

引用格式:卓伟,张治国,郑锐,等.基于时间 Petri 网的部分可观系统故障诊断[J].电光与控制,2018,25(9):93-100. ZHUO W, ZHANG Z G, ZHENG R, et al. Fault diagnosis for partial observable system with time Petri nets[J]. Electronics Optics & Control, 2018, 25(9):93-100.

基于时间 Petri 网的部分可观系统故障诊断

卓伟¹, 张治国², 郑锐², 刘久富²

(1. 郑州大学软件与应用科技学院, 郑州 450002; 2. 南京航空航天大学自动化学院, 南京 210016)

摘要:研究了 Petri 网在双组元推进气路系统中的故障诊断问题。针对气路系统故障率相对较高且部分关键信息无法通过传感器获取的问题,利用时间 Petri 网在实时系统中的重要作用,把部分可观时间 Petri 网和状态类图(SCG)结合,提出构建修正状态类图(MSCG)的方法。首先根据执行机构是否可观,分为可观测变迁和不可观测变迁,并结合变迁触发关系(同步、异步)修正各变迁时间区间,建立系统的修正状态类图(MSCG)。然后根据所提的故障诊断算法,寻找所有满足可观测变迁触发时间和序列信息的路径,判断所有路径组成的集合是否包含故障变迁,诊断系统是否发生故障。最后以双组元推进气路系统为例,结合气路系统各执行机构可观测状态,建立 Petri 网模型,对系统不可观测部分进行故障诊断,验证了算法的有效性。

关键词:故障诊断; 航天推进系统; 标签时间 Petri 网; 部分可观

中图分类号: TP391 **文献标志码:** A **doi:**10.3969/j.issn.1671-637X.2018.09.020

Fault Diagnosis for Partial Observable System with Time Petri Nets

ZHUO Wei¹, ZHANG Zhi-guo², ZHENG Rui², LIU Jiu-fu²

(1. College of Software and Applied Technology, Zhengzhou University, Zhengzhou 450002, China;
2. College of Automation, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: The fault diagnosis of gas path system in integral bipropellant propulsion is investigated. Aiming at the problems that the failure rate of gas path system is relatively high and some key information can't be obtained through the sensors, a method of building Modified State Class Graph (MSCG) based on Partially Observed Time Petri Nets (POTPN) and State Class Graph (SCG) is presented. Firstly, the transitions are divided into observable and unobservable transitions according to the observability of the actuators, and the time intervals are modified based on the different relationships of the transitions (synchronous and asynchronous). The MSCG is then built with time Petri nets. Based on the proposed fault diagnosis method, all the effective paths that satisfy the observable transition triggering time and sequence information are found out, and it is determined whether the effective paths have fault transitions. Finally, taking the gas path system in integral bipropellant propulsion as an example, and based on the observability of the actuators, a Petri net is built for making fault diagnosis to the unobservable part of the system, which verifies the effectiveness of the algorithm.

Key words: fault diagnosis; aerospace propulsion system; label time Petri net; partially observable

0 引言

大型卫星一般采用双组元挤压推进系统,其特点是对贮箱增压使推进剂输送系统输出相应流量的推进

剂,为发动机提供氧化剂和燃料^[1]。若增压系统出现故障,则航天器无法实现精确定位,甚至报废^[2]。国外公开航天器故障中,推进系统故障导致航天器工作异常占总故障的13%,储箱和管路故障在推进系统故障中占比为56%^[3]。

目前,故障诊断方法主要分为3种,即基于解析模型、基于信号处理和基于知识的方法。其中:基于解析模型的方法需要构建系统精确的解析模型,这对于具有

收稿日期:2017-08-25

修回日期:2018-07-24

基金项目:国家自然科学基金(61473144)

作者简介:卓伟(1978—),男,河南漯河人,硕士,讲师,研究方向为物联网技术、故障诊断、人工智能。

不确定性、时变的复杂系统或非线性系统而言都非常困难;基于信号处理的方法虽然不需要构建系统解析模型,但只有当故障发展到一定程度并影响到系统的外部特性时才有效;基于知识的方法能够克服上述两种方法的缺点,更适用于航天器故障诊断。基于定性模型的方法属于基于知识的方法,它利用系统不完备的先验知识,采用定性模型描述系统结构,定性地预测系统行为,通过与实际的系统行为进行比较,检测系统是否出现故障,通过推理诊断出系统的故障原因^[4-5]。

以往基于定性模型的故障诊断方法主要是对可观节点的故障诊断,对不可观节点的故障诊断还不够完备,因此提出一种基于部分可观时间 Petri 网的故障诊断方法,利用可观测节点的时序信息对不可观节点进行故障诊断。时间间隔比固定时延具有更强的表达能力,间隔既能反映事件发生的不确定性,又能刻画事件发生的时限性^[6-7]。时间 Petri 网不仅可以描述事件间异步、并发等逻辑关系,还可以反映事件时间层次的信息,是基本 Petri 网理论的功能扩充^[8]。本文将研究一种基于部分可观时间 Petri 网的故障诊断方法,在部分可观 Petri 网^[9]和状态类图(State Class Graph, SCG)^[10-11]的基础上,结合时间信息为每个变迁分配属性标签,将其分为可观测变迁与不可观测变迁,构建基于时间的修正状态类图(Modified State Class Graph, MSCG),把复杂的并行事件转变成求解满足时间约束的不等式集合,寻找所有有效路径并根据其属性判断系统是否发生故障。

1 标签时间 Petri 网的故障检测问题

1.1 标签时间 Petri 网

定义 1 Petri 网(Petri Nets, PN)定义为一个四元组 $N = (P, T, P_{re}, P_{ost})$, P 是 m 个库所(Place)的集合, T 是 n 个变迁(Transition)的集合, $P_{re}: P \times T \rightarrow \mathbf{N}$ 和 $P_{ost}: P \times T \rightarrow \mathbf{N}$ 分别是输入弧和输出弧的集合。定义矩阵 $C = P_{ost} - P_{re}$ 为 N 的关联矩阵, 关联矩阵 C 描述前一个变迁对后一个变迁的影响, 代表系统的实时状态。

库所 P 的标识 $M: P \rightarrow \mathbf{N}$ 为每个库所分配一个非负整数, 每个库所具有的资源个数记为 $M(p)$ 。当且仅当 $M \geq P_{re}(\cdot, t)$ 变迁 t 逻辑使能, 变迁 t 触发后标识 $M' = M + C(\cdot, t)$ 。标识 M 代表系统资源的实时分布情况, 是关联矩阵 C 的一个重要子集。 M 处触发使能的变迁集合为 $A(M) = \{t \in T \mid M \geq P_{re}(\cdot, t)\}$ 。

