网构软件可信性评估与保障技术

司冠南 | 著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网构软件可信性评估与保障技术

司冠南　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

网构软件是近年发展起来的研究领域，涵盖了软件构件、体系结构、软件开发方法等多方面，并为当前流行的云计算、物联网等概念提供了诸多核心技术。由于网构软件工作于开放、动态、难控的互联网环境，且组成实体多由第三方提供，其可信性问题就变得非常重要，如何保证软件整体及各组成实体的可信性成为网构软件研究领域中一个非常具有挑战性的新问题。本书从网构软件的实体模型、系统结构、软件演化、可信性评估等方面对其可信性评估与保障技术进行了阐述，并提出了解决方案。

本书可供计算机科学、可信计算、服务计算以及相关领域科学研究人员和工程应用人员参考，也可供高等院校和科研院（所）相关专业的教师和研究生阅读参考。

图书在版编目（CIP）数据

网构软件可信性评估与保障技术/司冠南著. —北京：电子工业出版社，2015.1
ISBN 978-7-121-25134-4
Ⅰ. ①网… Ⅱ. ①司… Ⅲ. ①软件设计－研究 Ⅳ. ①TP311.5
中国版本图书馆 CIP 数据核字（2014）第 294368 号

责任编辑：赵 娜　　特约编辑：王 纲
印　　刷：北京季蜂印刷有限公司
装　　订：北京季蜂印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1000　1/16　印张：13.75　字数：264 千字
版　　次：2015 年 1 月第 1 版
印　　次：2015 年 1 月第 1 次印刷
定　　价：42.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

存在于互联网各个节点上的主体化软件服务，通过多种机制进行协同、整合而形成的软件形态通称为网构软件。网构软件为有效进行异构资源整合、充分利用互联网上大量的软件服务提供了有效手段，但随着对网构软件功能需求的不断增加，系统的结构、体系变得日趋复杂，同时由于软件的运行环境从传统的“封闭、静态、可控”环境转变为“开放、动态、难控”的互联网环境，对可信性保证的要求变得日益突出。目前网构软件可信性保证技术在信任关系的约束机制、推荐信息的准确性、信任衰减参数的合理性、信任演化模型的系统化、可信性评估方法的切实性等方面还存在着不足。针对上述不足，本书在网构软件可信性保证关键技术方面进行了研究，具体研究内容与创新点包括 5 个方面。

（1）在实体个体层面，研究网构软件的可信实体模型。提出了具有自省性、自明性、自主性特点的网构软件强可信智能实体模型。定义了实体可信情况形式化描述语言（EDSADL），使实体能够通过自省机制实时监控与保障自身的可信性水平，并向外界公布以供验证。设计了业务功能模块与可信性保障模块分离的系统结构，保证了实体在向外界公开可信保障机制的同时对自身业务细节的保密性。设计了“环境感知—策略调度—行为触发”的机制，使实体具有感知环境刺激而自主演化的能力，保证了实体在外界环境可信性发生变化时能够做出适时的响应。

（2）在实体间协同层面，研究网构软件实体间的信任约束机制。引入

契约式设计思想，从服务使用者和提供者的角度出发，采用“承诺—评估”机制明确双方的权利和义务，为实体交互过程中的双边规范定义了从低层接口语义到高层可信性情况的约束。定义了信任契约中前置条件、后置条件和不变式三要素的描述方法，保证了服务使用者、提供者以及服务交互关系的可信性，为实体协同、合作和竞争提供了有力的评估依据。

（3）对于信任传递参数，研究实体间信任传递衰减参数的计算方法。综合主观信任与客观评估的优点，提出了基于评估的信任衰减过程。在对实体环境进行可信性评估的基础上，通过逐级计算、信息合并来综合多个推荐者实体的推荐信息，使用对实体间传输可信性的评估结果来修正推荐信息，计算得到信任传递过程中的衰减参数。该方法充分考虑了外部环境、实体自身条件等情况对主观信任值的影响，使信任传递过程中信任衰减参数的计算更加客观、准确。

