时间自动机可达性分析中的状态空间约减技术综述*)

陈铭松　赵建华　李宣东　郑国梁

（南京大学计算机软件新技术国家重点实验室　南京大学计算机科学与技术系　南京 210093）

摘　要　时间自动机是检验实时系统建模的有效工具，其可达性分析可以检验系统是否可能达到某些特定的状态，其算法通常采用对符号状态的枚举来遍历其状态空间。因为引入了时钟变量，时间自动机的可达性分析算法会产生大量的中间状态，需要巨大的存储空间，往往超出了计算机能力的极限，导致分析和检验不能完成。这就是所谓的“状态空间爆炸”。研究人员设计了很多种优化技术来约减可达性分析所需的存储空间，以解决或者缓解这个问题。本文首先介绍了时间自动机及其可达性分析的基本概念，然后分类讨论了现有的空间约减优化技术并对此做出总结，最后提出了一些未来的研究方向。

关键词　实时系统，时间自动机，状态空间爆炸，可达性分析

A Study of Optimization Techniques about Reachability in Timed Automata

CHEN Ming-Song　ZHAO Jian-Hua　LI Xuan-Dong　ZHENG Guo-Liang

(National Laboratory of Novel Software Technology, Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract　Timed automaton is a useful modeling tool for real-time systems. To check whether a system can reach a specific state, the reachability analysis algorithms explore the state space of timed automata by enumeration of symbolic states. Since clocks are used in timed automata, the algorithms generate large number of temporary states during state space exploration, so it requires a huge amount of computer memory. When such requirement excesses the feasible limitation, the model checking algorithm fails to return a result. This is the so called 'state space explosion' problem. Many researchers contrive various optimization techniques to solve or mitigate this headache problem. This paper firstly presents the basic introduction of timed automata, then discusses some useful optimization techniques and gives a conclusion. Finally, some future directions are proposed.

Keywords　Real-time system, Timed automata, State space explosion, Reachability analysis

1　引言

实时系统在各领域有着广泛的应用，它一般被用在对时间要求非常高的装置上。实时系统的一个重要特点就是：如果在逻辑、时序或者可达性设计时出现偏差，将会引起严重的后果。随着实时硬件和软件系统的规模及功能迅速地增加，这类系统设计的复杂性和设计中包含微小错误的可能性也随之增加，这就给软件和硬件产品的可靠性带来了重大的挑战。所以，工业界期望通过形式化方法和相应工具，在产品设计的早期阶段帮助设计人员发现逻辑错误。

时间自动机理论[1,2]是对实时系统进行模型检验的一种有效的理论工具。Alur 和 Dill[1]在上世纪 90 年代提出的时间自动机理论为时间自动机的模型检验的发展提供了扎实的基础。许多人认识到用时间自动机为实时系统建模非常直观和方便，因而把这一理论应用到工业案例的模型检验中。有关理论发展、工具开发和技术改进的文章不断涌现，这些成果已经在工业界的设计开发过程中得到了很好的应用。基于时间自动机的实时系统模型检验工具被工业界开始接受，目前比较流行的检验工具有 UPPAAL[3]，Kronos[4]等。

时间自动机在思想上是稠密时间模型和 ω-自动机的结合，它可以为实时系统在时间上的行为建模，在建模时引入有限多个实值时钟来描述带有时间约束的状态转换。由于时钟取值可以是实数，时间自动机具有无穷状态空间，而模型检验要求系统的空间是有穷的。为了解决这个问题，研究人员利用等价概念、使用符号状态来使用有穷的状态，对系统建模。虽然空间是有穷的，但是时钟的引入，使得“状态空间爆炸”问题更加突出。目前，时间自动机的一个主要研究方向集中在如何利用相关的优化技术来约减状态空间。

实时系统的许多属性可以用系统状态的可达性来表示，在可达性分析过程中不可避免地会遇到状态空间爆炸的问题，所以本文主要从时间自动机的可达性空间约减优化技术方面进行了分析与探讨。本文第 2 部分介绍了时间自动机的理论概念以及可达性搜索的基本算法。第 3 部分按照静态与动态方法分别对几种目前已有的基于时钟约束的优化技术进行了讨论，讨论的侧重点没有放在数据结构上。有关用于表示符号状态的数据结构的技术请见 BDD[5]，CDD[6]，DBM[7]等。第 4 部分主要讨论了基于路径遍历的优化技术。最后本文对这几个优化算法进行总结并讨论今后的研究方向。

2　时间自动机与可达性分析的基本介绍

在这一部分我们主要讨论时间自动机的基本概念、时间自动机的具体与符号的语义，以及相应的可达性算法。

2.1　时间自动机

我们用 $G(C)$ 表示基于时钟集合 C 上的时间卫式的集

*)本课题研究得到国家自然科学基金(No. 60203009, No. 60233020, No. 60425204)、江苏省自然科学基金(BK2003408)和国家重点基础研究 973 计划(No. 2002CB312001)的资助。**陈铭松**　硕士生，主要研究方向为模型检验、软件测试；**赵建华**　副教授、硕导，主要研究方向为形式化方法、软件工程及程序设计语言；**李宣东**　教授、博导，主要研究方向为面向对象技术、形式化方法；**郑国梁**　教授、博导，主要研究方向为软件工程、软件开发环境及面向对象技术。

合。时间卫式是形如 $x\sim n(x\in C,n$ 是常数，$\sim\in\{\leqslant,<,>,\geqslant\})$的原子公式的合取。本文用 $g_1,g_2,g_3\cdots$来表示 $G(C)$中的元素。在文[1]中，Alur 和 Dill 给出了时间自动机及其操作语义的定义。

定义 1(时间自动机) 一个时间自动机可以表示为五元组(L,l^0,C,E,I)：

1)L 是一个有限的位置集合；

2)$l^0\in L$，是起始位置；

3)C 是有限的时钟变量集合；

4)$E\subseteq L\times G(C)\times 2^C\times L$ 是一个转换的集合；

5)I 给 L 中的每一个位置 l 分配了一个位置不变式 $I(l)$ $(I(l)\in G(C))$，位置不变式中的所有原子公式都形如 $x\leqslant(<)n$。

时间自动机可以看作是一个有穷自动机添加了时钟变量与时间卫式，其具体状态可以用二元组(l,v)表示，这里 l 表示时间自动机的一个位置，v 表示满足 l 位置不变式的时钟取值。给定一个时钟变量 x，$v(x)$表示在状态(l,v)上 x 的值。随着时间的流逝，所有的时钟变量值都会同步增加。假设(l_1,g,r,l_2)为时间自动机上的一个转换，当自动机的当前位置为 l_1，且时钟取值满足时间卫式 g，转化就可能发生。转换发生后，时间自动机的当前位置变为 l_2，集合 r 中的时钟变量的值被重置为 0，而其它时钟变量的值保持不变。

