时, 输入库所或输出库所中变化的托肯数就是最大流入托肯数. 由于该算法和子网中变迁的个数有关, 当系统变复杂时, 无需遍历所有状态, 计算复杂度是多项式级的.

引理 2　给定Petri网中的一个故障变迁$t_{\rm f}$, 库所p表示$t_{\rm f}$的输入库所或输出库所, 若$t_{\rm f}$的上游子网中不存在单一库所与其多个输出变迁的子网, 则算法1中求得的$\theta(p,\omega)$为库所p在ω下的最大流入托肯数.

证　在Petri网中, 除一对一关系外, 库所和变迁构成的子网只有4种: 单一库所与其多个输入变迁、单一库所与其多个输出变迁、单一变迁与其多个输入库所以及单一变迁与其多个输出库所. 当已知单一库所中的托肯数, 针对每个变迁而言, 不确定经过每个变迁流出的托肯数是多少. 由于在$t_{\rm f}$的上游子网中托肯的流动数量是不确定的, 因此利用算法1最终得到的$\boldsymbol{m}(p)$是不确定的, 而对于由库所和变迁构成的其他子网结构而言, 托肯在子网中流动的情况是确定的. 又由于在Petri网中, 库所和变迁只构成这几种基本子网结构, 所以当$t_{\rm f}$的上游子网中不存在单一库所与其多个输出变迁的子网时, 算法1最终求得的$\theta(p,\omega)$为库所p在ω下的最大流入托肯数.

定义 13　给定Petri网中的一个库所p、初始标识$\boldsymbol{m}_0$和一个可观变迁序列ω, 若存在一个可观变迁序列$\omega_2=\rho(\omega,T'(p))$, 则$\xi(p,\omega):=\min\limits_{\boldsymbol{m}\in M_{\omega_2}}[\boldsymbol{m}(p)-\boldsymbol{m}_0(p)]$称作库所$p$在$\omega$下的最小流出托肯数.

为了计算$\xi(p,\omega)$, 下面给出算法2.

算法 2　计算$t_{\rm f}$输入库所或输出库所p的$\xi(p,\omega)$.

输入: $t_{\rm f}$的可诊断子网N, 可观变迁序列ω, 初始标识$\boldsymbol{m}_0$.

输出: $\xi(p,\omega)$.

Step 1　在N中, $\forall t\in T'(p)$, 利用式(2)计算$H(t)$;

Step 2　取$\omega_2=\rho(\omega,T'(p))$, 同一级号的变迁组成的变迁集$T_i=\{t\in T'(p)|H(t)=i\}$;

Step 3　令$T=T_i$, $\boldsymbol{m}=\boldsymbol{m}_0$, $i=1$, $q=0$;

Step 4　ω_2是否为空字符串, 是, 转Step 17; 否, 转Step 5;

Step 5　取ω_2的第一个变迁t;

Step 6 $\boldsymbol{m}$下t是否使能, 是, 转Step7; 否, 转Step 9;

Step 7 $\boldsymbol{m}=\boldsymbol{m}+D\cdot\boldsymbol{\delta}(t)$;

Step 8 将t从ω_2中删除, 转Step 4;

Step 9 i是否等于1, 是, 转Step 10; 否, 令$i=i-1$, 转Step 10;

Step 10 i是否等于$H(p^{\cdot})$, 是, 转Step 16; 否, 转Step 11;

Step 11 取$t\in T$;

Step 12 $\boldsymbol{m}$下t是否使能, 是, 转Step 13; 否, 转Step14;

Step 13 $\boldsymbol{m}=\boldsymbol{m}+D\cdot\boldsymbol{\delta}(t)$, 转Step 4;

Step 14 $T=T-\{t\}$, 判断T'是否为空集, 是, 转Step 15; 否, 转Step 11;

Step 15 $i=i+1$, 转Step 10;

Step 16 取$t\in T$, 判断在$\boldsymbol{m}$下t是否使能, 是, $q=q+1$, 转Step 13; 否, 转Step 17;

Step 17 $\xi(p,\omega)=q$, 退出算法.

