

# 云计算环境下聚合服务的随机模型检测

钮俊<sup>1,2</sup> 曾国荪<sup>2</sup>

(宁波大学信息科学与工程学院 宁波 315010)<sup>1</sup> (同济大学计算机科学与技术系 上海 201804)<sup>2</sup>

**摘要** 当前缺乏对聚合云服务正确性、响应时间和费用约束统一进行验证的有效方法。扩展基本工作流模式,增强概率、随机、不确定选择的刻画能力,用于定义聚合云服务的服务流程,将流程定义转换为连续时间 Markov 回报过程,扩展连续随机回报逻辑 CSRL,用以刻画增强行为描述的统一验证属性,给出随机模型检测方法。分析表明,该方法能有效刻画运行时云服务动态行为并对其进行正确性、可靠性进行验证。

**关键词** 云服务,工作流,Markov 过程,随机模型检测

**中图法分类号** TP391 **文献标识码** A

## Stochastic Model Checking Composed Services in Cloud Computing Environment

NIU Jun<sup>1,2</sup> ZENG Guo-sun<sup>2</sup>

(Faculty of Information Science and Engineering, Ningbo University, Ningbo 315010, China)<sup>1</sup>

(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)<sup>2</sup>

**Abstract** The existing works can not verify whether the composed service's function, response time and cost satisfy requester's requirement simultaneously, and treat it separately. We extended basic workflow patterns in order to depict probabilistic choice, stochastic time and nondeterministic choice of composed cloud services. An approach to mapping the extended patterns to continuous time Markov reward process was proposed. The existing temporal logic CSRL was extended for specifying the specifications which can depict function, response time and cost constraints, and the stochastic model checking approach was proposed. This paper shows that we can depict cloud service's runtime dynamic behaviors effectively and verify their correctness and availability.

**Keywords** Cloud service, Workflow, Markov processes, Stochastic model checking

## 1 引言

作为一种新型计算模式,云计算已受到学术界、产业界广泛关注<sup>[1]</sup>。它提供大量虚拟资源(计算、存储、网络传输等),屏蔽细节,并作为服务(Services)对外提供。用户可通过网络按需动态集成或配置复杂 IT 应用,实现隔离关注,并根据服务类型、数量或时间等向服务提供者支付费用。

聚合云服务的正确性、响应时间和服务费用是需关注的重点方面。功能等价的不同元服务的响应时间、费用或其它 QoS(Quality of Service)指标并非等同。由不同的候选元服务的集合所表示的聚合服务实例(instance)、累积响应时间或费用等指标也是不一样的。设计阶段,通过业务流程建模技术对应用逻辑进行规范,定义服务粒间的交互、协作、通信协议。功能正确是实施的前提,功能正确而响应时间或费用不满足需求约束的云服务不具备可行性。因此,对正确性、响应时间和费用统一进行验证,是聚合服务设计阶段的关键环节。当前的绝大多数工作仅停留于功能正确性的可信验证或事后的性能分析,割裂了正确性与可行性的统一,同时,对由于云

计算环境的动态性而产生的运行时非确定行为(nondeterministic)关注不够,包括服务失效概率、响应时间的随机性和不确定选择(indeterminacy)行为等。事实上,与其它动态并发系统一样,概率性、随机性、不确定选择是聚合云服务可观行为的重要特征<sup>[2]</sup>。

运用随机模型检测技术,对复杂并发系统功能、性能进行验证,是形式化验证领域的重点研究方向之一<sup>[3]</sup>。随机模型检测以系统的随机模型作为验证对象,用状态记录、标识动态过程中的可观测阶段,状态迁移关系描述可观行为,即功能表现;验证属性由某种随机或概率时态逻辑表示。不同于服务组合中采用的 Orchestration、Choreography 技术,本文引入工作流概念,用于描述、定义聚合云服务中参与服务粒间的服务流(service flow),而非控制流或信息流。大多数流程定制语言的流程模式均可表示为顺序、分支、并发和迭代或它们的组合<sup>[4]</sup>。扩展基本流程定义模式,使其具有概率、不确定选择等的刻画能力,给出扩展流程模式的定义,探讨将它们转换为连续时间 Markov 回报过程 CTMRP(Continuous Time Markov Reward Process)的方法,并将后者作为本文的验证对象,给

