广西科学院学报
Journal of Guangxi Academy of Sciences

2007,23(4):254~257
Vol. 23,No. 4 November 2007

一种嵌入式系统扩展流关系 Petri 网及应用*

An Extended Flow Petri Net for Embedded Systems and Application

张 辉,董荣胜,高 西
ZHANG Hui,DONG Rong-sheng,GAO Xi

(桂林电子科技大学计算机系,广西桂林 541004)
(Department of Computer Science,Guilin University of Electronic Technology, Guilin,Guangxi, 541004,China)

摘要:为了将数据流和控制流在同一个模型中明确标识,将经典 Petri 网的 4 元组结构扩展为 7 元组,定义一种新的嵌入式系统扩展流关系 Petri 网表示方法,应用该表示法对火车控制系统进行建模,并将该模转换成等价的时间自动机模型,用 UPPAAL 进行形式化验证。验证结果表明火车控制系统具有可达性和安全性,说明建立的模型是合理有效的。

关键词:Petri 网 时间自动机 CTL UPPAAL
中图法分类号:TP301.2 **文献标识码**:A **文章编号**:1002-7378(2007)04-0254-04

Abstract:In order to identify the control flow and data flow in one model, the classical four-tuple structure of Petri net is modified to a seven tuple in this paper. A new extended flow Petri net representation suited to embedded systems is presented. The representation is used to model for railway control system, and the model is translated into timed automata in order to verify the system by UPPAAL. Experimental results show the attainable ability and safety of the railway control system and demonstrate the validity of the model.

Key words:Petri net,timed automaton,computation tree logic,UPPAAL

随着嵌入式系统复杂度的不断增加,仅仅利用传统的模拟和仿真技术对其进行验证变得越来越困难。形式化验证方法逐渐成为一种可供选择的实用方法而受到广泛关注[1~5]。对嵌入式系统进行形式化验证时,首先必须建立系统的形式化模型,以便对系统的性能进行分析。Petri 网具有良好的模型描述特性和数学特性,能够提供一个集成的建模和分析环境,已经广泛的应用到嵌入式系统的建模与设计中。嵌入式系统的描述包括控制功能和数据操作两部分,其主要功能是在逻辑功能控制下进行数据交换[2]。基于这一思想,结合经典 Petri 网不能处理数据流的特点,Z. Peng[3]在 1994 年将扩展时间 Petri 网(ETPN)应用在 CAMAD 高级综合系统中。ETPN 包括控制部分和数据部分,控制部分是一种定时 Petri 网,数据部分被表示成一个有向图,有向图的节点用来描述对数据的操作和数据的存储。但是,由于 ETPN 的数据流和控制流分散在两个模型中,因此不能很好的连接。为了弥补这一缺陷,实现在同一模型中对数据域和控制域进行分析,出现了 PRES[4]、PRES+[5]和双变迁 Petri 网[2]模型。PRES 和 PRES+模型修改了托肯的定义,使托肯可以携带数据信息,而且,还可以用于不同层次的建模,支持层次化分解。双变迁 Petri 网扩充了数据变迁,将模型中的数据流和控制流分开进行标识,有利于进行嵌入式系统的行为分析。PRES 和 PRES+模型都没有将数据域和控制域明确分开,而是把数据流和控制流当作同一类数据流加以处理,不利于嵌入式系统的行为分析。双变迁 Petri 网对迁移及其对应的弧分别进行了扩充,使得基于这种扩展 Petri 网的表示法极为繁琐,不利于复杂嵌入式系统的建模与验

收稿日期:2007-08-13
作者简介:张 辉(1982-),男,硕士研究生,主要从事片上系统设计验证,形式化技术研究。
*广西研究生教育计划项目(2007105950812M17)资助。

证。为了将数据流和控制流在同一个模型中明确标识,同时考虑所建扩展 Petri 网模型的简洁性,本文将经典 Petri 网的 4 元组结构扩展为 7 元组。定义了嵌入式系统建模的一种新的扩展流关系 Petri 网。给出 EFPN 模型到时间自动机模型的转换过程,从而能够采用 UPPAAL 对属性进行验证。

1 扩展流关系 Petri 网

从基本定义、系统描述和动态行为规则三方面对 EFPN 进行定义。

1.1 基本定义

定义 1 扩展流关系 Petri 网结构可定义为七元组:$N=(P,T,I,O,C,G,M_0)$,其中,$P=\{p_1,p_2,\cdots,p_m\}$ 为非空有限位置集合;$T=\{t_1,t_2,\cdots,t_m\}$ 为非空有限迁移集合;$I\subseteq P\times T$ 为有限输入弧的集合,输入弧定义了位置和迁移之间的数据流关系;$O\subseteq T\times P$ 为有限输出弧的集合,输出弧定义了迁移和位置之间的数据流关系;$C\subseteq P\times T$ 为描述位置和迁移之间的控制流关系的集合;G 为迁移的控制函数,作用于控制流;M_0 是 Petri 网的初始标识。

