INTERNET OF THINGS

物联网环境下信任模型及其应用研究

◆陈振国 著

清华大学出版社
http://www.tup.com.cn
北京交通大学出版社
http://www.bjtup.com.cn

物联网环境下信任模型及其应用研究

陈振国　著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

随着智慧城市、数字医疗、智能家居等技术的发展和普及，物联网已经深入人们生产生活的各个领域，极大地便利和改善了人们的生产和生活水平，但其安全问题也日益凸显，如何保障物联网应用过程中的设备安全、通信安全、数据安全成为当下研究的热点。

本书从保障物联网中感知设备的可信和感知数据的可靠的角度出发，以感知数据为基础，并结合行为等因素构造了一个结构相对统一的信任框架模型，并对其应用形式进行了较为深入的研究。本书在概述研究背景、意义和动机的基础上，对当前物联网环境下的信任模型的研究及应用现状进行了较深入的分析，并就物联网环境下信任模型的设计及应用进行了五个方面的探索研究，取得了一定的成果。

图书在版编目(CIP)数据

物联网环境下信任模型及其应用研究/陈振国著.—北京：北京交通大学出版社：清华大学出版社，2019.3
ISBN 978-7-5121-3813-1

Ⅰ.①物… Ⅱ.①陈… Ⅲ.①互联网络-研究 Ⅳ.①TP393.4

中国版本图书馆 CIP 数据核字（2019）第 025287 号

物联网环境下信任模型及其应用研究
WULIANWANG HUANJING XIA XINREN MOXING JIQI YINGYONG YANJIU

责任编辑：谭文芳
出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010-62776969
　　北京交通大学出版社　邮编：100044　电话：010-51686414
印 刷 者：艺堂印刷（天津）有限公司
经　　销：全国新华书店
开　　本：145 mm×210 mm　印张：4.875　字数：131 千字
版　　次：2019 年 3 月第 1 版　2019 年 3 月第 1 次印刷
书　　号：ISBN 978-7-5121-3813-1/TP · 872
印　　数：1～1000 册　定价：48.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。
投诉电话：010-51686043；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

背景

自 1999 年物联网（Internet of things，IoT）的概念被提出以来，物联网在全球范围内获得了广泛的关注和认可，成为新一轮技术发展创新的动力，出现了大量的新技术、新产品和新的模式，其应用领域和应用范围不断拓展，已经逐步融入人们的生产和日常生活中。从智慧城市、智能电网、智慧农业、智能物流、智能家居到智能交通、车联网，再到应用于家庭的智能恒温器，智能电灯等设备，以及与身体健康相关的智能穿戴设备、雾霾监测系统等，每一种智能设备和系统的出现，都大大便利和提升了人们的生产和生活水平。但随之也带来了诸多的安全风险和隐私问题。在物联网环境中，智能的物理设备都能自发、自动地与其他智能设备或外部世界进行通信，这样就要求解决物联网中设备之间的信任问题。无处不在的物联网智能终端，诸如摄像头、智能恒温器等设备，在不定时地采集各种信息，也直接或间接地导致了隐私的泄露。此外，物联网的应用大多处于开放的环境中，所以很难定义一个安全的边界，并且也不能保证在感知、传输、处理或其他操作的过程中数据不会产生变化。在大规模的部署环境中，很难直接应用传统的安全策略和方法，因此如何保证物联网中数据的可靠和可信也成为当下研究的热点。