到稿日期:2012-01-05 返修日期:2012-04-11 本文受 863 项目(2007AA01Z425, 2009AA012201), 973 课题(2007CB316502), 国家自然科学基金项目(90718015), NSFC-微软亚洲研究院联合资助项目(60970155), 教育部博士点基金项目(20090072110035), 高效能服务器和存储技术国家重点实验室开放基金项目(2009HSSA06), 浙江省自然科学基金项目(LY12F02007), 宁波市自然科学基金项目(2012A610062)资助。

钮俊(1976—), 博士, 副教授, 主要研究方向为可信软件、高性能计算, E-mail: tongjinj@gmail.com; 曾国荪(1964—), 博士, 教授, 博士生导师, 主要研究方向为高性能计算、信息安全。

出基于随机模型检测的服务可信验证思路和方法。

## 2 建模需求及扩展 workflow 模式

已有业务流建模技术大多以确定的方式对待业务流程,不能准确刻画复杂环境的动态性带来的非确定性以及业务本身的概率性、随机性或不确定选择行为。如在服务 Orchestration 或 Choreography 中,一般均假定服务调用效果是确定的,但由于互联网环境的不可控性,实际情况并非如此。比如由于服务中心停机、网络阻塞或服务不可控的撤离、修复时间点或无效的访问地址等,被调用服务可能无法正常工作。

概率选择用概率分布来刻画多种可能的选择方式。随机时间表明服务时间为随机变量。不确定选择意即系统行为存在多种可能结果,与概率选择不一样的是,结果并非满足概率分布,而是以不确定的方式进行选择<sup>[5]</sup>。聚合服务建模中,不确定性的应用场景体现在如下方面:调度自由,多种可能的直接后继选择之间无法用概率分布描述;实现自由,设计时的抽象,实施时可能存在多个相互可替换实例,选择结果不满足概率分布;外部环境未知,多种可能的结果依赖于系统无法掌控的环境或用户的动态选择,且不满足概率分布等。

**定义 1(服务元)** 它分布于 Internet,可被用于构造增值逻辑的服务粒,包含调用地址、服务名、响应时间、失效率、费用率等信息,表示为:

$$service_i = \langle URL, name, time, failRate, costRate, des \rangle$$

其中,  $des$  表示服务的功能性说明等信息,可作为服务选择的依据。

**定义 2(服务元失效率)** 即单位时间内的失效次数,用以刻画服务的可靠性。

**定义 3(服务元费用率)** 即单位时间内用户需支付的费用。

**定义 4(聚合云服务)** 即所有参与服务元的集合及相互之间的流程关系定义,如顺序、分支、并发、迭代。

设计阶段,常用 BPEL(Business Process Execution Language)等过程描述语言定义服务的可执行脚本,这类做法关注聚合服务的信息流、控制流,粒度较细。本文以粗粒度的方式关注聚合服务的流程,符合服务设计中隔离关注的思想。工作流概念已被成功应用于复杂系统业务流程的自动呈现<sup>[4]</sup>。我们用工作流定义参与子服务间的交互、协作关系,进而定义服务流程。首先需要为工作流基本模式添加概率、随机时间和不确定性刻画能力。

**定义 5(顺序模式  $\langle P, r \rangle$ )**  $P$  为顺序执行的进程集,  $r$  为  $P$  中元素的某个偏序定义,是一个  $|P|$  维向量,定义进程间的顺序执行关系。

多个服务元的概率分支模式指前驱活动的结果面临多个选择,且结果满足特定的概率分布,需要标记每个分支的选择概率。

**定义 6(扩展的概率分支模式  $\langle P, \mu \rangle$ )**  $P$  为进程集,  $\mu$  为集  $P$  上的概率分布,满足  $\sum_{p \in P} \mu(p) = 1$ ,  $\mu(p)$  表示执行进程  $p$  的概率。

增强概率扩展的分支模式相比于传统的分支模式具有更加丰富的表达能力。在流程的某个执行点,可能存在多个可能执行的不确定分支,每个分支的后继活动满足某个概率分布,精确定义如下。

**定义 7(扩展的不确定选择模式  $\langle \langle P_1, \mu_1 \rangle \mid \langle P_2, \mu_2 \rangle \mid \dots \mid$**

$\langle P_n, \mu_n \rangle \mid \rangle$ ) 其中有选择符号“ $\mid$ ”隔开的多个不确定选择,  $P_i, \mu_i$  分别代表不确定分支  $i$  的进程集和对应概率分布。

