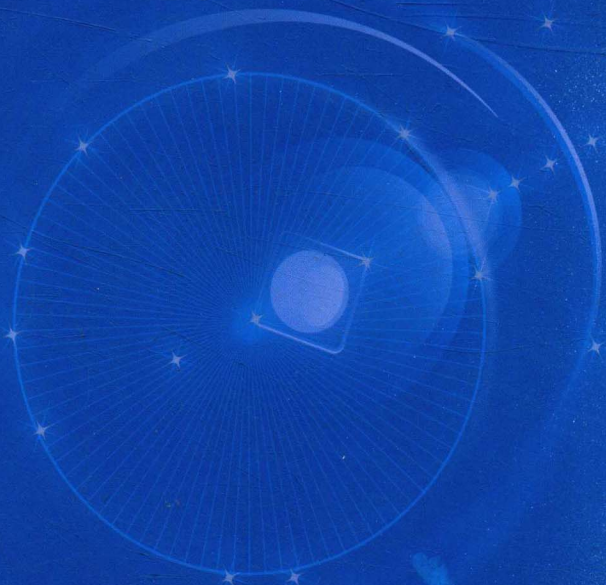
可信物联网技术

张德干　许光全　孙达志　著



科学出版社

可信物联网技术

张德干　许光全　孙达志　著

科学出版社

北京

内 容 简 介

可信物联网技术即确保物联网安全、可信或可靠的一系列技术，研究这些技术十分重要。本书阐述的“可信物联网技术”主要包括无线传感网络可靠定位、无线传感网络节能路由、无线 Mesh 网络多播路由优化、信任及其管理、信任量化及计算、用户智能卡实体认证、服务器辅助公开密钥认证和大数模幂计算等技术。

本书可供物联网、信息安全相关专业的高年级本科生、研究生、教师学习和参考，也适合相关领域的科研和工程技术人员阅读、参考。

图书在版编目 (CIP) 数据

可信物联网技术/张德干，许光全，孙达志著．—北京：科学出版社，2015.10

ISBN 978-7-03-046056-1

Ⅰ．①可… Ⅱ．①张… ②许… ③孙… Ⅲ．①互联网络－安全技术②智能技术－安全技术 Ⅳ．①TP393.4②TP18

中国版本图书馆 CIP 数据核字(2015)第 249491 号

责任编辑：任 静 / 责任校对：郭瑞芝

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

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2015 年 10 月第 一 版 开本：720×1 000 1/16

2015 年 10 月第一次印刷 印张：20

字数：375 000

定价：96.00 元

（如有印装质量问题，我社负责调换）

作 者 简 介

张德干，男，湖北黄冈英山县人，博士（后），教授，博导。研究方向为物联网、移动计算、智能控制、无线通信等技术。主持国家 863 计划项目、国家自然科学基金项目、教育部新世纪优秀人才计划项目等十余项，在国内外期刊和会议上以第一作者发表论文 130 余篇（40 篇 SCI 索引，90 篇 EI 索引）。出版学术专著多部，获得专利多项，获得科技奖励多项，是多个国际会议的大会主席。

个人主页：http://shenbo.org.tjut.edu.cn/tt/personinfo.asp?bianhao=199

许光全，男，湖南浏阳人，博士，副教授，硕导。研究方向为可信计算、信息与网络安全等技术。主持（或参与）国家自然科学基金项目、天津市自然科学基金项目等多项，在国内外期刊或学术会议上发表论文近 50 篇，获得发明专利多项，担任多项学术兼职。

个人主页：http://cs.tju.edu.cn/faculty/xugq/

孙达志，男，辽宁葫芦岛市人，博士（后），副教授，硕导。研究方向为信息与网络安全、可信计算、应用密码学、物联网等技术。主持（或参与）国家自然科学基金项目、天津市自然科学基金项目等多项，在国内外期刊和会议上发表论文 30 余篇，获得专利多项。