定义 2 时间 Petri 网(Time Petri Nets, TPN)定义为 $N_d = (N, Q)$, 其中: $N = (P, T, P_{re}, P_{ost})$ 是 Petri 网的四元组, $Q: T \rightarrow \mathbf{Q} \times (\mathbf{Q} \cup \{\infty\})$ 是变迁初始时间约束相关联的闭区间集合, 变迁 $t_i \in T$ 对应的 Q 由两个自然数组成 $Q(t_i) = (l_i, u_i)$, $l_i \geq 0, u_i \geq l_i, l_i \neq \infty$ 当且仅当在时间区

间 $[l_i, u_i]$ 内变迁 t_i 才能触发。

$\sigma = (t_0, \tau_0)(t_1, \tau_1)(t_2, \tau_2) \cdots (t_h, \tau_h) \in (T \times \mathbf{R}_0^+)$ 为变迁时间序列集合(Transition Time Sequence, TTS), 下标为 i 的变迁 $t_i \in T$ 对应下标为 i 的变迁触发时间点 τ_i , 记为 $M_0[t_0(\tau_0)]M_1[t_1(\tau_1)]M_2 \cdots [t_h(\tau_h)]M_k, t_0 \leq t_1 \leq t_2 \leq \cdots \leq t_k$, 简记为 $M_0[\sigma]M_k$ 或 $M_0[\sigma, \sigma$ 中最后触发变迁的时间 $t_i(\sigma) = \tau_h$ 。

以 $\tau_0 = 0$ 对应标识 (M_0, τ_0) 为初始点的时间 Petri 网 N_d 记为 TPN 系统, 简记为 $\langle N_d, M_0 \rangle$ 。一个 TPN 系统中所有满足 $M_0[\sigma]M$ 的 TTS, σ 记为 $R_i(N_d, M_0)$ 。TPN 系统 $\langle N_d, M_0 \rangle$ 为有界系统, $\forall M \in R_i(N_d, M_0), \exists k \in \mathbf{N}$ 满足 $M(p) \leq k$ 。

给定 TPN 系统 $\langle N_d, M_0 \rangle, M_0[\sigma]M_k$ 且 $t_1, t_2 \in \sigma$ 满足 $t_1, t_2 \in A(M_k)$, 定义 t_1, t_2 的同步距离为 $s_d(t_1, t_2)$, 同步距离是并发变迁的最大触发间隔。

定义 3 标签 Petri 网(Label Petri Nets, LPN)定义为 $\langle N, M_0, \mathcal{L} \rangle$, 标签函数 $\mathcal{L}: T \rightarrow L \cup \{\varepsilon\}$ 为每个变迁分配一个标签 L 或空符号 ε 。不可观标签和静止标签集合为 $T_u, T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$, 可观测标签集合为 $T_0, T_0 = \{t \in T \mid \mathcal{L}(t) = L\}$ 。

扩展标签函数满足: 若 $t_j \in T_0$, 则 $\mathcal{L}(t_j) = \gamma, \gamma \in L$; 若 $t_j \in T_u$, 则 $\mathcal{L}(t_j) = \varepsilon$; 若 $\sigma \in T \wedge t_j \in T$, 则 $\mathcal{L}(\sigma t_j) = \mathcal{L}(\sigma)\mathcal{L}(t_j)$; 若 λ 为空序列, 则 $\mathcal{L}(\lambda) = \varepsilon$ 。

时间标签序列集合(Time Label Sequence, TLS) $\delta_0 = (\gamma_{e_0}, \tau_{e_0})(\gamma_{e_1}, \tau_{e_1}) \cdots (\gamma_{e_h}, \tau_{e_h}) \in (L \times \mathbf{R}_0^+)$ 是可观测变迁和对应触发时间的序列集合, $t_l(\delta_0)$ 为最后触发的可观测变迁时间, $t_l(\delta_0) = \tau_{e_h}$, 任意 δ_0 至少存在一个 TTS, σ 与其对应。

1.2 故障检测问题

假设 1 任意变迁 $t_i \in T$ 在时间约束区间 $Q(t_i) = (l_i, u_i) (l, u \in \mathbf{Q})$ 内只发生一次, 且两次触发时间间隔不为零。

假设 2 同一标签 $\gamma \in L$ 可以关联多个变迁, 若 $\mathcal{L}(t_1) = \mathcal{L}(t_2) = \gamma$, 变迁 t_1, t_2 相互独立。

定义 4 给定一个 $\delta_0 \in (L \times \mathbf{R}_0^+)^*$ 和一个时间 $\tau \geq t_l(\delta_0)$, 对应的时间序列集合为

$$\Sigma(\delta_0, \tau) = \{\sigma \in (T \times \mathbf{R}_0^+)^* \mid M_0[\sigma]M, \mathcal{L}(\sigma) = \delta_0,$$

$$t_l(\sigma) = \bar{\tau}, \bar{\tau} \leq \tau,$$

$$\nexists t \in T_u: M[t], r_t(M_0, \sigma) \leq \tau - \bar{\tau}\} \quad (1)$$

式中: $r_t(M_0, \sigma)$ 表示以 M_0 为初始标识经过变迁时间序列 σ 对应变迁 t 触发后的剩余时间; $\bar{\tau}$ 为可观测变迁最后触发时间。式(1)保证时间区间 $\tau - \bar{\tau}$ 处标识 M 可以使能变迁, 但必须为可观测变迁且变迁触发时刻 τ_{e_h} 满足 $\tau_{e_h} \leq \tau$ 。

定义 5 给定一个 TLS 集合 $\delta_0 \in (L \times \mathbf{R}_0^+)^*$ 和一个时间 $\tau \geq \tau_l(\delta_0)$, 对应的标识集合为

$$C(\delta_0, \tau) = \{M \in \mathbf{N}^m \mid M_0[\sigma]M, \sigma \in \Sigma(\delta_0, \tau)\} \quad (2)$$

定义 6 给定一个 TLS 集合 $\delta_0 \in (L \times \mathbf{R}_0^+)^*$ 和一个时间 $\tau \geq t_l(\delta_0)$, 对应的状态集合为

$$S(\delta_0, \tau) = \{M_k, \Theta_k \mid M_k \in C(\delta_0, \tau), \Theta_k = \{\bar{l}_{k_i} \leq \theta_{k_i} \leq \bar{u}_{k_i} \mid t_k \in A(M_k)\}\} \quad (3)$$

