文章编号：1001 - 2486(2002)04 - 0086 - 05

HPN 基于网结构的冲突关系*

金 光

（国防科技大学人文与管理学院，湖南 长沙 410073）

摘 要：混合 Petri 网是为了解决复杂动态系统可靠性安全性分析而提出的一种 Petri 网扩展模型。定义混合 Petri 网模型的基于结构的冲突关系，有助于深入理解混合 Petri 网模型的语义，对其在动态系统可靠性安全性建模与分析以及模型分析求解中的应用也具有重要意义。

关键词：Petri 网；冲突

中图分类号：TP391.9 **文献标识码**：A

Structural Conflicts in HPN

JIN Guang

(College of Humanities and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Hybrid Petri Net is one of the extended types of Petri Nets, which is originally prompted to solve the problems of reliability and safety of the complex dynamic system. Definition of structural conflicts in Hybrid Petri Net helps to go deep into the Hybrid Petri Net's semantics. Defining structural conflicts are also very necessary and important when they are applied in analysis of dynamic system reliability and safety.

Key words: Petri Net; conflict

现代系统的可靠性安全性分析对模型建立与求解方法都提出了新的要求。由于旧的传统的可靠性安全性分析方法本质上是针对系统的某个瞬时或稳态行为，当应用于具有复杂的动态行为和相关性的的现代系统，如通信网、计算机容错系统时，一般会导致比较大的误差。Petri 网（Petri Net——PN）是目前分析动态系统的一种广泛研究和应用的模型，已经建立了坚实的理论基础，并针对具体问题提出了多种扩展模型。文献［5］针对动态系统可靠性建模与分析提出混合 Petri 网模型（Hybrid Petri Net——HPN），是一种混合系统建模语言，已经在计算机系统可靠性分析、带反馈控制的系统的安全性分析中得到初步应用。为了分析系统可靠性安全性 HPN 模型，如进行可达树（图）构造和不变量计算等定性分析以及基于 Markov 过程或计算机仿真的定量分析，需要认真研究 HPN 的行为特别是冲突关系。这关系到能否为 HPN 提供分析解决实际问题的有效方法，而不是仅仅作为一种系统描述语言。本文定义了 HPN 的基于网结构的冲突关系，它们是文献［2］的概念在 HPN 模型上的推广。但是由于 HPN 是一种非线性模型，所以本文的结论具有更深刻的涵义。

1 HPN 模型

为了描述清楚，需要代数中项目（TERM）的概念，一个与其有关的介绍见文献［1］。定义类型集合 R 至少包含自然数集和实数集，算子集合（至少能够描述所有简单函数。下面的讨论都是基于此多类型符号 $\Sigma = (R, \Omega)$ 上进行的。定义 HPN 是八元组

$$HPN = (P, T, S, C, A, H, \Pi, M_0)$$

其中：

P：位置集合；

T：转移集合；

S：非空有限的变量集合；

* 收稿日期：2002 - 04 - 30
作者简介：金光（1973 - ），男，讲师，博士。

$C: P \to 2^V$ 为位置的类型映射，$\forall p \in P$，$C(p)$ 称为位置 p 的描述；

$A \subseteq \cup (\{p\} \times C(p) \times T \cup T \times \{p\} \times C(p) \times TERM(C(p))$ 为权重映射集；

$H \subseteq \cup \{p\} \times C(p) \times T \times TERM(C(p))$ 为禁止映射集；

$\prod: T \to \mathscr{R}$ 为转移优先级函数；

$M_0 \in D(PLACE)$ 为初始标识，这里 $PLACE = \{(p, v) \mid p \in P, v \in C(p)\}$，$D(PLACE)$ 表示 $\{(p, v)\}$ 的所有允许取值的集合，简记为 D；$\overline{D}$ 表示 D 的补集。

