基于模型检测的时间空间性能验证方法

钮 俊[1),2),3)] 曾国荪[1),2)] 王 伟[1),2)]

[1)](同济大学计算机科学及技术系 上海 201804)

[2)](嵌入式系统与服务计算教育部重点实验室 上海 201804)

[3)](浙江工商职业技术学院信息工程学院 浙江 宁波 315012)

摘 要 对具有不确定性的复杂系统如网络协议等的性能进行分析是当前的研究热点.将空间资源分析纳入到性能评估过程,用模型检测技术验证时间或空间性能是否满足期望的需求约束.用能刻画不确定性的连续时间 Markov 回报过程(Continuous-Time Markov Reward Process,CTMRP)作为时间或空间性能验证模型;用正则式表示路径约束,扩展连续随机回报逻辑 CSRL(Continuous Stochastic Reward Logic)的时态路径算子,用以刻画更加广泛的基于状态或路径的时间或空间性能验证属性;提出并证明 CTMRP 在确定性策略下空间时间可达概率的对偶性质,将带有约束的空间性能验证最终转化为时间性能的可达分析,给出验证算法.文中的结论和算法为复杂系统的性能分析提供了新的思路和方法.

关键词 不确定性;模型检测;时间空间性能;可达概率;对偶

中图法分类号 TP301 **DOI 号**: 10.3724/SP.J.1016.2010.01621

An Approach of Model Checking Time or Space Performance

NIU Jun[1),2),3)] ZENG Guo-Sun[1),2)] WANG Wei[1),2)]

[1)](*Department of Computer Science and Technology, Tongji University, Shanghai* 201804)

[2)](*Embedded System and Service Computing Key Laboratory of Ministry of Education, Shanghai* 201804)

[3)](*College of Information Engineering, Zhejiang Business Technology Institute, Ningbo, Zhejiang* 315012)

Abstract It has been a research focus that the performance analysis of complex systems such as network protocols which include nondeterministic choices. Besides time, space aspect is also considered during the process of performance evaluation. By model checking, we can verify whether time or space performance meets expected constraints. The authors adopt CTMRP (Continuous-Time Markov Reward Process) as the verification model since it can depict nondeterminism intuitively. The temporal logic CSRL (Continuous Stochastic Reward Logic) is extended by replacing path operators with regular expressions in order to express more comprehensive time or spatial properties which are based on states or paths. For deterministic schedulers, a duality result of constrained reachability probabilities between time and space is proposed, and its correctness is proved based on the existing work. Based on the theoretical consequences, the verification of space performance is reduced to the corresponding analysis of time reachability. The model checking algorithm and a new approach for the performance evaluation of complex systems are given.

Keywords nondeterminism; model checking; time or space performance; reachability probabilities; duality

收稿日期:2010-04-21;最终修改稿收到日期:2010-08-02.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z425,2009AA012201)、国家"九七三"重点基础研究发展规划项目基金(2007CB316502)、国家自然科学基金(90718015)、NSFC-微软亚洲研究院联合项目(60970155)、教育部博士点基金(20090072110035)、上海市优秀学科带头人计划项目(10XD1404400)、高效能服务器和存储技术国家重点实验室开放基金(2009HSSA06)、同济大学青年优秀人才培养行动计划(0800219105,2009KJ030)和浙江省宁波市自然科学基金(2010A610123)资助.**钮 俊**,男,1976 年生,博士研究生,讲师,主要研究方向为模型检测、性能评估.E-mail:tongjinj@gmail.com.**曾国荪**,男,博士,教授,博士生导师,主要研究领域为模型检测、高性能计算、信息安全.**王 伟**,男,1979 年生,博士,讲师,主要研究方向为可信软件、性能评估.

1 引 言

作为人类最伟大的发明之一，上个世纪出现的互联网络，因其跨越时空的泛在、快速的优点，日益渗透到科技创新、经济发展、社会进步和日常生活等各个领域，深刻地改变着人们的生产、生活和学习方式. 在互联网络的应用中，需要设计和分析大量复杂、关键的非线性系统，如软件、硬件、通信系统等实体系统，或者网络体系结构、网络协议等刻画规则语义的逻辑系统，它们往往具有随机、概率、并发、动态等特征. 系统在运行过程中，需要消耗时间空间资源. 对系统的时间空间性能进行评估，是学术界、工程界一直关注的焦点. 系统正常运作，实现既定功能有着必然的性能约束，否则当完成某种功能需要环境不允许或不能承载的性能耗费，这样的功能是无法实现的，不具有实际可操作性. 性能也是一个系统可持续运行的非常重要的方面，性能低下的系统，运行过程中需要消耗大量的时间空间资源，不利于系统的持续运行. 比如在评价一个算法时，不仅要看其功能是否正确，重点还需把握该算法的时间空间复杂度. 文献[1]指出性能评估或评价是互联网络研究与应用的重要理论基础和支撑技术. 文献[2]认为在下一带互联网体系结构中，为了提供更加有效可靠的服务质量(Quality of Service，QoS)，需要对网络资源进行有效的控制和管理. 因此，在实施前，基于功能正确的保证，对复杂系统的性能进行评估，以判断其是否满足给定约束，是至关重要的. 在当前节能减排以及绿色计算[3]的国际大背景下，对系统的空间时间性能进行评估，显得尤为迫切. 通过评估可发现系统设计中的错误、漏洞或缺陷，作为改进设计的依据.

空间资源是系统在运行过程中与运行环境进行交互的所有非时间性资源的总称，如需要占用或消耗的存储空间、网络带宽、功耗能量或物理空间[3]等物理资源以及协商步骤、活动组件、冗余组织、备选子服务等逻辑资源. 人们总是希望系统能在尽可能短的时间内，消耗尽可能少的空间资源，完成既定功能. 比如在高效能计算机的研制中，尽可能地降低能耗是大家努力的目标；在博弈协商过程中，通过尽可能少的证书交换建立信任，是人们关注的焦点；文献[4]运用模型检测技术研究分析了移动设备中电池能量的优化技术，通过动态能量管理(Dynamic Power Management，DPM)策略，最小化活动组件的数量，使系统仍够提供最好的服务，从而达到降低能耗的目的.

互联网络中，不确定性、连续时间、概率选择是大量复杂系统的重要特征. 运用模型检测技术，对复杂系统的性能进行验证，是近年来性能评估领域的研究热点，已经出现了一些引人注目的研究成果. 这些工作一般根据需要评估的兴趣度和精度，构造近似的但保留充分细节的系统抽象模型，对如存储占用率、吞吐量、失效组件数量、能耗情况等进行评估. 文献[5-6]等将进程代数、标记传递系统与连续时间 Markov 链正交结合，得到一种交互式 Markov 链模型 IMC(Interactive Markov Chains)，将 CSL 扩展为 aCSL(action-based CSL)，可进行系统功能与时序性能的组合刻画，并给出了相应的模型检测算法. 尽管 IMC 能够刻画不确定性，但未能解决空间性能的验证. 文献[7-8]为连续时间 Markov 链(Continuous-Time Markov Chain，CTMC)的状态定义回报结构(reward structure)，用以标记系统驻留于某状态时单位时间内的空间资源消耗量，将扩展获得的 Markov 回报链(Markov Reward Model，MRM)作为时间空间性能分析模型，性能验证属性用 CSRL 公式表示，给出模型检测算法；在 MRM 的基础上，文献[4]为 CTMC 的转移添加类似的回报描述，建立带有 impulse reward 的 Markov 回报模型，并运用 CSRL 模型检测技术分析研究移动设备中电池能量的优化策略，但基于转移动作的瞬时性，回报值往往难以观测，因此，在实际应用中这种方法较难实施. 文献[9]提出一种能刻画功能和时间空间性能的随机验证模型 atsFPM，功能和时间空间性能属性用基于动作和状态的 CSRL 描述，通过求解功能属性自动机与原始模型的积模型的可达概率，对系统的功能和时间空间性能进行统一验证. 但是，由于不能直观地刻画不确定性，上述 3 种模型及验证算法的适用性并不强. 类似于 MRM 对 CTMC 的扩展，文献[10]等在离散时间 Markov 决策过程的基础上，为状态添加回报结构，得到离散时间 Markov 回报过程(Discrete-Time Markov Reward Process，DTMDP)，用扩展的概率 CTL(Probabilistic CTL，PCTL)作为性能验证属性的描述语言. 尽管 DTMDP 能刻画不确定性，但不能处理连续时间. 为了进行性能和可靠性分析，基于随机 Petri 网，文献[11]提出一种 Markov 再生随机 Petri 网(Markov Regenerative Stochastic Petri Nets，MRSPNs)；文献[12]为状态和变迁添加回报结构，将广义随机 Petri 网

(Generalized Stochastic Petri net, GSPN)扩展为GSPN-Reward;文献[13]提出一种 Markov 决策 Petri 网(Markov Decision Petri Nets, MDPNs),该模型能够同时表达概率性和不确定性.国内清华大学的林闯教授在性能分析方面也做了大量的研究工作,文献[14]综述了作者在基于随机 Petri 网的系统性能评价方面的研究成果;文献[1]介绍了性能评价的3种形式化方法,即排队论(Queuing Theory)、随机 Petri 网、随机进程代数.尽管这些基于 Petri 网的高层(High-level)模型能以图形化的方式给出系统模型,但对它们的评估在一定程度上最终都需要转换到 Markov 性模型上进行求解,不同于本文的形式验证工作.

