文章编号：2096-1472(2017)-03-01-04

一种面向业务流程模型的仿真验证方法

李 宁，徐 珞，郝 博，樊志强
（华北计算技术研究所，北京 100083）

摘 要：基于SOA软件构架成为分布式解决方案的主流技术，业务流程模型是SOA系统设计的核心，其是否存在缺陷对系统具有重要影响，因此，如何对业务流程进行验证成为一个关键问题。本文围绕业务流程模型验证需求，针对异构模型的联合仿真问题，提出基于HLA的业务流程模型仿真验证框架，通过对业务流程和网络部署进行仿真，有效对业务流程的功能和时间特性进行验证。相关实验表明，本文提出的方法能够有效发现业务流程中存在的设计缺陷。

关键词：业务流程；仿真；验证
中图分类号：TP316 **文献标识码**：A

A Simulation Verification Method of the Business Process Model

LI Ning,XU Luo,HAO Bo,FAN Zhiqiang
(*North China Institute of Computer Technology*, *Beijing* 100083,*China*)

Abstract:SOA software architecture has become the mainstream technology of distributed solutions.As the business process model is the core of SOA system design,it is significantly important whether there are some flaws in it.Therefore,the effective verification method of the business process model is quite critical.To meet the verification requirements of the business process model,this paper offers a solution to the collaborative simulation of the heterogeneous model,and puts forward the simulation verification framework of the business process model based on HLA.Through the simulation of the business process and the network deployment,the verification of the function and time characteristics is effectively implemented.The experimental results show that the proposed method can effectively find the design flaws in the business process.

Keywords:business process;simulation;verification

1 引言(Introduction)

随着软件开发技术的不断发展，信息系统的功能日新月异。但由于不同软件的开发平台、开发工具、操作系统在体系结构上的紧耦合性，使得物理分散的独立系统形成了所谓的“信息孤岛”。为了有效解决这一问题，需要一种标准化、开放性的体系结构完成从集中式到分布式的转换，在这一背景下，面向服务的体系结构SOA(Service Oriented Architecture)应运而生。

典型的基于SOA的软件开发过程往往首先建立业务流程模型，并以该模型作为系统设计，然后根据该模型，通过服务集成方法来自动或半自动的产生系统实现。因此，业务流程模型的正确性对最终系统质量具有重要影响。根据Ron Patton在《软件测试》中的论述可知，设计阶段存在的缺陷如果没有及时发现，在系统实现阶段修复该缺陷往往是设计阶段修复缺陷费用的100倍左右[1]，如果在用户大规模使用时发现该缺陷，修复该缺陷的费用往往是设计阶段修复缺陷费用的万倍以上。由此可见，对业务流程模型开展验证，对提高系统质量和降低软件开发费用大有益处。

2 相关研究(Related research)

目前，最常用的方法是模型检查(Model Checking)，即通过搜索系统的状态空间来对模型进行静态的形式化分析。随着模型规范化程度和可执行能力的提升，将测试手段应用于模型验证的方法必将被逐渐重视起来，例如可执行UML模型的测试。

(1)静态的模型检查方法

模型检查主要是对有限状态的系统模型进行静态的形式化分析，通过搜索系统的状态空间来检查该系统是否满足期望的性质。如果系统模型不能满足某一规格说明会给出反例。现有模型检查方法主要有基于语义网络的方法、基于PI-演算的方法、基于Petri网的方法和基于模型检测的方法。这

些验证方法通过将系统转化为形式化的模型(如Petri网和自动机模型)，借助模型检测器等自动化工具，验证协议和服务描述的完整性和一致性。经典模型检查理论已基本成熟，实现这些理论的经典模型检查器有SMV和SPINE等。