算法2是基于Petri网的特征结构提出的, 在库所p的下游子网中, 观测到一个可观变迁序列ω_2, 在ω_2中任取一个可观变迁t, 若t的激发次数小于其输入库所中的托肯数, 则不需要库所p的托肯数来补充, 因此库所p的最小流出托肯数为零, 若该可观变迁t的激发次数大于其输入库所中的托肯数, 就需要上一级号值的变迁激发, 从而来补充可观变迁t的输入库所中的托肯数, 以此类推, 直到需要最高级号值的变迁激发, 即库所p的输出变迁的激发来补充该可观变迁t的输入库所中的托肯数, 其他可观变迁也进行同样的步骤, 当全部的可观变迁全部激发完后, 此时, 总共需要补充的托肯的数量就是库所p在ω下的最小流出的托肯数.

引理 3 给定Petri网中的一个故障变迁$t_{\rm f}$, 库所p表示$t_{\rm f}$的输入库所或输出库所, 若$t_{\rm f}$的下游子网中不存在单一库所与其多个输入变迁的子网, 则算法2中求得的$\xi(p,\omega)$为库所p在ω下的最小流出托肯数.

证 在Petri网中, 除一对一关系外, 库所和变迁构成的子网只有4种: 单一库所与其多个输入变迁、单一库所与其多个输出变迁、单一变迁与其多个输入库所以及单一变迁与其多个输出库所.当已知单一库所中的托肯数, 针对每个变迁而言, 不确定经过每个变迁流入的托肯数是多少. 在$t_{\rm f}$的下游子网中托肯的流动数量是不确定的, 因此利用算法2最终得到的$\boldsymbol{m}(p)$是不确定的, 而对于库所和变迁构成的其他子网结构而言, 托肯在子网中流动的情况是确定的, 又由于在Petri网中, 库所和变迁只构成这几种基本子网结构, 所以当$t_{\rm f}$的下游子网中不存在逆分流子网时, 算法2最终求得的$\xi(p,\omega)$为库所p的最小流出托肯数.

在一个实际系统中, 库所和变迁构成的子网可以是以上4种子网的排列组合, 存在相当大数量的可能性, 当系统中故障变迁的子网满足引理2和引理3的条件时, 即除去故障变迁上游子网中不存在分流子网, 下游子网中不存在逆分流子网的一种可能情况, 系统可以由子网中的可观变迁的激发次数确定故障变迁的输入输出库所中的相应托肯数. 这种求解故障变迁输入输出库所中托肯数的方法确实存在一定的局限性, 但还是可以满足大部分实际系统的.

定义 14 给定Petri网中的一个库所p、可观变迁序列ω和初始标识$\boldsymbol{m}_0$, $\Phi(p,\omega):=\max\limits_{\boldsymbol{m}\in M_\omega}\boldsymbol{m}(p)$称作库所$p$在$\omega$下的最大滞留托肯数.

引理 4 给定一个故障变迁$t_{\rm f}$和一个可观变迁序列ω, 库所p表示$t_{\rm f}$的一个输入库所或输出库所, 库所p在可观变迁序列ω下的最大滞留托肯数$\Phi(p,\omega)=\theta(p,\omega)-\xi(p,\omega)+\boldsymbol{m}_0(p)$.

证 在可观变迁序列ω下, 假设库所p中的初始托肯数为$\boldsymbol{m}_0(p)$, 经过p的可观上游路径中变迁的激发, 当前标识为$\boldsymbol{m}'$, p在ω下的最大流入托肯数$\theta(p,\omega)=[\boldsymbol{m}'(p)-\boldsymbol{m}_0(p)]$; 又经过$p$的可观下游路径中变迁的激发, 最终当前标识为$\boldsymbol{m}$, 在$\omega$下最小流出托肯数$\xi(p,\omega)=[\boldsymbol{m}'(p)-\boldsymbol{m}(p)]$. 因此, 库所$p$在可观变迁序列$\omega$下的最大滞留托肯数为$\Phi(p,\omega)=\{[\boldsymbol{m}'(p)-\boldsymbol{m}_0(p)]-[\boldsymbol{m}'(p)-\boldsymbol{m}(p)]\}+\boldsymbol{m}_0(p)=\theta(p,\omega)-\xi(p,\omega)+\boldsymbol{m}_0(p)$.

定义 15 给定Petri网中一个故障变迁$t_{\rm f}$的子网, 在子网中定义一个故障函数, 是从可观变迁集和故障变迁集到集合$\{0,1,2\}$的映射, 即$\Delta T_{\rm o}^{\ *}\times T_{u,f}\to\{0,1,2\}$. 当$\Delta(\omega,t_{\rm f})=0$, 表示故障$t_{\rm f}$不会发生; $\Delta(\omega,t_{\rm f})=1$, 表示故障$t_{\rm f}$可能发生; $\Delta(\omega,t_{\rm f})=2$, 表示故障$t_{\rm f}$一定发生.