定义 2(时间自动机的操作语义) 具体状态的转化关系如下：

1)如果 $v+d$ 满足 l 的位置不变式，则$(l,v)\xrightarrow{d}(l,v+d)$，其中 $v+d$ 表示满足对所有的时钟变量 x，$(v+d)(x)=v(x)+d$ 的时钟变量取值；

2)如果 $e=(l_1,g,r,l_2)$，则$(l_1,v)\xrightarrow{e}(l_2,v')$，其中 v 满足 g 中的所有原子公式，且 $v'=r(v)$，其中 $r(v)$表示时钟变量取值满足：对于每一个时钟变量 c，如果 $c\in r$，则 $r(v)(c)=0$，否则 $r(v)(c)=v(c)$。

一个时间自动机网络是有穷多个时间自动机的平行组合。具体来说，由时间自动机 $A_1,A_2,\cdots,A_n$(其中 $A_i=(L_i,l_i^0,C_i,E_i,I_i)$)组成的时间自动机网络 $A_1\parallel A_2\cdots\parallel A_n$ 是个五元组(L,l^0,C,E,I)，其中 $L=L_1\times L_2\times\cdots\times L_n$，$l^0=l_1^0\times l_2^0\times\cdots\times l_n^0$，$C=C_1\cup C_2\cup\cdots\cup C_n$，$I(l)=\bigcap_{i=1}^{n}I_i(l_i)$；$E_i$ 由两种转换组成：一种是普通转换，是 E_i 中非同步转换的并集；另一种是同步转换，其具体状态形式为$((l_1\times l_2\times\cdots\times l_n),v)$。对于非同步的转化，如果$((l_1\times\cdots\times l_i\times\cdots\times l_n),v)\xrightarrow{g,r}((l_1\times\cdots\times l'_i\times\cdots\times l_n),v')$，必须满足 $v\models g$，$v'=r(v)$，且 $v'\models I_i(l'_i)\wedge\bigcap_{k\neq i}I_k(l_k)$；如果$((l_1\times\cdots\times l_n),v)\xrightarrow{d}((l_1\times\cdots\times l_n),v+d)$，$d\in R^+$，必须满足 $v\models\bigcap_k I_k(l_k)$，且 $v+d\models\bigcap_k I_k(l_k)$。对于同步转换，这里用 $a!$ 与 $a?$ 表示，如果$((l_1\times\cdots l_i\times\cdots\times l_j\times\cdots\times l_n),v)\xrightarrow[g_j,a?,r_j]{g_i,a!,r_i}((l_1\times\cdots l'_i\times\cdots\times l'_j\times\cdots\times l_n),v)$，需满足 $v\models g_i\wedge g_j$，$v'=(r_i\cup r_j)(v)$，且 $v'\models I_i(l_{i'})\wedge I_j(l_{j'})\wedge\bigcap_{k\neq i,j}I_k(l_k)$。

2.2 符号状态

因为时钟的定义域为非负实数 R^+，时间自动机的状态空间是无穷的，而模型检验的对象是有穷的系统，所以我们采用符号状态将无穷的状态空间转化为有穷的。在时序系统的验证技术中往往采用符号化技术，它利用布尔表达式来表示状态的集合。在表达式上的操作是状态转换的集合，这对压缩状态空间非常有效。时间自动机在验证的技术上采用了相似的技术，如 region 与 zone，它们是一些具体状态的集合。

设 C 为时钟集合，我们用 $B(C)$表示时钟集合 C 上的时间区域(time zone)的集合。每个时间区域是一组关于时钟变量的原子公式的合取式。时间区域的原子公式与时间卫式的原子公式不同，其原子公式都是形如 $x-y\sim n(x,y\in C\cup\{0\},\sim\in\{\leqslant,<\},n$ 为整数)的针对时钟变量的约束。显然，任意时钟集合 C，$G(C)\subseteq B(C)$。

设 D_1 与 D_2 是两个时间区域。如果 $D_2\Rightarrow D_1$，则称 D_1 包含 D_2，记为 $D_2\subseteq D_1$。如果 $D_2\subseteq D_1$ 且 $D_1\subseteq D_2$，则时间区域 D_1 与 D_2 等价。令 $d_1(x-y\sim_1 c_1)$、$d_2(y-z\sim_2 c_2)$为两个原子公式，这两个原子公式之间的连接 $x-z\sim_3 c_1+c_2$ 记为 $d_1\cdot d_2$，如果 $\sim_1$ 和 $\sim_2$ 均为$\leqslant$，则 $\sim_3$ 为$\leqslant$，否则 $\sim_3$ 为$<$。一个时间区域被称为是正则的，当且仅当对于任意两个它的原子公式 d_1、d_2，它必然有一个不弱于 $d_1\cdot d_2$ 的原子公式。

时间自动机中的符号状态定义为二元组(l,D)，其中 l 是符号状态的位置信息，D 是符号状态的时间区域，$D\in B(C)$。符号状态可以看作是相同位置满足某种时间约束的状态的集合$\{(l,v)\mid v$ 满足 D 中的所有原子公式$\}$。符号状态的后继 $SP_\delta(e,(l,D))$表示了具体状态的集合$\{(l',v')\mid\exists e,d,(l,v)$ 使得$(v\in D)\wedge(l,v)\xrightarrow{e}(l',v'')\xrightarrow{d}(l',v')\}$。转换 $e=(l,g,r,l')$，$SP_\delta(e,(l,D))$可以由$(l',(r(D\wedge g))\uparrow\wedge I(l'))$计算得到，其中，$I(l')$是位置 l' 的位置不变式，$r(D)$、$\uparrow$、$\wedge$ 都是针对于时间区域操作的运算符。有关这些运算符操作的具体细节请参考文[8]。实现时间区域存储以及相关语义操作的数据结构一般采用差分界限矩阵(DBM，Difference Bounds Matrix)。

2.3 时间自动机可达性分析的基本算法

对时间自动机来说，最有用的也是最常问的一个问题就是，给定一个或多个终止状态，是否可以从起始状态通过某个路径到达。可达性分析是可判定的，可达性问题一般刻画的是实时系统的安全属性(safety properties)，即系统能否避免到达某种危险状态。

