

8-14-2020

SMT Bounded Constrained Non Centralized Automaton Web Service Model Checking

Wei Rong

1. College of Humanities , Qinzhou University, Qinzhou 535000, China;;

Xibing Shen

1. College of Humanities , Qinzhou University, Qinzhou 535000, China;;

Yang Yi

2. College of Software, Guangxi University of Science and Technology, Liuzhou 545006, China;

Follow this and additional works at: <https://dc-china-simulation.researchcommons.org/journal>



Part of the [Artificial Intelligence and Robotics Commons](#), [Computer Engineering Commons](#), [Numerical Analysis and Scientific Computing Commons](#), [Operations Research](#), [Systems Engineering and Industrial Engineering Commons](#), and the [Systems Science Commons](#)

This Paper is brought to you for free and open access by Journal of System Simulation. It has been accepted for inclusion in Journal of System Simulation by an authorized editor of Journal of System Simulation.

SMT Bounded Constrained Non Centralized Automaton Web Service Model Checking

Abstract

Abstract: In model checking for web services applications, the combination of traditional finite state machine cannot guarantee the correctness of web service composition, *a method of non centralized automaton model for web service detection algorithm was put forward, based on which could meet of mode theory (satisfiability modulo of the nanocomposite, SMT)*. The SMT was used to detect the bounded model of timed automata, and the time automaton was directly converted into SMT identifiable logic formula and was solved; using the SMT timed automata theory, implementation of employee travel arrangements for composite web service was modeled and verified. Through the example analysis, verification of the algorithm in the lifting path deadlocks and network parameters optimization is effective.

Keywords

satisfiability modulo theories, automata, Web service, model checking, big data

Recommended Citation

Wei Rong, Shen Xibing, Yang Yi. SMT Bounded Constrained Non Centralized Automaton Web Service Model Checking[J]. Journal of System Simulation, 2016, 28(9): 2283-2288.

SMT 有界约束非集中自动机 web 服务模型检测

韦容¹, 申希兵¹, 杨毅²

(1.钦州学院人文学院, 广西 钦州 535000; 2.广西科技大学软件学院, 广西 柳州 545006)

摘要: 针对 web 服务模型检测应用中, 传统的有限状态机的组合方式无法保证 Web 组合服务的正确性问题, 提出一种基于可满足性模理论(satisfiability modulo theories, SMT)的非集中自动机的 web 服务模型检测算法。利用 SMT 对时间自动机进行有界模型检测, 将时间自动机模型直接转换成 SMT 可识别的逻辑公式, 并进行求解; 利用所提 SMT 时间自动机理论, 实现对雇员出差安排组合 web 服务进行建模和验证; 通过实例分析, 验证了算法在解除路径死锁及网络参数指标优化上的有效性。

关键词: 可满足性模理论; 自动机; web 服务; 模型检测; 大数据

中图分类号: TP391

文献标识码: A

文章编号: 1004-731X (2016) 09-2283-06

SMT Bounded Constrained Non Centralized Automaton Web Service Model Checking

Wei Rong¹, Shen Xibing¹, Yang Yi²

(1. College of Humanities, Qinzhou University, Qinzhou 535000, China;

2. College of Software, Guangxi University of Science and Technology, Liuzhou 545006, China)

Abstract: In model checking for web services applications, the combination of traditional finite state machine cannot guarantee the correctness of web service composition, a method of non centralized automaton model for web service detection algorithm was put forward, based on which could meet of mode theory (satisfiability modulo of the nanocomposite, SMT). The SMT was used to detect the bounded model of timed automata, and the time automaton was directly converted into SMT identifiable logic formula and was solved; using the SMT timed automata theory, implementation of employee travel arrangements for composite web service was modeled and verified. Through the example analysis, verification of the algorithm in the lifting path deadlocks and network parameters optimization is effective.