定义 7 给定 TLS 集合 $\delta_0 \in (L \times \mathbf{R}_0^+)^*$ 、截止时间 $\tau \in \mathbf{R}_0^+$ 和故障类型 T_f^i 组成的集合 (δ_0, τ, T_f^i) , 定义故障函数 $\Gamma: (L \times \mathbf{R}_0^+)^* \times \mathbf{R}_0^+ \times \{T_f^1, T_f^2, T_f^3, \dots, T_f^i\} \rightarrow \{N, U, F\}$ 为每个集合分配一个故障状态。其中, T_f^i 为故障类型, 包括建模错误和变迁故障。给定 TTS 集合 $\sigma = (t_0, \tau_0)(t_1, \tau_1)(t_2, \tau_2) \dots (t_h, \tau_h) \in (T \times \mathbf{R}_0^+)^*$, 记 $\lg \sigma = t_0, t_1, t_2, \dots, t_h$ 为 σ , 忽略触发时间 τ 的变迁序列集合。

1) $\forall \sigma \in \Sigma(\delta_0, \tau), \exists t_f \in T_f^i$, 满足 $t_f \notin \lg \sigma$, 则 $\Gamma(\delta_0, \tau, T_f^i) = N$, 故障 t_f 不能触发, 任何一个 TTS 集合 σ 都不包含故障变迁 t_f 。

2) $\exists \sigma \in \Sigma(\delta_0, \tau), \exists t_f \in T_f^i$ 满足 $t_f \in \lg \sigma$, 又 $\exists \sigma' \in \Sigma(\delta_0, \tau), \exists t_f \in T_f^i$ 满足 $t_f \notin \lg \sigma'$ 则 $\Gamma(\delta_0, \tau, T_f^i) = U$, 故障变迁 t_f 可能触发也可能没触发, 存在包含故障变迁 t_f 的 TTS 集合 σ , 也存在不包含故障变迁 t_f 的 TTS 集合 σ' 。

3) $\forall \sigma \in \Sigma(\delta_0, \tau), \exists t_f \in T_f^i$, 满足 $t_f \in \lg \sigma$, 则 $\Gamma(\delta_0, \tau, T_f^i) = F$, 故障 t_f 肯定触发, 任何一个 TTS 集合 σ 都包含故障变迁 t_f 。

观测序列中故障集出现的可信度称为置信度, 用 F_b 表示。给定故障变迁 t_f 对应的时间序列集合为

$$\Sigma(\delta_0, \tau, t_f) = \{\sigma \in (T \times \mathbf{R}_0^+)^* \mid t_i \in \sigma\}, M_0[\sigma]M$$

$$F_b = \frac{\Sigma(\delta_0, \tau, t_f)}{\Sigma(\delta_0, \tau)} \quad (4)$$

标签时间 Petri 网进行故障诊断要求设计一个状态估计方法, 寻找满足 TLS 集合 δ_0 和时间约束条件的所有 TTS 集合 σ , 分析时间序列集合 σ 是否包含故障变迁 $t_f \in T_f^i$, 判断 TPN 系统是否故障。

2 基于标签时间 Petri 网的故障诊断方法

2.1 构建 MSCG 图

在 SCG 方法^[11]的基础上添加时间变量和时间约束, 构建基于标签时间 Petri 网的修正状态类图 (MSCG)。MSCG 继承了 SCG, 区别主要是 MSCG 引入了时间变量和时间约束的信息, 可以估计状态集合 $S(\delta_0, \tau)$ 的信息。

2.1.1 构建修正状态类树 (MSCT)

构建 MSCG 图首先要根据算法 1 构建修正状态类树 (Modified State Class Tree, MSCT)。

算法 1 构建 MSCT。

输入 标签时间 Petri 网系统

输出 对应的修正状态类树 MSCT

Step 1 初始化: 根节点 C_0 对应标识 $M_0, l_i^0 = l_i, u_i^0 = u_i$, 根节点标记 $B(C) = E$, 约束条件是不等式集合: $\Theta_0 = \{l_i^0 \leq \theta_i \leq u_i^0 \mid t_i \in A(M_0)\}$,

while 存在一个标记 $B(C) = E$ 的节点 do

Step 2 选择一个新节点 C_k 标记 $B(C) = E$

Step 3 for 任意 $t_i \in A(M_k)$ do

Step 4 if $\max\{0, l_i^k\} \leq \min_{j: t_j \in A(M_k)} \{u_j^k\}$ then

Step 5 t_i 在标识 M_k 触发, $M_q = M_k + C(\cdot, t_i)$

Step 6 for $\forall t_r \in A(M_q)$ do

if $t_r \in A(M_k)$ 且 $M_k - P_{re}(\cdot, t_i) \geq P_{re}(\cdot, t_r)$ then

$$l_r^q = l_r^k - \Delta_i, u_r^q = u_r^k - \Delta_i$$

else

$$l_r^q = l_r, u_r^q = u_r$$

Step 7 建立新节点 C_q 标识为 M_q 约束集合为:

$$\Theta_q = \{\max\{0, l_r^q\} \leq \theta_r \leq u_r^q, \forall t_r \in A(M_q)\}$$

Step 8 C_q 和 C_k 边界为: $t_i, \mathfrak{B}(t_i), \Delta_i$

$$[\max\{0, l_i^k\}, \min_{j: t_j \in A(M_k)} \{u_j^k\}]$$

if 存在和 C_q 相同节点 then

C_q 节点标记 $B(C) = Z$

else

C_q 节点标记 $B(C) = E$

Step 1 定义初始条件 $l_i^0 = l_i, u_i^0 = u_i$, 时间 $\tau = 0$ 及对应时间约束 Θ_0 , 该时间约束 Θ_0 仅是静态时间约束, 不同变迁序列需根据算法 1 修正时间约束。Step 2 使用不同标记 $\mathfrak{B}: C \rightarrow \{E, Z\}$ 避免重复构建相同 MSCT 图, 在标记 $\mathfrak{B}(C) = E$ 的节点构建新的 MSCT 图。

同一个节点 C_k 中, 为保证其他变迁正常触发, 若变迁 $t_i \in T$ 不满足 $\max\{0, l_i^k\} \leq \min_{j: t_j \in A(M_k)} \{u_j^k\}$, 即使逻辑使能也无法触发, 因此标识 M_k 对应确定使能变迁 $A(M) = \{t \in T \mid M \geq P_{re}(\cdot, t)\}$ 只有部分可以触发 (Step 4), $\max\{0, l_i^k\}$ 保证下边界为非负数。Step 6 中, 若变迁 $t_r \in A(M_q)$ 满足 $t_r \in A(M_k)$ 且 $M_k - P_{re}(\cdot, t_i) \geq P_{re}(\cdot, t_r)$, t_r 在前一个标识 C_k 已触发使能, 修改约束条件 $l_r^q = l_r^k - \Delta_i, u_r^q = u_r^k - \Delta_i$, 否则 $l_r^q = l_r^k, u_r^q = u_r^k, \Delta_i$ 为上一步变迁 $t_i \in A(M_k)$ 触发到当前变迁 $t_r \in A(M_q)$ 触发所需时间。在修正状态树 (MSCT) 中复制标记为 $B(C) = Z$ 的节点, 构建 MSCG 图。