个人主页：http://cs.tju.edu.cn/faculty/sundazhi/

前　言

伴随着物联网（Internet of Things）的蓬勃发展，新型的网络计算模式不断涌现，为用户提供了各种简单、透明的方式来动态获取大规模计算和存储服务，有效推动了资源共享和综合利用。然而物联网环境固有的分布、自治、动态特征，应用领域的边界开放、需求动态增长趋势，使网络计算环境的信任管理技术面临诸多挑战。信任建立和隐私保护等成为当前可信计算（Trusted Computing）的重要问题。

可信物联网技术涵盖确保物联网安全、可信或可靠的众多技术，本书重点阐述了如下几方面：无线传感器网络的可靠定位、节能路由以及路由优化技术，适应不同网络应用环境的信任管理模型与量化计算技术，基于集成电路卡的认证技术和多维模幂计算方法，会话密钥协商协议等。

本书共分 10 章。第 2～4 章由张德干撰写，第 5 章和第 6 章由许光全撰写，第 7～9 章由孙达志撰写。第 1 章和第 10 章为三人共同撰写。全书由张德干策划和统稿。

本书得到国家 863 计划项目（No.2007AA01Z188）、国家自然科学基金项目（No.61572355、No.61202169、No.61571328）、教育部新世纪优秀人才计划项目（No.NCET-09-0895）、教育部科技计划重点项目（No.208010）、天津市自然科学基金项目（No.15JCYBJC15700）、天津市自然科学基金重点项目（No.13JCZDJC34600）、天津理工大学计算机与通信工程学院“智能计算及软件新技术”天津市重点实验室和“计算机视觉与系统”省部共建教育部重点实验室相关基金、天津市“物联网智能信息处理”科技创新团队基金（No.TD12-5016）、天津大学网络安全联合实验室基金的资助。

本书由张晓丹研究员和宁红云教授审阅。

本书在撰写过程中，多位教授和专家学者提出了宝贵意见，同时，得到了韩静、赵德新等同事，博士和硕士研究生明学超、朱亚男、赵晨鹏、宋孝东、郑可、潘兆华、刘思、戴文博、康学净、程英、王冬、胡玉霞、刘朝敬、梁彦嫔、董丹超等的支持和帮助，在此一并表示衷心的感谢。

本书属研究型专著，可供高等院校研究生、高年级本科生、相关领域的科研人员和工程技术人员参考。

限于作者水平，书中不足之处在所难免，真诚欢迎各位专家、读者批评指正。

作　者

2015 年 7 月

目　录

第1章 绪 论

1.1 信 任

1.1.1 简介

信任作为一种非正式的社会资本，无论在哪个社会中，它在维系社会稳定、推动社会进步方面的地位是独特的，同时也是无可替代的。人类社会有史以来，对信任的研究和探索就从来没有中断过。

古人把“仁义礼智信”作为君子的六大美德，其中最后的“信”，就是告诫人们，只有做到“守信，信守诺言，一诺千金”的人才有被称为“君子”的条件和资格。吉诺维希（1713—1779）和多利亚认为，信任某人就包含了一种相信被信任对象会履行这样的责任的信念（belief）。他们强调的是这样的一种信念，即相信被信任方不会以背叛的方式去行事。

在文集《信任：合作关系的建立与破坏》中，对信任的定义达成了一定程度的共识：信任（或不信任）是一个行动者（actor）评估另一个或一群行动者将会进行某一特定行动的主观概率水平。这里包含两层意思：首先，信任是建立在行动的基础上的，只有行动的存在，信任才有可能发生，否则信任是无从谈起的；其次，信任是行动者（施信者（trustor））对受信者（trustee）在行动上的行事方式的一种主观预测，这种预测的结果是以概率的方式来表述的。他的这种评估（预测）发生在监控（monitor）此特定行动之前（或者即使他能够监控此行动，也无法去监控），而且这种评估在一定的情境下做出，并影响了该行动者自己的行动。