Keywords: satisfiability modulo theories; automata; Web service; model checking; big data

引言

Internet中存在的可用Web服务可利用整合分布方式, 实现分布式应用的服务体系结构^[1]。通常基于工作流实现方式, 来对基本Web组合服务的增值组合, 建立不同服务器分布服务调用引擎。传统工作流方式是集中式调用方式, 需要在执行过程中

对所有通信信息进行调用和转发, 故而需要极大通信开销。因此, 相对集中式, 非集中式操作方式具备更好的操作性能^[1]。

时间自动机是一种特殊的对实时系统进行描述的有限自动机, 其带有实数域时钟。这种特点使其在现实中有广泛应用价值, 如电梯、网络、航空等领域, 在本文的Web服务组合优化中也可适用, 并且由于安全性要求较高, 因此研究意义更高。尽管时间自动机对实时系统具有很好的描述性能, 但是由于时钟存在, 导致其存在无限迁移域, 特别在web服务组合优化中, 存在效率不高的问题, 为此



收稿日期: 2015-06-10 修回日期: 2015-07-24;
作者简介: 韦容(1982-), 女, 广西上林, 硕士生, 高工, 研究方向为网络安全及系统分析、计算机图形学; 申希兵(1981-), 男, 山东沂水, 硕士, 讲师, 研究方向为地理信息系统; 杨毅(1975-), 男, 广西贵港, 硕士, 讲师, 研究方向为人工智能。

<http://www.china-simulation.com>

• 2283 •

需事先对时钟变量进行预处理,使其转化为有限迁移域^[2]。

早期研究成果对于该问题的研究,集中在将时间域进行等价区域划分,如文献[3]利用不一致约束矩阵对等价划分区域进行描述,构建有限区域图。文献[4]提出的有限模型区域图检测方法等。但问题是区划数量随时钟增加指数性增加,为解决此问题,文献[5-7]提出不同解决方案,都是基于对时钟预处理实现,但问题是对内存容量要求较高,增加计算负担,特别针对Web服务大数据组合优化的大数据实际应用问题受限。

对此本文基于可满足性模理论对时间自动机有界模型进行预处理,通过解决逻辑可满足性难题,实现逻辑公式对时间自动机表示,这种方式的实现无需时钟预处理和变量布尔化。

1 web 组合服务问题描述

1.1 有限自动机

Internet中Web服务组合优化的关键性问题是降低人工参与度,其在执行时多个基本服务间进行数据的相互传递,Web服务组合优化可基于一组状态迁移进行表达,具体过程为,从其他服务获取输入信息,经过处理后将信息进行转发广播,类似于一种输入输出顺序信息传递链,这与有限自动机特点极为近似,因此利用有限自动机进行模型检测和表达非常适合^[8]。有关定义如下^[8-9]:

定义1: 有限自动机五元组表达形式为: $A=(S,S^0,I,O,\Delta)$, 其中, S 是自动机状态集合, $S^0 \subseteq S$ 是状态集合的初始状态, I 和 O 分别为自动机的输入输出集合, 转换集合可表示为 $\Delta \subseteq S \times \bar{I} \times \bar{O} \times S$, $\Delta=(s,i,o,s')$ 表示转换初始状态为 $s \in S$, $i \in \bar{I}$ 是输入, $o \in \bar{O}$ 为输出, $s' \in S$ 为目的转换状态, 可表示为: $s \xrightarrow{i/o} s'$, $(s,i,o,s') \in \Delta$ 。

