信息安全技术丛书

# 主观逻辑及其应用

田俊峰　焦洪强　杜瑞忠　著

科学出版社

信息安全技术丛书

# 主观逻辑及其应用

田俊峰　焦洪强　杜瑞忠　著



科学出版社

北京

## 内 容 简 介

本书在简要介绍信任管理及信任模型、国内外学者的部分研究成果的基础上，主要介绍了作者在主观逻辑及其应用方面的研究成果。主要包括：主观逻辑理论的扩展与改进、基于主观逻辑扩展的软件行为动态信任评价模型、基于主观逻辑的可信软件评估模型、基于多维主观逻辑的 P2P 信任模型、基于扩展主观逻辑的电子商务信任模型等。

本书可以作为信息安全及相关专业研究生教材，也可供从事信息安全与电子商务相关研究和开发的人员阅读参考。

**图书在版编目 (CIP) 数据**

主观逻辑及其应用 / 田俊峰，焦洪强，杜瑞忠著．—北京：科学出版社，2015.9

（信息安全技术丛书）

ISBN 978-7-03-045807-0

Ⅰ．①主… Ⅱ．①田…②焦…③杜… Ⅲ．①计算机网络－安全技术 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2015）第 227330 号

责任编辑：陈 静 邢宝钦 / 责任校对：桂伟利

责任印制：张 倩 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

三河市骏杰印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2015 年 9 月第 一 版 开本：720×1 000 1/16

2015 年 9 月第一次印刷 印张：10 1/2

字数：211 680

**定价：58.00 元**

（如有印装质量问题，我社负责调换）

# 前　言

随着计算机网络和一些分布式系统支撑技术的飞速发展和普遍应用，人们开发了越来越多的大规模的分布式系统，使得信息和数据的安全变得越来越重要，资源共享将会是现在及未来的网络生活的主流。同时，也带来了一些未知的风险，在各式各样的资源面前，如何进行有效的真伪（安全）鉴别，即防止伪装的恶意节点带来的安全问题，以及发现之后又该怎样处理相应的问题。解决这些问题在很大程度上需要有一套相应的标准。

传统的安全机制集中在验证对象的某些特征的吻合，但是在目前分布式网络的应用环境下，这样的安全机制并不能解决所有问题。原因在于传统安全机制只能通过其“身份标识”来确定节点的真假，而不能通过对其行为变化的分析确定节点是善意还是恶意，因此不能及时地识别恶意实体。随着分布式网络应用的发展，传统安全机制已经无法适应新的网络场景对于动态安全性的要求。信任管理模型的引入，可以弥补这些传统安全机制的不足，同时信任管理模型自身也已经可以作为一种独立的安全机制而存在。在安全领域，传统的安全机制被称为“硬安全”，而信任管理模型被称为“软安全”。目前信任管理模型的应用集中在电子商务、文件共享系统、P2P 网络、移动自组网等应用环境中。

信任管理涉及社会学、心理学、管理学、人工智能等多个方面。近几年来，越来越多的学者都在该领域进行研究，也取得了很多研究成果，其中研究的很多信任模型和算法都是通用或值得借鉴的。Jøsang 等提出的主观逻辑信任模型，借鉴了 D-S 证据理论，引入不确定性，提出了主观逻辑理论，并在此基础上建模信任关系，取得了很好的效果，然而，其理论在实际应用中仍然存在许多问题。本书对 Jøsang 的主观逻辑理论进行了扩展和改进，对完善和发展信任模型具有较大的推动作用。

本书是作者所在的研究小组近几年在主观逻辑及其应用方面的阶段成果总结，很多思想方法是在作者的指导下，由作者的研究生在完成科研和学位论文的过程中产生的，这些成果的产生得益于他们的创新性研究和勤奋努力，在此对他们表示衷心的感谢！