时间自动机的可达性分析一般采用枚举符号状态的办法。分析算法从初始状态开始，不停地使用算子 SP_δ 来计算已经生成的符号状态的后继。这个过程一直到下面的两个条件之一成立才会终止：(1)已经不能生成新的符号状态；(2)算法生成了一个目标位置上的状态。

```
PASSED={}
WAITING={(l0,D0)};
repeat
从 WATING 中取一个符号状态(l,D)，取名为 S，WAITING=
WAITING-{S};
对于每条离开 l 的变换 e,
begin
  if SP δ(e,S)为空，then 尝试下一个变换；
  计算 S'=SP δ(e,S)，令 S'=(l',D')；
  if l'是指定的目标位置 l1，then 返回  成功；
  if 有一个符号状态 S''=(l',D'')在 WAITING ∪ PASSED 中且 D'
    ⊆D''，then 记录 S 到 S''的前趋势后继关系；
  else WAITING=WATING ∪ {S'}，记录 S 到 S'的前趋后继关系；
end
添加 S 到 PASSED;
until WAITING={}
返回  失败。
```

图 1 可达性分析的基本算法

图 1 中给出了基本的时间自动机可达性分析的算法。它的思想被广泛应用于不同的模型检验工具，具体请参见文[1,2,9]。算法给定了起始符号状态(l_0,D_0)，以及要求判定是否能够到达的位置 l_1。在状态空间的遍历过程中，所有的符号状态被分为两组 WATING 和 PASSED。WATING 中

保存了所有需要计算后继的符号状态，而 PASSED 中存放了所有后继已经被计算生成的符号状态。在分析开始时，PASSED 为空，而 WAITING 中只有起始符号状态。算法在执行过程中记录了相邻符号状态间的前驱后继关系。

3 可达性分析中针对时钟约束的空间约减技术

通过对可达性分析算法的理解，容易发现：如果在可达性分析向前搜索时能够在不影响结果的前提下扩张某些符号状态(弱化时钟约束，即弱化原子公式)的话，那么在后面生成的状态将会被包含在这些状态中，使得中间状态减少，状态空间以及搜索时间得以优化。

可达性空间方面针对时钟约束的优化算法主要分为以下 2 种：静态方法(static method)和动态方法(Dynamic method)。两者主要考虑的是如何利用状态之间时钟约束的依赖关系，减少中间状态的生成，有效地控制状态空间。不同的是，前者是通过在检验前分析模型中特定性质或者在检验中利用局部信息来弱化状态的时钟约束，指导状态的生成，约减可达性的空间。后者通过在模型检验过程中记录运行时的状态信息或者全局的状态信息，在系统执行过程中，边生成状态，边约减状态。目前有许多成功的基于时钟约束的优化技术。下面将按照这种分类方法讨论几种主要的优化技术。

3.1 静态约减技术

3.1.1 活跃时钟与等价时钟约减技术

时间自动机的空间状态爆炸是由于时钟的引入。验证时间自动机的复杂性与时钟个数以及时钟约束中的最大常数呈指数关系。所以，在实际的检验过程中，时钟的个数是时间自动机检验的最大障碍。

C. Daws 和 S. Yovine 提出了一种约减不活跃时钟与等价时钟的技术[10,11]。产生不活跃时钟与等价时钟的主要原因有两点：①实时系统的规约往往由高阶语言来描述，然后编译为相应的时间自动机。在同一时刻，有些时钟可能是无用的，即不活跃的，可以约减这些时钟。②复杂的系统往往是由一些只有少数时钟变量的子系统并行组成的，因为转换的同步关系，许多时钟经常被同时重置，这就使得这些时钟在某时间段上是相同的，并且递增的速度是一致的。此时，这些时钟只需要一个代表，可以约去其余的时钟。容易证明，约减后的自动机和约减前的自动机是互模拟(Bisimulation)的。

活跃时钟，直观上讲某个时钟在当前状态是活跃的指的是这个时钟将会影响到后继状态的生成。不活跃时钟指的是从当前状态出发的每条路径都不影响到后继状态的生成。不活跃时钟技术可以约减符号状态中与不活跃时钟相关的原子公式，扩张符号状态，约减状态空间。由于活跃时钟[10]针对的是单个自动机，文[11]中给出了所谓活跃性(Activity)的抽象方法，其思想与活跃时钟类似，不过针对的是时间自动机网络。

等价时钟，指的是两个时钟在所有的执行轨迹上的状态中，两者具有相同的值。也就是说，对于每个可达状态(s,v)，时钟 x,y 均满足 $v(x)=v(y)$。此时只需要其中的一个时钟作为代表，这样就约减了时钟的个数。

以上两种方法通过证明，保证了与约减前的系统在时间上是互模拟的，这就保证了可达性分析的正确性。两种技术都是在检验前通过对时间自动机的分析实现的，其优点在于花费的时间少，把不必要的时钟变量在检验开始时就剔除，使得验证需要的状存储态空间减小。

3.1.2 Convex Hull 抽象技术

抽象技术(Abstraction)[11]被公认为是一种有效解决“状态空间爆炸”的技术。在空间遍历的时候，模型检验使用抽象技术获得符号状态而不是具体状态，因为抽象状态包含的信息量要少于具体状态，但是又不损害系统的性质，也即不影响验证的结果。安全(safe)的抽象技术保证了，只要具体状态能够满足的性质，在安全抽象的符号状态也能获得这种性质。在时间自动机中，符号状态是一类性质相近的具体状态的集合，所以利用符号状态验证，将会提高时空效率。

在搜索过程中，将会在同一个位置 l 上有多个不同的符号状态，它们的时间区域 $D_1, D_2, \cdots, D_n$ 是不一样的。然而 $(l, \bigcup_{i=1}^{n} D_i)$ 通常不是符号状态，因为时钟区域的并通常是一个 non-convex 的集合。两个时间区域 $D1$ 和 $D2$ 的 convex hull D 被定义为满足 $D1 \subseteq D$ 且 $D2 \subseteq D$ 的最小时间区域。具体 DBM 操作为 $D_{i,j}=\max\{D1_{i,j}, D2_{i,j}\}$。图 2 中显示的是两种合并时间区域获得 convex hull 的情况。一般来说 convex hull 操作是并操作的超集，也就是说具体状态到达不了的状态，符号状态可以到达。