状态空间爆炸是模型检查中需要解决的一个关键问题，因此关于这方面存在大量研究。除了传统模型检查中的状态化简技术外，更多的方法结合了程序分析中的相关技术，例如：基于各种程序抽象技术计算源程序的抽象程序；利用程序切片减小程序规模；通过限定程序中不确定性的类型及其可能性的数量来获得程序状态空间的一个有限子集。

模型检查存在一定的局限性：在对大规模复杂系统进行模型检查时，状态空间爆炸问题几乎不可避免，因而难以对系统状态空间进行穷尽搜索；能够验证的指标受到模型描述能力的限制，对于系统需求中的一些非功能指标验证能力不足，也难以对系统的综合指标进行验证；模型检查的形式化模型和分析算法多种多样，没有统一的标准，如何决定最适合系统的方法存在一定难度。相较而言，软件测试方法则是一种“普适”方法，可以解决模型检查的上述问题。通过给出测试充分性准则，避免了对系统的状态进行穷尽的测试；测试方法可以很好的控制被测系统模型的运行状态，尤其适合业务流程模型的这类强调动态时变性的系统；测试的适用范围较宽，可以针对系统的多种功能和非功能指标进行测试。

(2)动态的模型测试方法

模型测试是指在系统开发早期利用软件测试手段对设计模型进行验证的方法。目前国内外对于这方面的研究相对较少，典型的研究如UML设计模型测试方面。UML(Unified Modeling Language)模型是软件领域中设计模型的常用表达方式。传统的UML设计模型的验证通常通过预排、检测和一些设计审查技术，大部分属于手工操作。对于庞大和复杂系统的UML设计模型的检查，检测人员需要手动的跟踪和关联多个视图中的概念，这是一项枯燥且容易出错的工作。近来，随着UML模型可执行性的提高，有些研究将软件测试方法应用到系统设计的早期验证中，如Trung Dinh-Trong和Nilesh Kawane等人提出了一种针对UML模型设计验证的软件测试方法。该方法基于UML类图、活动图、交互图生成被测模型的可测试执行体，并依据用户给出的测试充分性准则生成测试用例，最后通过模型的模拟执行进行测试。通过分析测试结果与系统需求的一致性来验证被测模型设计的正确性。由于UML中多数的视图并不具有可执行性，或者转换为可执行体的方法非常复杂，且多个视图是从不同的角度反映系统设计，因而很难形成一个完整的模型设计，因此，UML模型测试技术尚待发展，还有很多需要进一步研究的问题。

3 模型验证流程及建模(The modeling process and model verification)

3.1 业务流程模型仿真验证过程

本文提出的业务流程模型仿真验证过程如图1所示。根据该图可知，业务流程模型和网络部署模型需要在仿真引擎才能进行仿真执行，从而进行模型验证。

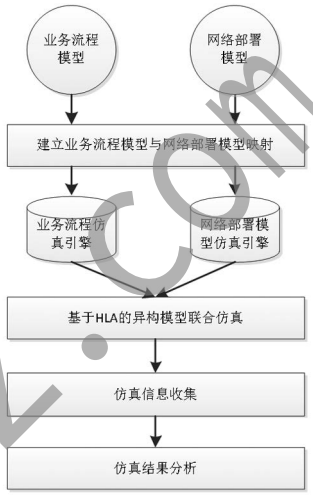


图1 业务流程模型仿真验证过程

Fig.1 Business process model simulation and verification process

实际上业务流程往往描述系统的整体流程，一般使用流程图或状态图进行描述；而网络部署模型往往描述系统实际的网络部署环境，往往使用特定的网络模型和仿真算法进行建模，由于这两类模型的差异较大，很难使用统一的仿真引擎进行仿真，因此需要为此选择适合各自模型特点的仿真引擎。

由于业务流程模型和网络部署模型需要使用不同的仿真引擎进行仿真执行，但在仿真过程中二者需要进行交互，这就需要对异构仿真模型进行协同仿真，针对这一问题，提出了基于HLA的异构模型联合仿真方法。在仿真过程中，通过仿真引擎将仿真过程中的信息进行打印输出，从而获取仿真信息，最后通过分析上述信息就能够实现对业务流程模型的仿真分析。