2.1.2 修正状态类图 (MSCG) 节点分析

MSCG 是有向图, 节点包含标识 $M \in R_i(N_d, M_0)$ 和使能变迁的时间约束 $\Theta_k = \{l_i \leq \theta_k \leq u_i \mid t_k \in A(M_k)\}$ 。节点之间边界记为 $(t, \gamma, \Delta \in [l^*, u^*])$, 变迁 $t \in T$ 是

源节点到目标节点触发的变迁, $\gamma = \mathfrak{L}(t)$ 是变迁 t 对应的标签属性, $\Delta \in [l^*, u^*]$ 是源节点到目标节点的时间约束。两个节点有相同的标识 M 和相同的时间约束 Θ , 则认为它们是等价的。

定理 1 给定时间 Petri 网系统 $\langle N_d, M_0 \rangle$, 根据算法 1 构建的 MSCG 图节点是有限的。

2.2 基于时间 Petri 网的状态估计

给定一个 TLS 集合 $\delta_0 = (\gamma_{i1}, \tau_1)(\gamma_{i2}, \tau_2) \cdots (\gamma_{ih}, \tau_h) \in (L \times \mathbf{R}_0^+)$ 和截止时间 $\tau \geq 0$ 对应的 MSCG 路径

$$\pi = \begin{cases} C_{q0}(M_{q0}, \Theta_{q0}), t_{i1}, \mathfrak{L}(t_{i1}) \\ \Delta^{(1)} \in [\max\{0, l_{i1}^{q0}\}, \min_{j:t_j \in A(M_{q0})} \{u_j^{q0}\}] \\ C_{q1}(M_{q1}, \Theta_{q1}), t_{i2}, \mathfrak{L}(t_{i2}) \\ \Delta^{(2)} \in [\max\{0, l_{i2}^{q1}\}, \min_{j:t_j \in A(M_{q1})} \{u_j^{q1}\}] \\ \vdots \\ C_{q(k-1)}(M_{q(k-1)}, \Theta_{q(k-1)}), t_{ik}, \mathfrak{L}(t_{ik}) \\ \Delta^{(k)} \in [\max\{0, l_{ik}^{q(k-1)}\}, \min_{j:t_j \in A(M_{q(k-1)})} \{u_j^{q(k-1)}\}] \end{cases} \quad (5)$$

给定路径 π , 定义 $o_{bs}(\pi)$ 为其对应的序列, 式(5)中, $o_{bs}(\pi) = \mathfrak{L}(t_{i1}, t_{i2}, t_{i3}, \dots, t_{ik})$ 。

定理 2 给定路径式(5)起始于根节点 C_{q0} 结束于 C_{qk} , 符合时间序列集 $\delta_0 = (\gamma_{i1}, \tau_1)(\gamma_{i2}, \tau_2) \cdots (\gamma_{ih}, \tau_h) \in (L \times \mathbf{R}_0^+)$ 满足约束

$$\begin{cases} \sum_{l=1}^k \Delta^{(l)} \leq \tau \\ \tau - \sum_{l=1}^k \Delta^{(l)} < \min r: t_r \in o_{bs}(C_{qk}) \{u_r^{qk}\} \\ \Delta^{(l)} \geq \max\{0, l_{il}^{q(l-1)}\} \quad l = 1, \dots, k \\ \Delta^{(l)} \leq \min j: t_j \in A(M_{q(l-1)}) \{u_j^{q(l-1)}\} \quad l = 1, \dots, k \\ \sum_{l=1}^q \Delta^{(l)} = \bar{\tau} \quad \forall t_{iq} \in \lg \delta_0 \end{cases} \quad (6)$$

式中: $o_{bs}(C_q)$ 为状态集合 C_q 的下边界; $\bar{\tau}$ 是可观测变迁 $\forall t_{iq} \in \lg \delta_0$ 最后触发时间。给定路径 π 不满足式(6), 则该路径不可能触发。

状态集合 (M_k, Θ_k) 是最后节点 C_{qk} 对应状态, 其中

$$\Theta_k = \{l_i^{qk} \leq \theta_i \leq u_i^{qk} : t_i \in A(M_k)\} \quad (7)$$

则 $(M_k, \Theta_k) \in S(\delta_0, \tau)$ 满足式(6)。且

$$\Theta_k' = \{\bar{l}_j \leq \theta_j \leq \bar{u}_j : t_j \in A(M_k)\} \quad (8)$$

$$\begin{cases} \bar{l}_j = \max\{0, l_j^{qk} - (\tau - \sum_{l=1}^k \Delta^{(l)})\} \\ \bar{u}_j = \max\{0, u_j^{qk} - (\tau - \sum_{l=1}^k \Delta^{(l)})\} \end{cases} \quad (9)$$

算法 2 基于 MSCG 的状态估计与诊断算法。

输入 TPN 系统及对应 MSCG 图, TLS 集合 $\delta_0 = (\gamma_{i1}, \tau_1) \cdots (\gamma_{ih}, \tau_h)$, 时间 τ 。

输出 故障诊断结果 $\Gamma(\delta_0, \tau, T_f^i)$

Step 1 初始化: $\delta_0 = \varepsilon, S(\delta_0, 0) = \emptyset$

Step 2 所有满足 $o_{bs}(\pi) = \varepsilon$ 路径放在集合 $\hat{\Pi}$ 。

Step 3 所有 $\pi \in \hat{\Pi}$ 且 $\tau = 0$ 满足式(6)的路径放在集合 Π 。

Step 4 for 所有 $\pi \in \Pi$ 路径 do

$S(\varepsilon, 0) = S(\varepsilon, 0) \cup \{(M, \Theta)\}$, (M, Θ) 是路径 π 最后节点。

Step 5 if 给定 $S(\varepsilon, 0), \tau > 0$ then

Step 6 $S(\varepsilon, \tau) = \emptyset$, 所有 $\pi \in \hat{\Pi}, \tau > 0$ 且满足式(6)的路径放在集合 Π_τ 。

Step 7 for 所有 $\pi \in \Pi_\tau$ do

$S(\varepsilon, \tau) = S(\varepsilon, \tau) \cup \{(M, \Theta')\}$, Θ' 是根据式(6)和式(8)、式(9)得出的最后节点时间约束。

