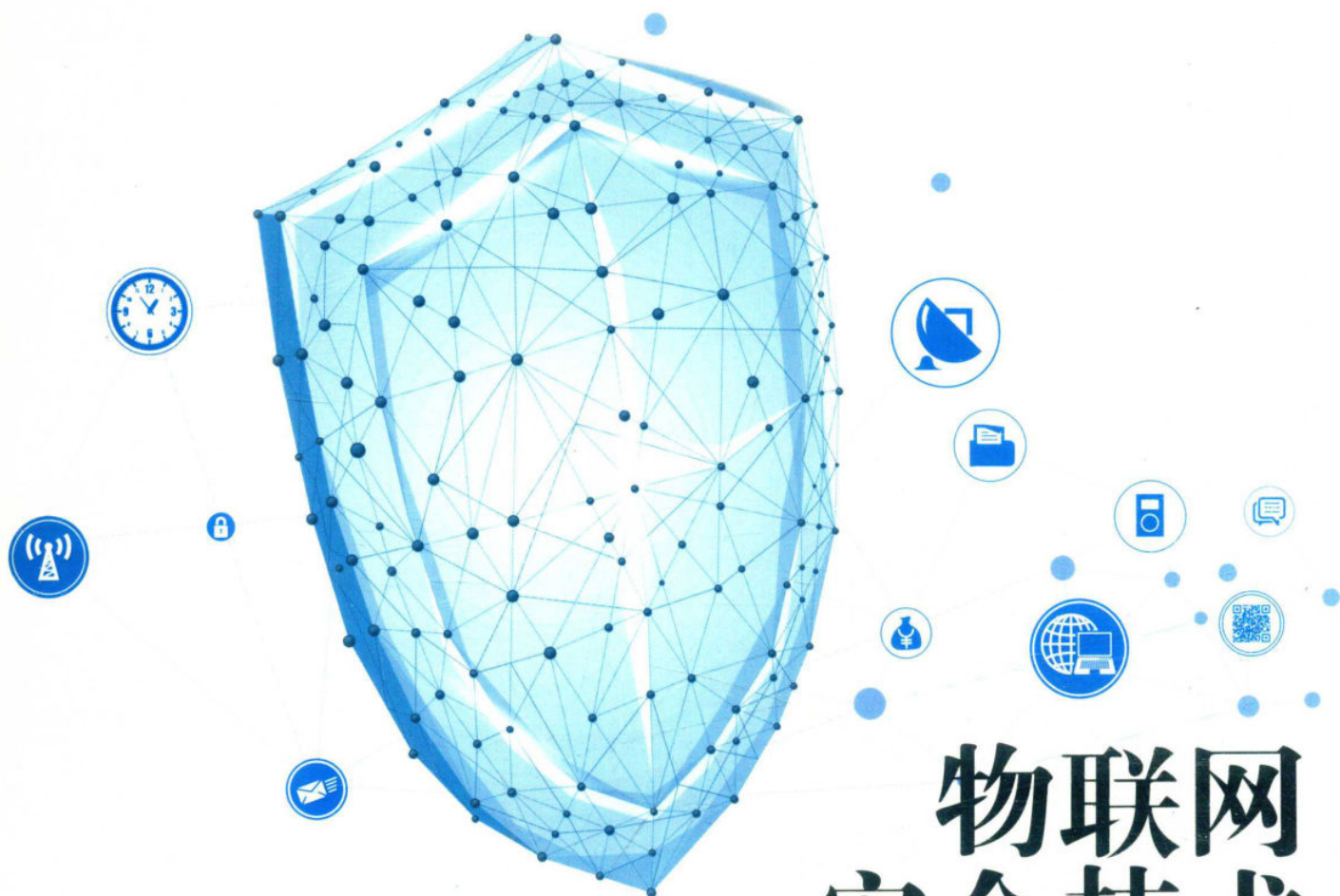




物联网工程专业系列教材



# 物联网 安全技术

武传坤 编著

SECURITY TECHNIQUES  
IN INTERNET OF  
THINGS



科学出版社

物联网工程专业系列教材

# 物联网安全技术

武传坤 编著

科学出版社

北 京

## 内 容 简 介

本书共三部分,分别为理论篇、技术篇与实践篇。其中,理论篇共有三章,主要介绍物联网安全架构、安全机制和密码学相关理论;技术篇共有六章,主要介绍物联网各个逻辑层的安全机制和安全技术、隐私保护技术和RFID安全技术;实践篇共有三章,主要介绍物联网安全需求分析和安全测评方法,分别针对安全等级保护需求和物联网感知层综合安全指标体系描述了测评方法。