3.2 业务流程模型仿真

根据业务流程模型特点，选择Stateflow插件作为为业务流程模型仿真建模工具。与常见的Matlab模型和Simulink模型相比，Stateflow插件具备可视化的建模界面，更易于建模人员进行建模，另外，Stateflow插件提供丰富的可扩展机制，以完成复杂的逻辑运算。

图2给出了使用Stateflow插件对某数据发布服务的建模实例。其中业务流程中的活动主要使用Stateflow中的状态进行描述；消息则使用Stateflow中的迁移进行描述；部分复杂的数学逻辑可在Matlab中自行定义，然后在Stateflow中以M文件调用的方式使用。

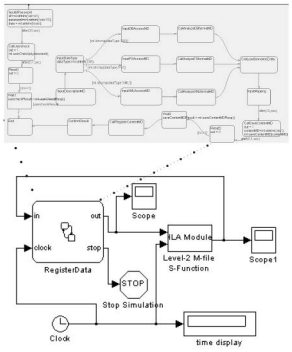


图2 使用Stateflow对业务流程模型建模

Fig.2 Modeling business process models using Stateflow

3.3 网络部署模型仿真

OPNET是目前最为常用的网络仿真工具，其采用阶层性的模拟方式，从协议间关系看，节点模块建模完全符合OSI标准，实现了从业务层→TCP层→IP层→IP封装层→ARP层→MAC层→物理层的各层仿真；从网络物件层次关系看，提供了三层建模机制，最底层为进程(Process)模型，以状态机来描述协议；其次为节点(Node)模型，由相应的协议模型构成，反映设备特性；最上层为网络模型。三层模型和实际的协议、设备、网络完全对应，全面反映了网络的相关特性。它的功能十分强大，采用网络、节点、进程三层建模机制，不仅支持面向对象的建模方式，还提供图形化的操作界面，使用方便快捷，能够为网络系统的建模提供良好的开发环境[3]。图3给出了使用OPNET建立的小型局域网模型。

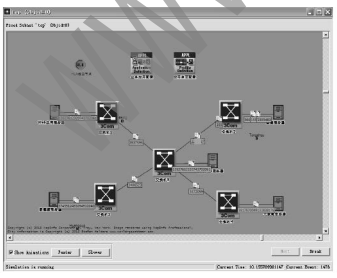


图3 使用OPNET 建立的小型局域网

Fig.3 LAN built using OPNET

4 基于HLA的异构模型联合仿真方法(Co simulation of heterogeneous model method based on HLA)

由于业务流程模型和网络部署模型采用了不同的仿真引擎，而在实际仿真过程中这两类模型之间必然存在交互，这就需要一种能够支持异构模型的联合仿真方法。

本文采用HLA机制用以解决异构模型联合仿真问题。HLA技术体制是IEEE公开发布的标准，该标准的主要目的是制定一套仿真框架，能够尽量涵盖仿真领域所涉及的各种不同的仿真模型，使得不同的仿真之间能够进行互操作，从而满足复杂大系统的仿真需求[4]。HLA使用联邦代表不同的仿真成员，其关注于如何由多个联邦成员构建联邦，通过协议规范进行各个联邦成员之间的交互活动。因此，HLA制定了十大规则，用以规范联邦(Federation)和联邦成员(Federate)的活动，最终组建一个用于数据交互的有序的公共虚拟执行环境。

RTI(Run-Time Infrastructure)是HLA接口规范的具体实现，是基于HLA的核心部件也是仿真应用程序的设计和运行的基础。同时，提供了仿真运行管理功能，底层通信传输服务，具有较好的扩充性，实现了仿真系统中各组成部件的“即插即用”。HLA的逻辑结构框架如图4所示。