由以上分析可知,已有相关工作均存在着一定的局限性.与上述有关工作类似,通过给状态添加回报结构,本文在连续时间 Markov 决策过程(Continuous-Time Markov Decision Process,CTMDP)的基础上,提出采用一种带标记的基于回报的连续时间 Markov 决策过程 CTMRP,作为复杂系统的时间空间性能分析模型.与已有模型相比,CTMRP 能统一刻画不确定性、连续时间及概率选择,同时,它也是很多性能分析模型如交互式 Markov 链、带有回报的广义随机 Petri 网、随机回报活动网等的语义模型[15],具有广泛的应用背景.本文首先阐述了时间空间性能验证要求,并提出问题;第3节介绍了 CTMRP 的相关概念,并给出精确的数学描述;第4节论述了刻画性能验证属性的时序逻辑规范的语法和语义;第5节给出空间时间可达概率对偶性质,并给出证明,将空间性能转换为时间性能进行分析;最后总结了全文.

2　验证要求及问题提出

系统的功能正确性和性能可满足性是人们关注的重要方面.在功能正确的前提下,性能是评价系统能力、可靠性、可用性、可信性等的关键因素.一般地,性能是复杂系统演进过程中可观测的时间空间资源消耗量的若干指标的总合,用以衡量或评估功能实施的优劣程度.通过性能评估,可对系统的行为进行研究和优化,使其能够提供更加优良的服务.一方面判断系统是否满足期望性能约束或对系统的性能进行预测,另一方面也可发现现有系统的性能缺陷和瓶颈,掌握改进设计的依据或方向[1].

从哲学上讲,任何系统都运行并作用于特定的时空环境(runtime context),依赖于环境而存在,产生人们期望的某些效益,即耗费资源,获得效用.除了时间外,可能消耗诸如处理单元、存储、带宽、能耗、物理空间等实体资源或者如活动组件、协商步骤等抽象资源.同时,也将产生某些效用.比如某个网络服务提供者单位时间内提供成功服务的数量,也是评价系统性能的一个重要方面.本文不打算在这方面做过多的展开,为了方便描述,先给出下面的定义.

定义 1.　空间资源.在运行过程中,系统与环境进行交互,而消耗或生产的一切具体或抽象的非时间资源的总称,包括输入和输出两个方面,输入是运行的前提,即物质基础,输出可用以评价对某种效用资源的生产能力.

本文中,资源的生产或消耗统称为资源要求.分析空间性能需要刻画运行中的空间资源要求情况.一般情况下,空间资源要求量随着时间的消逝而逐渐累积,我们用单位时间的资源要求量,即空间资源要求率来刻画系统的空间资源要求情况[9].系统驻留于不同的状态时,空间资源率可能是不一样的,比如处于数据传输状态时比在闲置状态时可能需要消耗更多的带宽.本文中将系统在运行时的空间资源要求率建模为系统的内在属性,即作为状态的一个属性,也即是引言部分所提到的状态的回报结构.注意本文中我们所关注的运行时状态,是根据验证需要对实际系统进行抽象建模而呈现出的状态,并非一一对应于真正物理状态,这对分析和验证来说是充分的,同时也避免带来影响验证可行性的状态爆炸问题(State Explosion Problem)[16-17],读者不难从本文的描述中获得理解.

分析系统性能首先要建立系统的动态行为模型,并对执行时间或空间资源要求率等参数进行标注.大多数实时系统在行为上都具有概率性、随机性和不确定性等特性.不确定性是复杂动态系统的重要行为特征,它用以刻画多种不同的运行方式,可分为内部不确定性和外部不确定性两种情况,适用场景主要体现在调度自由、实现自由、外部环境未知、不完全信息等方面[18].比如在动作细化理论(action refinement)[19]中,某个抽象动作在不同的情况下可能会做不同的替换,同时,这种替换并不满足特定的随机分布,故只能作不确定性处理,这体现了实现自由;或者,在研究网络协议的抗攻击模型时,由于不能事先确定攻击行为,在建模时,只能以不确定性描述,这体现了外部环境未知的情况.本文只考虑内部

不确定性.因此,性能评估模型需要能够刻画系统的实时性、概率性、不确定性及空间资源要求情况等.本文采用已经获得一定关注,并且能够满足上述要求的连续时间 Markov 回报过程 CTMRP 作为性能评估模型.本文的研究重点不在于运行时时间空间性能参数的获取过程以及模型建立方法,只关注如何在理论模型上运用模型检测技术对其进行性能验证.另外,在一次空间性能验证中,只考虑一种空间资源,比如只分析存储性能,或者只分析能耗性能,同时只关注其消耗或者生产,即状态的回报值要不全为正,要不全为负.由于正负可以转换,本文只关注回报值全为正的情况.为了描述方便,本文首先给出一个实例以提出问题.

例 1. 简单通信协议.某个通信系统在空闲状态时,接受到信息发送命令,进入发送准备状态;系统可能繁忙,需要等待,或者数据丢失,必须重新发送;准备就绪时,发送消息,有发送成功(success)和失败(fail)两种可能.

对于该协议,我们可能会关注以下类型的性能指标:

(1) 某信息在 5s 内成功发送的概率至少为 95%;

(2) 信息发送过程中,累积缓存占用超过 2MB 的概率至多为 1%;

(3) 完成某项任务经历失败状态的次数小于 2 次的概率至少为 80%;

(4) 信息发送过程中,数据丢失概率至多为 0.5%.

性能指标(1)描述了时间性能指标,(2)、(3)、(4)描述了空间性能指标.对上述量化性能指标的验证,不能用传统的功能验证的模型或方法进行.本文中,我们引入随机模型检测的方法,用以对类似上述问题进行验证评估,模型检测框架如图 1 所示.

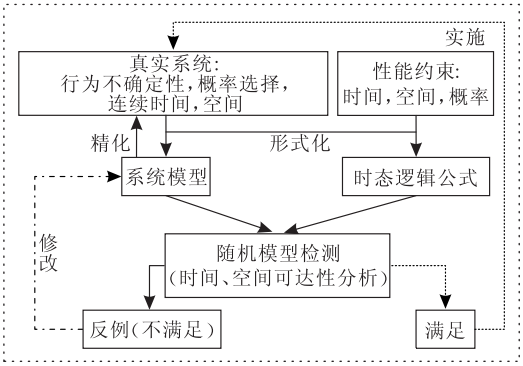


图 1 基于随机模型检测的性能验证框架

3 时间空间性能验证模型及数学描述

连续时间 Markov 回报过程 CTMRP 通过给连续时间 Markov 决策过程 CTMDP 的状态空间添加表征空间资源要求情况的回报结构而得到.对 CTMRP 的性能分析最终需要转换到对应的CTMDP 上进行.CTMRP、CTMDP 可分别看作 Markov 回报链 MRM、连续时间 Markov 链 CTMC 的一般形式[12],除了不确定性外,它们在概念上有很多重复的地方.因此,本节先给出 CTMC 和 MRM 的基本概念,最后引出 CTMDP 和 CTMRP 的相关定义.

3.1 连续时间 Markov 链和 Markov 回报链

定义 2. 带标记的连续时间 Markov 链 CTMC[17,20],为四元组 (S,AP,L,R),其中 S 为状态集,AP 为原子命题集,$L:S\to 2^{AP}$ 为状态标记函数,$R:S\times S\to\mathbb{R}_{\geq 0}$ 为转移函数.

如果 $R(s,s')>0$,则存在从状态 s 到状态 s' 的转移率为 $R(s,s')$ 的转移 $s\to s'$,且该转移在时间 t 内触发的概率为 $1-\mathrm{e}^{-R(s,s')\cdot t}$,$s\to s'$ 的延迟满足参数为 $R(s,s')$ 的指数分布.设 $E(s)=\sum_{s'\in S}R(s,s')$,如果 $E(s)=0$,则状态 s 为吸收态.

Markov 链是一种特殊的转移系统[17],状态 $s\in S$ 的后继状态由某个概率分布确定.该概率分布与系统在状态 s 之前的演化过程无关,具有无记忆性,转移延迟时间满足指数分布.常用作时间性能分析模型.为了能够刻画运行过程中的空间性能参数,可为 CTMC 的状态空间指定回报函数.

定义 3. 连续时间 Markov 回报链 MRM[7-8],为二元组 (C,ρ),其中 C 为带标记的连续时间 Markov 链,函数 $\rho:S\to\mathbb{R}_{\geq 0}$ 为回报结构:给每个状态 s 分配值 $\rho(s)$,用以刻画驻留于某状态时的空间资源要求率.

用 $s\xrightarrow{t}s'$ 表示 CTMC 或 MRM 中的状态转移,其中 t 表示转移延迟时间.多个转移构成的转移序列为执行路径.转移序列

$$s_0\xrightarrow{t_0}s_1\xrightarrow{t_1}s_2\xrightarrow{t_2}\cdots\xrightarrow{t_{n-2}}s_{n-1}\xrightarrow{t_{n-1}}s_n\cdots$$

表示一条无限路径,其中,对所有的非负整数 i,满足 $s_i\in S$、$R(s_i,s_{i+1})>0$ 且 $t_i\in\mathbb{R}_{\geq 0}$.如果 s_j 为吸收态,则称转移序列 $s_0\xrightarrow{t_0}s_1\xrightarrow{t_1}s_2\xrightarrow{t_2}\cdots\xrightarrow{t_{j-2}}s_{j-1}\xrightarrow{t_{j-1}}s_j$ 为一条有限路径.