本书可作为高等院校物联网相关专业“物联网安全”课程的教材,也可作为物联网安全研究人员的参考用书。

---

### 图书在版编目(CIP)数据

物联网安全技术/武传坤编著. —北京:科学出版社,2020.3

(物联网工程专业系列教材)

ISBN 978-7-03-063692-8

I. ①物… II. ①武… III. ①互联网络-应用-安全技术-高等学校-教材 ②智能技术-应用-安全技术-高等学校-教材 IV. ①TP393.408  
②TP18

中国版本图书馆CIP数据核字(2019)第280831号

---

责任编辑:赵丽欣 吴超莉 / 责任校对:王 颖

责任印制:吕春珉 / 封面设计:蒋宏工作室

**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

\*

2020年3月第 一 版 开本:889×1194 1/16

2020年3月第一次印刷 印张:13 3/4

字数:329 000

定价:48.00 元

(如有印装质量问题,我社负责调换〈骏杰〉)

销售部电话 010-62136230 编辑部电话 010-62134021

**版权所有,侵权必究**

举报电话:010-64030229; 010-64034315; 13501151303

## 作者简介



### 武传坤

先后获理学学士、理学硕士和工学博士学位。1988年至1995年任教于西安电子科技大学，先后晋升为讲师、副教授和教授。1995年9月在澳大利亚昆士兰理工大学从事博士后工作，之后任西悉尼大学研究员，澳大利亚国立大学讲师及高级讲师。

2002年入选中国科学院“百人计划”，任中国科学院信息安全国家重点实验室研究员、博士生导师，先后在中国科学院软件所、中国科学院信息工程研究所工作。2016年7月至2018年2月受聘于北京匡恩网络科技有限公司，任智能安全工业研究院副院长；2018年3月至2018年12月任北京奇安信科技有限公司（原360企业安全集团）的专家顾问；2018年12月至今任临沂大学特聘教授。

1993年获国务院政府特殊津贴，2000年起为IEEE高级会员，负责和参与完成多项国家科技项目。发表学术论文200余篇，出版专著多部，申请国家发明专利10余项。

研究领域包括布尔函数、密码算法、安全协议等。近年来的研究领域为物联网安全和工业控制安全，由之前的理论研究模式逐步向应用导向模式过渡。

**物联网导论 (第3版)**

书号: 978-7-03-051685-5

定价: 45元

作者: 刘云浩 编著

**射频识别技术原理、协议及系统设计 (第2版)**

书号: 978-7-03-049237-1

定价: 48元

作者: 谢磊 陆桑璐 编著

**物联网系统设计与应用**

书号: 978-7-03-052151-4

定价: 45元

作者: 郭忠文 著

**物联网安全技术**

书号: 978-7-03-063692-8

定价: 48元

作者: 武传坤 编著

**农业物联网导论**

书号: 978-7-03-035691-8

定价: 52元

作者: 李道亮 著

**NB-IoT技术详解与行业应用**

书号: 978-7-03-052702-8

定价: 98元

作者: 解运洲 编著

**边缘计算**

书号: 978-7-03-056144-2

定价: 48元

作者: 施巍松 刘芳 孙辉 裴庆祺 编著

**NB-IoT实战指南**

书号: 978-7-03-057329-2

定价: 39元

作者: 史治国 潘骏 陈积明 编著

**从创意到原型: 物联网应用快速开发**

书号: 978-7-03-061010-2

定价: 56元

作者: 董玮 高艺 编著

**物联网系统架构**

书号: 978-7-03-061991-4

定价: 58元

作者: 解运洲 编著



专业、行业、就业资讯共享, 请进“IoT科学讲堂”。

扫码加编辑微信, 或加微信“sciclassroom”邀请入群。

# 前 言

物联网是一种将虚拟世界与物理世界相结合的信息技术。近几年，物联网技术和产业都得到了飞速发展，物联网技术已经逐步渗透到不同的行业领域和人们的生活中，智慧物流、智慧家居、智慧医疗、智慧交通、智能电网、智能工厂等都是物联网技术在具体行业中的应用。

但是，在物联网时代，网络安全问题似乎比以往任何时期都更加突出，网络攻击造成的危害更严重。从工业设施被入侵攻击，到物联网设备被黑客入侵控制并发起分布式拒绝服务攻击，物联网安全问题越来越成为物联网行业健康发展的瓶颈。

