ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.2, February 2010, pp.177−178
http://www.jos.org.cn/1000-9825/3815.htm

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

可信软件的构造与演化分析专刊前言*

王怀民[1+], 徐 洁[2]

[1](国防科学技术大学 计算机学院,湖南 长沙 410073)

[2](School of Computing, University of Leeds, UK)

+ Corresponding author: E-mail: whm_w@163.com

王怀民,徐洁.可信软件的构造与演化分析专刊前言.软件学报,2010,21(2):177−178. http://www.jos.org.cn/1000-9825/3815.htm

近年来,软件及其运行环境发生了质的变化,边界开放、规模巨大、行为复杂等特点使得软件系统在可信性方面面临许多新的挑战.如何构造和维护可信的软件系统受到了工业界和学术界越来越多的关注和重视,多国政府、组织、企业、科研机构纷纷提出了与可信软件构造与演化相关的研究计划.为了总结国内外在该研究领域所取得的重要研究成果,特别是我国国家高技术研究发展计划(863)、国家重点基础研究发展计划(973)和国家自然科学基金重大研究项目在该领域的最新研究进展,进一步促进我国在该领域的研究和应用实践,展望其发展趋势、分析其面临的挑战以及展示其应用前景,我们特推出《可信软件的构造与演化专刊》.

该专刊得到了国内同行的广泛支持与参与,共收到稿件 96 篇.《软件学报》编辑部邀请了 20 余名国内同行专家,历时半年,严格按照《软件学报》审稿流程和评审要求对稿件进行了认真评审,最后经《软件学报》编委会终审,确定录用 16 篇论文,录用率为 17%.

在录用的 16 篇论文中,有 6 篇论文涉及可信软件检测的模型、方法与机制,有 4 篇论文研究可信软件构造和演化的方法与机制,有 6 篇探讨可信软件的度量、评估和验证技术.每一篇论文都有独到的学术贡献,希望能够引起读者的兴趣,有助于推动相关领域的深入研究.

论文《面向高可信软件的整数溢出错误的自动化测试》针对高可信软件提出了一种二进制级高危数溢出错误的全自动测试方法及其原型系统 IntHunter.该方法无需任何源码甚至是符号表的支持,即可对裸二进制程序进行全面测试,以自动发现高危整数溢出错误.

论文《一种资源敏感的 Web 应用性能诊断方法》提出了一种资源敏感的性能诊断方法,利用资源服务时间相对稳定的特点,建立性能特征链,并根据运行时资源服务时间的异常来实现性能异常的检测、定位和诊断.

论文《一种路径敏感的静态缺陷检测方法》提出了一种多项式复杂度的路径敏感缺陷检测算法.该方法可避免完整路径上下文分析的组合爆炸问题.测试结果表明,该方法能够减少误报.

论文《可扩展的多周期检查点设置》提出了一种多周期检查点设置算法,允许各个进程采用不同周期进行检查点的设置,以保证在提高检查点设置的自主性的同时,能够以尽可能低的开销来保证一致全局检查点的向前推进.

论文《基于 Petri 网的服务组合故障诊断与处理》提出了一种服务组合故障处理的框架,设计了服务组合故障处理正确性准则并证明其正确性,采用 CTL 描述相关性质并提出验证服务组合故障分析的实施算法,以解决服务组合的错误发现及其处理问题.

论文《基于动态描述逻辑的网构软件系统故障诊断》针对网构软件的故障诊断问题,通过将网构软件抽象为离散事件系统,运用动态描述逻辑来刻画系统的正常行为和异常行为,设计了网构软件的故障诊断算法,并进行了应用案例分析.

* Received 2009-12-29

论文《基于服务组合的可信软件动态演化机制》针对服务组合的可信问题,提出了一种面向可用性保障的组合服务演化方法,设计和实现了支持动态演化的组合服务执行引擎,并通过实验分析和验证了方法的有效性.

论文《一种面向服务的可靠多媒体传输算法》针对在面向服务的实时多媒体传输系统中如何选择具有低时延和高可靠性路径的问题,提出了一种 LD/RPath 算法.实验表明,该算法具有较好的路径选择效果和较低的系统开销.

论文《一种从 UML 模型到可靠性分析模型的转换方法》提出了一种将 UML 模型自动地转换为可靠性分析模型 Markov 链的方法.该方法产生的结果能够直接作为现有可靠性相关的数学分析方法的输入,使可靠性分析工作变得更加方便和高效.

论文《字节码虚拟机的构造和验证》给出了字节码程序运行环境的形式定义,采用机器语言构造虚拟机,证明了该虚拟机符合相应的程序规范,同时证明虚拟机的实现程序和字节码程序运行环境之间存在模拟关系,并利用辅助工具给出所有证明均可机器自动检查.

论文《面向参数化LTL的预测监控器构造技术》提出了一种基于自动机理论的参数化LTL(P_ALTL)公式运行时预测监控器构造方法.该方法通过描述系统中动态对象和数据结构的相关性质,采用静态和动态两种方式验证当前程序运行是否满足指定的参数化性质规约,并能精确识别被验证性质的最小好、坏前缀.

论文《处理指针相等关系不确定的指针逻辑》通过增加相等关系不确定的指针类型访问路径集合,使得指针逻辑可以应用于有向图等指针相等关系不确定的抽象数据结构,以支持指针程序性质证明.

论文《一种关键任务系统自律可信性模型与量化分析》提出了一种基于 SM-PEPA 的关键任务系统自律可信性模型以及自律可信性度量方法,以支持对自律可信性的影响进行分析.

论文《一种支持软件资源可信评估的框架》提出了一种软件资源可信评估框架,设计并实现了动态的软件资源可信评估机制,并进行了详细的实例分析,从而为复用者提供可信的软件资源.

论文《基于 TPM 的运行时软件可信证据收集机制》提出了一种基于可信计算技术的软件运行时可信证据收集机制,通过引入可信证据收集代理,从而客观地收集目标应用程序在运行时可作为软件可信证据的信息,并保障可信证据本身的可信性.

论文《面向可信服务选取的基于声誉的推荐者发现方法》提出了一种基于声誉的推荐者发现方法.该方法通过引入一个相关因子量化不同上下文中的推荐信任关系,应用信任子网分割算法得到评估发起者的可信推荐者群,通过主体群内的信任传递与迭代计算确定具有高声誉值的推荐信息源.实验表明,该方法可有效提高可信服务评估的效率.

这些论文记述的成果仅仅是我国学者在可信软件的构造与演化领域的部分成果.由于篇幅和时间的限制,还有许多有价值的成果不能通过本专辑得到发表.我们希望有更多、更好的成果能够在相关学术期刊和会议上发表和交流.

王怀民(1962－),男,江苏南京人,博士,教授,博士生导师,CCF 高级会员,国防科学技术大学长江学者特聘教授,国家杰出青年科学基金获得者,“新世纪百千万人才工程”国家级人选.主要从事面向网络计算的软件技术研究,主持或参加了国家自然科学基金、国家重点基础研究发展计划(973)、国家高技术研究发展计划(863)、国防型号工程、武器装备预研以及国际合作等 20 多项科研课题,在国际期刊、国际会议和国内一级学报上发表学术论文 100 余篇.

徐洁(1963－),男,博士,教授,博士生导师,目前任教于英国利兹大学,重庆大学长江学者讲座教授,主要从事可靠的分布式系统和容错计算的研究,在计算机系统故障诊断、容错软件和可靠的分布式系统领域发表论文 120 余篇,曾参与 e-Demand, IBHIS,Flexx,e-Actions,SeCode,MVD 和 TestDES 等重大研究项目.