定理 1 给定一个故障变迁$t_{\rm f}$、一个可观变迁序列ω和初始标识$\boldsymbol{m}_0$, $p\in{}^{\bullet}t_{\rm f}$, $p'\in t_{\rm f}^{\bullet}$, 若$t_{\rm f}$的上游子网中不存在分流子网, 下游子网中不存在逆分流子网, 则变迁$t_{\rm f}$的故障函数如下:

$$\Delta(\omega,t_{\rm f})=\begin{cases}0,\ \text{如果}\exists p\in{}^{\bullet}t_{\rm f},\ \Phi(p,\omega)=0,\\ 1,\ \text{如果}\forall p\in{}^{\bullet}t_{\rm f},\ \{\Phi(p,\omega)\neq 0\wedge\Phi(p',\omega)\geqslant 0\},\\ 2,\ \text{如果}\forall p'\in t_{\rm f}^{\bullet},\ \Phi(p',\omega)<0.\end{cases}\tag{3}$$

证 当存在可诊断子网时, 该故障变迁$t_{\rm f}$是可诊断的. 在当前标识下, 若满足$t_{\rm f}$的上游子网中不存在分流子网, $t_{\rm f}$的下游子网中不存在逆分流子网, 根据引理2和引理3可得到$t_{\rm f}$的输入库所p和输出库所p'的最大流入托肯数和最小流出托肯数, 然后根据引理4可

得到库所p和p'的最大滞留托肯数$\Phi(p,\omega)$和$\Phi(p',\omega)$. 在故障变迁$t_{\rm f}$的可诊断子网中, 若存在任意一个输入库所p的$\Phi(p,\omega)$为零时, 表示输入库所p内增加的托肯数抵消了初始托肯数, 即此时p内无托肯, 变迁$t_{\rm f}$不使能, 因此在这种情况下故障变迁$t_{\rm f}$不会发生; 当任意一个输出库所p'的$\Phi(p',\omega)$小于零时, 即输出库所p'流出的托肯数大于流入的托肯数和初始托肯数之和, 这种情况是不合理的, 因此需要故障变迁$t_{\rm f}$的激发来补充流入p'中的托肯数, 因此故障变迁$t_{\rm f}$一定发生, 当任意一个输入库所p的$\Phi(p,\omega)$不等于零且任意任意一个输出库所p'的$\Phi(p',\omega)$大于零时, 故障变迁$t_{\rm f}$使能, 情况不能判定, 故障可能发生.

在一个实际系统中, 若该系统中某一资源存在资源分享或资源冲突的问题, 即多个事件同时占有同一资源, 且其中任意一个事件经过有限个事件后会导致一个故障的发生, 该类实际系统的故障问题不可以用上述方法诊断. 比如针对一个通信系统, 存在一个数据包可以通过多条单独通道进行传输, 其中一条或多条传输通道存在的故障问题不可以利用上述方法诊断. 但是由于实际系统的子网是由单一库所与多个输出变迁、多个库所与单一输出变迁、多个变迁和单一输出库所、单一变迁和多个输出库所排列组合构成的, 存在很多种可能性, 而这只是其中一种不能满足的情况, 因此该方法还是可以满足大部分实际系统的.

将上述几个部分总结成一个完整的算法, 如下所示:

算法 3　基于Petri网结构信息的故障诊断方法.

输入: Petri网N, 故障变迁$t_{\rm f}$, 可观变迁序列ω以及初始标识$\boldsymbol{m}_0$.

输出: $\Delta(\omega,t_{\rm f})$.

Step 1　构建故障变迁$t_{\rm f}$的故障子网$N_{t_{\rm f}}$;

Step 2　根据引理1判断$t_{\rm f}$是否是可诊断的, 是, 转Step 3; 否, 转Step 7;

Step 3　$\forall p\in {}^{\bullet}t_{\rm f}$, 根据算法1和算法2计算库所$p$的$\theta(p,\omega)$和$\xi(p,\omega)$;

Step 4　$\forall p'\in t_{\rm f}^{\bullet}$, 根据算法1和算法2计算库所$p'$的$\theta(p',\omega)$和$\xi(p',\omega)$;

Step 5　计算$\Phi(p,\omega)$和$\Phi(p',\omega)$;

Step 6　根据式(3)计算故障函数$\Delta(\omega,t_{\rm f})$;

Step 7　退出算法.