令 σ 为某条有限路径,记 $\sigma[i]=s_i$ 为路径中的

第 $i+1$ 个状态. $\delta(\sigma,i)=t_i$ 表示路径在状态 s_i 的停留时间. $\tau(\sigma)=\sum_{m=0}^{j-1}t_m$ 为路径 σ 上的累计时间消耗. 当 $t\leq\tau(\sigma)$ 时，路径 σ 在时刻 t 所处的状态用 $\sigma@t$ 表示，$\sigma@t=\sigma[k]$，其中，$k=min_i\left(t\leq\sum_{j=0}^{i}t_j\right)$. 记 $Path^{CM}(s)$ 为 CTMC 或 MRM 模型 CM 中，从状态 s 出发的所有路径的集合. 通过构造集合 $Path^{CM}(s)$ 上的 Borel 空间，为路径集合定义概率测度 $Pr^{CM,s}$，简记为 Pr^{CM}，详细说明参考文献[20]. 给定 CM，从状态 s 出发，在时刻 t 处于状态 s' 的概率，用 $\pi^{CM}(s,s',t)$ 表示，即 $\pi^{CM}(s,s',t)=Pr^{CM}\{\sigma\in Path^{CM}(s)\mid\sigma@t=s'\}$，表示瞬时概率，$\pi^{CM}(s,s')=\lim_{t\to\infty}(\pi^{CM}(s,s',t))$ 表示稳态概率，即一直停留于状态 s' 的概率. 令 $S'\in 2^S$，记 $\pi^{CM}(s,S')=\sum_{s'\in S'}\pi^{CM}(s,s')$. σ 在时刻 t 的累积空间资源要求总和定义为 $y(\sigma,t)$，即，当 $t=\sum_{j=0}^{k-1}t_j+t'$ 且 $t'\leq t_k$ 时，$y(\sigma,t)=\sum_{j=0}^{k-1}t_j\cdot\rho(s_j)+t'\cdot\rho(s_k)$，其中 t_j 为在状态 s_j 的停留时间.

定义 4.　概率分布. 集合 S 上的函数 μ，满足 $\sum_{s\in S}\mu(s)=1$.

集合 S 所有概率分布的集合记为 $Distr(S)$.

3.2　带标记连续时间 Markov 回报过程

定义 5.　带标记的连续时间 Markov 决策过程 CTMDP，为六元组 (S,AP,Act,R,L,v)，其中 S 和 Act 分别为状态和动作的非空可数有限集，AP 为原子命题集合，$R:S\times Act\times S\to\mathbb{R}_{\geq 0}$ 为转移率矩阵，$L:S\to 2^{AP}$ 状态标记函数，$v\in Distr(S)$ 为初始分布.

在 CTMDP 中，如果 $|Act|=1$，则其为连续时间 Markov 链，原因在于，如果所有转移动作都相同，则可忽略该动作标记. 如果 $R(s,a,s')=\lambda>0$，则存在一个从状态 s 到状态 s' 的 α 转移，状态 s 在动作 α 下的停留时间的离开率为 $E(s,a)=\sum_{s'\in S}R(s,a,s')$. 如果 $E(s,a)>0$，则称动作 α 在状态 s 是使能的，集合 $Act(s)=\{a\in Act\mid E(s,a)>0\}$ 代表状态 s 的使能动作集合并且确定了状态 s 的所有不确定选择. 如果从状态 s 出发，有多个不确定性动作，即 $|Act(s)|>1$，则将不确定性地选择某个动作 $a\in Act(s)$. λ 代表转移延迟的指数分布的参数，如果动作 α 被选择，则该转移在时间范围 $[l,m]$ $(l,m\in 0)$ 内执行的概率为 $\int_l^m\lambda e^{-\lambda t}dt$. 如果从状态 s 出发，有多个 α 转移，则将会出现竞争条件：首先完成自己的延迟时间的 α 转移先执行状态转移，并确定动作 α 下在状态 s 的停留时间.

CTMDP 中，有限路径为形如 $\pi=s_0\xrightarrow{t_0,a_0}s_1\xrightarrow{t_1,a_1}\cdots\xrightarrow{t_{n-1},a_{n-1}}s_n$ 的序列，其中，$s_i\in S$，$a_i\in Act$，$t_i\geq 0$ $(i\leq n)$，n 为路径的长度，记为 $|\pi|=n$. 记路径 π 被抽取动作信息后的形式为 $\pi'=s_0\xrightarrow{t_0}s_1\xrightarrow{t_1}\cdots\xrightarrow{t_{n-1}}s_n$，相关定义类似于连续时间 Markov 链和 Markov 回报链. 用 $last(\pi)$ 表示路径 π 的最后一个状态.

从 CTMDP 的定义可以看出，它是一种基于动作和状态的随机系统模型，能同时进行功能刻画和性能描述. 特别地，该模型能够直观地刻画非确定性，这对大型复杂并发系统的刻画尤为重要，这也是本文采用该模型的原因和目的所在. 通过为 CTMDP 添加类似于 MRM 中的回报结构，就得到本文重点关注的时间空间性能评估模型.

定义 6.　连续时间Markov回报过程 CTMRP，为二元组 $M=(M',\rho)$，其中 M' 为带标记的连续时间 Markov 决策过程，$\rho:S\to\mathbb{R}_{\geq 0}$ 为回报函数，为每个状态 s 分配一个成本或收益值 $\rho(s)$. M' 称为 CTMRP 的内置 CTMDP，其它相关定义参见前面的描述.

定义 6′.　均匀 Markov 回报过程（uniform CTMRP），设连续时间 Markov 回报过程为 $M=(M',\rho)$，其中 M' 为其内置 CTMDP，如果对所有 $s\in S$ 及 $a\in Act(s)$，存在 $\widetilde{E}>0$，满足 $E(s,a)=\widetilde{E}$，则称 M 是均匀的，其中 $\widetilde{E}$ 称为均匀转出率.

显然，通过为状态添加到自身的转移，可以将任何 CTMRP 模型均匀化，并且均匀化模型与原模型互模拟等价[15].

例 2.　例 1 中简单通信协议的 CTMRP 模型如图 2 所示. 模型包含 6 个状态，用圆圈表示，分别标记为 $\{init\}$、$\{try\}$、$\{busy\}$、$\{lost\}$、$\{fail\}$、

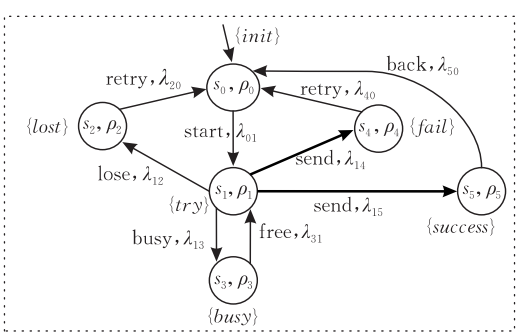


图 2　简单通信协议的 CTMRP 模型

$\{success\}$. 状态信息包括状态名和该状态的回报率. 转移用有向箭头表示. 为了便于描述,转移标记由动作名和对应的转移率表示,如 s_1,ρ_1. 状态 s_1 具有不确定性,3 个使能动作分别为 send、busy、lose. 动作标记相同的转移对应于同一个概率分布,如转移 $s_1 \xrightarrow{\text{send}} s_4$ 和 $s_1 \xrightarrow{\text{send}} s_5$.

3.3 不确定性的消解

不确定性是 CTMRP 区别于 Markov 链和 Markov 回报链的固有属性,能保证大多数场景下复杂系统的建模需要. 但正由于不确定性的存在,不能在 CTMRP 上直接进行概率计算,进而得到评估结果. 为了进行性能分析,需要消除具有多个后继动作的状态的不确定性. 这可通过明确指定从该状态出发将要执行的具体动作而实现,即状态 s_i 如果满足 $|Act(s_i)|\geq 2$(该状态也被称作决策点),则需要选取动作 $\alpha\in Act(s_i)$ 作为执行动作. 比如对于图 2 所示 CTMRP 模型,在状态 s_1 存在多个可选的后继动作,每个动作对应一个概率分布,可通过明确指定状态的后继动作,比如 send,来消除该状态的不确定性. 一次完整的对模型中所有具有不确定性的状态的不确定性进行消解的方式和过程,称为一个策略(policy 或 scheduler)[17-18].

在策略中,状态 s 下一步将要执行的动作的选取可依赖于从初始状态到状态 s 的路径片段上的历史信息和动作选取方式. 路径上的信息包括路径上的状态信息、动作信息及该路径上所消费的时间等,本文不考虑时间信息;动作的选取有两种方式:确定性选取或随机选取. 前者明确指定某个动作作为后继执行动作,后者意味着后继动作选取依据某个概率分布. 根据对历史信息的依赖程度,策略可分为历史相关和无记忆两种. 一个策略是历史相关的(history-dependent),如果它依赖于系统的过去历史信息;如果策略只依赖于当前状态信息,则称其是无记忆性的(Memoryless). 如果依据特定的概率分布选择后继动作,称策略是随机的(randomized);否则为确定性策略(deterministic). 故策略可分为历史相关的随机策略(HR)、历史相关的确定性策略(HD)、无记忆性的随机策略(MR)和无记忆性的确定性策略(MD)等类型[18].