无论哪个时代，对信息内容的安全保护都是非常重要的。在计算机时代，信息安全问题主要是防止非法用户盗取计算机内存储的内容，账户管理是信息安全保护的主要手段；在网络时代，出现了多种网络攻击手段，不仅有对信息的非法获取，还包括假冒、伪造、篡改、病毒入侵、拒绝服务等，有些攻击手段还结合了多种技巧，使用户防不胜防；在物联网时代，数据的价值会更高，特别是一些指令性数据，其价值不是体现在数据本身，而是对具体物理设备和设施的控制作用。攻击者对物联网系统的攻击手段将会更复杂、多变甚至更智能，其团体势力以及背后的支撑力量也日益庞大，物联网系统的安全保护面临空前的挑战。

为了更好地培养物联网安全领域的人才，或者让物联网工程方面的人员增加一些物联网安全知识，从而提升对物联网系统的网络安全保护措施，并在物联网系统的建设和运营过程中提供更好的网络安全保护，作者编写了本书。

本书的许多内容是基于 2013 年科学出版社出版的《物联网安全基础》，因此在这里特别列出《物联网安全基础》的编写参与者，他们是刘峰、张锐、徐静、冯秀涛、陈驰、王雅哲、张文涛、刘卓华、翟黎、滕济凯、皮兰。从某种意义上说，本书是这些作者共

同贡献的结果。读者不难发现，2013 年出版的《物联网安全基础》主要侧重理论知识，而本书在理论知识方面较为浅显，但增加了对实用技术的介绍。

考虑到物联网安全是一门与实际应用密不可分的课程，本书在技术方面的内容主要参考国家在物联网安全方面的等级保护标准，在应用方面努力以行业应用特色为背景。但由于物联网安全技术行业中的应用还在初步阶段，而且它在行业中的具体应用还不够系统规范，因此本书应用部分的内容是基于行业应用背景的模拟环境而建立的。

作者在写作过程中努力使本书具有实用性。但由于时间仓促、精力有限，疏漏之处在所难免。一些技术观点也仅代表作者当前的理解水平。对本书介绍的非标准化的探索性学术观点和技术方法，希望读者保持审慎态度。读者在阅读本书过程中如果遇到问题、发现错误等，敬请不吝指正。

最后，在书稿的组织、内容编校、推广宣传等诸多方面，感谢科学出版社的大力支持。我们也期待汲取读者的宝贵意见不断改进本书内容，使本书成为一本有用的教材和参考书。

武传坤

2019 年 7 月 25 日

# 目 录

## 理 论 篇

|                            |    |
|----------------------------|----|
| 第 1 章 物联网的基本概念和架构 .....    | 3  |
| 1.1 引言 .....               | 3  |
| 1.2 物联网的架构 .....           | 4  |
| 1.2.1 按照数据流程定义的物联网架构 ..... | 4  |
| 1.2.2 按照设备形态定义的物联网架构 ..... | 5  |
| 1.2.3 按照功能定义的物联网架构 .....   | 7  |
| 1.3 物联网关键技术 .....          | 9  |
| 1.4 物联网的技术标准 .....         | 10 |
| 1.5 物联网的网络安全和隐私保护问题 .....  | 11 |
| 1.6 物联网典型行业应用及其特点 .....    | 13 |
| 1.7 小结 .....               | 14 |
| 习题 .....                   | 15 |
| 第 2 章 物联网的安全架构 .....       | 16 |
| 2.1 引言 .....               | 16 |
| 2.2 物联网的安全架构模型 .....       | 16 |
| 2.3 感知层的安全机制 .....         | 17 |
| 2.3.1 终端感知节点的安全问题 .....    | 18 |
| 2.3.2 网关节点的安全问题与技术 .....   | 19 |
| 2.3.3 RFID 的安全问题与技术 .....  | 20 |
| 2.3.4 感知层的安全技术 .....       | 22 |
| 2.4 传输层的安全机制 .....         | 24 |
| 2.4.1 因特网的安全问题与技术 .....    | 24 |
| 2.4.2 移动通信网络的安全问题与技术 ..... | 25 |
| 2.4.3 传输层的安全需求 .....       | 26 |
| 2.5 处理层的安全机制 .....         | 26 |
| 2.6 应用层的安全机制 .....         | 28 |
| 2.7 物联网系统的信任体系与密钥管理 .....  | 30 |
| 2.8 物联网系统的安全测评与运维监督 .....  | 32 |