算法3正确性的分析: 针对一个系统的Petri网模型, 首先需要判断其中故障变迁的可诊断性, 如果可以确定故障变迁的输入库所和输出库所中滞留的托肯数, 就可以利用算法3进行故障诊断, 因此对于故障变迁, 利用引理1, 保证了若存在可诊断子网, 就可以从可观变迁序列ω蕴含的信息中判断托肯在子网内的流动情况, 即故障是可诊断的. 在故障变迁可诊断子网内, 利用引理2和引理3, 在已知子网内可观变迁激发次数的基础上, 推算出故障变迁$t_{\rm f}$的所有输入库所p和所有输出库所p'内的最大滞留托肯数$\Phi(p,\omega)$和$\Phi(p',\omega)$, 在当前标识下, 当任意一个输入库所p的$\Phi(p,\omega)$为零时, 对应的库所p内无托肯, 故障变迁不使能, 故障不会发生; 当任意一个库所p'的$\Phi(p',\omega)$小于零时, 对应的库所p'内流出的托肯数大于流入的托肯数, 库所p'中的托肯数为负数, 这种情况是不合理的, 则需要故障变迁激发来补充流入的托肯, 则故障变迁一定发生, 当任意一个输入库所p的$\Phi(p,\omega)$不等于零且任意一个库所p'的$\Phi(p',\omega)$大于零时, 故障变迁使能, 故障可能发生.

算法3的复杂性分析: 当系统的复杂度增加时, 系统的状态数呈现指数级增长, 但是系统Petri网模型中的结点数却随着系统的单元数呈现多项式级增加, 即有n个单元数, 系统状态数为2^n, Petri网的结点数为m个. 由于故障变迁的可诊断子网也是由结点构成的, 因此可诊断子网的结点数也随着系统的单元数呈现多项式级增加, 与系统的状态数无关. 由于本文的方法是通过提取可诊断子网内的结点信息, 对故障变迁进行诊断, 因此该方法的计算复杂度随着系统单元数的增加呈现多项式级增长, 适用于工程应用.

下面具体解释如何利用算法3进行故障诊断. 如图3所示.

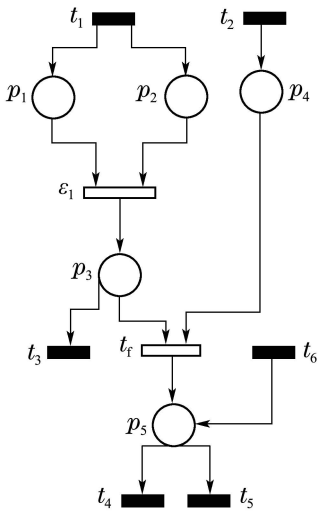

图 3　一个可诊断子网模型

Fig. 3　A model of diagnosable subnet

图3是故障变迁$t_{\rm f}$的可诊断子网模型, 在初始标识下, $\boldsymbol{m}(p_3)$, $\boldsymbol{m}(p_4)$, $\boldsymbol{m}(p_5)$均为零, 假设变迁t_1激发$\theta(p_3)$次, 则进入库所p_1, p_2中的托肯数均为$\theta(p_3)$, 在ε_1和p_1, p_2构成子网中, ε_1的激发次数为$\theta(p_3)$, 最大流入库所p_3的托肯数为$\theta(p_3)$, 若变迁t_3的激发次数为$\xi(p_3)$, 则最小流出库所p_3的托肯数为$\xi(p_3)$, 因此库