内容

本书从保障物联网中感知设备的可信和感知数据的可靠两

方面出发，以感知数据为基础，并结合行为等因素构造了一个结构相对统一的信任框架模型，并对其应用形式进行较为深入的研究。本书在概述研究背景、意义和动机的基础上，对当前物联网环境下的信任模型及应用现状进行了较深入的分析，并就物联网环境下信任模型的设计及应用进行了五个方面的探索研究，取得了一定的成果。本书第 3 章基于物联网中感知数据与感知设备的状态具有直接相关的特点，提出了一种数据驱动的信任模型设计方法；而后在第 4 章结合雾霾感知源数据敏感的特点，给出了一种利用监测数据构建信任模型并对雾霾感知源进行评价的方法；第 5 章将数据和行为等因素作为信任评价的依据，提出一种多因素信任模型，并对其在传感器数据融合方面的应用进行了探索；第 6 章则通过统计人与物之间的交互数据构造信任模型，再结合社会关系中朋友推荐策略，构造了一种基于交互信任的物联网隐私保护方法；第 7 章则通过统计物联网数据平台下用户的历史行为、用户之间的交互行为，构造了基于用户行为数据的信任评价方法，实现用户的异常检测及访问控制。最后对本书的主要研究成果进行了梳理和总结，并对后续的研究方向和研究内容进行了展望。

致谢

作者的研究工作得到了河北省物联网监控工程技术研究中心、廊坊市市级大数据智能处理与安全保障重点实验室的支持，得到了国家重点基础研究发展计划（973 计划）前期专项（2011CB311809），国家自然科学基金项目（61163050，61472137），河北省科技计划项目（15210703），中央高校基本科研业务费（3142015022，3142013098，3142013070）的资助。

本书的研究工作是在导师林闯教授的指导下完成的，感谢林老师的教诲和帮助；另外，也非常感谢田立勤教授对本书研究工作所提供的指导和帮助，感谢谭文芳老师在本书出版过程中所做的细致、辛苦的工作。

由于作者水平所限，加之物联网安全领域的新技术、新方法仍在不断地发展和变化，书中不足之处在所难免，恳请专家、读者指正。

作　者

2018 年 6 月

目　录

第1章 概 述

1.1 物联网发展进入新阶段

当前，面对世界经济复苏曲折的背景，以及以物联网、云计算、大数据等为代表的信息技术正在转化为现实生产力的历史机遇，各个国家纷纷利用自身优势加快在行业应用、传感器件等技术方面的布局，把握物联网新一轮的发展机遇。中国信息通信研究院2016年发布的物联网白皮书中指出，物联网应用在全球范围内呈现加速发展的态势，各种物联网应用的普及和技术的不断成熟，逐步推动网络技术进入万物互联的新时代，物联网已经逐步融入人们的生产和日常生活中。从智慧城市、智能电网、智慧农业、智能物流、智能家居到智能交通、车联网，再到应用于家庭的智能恒温器，智能电灯等设备，以及与身体健康相关的智能穿戴设备、雾霾监测系统等，每一种智能设备和系统的出现，都大大便利和提升了人们的生产和生活水平[1-7]。

另外，传统产业的智能化升级成为进一步推动物联网创新发展的契机，而规模化消费市场的兴起则加速了物联网的推广和扩展。面对经济下行的压力和新技术的出现，各重要国家都制定了新的工业发展的战略方案，如美国的“先进制造业伙伴”计划、德国的“工业4.0”计划和中国的“中国制造2025”计划等。这些都奠定了物联网作为工业互联网、智能制造发展的基础，成为生产能力加速提升和服务化转型的主要推动者。

从全球范围来看，物联网技术及应用的发展进入到新的阶段。各主要国家构建了基于物联网的立体化信息采集网络，实现了对多种信息的全面实时采集，同时开展各领域应用技术的研发和试验示范，推动了物联网在各领域应用的发展。2016 年统计，美国的物联网支出将从 2 320 亿美元增长到 2019 年的 3 570 亿美元，复合年增长率将达到 15.4%，并重点推动智能传感器、数据分析和系统控制的研发、部署和应用。欧盟则通过“地平线 2020”研发计划，在物联网领域投入近 2 亿欧元，推动物联网集成和平台研究的创新，重点在智慧城市、智能农业和食品安全等领域开展大规模示范，为物联网的应用扩展奠基。日本、韩国和俄罗斯同样在物联网领域持续加大推进力度，预计日本 2020 年物联网的产业规模将达到 138 000 亿日元；韩国则准备在未来 10 年投入超过 2 万亿韩元的研究基金，推动智慧城市等九大项目的实施；俄罗斯则首次对外宣称启动物联网研究和应用部署，预计 2020 年至少实施 20 个试验项目。我国物联网的发展在政府、行业等的共同努力下，取得了显著成效，2015 年的产业规模超过 7 500 亿元，年复合增长率超过 25%，新制定或梳理相关标准 900 余项，已形成环渤海、长三角、泛珠三角及中西部地区四大产业聚集区，在智能制造、智慧城市、车联网等领域取得了长足发展。具国际数据公司预测，到 2020 年全球物联网的市场规模将达到 7 万亿美元[8]。