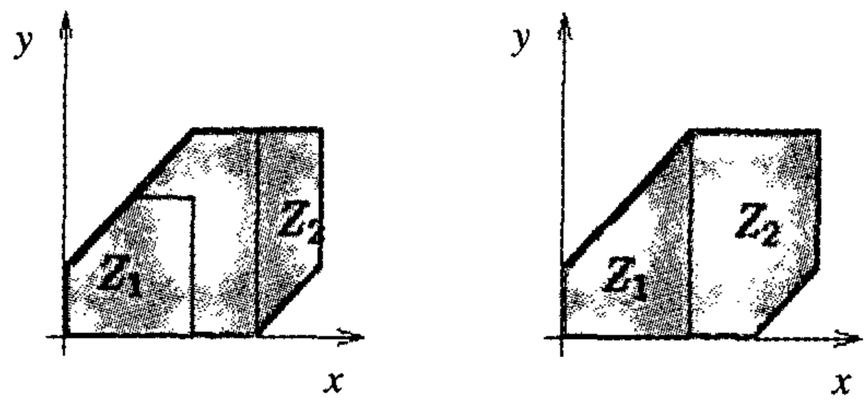

图 2 convex hull 的两个例子

Convex hull 抽象技术具有不完备性的特点，在符号状态空间能够到达的状态，在具体状态空间不一定能够到达。convex hull 一般用在诊断方面，使用抽象技术发现目标，然后利用模拟运行技术，通过具体状态来验证这个目标是否可达。如果可达，系统就满足某种性质。

Convex hull 作为一种抽象技术，减少了生成的状态个数，所以约减了状态空间。虽然 convex hull 的符号状态可能到达具体状态到达不了的状态，但是它在可达性的实际运用中非常有用。因为，如果一个状态在符号状态搜索空间中不可达，那么在具体状态空间中必然也是不可达的。如果在具体状态空间中可达，可以通过重新执行具体状态的方法来确认可达性。这种方法仍然可以提高系统的可信度。

3.1.3 针对时钟上下界的约减技术

时间自动机的具体状态是无穷的，但是为了验证，起初 Alur 与 Dill 提出了 region-graph[4] 的概念，利用等价的关系，将无穷化为有穷。但是，这样的方法往往使得验证过程中产生大量的状态。在实际的运用中，一般采用时间区域(time zone)的方法，它对时间的划分 region-graph 的粒度要粗，当然验证的效果要好。Gerd Behrmann 和 Patricia Bouyer 等人提出了通过区分时间自动机时钟的最大上界与下界，来获取对时间区域更加宽泛的表达形式，也即使得生成的时间区域比原先的时间区域要大，这种方法是活跃时钟约减技术的泛化形式。在文[12,13]中，通过互模拟，Gerd Behrmann 和 Patricia Bouyer 证明了对于时间自动机的可达性质，关于时钟的上下界的约减技术是合理与完备的(sound and complete)，并且这种验证优化技术是有穷且有效的。他们将技术应用于 UPPAAL 上，实验证明，它能够有效地提高验证速度，减少存储空间的使用，并且有着很好的可扩充性。

Gerd Behrmann 等人在文[12]中提出了静态卫式分析的技术，这种技术与自动机的位置信息是相关的，是基于位置的

有限时间区域的抽象。实验证明，它在某些情况下能够指数级地提高验证算法的效率。为了保证算法的效率，在可达性分析的过程中应该考虑时钟约束中的最大常量，对于那些状态相同但是时钟值超过最大常量的状态应该加以注意。如果对最大常量的值选得越小，那么抽象的粒度越高。到目前为止，获得时钟的最大常量必须通过对检验模型全局的分析。文[12]中针对特定状态相关卫式的最大常量，提出了一个基于位置的粗粒度的抽象。如图 3 所示，在全局分析中 10^6 是时钟 y 的最大常量，但是卫式 $y\geqslant 10^6$ 显然在 l_2 和 l_3 中是无关的，因为从这些位置到卫式 $y\geqslant 10^6$ 必须对 y 进行重置。因此，应该为 y 合理地在位置 l_2 和 l_3 上选择合适的最大常量 max2，max3 而不是 10^6。因为相关卫式 $y\geqslant 5$，所以 max2，max3$\geqslant$5，但是 5 不一定是 y 在 l_2 和 l_3 上的最大常量，$z=y+1$ 与 $z<8$ 的组合可以推导出 $y<7$，所以 max2，max3$\geqslant$7。事实上，$x:=z+3$ 和不变式 $x<14$ 与 l_2 和 l_3 相关，所以 max2，max3=10 是 y 在 l_2 和 l_3 的最小常数。文[12]中给出了有效地通过静态的全局分析识别位置相关的最大常量。同时，证明了对于位置可达性，这种抽象是正确的。同时，文[12]还将这种粗粒度的抽象扩充至时间自动机网络。实验证明效率有指数级的提高。

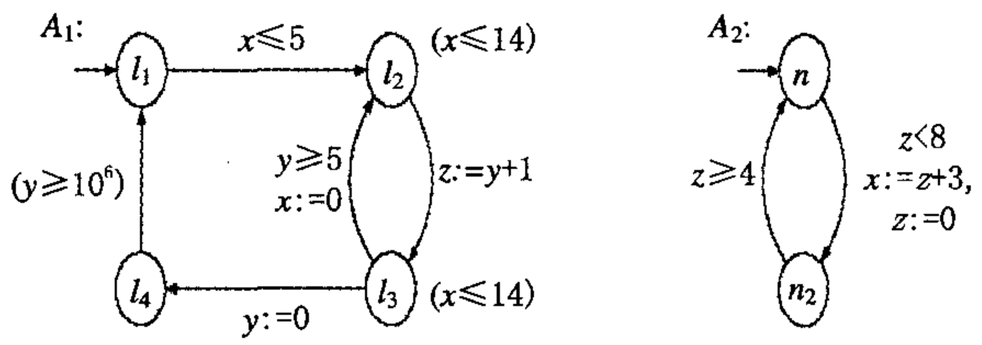

图 3　时间自动机网络 A1 ‖ A2

为了验证可达性，一般比较时钟的最大常量，采用基于时间区域的抽象。文[13]中提出了一个最大时钟上界与下界的方法，它将时钟 x 的最大上界记为 $U(x)$，最大下界记为 $L(x)$。区分上界与下界的思想如下：如果知道 x 的值在 2 与 4 之间，如果想检验约束 $x\leqslant 5$ 能否满足，唯一相关的信息就是 $x\geqslant 2$，而不是 $x\leqslant 4$。换句话说，如果想检验区间 $[c,d]$ 与 $[-\infty,5]$ 的交集为空，只需检验 $c>5$，d 的信息是无关的。这种思想使得抽象的粒度进一步扩大。文[13]同时证明了这种抽象方法在可达性上的合理性与完备性，并给出了一种基于 DBM 验证的数据结构与相兼容的操作。实验表明，这种抽象方法对于可达性的验证有较高的效率。