所p_3中最大滞留托肯数为$\Phi(p_3)=\theta(p_3)-\xi(p_3)$; 同理若变迁$t_2$激发次数为$\theta(p_4)$, 由于无流出库所$p_4$的托肯, 则$p_4$中最大滞留托肯数为$\Phi(p_4)=\theta(p_4)$. 由于$p_3$和$p_4$都是故障变迁$t_{\rm f}$的输入库所, 因此只要任意一个输入库所的最大滞留托肯数为0, 故障变迁$t_{\rm f}$就不会发生. 若变迁t_4的激发次数为$\xi_1(p_5)$, 变迁t_5的激发次数为$\xi_2(p_5)$, p_5, t_4和t_5构成分流结构, 则库所p_5的最小流出托肯数为$\xi(p_5)=\xi_1(p_5)+\xi_2(p_5)$; 变迁$t_6$激发次数为$\theta(p_5)$, 则$p_5$中最大流入托肯数为$\theta(p_5)$, 因此库所$p_5$中最大滞留托肯数为$\Phi(p_5)=\theta(p_5)-\xi(p_5)$. 当库所$p_5$中的最大滞留托肯数小于0时, 需要故障变迁$t_{\rm f}$激发来补充托肯, 激发来补充托肯, 因此故障变迁$t_{\rm f}$一定发生. 当库所$p_3$和$p_4$中最大滞留托肯数均不为0, 即$\Phi(p_3)\neq 0$, $\Phi(p_4)\neq 0$, 且库所p_5中最大滞留托肯数大于等于0, 即$\Phi(p_5)\geqslant 0$, 此时故障变迁$t_{\rm f}$使能, 故障可能发生.

4 实例(Example)

如图4所示, 给出了一个加工生产线的Petri网模型[15]. 其中: 可观变迁集$T_{\rm o}=\{t_1,t_2,t_3,t_4,t_5\}$, 不可观变迁集$T_{\rm u}=\{\varepsilon_6,\varepsilon_7,\varepsilon_8,\varepsilon_9,\varepsilon_{10},\varepsilon_{11},\varepsilon_{12},\varepsilon_{13}\}$, 故障变迁为$\varepsilon_{13}$. 初始状态为库所$p_1$中有托肯, 代表零件准备生产, 生产零件所用的板坯和板块准备进入生产线. 经过变迁t_1, 板坯和板块被分开, 两个板块进入图4中上面的生产线, 即库所p_2到p_6, 板坯进入下面的生产线, 即p_7到p_{11}. 在这两条线中, 板块和板坯被加工, 即需要经过打滑、清理、上漆以及抛光等一系列步骤, 相对应的是可观变迁t_2的激发和不可观变迁ε_6到ε_{12}的激发. 在上面的生产线中, 当托肯由库所p_{14}进入库所p_5时, 代表一个板块被上漆, 这时系统会发出一个信号. 最终, 板块插入到板坯中的正确位置, 代表零件加工完成, 即变迁t_5的激发. 假设当其中一个板块进入到下面的生产线时, 代表故障发生, 用故障变迁ε_{13}表示.

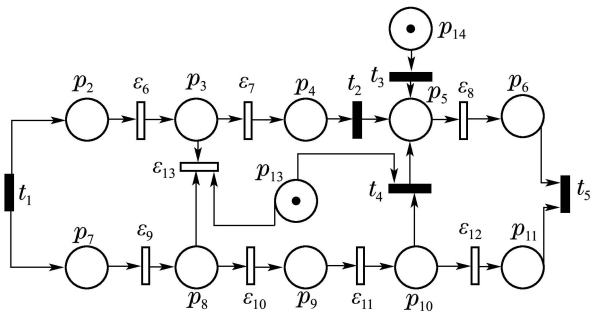

图 4 损坏部件生产线Petri网模型

Fig. 4 Petri net model of damaged parts production line

首先确定ε_{13}的可诊断性, ε_{13}的输入库所和输出库所分别为p_3, p_{13}和p_8, 根据定义4得到ε_{13}的故障子网, 如图5所示. 判断ε_{13}的故障子网是可诊断子网, 根据引理1得到该故障变迁ε_{13}是可诊断的.

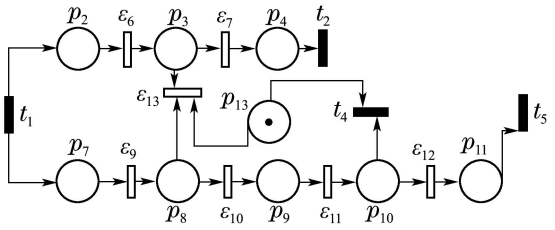

图 5 故障变迁的可诊断子网

Fig. 5 The fault subnet of fault transition

其次, 得到故障变迁ε_{13}的可诊断子网模型, 分析故障变迁的可诊断子网的结构信息. 如图5所示, 各个变迁的级号值如下: $K(t_1)=0$, $K(\varepsilon_6)=K(\varepsilon_9)=1$, $H(t_2)=H(t_4)=H(t_5)=0$, $H(\varepsilon_7)=H(\varepsilon_{12})=1$, $H(\varepsilon_{11})=2$, $H(\varepsilon_{10})=3$. 由于故障变迁ε_{13}的上游子网中不存在分流子网, 下游子网中不存在逆分流子网, 因此, 利用算法1−3计算出输入库所和输出库所的最大滞留托肯数, 如表1所示.