（4）在系统层面，研究网构软件可信性演化模型。提出了一种对网构软件体系结构进行形式化的建模方法，建立了系统结构模型，并据此提出了基于分层 Petri 网的网构软件可信性演化模型；通过上层 Petri 网对实体之间的各种基本协同关系进行了建模，以此形成系统整体组成结构的描述，反映了实体间信任关系的演化；通过下层 Petri 网对实体内部的契约协商策略进行了建模，设计了基于信任等级带有路径引导的信任契约协商方法。从系统整体的角度建立起动静结合、层次分明、描述统一的网构软件可信性演化模型。

（5）在系统测试与可信性评估层面，研究网构软件系统可信性评估模型。提出了符合网构软件异构性、结构化、动态化特征的可信性评估方法。定义了基于贝叶斯网络的网构软件可信性评估体系，通过树形结构整合了传统的静态指标以及适用于网构软件的动态指标。提出了基于结构模式的可信性评

估指标及其计算方法，在描述各实体之间结构关系、语义关系的基础上，涵盖了对网构软件系统整体及其组成实体可信性的评估。建立起不但能对系统进行评估，还能为用户选择最优化实体提供帮助的可信性评估模型。

本书内容分为 8 章。第 1 章阐述了网构软件可信性相关概念。第 2 章介绍了网构软件可信性保证的相关研究现状，以及本书的主要研究内容、意义和创新之处。第 3 章对网构软件可信实体模型进行了研究，对现有的网构软件实体模型进行了分析，并给出了网构软件强可信智能实体模型及其结构和行为设计。第 4 章对网构软件实体间信任约束机制进行了研究，分析了目前常用的网构软件的信任度量及演化模型，建立了基于契约的网构软件实体交互模型，并提出了基于评估的信任衰减过程。第 5 章是对网构软件可信性演化模型的研究，建立了系统结构模型，根据此模型建立了基于分层 Petri 网的网构软件可信性演化模型，并描述了网构软件系统运行中的可信性演化机制。第 6 章是对网构软件可信性评估模型的研究，建立了基于贝叶斯网络的可信性评估体系，并介绍了评估体系中各指标及系统整体可信性的计算方法。第 7 章是对网构软件动态可信性指标评估技术的介绍，从 Web 应用安全漏洞渗透测试中 SQL 注入攻击建模和 SQL 注入渗透测试用例形式化建模等方面进行了阐述。第 8 章总结了本书已经完成的工作，并对未来的研究做出了展望。

本书第 7 章的编写工作得到了天津工业大学田伟老师的大力支持，在此表示衷心感谢。由于作者水平有限，书中错误与不妥之处在所难免，欢迎各界专家和读者朋友批评指正。

山东交通学院

司冠南

2014 年 10 月

反侵权盗版声明

目　录

第 1 章

网构软件可信性相关概念

互联网发展日新月异，随着网络上信息量的急剧膨胀，越来越多的用户对网络服务和应用提出了实时、动态、开放、可信的要求。如何整合分布式异构资源，为网络使用者提供快速、高效、可信的动态服务是信息技术发展面临的严峻挑战，也是国家及各行业领域一系列重大需求的共同基础。为了适应这些应用领域及信息技术方面的重大需求，在面向对象、软件构件等技术支持下，形成了基于互联网环境的新的软件形态，即网构软件（Internetware）[1]。由于网构软件工作于开放、动态、难控的互联网环境，且组成实体多由第三方提供，软件的可信性问题就变得非常重要。因此，如何保证网构软件整体及各组成实体的可信性成为网构软件研究领域一个非常具有挑战性的新问题。

1.1 网构软件

为了适应人们不断增加的功能需求，软件系统的结构、体系变得日趋复杂。同时，在飞速发展的互联网技术的推动下，软件的组成逐步由

固定转向多样，软件的行为逐步由静态转向动态，软件的开发逐步由封闭转向开放。从软件实体的角度看，主要经历了对象、构件、服务，并发展了软件 Agent 技术，软件实体的主体化（内容的自包含性、结构的独立性与实体的适应性）程度不断提高；从软件开发的角度看，主要经历了 3 个发展层次：面向对象、基于构件和面向服务[2~11]。