在通常情况下，信任包含着可靠性，即认为合作者可信赖、守信用。然而，诚实和可靠并不总是会促进信任。如果一位合作伙伴经常要惩罚你并且真的那么做，那么他可能是诚实可靠的，但却不是值得信任的。真正的信任是，双方建立起这样的关系：一方关心另一方的利益，任何一方在采取行动之前都会考虑自己的行动对另一方所产生的影响。总之，对于信任概念的理解，有以下几点。

（1）对他人行为处于不了解或不确定状态，这是信任概念的核心。这一点涉及人类认知能力的局限性——即不可能获取有关别人的完全知识。信任是对于未知领域的一种暂时性的本质上很脆弱的反应，是弥补“预见能力有限性”的一种方法。

（2）信任还与行动者有可能使人们的期望落空这一事实有关。在需要信任的场合，也必定存在退出、出卖和背叛的可能。

（3）信任一个人意味着相信他即使在有机会伤害别人的情况下，也不会以一种伤害的方式去行动。

（4）信任是特殊的信念，它的出现不是依赖于正面证据而是依赖于缺乏反面证据——这个特征使得信任极容易被蓄意破坏。相反，深厚的不信任却很难通过经验而被消除，因为它阻止人们参与恰当的社会实践，而且更为糟糕的是它导致了那些反过来又进一步促进不信任的行为发生。

（5）信任可以通过使用而增加。如果它不是无条件地赐予，那么它可以在接受方激起更强的责任感。事实上，信任既是一种“非正式制度”，又是一种“社会资本”，这种社会资本不是针对个体资本的社会资本，而是针对物质资本和人力资本的社会关系资本。一般地，人们不会以对自己有害的方式行事，在这个社会关系网络中，人们只会以责任来回报信任。因为人们都清楚“一荣俱荣，一损俱损”的道理。当然，因为制度和监控手段的缺乏和无力，少数的欺骗和背叛的存在是可以理解的。

（6）信任至少包含两个方面的含义：首先，它与交互行为（多次行动的结果就演化为行为）的发生过程紧密联系在一起，没有交互行动的存在，信任也就失去了滋生的土壤。只有在行动中，信任才有存在的可能和必要。这里必须强调：这一点与信誉、依赖性等不同，信誉的存在是因为以往交互行为的积累而产生的一种感观上的印象。其次，信任是一种信念，或者叫做倾向、势，这与重力势能类似。只有这种信任势的存在，信任才有可能发生。

目前，尽管许多研究人员都给出各自的关于信任概念方面的定义和描述，但还不存在一个广为接受的定义，我们认为信任的概念描述至少应该由三部分组成：信任是什么？产生信任的前提条件（或场合）和作用等相关方面的描述。信任的特性。

信任是信任主体（包括施信者与受信者）在交互过程中体现出来的一种情感倾向（affective propensity/attitude），它典型地存在于劳动力分工的商品社会中，人与人之间必须要进行相互依赖的风险（并且这时候风险总是在理性选择的接受范围之外）活动中，它具有社会性（sociality）、交互性（interaction）、历史性（historicity）和动态性（dynamic）等特征。

上述定义很好地回答了前面提到的三个问题。

（1）信任是什么？

从定义可以知道，信任是一种情感倾向（或者叫做“信任势能”），但是它不同于普通的情感，它必须包括典型的信任结构：信任人（施信者）+被信任人（受信者）+交互行为+交互环境，而且很明显，我们的定义是与下面提到的三方互惠决定论（人、行为、环境）一致的。

（2）产生信任的前提条件（或场合）和作用等相关方面的描述。

很明显，定义明确说明信任产生的场合和作用：典型地存在于劳动力分工的商品社会中，人与人之间必须要进行相互依赖的风险（并且这时候风险总是在理性选择的

接受范围之外）活动中。也就是说，劳动力分工和相互依赖的存在迫使人们选择伴有信任的交互行为，这种行为的开展从根本上进一步促进了劳动力分工的进程，也可以说促进了整个社会的进步。