给定初始状态 s 和策略 d,CTMDP 将演变成随机过程[15]. 特别地,对于确定性策略,如 HD、MD 或 SMD 等,该随机过程为连续时间 Markov 链. 为了便于分析,本文考虑 HD 型策略. 很显然,HD 型策略可用函数 $d:S^+\rightarrow Act$ 刻画,原因在于策略信息是历史相关的,由历史状态的序列 $q\in S^+$ 决定动作的选取方式. 为了便于本文的分析,先给出下列命题.

命题 1. 在确定性策略 HD 下,连续时间 Markov 回报过程将演变为连续时间 Markov 回报链.

证明. 根据前文的说明,HD 型策略可用函数 $d:S^+\rightarrow Act$ 表示. 显然,通过 HD 型策略的不确定性消解,CTMDP 模型 $M'=(S',AP',Act',R',L',v')$ 将诱导产生对应的连续时间 Markov 链 $M=(S,AP,L,R)$,二者互模拟等价[15]. 其中,原子命题集和状态标记函数不变,M' 中的路径集合构成 CTMC 模型 M 的状态空间,即 $S=S'^+$,转移关系[15]为

$$R(\sigma,\sigma')=\begin{cases}R'(last(\sigma),d(\sigma),s), & \text{如果 } \sigma'=\sigma\rightarrow s\\ 0, & \text{其它}\end{cases}.$$

由相关定义可知,将回报过程 CTMRP 的回报结构平移到由 CTMRP 对应的 CTMDP 诱导产生的 CTMC,则得到对应的连续时间 Markov 回报链.

为了便于下文分析,将由策略 d 诱导产生的 MRM 模型 M 上的概率测度定义为 $Pr_d^{M,s}$,并记当前所考虑策略类型中所有策略的集合为 D.

例 3. 图 2 的 CTMRP 模型中,状态 s_1 有 3 个使能动作,具有不确定性. 设策略 d_1 按照 send、lost、busy 的动作选择顺序消除不确定性,即 $d_1(s_0s_1)=$ send,$d_1(s_0s_1s_4s_0s_1)=$ busy,…;策略 d_2 按照 busy、send、lost 的动作选择顺序消除不确定性,即 $d_1(s_0s_1)=$ busy,$d_1(s_0s_1s_4s_0s_1)=$ send,…. 在策略 d_1 下所得到的 Markov 回报模型如图 3 所示. 为了简洁,图 3 中只给出状态转移情况,忽略了其它标记.

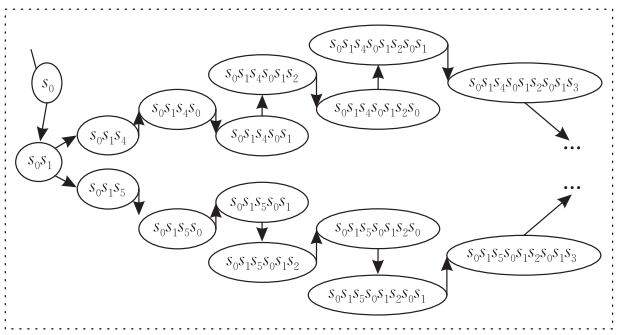


图 3 策略 d_1 下简单通信协议的 Markov 回报模型

4 刻画性能属性的随机时序逻辑

模型检测是在给定模型上,以自动化的方法验证系统的时态或模态性质. 性质用某种时态逻辑公式表示,验证结果为满足性质的状态集合[21-22]. 根

据前面的描述，在对 CTMRP 进行时间或空间性能的随机模型检测过程中，验证属性要能够刻画路径的时态约束、路径上的时间空间约束以及满足这些约束的路径集合的概率范围. 概率计算树逻辑 PCTL 只能刻画离散时间属性，连续随机逻辑 CSL (Continuous Stochastic Logic)不能刻画空间约束. 作为 PCTL、CSL 等时态逻辑的扩展，CSRL 是一种能够同时表达空间和连续时间性能属性的时态逻辑规范，能够刻画时间或空间验证属性. 为了支持本文的验证需求，本文对 CSRL 做了改进，将 CSRL 中的路径公式用正则式或与之等价的自动机表示，使其能够刻画更加广泛地基于状态或路径的性能属性[21,23]. 本节给出 CSRL 的语法和语义.

定义 7.　状态公式语法.

$\Phi ::= \text{false} \mid ap \mid \neg\Phi \mid \Phi \vee \Phi \mid \mathcal{S}_{\infty p}(\Phi) \mid \mathcal{P}_{\infty p}(\varphi)$,

其中，false 代表逻辑恒假，ap 为原子命题，Φ 为状态公式，符号 $\neg$、$\vee$ 为基本逻辑运算符，$\infty \in \{<, \leq, >, \geq\}$ 为算术比较算子，$p \in [0,1]$ 表示概率，$\mathcal{S}_{\infty p}(\Phi)$ 为稳态概率算子，表示最终停留于 Φ 状态的路径集合的概率满足 ∞p，瞬时概率算子 $\mathcal{P}_{\infty p}(\varphi)$ 算子代替了传统 CTL 中的路径算子 $\exists$ 和 $\forall$，表示其中状态序列满足路径公式 φ 的所有路径集合的概率满足 ∞p.

其它基本逻辑运算符如 $\wedge$、$\rightarrow$ 等可通过该运算符之间的等价运算规则而得到，如 $\text{true} = ap \vee \neg ap$，$\text{true} = \neg\text{false}$，$\Diamond\Phi = \text{true} \bigcup \Phi$；$\Phi_1 \vee \Phi_2 = \neg(\neg\Phi_1 \wedge \neg\Phi_2)$，$\Phi_1 \rightarrow \Phi_2 = \neg\Phi_1 \vee \Phi_2$，$\mathcal{P}_{\geq p}(\Box\Phi) = \neg\mathcal{P}_{\geq 1-p}(\Diamond\neg\Phi)$；$\mathcal{P}_{\infty p}(\Diamond\Phi) = \mathcal{P}_{\infty p}(\text{true} \bigcup \Phi)$ 等.

状态公式刻画状态需要满足的性质. 一个状态公式对应了满足该公式的所有状态的集合. 状态和状态公式之间的可满足关系用 $\models_s$ 表示，其规则定义如下.

定义 8.　状态公式语义. 设 $M = (S, AP, Act, R, L, v, \rho)$ 为 CTMRP 模型，s 为状态，则

$M, s \models_s \text{false}$　iff　$s \notin S$；

$M, s \models_s ap$　iff　$ap \in L(s)$；

$M, s \models_s \neg\Phi$　iff　$s \not\models \Phi$；

$M, s \models_s \Phi_1 \vee \Phi_2$　iff　$s \models \Phi_1 \vee s \models \Phi_2$；

$M, s \models_s \mathcal{S}_{\infty p}(\Phi)$　iff　$\forall d \in D. \pi^{M'}(s, Sat(\Phi)) \infty p$；

$M, s \models_s \mathcal{P}_{\infty p}(\varphi)$　iff　$\forall d \in D. Prob_d^{M,s}(s, \varphi) \infty p$.

其中，D 为某种类型的策略集，φ 为路径公式. M' 为模型 M 在策略 d 下所诱导产生的 Markov 回报模型，$Prob_d^{M,s}(s, \varphi) = Pr_d^{M',s}\{\sigma \in Path^{M'}(s) \mid \sigma \models \varphi\}$ 表示从模型 M 的状态 s 出发，满足路径公式 φ 的所有路径的集合的概率.

状态公式语义规则的第 1 条表明，状态集 S 中的所有状态均不满足命题 false，与命题逻辑中的语义规则相同. 第 2 条表明当前状态满足该状态标记集合中的任何一个原子命题；$s \models \mathcal{S}_{\infty p}(\Phi)$ 表示从状态 s 出发，最终满足状态公式 Φ 的路径集合的概率满足限定 ∞p，$s \models \mathcal{P}_{\infty p}(\varphi)$ 表示从状态 s 出发，路径规范满足 φ 的路径集合的概率满足限定 ∞p. 比如对于例 1，我们可给出如下状态公式：$success$，$lost \vee fail$，$\mathcal{P}_{<0.2}(fail \vee \mathcal{S}_{<0.1}(busy \vee lost))$.

在性能及可靠性评估中，CSRL 公式和基于路径的(Path-based)的回报变量是指定包含空间约束的性能属性的重要方式，可方便地表达多种性能规范[5]. CSRL 中的 X 和 U 算子能表达简单的路径属性，表达形式不够灵活. 本文中，我们用正则表达式或与之等价的有限自动机表示路径属性[21]，即路径应该满足的性质，使得路径的表达更加灵活，增强了路径公式的刻画能力. 在具体表达中，上述正则式的字符集为由状态和在该状态上可能触发的动作所组成的有序对的集合，则路径属性正则式可定义为 $\alpha ::= \varepsilon \mid (\Phi, b) \mid a; a \mid a\text{U}a \mid a^*$，其中，为 Φ 状态公式，b 为从满足公式 Φ 的状态出发的可能动作，ε 表示空路径，算子“;”、“U”、“$*$”分别代表顺序组合、选择及 Kleene 闭包操作[21].