本书共 7 章，由田俊峰、焦洪强、杜瑞忠等撰写，全书由田俊峰统稿和审校。第 1 章对信任的定义、信任的分类、信任的特征、信任管理、信任理论及现状等基本问题进行介绍。第 2 章介绍 Jøsang 的主观逻辑理论。第 3 章介绍改进和扩展 Jøsang 的主观逻辑理论，增强该理论适应动态变化的客观环境的能力，使之能够更好地进行信任建模。第 4～7 章将扩展的主观逻辑理论应用在电子商务信任、信任建模、软件可信性评估等方面。

本书的部分研究内容得到了国家自然科学基金项目（编号：61170254、60873203）、

河北省杰出青年科学基金项目（编号：F201000317）、河北省自然科学基金（编号：F2014201117、F2014201098、F2014201165）、河北省高等学校科学技术研究重点项目（编号：ZH2012029）的资助，特此致谢。

由于作者学识和水平有限，书中难免会有不足之处，恳请读者批评指正。

作　者

2015 年 6 月

# 目　录

# 第 1 章　信任模型与信任管理

近年来，随着网格计算、普适计算、云计算、Ad Hoc 等大规模分布式应用系统的深入研究，系统表现为一些节点集合组成的自治网络，网络中的节点信息是可以共享的，任意节点可以通过信任网络搜索，找到声称拥有所需文件的节点；发起搜索行为的节点可以通过一定的算法找到信任评价值最高的节点进行交互行为，但是，在享受资源共享和高使用率的同时，也面临着许多安全威胁。一方面，分布式系统中，系统对节点缺乏一定的约束，使环境中的节点具有更多的自由，这更有利于节点之间的交互；另一方面，在开放的分布式环境中，源节点往往要与不了解甚至完全陌生的节点进行交互，但是节点之间又缺乏信任，这就导致了恶意节点大量的欺骗行为和不可信的服务，使节点之间的交互具有极大的风险性。因此，基于凭证式的静态信任机制不能有效地抑制这类节点的恶意行为，不能很好地适应大规模分布式网络的发展。此时，建立有效的动态信任管理机制，在节点交互之前对其行为进行预估，并在交互完成后进行信任评价的动态更新，对云计算、分布式网络以及电子商务的健康发展具有重要意义。通过信任机制，可以使节点在交互之前对对方的诚信度、可靠度进行很好的预估，防范恶意节点的攻击，从而确保交互的可靠性和安全性。

信任管理是当前分布式网络环境下的一个热点问题，本章对信任的定义、信任的分类、信任的特征、信任管理、信任理论及现状等基本问题进行介绍。

## 1.1　信 任 概 述

### 1.1.1　信任的定义

信任原本是一个心理学概念，是人们在交往的过程中表现出来的一种复杂的社会心理现象。信任是一种心理状态，在这种心理状态下，信任者愿意处于一种脆弱地位，有可能导致被信任者伤害自己；同时，信任者认为被信任者会做和预期一样的行为，其内在含义为相信被信任者会做承诺要做的事，不会做出信任者不希望做的事情。

社会学家将信任作为一种与社会环境紧密相关的社会现象，不少学者认为信任是社会制度和文化规范相结合的产物，是建立在理性的法规制度、道德和习俗基础上的社会现象。

经济学领域中，主要强调信任的可计算性，即经济学认为信任是基于计算的理性行为。经济学家是在经济的基础上研究信任，认为信任不应掺杂任何感情等非理

性因素。这与社会学家和心理学家不同，社会学家和心理学家都认为信任是无法确切计算出来的，心理学家认为信任是一种非理性的行为，而社会学家强调信任的社会性和文化性。

Zhang 在其著作中，综合社会学和心理学两种角度，认为信任至少包含两层含义[1]：信任关系在一定情景下由施信者和受信者组成，缺一不可，在相互信任关系中，每一个关系主体同时扮演两种角色；信任是一种心理活动，体现为施信者对受信者行为的预期偏好，并通过一定的外在行为表现出来，如遵守有关的合约、实现承诺等。他指出信任的概念涉及三个重要的构成要素，即信任者、被信任者和环境。