（3）信任的特性。

最后一句话很明白地说明了信任的一些基本特征：社会性、交互性、历史性和动态性等。

说完信任本身，还要解释一下与之相关的一些概念。目前，关于信任研究中提出的相关概念很多，而且各个概念之间相互混用的情况也比比皆是。以下是一些常见的有关概念：信任 trust(vt., n.)，可信赖的、可靠的 trustworthy（adj.）(-thiness 可靠)，信誉（声誉）reputation 或 credit (n.)，相信 believe (v.)，信心 belief 或 confidence (n.)、信念 faith (n.)等。

一般地，可以从以下几点加以区分和理解上述提及的常见概念。

（1）“信任（trust）”与“信用（trustworthiness；credit）”、“信誉（credit；prestige）”是同中有异的一组概念。在信用或信誉中，存在着信任的涵义，这样，信任就可以理解为这一组概念的基础性概念。其实信任本身具有两重含义，其一是心理情感的一面；其二是行为表现的一面（这就是信任关系，现有研究没有区别“信任”和“信任关系”，这也就为此领域研究增加了许多难以澄清的争执），心理情感影响人的行为表现，但二者并不一定统一。

（2）一般认为，信任作为一种情感倾向，可用作动词也可以用作名词。作动词时是及物动词，后面必须有受信者；作名词时指的是施信者对整个交互的一个预期倾向。它的影响因素很多，包括信任主体的信誉（reputation 或 credit）情况，信任主体对整个交互行为成功的信心（belief 或 confidence），信任主体的某些信念（如信任偏向，有的人喜欢信任亲人——亲缘（类亲缘）信任群，有的人喜欢信任同一组织的人——群体（组织）归属信任群，有的人喜欢信任男人/女人，有的人喜欢信任共同经历的人——经历共鸣信任群），以及其他的一些更加复杂的因素。可信赖的、可靠的 trustworthy（-thiness 可靠）可以用来表示信任的整体评价。

（3）信誉作为信任主体在以往交互中的表现情况的载体，是信任主体的信任量表，是历史显现物（history unfold），它有时是可靠的，有时却是带有欺骗性的，它在作信任决定时所起的作用往往是关键的，因为在有选择的交互活动中，其他因素可能大致相同，但是个体的信誉情况有时候是大相径庭的。有的研究人员把信誉作为信任值来看待。

（4）信任和信誉都是社会认知概念，前者具有更加复杂的表现形式和认知结构；它们都与其他认知概念一样，在可度量性方面的讨论由来已久。个人认为，信任作为一种情感倾向，是与具体的交互活动联系在一起的，它只有在交互环境下才有讨论和研究的意义，它的研究对象是整个交互活动涉及的所有要素（包括信任主体、交互活动本身、环境等），所以说信任与其说是行动的，不如说是关联的。

（5）著名的社会学家卢曼（Luhmann）则区分了信任和相信：信任和相信是两种不同的声明自己期望的途径（前者通过具体的交互活动，后者则与认知心理紧密相连，是基于事先评估的），这种期望可能会落空。二者在人们获得自我证实的感觉或者（用Gambetta 的话说）面临不确定性时所采取的行动方面也是不同的（前者在采取行动时是主动的关联行为，后者是被动的孤立行为）。

（6）信心 belief 或 confidence (n.)、信念 faith (n.)指的是信任主体针对信任认知结构中的每一成分所持有的评估和预期。例如，对受信者完成任务的能力的信心，对对方对自己的依赖的信心(这是在有选择余地的时候)，对信任主体的道德估计的信心等。

总之，这几个概念是既有联系又有区别的，在使用术语时，应尽量避免指代不明的情况。其中，信任是统领其他几个概念的总纲，其他概念都是因为信任的存在而衍生出来的，目前大部分对信任的研究主要集中在信任主体的信誉研究上，而忽视了对其他认知成分的必要探究。

1.1.2　信任的功能、分类及其构建

前面已经提到，信任在人类社会中所扮演的角色是举足轻重的，同时也是无可替代的。只要人与人之间存在着交互，总会由于各种不确定性要素而存在着风险，这样交互双方就不得不选择“信任”这样的方式来行事。因此，信任首先是促进了交互行动，其直接后果就是推动了商品交易，推进了商品经济的发展，促进了商品社会的进步。其次，信任还在充当着可靠的“社会资本”和“非正式制度”的基础上，维系着整个社会的稳定和有条不紊的秩序。