3.1.4　*无关原子公式以及通过静态分析寻找无关公式的技术*

前面的例子是在检验前针对时钟的约减与弱化，检验中对符号状态中的原子公式的操作也可以使得符号状态扩张。如果在符号状态中删除了某些原子公式而不影响验证的结果，这类原子公式就称为无关原子公式，文[14]中给出了无关原子公式的定义。

定义 3(无关原子公式)　时间自动机 A 有一个符号状态 (l,D)，d 是 D 中得一个原子公式。从 D 中删除原子公式，得到时间区域 D'，如果 (l,D') 能够到达的所有状态均为时间自动机的可达状态，那么 d 就是无关原子公式。

利用静态分析的方法寻找无关原子公式的基本思想是使用时钟重置与时钟测试的信息来识别无关原子公式。文[14]中定义了 Greater-test-free 时钟，直观地说就是在某个位置 l 上的时钟 x，每个离开 l 的转换的路径中都没有在重置 x 之前就测试 x 下界的转换。对于时间自动机的并行组合，因为一个时钟一般都是被本地转换重置与测试，所以获取有关重置与测试的信息的计算量和所需空间都很小。文[14]中同时给出证明，在符号状态 (l,D) 中，其中 D 是正则，如果时钟 x_0 在 l 上是 Greater-test-free 的话，D 中形如 $x_0-y\leqslant(<)c(y\in C\cup\{0\})$ 的原子公式都是无关的。

这种方法是不活跃时钟约减方法的改进形式。通过静态分析约减无关原子公式的方法除了能够发现不活跃时钟外，还能发现 Greater-test-free 或者 Less-test-free 时钟，所以消除得更彻底。

3.2　动态约减技术

动态约减技术通过在模型检验过程中记录运行时的状态信息或者全局的状态信息，在系统执行过程中，边生成状态，边约减状态。这一节主要讨论动态寻找无关原子公式的技术。

动态寻找并约减无关原子公式的基本思想如下。假设有符号状态 (l,D)，有 n 个转换 $e_1,e_2,\cdots,e_n$ 离开位置 l，而 (l_i,D_i) 是关于 e_i 的后继。如果它们满足：(1)如果 $SP_\delta(e_i)(l,D)\neq\emptyset$，$SP_\delta(e_i)(l,D)\subseteq(l_i,D_i)$；(2)如果 $SP_\delta(e_i)(l,D)=\emptyset$，$D_i=\emptyset$。如果从 D 中删除原子公式 d，得到符号状态 D' 之后满足条件 $SP_\delta(e_i)(l,D')\subseteq(l_i,D_i)$，那么 d 就是关于 e_i 可约减的。如果 d 对于所有的 $e_i(1\leqslant i\leqslant n)$ 都是可约减的，那么这个公式就是无关原子公式。被动态约减技术所消除的无关原子公式往往通过静态的方法不能找出，所以两者通常结合使用。

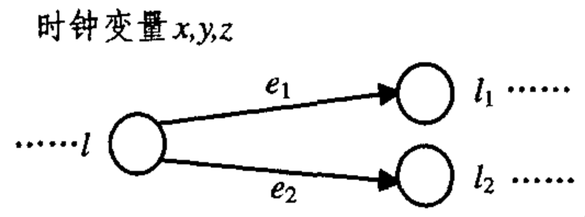

图 4　动态扩展符号状态的实例

图 4 中给出了一个在状态生成过程中动态扩展符号状态的例子。此图描述的是运行到某个阶段的时间自动机的一个局部片断，其基本数据如下：设 $e_1=(l,x<1,\emptyset,l_1)$，$e_2=(l,x>1,\{z\},l_2)$，假设模型检验中的某个时刻，在 PASSED 已经有了符号状态 $S_1=(l,x\geqslant 2\wedge y>1\wedge z>3)$、$S_2=(l,x\geqslant 2\wedge y>1\wedge z<2)$，符号状态 $S_3=(l_2,x\geqslant 2\wedge y>1)$ 在 WAITING 中。S_1 的 e_1 后继与 S_2 的 e_1 后继符号状态均为 $\emptyset$，S_1 的 e_2 后继符号状态与 S_2 的 e_2 后继符号状态均为 S_3 在 WAITING 中。由图 4 中的算法可知，S_1、S_2 中的原子公式 $x\geqslant 2$ 是关键公式，从而也是相关公式；而 $y>1$ 为无关公式，S_1 中的 $z>3$ 与 S_2 中的 $z<2$ 均为无关公式，可以删除。从 S_1、S_2 中删除了无关公式后得到的状态是相同的，所以可以合并两个状态并重新计算前后继关系。上面的做法虽然扩展了符号状态，但算法的验证结果不会改变。这种处理方法不仅消减了符号状态个数，降低了内存的需求，同时由于扩展了 PASSED 符号状态，算法将丢弃更多的状态而不去生成它们的后继，因此减少了花费在生成后继上的 CPU 时间，加快了可达性分析的速度。

易见文[14]中所述的静态约减无关原子公式是一种向前探索的过程，是在生成后继符号状态的时候约去当前符号状态的无关原子公式，使得当前符号状态以及后继符号状态扩张。而动态原子公式则相反，它利用搜索时的历史信息，回溯删除前驱状态中的无关原子公式。文[14]中给出了两者结合的优化算法，它是对图 1 算法的改进，基本思想如下：

1)每当一个符号状态产生的时候，使用静态约减技术删除当前符号状态的原子公式；

2)当算法计算出了一个符号状态 (l,D) 的所有后继状态时，通过动态的方法寻找并删除 D 中的无关原子公式。

往往动态约减无关公式能够进一步发现静态方法不能发现的原子公式，更好地扩张符号状态。一般来说，静态方法与动态方法结合起来使用，可以在时间与空间的效率上有更大的提高。

4 针对搜索路径的偏序约减技术

仔细研究图 1 中的可达性分析算法，可以发现：如果在可达性分析向前搜索时，能够在不影响结果的前提下选择搜索路径，或者放弃对某些路径搜索的话，将会使得中间状态减少，状态空间以及搜索时间得以优化。目前针对路径遍历的空间约减技术主要集中在偏序约减技术。

偏序约减[15]是在时序模型检验中首先提出来的，并且在非时间系统（例如并发系统）的模型检验中获得了巨大的成功。其基本思想就是在检验过程中，对于独立的转换，有许多不同的转换的交叉组合。因为独立转换的发生次序对结果没有影响，所以对于许多交叉组合，只要有代表性地选择一条路径就可以了，这就是所谓的“All from one, one for all”[16]。因为状态空间爆炸往往是一种组合式的爆炸，所以这种技术能够大大减少无目的的搜索。