定义 9.　路径公式语法，$\varphi ::= \alpha^I \mid \alpha_J$. 其中，$\alpha$ 为表示路径属性的正则式，Φ 为状态公式，I, J 为非负实数区间集，分别表示满足 α 所指定的路径属性的路径上的时间、空间约束. 为了便于分析，本文假定 I, J 为形如 $[0, s]$，$[0, t]$ 的非负区间，其中 $s, t \geq 0$.

为了简化验证过程，本文暂不考虑形如 α_J^I 的路径公式. 路径公式用来刻画 CTMRP 中的路径可能满足的性质. 与状态公式类似，一个路径公式对应于满足该公式的所有路径的集合. 路径和路径公式之间的可满足关系用 $\models_p$ 表示，规则定义如下.

定义 10.　路径公式语义. 设 $M = (S, AP, Act, R, L, v, \rho)$ 为 CTMRP 模型，σ 为 M 中路径，则

$M, \sigma \models_p \alpha^I$　iff　$\sigma \in Path^M(\alpha) \wedge \tau(\sigma) \in I$；

$M, \sigma \models_p \alpha_J$　iff　$\sigma \in Path^M(\alpha) \wedge y(\sigma, \tau(\sigma)) \in J$，

其中，$Path^M(\alpha)$ 表示模型 M 中满足 α 的路径集合，其定义参见文献[21]. 第(1)条表示满足 α 并且时间约束在区间 I 内的路径；第(2)条表明满足 α，且累计空间消耗落在区间 J 内的路径.

例 4.　考虑本文的简单通信协议，设路径规

范为

$\alpha=(init,\text{start});((try,\text{send});(fail,\text{retry}))^*;(try,\text{send})$,

表示某个任务可能经过若干次失败后最终被成功发送,则可进行如下的性能描述:

时间性能:$\mathcal{P}_{<0.2}(\alpha^{\leq 2})$刻画在 2s 内最终达到 *success* 状态的概率小于 0.2;

空间性能:$\mathcal{P}_{\geq 0.8}(\alpha_{\leq 25})$表示最终达到 *success* 状态,且累计空间资源消耗不大于 25 的概率至少为 0.8.

另外,当需要验证除了时间属性外的其它多个空间属性时,需要对路径公式进行扩展,即将原来的空间约束变化成空间约束矢量,扩展后的路径公式的形式为 $\alpha_{(J_1,J_2,\cdots,J_n)}$,对这种情况本文暂不做讨论.

5 基于模型检测的性能验证方法

5.1 模型检测的基本思想

本文用模型检测技术验证复杂系统的时间空间性能.一旦我们已经形式化地指定了性能属性的 CSRL 状态公式 Φ 以及当前考虑系统的验证模型,模型检测关键问题是求解状态集 S 中满足公式 Φ 的状态子集 $Sat(\Phi)$.其基本思想与 CTL[16] 和 CSL[20] 中情况类似,对 Φ 的子公式进行自底向上的遍历,则可满足集合 $Sat(\Phi)$可通过递归计算而得到.根据本文目的,暂不考虑稳态公式$\mathcal{S}_{\sim p}(\Phi)$.可满足集合的计算规则如下.

定义 11. 可满足集合计算规则

$Sat(\text{true})=S$,

$Sat(\text{false})=\varnothing$,

$Sat(ap)=(s\mid ap\in L(s))$,

$Sat(\neg\Phi)=S\backslash Sat(\Phi)$,

$Sat(\Phi_1\vee\Phi_2)=Sat(\Phi_1)\vee Sat(\Phi_2)$,

$Sat(\mathcal{P}_{\sim p}(\varphi))=\{s\in S\mid \sup_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p\}$

(或$\{s\in S\mid \inf_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p\}$).

由上述规则可知,除$\mathcal{P}_{\sim p}(\varphi)$外,其它算子的处理与 CTMC 或 MRM 中一样.比如 $Sat(\Phi_1\wedge\Phi_2)$可通过递归计算 $Sat(\Phi_1)$和 $Sat(\Phi_2)$而得到,$Sat(\neg\Phi)$为状态空间 S 相对于集合 $Sat(\Phi)$的补.对于算子$P_{\sim p}(\varphi)$,需要确定对于当前考虑的策略类型下的所有策略d, $\sup_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p$}或$\inf_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p$ 是否成立.直观地,这需要对所有策略进行遍历,计算满足 φ 的所有路径集合的概率,并求其上(或下)确界,进而判断是否满足限定$\sim p$.

如果比较算子为$\leq$或$<$,则

$Sat(\mathcal{P}_{\sim p}(\varphi))=\{s\in S\mid \sup_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p\}$;

如果比较算子为$\geq$或$>$,则

$Sat(\mathcal{P}_{\sim p}(\varphi))=\{s\in S\mid \inf_{d\in D}[Prob_d^{M,s}(s,\varphi)]\sim p\}$.

因此,在随机模型检测过程中,需要解满足路径公式 φ 的路径集合的概率的上(或下)确界.本文所采用方法的主要思想是求解原始验证模型 CTMRP 与表达路径属性的正则式所对应的有限自动机的积 CTMRP 模型,也即在原始模型中模拟自动机的运行,在积 CTMRP 中标注原始模型中满足自动机所规定的路径属性的所有路径,给这些路径的所有终止状态一个特殊的标记,如原子命题 *accept*[21];再根据时间或空间性能约束进一步得到满足约束的路径集合,将问题转化为积 CTMRP 中对应可达事件概率的求解,进而求可达概率的上(或下)确界.如果验证时间性能,则求解事件$\Diamond^I accept$,如果验证空间性能,则求解$\Diamond_J accept$.直观的做法是遍历 CTMRP 中的所有策略,在所诱导的连续时间 Markov 回报模型中求解概率$Prob_d^{M,s}(s,\varphi)$,进而得到$\sup_{d\in D}[Prob_d^{M,s}(s,\varphi)]$.文献[15]给出了一种能够提高计算效率的启发式算法,阐述了在验证时间性能的过程中,在所有策略下事件$\Diamond^I accept$ 的概率的上确界的计算方法,但未给出对事件$\Diamond_J accept$ 的处理.本文基于 CTMRP 中时间空间性能的对偶性质[24],给出时间空间可达概率上确界计算中的对偶性质,将 CTMRP 中$\Diamond_J accept$ 的计算转化为对$\Diamond^I accept$的求解.可达概率下确界的处理亦类似,本文不做特别讨论.

5.2 空间时间可达概率对偶性质

在系统演化过程中,连续空间资源的累积可类比于时间的推进积累,反之亦然,文献[24]在 CTMRP 模型上给出空间时间性能验证中的对偶性质.本文在该理论基础上,得到最大时间空间可达概率的对偶性质,将空间性能可达概率上确界的计算转换为时间可达概率上确界的计算.

定义 12. 对偶 CTMRP,设 CTMRP 模型 $M=(M',\rho)$满足对所有的 $s\in S$ 和 $a\in Act$,$\rho(s,a)>0$,$M'=(S,AP,Act,R,L,v)$为 M 内置 CTMDP 模型,则其对偶 CTMRP 模型定义为 $M^{-1}=(M'^{-1},\rho^{-1})$,其中,$M'^{-1}=(S,AP,Act,R^{-1},L,v,\rho^{-1})$,$R^{-1}(s,a,s')=\dfrac{R(s,a,s')}{\rho(s,a)}$, $\rho^{-1}(s,a)=\dfrac{1}{\rho(s,a)}$.

在CTMRP中存在如下的时间空间对偶性质[24]：设M^{-1}为CTMRP模型$M=(S,Act,R,L,\rho)$的对偶，则下式成立：

$$Prob_d^{M,s}(s,\mathrm{CU}_J^I B)=Prob_d^{M^{-1},s}(s,\mathrm{CU}_I^J B) \quad (1)$$

其中，$C\subseteq S$，$B\subseteq S$，$I=[0,t](t>0)$，$J=[0,r](r>0)$，U为CSL路径算子，实区间I、J分别代表U算子的时间、空间约束. 由于本文并不考虑动作上的回报，故上述定义中$\rho(s,a)>0$等同于$\rho(s)>0$.