Step 8 给定可观测变迁 $(e, \bar{\tau})$ 。

Step 9 $\delta_0' = \delta_0, \delta_0 = \delta_0'(e, \bar{\tau}), \Pi' = \Pi, S(\delta_0, \bar{\tau}) = \emptyset$ 。

Step 10 所有 $\pi \in \Pi', o_{bs}(\pi) = \lg \delta_0$ 路径放在集合 $\hat{\Pi}$ 。

Step 11 所有 $\pi \in \hat{\Pi}, \tau = \bar{\tau}$ 满足约束式(6)的路径 π 放在集合 Π 。

Step 12 for $\pi \in \Pi$ do

$$S(\delta_0, \bar{\tau}) = S(\delta_0, \bar{\tau}) \cup \{(M, \Theta)\}$$

Step 13 if 给定 $S(\varepsilon, 0), \tau > \bar{\tau}$ then

Step 14 令 $S(\delta_0, \tau) = \emptyset$, 所有 $\pi \in \hat{\Pi}, \tau > \bar{\tau}$ 且满足式(6)的路径放在集合 Π_τ 。

Step 15 for 所有 $\pi \in \Pi_\tau$ do

$$S(\delta_0, \tau) = S(\delta_0, \tau) \cup \{(M, \Theta')\}$$

Step 16 for $i = 1, \dots, r$ do

If $\forall \pi \in \Pi \wedge \forall t_f \in T_f^i, t_f \notin \pi$ then

$$\Gamma(\delta_0, \tau, T_f^i) = N$$

else if $\exists \pi \in \Pi, \pi' \in \Pi, (1) \exists t_f \in T_f^i, t_f \in \pi(2)$

$\forall t_f \in T_f^i, t_f \notin \pi'$ then

$$\Gamma(\delta_0, \tau, T_f^i) = U$$

else if $\forall \pi \in \Pi, \forall t_f \in T_f^i, t_f \in \pi$

$$\Gamma(\delta_0, \tau, T_f^i) = F$$

算法 2 寻找满足 TLS 集合 δ_0 及时间约束的变迁时间序列 σ 集合 Π , 判断系统故障状态 $\Gamma(\delta_0, \tau, T_f^i)$ 。

算法分析: Step 2 ~ Step 4 寻找截止时间 $\tau = 0$, 满足式(6)但没有可观测测量 $(\gamma, 0)$ 的路径 π , 包括只在根节点触发和 0 时刻完成所有变迁触发的路径 π 。后面

算法寻找 $\tau > 0$ 且满足式(6)的路径 π , 包括没有可观测量 $(\gamma, 0)$ 的路径 $\pi, \tau = \bar{\tau}$ 时可观测量 $(\gamma, \bar{\tau})$ 触发两种类型。集合 Π 存放所有满足时间约束的路径 π 。

Step 17 根据集合 Π 中所有路径 π 是否包含故障变迁 $t_f \in T_f^i$ 判断系统故障状态。任意 $\pi \in \Pi$, 都不存在 $t_f \in \pi$, 则系统没有故障; 存在 $\pi \in \Pi$, 满足 $t_f \in \pi$ 同时存在 $\pi' \in \Pi$ 满足 $t_f \notin \pi'$, 系统是否发生故障无法判断, 需配合其他故障诊断方法做进一步判断; 所有 $\pi \in \Pi$ 都满足 $t_f \in \pi$, 系统肯定发生故障。

2.3 复杂度分析

算法1 构建 MSCG 图, Step 3 ~ Step 8 根据变迁 $t_i \in A(M_q)$ 在标识 M_k 使能情况, 修正其对应时间约束, 建立新节点 C_q , 对应的计算复杂度为 $\mathcal{O}(|T|^2)$ 。由假设1可知, 给定截止时间 τ , 满足 δ_0 的路径个数有限, 定义 l_{\max} 为 MSCG 中满足 δ_0 的最长路径, 所有满足 δ_0 的 σ 数最多为 $|T|^{l_{\max}}$, 所以算法1的计算复杂度为 $\mathcal{O}(|T|^{l_{\max}})$ 。

算法2 寻找满足 TLS 集合 δ_0 的路径 π , 最多为 $|T|^{l_{\max}}$ 。式(6)判断每条路径 π 是否可触发, 对应的复杂度为 $\mathcal{O}(l_{\max} |T|)$, 综上, 算法2的计算复杂度为 $\mathcal{O}(l_{\max} |T|^{l_{\max}})$ 。

3 实例分析与验证

气体减压阀是气路系统的关键部分, 根据上下游气压差决定开启与关闭^[12-13], 减压阀容易发生故障导致气路失效^[14-15]。以 SAST-5000 卫星平台推进系统气路部分为例验证本文所提算法。

3.1 气路系统模型构建

本文研究双组元统一推进系统气路充气过程的故障诊断, 建立气路系统 Petri 网模型(如图1所示), 变迁 t_4 和 t_6 是减压阀故障导致的故障变迁。由于零部件本身差异及气路下游对上游的影响^[16], 零部件工作开启时间会存在一定差异, 根据设计规格及大量实验测试得出各工作部件触发时间, 如表1所示。

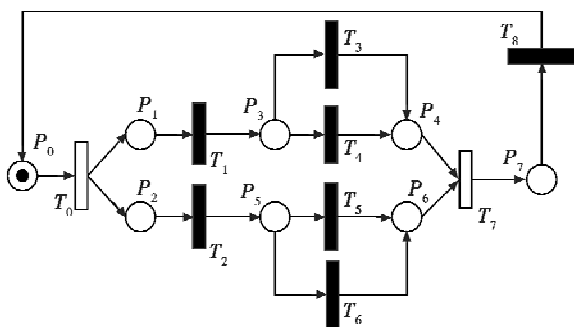


图1 气路系统 Petri 网模型

Fig.1 The Petri net model of the gas path system

图1以气路系统充气过程中关键节点为库所, 关

键动作作为变迁建立 Petri 网模型, 模拟气路系统充气过程, 各库所、变迁含义如表2、表3所示。

双组元挤压推进系统气路充气过程: 高压气瓶阀门打开, 气体从高压气瓶到达减压阀使其两端产生气压差并不断增加至设计规格, 减压阀打开, 气路压强保持恒定到达单向阀, 单向阀功能是气体只能从单一方向通过否则阀门关闭, 气体经过单向阀进入储箱引起储箱压强变化, 挤压储箱输出推进剂。