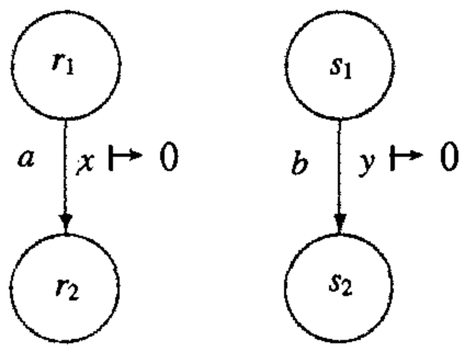

图 5 一个偏序约减的实例

虽然偏序技术在有穷的异步系统中有着广泛的应用，但是这种技术在时间自动机中的应用迟迟没有动静，其主要原因在于，不同时间自动机中的时钟的增长速率是一致的，这就导致转化发生的次序不同，得到结果就极有可能不同。图 5 中是两个自动机的网络，其初始状态是$\langle(r_1, s_1), x=y\rangle$，如果先发生转换 a，得到状态$\langle(r_2, s_1), x\leqslant y\rangle$。然后发生转换 b，得到最终状态$\langle(r_2, s_2), y\leqslant x\rangle$，如果先发生转换 b，得到状态$\langle(r_1, s_2), y\leqslant x\rangle$，然后发生转换 a，得到最终状态$\langle(r_2, s_2), x\leqslant y\rangle$，易见时钟是偏序技术的最大障碍之一。

对于实时系统的状态，Yoneda 和 Schlingloff 研究了在 petri nets 下的偏序约减技术。在文[17]中，Pagani 具体分析了转换之间的依赖关系，指出在许多情况下，时钟的引入，使得偏序技术的约减能力减弱。Pagani 研究的主要侧重点在于死锁的检测。Bengtsson[18]等人的研究指出，时间自动机网络中，不同时间自动机的时钟同步极大地影响了偏序约减技术。基于这种思想，Bengtsson 提出了一种方法来消除时间自动机网络中隐含的时钟同步信息，其基本思路是网络中每个时间自动机独立地运行，当时间自动机通讯的时候，才将本地时钟与其它时间自动机的时钟同步。这就将时间自动机的全局语义转换为局部语义，避免了对不必要的独立转换的交叉组合的搜索。这就使得在可达性分析中可以使用标准的偏序约减技术到时间自动机上。这个方法的缺点在于需要引入辅助时钟来对本地时钟进行同步，有一定的时空开销。文[18]中给出了一个基于 DBM 的利用符号状态检验的框架。Minea[19]在 Bengtsson 思想的基础上，将偏序技术用到了针对时间自动机事件发生的 LTL 模型检验上。

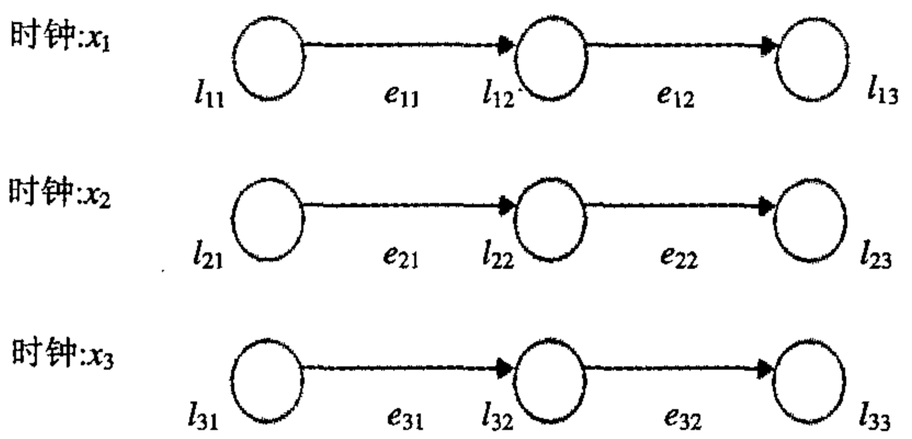

图 6 偏序路径的例子

文[20]在可达性分析中，提出了一个所谓“偏序路径”的概念。对于给定的符号状态，其计算的不是单个转换的后继，而是针对某条偏序路径的后继。其基本思想如下：如图 6 中的时间自动机网络的当前状态是$(\langle l_{11}, l_{21}, l_{31}\rangle, x\geqslant 0 \wedge y\geqslant 0 \wedge z\geqslant 0)$。A1 通过 e_{11} 到达 l_{12}，A2 通过 e_{21} 到达 l_{22}，A3 通过 e_{31} 到达 l_{32}。这样，到达位置$\langle l_{12}, l_{22}, l_{32}\rangle$的路径就有：$e_{11}\rightarrow e_{21}\rightarrow e_{31}$，$e_{11}\rightarrow e_{31}\rightarrow e_{21}$等。假设转换 e_{11}, e_{21}, e_{31} 分别重置 x_1, x_2, x_3。那么前面两条路径的后继中将分别包含原子公式 $x_3-x_2\leqslant 0, x_2-x_3\leqslant 0$。而如果 e_{11}, e_{21}, e_{31} 中没有同步转换，次序是不重要的。按照传统做法，为一个转换产生一个后继，$\langle l_{11}, l_{21}, l_{31}\rangle$到$\langle l_{12}, l_{22}, l_{32}\rangle$将会有 6 个后继产生。然而，如果次序不重要的话，可以合并这 6 个状态，得到状态$(\langle l_{12}, l_{22}, l_{32}\rangle, x\geqslant 0 \wedge y\geqslant 0 \wedge z\geqslant 0)$。一般来说，$n$ 个独立的转换将会产生 $n!$ 个后继。如果合并这些后继，不仅压缩了搜索空间，还扩大了符号状态，节省了时间。文[20]中给出了检验可达性的算法，它采用了 Bengtsson 的思想，时间自动机网络中的每个自动机单独运行，在需要同步的时候通过辅助时钟进行同步，同时它在此基础上提出了“偏序路径”。一条“偏序路径”是多条路径的组合，通过计算偏序路径的后继而不是单个转换的后继，检验效率大大提高。大部分空间遍历的性质通过“偏序路径”能够检验。

结束语 本文首先给出了时间自动机与可达性分析算法的基本概念，然后对可达性分析中具有代表性的优化技术的工作原理进行了探讨与研究。这些优化技术的思想之间虽然具有共性，同时又各有特点。本文将几种比较流行的优化技术分为针对时钟约束和针对路径遍历两种。针对时钟约束的优化技术又分为静态优化技术与动态优化技术两类。静态技术是一种在检验之前进行分析或者利用局部的信息的优化方法，包括如活跃时钟与等价时钟的约减、Convex Hull、基于时钟最大上下界的优化、静态删除无关原子公式等优化技术；动态技术是一种在检验过程中进行分析或者利用全局信息的优化方法，包括动态删除无关原子公式等。针对路径遍历的技术，我们主要讨论了偏序优化技术。一般来说，这些优化技术之间是正交的，即可以同时使用。这样，可以结合多种优化方法的优点，更好地约减空间状态。