1.2　物联网安全问题日益凸显

随着物联网、云计算、大数据等新技术的兴起和不断地发展成熟，其应用领域也在不断地拓展，由此带来的安全问题日益受到人们的关注。物联网的基础与核心仍然是互联网，物联网是互联网的延伸，而云计算、大数据等技术则使得物联网的

应用架构更为完整。因此物联网不仅天然携带了互联网的安全问题，同时由于其自身网络泛在、全面感知、可靠传输和智能处理等特征，使得物联网面临的安全威胁更为突出，不仅会产生重大的财产损失和隐私问题，甚至会威胁到生命安全。如2010年爆出的震网病毒就对多国的电力系统造成了大规模的破坏[9]；2016年Mirai僵尸网络通过感染网络摄像头等物联网设备进行传播，对DNS提供商Dyn发起了拒绝服务攻击，造成大面积断网[10]。另外，当前国家、行业和个人的物联网安全和隐私保护意识薄弱，而物联网应用所部署的很多信息采集设备都会直接或间接地暴露用户的隐私信息，Pew研究中心最新的统计结果表明，52%的患者同意共享其医疗数据，44%的用户同意共享其居住环境的数据，这些都存在巨大的安全和隐私泄露的风险[11]。同时，物联网设备生产相关企业大多认为增加安全措施不会对其产品的市场销售有太大的促进作用，而且还会增加额外的成本，因此物联网中的大量设备存在无安全措施或者仅有简单的安全策略的状况[12]，这使得物联网中的设备极易受到伪装、捕获、数据泄露和篡改等攻击。

近年来，世界范围内由物联网引发的安全事件更加频繁且严重。2016年8月研究人员发现了汽车遥控钥匙的两大漏洞，黑客可利用技术手段非常容易地入侵汽车遥控门锁系统，致使全世界有一亿辆汽车受到影响。2016年11月俄罗斯五家主流大型银行遭遇来自30个国家2.4万台智能设备构成的僵尸网络持续两天不间断的DDoS攻击，攻击源和攻击形式多样，该僵尸网络不仅包含计算机，还包括物联网设备，甚至微波炉之类的家用电器也牵扯其中。面对这些问题，互联网提供商使用的标准安全手段难以发挥作用。在我国，物联网带来的安全问题也非常严峻，某公司安全团队发现了多个汽车的云漏洞，并攻破了某些智能家居、豆浆机、智能烤箱等设备的控制系统。这些都

表明，物联网的安全问题日益凸显。

鉴于物联网与大数据的紧密联系，因此在物联网快速发展的当下，物联网应用所产生的数据规模越来越大，每个人都是数据的产生者、拥有者和消费者，而数据在采集、传输、处理和应用中面临着诸多安全风险。在物联网中的应用，若安全问题不能有效解决必然导致数据的不可信和虚假，而虚假数据将导致错误或无效的数据分析结果。另外，数据来源形式多样，可以是人们在（移动）互联网活动中所产生的各种信息，也可以是各类计算机信息系统所产生的数据，也可以是各种感知设备所感知或采集的数据。每一种来源都存在复杂的数据产生、传输环境，再加上数据在存储过程中所面临的各种风险，这些都有可能导致数据的无效，因此如何保障物联网数据的可信与有效也成为当前研究者关注的重要问题[13-16]。