由于迭代体中所有服务元均一次完成执行才能被看成一次成功迭代,因此为了避免复杂性,采用与文献[6]类似的方式,设迭代出口处,退出迭代的概率为  $p$ ,则继续停留在循环体内的概率为  $1-p$ 。

**定义 8(扩展的迭代模式  $\langle P, p \rangle$ )** 其中  $P$  表示迭代体所包含的进程集合,  $p$  为一次迭代后退出迭代执行的概率。

结合本文的抽象水平假设和建模需要,由于并发体往往协同表示某种逻辑,只有所有参与者都完成,并发体才完成执行,故将并发进程作为单个服务元看待,这样便于参数标注,同时不影响验证。并发结构的失效率、修复率,可通过已有方法获得<sup>[7-10]</sup>。直观地,我们可定义上述扩展模式的 BPEL 脚本定义语法。

## 3 构造聚合云服务 Markov 模型

假定云服务在时刻  $t(t \geq 0)$  时处于状态  $X_t$ 。由于服务元执行时间的随机性以及执行结果的非确定性,在所有观测时刻  $t_1, t_2, t_3, \dots, X_t$  为随机变量,序列  $\{X_t, t=0, 1, 2, \dots\}$  为随机过程,并满足 Markov 性<sup>[8]</sup>。基于本文的验证需求,除了功能外,还需关注聚合云服务的时间、成本等性能或可靠性指标,我们采用连续时间 Markov 回报过程作为分析模型。

### 3.1 模型的基本概念及描述

**定义 9(带标记连续时间 Markov 链)** 为四元组  $(S, AP, L, R)$ , 其中  $S$  为状态集,  $AP$  为原子命题集,  $L: S \rightarrow 2^{AP}$  为状态标记函数,  $R: S \times S \rightarrow \mathbb{R}_{\geq 0}$  为转移矩阵。

**定义 10(连续时间 Markov 回报链 MRM, Markov Reward Model)** 为二元组  $(C, \rho)$ , 其中  $C$  为带标记连续时间 Markov 链, 函数  $\rho: S \rightarrow \mathbb{R}_{\geq 0}$  为状态  $s$  分配值  $\rho(s)$ , 刻画单位时间内某个非时间量如费用量、通信量、吞吐量、资源消耗量等的增量<sup>[11]</sup>。

**定义 11(聚合云服务动态模型)** 为带标记连续时间 Markov 回报过程 CTMRP:  $(S, AP, Act, R, L, v, \rho)$ <sup>[12]</sup>, 其中  $v$  为初始分布,  $Act$  为动作集,  $R: S \times Act \times S \rightarrow \mathbb{R}_{\geq 0}$  为转移矩阵, 其它元素的定义参照定义 9、定义 10。

上述定义包含两个方面:状态结构和动态行为。状态记录聚合云服务执行过程中的可观测阶段,并赋以可辨别的状态标记,标记为原子命题的集合。动态行为由转移率矩阵  $R$  描述,量化状态转移关系。如果  $\lambda = R(s, a, s') > 0$ , 则表明将发生从状态  $s$  到  $s'$  的转移,且状态  $s$  的停留时间  $t$  满足参数为  $\lambda$  的指数分布<sup>[13]</sup>, 记为:  $s \xrightarrow{a, t} s'$ 。

CTMRP 中,执行路径为转移  $s \xrightarrow{a, t} s'$  的有穷或无穷序列。有穷路径  $\sigma$  包含的转移数称为路径长度,记为  $|\sigma|$ ,  $last(\sigma)$  表示其最后一个状态,时刻  $t$  所处状态记为  $\sigma @ t$ , 可计算出该条路径所花费的总的时间和费用并分别记为  $\tau(\sigma)$ ,  $y(\sigma, \tau(\sigma))$ <sup>[6]</sup>。集合  $Act(s) = \{a \in Act \mid \exists \lambda > 0 \wedge s' \in S. R(s, a, s') > 0\}$  表示从状态  $s$  出发的可能触发的动作集并确定了状态  $s$  的所有不确定选择,即如果  $|Act(s)| > 1$ , 则将以不确定方式选择执行动作  $a \in Act(s)$ 。不确定性动作的选择方式定义称为调度(Scheduler)。在确定型调度下,连续时间 Markov 回报过程将演变成 Markov 回报模型<sup>[12]</sup>。记  $Path^M(s)$  为 CTMRP 在确定型调度下的 MRM 模型  $M$  中从状态  $s$  出发的所有路径的集合。可定义  $Path^M(s)$  上的测度空间,以为路径集合定