表1 气路系统各部件触发时间

Table 1 The triggering time of the devices in gas path system

部 件	触发时间/(10 ⁻¹ s)
气路阀门打开	0
1 支路减压阀工作	3.5 ~ 5
1 支路单向阀工作	2 ~ 4
1 支路单向阀工作(减压阀故障)	4 ~ 12
2 支路减压阀工作	3 ~ 4.5
2 支路单向阀工作	2 ~ 4.5
2 支路单向阀工作(减压阀故障)	4.5 ~ 12
两储箱都检测到气压变化	4 ~ 5
输出推进剂	2 ~ 3.5

表2 Petri 网模型中各库所物理含义

Table 2 The implication of each place in Petri net model

库所	库所含义
P_0	气路阀门准备就绪
P_1	氮气到达1 减压阀前
P_2	氮气到达2 减压阀前
P_3	氮气到达1 单向阀前
P_4	氮气通过1 单向阀
P_5	氮气到达2 单向阀前
P_6	氮气通过2 单向阀
P_7	储箱气压增加

表3 Petri 网模型中各变迁物理含义及可观测性

Table 3 The implication and observability of each transition in Petri net model

库所	库所含义	可观测性
T_0	气路阀门打开	可观
T_1	1 减压阀打开	不可观
T_2	2 减压阀打开	不可观
T_3	1 单向阀打开	不可观
T_4	1 单向阀打开(1 管路泄漏)	不可观
T_5	2 单向阀打开	不可观
T_6	2 单向阀打开(2 管路泄漏)	不可观
T_7	检测到两个储箱入口气压变化	可观
T_8	输出推进剂	不可观

3.2 气路系统故障诊断

3.2.1 建立气路系统 MSCG 图

构建 MSCG 如图2所示, 每个节点由状态集合 $S(\delta_0, \tau)$ 组成, 包括标识 M 及对应时间约束 Θ , 所有可

能路径为 $t_0 t_1 t_2 t_3 t_5 t_7$, $t_0 t_1 t_2 t_3 t_5 t_7$, $t_0 t_1 t_2 t_3 t_5 t_7$, $t_0 t_1 t_3 t_2 t_5 t_7$, $t_0 t_2 t_5 t_1 t_3 t_7$, $t_0 t_1 t_2 t_4 t_5 t_7$, $t_0 t_1 t_2 t_5 t_4 t_7$ 等。

图 2 是变迁 t_1 先于 t_2 触发对应的 MSCG 图, 每个节点对应可达标识集合 $M \in R_i(N_d, M_0)$ 和时间约束 Θ 。初始节点 C_0 对应标识 M_0 和时间约束 Θ_0 , 可观测变迁 t_0 触发使能; 变迁 t_0 在 C_0 触发得到节点 C_1 , 对应标识 $M_1 = [0 1 1 0 0 0 0 0]$ 不可观测变迁 t_1 和 t_2 触发使能 $Q(t_1) = [3.5, 5]$, $Q(t_2) = [3, 4.5]$; 变迁 t_1 在 C_1 触发得

到节点 C_2 , 对应标识 $M_2 = [0 0 1 1 0 0 0 0]$ 为保证 t_2 触发必须满足 $\Delta_1 \leq \min\{u_1, u_2\}$, 修正 t_2 的时间约束为 $Q(t_2) = [3 - \Delta_1, 4.5 - \Delta_1]$ 使能变迁为 t_2, t_3, t_4 ; 变迁 t_4 在节点 C_2 触发得到节点 C_3 , 对应标识 $M_3 = [0 0 1 0 1 0 0 0]$ 为保证 t_2 触发必须满足 $\Delta_4 \leq \min\{u_4, u_2 - \Delta_1\}$, 修正 t_2 的时间约束为 $Q(t_2) = [3 - \Delta_1 - \Delta_4, 4.5 - \Delta_1 - \Delta_4]$ 使能变迁为 t_2 , 变迁 t_4 触发则 t_3 不能触发, 不需考虑 t_3 时间约束。同理构建节点 $C_4 \sim C_{11}$, 如图 2 所示。