表 1 故障变迁的故障诊断表

Table 1 The fault diagnosis table

ω	$\theta(p_i,\omega)$	$\xi(p_i,\omega)$	$\Phi(p_i,\omega)$	$\Delta(\omega,\varepsilon_{13})$
t_1	$i=3,\ \theta=2$ $i=13,\ \theta=1$ $i=8,\ \theta=1$	$i=3,\ \xi=0$ $i=13,\ \xi=0$ $i=8,\ \xi=0$	$i=3,\ \Phi=2$ $i=13,\ \Phi=1$ $i=8,\ \Phi=1$	1
$t_1t_2t_4$	$i=3,\ \theta=2$ $i=13,\ \theta=1$ $i=8,\ \theta=1$	$i=3,\ \xi=1$ $i=13,\ \xi=1$ $i=8,\ \xi=1$	$i=3,\ \Phi=1$ $i=13,\ \Phi=0$ $i=8,\ \Phi=0$	0
$t_1t_2t_5t_5$	$i=3,\ \theta=2$ $i=13,\ \theta=1$ $i=8,\ \theta=1$	$i=3,\ \xi=1$ $i=13,\ \xi=0$ $i=8,\ \xi=2$	$i=3,\ \Phi=1$ $i=13,\ \Phi=1$ $i=8,\ \Phi=-1$	2

$\omega=t_1$, t_1激发1次, 库所p_3中最大流入托肯数为2. t_2激发0次, 则p_3中最小流出托肯为0, 因此p_3中最大滞留托肯数为2. 同理可得p_{13}中最大滞留托肯数为1. t_1激发1次, 推出库所p_8中最大流入托肯数为1. t_4, t_5激发次数为0, 则库所p_8中最小流出托肯数也为0, 则p_8中最大滞留托肯数为1. $\Delta(t_1,\varepsilon_{13})=1$, 因此故障$\varepsilon_{13}$可能发生.

$\omega=t_1t_2t_4$, t_1激发1次, 库所p_3中最大流入托肯数为2. t_2激发1次, 则p_3中最小流出托肯为1, 因此p_3中最大滞留托肯数为1. 同理可得p_{13}中最大滞留托肯数为0. t_1激发1次, 推出库所p_8中最大流入托肯数为1. t_4激发1次, 则库所p_8中最小流出托肯数为1, 则库所p_8中最大滞留托肯数为0. $\Delta(t_1t_2t_4,\varepsilon_{13})=0$, 因此故障$\varepsilon_{13}$一定不会发生.

$\omega=t_1t_2t_5t_5$, t_1激发1次, 库所p_3中最大流入托肯数为2. t_2激发1次, 则p_3中最小流出托肯数为1. 因此p_3中最大滞留托肯数为1. 同理可得p_{13}中最大滞留托肯数为1. t_1激发1次, 推出库所p_8中最大流入托肯

数为1. t_5激发2次, 则库所p_8中最小流出托肯数为2, 则库所p_8中最大滞留托肯数为-1. $\Delta(t_1t_2t_5t_5, \varepsilon_{13}) = 2$, 因此故障$\varepsilon_{13}$一定发生.

根据上述实例的Petri网可达图, 可以验证该诊断方法的正确性, 限于篇幅, 这里不做详细说明.

Giua[10]的基础标识方法是通过系统的可达图来实现的. 假设观测到的变迁序列为$\omega = t_1t_2t_3t_5t_5$, 则基础标识的方法需要考虑t_3所携带的信息, 但是由于t_3所携带的信息对于故障变迁ε_{13}是否发生不产生直接影响, 因此当系统单元数增加时, 需要遍历系统的整个状态空间, 判断的信息量会随之增大, 这会使基础标识方法的计算复杂性增加, 诊断效率大大降低, 而本文的方法由于是基于系统结构来判断, 从本质上弥补了这个缺点.

5　结论(Conclusions)

针对部分可观 Petri 网, 本文提出了一种基于 Petri 结构信息的故障诊断方法. 根据路径、子网的概念等, 给出了故障变迁的可诊断的条件, 并在可诊断的基础上, 在故障变迁的可诊断子网内提出具体的诊断方法.