定理1.　空间时间可达概率对偶性质. 设M^{-1}为均匀CTMRP模型M的对偶，下式成立：

$$\sup_{d\in D}[Prob_d^{M,s}(s,\Diamond_J accept)]=\sup_{d\in D}[Prob_d^{M^{-1},s}(s,\Diamond^J accept)] \quad (2)$$

证明.　设区间I为$[0,x](x>0)$，由式(1)，下式显然成立：

$$Prob_d^{M,s}(s,\mathrm{CU}_J^{[0,x]}B)=Prob_d^{M^{-1},s}(s,\mathrm{CU}_{[0,x]}^J B) \quad (3)$$

直观地，当在U算子中仅考虑空间约束，即时间约束不受限时，相当于时间约束区间为$[0,\infty)$，也即是

$$Prob_d^{M,s}(s,\mathrm{CU}_J B)=Prob_d^{M,s}(s\models\mathrm{CU}_J^{[0,\infty)}B),$$

$$Prob_d^{M^{-1},s}(s,\mathrm{CU}^J B)=Prob_d^{M^{-1},s}(s\models\mathrm{CU}_{[0,\infty)}^J B) \quad (4)$$

又因为

$$Prob_d^{M,s}(s,\mathrm{CU}_J^{[0,\infty)}B)=\lim_{x\to\infty}Prob_d^{M,s}(s,\mathrm{CU}_J^{[0,x]}B),$$

$$Prob_d^{M^{-1},s}(s\models\mathrm{CU}_{[0,\infty)}^J B)=\lim_{x\to\infty}Prob_d^{M^{-1},s}(s,\mathrm{CU}_{[0,x]}^J B) \quad (5)$$

对式(3)两边取极限$\lim_{x\to\infty}$并利用式(4)、(5)，可得

$$Prob_d^{M,s}(s,\mathrm{CU}_J B)=Prob_d^{M^{-1},s}(s,\mathrm{CU}^J B) \quad (6)$$

又因为$\Diamond_J accept=\mathrm{true}\,\mathrm{U}_J accept$，对式(6)两边取确界运算$\sup_{d\in D}[\cdots]$，得结论.　　证毕.

定理1表明，积CTMRP模型中空间性能的可达概率上确界的计算，可在其对偶CTMRP模型中，通过求解时间性能可达概率上确界而达到. 因此，对具有不确定性系统的空间性能进行分析验证时，可借助于已有的针对时间性能的分析验证方法.

5.3　CTMRP中时间可达概率分析

由前面相关描述可知，在积CTMRP中计算$\sup_{d\in D}Prob_d^{M,s}(s,\Diamond^I accept)$，需计算在所有策略下，从$s$出发最终达到$accept$状态$\{s\in S\mid accept\in L(s)\}$，且累积执行时间在$I$内的所有路径集合的概率的上确界，其中$D$为某种确定性策略的所有策略的集合，$I=[0,t]$，$t\geq 0$，$s\in S$. 存在策略$d_0$满足条件$Prob_{d_0}^{M,s}(s,\Diamond^I B)=\max_{d\in D}[Prob_d^{M,s}(s,\Diamond^I B)]=\sup_{d\in D}[Prob_d^{M,s}(s,\Diamond^I B)](B\in S)$[12]，故$\sup_{d\in D}[Prob_d^{M,s}(s,\Diamond^I B)]$应为所有策略$d$下可达事件$\Diamond^I B$的概率的最大值. 又由命题1可知，在策略$d\in D$下，CTMRP将演变成MRM.

根据互模拟等价[12]，计算从状态s出发达到目标状态$accept$的所有路径的概率$Prob_d^{M,s}(s,\Diamond^I accept)$，相当于计算在由策略$d$所诱导的Markov回报模型中，从以状态$s$作为最后一个状态的所有路径$\sigma(\sigma\in S^+)$出发，达到$\ddot{B}$状态的概率，其中$\ddot{B}$状态表示该回报模型中最后一个状态为$accept$状态的所有“路径”状态，即集合$\{\sigma\in S^+\mid accept\in L(last(\sigma))\}$[15].

考虑MD型策略：$d:S\times\{1,\cdots,k\}\to Act$. 对于某个使得$Prob_d^{M,s}(s,\Diamond^I accept)$可能取得最大值的策略$d_0$，该最大值只与其前面$k$个决策点的不确定性动作选取结果有关，其中$k$值为满足条件$\sum_{n=k+1}^{\infty}\mathrm{e}^{-\tilde{E}\cdot t}\cdot\frac{(\tilde{E}\cdot t)^n}{n!}\leq\varepsilon$的最大值[15]. 假设已经获得满足上述条件的策略d_0：$d_0(s,i)=act(s,i)\in Act(s)(0<i\leq k)$. 令$|S|\times|S|$阶矩阵$\boldsymbol{P}_i$表示由$d_0$在第$i$步所诱导的随机过程的概率矩阵.

当$s\notin B$时，动作$act(s,i)$可用逆向方式获得[15]. 从第k步$i=k$时开始，选择动作$act(s,k)\in Act(s)$满足$P_k(s,B)=P(s,act(s,k),B)=\max_{a\in Act(s)}P(s,a,B)$，即经过单个转移到达$B$状态的概率是最大的. 当$i<k$时，假设当$i<j\leq k$时，$act(s,j)$已经确定，则$act(s,i)$必须保证在策略$d:S\times\{1,\cdots,k-i+1\}\to Act$下，在最多$k-i+1$步内移动到$B$状态的概率是最大的，其中当$0<j\leq k-i+1$时，策略由$d(s,j)=act(s,i+j-1)$确定. 因此，对$i\geq 1$时，$\boldsymbol{P}_i$满足在形如$\sum_{n=i}^{k}\psi(n)\cdot\boldsymbol{P}_*\cdot\boldsymbol{P}_{i+1}\cdot\cdots\cdot\boldsymbol{P}_n\cdot\boldsymbol{i}_B$的所有向量中，向量$\boldsymbol{q}_i=\sum_{n=i}^{k}\psi(n)\cdot\boldsymbol{P}_i\cdot\boldsymbol{P}_{i+1}\cdot\cdots\cdot\boldsymbol{P}_n\cdot\boldsymbol{i}_B$是最大的，其中$\psi(n)$表示发生率为$E$时在时间$t$内$n$次事件出现的泊松概率，$\boldsymbol{i}_B$为状态空间$S$的占位向量，即如果$s\in B(s\in S)$，则$\boldsymbol{i}_B(s)$为$\mathbf{1}$，否则为$\mathbf{0}$，$|S|$阶方阵$\boldsymbol{P}_*$的定义参见文献[15]，$q_i(s)$表示在$t$个时间单位内，经过$i$至$k$步转移到达$B$状态的最大条件概率. 令$\boldsymbol{q}=\psi(0)\cdot\boldsymbol{i}_B+\boldsymbol{q}_1$，则当$s\notin B$时，$\boldsymbol{q}(s)=\psi(0)\cdot\boldsymbol{i}_B(s)+\boldsymbol{q}_1(s)=\boldsymbol{q}_1(s)(\boldsymbol{i}_B(s)=\mathbf{0})$，故须最终求解$\boldsymbol{q}_i=\psi(i)\cdot\boldsymbol{P}_i\cdot\boldsymbol{i}_B+\boldsymbol{P}_i\cdot\boldsymbol{q}_{i+1}$. 其中$k$可通过泊松过程的截取算法获得[15]，$\tilde{E}$为均匀转出率.

可通过递归算法实现向量 $\boldsymbol{q}_i=\psi(i)\cdot\boldsymbol{P}_i\cdot\boldsymbol{i}_B+\boldsymbol{P}_i\cdot\boldsymbol{q}_{i+1}$ 的计算，基于已有工作[15]，计算过程如算法 1 所示.

算法 1. 向量 $\boldsymbol{q}_i=\psi(i)\cdot\boldsymbol{P}_i\cdot\boldsymbol{i}_B+\boldsymbol{P}_i\cdot\boldsymbol{q}_{i+1}$ 求解算法.

```
compute_Vector(s,t,k,B)
//输入:初始状态,时间约束区间上界,精度,目标状态集
{
  for (;s∈S;) {q_{k+1}(s)=0;}
  for (i=k; i<=k, i--) { //后向迭代
    while (s∈S\B){
      max_value=-1;
      while (α∈Act(s)){max_value=max(m, ψ(i)·
            P(s,α,B)+Σ_{s'∈S} P(s,a,s')·q_{i+1}(s'));}
      q_i(s)=max_value;
    }
    while (s∈S\B){q_i(s)=ψ(i)+q_{i+1}(s);}
  }
  while (s∈S) {if (s∉B) q(s)=q_1(s); else q(s)=1; }
}
```

其中 $\boldsymbol{q}_i$ 中记录的是在第 i 步计算中各状态到目标状态的可达概率的最大值. 通过 $\boldsymbol{q}_i$ 即可求得可达概率的上(下)确界，算法复杂度分析参考相关文献. $\inf_{d\in D}Prob_d^{M,s}(s,\Diamond^{\leq t}accept)$ 的求解方法与之类似. 注意这里只考虑了 MD 型策略，该方法同样适应于其它相关类型策略[15].

5.4 CTMRP 时间空间性能验证算法

由德国 RWTH Aachen 大学、荷兰 Twente 大学等合作开发的模型检测器 MRMC (Markov Reward Model Checker)已经实现了 5.3 小节中的算法. MRMC 是由 C 语言开发的命令行验证工具，能运行于 Windows、Linux 等操作系统. 目前支持的验证模型有离散(连续)时间 Markov 链、Markov 回报模型和具有内部不确定性的 CTMDP 等[25]，支持的属性描述时序逻辑如 PCTL、CSL、CSRL 等. 它也是目前唯一支持 CTMDP 的验证工具. 验证过程中，需要将系统 CTMDP 模型的相关信息，如状态、状态标记、转移关系、状态回报结构等以文本文件的形式作为输入，根据从命令行输入的验证公式，得到验证结果.