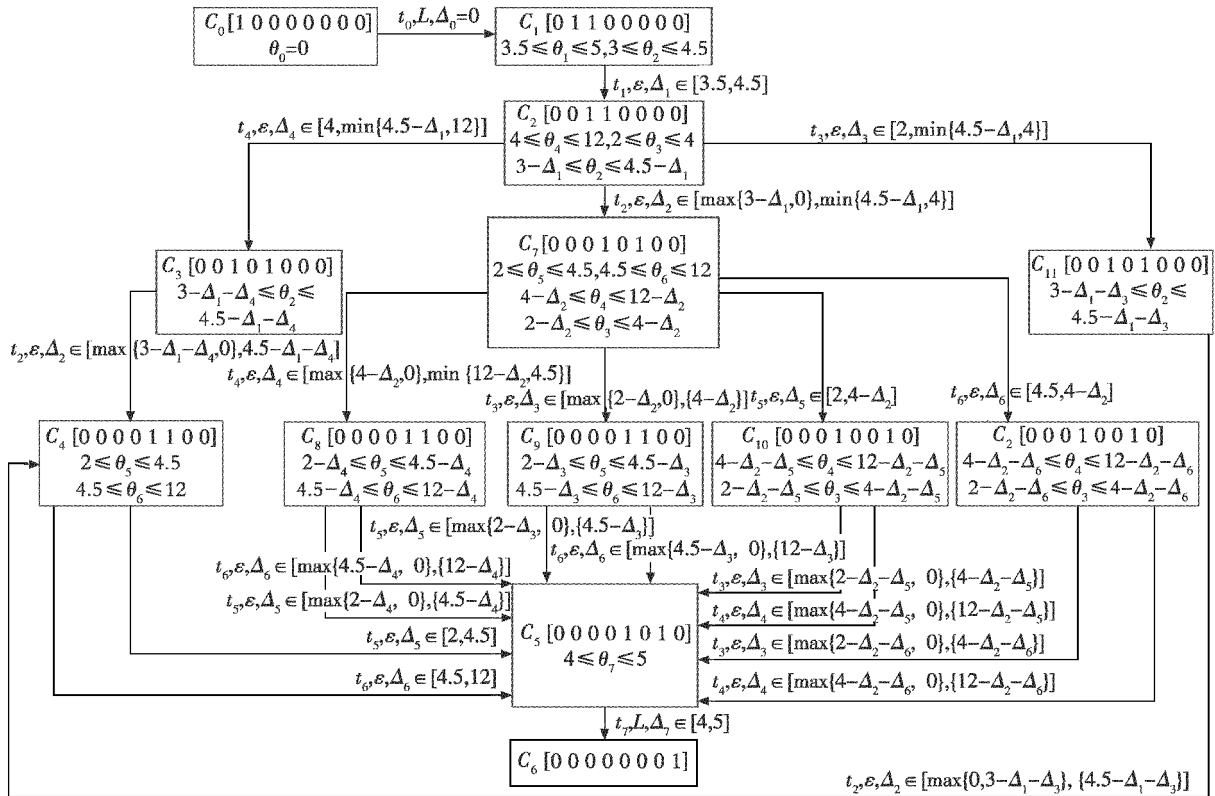


图 2 气路系统 MSCG 图

Fig. 2 The MSCG of gas path system

3.2.2 基于 MSCG 图气路系统故障诊断结果

本文 Petri 网模型中管路泄漏会导致下游单向阀打开时间变长, 表现出故障属性, 对应的变迁分别是 t_4 和 t_6 。

表 4 为根据地面面试车试验数据及本文提出的算法进行故障诊断得出的结果。

由表 4 可知, 第一次试验中满足时间约束的 σ 共 4 条, 系统故障发生的置信度为 0, 本次试验肯定没发生故障, 同步距离 $s_d(t_1, t_2)$ 为 1 即本次试验两路减压阀同步性很好, 系统工作在理想状态。第二次试验中,

可观测序列 t_0, t_7 分别在 0 s 和 11.9×10^{-1} s 发生变迁满足 $\bar{\tau} \leq \tau$ 。由算法 2 计算所有满足时间约束的 TTS 集合 σ 共 14 条, 其中, 不包含故障变迁的 σ 为 5 条, 包含故障变迁 t_4 的 σ 为 6 条, 包含故障变迁 t_6 的 σ 为 5 条, 系统故障发生的置信度为 0.643, 同步距离为 2, 本次试验两路减压阀工作同步性较差, 系统工作在非理想状态, 可能发生故障。第三次试验中满足时间约束的 σ 共 8 条, 系统故障发生的置信度为 1, 本次试验肯定发生故障。

表4 气路系统故障诊断结果

Table 4 The fault diagnosis of gas path system

可观序列 $\delta_0/(10^{-1}s)$	截止时间 $\tau/(10^{-1}s)$	无故障变迁 $lg \sigma$	含故障变迁 $t_4 lg \sigma$	含故障变迁 $t_6 lg \sigma$	置信度 F_s	同步距离 $s_d(t_1, t_2)$	诊断结果 $\Gamma(\delta_0, \tau, T_f^i)$	实际状态
$\{(t_0, 0)$ $(t_7, 10.2)\}$	15.1	$\{t_0 t_1 t_2 t_3 t_5 t_7\}$	ϕ	ϕ	0	1	N	无故障
		$\{t_0 t_1 t_2 t_3 t_4 t_7\}$	ϕ	ϕ				
		$\{t_0 t_2 t_1 t_3 t_5 t_7\}$	ϕ	ϕ				
		$\{t_0 t_2 t_1 t_3 t_4 t_7\}$	ϕ	ϕ				
$(t_0, 0)$ $(t_7, 11.9)$	15.8	$\{t_0 t_1 t_2 t_3 t_5 t_7\}$	$\{t_0 t_1 t_2 t_4 t_5 t_7\}$	$\{t_0 t_2 t_1 t_6 t_3 t_7\}$	0.643	2	U	可能发生 故障
		$\{t_0 t_1 t_2 t_3 t_4 t_7\}$	$\{t_0 t_1 t_2 t_5 t_4 t_7\}$	$\{t_0 t_2 t_1 t_3 t_6 t_7\}$				
		$\{t_0 t_2 t_1 t_3 t_5 t_7\}$	$\{t_0 t_2 t_1 t_4 t_5 t_7\}$	$\{t_0 t_2 t_1 t_6 t_3 t_7\}$				
		$\{t_0 t_2 t_1 t_3 t_4 t_7\}$	$\{t_0 t_2 t_1 t_5 t_4 t_7\}$	$\{t_0 t_2 t_1 t_6 t_4 t_7\}$				
		$\{t_0 t_2 t_5 t_1 t_3 t_7\}$	$\{t_0 t_2 t_1 t_6 t_4 t_7\}$	$\{t_0 t_2 t_1 t_4 t_6 t_7\}$				
		ϕ	$\{t_0 t_2 t_1 t_4 t_6 t_7\}$	ϕ				
$(t_0, 0)$ $(t_7, 14.1)$	15.4	ϕ	$\{t_0 t_1 t_2 t_5 t_4 t_7\}$	$\{t_0 t_1 t_2 t_3 t_6 t_7\}$	1	2	F	故障
		ϕ	$\{t_0 t_2 t_1 t_5 t_4 t_7\}$	$\{t_0 t_2 t_1 t_3 t_6 t_7\}$				
		ϕ	$\{t_0 t_2 t_5 t_1 t_4 t_7\}$	$\{t_0 t_1 t_2 t_4 t_6 t_7\}$				
		ϕ	$\{t_0 t_1 t_2 t_4 t_6 t_7\}$	$\{t_0 t_2 t_1 t_6 t_4 t_7\}$				
		ϕ	$\{t_0 t_2 t_1 t_6 t_4 t_7\}$	$\{t_0 t_2 t_1 t_4 t_6 t_7\}$				
		ϕ	$\{t_0 t_2 t_1 t_4 t_6 t_7\}$	ϕ				

3.3 算法比较

表5所示为文献[17]与本文算法的性能比较。

表5 文献[17]与本文算法诊断性能比较

Table 5 Diagnostic performance comparison between algorithm in [17] and the proposed algorithm

算法	传感器最少个数	计算复杂度
文献[17]	4	5.27×10^8
本文算法	2	3.87×10^8

文献[17]算法诊断本系统需构建可诊断子网,至少需安置4处传感器,其计算复杂度为 5.27×10^8 ;本文算法在气路阀门和储箱入口安置2处传感器便可进行故障诊断,降低了传感器可靠性对故障诊断的影响,构建MSCG图的计算复杂度为 4.30×10^7 ,在MSCG中寻找满足时间约束的路径 π 和判断系统是否发生故障计算复杂度为 3.44×10^8 ,因此使用本文算法诊断系统的计算复杂度为 3.87×10^8 。

4 结论

1) 针对当前故障诊断算法对传感器布置要求高,本文基于状态类图(SCG)故障诊断方法,引入时间约束信息,提出一种含不可观变迁时间Petri网的故障诊断算法。构建模型的修正状态类图(MSCG)并根据变迁触发序列修改时间约束信息,在线计算机只需根据序列状态集合 $S(\delta_0, \tau)$ 和算法2求解所有满足时间约束序列并判断是否含故障变迁,确定系统是否发生故障。

2) 建立双组元推进气路系统故障诊断模型并通过仿真实验验证了本文算法的有效性,通过与其他方法的比较证明其可行性。

3) 在今后研究工作中需进一步研究算法可诊断

性及随机时间Petri网故障诊断问题。

参考文献

[1] KRISTIANSEN R, NICKLASSON P J. Spacecraft formation flying: a review and new results on state feedback control [J]. Acta Astronautica, 2009, 65(11/12): 1537-1552.