图1给出有限自动机的非集中执行方式,服务s3可基本服务r1,r2,r3表示,有限自动机的非集中执行方式,将整个自动机输入或输出看作目标自动机的输入或输出。

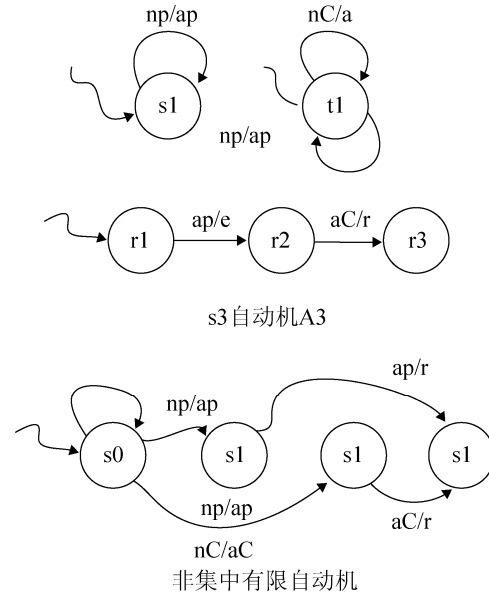


图1 非集中式有限自动机

1.2 Web服务易货交易系统结构

易货交易系统是典型的Web组合服务,其非集中执行方式如图2所示。

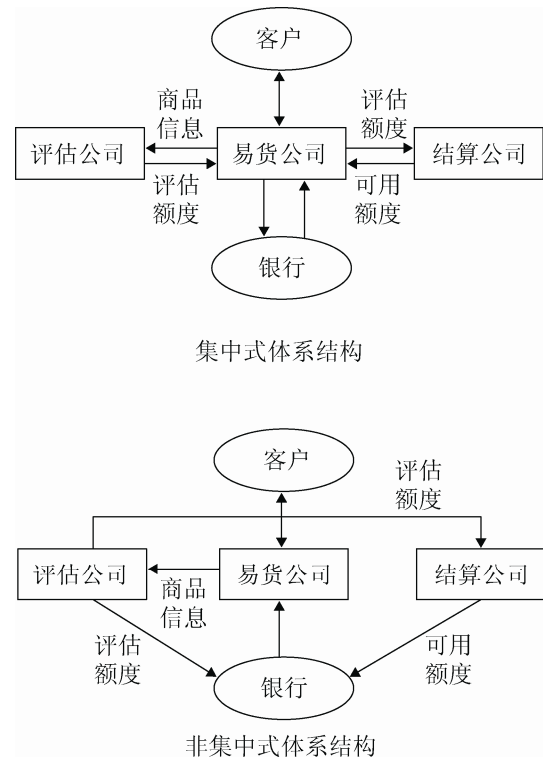


图2 易货交易系统结构

具体执行步骤为:客户在易货公司节点进行商品发布,并经易货公司商品审核,第一步将商品信

息由客户端传递至评估公司, 由其进行额度评估, 并将其反馈至易货公司。第二步通过易货公司将额度信息转发至结算公司, 由其扣除佣金后, 反馈可用额度至易货公司。最后一步是易货公司将评估及可用的额度传递至银行, 由其为客户制定信用及交易额度。上述系统由评估公司、结算公司及银行三部分Web服务组成, 并可作为一个模块供易货公司调用^[10]。

图2中展示了易货交易Web组合服务的集中和非集中执行形式, 通过对比可见非集中易货交易体系结构的消息传递数量要明显少于集中式的易货交易体系结构, 因此这种方式的Web组合服务形式具有更高的执行效率。

2 SMT 时间自动机

2.1 SMT有界模型检测

给定有限模型 M 以及模型性质 f , 则模型检测问题可归结为模型 M 是否满足模型性质 f 。传统的模型生成方式所获取的状态空间一般较大, 受制于计算硬件条件, 对于Web组合服务的大数据形式来说, 传统模型检测方式并不实用。为解决该问题, 有界检测模型方式可较为有效的解决该问题, 文献[11]给出这种模型检测方式的执行思路: 对于普通模型检测的存在性问题 $M \models Ef$, 可在有限执行步骤内寻找到实例, 满足模型 M 满足性质 f 。对于给定的 k , 上述模型检测问题可构建可满足性逻辑公式问题。若满足条件 $[M, f]_k$, 则证明上述 k 步骤内寻找到满足条件实例成立, 并且同步证明了模型 M 满足模型性质 f 。否则, 上述 k 步骤内无法寻找到满足条件实例, 但无法证明 $k' > k$ 时是否可寻找到满足条件实例。