信任是一个非常复杂的概念，心理学、社会学、经济学、管理学、计算机科学等不同的研究领域对信任有着不同的定义，目前，关于信任还没有形成被广泛接受的、统一的定义。Gambetta[2]认为信任是一个概率分布的概念，把信任定义为一个实体评估另一实体在对待某一特定行为的主观可能性程度。文献[3]将信任定义为在特定的情境下，对某一实体能独立、安全且可靠地完成特定任务的能力的相信程度或坚固信念。文献[4]认为信任是对实体执行某种动作的概率的特殊反映，是经验的体现。Olmedilla 等[5]把信任定义为某一实体 $A$ 根据另一实体 $B$ 在具体阶段、具体环境中关于某一服务的行为表现对实体 $B$ 的信任进行的计算，强调信任的环境、服务域和可计算性。可信计算组织（Trust Computing Group，TCG）把可信定义如下：一个实体的行为如果总是以预期的方式运行，并能达到既定的目标，则实体是可信的[6]。文献[7]把信任定义为根据对某一实体提供服务或行为的长期观察得出对该实体当前提供服务或行为的可信程度或期望评价。总之，信任是对实体行为的主观判断，会随着实体交互行为和时间的变化而变化，并受环境等多种因素的影响，具有主观性、不确定性、传递性等特性。

### 1.1.2　信任的分类

对一个实体的信任不仅限于对实体身份的认证，还需要关注该实体的行为是否在预定范围内合法、有效地实施，实体的行为是否超出了它的授权范围等。基于此将信任划分为两类[8]。

（1）身份信任。这是最传统的可信认证机制，确定实体身份并决定实体的授权。身份信任涉及用户或服务器的身份认证，也就是对主体所声称的身份进行确认，这方面的技术有加密、数据隐藏、数字签名、授权协议及访问控制。

（2）行为信任。相较于身份信任，对实体行为的可信认证更加宽泛，它更注重实体是否能够按照预期完成某项任务，重在对实体行为的评价，通过观察实体行为对实体的能力进行可靠性认证。

通过对实体进行身份认证，可以确定该实体就是要与之进行交易的实体，而不是有人假冒，但是这并不能保证该实体能够按照所期望的那样提供优质服务或供给与请求相符的商品，因此必须对实体的行为进行认证。只有在双重认证的保证下才敢和对方合作。因此，身份信任为交易奠定了基础，而行为信任保证了交易的顺利进行，两

者缺一不可。比较而言，身份信任是静态的，仅是在实体交易开始前对实体进行一些必要检查，确保不存在假冒事件；而行为信任则是动态的，可根据实体间的交易行为动态更新实体间的信任关系，更符合当前网络所需。

在现实生活中，人们通常倾向于和声望值高的人交易，然而，在任何情况下都能完全了解一个人的声望是不可能的，这时其他人的经验就提供了一个参考，因此信任关系又可分为直接信任和推荐信任。

（1）直接信任。在给定的上下文环境中，实体间通过过去的直接交互经验得出对对方实体的信任程度，是对现实中“认识或了解”的抽象，通过直接信任度进行定量表示。

（2）推荐信任。实体间通过第三方（推荐实体）的推荐得出的信任程度，是对现实中“介绍或据说”的抽象，也称为间接信任。

因此，一个实体对另一个实体的可信度量是直接信任和推荐信任的综合，交互的重要程度是对其完成任务的能力、诚实度、可靠性等因素的综合判定。直接信任度的计算依赖于实体间的交互次数、交互时间和交互结果；推荐信任是对不同推荐实体推荐的综合，推荐信任值的大小取决于推荐实体本身的推荐可信度和对目标实体的推荐值。

### 1.1.3　信任的特征

信任来自于人类社会，计算机领域中的信任是对人类社会中的信任的模拟，以人类社会中的信任为基础，根据信任的定义可知，信任具有几个重要特征。

（1）非对称性。信任是单向的、单方面的，不具有对称性。实体 $A$ 信任实体 $B$ 并不意味着实体 $B$ 信任实体 $A$，即使实体间相互信任，它们对对方的信任程度通常也是不同的，$A$ 对 $B$ 的信任值一般不等同于 $B$ 对 $A$ 的信任值。因为信任是主观的，个体间的差异使得对信任的判断也不相同。