1.3　研究动机与意义

1.3.1　研究动机

本书的主要研究目标是以感知数据和结点行为为基础，力图构建结构相对统一的信任框架模型，并对其应用策略进行研究，实现物联网中结点、数据的安全可靠。之所以以此为研究目标，主要有如下几个方面的原因。

（1）信任模型利于物联网的应用场景

在物联网应用场景中，很多物理设备都是资源（计算、存储、能量）受限的，使得传统算法难以有效发挥作用，即便进行了轻量化处理，资源消耗仍较多，而信任机制则可以充分利用物联网已有的信息，实现对物联网中的设备和数据的安全保障，且计算、能耗开销小，适合资源受限的环境。

(2) 物联网中的感知数据对结点状态具有直观反映

通过分析发现，有很大比例的物联网应用都有感知或捕获数据的需要，并且很多情况下，所感知或捕获的数据存在时间上连续、非跳跃的特点。而对于具有感知或捕获数据功能的物联网应用，其所感知或捕获的数据的可靠与否是结点状态是否正常的直观反映，因此可以通过感知数据的分析对结点的状态进行判断，从而发现并剔除异常数据确保感知数据的可靠。

(3) 在感知数据的基础上考虑其他影响因素实现信任模型构建可提升信任评价的效果和准确性

感知数据能够直观地反映结点的状态，而结点的行为同样是结点状态的一个直观体现，因此结合数据和行为等多个因素可以实现更为准确的评价。

1.3.2 研究意义

随着物联网技术的发展和普及，物联网的安全问题成为我们不能回避的话题，与其他传统网络相比，由于物联网自身的开放性和资源有限的特点，使得它极易受到非法的入侵和攻击，因此对物联网的安全性进行研究，构建物联网环境下的安全策略具有非常重要的理论和现实意义。

物联网是大数据的重要来源之一，例如各个城市的视频监控每时每刻都在采集巨量的流媒体数据，工业设备的监控也带来了巨量的数据。物联网大数据在收集、传输、存储和使用过程中面临着诸多安全风险，虚假数据将导致错误或无效的大数据分析结果，因此保障数据本身的可用性至关重要。另外，大数据也为信息安全提供了一种新的研究思路和手段，如果数据量够大，即使是表面看起来互不相关的数据，也能挖掘出用户的行为规律。通过大量分散的数据信息对某些感兴趣的事件、

对象进行监测和行为预判，反过来也可以对数据感知及数据传输过程中的不可靠和低效的行为进行修正。

针对物联网及大数据安全的研究已有一些成果，但整体来看仍然处于起步阶段，结合物联网应用和部署的特点，研究物联网的安全控制策略及数据可用性保障机制是非常有意义的。

1.4 研究内容与贡献

基于上述研究背景与动机分析，本书的主要研究工作围绕物联网环境下数据驱动的信任模型及其应用等问题进行研究，研究的内容主要包括以下几个方面。

（1）数据驱动的信任模型设计

为了解决物联网中结点异常检测和数据可靠可信的问题，给出一种数据驱动的信任模型，该模型通过构建评测单元，借助所感知的数据存在非跳变性及区域相似性的特点，实现基于数据驱动的信任计算。由结点自身的实时和历史数据得到直接信任，并通过评测单元中的伴生结点、判决结点和工作结点之间数据的相关性，实现监督信任的计算。评测单元内工作结点之间的数据是相似的，由此可实现单元推荐信任的计算。再结合历史信任，可得到该结点综合信任值。该模型可用于结点的异常检测和数据的可靠性保证，实验证明该模型具有结点感知数据可靠、灵活可扩展等特点，能够有效提高物联网数据源头的可靠性。

（2）雾霾感知源信任评价机制

为了及时发现异常雾霾监测点，降低错误数据的产生，给出一种雾霾感知源信任评价方法。在该方法中将每个雾霾监测点作为一个整体，基于该监测点所监测的数据指标存在连续性，