义概率测度  $\Pr^M(s)^{[13]}$ 。给定  $M$ , 从状态  $s$  出发, 在时刻  $t$  处于状态  $s'$  的概率  $\pi^M(s, s', t) = \Pr^M(s) \{ \sigma \in \text{Path}^M(s) \mid \sigma @ t = s' \}$  表示瞬态概率(Transient state),  $\pi^M(s, s') = \lim_{t \rightarrow \infty} (\pi^M(s, s', t))$  表示稳态概率(Steady state), 即一直停留于状态  $s'$  的概率。

### 3.2 工作流脚本到 CTMRP 模型的转换

对于以基本 BPEL 脚本呈现的服务流程, 已经存在将其转化为 LTS(Labeled Transition Systems)的方法<sup>[14]</sup>。既然 CTMRP 是 LTS 的带有时间、费用的扩展<sup>[12]</sup>, 基于已有工作, 很容易实现我们的转换。CTMRP 模型是一种基于状态的系统模型, 转换过程中, 首先需要标注聚合服务的状态空间。

模拟聚合云服务的执行过程, 根据服务元的执行阶段进行状态划分: 将服务元的整个执行过程标记为一个状态; 处于执行阶段的服务元, 称其处于活动状态, 否则称其处于非活动状态。同时, 考虑到本文的验证目标, 还需为状态添加由于失效而进行修复的修复状态, 这些状态并非为聚合服务的“真”状态, 可直接进行标记。

假定有  $m$  个参与服务元, 每个服务元  $k$  有  $n$  个操作。状态可用布尔元组表示, 即  $s = (f_1, \dots, f_i, \dots, f_m)$ , 其中  $f_i \in \{0, 1\} (1 \leq i \leq m)$ 。如果服务元  $j$  是活动的, 则  $f_j = 1$ , 否则  $f_j = 0$ 。初始状态时, 所有活动都处于非活动状态。理论上, 对于包含有  $m$  个参与服务元的聚合云服务, 最大状态数可为  $2^m$ , 随着  $m$  的增加, 可能产生状态爆炸问题。但事实上, 多个服务元同时处于活动状态的情况很少<sup>[8]</sup>, 即状态爆炸问题的实际产生几率很小。对于可能出现的状态爆炸问题, 模型验证过程中可采用一些状态约简技术, 如抽象、互模拟、等价、偏序约简等进行处理<sup>[3]</sup>。

### 3.3 聚合云服务 CTMRP 模型参数标注

第 3.2 节中对状态编码的目的是辨别服务执行中的不同阶段。为了进一步对状态的本质特征进行描述及验证的需要, 用原子命题集作为聚合云服务模型的状态标记。这些逻辑命题根据业务流程, 明确指定执行阶段。如在“酒店预订”状态, 可将其标记为集合  $\{\text{ordering\_hotel}, \dots\}$ 。CTMRP 中, 动作描述聚合云服务的可观行为, 与标记的逻辑命题一样, 遵循业务过程的表达, 用业务术语对行为动作进行标注。对服务元的失效和修复动作, 因不属于云服务的业务逻辑, 可直接进行标注。

转移率的物理意义为单位时间内转移发生的次数。同时, 它也决定了转移出发状态的驻留时间, 即被调用服务的响应时间。在顺序模式中, 各个服务元的执行阶段比较明显, 故对应状态的停留时间和费用可直接由服务元的对应参数得到。对于由多个服务元同时处于活动态而构成的“复合”状态, 其转移率和服务费用可根据已有规则计算得到, 具体细节参考文献<sup>[6, 7]</sup>。修复状态对服务请求者不产生有效费用, 费用率标记为 0。

## 4 聚合云服务验证性质描述及可满足语义

时态逻辑能够精确刻画验证性质, 也便于自动处理。连续随机回报逻辑 CSRL(Continuous Stochastic Reward logic)<sup>[15]</sup> 是对连续随机逻辑 CSL(Continuous stochastic logic)的扩展, 能够同时描述时间及费用约束<sup>[5]</sup>。本文验证目标要求能够同时刻画聚合云服务的行为、响应时间或费用约束, 考虑到通用性, 与文献<sup>[16]</sup>的做法类似, 采用扩展的基于动作的 CSRL 作为聚合云服务的验证性质描述语言。