（2）有限范围性。实体 $A$ 信任实体 $B$ 并不一定对 $B$ 的一切行为都是信任的，实体 $A$ 对实体 $B$ 的信任是有一定的范围限制的，如服务领域、实体身份等。

（3）时间衰减性。信任随着时间的推移而衰减。一个长时间没有发生过交易的可信任节点可能已经不可信任。离现在越近的交易记录，对信任的影响越大；相反，越久远的历史交易记录，对信任的影响越小。应保证网络中可信的实体不一定永远可信，不可信的实体不一定永远不可信。

（4）传递的有限性。信任不具有完全传递性，信任传递性只在一定条件约束下成立。实体 $A$ 信任实体 $B$，实体 $B$ 信任实体 $C$，并不能推出实体 $A$ 就信任实体 $C$ 的结论。因为实体之间的信任不完全相同，信任会随着路径跳数的增长而衰减，实体 $A$ 对实体 $C$ 的信任程度很可能低于实体 $B$ 对实体 $C$ 的信任程度。非同一信任领域内的信任更不具有传递性。

（5）内容相关性。当一个实体在某种程度上信任其他客体时，总是针对某一特定内容。例如，实体 $A$ 曾经和实体 $B$ 发生过交易，对 $B$ 提供的某种商品非常满意，但是对 $B$ 提供的其他商品就未必有同样的信任程度。

（6）多种对应关系。类似于几何学中集合之间的映射关系，这里实体之间的信任关系同样可以分为一对一、一对多、多对一和多对多的关系。

（7）信任的双重性。信任既具有主观性，又具有客观性。

（8）动态性。动态性即信任与环境（上下文）和时间等因素相关，信任随时间以及上下文的变化而变化，是随时更新的一个动态变量。

（9）可度量性。度量实体的可信程度，划分信任等级。

（10）信任具有不确定性。这是由信任的主观性所决定的。信任的不确定性来自对实体本身的不了解。

（11）信任具有相互性。信任不是单向的，而是双向的。正方向的信任决定是否采取交互行为，而反方向的信任决定对方提供什么质量的服务。

（12）信任程度与当前事件的重要程度有关。当前事件越重要，信任程度可能越低；反之亦然。信任程度与特定事件有关，当我们信任一名技术高超的医生，认为他能医治好我们的疾病时，并不意味着我们同样信任他会是一名好厨师。

## 1.2　信任管理现状

信任管理（trust management）的概念首先由 Blaze 等[9]提出，这是一个涉及社会学、心理学等多个学科的非常重要的研究领域，其基本思想是承认开放系统中安全信息的不完整性，系统的安全决策需要依靠可信任的第三方提供附加的安全信息。Rahman 等[10]则从信任的角度出发，对信任内容和信任程度进行划分，建立相应的信任模型用于信任的数值评估。信任是一个实体对另一个实体的可信赖程度，可区分为身份信任和行为信任。身份信任是对实体身份的信任，基于客观证据，可通过核实标识、证书的真实性和有效性来实现。但身份可信的实体，其行为不一定是可信的，同一个实体在不同的上下文语义下所进行的行为的可信程度也不一定相同，行为信任即判断实体提供某项服务的能力和品质。当前，人们对行为信任管理的研究主要通过建立信任模型加以解决。近几年，国内外众多学者采用不同的理论和方法对行为信任相关问题进行了卓有成效的研究，并提出了很多信任评估模型。

信任模型是对信任关系进行建立和管理的模型，主要是用来解决信任评价的度量问题。通过信任模型的规则计算，信任主体最终可以得到对信任客体的综合评价。信任模型中有以下三个问题值得考虑。