通常做法是, 逐步增加 k 值, 直至寻找到满足条件实例, 或者达到最大执行步骤。这种检测方式无需在整个状态空间中进行展开执行, 可有效节省计算存储空间, 对此在进行时间自动机验证时, 无需时钟预处理即可获得时间自动机有限空间。这种

方式需依赖对逻辑公式进行求解, 因此需要将上述时间自动机模型转化为逻辑模型形式, 且需要将变量进行布尔形式化, 不利于算法实现的简化。

可满足性模理论(SMT)可处理整数或实数等非布尔变量逻辑公式, 对此, 本文提出一种非变量布尔化有界时间自动机模型检测, 并且将该模型应用到Web组合服务优化应用中。

2.2 M模型k步路径逻辑公式

假定 $M = \langle A_0, A_1, \dots, A_n \rangle$ 为时间自动机模型, 其中 $A_i = (\Sigma^i, S^i, S_0^i, X^i, I^i, T^i)$ 。令命题为 $f = EFp | AGp$, 其中 $p = a | \neg p | p_1 \wedge p_2 | p_1 \vee p_2$, 式中 a 是原子命题。构建时间自动机的逻辑公式形式为 $[M, f]_k$, 令 $[M]_k$ 表示为时间自动机可行路径, 并将模型性质 f 表达成 $[f]_k$ 形式。

那么时间自动机模型下, 有穷 k 步序列状态形式为: $(s_0, v_0) \xrightarrow{d_0} (s_1, v_1) \xrightarrow{d_1} \dots \xrightarrow{d_{n-1}} (s_k, v_k)$, 其中 (s_0, v_0) 为有穷序列的初始路径点, $[M]_k$ 的组成部分如下:

(1) 初始路径点 (s_0, v_0) : $\text{Init} = \text{Init}_0 \wedge \dots \wedge \text{Init}_{n-1}$, 其中:

$$\text{Init}_i = [\bigvee_{s \in S_0^i} (s_0 = s)] \wedge [\bigvee_{t \in X^i} (t = 0)] \quad (1)$$

公式(1)中, 给定自动机 j 的初始路径点, 且将时钟初始值设定成0状态。

(2) 中间量状态 (s_i, v_i) :

$$\begin{cases} \text{Const}_i = \text{Const}_i(0) \wedge \dots \wedge \text{Const}_i(n-1) \\ \text{Const}_i(j) = \left[\bigvee_{s \in S_0^i \wedge S \neq S_\mu} (s_0 \neq s_v) \right] \wedge I^i(S_\mu) \end{cases} \quad (2)$$

公式(2)中, $\text{Const}_i(j)$ 自动机 j 的状态 i 变量约束。 t_i 为时钟 t 的第 i 状态值。 $t_i \geq 0$ 表明时钟状态的非负性。 S_i 为第 i 系统状态位置。其余部分用来保证自动机状态的位置唯一性, 且状态 $I^i(S_\mu)$ 的不变性。

(3) 序列 i 步骤: $(s_i, v_i) \xrightarrow{d_i} (s_{i+1}, v_{i+1})$: $\text{step}_i = \text{step}_i(j) \wedge \dots \wedge \text{step}_i(n-1)$, $i \in [0, k-1]$, 其中变量:

$$\text{step}_i(j) = \bigvee_{T_\mu} (\text{Exl}_\mu^j(i) \wedge T_\mu^j(i) \wedge d_i > 0) \quad (3)$$

$$\text{Exl}_\mu^j(i) = \bigwedge_{T_\mu} \neg a_\nu^i \quad (4)$$

$$T_\mu^j(i) = \neg a_\nu^i \wedge (s_i = s_\mu) \wedge \bigwedge_{t \in X_f} (t_{i+1} = t_i + d_i) \quad (5)$$

$$T_\mu^j = a_\nu^i \wedge (s_i = s_\mu) \wedge \bigwedge_{t \in \lambda_\mu^f} (t_{i+1} = 0) \wedge \bigwedge_{t \notin \lambda_\mu^f} (t_{i+1} = t_i + d_i) \quad (6)$$