冲突是 PN 及其扩展模型的重要行为，又称有效冲突（effective conflict – EC）[2~4]。在经典 PN 中，冲突指两个转移都有发生权，但只有一个能点火的关系。在没有禁止弧和优先级的 PN 中，冲突关系是可交换的。将冲突的概念推广至带禁止弧和优先级的 PN 后，由于转移的授权和使能是两个不同的概念，所以冲突关系不满足自反性、交换性和传递性。冲突的充分性是依赖于初始标识的，所以基于等价类的不依赖于可达树的冲突判定机制，能够将有效冲突限制在更小的范围内，对建模和分析都有益。

在讨论 HPN 的基于网结构的冲突机制前，我们需要权重映射和禁止映射的单调性假设：如果在标识 M_1 下转移 t 有发生权，标识 M_2 满足：转移 t 的输入位置变量的值不小于 M_1 下的值，禁止位置变量的值不大于 M_1 下的值，则在标识 M_2 下 t 也有发生权。从占用或使用资源的角度看这一假设是合理的。单调性假设包含了恒等映射和常数，所以 HPN 模型是非线性的[5]。为了描述更复杂的行为，可以通过将一般函数分解为单调函数（这种分解总是存在的），并定义等价的模型来进行分析。另外，本文的讨论都假设没有冲撞出现，否则认为模型的语义错误。

2 基于网结构的冲突关系

在本节的讨论中，t 表示转移，p 表示位置，v 表示变量。π_i、π_t 表示转移 t_i、t 的优先级，即 $\pi_i = \prod(t_i)$，$\pi_t = \prod(t)$。若 $h = (p, v, t, f) \in H$，则记 $f = H(p, t)[v]$；若 $a = (p, v, t, f) \in A$，则记 $f = A(p, t)[v]$；若 $a = (t, p, v, f) \in A$，则记 $f = A(t, p)[v]$。

定义转移 t 的向前转移点火函数 $C^+(t)$ 为转移 t 点火后所有位置上变量值的增加，其对应于 $j \equiv (p, v) \in PLACE$ 的分量为 $\max\{A(t, p)[v] - A(p, t)[v], 0\} \equiv c_j^+(t)$；定义转移 t 的向后转移点火函数 $C(t)$ 为转移 t 点火后所有位置上变量值的减少，即其对应于 $j \equiv (p, v) \in PLACE$ 的分量为 $\max\{A(p, t)[v] - A(t, p)[v], 0\} \equiv c_j^-(t)$。$A(t)$、$A^+(t)$ 和 $A^H(t)$ 分别表示由 $A(p, t)[\cdot]$、$A(t, p)[\cdot]$ 和 $H(p, t)[\cdot]$ 按同样方式构成的向量函数。再定义如下两个集合：

位置 p 对转移 t 的禁止标识集 $K(p, t)$：若 $\forall v \in C(p)$，都有 $H(p, t)[v] \equiv +\infty$，则 $K(p, t) = \varnothing$，并称 (p, t) 不是禁止弧；否则 $K(p, t) = \{M \in D: \forall v \in C(p), H(p, t)[v](M) \geqslant M(v)\}$，并称 (p, t) 是禁止弧。

位置 p 对转移 t 的允许标识集 $L(p, t)$：若 $\forall v \in C(p)$，都有 $A(p, t)[v] \equiv 0$，则 $L(p, t) = D$，并称 (p, t) 不是弧；否则 $L(p, t) = \{M \in D: \forall v \in X(p), M(v) \geqslant A(p, t)[v](M)\}$，并称 (p, t) 是弧。为叙述方便，亦称 (t, p) 是弧。

下面约定“$\cdot(p, t)[v]$”中出现的 p、v 满足关系 $\forall v \in C(p)$。对一般 HPN 来说，转移可能有任意小的点火重数，我们排除这种情况发生的可能性，以便保证以下讨论的“合理性”。不失一般性，我们假设在任何标识下任何使能转移的点火重数不小于 1。

2.1 不冲突的必要条件

定义 1　两个转移 t_l 与 t_m 是有效互斥的（effectively mutually exclusive – EME），记作 t_l EME t_m，当且仅当在任何可达标识 $M \in [M_0 >$ 下 t_l 与 t_m 都不会同时使能。