位置集和迁移集是 Petri 网的基本成分,且 $P\cap Q=\varnothing$,流关系由它们构造所得。如图 1 所示,$P=\{p_a,p_b,p_c,p_d,p_e,p_f\}$,$T=\{t_1,t_2,t_3,t_4,t_5\}$。

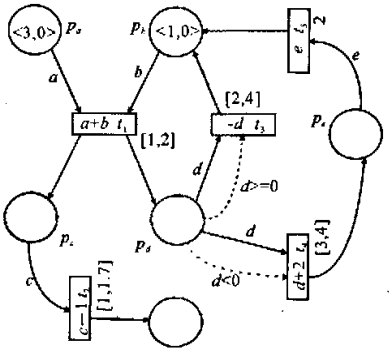


图 1 扩展 Petri 网模型

○:位置;□:迁移;⟶:数据流关系;⋯⋯→:控制流关系。

定义 2 托肯是一个有序二元组 $k=<v,r>$,其中,v 是托肯数值,且数值可为任意类型,如布尔型、整型或用户自定义类型;r 是托肯时间,用一个非负实数代表托肯的时间戳。集合 K 表示所给出系统中所有可能的托肯类型集合。

定义 3 标识 $M:P\to\{0,1\}$ 是用于标识 Petri 网位置中是否存在托肯的函数。

本文所提出的扩展 Petri 网 N 每个位置 p 最多只能有一个托肯。当位置 p 被标识时,$M(p)=1$;反之,$M(p)=0$。图 1 中,$M(p_a)=M(p_b)=1$,$M(p_c)=M(p_d)=M(p_e)=M(p_f)=0$。托肯 $k_a=<3,0>$ 是指位置 p_a 具有数值 3 并且时间戳为 0。

定义 4 类型函数 $\tau:P\to K$ 是一个联合位置和托肯类型的二元关系。$\tau(p)$ 表示位置 p 的托肯类型。

1.2 系统描述

定义 5 迁移的前集 ${}^\circ t=\{p\in P|(p,t)\in I,(p,t)\in C\}$ 为迁移 t 的输入位置的集合;迁移的后集 $t^\circ=\{p\in P|(t,p)\in O\}$ 为迁移 t 的输出位置的集合。

定义 6 对于任意迁移 t,存在一个与之相关的迁移函数 f。对任意迁移 $t\in T$,$\exists\ f:\tau(q_1)\times\tau(q_2)\times\cdots\times\tau(q_a)\to\tau(p)$,其中 ${}^\circ t=\{q_1,q_2,\cdots,q_a\}$ 且 $p=t^\circ$。

迁移函数标记在迁移的方框中。如图 1 中,迁移 t_4 的迁移函数 $f_4(d)=(d+2)$ 被标记在迁移方框中的左边。对任意迁移 t,所有输出位置有同样的托肯类型。若 $p,q\in t^\circ$,则 $\tau(p)=\tau(q)$。对任意迁移 t,存在非负实数类型的最小迁移时延 d^- 和最大迁移时延 d^+。d^- 和 d^+ 分别代表迁移函数执行时间的下界和上界。对于 $\forall\ t\in T,\exists\ d^-,d^+\in R^+$,其中 $d^+\geqslant d^-$。若 $d^+=d^-$,则直接把 d^+ 或者 d^- 标记在迁移方框的下方。从图 1 可以看出,迁移 t_2 的最小迁移时延 d_1^- 为 1 个时间单元,最大迁移时延 d_1^+ 为 1.7 个时间单元。而对于迁移 t_5,$d_5^-=d_5^+$,所以直接标记 2。

定义 7 迁移 t 的控制函数 G_t 是当迁移 t 的所有输入位置拥有托肯时,为使迁移 t 使能而必须要满足的布尔条件集,作用于控制流。

迁移 t 的控制函数 $G:\tau(p_1)\times\tau(p_2)\times\cdots\times\tau(p_a)\to\{0,1\}$,其中 ${}^\circ t=\{p_1,p_2,\cdots p_a\}$。图 1 中,迁移 t_3 的控制函数 $G_{t3}=(d\geqslant 3)$,标记于控制流。