式中 step_i 为模型的迁移过程 i ，实质上是所有自动机在步骤 i 的迁移 $\text{step}_i(j)$ 的并集。 d_i 为系统的时钟延迟。公式(4)为所有自动机互斥的内部迁移，这种限制保证每个自动机在一个周期内只能迁移一步。而公式(5)和公式(6)分别给出时延迁移和动作迁移。根据 step_i 可以获取自动机在第 k 步的路径为 $\text{Path}_k = \bigwedge_{i \in [0, k]} \text{step}_{ii}$ 。

那么时间自动机的逻辑公式模型可表示为：

$$[[M, f]]_k = \text{Init} \wedge \bigwedge_{i \in [0, k]} \text{Const}_i \wedge \text{Path}_k \quad (7)$$

2.3 SMT逻辑公式求解

基于逻辑公式模型的可达性， $f = EFp$ 为自动机运行的状态成立路径，由此可得如下条件 $[[f]]_k = \bigvee_{i \in [0, k]} [[p]]_k$ 成立，其中 $[[p]]_k$ 可基于逻辑转换，如 $[[\neg a \wedge (b \vee c)]]_k = \neg a_i \wedge (b_i \vee c_i)$ 。而对于模型的安全性 $f = AGp$ ，则与模型可达性正好相反，表明路径所有状态 p 均成立。对此可利用取反操作实现模型可达性与模型安全性的相互转化。若 $f' = EF\neg p$ 模型性质成立，则存在路径满足模型性质 $\neg p$ ，说明模型性质 f 不成了，反之， f' 不满足同步证明自动机模型性质 f 成立。

SMT是一种解决逻辑命题的实用工具，可进行含非布尔变量逻辑问题解决，比如SMT算法不仅可用来解决形如 $\neg a \wedge (b \vee c)$ 逻辑问题，还可解决 $(a + b > 3) \wedge (a > 2)$ 含整数等非布尔变量逻辑问题，可简化模型检测。

逻辑验证过程以模型 M 、模型性质 f 以及执行步骤上限 K 作为输入，对于 $k < K$ ，其对应逻辑问

题公式为 $[[M, f]]_k = [[M]]_k \wedge [[f]]_k$ ，基于SMT工具进行求解，若得到的结果输出为 **unsat**，则 $k = k + 1$ ，直到寻找到输出为 **sat** 或满足执行步骤上限 K 。若无法寻找到 **sat** 结果则说明， K 执行过程内安全性满足可达性不满足，反之说明可达性满足安全性不满足。

3 实验与结果分析

3.1 算法模型检测

选取文献[12]算法进行实验对比，该算法特点是自动机合时钟的同步建模。其适用性较为广泛，比如含时钟量系统，并可实现多线程系统变量共享机制。对比实验的计算机硬件条件设置为：CPU处理器：Intel i3 2.4 GHz，内存为6G RAM，操作系统为Ubuntu，选取测试对象如图3所示。运行时间对比结果见表1所示。