显然，t_l EME $t_m \Rightarrow t_l EC t_m$。EME 关系对于带禁止弧和优先级的 PN 模型是特定的，是一种非自反和可交换关系，因为 t_l 与 t_m 可能同时有发生权但不同时使能。为了确定 EMC 关系，需要点火序列的全部知识，当系统规模较大或状态数较多时，构造可达树是费时、费力甚至不可行的。所以，如果能找

到与之等价的一些关系，或者，使该关系成立的一些必要条件则将是有益的。特别地，有时这些关系是 EME 的充分必要条件。

首先，根据 HPN 的定义，具有不同优先级的两个转移必定是具有 EME 关系的。

定义 2 称转移 t_l 与 t_m 是优先级互斥的，记作 $t_l \amalg ME\ t_m$，如果它们同时具有发生权的必要条件是另外一个比二者具有更高优先级的转移 t_k 有发生权。描述为：

$t_l \amalg ME\ t_m$ *iff* $\exists t_k : \pi_k > \pi_l \wedge \pi_k > \pi_m \wedge \forall p \in P :$

$(D(p,t_k) \subseteq D(p,t_l) \cup D(p,t_m)) \wedge (H(p,t_k) = \varnothing \vee H(p,t_k) \supseteq H(p,t_l) \cap H(p,t_m))$

定义 3 称转移 t_l 与 t_m 是禁止互斥的，记作 $t_l\ HME\ t_m$，是指存在位置 p 属于转移 t_l（或 t_m）的输入集，同时又属于 t_m（或 t_l）的禁止集，并且对应的弧满足：若一个有发生权，则另一个没有，或者相反。描述为：

$$t_l\ HME\ t_m \ iff\ \exists p \in P : D(p, t_l) \supseteq H(p, t_m) \neq \varnothing \vee D(p, t_m) \supseteq H(p, t_l) \neq \varnothing$$

定义 4 称转移 t_l 与 t_m 是标识互斥的，记作 $t_l\ MME\ t_m$，是指在标识守恒的约束下，两个转移不可能在任何标识下同时具有发生权。对于单调增系统，描述为：

$t_l\ MME\ t_m$ *iff* $\exists$ 守恒函数为 H 的不变量（变量的子集）$\widetilde{V} \subset V$，$H(\widetilde{V}) = C$，使得

$$H(V_m) > C$$

比如线性不变量 $y = \sum_{j=1}^{|V|} y_j v_j$，$\sum_{v_j \in p} y_j \max\{\min_D\{A(p, t_l)[v_j]\}, \min_D\{A(p, t_m)[v_j]\}\} > \tau y(M_0)$所约束的不冲突关系是最容易识别和应用的一种关系。

定义 5 称转移 t_l 与 t_m 是结构互斥的（structural mutually exclusive – SME），记作 $t_l\ SME\ t_m$，当且仅当 $t_l \amalg ME\ t_m \vee t_l\ HME\ t_m \vee t_l\ MME\ t_m$。

命题 1 如果 t_l 与 t_m 具有不同的优先级，或者 $t_l\ SME\ t_m$，则必有 $t_l\ EME\ t_m$。

证明：如果 t_l 与 t_m 具有不同的优先级，则根据 HPN 的行为的定义[5]，t_l 与 t_m 肯定不会同时使能。如果 $t_l \amalg ME\ t_m$，则 t_l 与 t_m 永远不可能同时授权，从而不会同时使用。如果 $t_l\ HME\ t_m$，则其中一个转移的授权意味着另一个转移的被禁止授权，所以 t_l 与 t_m 不可能同时使能。如果 $t_l\ MME\ t_m$，并且假设两个转移都被授权，则应有 $H(\widetilde{V}) > C$，但根据不变量的定义，又有 $H(\widetilde{V}) = C$，4 矛盾。综上所述，如果命题条件成立，则 t_l 与 t_m 不会同时授权，从而不会同时使能，即 $t_l\ EME\ t_m$。证毕。