目前对时间自动机状态中时间约束的静态分析比较广泛，但是在动态分析时间自动机网络中的时间约束的关系研究得还不够。如何动态发现无关原子公式和弱化时钟约束方面还值得进一步研究。例如，可以通过分析原子公式之间的依赖关系删除无关原子公式，扩大符号状态，最终约减状态空间。同时，偏序技术在实际的检验工具中还没有成熟，并且还有许多方面没有进行研究。这些方面将是我们下一步研究的方向。

参 考 文 献

1 Alur R, Dill D. Automata for modeling real-time systems. In:

Proc. of 17th International Colloquium on Automata, Languages and Programming (ICALP'90), Warwick University, England, 1990, LNCS443:322～335
2 Alur R, Dill D. A theory of timed automata. Theoretical Computer Science(TCS),1994,26(2):183～235
3 Behrmann G, David A, Larsen K G, et al. Uppaal - Present and Future. In: Proc. of the 40th IEEE Conference on Decision and Control(CDC'2001),Orlando,Florida,USA,December 2001
4 Daws C, Olivero A, Tripakis S, et al. The tool Kronos. In: DIMACS Workshop on Verification and Control of Hybrid Systems, New Brunswick,NJ,USA,October 1995, LNCS1066:208～219
5 Bryant R E. Graph-Based Algorithms for Boolean Function Manipulation. IEEE Trans on Computers,1986,35(8):677～691
6 Larsen K G, Weise C, Wang Yi, et al. Clock Difference Diagrams. Nordic Journal of computing,1999,6(3):271～298
7 Dill D. Time Assumptions and Verification of Finite-State Concurrent Systems. In:Proc. of automatic verification Methods for Finite State Systems,Grenoble,France,1989, LNCS 407:197～212
8 Bengtsson J, Wang Yi. Timed Automata: Semantics,Algorithms and Tools. Lecture Notes on Concurrency and Petri Nets. Reisig W, Rozenberg G. eds. LNCS 3098,Springer-Verlag,2004
9 Wang Farn. RED: Model-Checker for Timed Automata with Clock-Restriction Diagram. In: Proc. of Workshop on Real-Time Tools,Aalborg University,Denmark,August,2001
10 Daws C, Yovine S. Reducing the number of clock variables of timed automata. In: Proc. of the 17th IEEE Real-Time Systems Symposium(RTSS '96),Washington,DC,USA,December 1996
11 Daws C,Tripakis S. Model checking of real-time reachability properties using abstractions. In: Proc. of the 4th International Conf on Tools and Algorithms for Construction and Analysis of Systems (TACAS '98),Lisbon,Portugal,1998,LNCS1384:313～329
12 Behrmann G, Bouyer P,Emmanuel Fleury E,et al. Static Guard Analysis in Timed Automata Verification. In: Proc. of the 9th International Conf on Tools and Algorithms for Construction and Analysis of Systems (TACAS '2003), Warsaw, Poland, 2003, LNCS 2619:254～277

(下转第 100 页)

会议及征文消息

2006 年全国工业控制计算机年会

主办单位:中国计算机学会工业控制计算机专业委员会
会议日期:2006 年 11 月 27 日至 12 月 1 日 三亚　截稿日期:2006 年 10 月 10 日
投稿请寄:南京市锁金村 75 号《工业控制计算机》杂志社　邮编:210042　电话:(025)85411811,85414554
传真:(025)85414554　E-mail:ipcm_nj@163.com 或 ipcm@public1.ptt.js.cn

中国计算机学会信息保密专业委员会 2006 年学术会议

主办单位:中国计算机学会信息保密专业委员会
会议日期:2006 年 9 月中旬 沈阳　截稿日期:32006 年 7 月 20 日
投稿请寄:北京市海淀区交大东路甲 56 号　姜放 收　邮政编码:100044　电话/传真 010 82210912

全国第六届嵌入式系统学术交流暨产品展示会

主办单位:中国计算机学会微机(嵌入式系统)专业委员会
会议主题:嵌入式系统与技术创新
会议日期:2006 年 10 月 28 至 30 日 西安　截稿日期:2006 年 8 月 31 日(以邮戳为准)
联 系 人:张　维　北京大学信息科学技术学院　邮编:100871　电话:010－62763331　E-mail:wwzhang@pku.edu.cn
王铁鹰　《计算机技术与发展》编辑部　邮编:710054　电话:029－85522163 029－68810921
E-mail:wjfz@sninfo.gov.cn　wjfz@163.com

2006 年全国高性能计算学术会议

主办单位:中国计算机学会高性能计算专业委员会
会议日期:2006 年 10 月 27 至 29 日 北京　截稿日期:2006 年 8 月 30 日
会议网址:http://www.sccas.cn/hpcchina2006/　投稿地址:hpcchina2006@sccas.cn 或 chi@sccas.cn

CAD/CG 专委第十四届计算机辅助设计与图形学学术会议

主办单位:中国计算机学会 CAD/CG 专委会主办
会议日期:2006 年 10 月 18 至 20 日 济南　会议网站:http://cadcg2006.sdu.edu.cn

外围设备专委 2006 年学术会议

主办单位:中国计算机学会外围设备专业委员会
会议日期:2006 年 10 月 20 至 23 日 无锡　截稿日期:2006 年 7 月 30 日
投稿地址:无锡　南计算技术研究所　张石磊　电话:0510－85155332　E-mail:0510zsl@sina.com
无锡　江南大学信息工程学院　刘渊　电话:0510－85912151　Email:lyuan@sytu.edu.cn

全国第九届 Java 技术及其应用学术交流会

主办单位:中国计算机学会计算机应用委员会　中国自动化学会计算机应用委员会　中国电子学会计算机工程与应用委员会
中国信息产业商会微型机与应用分会　中国软件行业协会 java 分会
会议日期:2006 年 9 月中旬　北京　截稿日期:2006 年 7 月 15 日
来稿请寄:100083　北京 927 信箱　贾志梅　梁钢　龚炳铮收　或电子邮件:jiazm@ncse.com.cn gary@teamsun.com.cn
gongbz@ncse.com.cn　联系电话:(010)62327331－115/111　传真:(010)62311179、62325267