（1）如何构建信任网络，即如何得到简单有效的信任网络推荐关系图。

（2）如何得到信任评价的综合计算，即信任评价的计算算子要规范，保证最终得到的信任评价符合客观实际。

（3）如何保证信任的动态更新，即要考虑信任具有的动态性，对信任评价进行实时更新。

### 1.2.1　信任网络构建

在信任模型中，节点之间的信任关系是通过直接交互来建立的，当缺乏直接的交互经验时，就要通过可信第三方的推荐，对信任关系进行建立，从而形成从源节点到目的节点的信任网络推荐关系图。以信任网络推荐关系图为基础，通过信任的传递与聚合，最终得到源节点对目的节点的综合评价。信任搜索作为信任模型研究的基础，是保证最终得到的信任评价是否符合客观实际的关键所在。因此，设计高效合理的信任网络搜索算法至关重要。

针对信任网络的搜索，现有的大多数信任模型都是以洪泛搜索为基础的。苏锦钿等[11]基于信任网，提出了一种新的推荐机制，通过洪泛搜索，得到信任网中的推荐链，并将推荐链归纳为无依赖、部分依赖和完全依赖三种关系，同时给出了三种策略用于解决完全依赖问题。此推荐机制在一定程度上减少了恶意节点的推荐行为。

蒋黎明等[12]针对证据信任模型中的信任传递与聚合问题，通过结合 D-S 证据理论和图论的方法，引入了信任子图的概念，并通过 EDTR 算法消除了推荐链间的依赖关系，使聚合过程中推荐信息的重复计算等问题得到有效解决，同时也提高了信任传递与聚合的准确性。该模型同样建立在洪泛搜索的基础之上。

秦艳琳等[13]提出了一种分布式环境下信任路径选择性搜索及聚合方法，该算法利用控制条件实现对包含有效信息的路径进行搜索并停止对冗余路径的搜索，在搜索过程中有效地规避了恶意节点。

针对信任评价的综合计算，陈建钧等[14]在考虑复杂网络环境中不确定因素对用户信任影响的基础上，引入正态云模型，提出基于云模型和信任链的信任评价模型。模型中给出了信任传递和聚合的计算规则，解决了由信任链过长导致的评价结果不准确问题。但对于如何防范节点的恶意推荐，该模型并没有提供很好的解决方案。

蒋黎明等[15]根据图论方法提出证据信任模型，在信任聚合过程中，模型解决了普遍存在于现有证据信任模型中的因为对信任链之间依赖关系的无法处理而产生的模型性能下降问题。另外，模型在建模信任度时区分实体的反馈信任度与服务信任度，在证据理论框架下，设计了两种不同的信任传递方法，用于增强模型抵抗恶意推荐攻击的能力。

田春岐等[16]针对 P2P 网络中节点之间难以建立信任关系的现状，提出一种基于聚集超级节点的 P2P 网路信任模型，通过节点分类和反馈信任过滤，使该模型可实现对恶意节点攻击行为的抵御，同时具有低查询开销。

### 1.2.2　信任评价的综合计算

王守信等[17]基于云模型，提出了一种新的主观信任评价方法，此方法以信任云的形式来描述和度量信任程度和不确定度，充分考虑了实体之间信任具有的模糊性和随

机性，并通过主观信任云的历史信息来构造信任变化云，使本方法能够有效地对信任主体的信任决策提供辅助支持。

高伟等[18]改进了 D-S 证据合成规则，将这种规则应用在 P2P 网络信任建模上，他认为基于 D-S 理论的信任模型无法有效合成证据信息，重新分配冲突概率与引入权重系数的策略能够解决该问题。其建立的一种基于 D-S 证据理论的 P2P 信任模型，用来解决传统信任模型很难处理冲突程度高而引起的无法准确计算信任度的问题。

张欣怡等[19]改进证据收集方法来提高证据质量，解决证据收集和冲突证据合成产生不合理结果的问题，在证据合成过程中将冲突证据进行重新分配，结合了证据距离、相似度、支持度和可信度。