命题 1 表明，四种关系对于 EME 来说是充分的，或等价的，它们是转移 t_l 与 t_m 没有冲突的必要条件，可以避免分析转移序列。其不足之处是无法保证所识别的 EME 关系肯定也是 SME 关系。关于何种情况下 EME 也是 SME 的，则还没有一般可操作的的结果。但是对一类特殊结构的模型如树形经典 Petri 网，可以保证 SME⇔EME[5]。

3.2 冲突的必要条件

转移冲突的一个前提条件是点火的转移（通过某个点火序列）耗费了其他转移的资源，使得其他转移不再具有发生权或使能。所以可以基于网的“连接关系”预测两个转移发生冲突的“可能”，即得到一些基于网结构的冲突的必要条件。

首先，如果转移 t_l 点火或者减少 t_m 的输入位置变量的值，或者增加 t_m 的禁止位置变量的值，则 t_l 与 t_m 是可能发生冲突的，此即结构冲突（structural conflict – SC）的概念，它是非自反、非传递的二元关系。但是对于 HPN 来说，还有一个特殊的问题，即一个转移的点火对另一个转移的输入和禁止位置变量的影响是微不足道的，从而对另一个转移没有实质上的影响。但是考虑到实际问题的特点，特别是竞争资源问题，排除这种可能也是合理的。

定义 6 称转移 t_l 与 t_m 是结构互斥的，记作 $t_l SC t_m$，当且仅当

$$A^-(t_m) \cdot C^-(t_l) > 0 \vee A^H(t_m) \cdot C^+(t_l) > 0$$

如果转移 t_l 点火后，或者增加 t_m 的输入位置的描述变量的值，或者减少 t_m 的禁止位置的描述变

量的值，则可能会因 t_l 的点火使得先前没有发生权的转移 t_m 拥有发生权，于是得到 SC 的对偶概念——偶然连接（casual connection – CC），定义如下。

定义 7 称转移 t_l 与 t_m 是偶然连结的，记作 $t_l CC t_m$，当且仅当

$$A^-(t_m)\cdot C^+(t_l) > 0 \vee A^H(t_m)\cdot C^-(t_l) > 0$$

如果将 t_l 点火定义为对系统状态的变换 θ_l，则在单调假设不成立的情况下，可以将 SC 关系理解为 $(D(p, t_m) \setminus (\theta_l(D(p, t_m)))) \cup (\theta_l(H^c(p, t_m)) \cap H(p, t_m)) \neq \emptyset$。而 CC 关系理解为 $(\theta_l(D(p, t_m)) \cap D^c(p, t_m)) \cup (H(p, t_m) \setminus (\theta_l(H(p, t_m)))) \neq \emptyset$。对单调系统而言，$t_l CC t_m \Rightarrow \neg\, t_l SC t_m$，但在单调假设不成立的情况下，可能即有 $t_l CC t_m$，也有 $t_l SC t_m$，所以讨论 SC 和 CC 仅对单调系统是有实际意义的。

在具有优先级的 PN 模型中，由于优先级关系的存在，可能存在一种“条件偶然连接”关系。如图 1，t_1 和 t_2 具有相同的优先级，t_3 具有比二者更高的优先级。转移 t_2 和 t_3 满足 SC 关系，当 t_1 点火后，t_3 必定立即点火。所以如果 t_2 不是在 t_1 之前点火，则它将不再有点火的机会。也就是说，在 t_1 和 t_2 之间进行的选择实际上已经决定了 t_2 是否能点火。条件偶然连接（conditional casual connection – CCC）关系建立在 CC 概念基础上，它描述了 t_m 使能的条件下，t_l 点火的影响，即 t_l 点火后导致对 t_m 和 t_k 的公共输入位置变量的值的增加以及对 t_m 和 t_k 的公共禁止位置变量的值的减小，从而可能影响它们的授权或使能情况。