但是，MRMC 目前仅支持时间有界的可达概率求解. 为了进行空间性能验证，由本文的描述可知，首先，将 CTMRP 模型均匀化，并求其对偶 CTMRP 模型；其次，在对偶 CTMRP 的内置 CTMDP 模型中，将空间性能验证转换为对应的时间可达概率的计算.

CTMRP 模型中的时间或空间性能验证算法如算法 2 所示.

算法 2. CTMRP 时间或空间性能验证算法.

```
Sat_set check_CTMRP(M,Φ)
        //输入:CTMRP 实例模型,验证公式 Φ
{       //根据本文目的,暂不考虑稳态算子 S_{∞p}(Φ)
  sat=∅;
  if (Φ∈AP)        sat={s|Φ∈L(s)};
  if (Φ=Φ1∧Φ2)     sat=check_CTMRP(Φ1)∧
                       check_CTMRP(Φ2);
  if (Φ=¬Φ1)       sat=S\check_CTMRP(Φ1);
                   //S 为 CTMRP 模型的状态集
  if (Φ=P_{∞p}(φ))) {
    if (φ=α^I){        //处理时间性能
      将 α 转化成自动机 A,求其与 CTMRP 实例 M
      的积 CTMRP 模型 M×A 并均匀化处理;
      if (∞∈{≤,<})
          { if (sup_{d∈D} Prob_d^{M×A,s}(s,◇^I accept)∞p)
              sat=sat∪{s};}
      if (∞∈{≥,>})
          { if (inf_{d∈D} Prob_d^{M×A,s}(s,◇^I accept)∞p)
              sat=sat∪{s}; }
    }
    if (φ=α_J){ //处理空间性能(转化为时间性能分析)
      将 α 转化成自动机 A,并求该自动机与 CTMRP
      实例 M 的积 CTMRP 模型 M×A 并均匀化处理;
      Get_Duality_Model ();
                   //获得积 CTMRP 模型的对偶
      if (∞∈{≤,<})
          { if (sup_{d∈D} Prob_d^{M×A,s}(s,◇^J accept)∞p)
              sat=sat∪{s}; }
      if (∞∈{≥,>})
          { if (inf_{d∈D} Prob_d^{M×A,s}(s,◇^J accept)∞p)
              sat=sat∪{s}; }
    }
  return sat;          //输出:可满足集合
  }
}
```

上述算法中，除了可达概率的计算外，对于形如 α^I 或 α_J 的路径公式，算法的复杂度分析与文献[21]中类似.

5.5 实例结果

对于本文例 1 中的简单通信协议，其 CTMRP 模型 M 如图 2 所示. 考虑例 4 中给出的性能描述，路径属性正则式 $\alpha=(init,\text{start});((try,\text{send});$

$(fail,\text{retry}))^*$；(try,send)对应的有穷自动机 A 如图 4 所示. 二者的积 CTMRP 模型 $M\times A$ 如图 5 所示，其中，阴影状态为包含有命题 $accept$ 的状态.

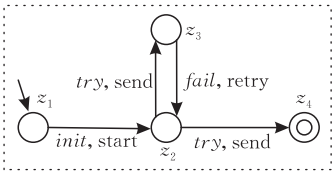


图 4　α 对应有穷自动机 A

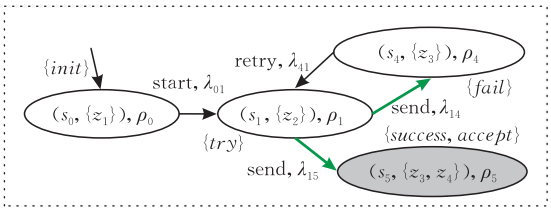


图 5　积 $CTMRP$ 模型 $M\times A$

设需要用到的原始参数值分别为

$\lambda_{01}=4$，$\lambda_{14}=2$，$\lambda_{15}=8$，$\lambda_{41}=3$，$\rho(s_0)=0.3$，

$\rho(s_1)=5$，$\rho(s_4)=15$，$\rho(s_5)=0.5$，

则 $M\times A$ 对应的对偶 CTMRP 模型 $(M\times A)^{-1}$ 中的参数值分别为

$\rho^{-1}(s_0)=1/\rho(s_0)=3.33$，$\rho^{-1}(s_1)=1/\rho(s_1)=0.20$，

$\rho^{-1}(s_4)=1/\rho(s_4)=0.07$，$\rho^{-1}(s_5)=1/\rho(s_5)=2$；

$\lambda_{01}^{-1}=\lambda_{01}/\rho(s_0)=13.33$，$\lambda_{14}^{-1}=\lambda_{14}/\rho(s_1)=0.40$，

$\lambda_{41}^{-1}=\lambda_{41}/\rho(s_4)=0.20$，$\lambda_{15}^{-1}=\lambda_{15}/\rho(s_1)=1.60$.

注意状态 $(s_5,\{z_3,z_4\})$ 没有输出转移，故不需要计算转出率.

对于时间性能公式 $\mathcal{P}_{<0.2}(\alpha^{\leqslant 2})$，可以直接进行计算. 由于比较运算算子为 $<$，须求解 $\sup\limits_{d\in D}[Prob_d^{M\times A,s}(s,\mathcal{P}_{<0.2}(\alpha^{\leqslant 2}))]$. 空间性能公式 $\mathcal{P}_{\geq 0.8}(\alpha_{\leqslant 25})$ 中比较运算算子为 $>$，故须求解 $\inf\limits_{d\in D}[Prob_d^{M\times A,s}(s,\mathcal{P}_{\geq 0.8}(\alpha_{\leqslant 25}))]=\inf\limits_{d\in D}[Prob_d^{(M\times A)^{-1},s}(s,\mathcal{P}_{\geq 0.8}(\alpha^{\leqslant 25}))]$ (转换到对偶模型 $(M\times A)^{-1}$ 中进行). 计算结果：

$$\sup_{d\in D}[Prob_d^{M\times A,s_1}(s_1,\mathcal{P}_{<0.2}(\alpha^{\leqslant 2}))]=0.187868,$$

$$\inf_{d\in D}[Prob_d^{(M\times A)^{-1},s_1}(s_1,\mathcal{P}_{\geq 0.8}(\alpha^{\leqslant 25}))]=0.563275.$$

前者表明状态 s_1 满足时间性能约束的可能性最多为 18.7868%，后者表明从 s_1 出发空间性能约束的可能性至少为 56.3275%. 因此，$Sat(\mathcal{P}_{<0.2}(\alpha^{\leqslant 2}))=\{s_1\}$，$Sat(\mathcal{P}_{\geq 0.8}(\alpha_{\leqslant 25}))=\varnothing$. 注意上面的求解式中仅仅考虑状态 s_1 的原因在于只有该状态满足路径属性正则式 α.

5.6　性能验证过程中的状态爆炸问题

在 CTMRP 模型中进行时间或空间性能验证，需要应对可能出现的状态爆炸问题，即在保证验证结果正确的前提下，缩小模型检测过程中需要遍历的状态空间. 因此，状态爆炸问题的解决方法与系统模型以及待验证的性质有关. 目前，已有多种技术可用于解决模型检测过程中的状态爆炸问题，如互模拟、抽象、on_the_fly 模型检测、基于 OBDD 的符号模型检测、定界模型检测等. 其中，抽象技术将具体状态压缩成抽象状态，以获得比较小的系统模型. 根据状态空间的划分方式，目前已经存在如对称约简、互模拟约简、偏序约简(partial order reduction)等技术[25].

偏序约简依据扫描迹等价(stuttering equivalence)理论，通过确定状态的部分且充分的后继动作集(ample set)，在搜索时仅搜索充分集中动作的后继状态，达到减小需访问的状态空间的目的[16-17]. 偏序约简技术的关键是根据验证性质定义动作独立关系和充分动作集的确定规则. 文献[26-27]研究了离散时间 Markov 过程对于 PCTL 公式的偏序约简规则，并给出了规则的正确性证明. 将 PCTL 改变为一种仅带有回报约束的空间性能属性描述语言，文献[28]提出带有回报结构的离散时间 Markov 回报过程相对于该语言所刻画的性能属性的约简规则. 连续时间的处理相对来说比较复杂. 在已有基础上，我们给出了连续时间 Markov 回报过程的偏序约简的充分集求解规则，并证明了其正确性. 有关这方面的研究工作还在进一步进行中，其结果将在后续论文中阐述.

6　结束语

互联网中存在着大量具有不确定性的复杂动态系统，本文用能够刻画行为不确定性、时间及空间性能特征的连续时间 Markov 回报过程 CTMRP 作为验证模型，并运用模型检测技术，对复杂系统的时间空间性能，进行形式化验证. 在 CTMRP 中，状态的驻留时间由状态间的转移率刻画，空间要求数据用回报结构描述，用有界的基于路径的回报变量刻画空间性能约束. 本文的空间要求数据表示当系统驻留于某状态时，单位时间内空间资源的要求量，可用于刻画系统基于空间资源的性能指标. 对 CTMRP 进行时间或空间性能验证的关键是需要求解不同策略下可达概率的上(或下)确界，在时间性能验证方

面,已经出现高效的贪婪算法.基于确定性策略,本文给出并证明空间时间可达概率对偶性质.通过使用该性质,可将空间性能验证中可达概率的计算转换成对应的时间性能可达分析.最后给出了模型检测算法.与已有的工作相比,本文探索了用模型检测技术对具有不确定性、连续时间及概率选择的复杂系统的性能进行验证或评估的方法,为复杂系统时间空间性能评估指明了新的思路和方向.特别地,本文给出了空间性能验证方法,该方法可对诸如存储、带宽、能耗等空间性能进行验证,从而给出系统性能是否满足约束的更为全面的准确判断.下一步,我们将探索对具有混合回报结构的 CTMRP 进行空间性能验证的方法,所谓混合回报结构即指状态的回报值不全为正的情况,并给出状态爆炸问题的解决思路和方法.