汤志海等[20]认为很多国内的电子商务平台选用 eBay 信任模型，而该模型只是对买家反馈评分进行简单累加，进而得到卖家信誉值，并没有区分买家反馈评分的参考价值的重要性和合理性。因此，他提出一种基于群组的 C2C 电子商务信任模型，模型通过计算买卖双方的熟悉程度，计算买家的可信度，充分考虑交易价格、反馈评分、交易时间、交易次数、以往买家的可信度对信誉的影响，建立了电子商务信任模型。

乔秀全等[21]根据社会心理学中的信任产生原理，设计了计算社交网络中基于用户上下文的信任度的方法。社交网络中用户之间的信任度被分为熟悉性信任度和相似性信任度。依据其所起作用的重要度的不同，把相似性分为内部相似性和外部相似性，最后给出了信任度量的具体计算方法。

汪京培等[22]提出了一种基于可信建模过程的信任模型评估算法。将信任模型按照信任生命周期分解成信任的产生、建模、计算、决策和传递这五个部分，然后对每个部分进行可信性分析，最后模糊量化评价结果，用贝叶斯融合形成综合的评估结果。

### 1.2.3　信任的动态更新

李道丰等[23]对实体的状态和所表现的行为进行了充分考虑，提出一种可信网络动态信任模型，模型利用灰色系统理论，通过对实体的状态行为关联进行分析，实现信息的提取过程。此模型能够有效地处理恶意节点的攻击，但模型没有考虑上下文的动态变化。

李小勇等[24]提出了一种符合人类心理认知习惯的动态信任预测模型。模型建立了自适应的基于历史证据窗口的可信性决策方案，该方案克服已有模型常用的计算权重的主观判断方法，解决直接证据不足时的可信性预测问题。利用现有的 DTT（direct trust tree）机制完成对全局反馈信任信息的搜索与结合，进而降低了网络带宽损耗，增强了系统的可扩展性；提出诱导有序加权平均算子的概念，建立了基于该算子的直接信任预测模型，用于克服传统预测模型动态适应能力不高的问题。

Chong 等[25]讨论了能够影响现有信任管理系统的可靠性的威胁和挑战，研究了影响信任管理的重要因素，特别是在处理来自电子商务用户的恶意反馈评级方面。认为即使在动态条件下信任模型必须能够保持准确性，适应从其他方面导致的变化。现有

的工作中，电子商务信任系统经常基于整体性能而不是个体服务性能。这是由于没有把证据的上下文相关性考虑到信任评估中。

国内外研究学者基于不同的理论来度量和构建信任模型，如基于经验和概率的信任模型、基于贝叶斯网络的信任模型、离散的信任模型、基于权重的信任传递方法、基于证据理论的信任模型等。对信任的合并操作采用的方法有算术平均、加权平均、基于权重的信任路径合并、D-S 证据合成规则。分析现有的信任模型，对信任合并和传递的研究还远不够，对信任的研究大多是基于二项式的，对多维信任的研究还不够充分。

分析上面的信任模型，都存在一个问题：没有考虑到人认识事物的主观性。因为信任评价是人给出的，具有主观性、不确定性等特性，无论信任评价如何准确，都不能忽视人的主观因素的影响。

主观逻辑是关于现实世界的主观信任操作的逻辑，Jøsang 等利用主观逻辑[26]对信任关系进行建模，并取得了可喜的成果[27-34]。他提出了主观逻辑信任评价模型，引入证据空间和观点空间的概念来描述和度量信任关系。Jøsang 的 Beta 信任模型已经成为信任管理领域中经典的信任模型之一，他将其很好地应用在开放社区的信任管理中，对计算中的信任进行推理和表示。文献[27]利用主观逻辑进行信任网络分析，它为信任的传递关系提供了一种简单的表达方式，并提供了一种简化网络的方法，这样就可以准确地计算和分析信任网络，然而其折扣算子在信任传递过程中存在信任下降过快的问题。文献[28]对主观逻辑理论做了多项式的扩展，提出四种不同但等价的主观观点表达。它使得我们能够从不同角度来看不确定概率，能够最自然地表达一个具体的现实世界的情况。文献[29]将条件推理从二项扩展到多项观点，使得其能够在任意大小的辨识框架上表达条件和证据观点，使得主观逻辑在引入已知和未知信息条件推理情况下为一个强大的工具，改进和完善了主观逻辑，但其给出的多项式融合算子在融合三个以上观点时，仍然不满足交换率和结合律，导致融合结果不唯一。文献[30]对贝叶斯信誉系统丰富的特征进行了综述，说明其适用于很多不同的问题和环境。文献[31]提出了累积融合算子和平均融合算子，改进原有主观逻辑，而上述问题依然存在。文献[32]利用主观逻辑对条件到结果的映射进行了扩展与新的定义。文献[33]通过简洁的符号表达并行组合信任路径，构造有向系列平行图，融合计算信任路径，然而，其计算复杂度过高，所得结果的准确性也会因为舍弃有用的路径信息变低。因此 Jøsang 等[34]又提出了另一种传递信任网络分析方法保障信任图的规范性。然而，该方法没有描述节点分裂后新出现的边的权重计算方法。