聚合云服务的行为体现为其对应 Markov 回报过程中的路径集合。因此, 行为需要满足的性质可通过规定执行路径中动作序列或状态序列的特征来刻画。尽管状态序列也可描述服务动态行为的时序特征, 但为了直观地刻画聚合服务的业务流程, 以便于理解, 我们采用动作序列来体现系统的动态行为。路径信息包括两个部分: 动作序列以及该路径的累计执行时间和累积回报量。在刻画路径性质的时候, 这两个方面都要包括进来。完成相同行为的路径的时间或空间量可能不一样, 先规范动作序列。由于多个不确定选择动作的存在, 在刻画路径属性时, 需要同时包含当前状态以及从该状态出发选择的执行动作。因此, 路径应该为形如  $(\Phi, \text{action})$  的序列, 即同时包含动作标记和状态标记, 其中  $\Phi$  为状态标识, 即下文中的状态公式,  $\text{action} \in \text{Act}$  表示动作。

**定义 12** 带有状态标记和动作标记的扩展状态为元组  $(\Phi, \text{action})$ , 其中,  $\Phi$  为状态公式,  $\text{action}$  为从  $\Phi$  状态(满足  $\Phi$ )出发的可能选择动作, 模型中的所有扩展状态集定义为  $\text{States}$ 。

**定义 13** 路径行为属性用正则式表示, 符号集为  $\text{States} \cup \{\epsilon\}$ ,  $\epsilon$  表示空路径, 组合规则可表示为  $\alpha; \alpha, \alpha \cup \alpha$  或  $\alpha^n (n \in \mathbb{N})$ , 分别代表顺序、选择及循环。

传统模型验证中, 功能分析模型 LTS 的功能性质一般用 LTL(Linear Temporal Logic)、CTL(Computation Tree Logic)等刻画。由于某种程度上时态逻辑公式与自动机的语义等价性, 同时, 正则式也与自动机等价, 因此, 上述表示方法是完备的。基于已有技术, 容易实现正则式到自动机的转换<sup>[16]</sup>。

**定义 14(路径属性)** 聚合服务路径行为属性及刻画路径应该满足的响应时间或费用约束, 用  $\varphi ::= a^T \mid a^C \mid a^{\bar{C}}$  表示。其中,  $a$  为路径行为属性正则式,  $\Phi$  为状态公式,  $T, C$  为非负实数区间, 分别表示响应时间或费用约束。为了便于分析, 假定  $T, C$  为形如  $[0, t], [0, r] (t, r \geq 0)$  的非负实数区间。

路径属性刻画路径需要满足的性质, 对应于满足该属性的所有路径的集合。路径和路径属性之间的可满足关系用  $\models_p$  表示。设  $M$  为 CTMRP 模型,  $\sigma$  为  $M$  中路径, 则:

$$M, \sigma \models_p a^T \text{ iff } \sigma \in \text{Path}^M(a) \wedge \tau(\sigma) \in T$$

$$M, \sigma \models_p a^C \text{ iff } \sigma \in \text{Path}^M(a) \wedge \gamma(\sigma, \tau(\sigma)) \in C$$

$$M, \sigma \models_p a^{\bar{C}} \text{ iff } \sigma \in \text{Path}^M(a) \wedge \tau(\sigma) \in T \wedge \gamma(\sigma, \tau(\sigma)) \in C$$

其中,  $\text{Path}^M(a)$  表示  $M$  中满足  $a$  的路径集合, 其定义参见文献<sup>[16]</sup>。第(1)条表示行为属性满足  $a$  并且累计响应时间落在区间  $T$  内的路径集; 第(2)条表明行为属性满足  $a$ , 且累计费用落在区间  $C$  内的路径集; 第(3)条表明行为属性满足  $a$ , 且累计响应时间和费用分别落在区间  $T, C$  内的路径集。