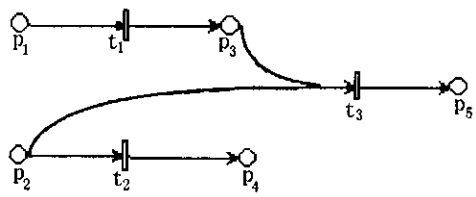

图 1 条件偶然连接

Fig. 1 Linking of conditional occasion

定义 8 t_l 与 t_k 是 t_m – CCC 的，指

$$t_l CCC\ t_m\ iff \pi_l \geqslant \pi \wedge \neg\,(t_l SME t_m \vee t_k\ SME\ t_m) \wedge \Big(\sum_{v_j \in V} c_j^+(t_l)\cdot \max\{A(p,t_k)[v_j] - A(p,t_m)[v_j], 0\} + \sum_{v_j \in V} c_j^-(t_l)\cdot \max\{I(p,t_m)[v_j] - I(p,t_k)[v_j], 0\} > 0\Big)$$

据此定义偶然连接集合（casual connected set – CCS）为

$$CCS_{\pi,t_m}(t_k) = \{t_l : \pi_l = \pi \wedge t_l CCC_{\pi,t_m} CCC^{*}_{\pi+1,t_m} t_k\}$$

其中符号“$*$”表示二元关系的传递和反射闭包，关于 t_k 的 CCS 包括了所有不改变 t_m 的使能条件的与 t_k 有关的偶然连接。于是可以定义间接结构冲突（indirect structural conflict – ISC）关系为

$$t_l\ ISC\ t_m\ iff \exists\, t_k : \pi_k > \pi_m \wedge t_k SC t_m \wedge t_l \in CCS_{\pi_m,t_m}(t_k)$$

ISC 表达了转移 t_l 的点火通过一个具有更高优先级的点火序列使 t_m 不使能的一种必要条件。根据定义，得到命题 2 如下。

命题 2 设在标识 M 下 t_l 与 t_m 使能，但 t_l 点火后 t_m 不再使能，则 $t_l SC t_m \vee t_l ISC t_m$。

证明：容易知道，t_l 点火后 t_m 不再使能的原因无外乎 t_l 点火导致 t_m 不再具有授权，或者有授权但不再使能，并经长度为 $n > 1$ 的变迁序列发生后 t_m 失去授权。而前者可以认为是对应于变迁序列长度为 0 的情况。根据定义 6，t_l 点火导致 t_m 不再具有授权的原因是由于 $t_l SC t_m$。而 t_l 点火导致 t_m 不再使能，并由于另外一个转移点火使 t_m 失去授权，便对应于长度为 $n = 1$ 的点火序列的影响，而此情形便对应于定义 8，即存在 t_k 使得 t_l 与 t_k 是 t_m – CCC 的，并且 t_k 点火导致 t_l 不再具有授权。对于长度大于 1 的点火序列，同理。综合起来便对应于 $t_l ISC t_m$。证毕。

需要注意的是，命题中 M 未必是可达标识，所以可能出现这样的情况：给定初始标识 M_0，对任何 M_0 的可达标识 M，在 M 下 t_l 与 t_m 同时使能并且能够同时点火。所以 SC 与 ISC 仅仅是冲突的必要条件。并且，由于这两个关系不是可逆的，所以 $t_l SC t_m \vee t_l ISC t_m$ 条件下，如果 t_m 首先点火，可能不会影响 t_l 的使能条件。

3 基于网结构的冲突关系应用

利用基于网结构的冲突和不冲突描述，不仅有助于缩小冲突检查的范围，而且基于此可以定义对建模具有重要意义的对称的结构冲突关系（symmetric structural conflict – SSC）：

$$t_l SSC t_m \ iff \neg \ (t_l \ SME \ t_m \vee \pi_m \neq \pi_l) \ \wedge t_l SC t_m \vee t_l ISC t_m \vee t_m \ SC \ t_l \vee t_m \ ISC \ t_l)$$