面向对象的方法与技术很好地发展了信息隐蔽原理及抽象数据类型概念，使人们能够从认知的角度控制大型软件设计与开发过程的复杂性。其基于继承的代码复用和多态执行的机制，将各种相关的对象加以有机关联，使所设计的软件对软件工程实践中常遇到的功能易变性具有一定的适应能力。软件的设计与开发也由对功能固定、结构封闭的问题进行自顶向下、逐步精化的结构化方法求解，转变为对功能可变、结构开放的问题进行结构化适应。所使用的开发方法面向具体问题，支撑个体软件开发者，系统开发呈现一阶段集中式结构。

软件构件的概念诞生于 20 世纪 60 年代后期，人们从不同的角度给出了不同的定义，OMG 组织[12]、Carnegie Mellon 大学软件工程研究所（SEI）的 Bachman[13]，以及著名构件学者 Szyperski[14]等均对构件给出了定义。我们认为，Szyperski[14]的定义较好地体现了构件的特征，其定义如下：软件构件是一种用于组装的单元，它具有规范的接口规约和显式的上下文依赖，软件构件可以被独立部署并由第三方组装软件。构件一般由为组装提供基础支撑的构件接口与包含功能具体实现的构件体组成。构件通常比对象具有更大的粒度和更强的复用性，可以在基本不改变内部实现细节的情况下被重复应用于多个软件系统。这样构件就可以由第三方通过一定的外部手段进行一定的剪裁与调节，进而应用于更加广泛与开放的环境中。由此可见，构件能够在解决已有问题的基础上

对未来的同类问题提供支持，满足了大规模工业化生产软件的需求。基于构件软件的开发面向群体问题，支撑群体开发者工业化开发，构件开发与系统组装呈现两阶段分离式结构。

随着互联网的发展，软件的使用环境也逐渐变得更加开放、动态和多变。而开放网络环境中各类资源的共享和集成也对计算机软件技术提出了新的挑战。软件服务的概念就是在这种环境下产生的，并较对象、构件有了新的发展，主要是应对开放网络环境中各类资源的共享和集成对计算机软件技术提出的挑战。首先，软件服务的业务功能相对独立，通常基于可共享或集成的资源构建，因而具有更大的粒度与更强的独立性，更便于使用者直接使用。其次，软件服务具有较高的抽象级别，屏蔽了开放环境带来的异构性问题，且具有松耦合性，可以灵活、动态地组合以生成增值服务。最后，由于开放环境下存在大量类似的资源，使用者可以在量大面广、推陈出新的多个相同或相似服务中不断选择最合适的服务以构建最优的系统。基于服务软件的开发面向问题解，支撑大量软件最终使用者及开发者，服务发布/查询/使用呈现三阶段松耦合结构。

软件 Agent 是近年兴起的一种新技术，通过将人工智能技术与软件技术相结合，建立软件实体内部机制，以使其能够应对开放、动态与难控的外部环境。对于智能 Agent 的认识，Wooldridge 认为[15]“Agent 是这样的一个计算机系统，其位于某个环境中，且能在该环境中采取一定的自治动作以满足其设计目标”。智能 Agent 具有反应性、目标驱动性、社会性，可以感知环境并及时做出反应，以目标为导向驱动行为，相互间进行交互，以此来满足其设计目标[15,16]。这样软件实体就具有了以下能力与特性：对外部环境的感知能力，并通过自身行为对外界产生作用；

推理与决策能力，通过控制与推理使自身行为更具自主性；与其他实体进行有效交互的反应性、目标驱动性和社会性等特性。

在上述技术与方法的支持下，逐渐形成了网构软件的概念。网构软件是由分布在广域范围内、通常由第三方提供、具有主体化服务特征的一组软件实体，通过各类风格各异的协同连接子加以互连互通而形成的联盟，是开放、动态和难控网络环境下的分布式软件系统的一种抽象[17]。它既是传统软件结构的自然延伸，又具有区别于在集中封闭环境下发展起来的传统软件形态的独有的基本特征[18]。