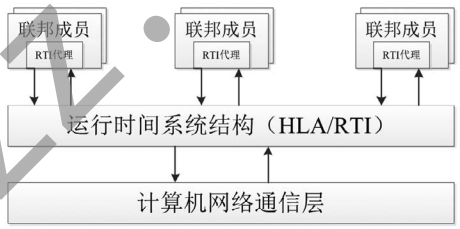


图4 HLA的逻辑结构图

Fig.4 HLA logic structure

RTI为不同的联邦成员提供统一的支撑运行环境，联邦成员之间按照HLA协议规范的要求，通过各自的RTI代理与RTI进程之间的交互，可以进行联合分布式仿真，完成联邦成员的同步交互和联邦的构建。

根据HLA技术机制，结合本文需要解决的技术问题，提出了一套基于HLA的异构模型联合仿真方法，该方法的主要结构如图5所示。由该图可知，该结构逻辑上分为模型层和运行层。模型层负责业务流程和网络部署模型的设计、仿真参数的配置、邦元集成接口约定和邦元数据交互模型，为运行层提供仿真实体模型；运行层负责封装各类模型并集成RTI代理组成不同的联邦成员。

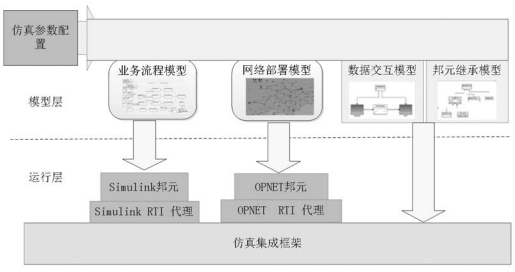


图5 基于HLA的业务流程模型结构图

Fig.5 Structure of business process model based on HLA

RTI代理的执行流程如图6所示。

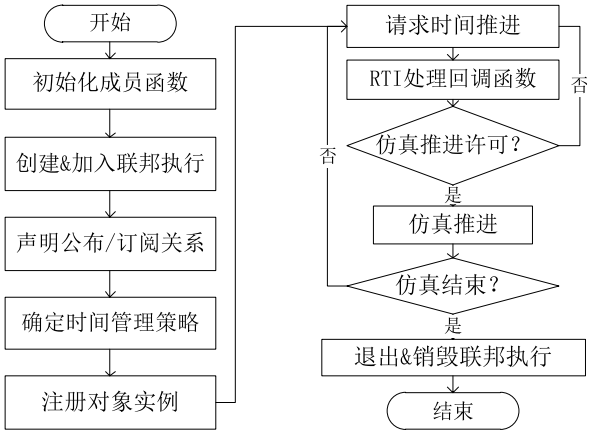


图6 RTI代理执行流程

Fig.6 RTI proxy execution flow

一般而言，进行时间推进之前，需要完成所有的初始化工作；此外，联邦成员的设计模式(单/多线程)取决于仿真软件所支持的方式，如VC支持多线程，可采用多线程模式设计；MATLAB不支持多线程，可利用S-Function自带的循环采样方式设计；OPNET不支持多线程，可利用设置循环自中断事件的方式设计。

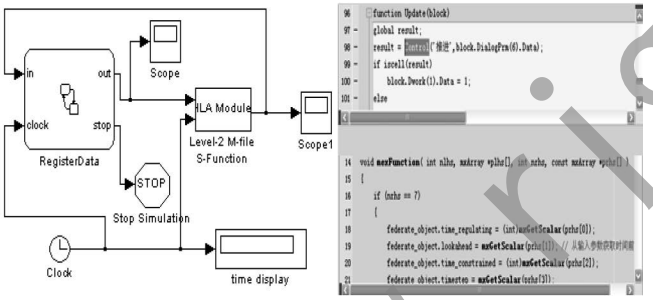


图7 S_Function实现的RTI代理

Fig.7 S_Function implementation of the RTI proxy

5 系统实现与实验验证(System implementation and experimental verification)