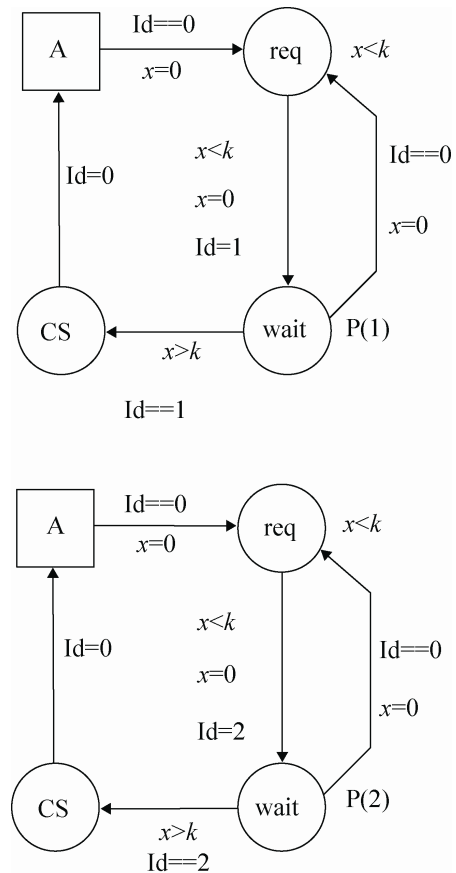


图3 测试对象

表1 运行时间对比

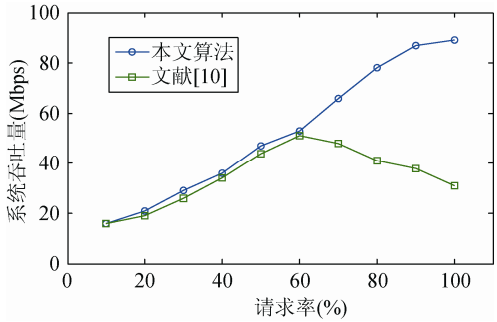
同步进程数	本文算法	文献[10]算法
3	0 m 0.324 s	0 m 0.025 s
4	0 m 0.236 s	0 m 0.053 s
5	0 m 0.323 s	0 m 0.055 s
6	0 m 0.442 s	0 m 0.112 s
7	0 m 0.712 s	0 m 0.298 s
8	0 m 1.464 s	0 m 1.357 s
9	0 m 3.367 s	0 m 5.795 s
10	0 m 8.258 s	0 m 24.653 s
11	0 m 25.580 s	1 m 37.951 s
12	2 m 49.638 s	6 m 43.834 s
13	9 m 14.344 s	Time>60 m

表1给出本文算法执行时间实验结果与文献[12]算法运行所获得的计算时间结果的对比情况。实验结果显示,基于SMT算法理论的时间自动机模型检测的计算时间与文献[12]算法计算时间相比,在并行进程数较少情况下,优势并不明显,但是随着自动机模型进程数的增加,基于SMT算法理论的时间自动机模型检测算法在计算时间上要明显优于文献[12]算法。这说明本文算法更适合Web服务组合优化这种大数据问题处理。

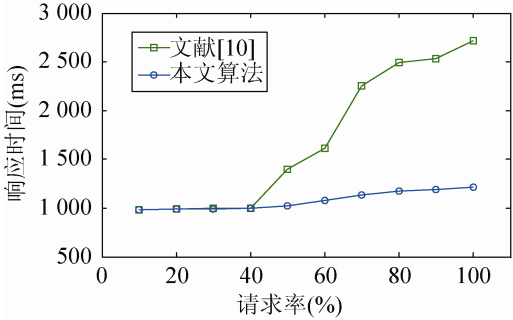
3.2 Web服务应用实验

仿真实例采用如图2的易货交易系统结构,在Web服务组合优化问题中,服务响应时间以及网络吞吐量是常用的两个评价指标。对比本文所提Web服务组合优化模型和文献[12]时间自动机模型,在图2所示的易货交易中的性能表现,仿真对比结果如图4所示。

图4给出易货交易系统中本文算法与文献[12]算法的系统吞吐量和相应时间对比情况。从图4(a)可看出,在请求率较低时中本文算法与文献[12]算法的系统吞吐量指标相差不大,其中本文算法略优于文献[12]算法,当请求率达到60%时,文献[12]算法的处理性能达到饱和放那极限,此后的请求处在等待状态,并且随着请求的增大,网络吞吐量数量逐渐降低。而本文算法的系统吞吐量是随着请求的增加逐渐增加,侧面说明网络的通畅性。