SSC 的传递和反射闭包 SSC^* 是一个等价关系，可以用来将转移划分为冲突类，于是定义关于转移 t_l 的扩展的冲突集合（Extended conflict Set – ECS）为

$$ESC\ (t_l) \ = \ \{_m : t_l \ SSC^* \ t_m\}$$

在一般的 PN 中，与同时使能的转移关联的不确定性导致转移点火顺序对模型的演化有重要影响的。事实上，真正的解冲突可能依赖于互不冲突的转移的点火序列，此即所谓“混惑”[2,3]。为了利用 ECS，我们需要假定模型中不包含混惑，否则认为该模型有语义错误。基于 ESC 的解冲突算法首先定义转移的（可能是依赖于标识的）权函数（又称点火频率函数）$\Lambda : T \rightarrow \square^+$。对任何 $t \in T$，$\Lambda\ (t)$ 表示当 t 与其它有相同优先级的转移冲突时，选取 t 作为点火转移的可能性的权重。对线性模型，转移的点火的方式不会改变模型的行为，并且由于 ECS 之间的独立性，从不同 ECS 中选出的转移的并发与从候选转移中以某种方式或任选一转移点火的后果是相同的，所以可以根据模型执行的方便选择适当的点火方式。设当前标识为 M，使能转移集合为 $\Gamma = \sum_i \Gamma \cap ECS_i$。在 $\Gamma \cap ECSi$ 中依概率

$$P\ (t_l) \ = \Lambda\ (t_l) \ / \ \sum_{t \in \Gamma \cap ECS_i} \Lambda\ (T)$$

选取转移 t_l 点火，由所有选取出来的转移构成当前标识下一个可并发点火转移集合。

转移使能函数（transition enable function—TEF[3~5]）是一种可以使模型更加紧凑的建模元素，通过要求 R 包含布尔类型，Ω 包含有关布尔操作的算子，可以定义 TEF。为了刻划资源调度，可以定义位置的资源调度函数 $Q \in \bigcup_{p \in P} \{p\} \times C\ (p) \times TERM\ (C\ (p))$[5]。在这两种情况下冲突的行为更加复杂，需要进一步研究。

利用 ECS，我们能够“显式”描述实际系统的资源竞争及其对应的冲突消解过程，对于描述系统可靠性模型中的多种失效模式部件、备件策略、维修方案等都具有重要意义。基于人为定义的网结构冲突并利用这里的解冲突方式能够表达分支事件的概念，HPN 能够模拟一般离散事件系统[4,5]。限于篇幅，我们不在此详细讨论，有兴趣者可以参考文献［5］。

4 小结

在文献［5］的基础上，进一步讨论了基于网结构的冲突关系，不仅提供了一种解冲突机制，而且提供了一种模型确认的途径，使得在模型开发时可以检查是否存在错误，而这对于动态系统可靠性安全性建模与分析都是非常重要的。

参考文献：

[1] High – Level Petri Nets – Concepts，Definitions and Graphical Notation［R］. Committee Draft ISO/IEC 15909，October 2，1997，Version 3.4.

[2] Giovanni Chiola，Macro Ajmone Marsan，Gianfranco Balbo，Gianni Conte. Generalized Stochastic Petri Nets：A Definition at the Net Level and Its Implications［J］. IEEE Trans. Soft. Eng.，1993，19（2）：89 – 107.

[3] Tadao Murata. Petri Nets：Properties，Analysis and Applications［J］，Proc. IEEE，1989，77（4）：541 – 580.

[4] Gianfranco Ciardo，Reinhard German，Christoph Lindemann. A Characterization of the Stochastic Process Underlying a Stochastic Petri Net，IEEE Trans. Soft. Eng.，1994，20（7）：506 – 515.

[5] 金光. 动态系统可靠性建模与高可靠度系统仿真［D］. 国防科技大学博士学位论文，2000.