5.1 系统设计与实现

本文提出的仿真验证方法实现的原型系统结构如图8所示。由于仿真引擎在仿真过程中占用的系统资源较多，为了尽可能的提高仿真效率，我们将不同仿真引擎部署在不同机器上，这就需要在仿真过程中对整体仿真环境进行统一的控制，因此我们设计了分布式仿真控制模块，该模块能够辅助仿真分析人员对整体仿真环境进行统一的控制。除此之外，设计了统一的数据存储环境，将分布式仿真过程中的产生的仿真信息统一存储到数据库中，待仿真结束后，使用结果分析工具从数据库中抽取仿真信息，进行功能、性能以及可靠性等方面的分析。

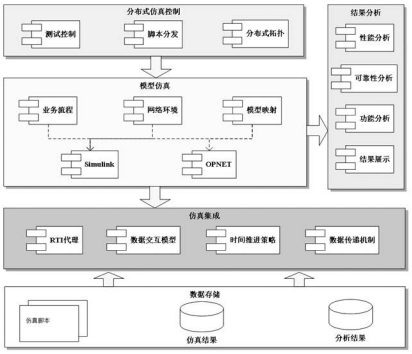


图8 业务流程模型仿真验证系统结构

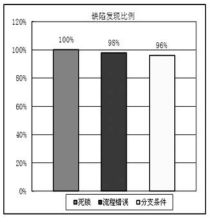
Fig.8 Business process model simulation verification system structure

系统使用C++语言在VS 2010环境中进行开发。系统使用过程中，仿真人员需要开发仿真脚本，然后使用分布式仿真控制端将仿真脚本分发到仿真引擎所在机器，然后发布联合仿真请求；仿真引擎收到仿真脚本后，根据仿真脚本中设置的相关参数启动仿真引擎并加入联合仿真环境，然后读取仿真脚本开始联合仿真；仿真过程中产生的相关信息存入远程数据库；当仿真结束后，通知测试人员仿真结束，测试人员使用测试结果分析工具进行结果分析，完成整个仿真验证过程。

5.2 实验验证

为了对本文提出的业务流程模型验证方法进行有效性验证，本文以某数据发布服务的业务流程作为待验模型进行典型实验。实验过程中对业务流程模型随机植入缺陷，进行多次实验统计缺陷发现比例，将缺陷发现比例作为评价方法有效性的标准。

参考文献[5]指出，常见设计缺陷主要包括：死锁、状态不可达、分支条件以及流程错误等。根据上述缺陷的特点，从业务流程中选择40个缺陷植入位置，每次实验从上述植入位置中任选三个缺陷进行植入，共进行30次实验，每次实验计算各类典型缺陷的发现比例，最终实验结果如图9左方柱状图所示。除此之外，由于本方法还对网络环境进行了仿真，因此能够统计网络仿真情况，图9右方的表格给出了流程平均执行时间和网络节点忙闲比等信息。



流程平均执行时间	6.6s
活动平均忙闲比	26.40%
节点平均忙闲比	41.90%
节点平均流量	10M/s

图9 实验结果

Fig.9 Experimental result

由该实验可知：在功能缺陷方面，能够准确发现死锁、流程错误和绝大部分分支条件错误；在非功能分析方面，可以获取模型执行时间、节点空闲比和网络流量等信息，能够支持一定的设计方案分析。

6 结论(Conclusion)

本文提出使用仿真手段对模型进行验证，以降低系统实现的风险。与常规模型验证方法相比，该方法能够有效检验系统实际运行才能表现出的缺陷，除此之外，该方法尝试对影响业务能力的网络环境等因素进行建模，并进行联合仿真，能够支持对系统更为全面的分析。

随着信息系统愈发复杂，对系统进行多角度建模称为未来仿真验证的必然趋势。本文的下一步工作将进一步分析影响系统业务能力的技术因素，并分析这些技术因素的仿真建模方法，从而能够对系统进行更为全面的仿真验证；除此之外，将并选择规模更大的业务流程模型进行仿真验证，以不断完善和优化整体方法。

参考文献(References)

[1] B Homes.Fundamentals of Software Testing[J].European Journal of Endocrinology,2016,150(3):243−255.