（1）自主性：指网构软件系统中的软件实体具有相对独立性、主动性和自适应性。

（2）协同性：指网构软件系统中软件实体与软件实体之间可按多种静态连接和动态合作方式在开放的网络环境下加以互连互通、协作和联盟。

（3）反应性：指网构软件具有感知外部运行和使用环境，并对系统演化提供有用信息的能力。

（4）演化性：指网构软件结构可根据应用需求和网络环境变化而发生动态演化，主要表现在其实体元素数目的可变性，结构关系的可调节性和结构形态的动态可配置性。

（5）多态性：指网构软件系统的效果体现出相容的多目标性，它可根据某些基本协同原则，在动态变化的网络环境下，满足多种相容的目标形态。

网构软件的组成结构如图 1.1 所示。由图 1.1 可以看出，网构软件是由软件实体层、网构软件层和介于二者之间的标准接口层组成的，它们连同软件用户都是互联网平台的一员。各实体均为散布在互联网的软

件系统，彼此独立、自主运行，不受任何机构或组织的统一控制，在开放、动态和多变的环境中进行协同。

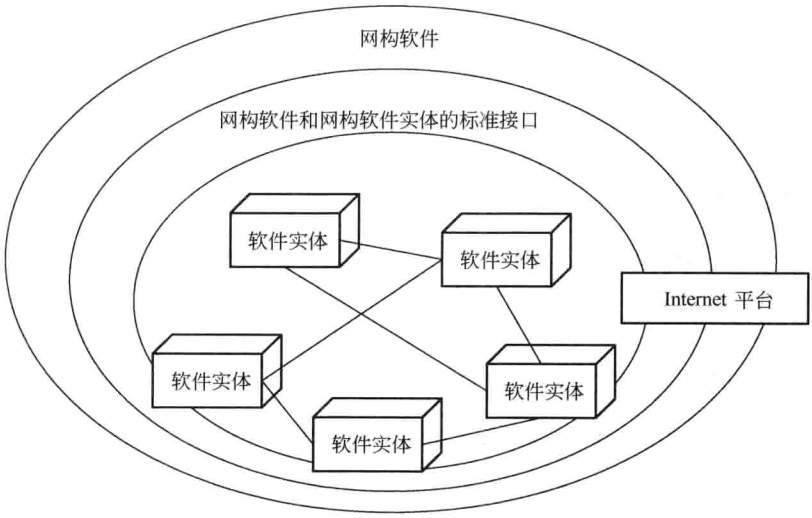

图 1.1　网构软件组成结构图

网构软件的各个实体首先是一个构件，具有与传统软件构件类似的业务接口及构件体内部实现。这样各实体可以独立部署、运行与演化，并通过业务接口提供计算、控制或连接等功能。但互联网“天然”的异构性决定了网构软件实体并不等同于传统软件构件，其具备个体感知能力、环境感知能力和个体适应能力等。这些能力主要以反射接口所提供的对网构软件实体自身业务的监测、分析、规划、调整等反射功能为基础，进而实现网构软件整体的自主性、演化性、协同性、多态性和反应性等特性。对于网构软件整体而言，既可以作为一个部署于互联网上的软件系统为处于不同时区的用户服务，也可以作为一个软件实体对随时到达的其他网构软件的请求进行响应。从长期来看，网构软件的动态模型使其能够自主演化，主动适应开放、动态和多变的互联网环境，以满

足某一时段内用户的个性化需求。并且根据环境的变化随时对运行系统按照所需的指标加以调整与演化，从而使系统在下一个时段能更好地满足用户的需求。

网构软件的研究工作借鉴和涵盖了当前最新的研究理念与成果，主要包括基本理念、实现主体、软件协同、运行机制、安全保障、系统管理自主化等多个方面。

在基本理念方面，英国学者提出的 GUC（Global Ubiquitous Computer）理念[19]从概念的角度，论述了包含 UC（Ubiquitous Computer）和 Global Computing 的观念；Shaw[20]等从资源集成与共享的角度提出了 ORC（Open Resources Coalitions）的概念，ORC 是指分布自主的资源所动态形成的、面向特定任务的临时联盟，这些资源可以是信息、计算、通信、控制或服务；浙江大学的张三元教授及其研究团队建立了在 P2P 网络拓扑结构上的网构软件模型 P2P-IWRM，通过引入构件副本、构件复用形式及构件副本测试状态，建立了本地构件库和网络构件库，增强了网构软件的自适应性[21]。