[2] YANG H, JIANG B, COCQUEMPOT V, et al. Spacecraft formation stabilization and fault tolerance: a state-varying switched system approach [J]. Systems & Control Letters, 2013, 62(9): 715-722.

[3] HWANG I, KIM S, KIM Y, et al. A survey of fault detection, isolation, and reconfiguration methods [J]. IEEE Transactions on Control Systems Technology, 2010, 18(3): 636-653.

[4] 李勇, 曹东. 基于解析模型的飞控系统执行机构的故障诊断 [J]. 电光与控制, 2016, 23(10): 104-107, 111.

[5] 蔡宗平, 汤正平, 王跃钢, 等. 控制系统故障诊断浅析 [J]. 电光与控制, 2007, 14(4): 19-22, 26.

[6] LEFEBVRE D. On-line fault diagnosis with partially observed Petri nets [J]. IEEE Transactions on Automatic Control, 2013, 59(7): 1919-1924.

[7] CABASINO M P, GIUA A, SEATZU C. Diagnosability of discrete event systems using labeled Petri nets [J]. IEEE Transactions on Automation Science & Engineering, 2014, 11(1): 144-153.

[8] DECLERCK P, BONHOMME P. State estimation of timed labeled Petri nets with unobservable transitions [J]. IEEE Transactions on Automation Science & Engineering,

- 2014, 11(1):103-110.
- [9] BERNARDI S, CAMPOS J, MERSEGUER J. Timing-failure risk assessment of UML design using time Petri net bound techniques [J]. *IEEE Transactions on Industrial Informatics*, 2011, 7(1):90-104.
- [10] CABASINO M P, LAFORTUNE S, SEATZU C. Optimal sensor selection for ensuring diagnosability in labeled Petri nets[J]. *Automatica*, 2013, 49(8):2373-2383.
- [11] LIME D, ROUX O H. Model checking of time Petri nets using the state class timed automaton[J]. *Discrete Event Dynamic Systems*, 2006, 16(2):179-205.
- [12] 刘君,袁化成,郭荣伟. 内并联式 TBCC 进气道模态转换过程流动特性分析 [J]. *宇航学报*, 2016, 37(4):461-469.
- [13] DARBY R. The dynamic response of pressure relief valves in vapor or gas service[J]. *Journal of Loss Prevention in the Process Industries*, 2013, 26(6):1262-1268.
- [14] 鲁峰,黄金泉,吕怡秋,等. 基于非线性自适应滤波的发动机气路部件健康诊断方法[J]. *航空学报*, 2013, 34(11):2529-2538.
- [15] ZAFER N, LUECKE G R. Stability of gas pressure regulators [J]. *Applied Mathematical Modeling*, 2008, 32(1):61-82.
- [16] 徐志鹏,王宣银,罗语溪. 滑阀先导式高压气动减压阀结冰特性[J]. *航空学报*, 2009, 30(5):819-824.
- [17] 叶丹丹,罗继亮. 部分可观 Petri 网结构信息在故障诊断中的应用[J]. *控制理论与应用*, 2015, 32(3):366-373.
-
- (上接第 52 页)
- [4] KUBE C R, ZHANG H. The use of perceptual cues in multi-robot box-pushing[C]//*Proceedings of IEEE International Conference on Robotics and Automation*, 1996:2085-2090.
- [5] CASBEER D W, KINGSTON D B, BEARD R W, et al. Cooperative forest fire surveillance using a team of small unmanned air vehicles[J]. *International Journal of Systems Sciences*, 2006, 37(6):351-360.
- [6] BREAD R W, MCLAIN T W, GOODRICH M A, et al. Coordinated target assignment and intercept for unmanned air vehicles[J]. *IEEE Transactions on Robotics and Automation*, 2002, 18(6):911-922.
- [7] 吴青坡,周绍磊,尹高扬,等. 多无人机协同区域覆盖搜索算法的改进[J]. *电光与控制*, 2016, 23(1):80-84.
- [8] BAYEZIT I, FIDAN B. Distributed cohesive motion control of flight vehicle formations[J]. *IEEE Transactions on Industrial Electronics*, 2013, 60(12):5763-5772.
- [9] BELTA C, KUMAR V. Abstraction and control for groups of robots[J]. *IEEE Transactions on Robotics and Automation*, 2004, 20(5):865-875.
- [10] LAWTON J R T, BEARD R W. A decentralized approach to formation maneuvers[J]. *IEEE Transactions on Robotics and Automation*, 2003, 19(6):933-941.
- [11] MASTELLONE S, STIPANOVIC D, GRAUNKE C R, et al. Formation control and collision avoidance for multi-agent non-holonomic systems;theory and experiments[J]. *International Journal of Robotics Research*, 2008, 27(1):107-126.
- [12] REN W. Consensus strategies for cooperative control of vehicle formations[J]. *IET Control Theory & Applications*, 2007, 1(2):505-512.
- [13] 邱华鑫,段海滨,范彦铭. 基于鸽群行为机制的多无人机自主编队[J]. *控制理论与应用*, 2015, 32(10):1298-1304.
- [14] DONG X W, YU B C, SHI Z Y, et al. Time-varying formation control for unmanned aerial vehicles;theories and applications[J]. *IEEE Transactions on Control System Technology*, 2015, 23(1):340-348.
- [15] DONG X W, ZHOU Y, REN Z, et al. Time-varying formation control for unmanned aerial vehicles with switching interaction topologies[J]. *Control Engineering Practice*, 2016(46):26-36.
- [16] 刘伟,周绍磊,祁亚辉,等. 有向切换通信拓扑下多无人机分布式编队控制[J]. *控制理论与应用*, 2015, 32(10):1422-1427.
- [17] CARPENTER J R. Decentralized control of satellite formations[J]. *International Journal of Robust and Nonlinear Control*, 2002, 12(2/3):141-161.
- [18] REN W. Second-order consensus algorithm with extensions to switching topologies and reference models [C]//*Proceedings of the American Control Conference*, New York: IEEE, 2007:1431-1436.
- [19] REN W. On consensus algorithms for double-integrator dynamics[J]. *IEEE Transactions on Automatic Control*, 2008, 53(6):1503-1509.
- [20] REN W. Multi-vehicle consensus with a time-varying reference state [J]. *System and Control Letters*, 2007, 56(7/8):474-483.