(a) 系统吞吐量



(b) 响应时间

图4 易货交易系统响应指标对比

在网络响应时间对比指标中,请求数量较少时,本文算法与文献[12]算法的网络响应时间指标相差不大,在请求率到达系统承载量的40%时,文献[12]算法的响应时间随着请求率的增加而迅速增大。而本文算法的响应时间随着请求率的增加而变化不大,也体现了网络系统的运行通畅性。

4 结论

本文基于 SMT 对时间自动机进行有界模型检测方法,对 web 服务组合问题进行优化,并基于非集中式控制方式,把有限自动机模型通过非集中模型形式进行执行,Web 服务基本通信过程通过自动机状态迁移过程实现。基于闭包自动机传递方式实现各状态迁移模拟,并把服务、目标以及通信成本作为模型输入参数。通过仿真对比,显示了本文所提算法在易货交易模型中应用的有效性,验证了本文算法的性能指标优越性。由于实际应用中,还存在服务间的访问权限问题,对于实际的执行性能存在不确定影响。今后,研究方向是对于大量 Web 服务组合优化问题研究。

参考文献:

- [1] Sharma, Meenakshi, Siddiqui, Adil. RFID based mobiles: Next generation applications [C]// IEEE Xplore The 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China, April 2010. USA: IEEE Xplore, 2010: 523-526.
- [2] Walter B, Ion C Boi. Decentralized Orchestration of Composite Web Services [C]// Proceedings of IEEE International Conference on Web Services (ICWS'06). Chicago, IL, USA. USA: IEEE, 2006.
- [3] Ekwall R, Mena S, Pleisch S. Towards Flexible Finite State Machine Based Protocol Composition [C]// Proceedings of Third IEEE International Symposium on Network Computing and Applications (NCA'04), Boston, USA. USA: IEEE, 2004.
- [4] Girish C, Sunil C, Vijay M. Decentralized Orchestration of Composite Web Services [C]// International World Wide Web Conference on Alternate Track Papers and Posters, New York, NY, USA: ACM Press, 2004: 134-143.
- [5] 于守健, 何丰, 乐嘉锦. 基于接口匹配的 Web 服务自动组合 [J]. 计算机科学, 2007, 34(3): 61-68.
- [6] Gereade C E, Hull R, Ibarra O H. Automated Composition of Eservices: Lookaheads [C]// Proceedings of 2nd International Conference on Service-Oriented Computing, New York, NY, USA: ACM, 2004: 252-262.
- [7] 于守健, 李卫民, 吴国文. BPEL 中基于有限状态自动机的 Web 服务自动组合 [J]. 小型微型计算机系统, 2007, 28(4): 742-747.
- [8] Diego Zuquim, Guimar Garcia, Maria Beatriz. Quality of Service Management for Web Service Compositions [C]// Proceedings of 11th IEEE International Conference on Computational Science and Engineering, Sao Paulo, Brazil, 2008. USA: IEEE, 2008: 189-196.
- [9] 张耀峰, 肖人彬. 基于元胞自动机的网络群体事件舆论同步的涌现机制 [J]. 系统工程理论与实践, 2014, 34(10): 2600-2608.
- [10] Kaiyu Wang, Naishuo Tian. Performance Modeling of Composite Web Services [C]// Proceedings of 2009 Pacific-Asia Conference on Circuits, Communications and System, 2009, Chengdu, China: PACCS 2009: 127-130.
- [11] 朱昶胜, 王兵, 黄军强. 元胞自动机交通流 NS 模型相图研究 [J]. 计算机工程与应用, 2014, 50(21): 48-53.
- [12] Liangzhao Zeng, Boualem B, Marlon D. Quality Driven Web Services Composition [C]// Proceedings of 12th Int'l Conference on World Wide Web (WWW'03), New York, NY, USA: ACM, 2003: 411-421.