在实现主体方面，北京大学的梅宏教授[22,23]及其研究团队通过改装已有普通构件，将 Agent 技术与构件技术结合起来，为构件定制行为规则和规划，使之具有自主性，并提出了一种基于自主构件的协作框架，借助环境改变来引导自主构件间的协作；吕建等[24]以开放网络环境下的网构软件需求为切入点，基于软件 Agent 的原理、方法和技术，提出了一种开放协同软件模型来作为网构软件的基础模型，并在此基础上提出了一条建立基于 Agent 的网构软件模型的技术途径，即网构软件模型=开放协同模型+环境驱动模型+智能可信模型；常志明等[25]基于动态 Agent 理论为网构软件建模，描述了构件的运行状态、自主运行及自适应演化

运行机制；王怀民等[26]提出了一种支持软件环境适应能力细粒度在线调整的构件模型 ACOE，将软件环境适应能力中的感知、决策、执行等关注点封装为独立的构件和连接子，通过动态软件体系结构技术来支持它们的在线重配置。

在软件协同方面，Carriero 和 Gelernter 提出了 Programming = Coordination + Computation 的理念，即分布式程序设计中将协同与计算分离[27]，在此理念指导下，Linda 语言使用基于共享空间的协同语言或协同框架，这类协同模式解除了各个软件实体之间的直接耦合，而使用共享空间来进行基于通信内容的匿名通信；金芝教授[28]及其研究团队为构件建立环境本体，以环境为桥梁实现需求和构件的相互理解，以环境的状态变迁为驱动进行构件的组合。

在运行机制方面，构造能够热演化或自演化的软件系统难度非常大，SA（Software Architecture）[29]技术的发展与成熟为研究软件系统的自演化提供了结构化的基础。演化方面的技术较多地采用框架结构方法，通过对框架结构的改变来演化系统，也有一些做法是采用动态转化（Software Dynamic Translator）[30]等。南京大学吕建等[31,32]对软件热演化进行了研究，开发出了自演化软件支撑平台 Artemis-MAC。

在安全保障方面，Blaze[33]在 1996 年首次明确提出可信管理，主要使用早期的分布式身份认证技术，并在单纯的身份认证的基础上进行了扩充。吕建等[34]针对网构软件的特性，设计了一个基于层次式 Monitor 的信任管理系统。可信管理与可信评估的有机结合将是研究的重要方向，Grandison 等[35]提出了一个更为一般的可信管理的定义将可信管理与可信评估统一起来。

在系统管理方面，提出了自治式计算的概念。其中，文献[36]介绍

了一种基于 Agent 的软件框架结构，软件 Agent 被用以封装系统内的各个组件，系统的自主管理通过 Agent 的自主性得以实现。Hot Swapping 技术[37]利用代码插入（Code inter-positioning）和代码替换（Code Replacement）等技术实现了构件的自监控等自管理机制。

1.2 可信计算

由于互联网环境的开放性、动态性、多变性，可信问题越来越受到人们的广泛关注。可信的概念来源于可信计算，并在诸多领域得到了大力推广。

可信计算是一种包括可信硬件、可信软件、可信网络和可信计算应用等诸多方面的新的信息系统安全技术，其思想源于人类社会，把人类社会成功的管理经验用于计算机信息系统和网络空间，以确保计算机信息系统和网络空间的安全可信[38]。可信计算组织（TCG）认为[39]，可信计算的总体目标是提高计算机系统的安全性，现阶段的主要目标是确保系统数据的完整性、数据的安全存储和平台可信性的远程证明。

可信计算的基本思想如下[39]：

（1）首先在计算机系统中建立一个信任根，信任根的可信性由物理安全、技术安全与管理安全共同确保；

（2）再建立一条信任链，从信任根开始到硬件平台、操作系统，再到应用，一级测量一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。

TCG 的信任链如图 1.2 所示。