限等信息。根据用户的请求，这些信息被送往 DA 或 MA。

(4)DA 被用作应用服务或数据库中间件，通过 Servlet 技术，在网格环境中，它被用来作为本地的数据库中安全存取数据接口。经过 DA，IGA 的所有安全信息被存取到本地数据库。

(5)QA 接受 UA 的请求，并根据用户的请求，在全局数据库中查询安全审计信息。如果全局数据库中没有用户的安全审计记录，通过 MA，用户的请求被分派到各个站点，然后在本地数据库中查询安全审计信息。

(6)MA 接收来自 QA 或 UA 的信息，这些信息能够从一个站点传输到另一个站点。

随着 Java 技术的快速发展，越来越多的应用选择纯 Java 语言。在本文中，我们选择基于 Java 的 IBM Aglet 作为移动 Agent 平台。一方面，由于 Java 语言跨平台的特性，有利于用户程序的开发和部署；另一方面、IBM Aglet 提供了移动 Agent 有效的编程模型和 Agent 之间动态的通信机制。此外，通过 Aglet 系统提供的上下文环境，Aglet 能够管理 aglet 的行为。利用 com. ibm. aglets. security 包，能够实现 Agent 的安全性，利用 com. ibm. maf. mAFAgentSystem 包，实现 Agent 的互操作性。利用 Servlet 技术完成与用户的交互，利用 KQML 完成 Agent 之间的通信。最后，通过代理提供安全的接口，当 Aglet 与远程 Aglet 连接时，系统在本地上下文环境中产生一个代理，类似于网格中的授权管理链。

3.3 用户审计服务

用户审计服务由底层的服务构建。审计需求处理使用 Apache AXIS 作为它们 Web 服务的引擎，所有服务在 J2EE/J2SE Web 容器中执行。这些服务也能够直接存取审计结果，监控异质资源和每一个节点的状态。

结论和未来的工作 网格安全的研究与实现是一个难度很大的课题。本文提出的跨域安全审计体系结构，是实现网格安全的一种新的尝试。获取安全的代价常常导致系统开销的增加。为了使安全机制的实施对网格性能产生的影响最小，本文所提出的一种新的授权安全机制“审计一次，授权多次”能有效地降低网格的开销。基于信任关系的动态审计策略非常符合网格自身的动态变化特性。基于 GT3 和 Aglet 平台的跨域安全审计体系结构的实现是本文研究工作的一次新的工程性探索。

未来的工作是计划通过实际复杂的应用来完善 CDSA 体系结构，并研究更优的审计策略。

参 考 文 献

1 Humphrey M, Thompson M R, Jackson K R. Security for Grids. Proceedings of The IEEE, 2005, 93(3): 644～652

2 GGF SAAAR RG. Grid Authentication Authorization and Accounting Requirements Draft 5. May 21, 2004. https://forge.gridforum. org/projects/saaa-rg/document/draft -ggf-saaar-reqs-5. txt/en/1

3 Thompson M, Olson D, Cowles R, et al. CA-Based Trust Model for Grid Authentication and Identity Delegation. Grid Certificate Policy Working Group, 2002

4 Mendes S, Huitema C. A New Approach to The X. 509 Framework: Allowing A Global Authentication Infrastructure Without A Global Trust Model. In: Proceedings of NDSS'95, 1995

5 Ellison C, Frantz B, Lampson B, et al. SPKI Certificate Theory, Internet Request for Comments: 2693, 1999

6 Li T Y, Zhu H F, Lam K Y. A Novel Two-Level Trust Model for Grid. In: ICICS 2003, LNCS 2836, 2003. 214～225

7 Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems. In: Canadian Conference on Electrical and Computer Engineering, IEEE CCECE 2002, 2002. 1424～1429

8 Foster I, Kessslman C, Nick J, et al. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. http://www. nesc. ac. uk/talks/ggf5_hpdcll/physio_o_grid220702. pdf

9 Gou X T, Jin W D, Zhang G X. Multi-agent Based Security Auditing System of Broadband MAN. In: Proceedings of the 2004 International Conference on Intelligent Mechatronics and Automation, Chengdu, China, 2004. 939～944.

10 Raghnnathan S, Mikler A, Cozzolino C. Secure Agent Computation: X. 509 Proxy Certificates in a Multi-lingual Agent Framework. The Journal of Systems and Software, 2005, 75: 125～137

11 Shakshuki E, Ghenniwa H, Kamel M. A Multi-agent System Architecture for Information Gathering, Database and Expert Systems Applications 2000. In: Proceeding 11th International Workshop on, 2000. 732～736

12 Huang Y C, Chen Y, Li , et al. Research On Network Secure Auditing System Using Distributed Agents. In: Proc. of IEEE TECCON'02, 2002. 391～395

13 战晓苏，张少华译. 网格计算. 北京：清华大学出版社，2005

(上接第 6 页)

13 Behrmann G, Bouyer P, Larsen K G, et al. Lower and Upper Bounds in Zone Based Abstractions of Timed Automata. In: Proc. of the 10th International Conf on Tools and Algorithms for Construction and Analysis of Systems (TACAS '2004), Barcelona, Spain, 2004

14 ZHAO Jianhua, LI Xuandong, ZHENG Tao, et al. Removing Irrelevant Atomic Formulas for Checking Timed Automata Efficiently. In: Proc. of First International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS), Marseille, France, 2003, LNCS 2791: 34～45

15 Godefroid P. Partial-order methods for the verification of concurrent systems: an approach to the state-explosion problem. LNCS1032, Springer-Verlag, January 1996

16 Peled D. All from one, one for all: on model checking using representatives. In: Proc. of the 5th International Conference on Computer Aided Verification (CAV' 1993), Elounda, Greece, 1993, LNCS697: 409～423

17 Pagani F. Partial orders and verification of real-time systems. In: Proc. of the 4th International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems(FTRTFT'96), Uppsala, Sweden, 1996, LNCS1135: 327～346

18 Bengtsson J, Jonsson B, Lilius J, et al. Partial order reductions for timed systems. In: Proc. of 9th International Conference on Concurrency Theory(CONCUR'98), Nice, France, 1998

19 Minea M. Partial order reduction for model checking of timed automata. In: Proc. of 10th International Conference on Concurrency Theory (CONCUR ' 99), Eindhoven, Netherlands1999, LNCS1664: 431～446

20 Zhao Jianhua, Xu He, Li Xuandong, et al. Partial Order Path Technique for Checking Parallel Timed Automata. In: 7th International Symposium on Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT 2002), University of Oldenburg, Germany, 2002: LNCS2469. 417～432