[2] M Dabaghchian,M Abdollahi Azgomi.Model checking the observational determinism security property using PROMELA and SPIN[J].Formal Aspects of Computing,2015,27(5):789−804.

[3] MAH Sadi,et al.OPNET/Simulink Based Testbed for Disturbance Detection in the Smart Grid[J].Cyber & Information Security Research,2015:17−26.

[4] 尹桥宣,等.基于HLA/Agent的能源系统与信息通信系统联合仿真设计[J].电力系统自动化,2016,40(17):22−29.

[5] 程铭,毋国庆,袁梦霆.基于迁移学习的软件缺陷预测[J].电子学报,2016,44(1):115−122.

作者简介：

李　宁(1986−)，男，硕士，工程师.研究领域：软件测试，软件开发.

徐　珞(1976−)，男，博士，研究员级高工.研究领域：体系结构，试验验证.

郝　博(1986−)，女，硕士，工程师.研究领域：软件测试，软件开发.

樊志强(1982−)，男，博士，高级工程师.研究领域：体系结构，试验验证.

(上接第44页)

性，较高的准确性和实时性，系统结构简单，无需复杂的布线，具有功耗低等特点，达到了预期的设计目标。

参考文献(References)

[1] LuoXiaomu,et al.Abnormal Activity Detection Using Pyroelectric Infrared Sensors[J].Sensors,2016,16(6):822.

[2] XiongJi,LiFangmin,LiuJian.Fusion of Different Height PyroelectricInfraredSensors for Person Identification[J].IEEESENSORS JOURNAL,2016,16(2):436−446.

[3] AiHong,ZhengYuning.Characterization of a Traffic Management System Using Pyroelectric Infrared Sensors[J].NSTRUMENTATION SCIENCE & TECHNOLOGY,2015,43(3):319−333.

[4] 廖平,乔刚.基于nRF2401的近距离点对多点无线通信系统[J].现代电子技术,2006,11:18−20.

[5] 张永宏,曹健,王丽华.基于51单片机与nRF24L01无线门禁控制系统设计[J].江苏科技大学学报(自然科学版),2013,27(1):64−69.

[6] 尚小燕.热释电红外报警系统设计[J].现代科学仪器,2012,2:65−67.

[7] 朱嵘涛,徐爱钧,叶传涛.STC15单片机和nRF2401的无线门禁系统设计[J].单片机与嵌入式系统应用,2014,26:57−60.

[8] 红外探测设计报告[DB/OL].http://www.docin.com/p−461210304.html.

[9] 吕璠.热释电红外报警器的设计[J].廊坊师范学院学报(自然科学版),2009,9(3):62−64.

[10] 杨波,张兴敢.基于PIC单片机的被动式红外报警系统的设计[J].电子测量技术,2008,31(1):53−56.

[11] 陈丽娟,常丹华.基于nRF2401芯片的无线数据通信[J].2006,29(1):248−250.

[12] 丁永红,孙远强.基于nRF2401的无线数传系统设计[J].中国科技核心期刊,2008,27(4):45−47.

作者简介：

路文超(1995−)，男，本科生.研究领域：电气工程及其自动化.

权　伟(1982−)，男，博士，讲师.研究领域：控制科学与工程. 本文通讯作者.

杨　雯(1996−)，女，本科生.研究领域：机械设计制造及其自动化.

郭培峰(1996−)，男，本科生.研究领域：电气工程及其自动化.

和腾龙(1996−)，男，本科生.研究领域：车辆工程.

杨应山(1996−)，男，本科生.研究领域：电气工程及其自动化.