Luhmann 认为：信任最基本的功能就是“简化”社会交往复杂性的功能。在卢曼看来，归根结底，信任在社会中所起的作用就是简化了交易程序。或者可以这么说，正是由于信任的存在，那些对交易对象有所踌躇的行动者在进行交易决策的时候就会变得简单多了。但社会需求的不止是一种“简化”功能。卢曼甚至认为，“不信任”和“信任”是相辅相成的，同样具有“简化”功能，只有在一个“不信任”被制度化了的系统里，也就是说具有完备的监督机制的系统里，“信任”机制才能正常地发挥它的功能。

此外，卢曼、威廉姆森和科尔曼都一致把信任视为降低交易和监督成本的机制的同时，也都指出，信任实质上是建立在成本—收益上的一种“风险行动”。显然，在大多数场合，交易双方依赖的是信任。只有把交易行为建立在信任的基础上，那些依赖正式制度和法律等监督手段与交易的成本才有可能得到控制和降低。但是，事实上，这样的一种非正式化的社会资本有时候又只是一种带有风险的“脆弱”的行动。

继卢曼之后，美国学者巴伯（Barber）在《信任的逻辑和局限》一书中，把人们的信任分成不同的层次：最高的层次就是对自然秩序和社会秩序的信任，其次是信任专业和权威人士控制社会秩序的能力，最后是信任社会交往的对方能够履行其义务和

责任。在巴伯看来，信任体系的危机通常是发生在后两个层次，它来自权力、知识的滥用带来的监督失效。

我们认为，信任关系决定了信任的基本内涵，即人情信用＋契约信用＝信任。所以说，人情信用和契约信用二者并不具有完全替代的意义，它们从不同的层次，调节着人们的社会经济生活。尽管二者的具体运行规则不同，但深层的道理都是一样的。

意大利学者吉诺维希认为，正是这种信任（公众信任），也只有这种信任不仅支持了整个国家内部的整合，而且构成了它对于其他国家的可信性。私人信任是公众信任的必要条件，固然，信任（公众信任）依赖于预见的可靠性。公正正是信任的必要条件，这是因为没有人会信任与他处于不同法律地位的人。这或许可以作为信任的最完整的功能来描述。

除了卢曼的人际信任和制度信任以及吉诺维希的公众信任和私人信任，还有德国社会学家韦伯（Webber）的普遍信任和特殊信任。韦伯所谓特殊信任是指对有共同经历、相互熟悉或有特殊关系的人的信任，而一般信任（普遍信任、社会信任）指对普通人的信任，两者共同构成了人际信任。前者是指信任的确立是以特殊的亲情如血缘、亲戚、朋友、地域等为基础，并以道德、意识形态等非制度化的东西作为保障，信任的主体可以是个人、家庭、家族，也可以大到一个地方。人际信任的信任半径较之社会信任要小，主要限于亲属、朋友等特殊的私人关系范围，因此又可称为特殊信任，而社会信任在被信任者与给予信任者之间并无特殊关系，即信任可以被贯彻到与自己无血缘关系或私人关系的其他人身上。

关于信任与人际关系的讨论，列维斯和维尔加特直接将信任理解为人际关系的产物，提出了不同类型群体中信任的不同内涵。他们认为，信任是由人际关系中的理性计算和情感关联决定的人际态度。理性与情感是人际信任中的两个重要维度，两者的不同组合可以形成不同类型的信任。其中，认知型信任（cognitive trust）和情感型信任（emotional trust）是最重要的两种。日常生活中的人际信任大多是这两种信任的组合。在首属团体关系（家庭）中，信任的主要内容以感情为主，在次属群体关系中，信任主要以理性为基础。他们还认为，随着人口增长，社会结构分化，越来越多的社会关系是以认知型信任而不是以情感型信任为基础的。