根据几种基本子网来描述故障变迁的可诊断子网的结构信息, 同时借助已知的可观测变迁序列, 推断出可诊断子网内部托肯的流动情况, 计算故障变迁的输入库所或输出库所内的最大滞留托肯数, 最终得到故障变迁的故障函数值, 利用此函数值判断故障变迁的发生情况. 由于该方法是利用故障变迁子网的结构特征来完成的, 无需遍历整个状态空间, 大大减少了系统的状态个数, 所以当系统的复杂性增加时, 计算复杂性是多项式级的, 可以用于工程计算.

参考文献(References):

[1] SAMPSTH M, LAFORTUNE S, TENEKETZIS D. Active diagnosis of discrete-event systems [J]. *IEEE Transactions on Automatic Control*, 1998, 43(7): 908 – 929.

[2] ZAD S H, KWONG R H, WONHAM W M. Fault diagnosis in discrete-event system:framework and model reduction [J]. *IEEE Transaction on Automatic Control*, 2003, 48(7): 1199 – 1212.

[3] CORONA D, GIUA A, SEATZU C. Marking estimation of Petri nets with silent transitions [J]. *IEEE Transactions on Automatic Control*, 2007, 52(9): 1695 – 1699.

[4] BASILE F, TOMMASI G D. An effincient approach for online diagnosis of discrete event systems [J]. *IEEE Transactions on Automatic Control*, 2009, 54(4): 748 – 759.

[5] LEFEBVRE D, DELHERM C. Diagnosis of EDS with Petri net models [J]. *IEEE Transactions on Automation Science and Engineering*, 2007, 4(1): 114 – 118.

[6] 郑永煌, 田锋, 李人厚, 等. 基于Petri网的液体火箭发动机启动过程实时在线故障诊断方法 [J]. 信息与控制, 2010, 39(2): 207 – 221. (ZHENG Yonghuang, TIAN feng, LI Renhou, et al. A real time online fault diagnosis algorithm based on Petri net for the starting process of liquid propellant rocket engine [J]. *Information and Control*, 2010, 39(2): 207 – 221.)

[7] CABASINO M P, GIUA A, SEATZU C, et al. Fault diagnosis of an ABS system using Petri nets [C] //*IEEE International Conference on Automation Science and Engineering* . Trieste, Italy: IEEE, 2011, 8: 24 – 27.

[8] HASHIZUME S, YAJIMA T, KUWASHITA Y, et al. Integration of fault analysis and interlock controller synthesis for batch processes [J]. *Chinese Journal of Chemical Engineer*, 2008, 16(1): 57 – 61.

[9] YU R, HADJICOSTIS C N. Fault diagnosis in discrete event system modeled by partially observed Petri nets [J]. *Discrete Event Dynamic Systems*, 2009, 19(4): 551 – 575.

[10] CABASINO M P, GIUA A, SEATZU C. Fault detection for discrete event systems using Petri nets with unobserved transitions [J]. *Automatica*, 2010, 46(9): 1531 – 1539.

[11] CABASINO M P, GIUA A, PAOLI A, et al. Decentralized diagnosis of discrete-event systems using labeled Petri nets [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2013, 43(6): 1477 – 1485.

[12] CABASINO M P, GIUA A, SEATZU C. Diagnosability of bounded Petri nets [C] //*The 28th Chinese Control Conference on Decision and Control*. shanghai: IEEE, 2009, 12: 16 – 18.

[13] CABASINO M P, GIUA A, LAFORTUNE S, et al. A new approach for diagnosability analysis of Petri nets using verifier nets [J]. *IEEE Transaction on Automatic Control*, 2012, 57(12): 3104 – 3117.

[14] CABASINO M P, GIUA A, POCCI M, et al. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems [J]. *Control Engineering Practice*, 2011, 19(9): 989 – 1001.

[15] CABASINO M P, GIUA A, SEATZU C. Diagnosis using labeled Petri nets with silent or undistinguishable fault event [J]. *IEEE Transactions on System, Man, and Cybernetics, Part A: Systems and Humans*, 2013, 43(2): 345 – 355.

作者简介:

叶丹丹　(1991–), 女, 硕士研究生, 主要从事离散事件系统和Petri网理论与应用等究, E-mail: zuietianshiydd@163.com;

罗继亮　(1977–), 男, 副教授, 博士, 主要从事离散事件系统监控理论和Petri网理论与应用等研究, E-mail: jlluo@hqu.edu.cn.