主观逻辑理论对信任管理而言是一个较好的信任推理和表示的理论基础，所以，很多学者越来越重视对主观逻辑理论的研究。

Nir 等[35]借鉴论据理论创造了一个强大的推理机制框架，用来作为证据和推理诊断，通过引入代理交互对话、交流观点和嗅探环境附加信息的传感器，结合来自传感器的信息和观点来构造一个共享的世界观点。

Venkat 等[36]提出了一种新的基于主观逻辑的信任模型用来表达和管理移动节点在与其他节点建立信任关系时的不确定性，提高移动自组网的安全性。

在国内，利用主观逻辑对信任模型的研究相对较少，主要是对主观逻辑的应用研究。

林剑柠等[37]通过对不同交互行为提出的质量要求加以区分，以历史经验作为下次信任评估的重要参考并引入约束关系，根据主观逻辑将其转换为节点间的推荐信任意见。

王勇等[38]借鉴模块之间的执行约束关系，抽象出四种基本约束模式，给出对应直接和推荐信任度的计算方法，而书中循环约束模式的逻辑表示存在一定问题，并且所提出的方法计算复杂度较高。

毕方明等[39]利用方差反映路径推荐值的集中程度，通过引入信任程度参数来划分等级，提出了信任模型，模型中考虑了影响信任的两个重要因素：声誉和风险。

雷环等[40]提出一种结合主观逻辑与声誉的信任网络分析方法，结合朋友间的信任关系和声誉来计算信任值。

谢福鼎等[41]改进了基于信誉随机变量期望的信任更新，减少了当反映当前节点行为时，刻画长期行为趋势的信任更新而出现的失真。

施光源等[42]建立基于行为证明的信任关系评估模型，利用确定下推自动机刻画程序的预期行为，利用虚拟机内省技术考量程序的实际行为与预期行为的一致性，进而判断程序的可信性，根据证明结果进行信任关系评估。

## 1.3 本章小结

在开放网络中，信息安全是至关重要的，而信任管理是信息安全的前提与基础。近几年，研究小组在信任模型相关问题上进行了深入研究，在信任网络构建、信任模型扩展、风险评估、软件行为可信方面均取得了一定成果，主要工作如下。

1. 在信任网络构建方面

（1）提出了基于信任领域的信任模型[43]，将网络划分为多个信任域，每个域由一个域代理和若干个实体代理分层组织管理网络实体。通过代理间周期性地通信避免了代理间维护信息的不一致性问题。模型区分节点在不同交易行为时的可信程度，计算节点的全局买声誉和卖声誉。为了给用户提供信任度高且和用户要求的服务更匹配的服务，模型将服务提供者对服务的认知度作为重要因素考虑进来，用服务的相似度加权调和综合信任值，而且模型每次交易完成后对实体全局声誉的及时更新节省了用户等待服务请求响应的时间。

（2）提出了基于加权紧密度的信任路径合并策略[44]，旨在为分布式网络安全和信任机制提供支撑。利用加权紧密度实现信任路径的合并，充分考虑了网络中的信任路