1.3 动态行为规则

定义 8 迁移 t 使能,当且仅当

(1)$G_t=1$;

(2)$\forall\ p\in{}^\circ t,M(p)=1$;

(3)$\forall\ q\in(t^\circ-{}^\circ t),M(q)=0$。

定义 9 每个使能迁移都有一个触发时间 et 用于表示多少时间后迁移能够引发。迁移的触发时间是这个迁移的所有输入位置的托肯时间中最大的一个,即 $et=\max(r_1,r_2,\cdots,r_a)$,其中 t 的前集 ${}^\circ t=\{p_1,p_2,\cdots,p_a\}$。

使能迁移的最早引发时间 t^- 和最晚引发时间

t^+ 是迁移引发时间的上、下界，其中，$t^- = et + d^-$，$t^+ = et + d^+$。使能迁移 t 的引发不能早于它的最早引发时间，也不迟于它的最晚引发时间，除非由于其它迁移的引发而导致这个迁移不使能。

使能迁移的引发将标识 M 改变为 M^+。迁移 t 的前集 $^\circ t = \{p_1, p_2, \cdots, p_a\}$，迁移引发后，将会发生如下事件：

(1) 属于迁移前集且不属于迁移后集的位置中的托肯被去掉，即

$$\forall\, p \in (^\circ t - t^\circ), M^+(p) = 0;$$

(2) 迁移后集中的每个位置将具有托肯，即

$$\forall\, q \in t^\circ, M^+(p) = 1;$$

(3) 迁移后集中的新托肯将有一个新的托肯值。新托肯值通过迁移函数计算得到，即

$$\forall\, q_i \in t^\circ, v_i = f(v_1, v_2, \cdots, v_a);$$

(4) 迁移后集中新托肯的托肯时间戳是迁移的引发时间，即

$$\forall\, q_i \in t^\circ, r_i = t^*, \text{其中 } t^* \in [t^-, t^+]。$$

2 应用

Petri 网自身的分析能力有一定的局限性，我们把 EFPN 模型转换成等价的 TA 模型[6,7]，并用 CTL[8]进行系统属性描述。

2.1 转换过程

以火车控制系统[9]为例来说明具体的转换过程。用扩展流关系 Petri 网分别对此系统的火车部分和控制器部分建模，得到简化的扩展 Petri 网模型，如图 2 所示。

把 EFPN 模型转换成相应的 TA 模型。具体的转换过程如下：

(1)扩展流关系 Petri 网模型的每个位置 P_i 将对应 TA 中的一个结点变量 l_i。若位置中存在托肯值 v_M，则定义其为初始结点变量。

(2)声明位置结点时钟约束函数 inv：$L \to \Psi(C)$，用于约束位置结点。此时钟约束函数对应于扩展流关系 Petri 网中的使能迁移引发时间。

(3)声明边的时钟约束函数，表示转换的约束条件，对结点间的转换做出必要的限制。与此对应，PN 中用虚线条表示的控制流关系对是否迁移也做出限制。

(4)声明边的 update 以改变系统的状态，包括更新时钟。在节点间进行转换时，应对边的 update 进行计算。

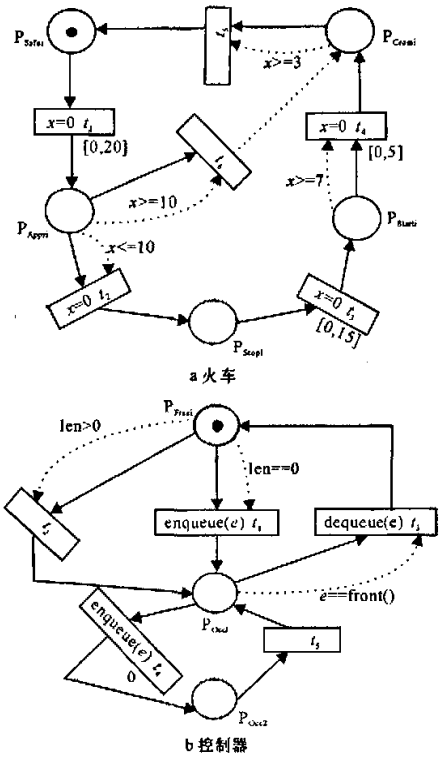


图 2 简化的扩展流关系 Petri 网模型

○：位置；□：迁移；→：数据流关系；⋯→：控制流关系。

(5)定义信道对进程进行同步。同步标签采用 exp? 或者 exp! 的形式标注时间自动机模型的边，其中 e 是信道的效果评测表达式。若两个进程被同步，则标注同步标签的两个边将同时触发。定义为紧急信道的同步在能够触发时必须立刻执行。