**定义 15** 状态需要满足的性质用状态公式刻画, 语法为  $\Phi ::= \text{false} \mid ap \mid \neg \Phi \mid \Phi \wedge \Phi \mid S_{\infty p}(\Phi) \mid P_{\infty p}(\varphi)$ , 其中,  $\Phi$  为状态公式,  $\neg, \wedge$  为命题逻辑运算符,  $\in \{ \leq, \geq, <, > \}$  为比较运算符, 概率值  $p \in [0, 1]$  表示可靠性精度;  $\text{false}$  为逻辑“假”值,  $ap$  为原子命题; 稳态算子  $S_{\infty p}(\Phi)$  表示最终停留于  $\Phi$  状态的路径集合的概率满足  $\infty p$ ; 瞬态算子  $P_{\infty p}(\varphi)$  表示路径属性满足  $\varphi$  的所有路径的集合的概率满足  $\infty p$ 。其它逻辑运算符可通过等价运算规则化归为上述表示的组合。

状态公式对应于满足该公式的所有状态的集合, 该可满足关系用  $\models_s$  表示。上述基本状态公式的可满足语义规则是显然的, 如  $M, s \models_s \text{false}$  当且仅当  $s \notin S, M, s \models_s ap$  当且仅当

$ap \in L(s)$ 等。对于瞬时算子  $P_{\infty p}(\varphi)$ , 相对比较复杂, 其可满足语义定义为:  $M, s \models P_{\infty p}(\varphi)$  当且仅当  $\forall d \in D. \text{Prob}_d^{M,s}(s, \varphi) \propto p$ , 其中,  $D$  为调度集(暂考虑确定型调度),  $\varphi$  为路径公式。 $M'$  为模型  $M$  在调度  $d$  下所诱导产生的 Markov 回报模型,  $\text{Prob}_d^{M',s}(s, \varphi) = \text{Pr}_d^{M'}\{\sigma \in \text{Path}^M(s) \mid \sigma \models_p \varphi\}$  表示从模型  $M$  的状态  $s$  出发, 满足路径公式  $\varphi$  的所有路径的集合的概率。

## 5 聚合云服务随机模型检测过程

获得云服务的形式化模型和验证性质的精确描述后, 可运用模型检测技术验证其功能性能。通过遍历聚合云服务模型的所有状态, 最终获得满足验证性质的状态集<sup>[3]</sup>。

由扩展 CSRL 状态公式的可满足语义, 命题 *false*、原子命题和基本逻辑算子  $\neg$ 、 $\wedge$  以及稳态算子  $S_{\infty p}(\Phi)$  的处理与 CSL<sup>[13]</sup> 中一样, 如  $\text{Sat}(\Phi \wedge \Psi)$  为  $\text{Sat}(\Phi)$  和  $\text{Sat}(\Psi)$  的交集, 瞬时算子  $P_{\infty p}(\varphi)$  的处理类似于文献[16]中的做法。首先将路径行为正则式转换成与之等价的自动机, 求 CTMRP 模型与自动机的积, 将原始模型中的验证转换成积模型中的可达概率分析, 进一步地, 转化为积模型中的可达性质  $\diamond^T$ 、 $\diamond_c$ 、 $\diamond_{\bar{c}}$  上下确界的求解<sup>[12]</sup>。第一种情况可借助于模型检测工具 MRMC (Markov Reward Model Checker) 实现, 基于时间空间约束可达概率对偶性<sup>[15]</sup>, 第二种情况也可转换为第一种进行求解。对于第三种情况, 我们正在研究求解的启发式算法。

整个模型检测过程为: 首先根据需求, 设计聚合服务的流程定义; 运用已有技术, 将流程定义转换为 CTMRP 模型; 用扩展的 CSRL 逻辑表示系统需满足的性质; 将模型和性质描述作为模型检测工具或算法的输入, 得到验证结果。如果当前模型不满足期望性质, 则修改设计, 为实施提供有效的可信保证。验证过程如图 1 所示。与已有工作相比, 其不仅能够同时验证聚合服务的流程正确性, 同时还能够对服务调用可能产生的费用约束进行判定, 从而全面给出聚合服务的可信判断。