参 考 文 献

[1] Lin Chuang, Li Ya-Juan, Wang Zhong-Min. Status and development of formal methods for performance evaluation. Acta Electronica Sinica, 2002, 30(12A): 1917-1922(in Chinese)
(林闯,李雅娟,王忠民. 性能评价形式化方法的现状和发展. 电子学报, 2002, 30(12A): 1917-1922)

[2] Lin Chuang, Lei Lei. Research on next generation internet architecture. Chinese Journal of Computers, 2007, 30(5): 693-711(in Chinese)
(林闯,雷蕾. 下一代互联网体系结构研究. 计算机学报, 2007, 30(5): 693-711)

[3] Guo Bing, Shen Yan, Shao Zi-Li. The redefinition and some discussion of green computing. Chinese Journal of Computers, 2009, 32(12): 2311-2319(in Chinese)
(郭兵,沈艳,邵子立. 绿色计算的重定义与若干探讨. 计算机学报, 2009, 32(12): 2311-2319)

[4] Cloth L, Katoen J-P, Khattri M, Pulungan R. Model checking Markov reward models with impulse rewards//Proceedings of the International Conference on Dependable Systems and Networks(DSN'05). Yokohama, Japan, 2005: 722-731

[5] Hermanns H. Interactive Markov chains [Ph. D. dissertation]. Friedrich-Alexander University, Erlangen-Nurnberg, 1998

[6] Johr S. Model checking compositional Markov systems [Ph. D. dissertation]. Universität des Saarlandes, Germany, 2007

[7] Baier C, Haverkort B, Hermanns H, Katoen J-P. On the logical characterisation of performability properties//Proceedings of the ICALP 2000: Automata, Languages and Programming, Geneva Switzerland, 2000: 780-792

[8] Haverkort B, Cloth L, Hermanns H, Katoen J-P, Baier C. Model checking performability properties//Proceedings of the DSN 2002. Washington, USA, 2002: 103-112

[9] Niu Jun, Zeng Guo-Sun, Chen Bo. An integrated verification model atsFPM based on functional, time and spatial constraints. Chinese Journal of Computers, 2009, 32(4): 740-750(in Chinese)
(钮俊,曾国荪,陈波. 一种刻画功能和时间空间性能的统一验证模型 atsFPM. 计算机学报, 2009, 32(4): 740-750)

[10] Baier C, D'Argenio Pedro, Groesser Marcus. Partial order reduction for probabilistic branching time. Electronic Notes in Theoretical Computer Science, 2006, 153(2): 97-116

[11] Mura I, Bondavalli A. Markov regenerative stochastic petri nets to model and evaluate phased mission systems dependability. IEEE Transactions on Computers, 2001, 50(12): 1337-1351

[12] Ciardo G, Muppala J, Trivedi K S. On the solution of GSPN reward models. Performance Evaluation, 1991, 12(4): 237-253

[13] Beccuti M, Franceschinis G, Haddad S. Markov decision Petri net and Markov decision well- formed net formalisms. Lecture Notes in Computer Science, 2007, 4546: 43-62

[14] Lin Chuang, Li Ya-Juan, Shan Zhi-Guang. Performance evaluation of systems using stochastic Petri nets. Journal of Tsinghua University (Science and Technology), 2003, 43(4): 475-479(in Chinese)
(林闯,李雅娟,单志广. 基于随机 Petri 网的系统性能评价. 清华大学学报(自然科学版), 2003, 43(4): 475-479)

[15] Baier C, Hermanns H, Katoen J-P, Haverkort B R. Efficient computation of time-bounded reachability probabilities in uniform continuous-time Markov decision processes. Theoretical Computer Science, 2005, 345(1): 2-26

[16] Clarke E M, Grumberg O, Peled D A. Model Checking. Cambridge: MIT Press, 2000

[17] Baier C, Katoen J-P. Principles of Model Checking. Massachusetts: The MIT Press, 2008

[18] Puterman M L. Markov Decision Processes: Discrete Stochastic Dynamic Programming. New Jersey: John Wiley & Sons, 1994

[19] Aceto L. Action refinement in process algebras [Ph. D. dissertation]. University of Sussex, Cambridge, 1992

[20] Baier C, Haverkort B, Hermanns H, Katoen J-P. Model-checking algorithms for continuous time Markov chains. IEEE Transactions on Software Engineering, 2003, 29(6): 524-541

[21] Baier C, Cloth L, Haverkort B, Kuntz M, Siegle M. Model checking Markov chains with actions and state labels. IEEE Transactions on Software Engineering, 2007, 33(4): 209-224

[22] Dong Wei, Wang Ji, Qi Zhi-Chang. An approach of model checking UML Statecharts. Journal of Software, 2003, 14(4): 750-756(in Chinese)

(董威，王戟，齐治昌. UML Statecharts 的模型检验方法. 软件学报，2003，14(4)：750-756)

[23] Cloth L，Haverkort B，Hermanns H，Katoen J-P，Baier C. Model checking pathCSL//Proceedings of the PMCCS-6. Illinois USA，2003：19-22

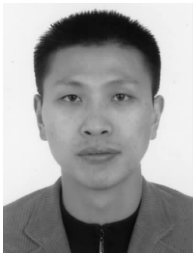
[24] Baier C，Haverkort Boudewijn R，Hermanns H，Katoen J-P. Reachability in continuous-time Markov reward decision processes//Proceedings of the Occasion of Wolfgang Thomas's 60th Birthday. Aachen Germany，2007：53-72

[25] Katoen J-P. Perspectives in probabilistic verification//Proceedings of the 2nd IFIP/IEEE International Symposium on Theoretical Aspects of Software Engineering. Nanjing，China，2008：3-10

[26] Baier C，Größer M，Ciesinski F. Partial order reduction for probabilistic systems//Proceedings of the QEST'04. Enschede Netherlands，2004：230-239

[27] D'Argenio P R，Niebert P. Partial order reduction on concurrent probabilistic programs//Proceedings of the QEST'04. Enschede Netherlands，2004：240-249

[28] Größer M，Norman G，Baier C，Ciesinski F，Kwiatkowska M，Parker D. On reduction criteria for probabilistic reward models//Proceedings of the FSTTCS 2006. Kolkata India，2006：309-320



NIU Jun，born in 1976，Ph. D. candidate，lecturer. His main research interests include model checking and performance evaluation.

ZENG Guo-Sun，born in 1964，Ph. D.，professor，Ph. D. supervisor. His research interests include model checking，high performance computing and information security.

WANG Wei，born in 1979，Ph. D.，lecturer. His main research interests include trusted software and performance evaluation.

Background

This work is supported by the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z425 and No. 2009AA012201，National Basic Research Program of China (973 Program) under grant No. 2007CB316502，the National Natural Science Foundation of China under grant No. 90718015，the joint of NSFC and Microsoft Asia Research under grant No. 60970155，the Ph. D. Programs Foundation of Ministry of Education under grant No. 20090072110035，the Program of Shanghai Subject Chief Scientist under grant No. 10XD1404400，the State Key Laboratory of High-end Server & Storage Technology under grant No. 2009HSSA06，the program for Young Excellent Talents in Tongji University under grant Nos. 0800219105 and 2009KJ030，and the Natural Science Foundation of Ningbo under grant No. 2010A610123.

An important object of these projects is to investigate how to analyze and verify complicated network system such as software，hardware，network architecture，network protocol，etc. by formal methods automatically，and come to a conclusion whether the system is secure，dependable and trustworthy. The main task is focused on verifying network system's performance and dependability by stochastic model checking. The authors use Markov Reward Model and Markov Process as the verification models.

The traditional work mainly focuses on functionality analysis of the considered network system. Concerning performance and dependability analysis approaches，there have been some existing non-formalist methods such as statistics methods etc. which are not automatic or incomplete. It is important that there are few efforts on treating non-time aspects such as memory，bandwidth，power，cost，etc. Some approaches by which we can pursue performance analysis on time or space have been existed. The time properties are described by adding time parameters on transition labels and the spatial properties are described by adding the information which expresses the constraints of spatial resource. The research group proposed several verification approaches about the web service's security by the analysis of their behavior chains patterns.

In order to depict probabilistic choices，stochastic time and nondeterminacy which network system may exhibit when running because of the dynamicity and nondeterminacy of network environment，this paper introduces continuous time Markov reward process as the performance and dependability verification model，expresses time or spatial properties by extended continuous stochastic reward logic with actions labels，and state the model checking procedure of time-interval-bounds properties. As for spatial-interval-bounds properties，the authors study time-interval- as well as spatial-interval-bounds duality by which we can treat the latter as that in the former. The results show that the approaches would be helpful to one when verifying performance and dependability of network systems.