图 3 即为转换后的火车控制系统的时间自动机模型。

2.2 属性验证

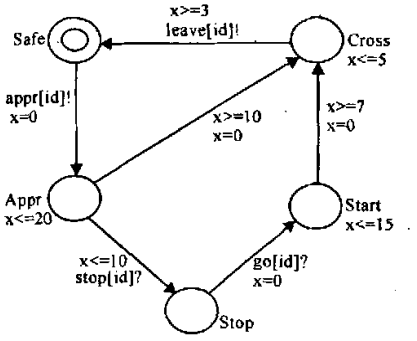
采用模型检验工具 UPPAAL[10]对火车控制系统进行属性验证。

2.2.1 验证系统是否具有可达性

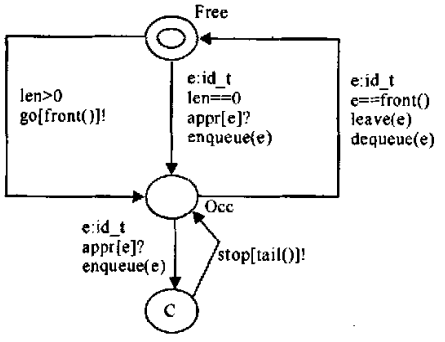
E<> Train(1).Cross and (forall(i:id_t)i! = 1 imply Train(i).Stop)。UPPAAL 验证器的验证结果为：satisfied。结果表明，该系统满足此属性，即在其余火车等待过桥时，第一辆火车可以过桥。类似可以验证其余火车的相似属性。因此，该系统具有可达性。

2.2.2 验证系统是否具有安全性

A[] forall (i : id_t) forall (j : id_t) Train(i).Cross && Train(j).Cross imply i == j。



a 火车



b 控制器

图 3 时间自动机模型

验证结果是 satisfied,说明在任何时刻,只会有一辆火车过桥。因此,该系统具有安全性。

3 结束语

本文通过对经典 Petri 网进行扩展,提出一种可以有效的对嵌入式系统进行建模的 EFPN 模型,并给出了将 EFPN 模型转换成对应的 TA 模型的转换过程,用模型检验工具 UPPAAL 对系统进行验证。验证结果表明所建模型是有效的。

参考文献:

[1] LUIS ALEJANDRO CORTES, PETRU ELES, ZEBO PENG. Verification of real-time embedded systems using petri net models and timed automata: 8th International Conference on Real-Time Computing Systems and Applications (RTCSA 2002), Tokyo, Japan, March [C]. Tokyo: [s. n.], 2002: 18-20, 191-199.

[2] VAREA M, HASHIMI B A. Dual transitions petri net based modeling technique for embedded systems specification: proceeding of the 4th Design, Automation and Test in Europe (DATE), Munich, Germany [C]. Munich: [s. n.], 2001: 566-571.

[3] PENG Z, KUCHCINSKI K. Automated transformation of algorithms into register-transfer level implementations[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 1994: 13(2): 150-166.

[4] CORT'ES L A, ELES P, PENG Z. A petri net based model for heterogeneous embedded systems[J]. IEEE NORCHIP Conference, 1999, 8-9: 248-255.

[5] LUIS ALEJANDRO CORTES, PETRU ELES, ZEBO PENG. Verification of embedded systems using a petri net based representation: 13th International Symposium on System Synthesis (ISSS 2000), Madrid, Spain, Sept [C]. Madrid: [s. n.], 2000: 20-22, 149-155.

[6] ALUR R, CORCOUETIS C, DILL D. Model checking in dense real-time[J]. Information and Computation, 1993, 104(1): 2-34.

[7] 钱俊彦,赵岭忠,古天龙. 一种基于时间自动机的时钟等价性优化方法[J]. 计算机工程,2005,9,31(18):71-73.

[8] CLARKE E, GRUMBERG O, PELED D. Model checking[M]. [S. l.]: MIT Press, 1999.

[9] WANG YI, PAUL PETTERSSON, MATS DANIELS. Automatic verification of real-time communicating systems by constraint solving: proceedings of the 7th International Conference on Formal Description Techniques, North-Holland [C]. Sweden: [s. n.], 1994: 223-238.

[10] GERD BEHRMANN, ALEXANDRE DAVID, KIM G LARSEN. Formal Methods for the Design of Computer [M]. Heidelberg: spring Berlin, 2004: 200-236.

(责任编辑:尹 闯 邓大玉)