祖克尔为了说明控制与信任的关系，从发生学的角度提出了信任的三个层面构建：一是基于交往经验（过程）的信任。这种信任来自于交往、交换和交易经验的积累，互惠性是其核心。二是基于行动者具有的社会的、文化的特性的信任。Good 认为，信任的基础是个体的，是产生于个性的合法行为。他指出这种信任强调团体成员的身份、资格和熟悉度。对于以上两种信任，Creed 和 Miles 给出了一个函数表达式：信任＝f｛嵌入对信任的偏好、模仿性特征、互惠性经验｝。三是基于制度的信任。这种信任是建立在社会规范和制度基础上。

按照信任的来源，可以分为两大类：感性信任和理性信任。怎么定义感性信任和理性信任呢？假设在一个组织中，有两个系统管理员，各自管理自己的系统，也相互

尊重个人的技能。每个管理员都信任自己的和对方的系统，尽管信任程度可能相同，但信任机制完全不同。前者是基于对自己系统的完全控制，这是理性的；后者是基于对对方的相信，这是感性的。因此，定义感性信任某个实体是指相信它不会有恶意的行为，理性信任（BAN-Logic 和安全评价标准（security evaluation criteria）是两种常用的模型）某个实体是指相信它能抵抗任意恶意的攻击。

总之，当代社会学对信任的研究由两支理论组成：一支关注信任的功能，认为信任是一种简化机制，它由卢曼提出（1979 年《信任与权力》以及 1988 年《熟悉、信赖、信任：问题与替代选择》）。信任将复杂事物简化，将不确定性简化，以此来确定是否与之合作。所谓疑人不用，用人不疑。由此信任简化打开了行动的可能。另一支关注信任的结构，就是说信任如何构成，是因什么而信任。此支理论由以色列社会学家艾森斯塔德提出，在古登斯那里得到很好地概括。古登斯认为信任存在两类，即人格信任和系统信任。

1.1.3　信任、信誉与评价机制

有效的评价机制是信任建立和管理的必要前提。当施信者在寻找合作伙伴的时候，他们总是会利用已有的直接经验或者间接经验，以及与之相关的社会网络关系来对合作候选人进行评估，根据评估结果和自身的一些经验知识（有时候还包括一些非理性的东西，如感情用事、盲目信任或者不信任）对合作的前景进行预测，看看获利情况是否理想，或者是否实现交互目标等来判断是否与之交互合作。需要指出的是，根据牛津英语词典，信誉是“关于一个人的个性和其他品质方面的总体评价”。这种评价必须是在不同信息源的帮助下形成和不断更新的。由此可见，一个人的信誉情况其实是对这个人的几乎所有品质的一个总体描述，其中不仅包括每个个体之间千差万别的个性（性格），还有其他人类至今仍然没有完全了解的如情感、感知等非常复杂的思维规律，因此，对一个人的信誉进行评估和预测是一个系统的、综合的相当复杂的伟大工程，它的探索过程必然是漫长的、艰辛的。但是，随着计算机、心理学、神经学、人工智能等各方面的科学技术的快速发展，相信人们很快就会在相关的研究领域取得突破，信任和信誉机制也将会更好地掌握。

关于信任与合作的关系，首先，有一个问题值得深思：信任是合作产生的前提还是结果？动物之间存在合作好像表明合作的发生并不一定要以信任为前提——动物不可能具有信任这种主观的东西。因此说信任是合作的成果而非前提。在刚开始时，合作可能只是随机的由一系列幸运的实践促成的，而不是由信任促成的，然后（借助于不同程度的学习和主观意愿）得以选择地保留下来。

合作经常需要一定程度的信任，特别是相互信任。一般情况下，没有信任的存在，合作是很难建立起来的。当然，事实表明，在某些场合，不借助信任也是可以产生合作的，其中的一种方法是：集中力量对约束和利益进行操纵，因为这些正是人们能有意识地、最有效地加以控制的合作条件。实际上，在约束和利益能够完全被操控（当