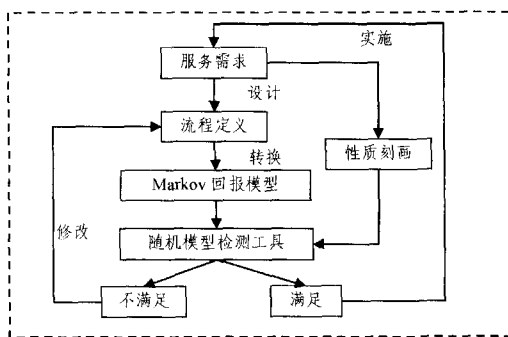


图 1 聚合云服务模型检测过程

**结束语** 将费用约束引入到聚合服务的验证过程, 提出设计阶段功能性能统一的模型检测思路和方法。扩展基本流程模式, 使其能够刻画概率、随机及不确定性。将扩展的流程定义模式转换成连续时间 Markov 回报过程, 作为功能、响应时间或费用约束的统一验证模型, 并运用时态逻辑对服务性质进行精确描述。和已有工作相比, 本文关注服务的真实动态行为, 克服了传统方法中功能正确性与响应时间可满足性隔离验证且无法有效融合服务费用分析的困难, 为云服务的实施提供了可信保证。

## 参考文献

[1] Buyya R, Yeo C S, Venugopal S, et al. Cloud computing and e-

merging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility[J]. Future Generation Computer Systems, 2009, 25(6): 599-616

- [2] Doshi P, Goodwin R, Akkijaru R, et al. Dynamic Workflow Composition using Markov Decision Processes [J]. International Journal of Web Services Research, 2005, 2(1): 1-17
- [3] Baier C, Katoen J-P. Principles of Model Checking [M]. Massachusetts: The MIT Press, 2008
- [4] Aalst V D, Wil M, Hofstede T, et al. Workflow Patterns [J]. Distributed and Parallel Databases, 2003, 14(1): 5-51
- [5] Puterman M L. Markov Decision Processes: Discrete Stochastic Dynamic Programming [M]. New Jersey: John Wiley & Sons, 1994
- [6] Gao A Q, Yang D Q, Tang S W, et al. Web service composition using Markov decision processes [C] // Fan WF, Wu ZH, Yang J, eds. Proc. the 6th Int'l Conf. on Web-Age Information Management. LNCS 3739, 2005: 308-319
- [7] Gao A Q, Yang D Q, Tang S W, et al. Mining Models of Composite Web Services for Performance Analysis [C] // Proc. the 6th Int'l Conf. on Web-Age Information Management. LNCS 3882, 2006: 828-837
- [8] Klingemann J, Wäsch J, Aberer K. Deriving Service Models in Cross-Organizational Workflows [C] // Proc. RIDE-VE '99. Sydney, Australia, March 1999: 100-107
- [9] Gallotti S, Ghezzi C, Mirandola R, et al. Quality prediction of service compositions through probabilistic model checking [C] // Proc. 4th International Conference on the Quality of Software Architectures. LNCS 5281, Karlsruhe Germany, Springer, October 2008: 119-134
- [10] Dong Yu-xiang, Xia Yun-ni, Zhu Qing-sheng, et al. A Stochastic Approach to Predicting Performance of Web Service Composition [J]. Journal of Computers, 2009, 4(6): 485-493
- [11] 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 [J]. 计算机学报, 2009, 32(4): 740-750
- [12] Baier C, Hermanns H, Katoen J P, et al. Efficient computation of time-bounded reachability probabilities in uniform continuous-time Markov decision processes [J]. Theoretical Computer Science, 2005, 345(1): 2-26
- [13] Baier L C, Haverkort B, Hermanns H, et al. Model-Checking algorithms for continuous time Markov chains [J]. IEEE Transaction on Software Engineering, 2003, 29(6): 524-541
- [14] Mongiello M, Castelluccia D. Modelling and verification of BPEL business processes [C] // Proc. the Fourth Workshop on Model-Based Development of Computer-Based Systems and Third International Workshop on Model-Based Methodologies for Pervasive and Embedded Software. IEEE, 2006
- [15] Baier C, Haverkort B, Hermanns H, et al. On the Logical Characterisation of Performability Properties [C] // Proc. ICALP 2000: Automata, Languages and Programming. Geneva Switzerland; Springer Berlin/Heidelberg, 2000: 780-792
- [16] Baier C, Cloth L, Haverkort B, et al. Model Checking Markov Chains with Actions and State Labels [J]. IEEE Transactions on software engineering, 2007, 33(4): 209-224
- [17] Katoen J P. Perspectives in probabilistic verification [C] // Proc. 2nd IFIP/IEEE International Symposium on Theoretical Aspects of Software Engineering, Nanjing China, 2008. New York: IEEE CS Press, 2008: 3-10