|                             |           |
|-----------------------------|-----------|
| 2.9 小结 .....                | 33        |
| 习题 .....                    | 33        |
| <b>第3章 密码学与安全协议基础 .....</b> | <b>35</b> |
| 3.1 引言 .....                | 35        |
| 3.2 数据加密算法 .....            | 35        |
| 3.2.1 对称密码算法 .....          | 36        |
| 3.2.2 轻量级分组算法 PRESENT ..... | 37        |
| 3.2.3 非对称密码算法 .....         | 40        |
| 3.2.4 RSA 公钥密码算法 .....      | 40        |
| 3.3 密码杂凑函数 (Hash 函数) .....  | 41        |
| 3.4 消息认证码 .....             | 42        |
| 3.5 数字签名算法 .....            | 42        |
| 3.6 密码算法提供的安全服务 .....       | 43        |
| 3.7 网络安全协议基础 .....          | 44        |
| 3.7.1 密钥协商协议 .....          | 44        |
| 3.7.2 公钥基础设施 .....          | 45        |
| 3.7.3 身份认证协议 .....          | 46        |
| 3.7.4 秘密共享协议 .....          | 49        |
| 3.8 小结 .....                | 49        |
| 习题 .....                    | 50        |

## 技 术 篇

|                                    |           |
|------------------------------------|-----------|
| <b>第4章 物联网的信任体系与密钥管理 .....</b>     | <b>53</b> |
| 4.1 引言 .....                       | 53        |
| 4.2 物联网系统的身份标识与身份认证 .....          | 53        |
| 4.2.1 账户类身份 .....                  | 54        |
| 4.2.2 地址类身份 .....                  | 55        |
| 4.2.3 标识类身份 .....                  | 55        |
| 4.2.4 身份标识的统一性问题 .....             | 55        |
| 4.2.5 账户类身份认证 .....                | 55        |
| 4.3 网络环境下信任的定义和信任的建立 .....         | 57        |
| 4.3.1 初始信任的实现方法 (一): 预置对称密钥 .....  | 58        |
| 4.3.2 初始信任的实现方法 (二): 预置公钥根证书 ..... | 58        |
| 4.4 公钥基础设施 (PKI) 简介 .....          | 59        |
| 4.4.1 X.509 公钥证书 .....             | 60        |

|                        |           |
|------------------------|-----------|
| 4.4.2 X.509 公钥证书的使用过程  | 62        |
| 4.4.3 X.509 中 CA 的信任关系 | 62        |
| 4.5 适合物联网应用的小证书        | 64        |
| 4.6 小结                 | 66        |
| 习题                     | 67        |
| <b>第 5 章 感知层安全关键技术</b> | <b>68</b> |
| 5.1 引言                 | 68        |
| 5.2 物联网感知层的安全威胁        | 69        |
| 5.3 物联网感知层的安全需求和安全保护技术 | 70        |
| 5.4 小结                 | 73        |
| 习题                     | 74        |
| <b>第 6 章 传输层安全关键技术</b> | <b>75</b> |
| 6.1 引言                 | 75        |
| 6.2 广域网通信技术简介          | 75        |
| 6.2.1 有线网络通信技术         | 76        |
| 6.2.2 移动通信网络技术         | 77        |
| 6.2.3 低功耗广域网无线通信技术     | 79        |
| 6.3 物联网传输层的典型特征        | 80        |
| 6.4 物联网传输层面临的安全威胁      | 80        |
| 6.5 传输层安全关键技术          | 81        |
| 6.6 互联网安全技术            | 81        |
| 6.6.1 概述               | 81        |
| 6.6.2 IPSec 协议         | 82        |
| 6.6.3 SSL 协议           | 87        |
| 6.6.4 VPN              | 88        |
| 6.7 移动通信网络安全技术         | 92        |
| 6.7.1 概述               | 92        |
| 6.7.2 LTE 网络简介         | 92        |
| 6.7.3 LTE 网络的构成        | 93        |
| 6.7.4 LTE 网络安全架构       | 94        |
| 6.7.5 LTE 两层安全体系       | 94        |
| 6.7.6 LTE 密钥管理         | 95        |
| 6.7.7 移动通信中的 AKA 协议    | 96        |
| 6.8 LPWAN 网络安全技术       | 97        |
| 6.8.1 LoRa 网络的安全技术     | 98        |

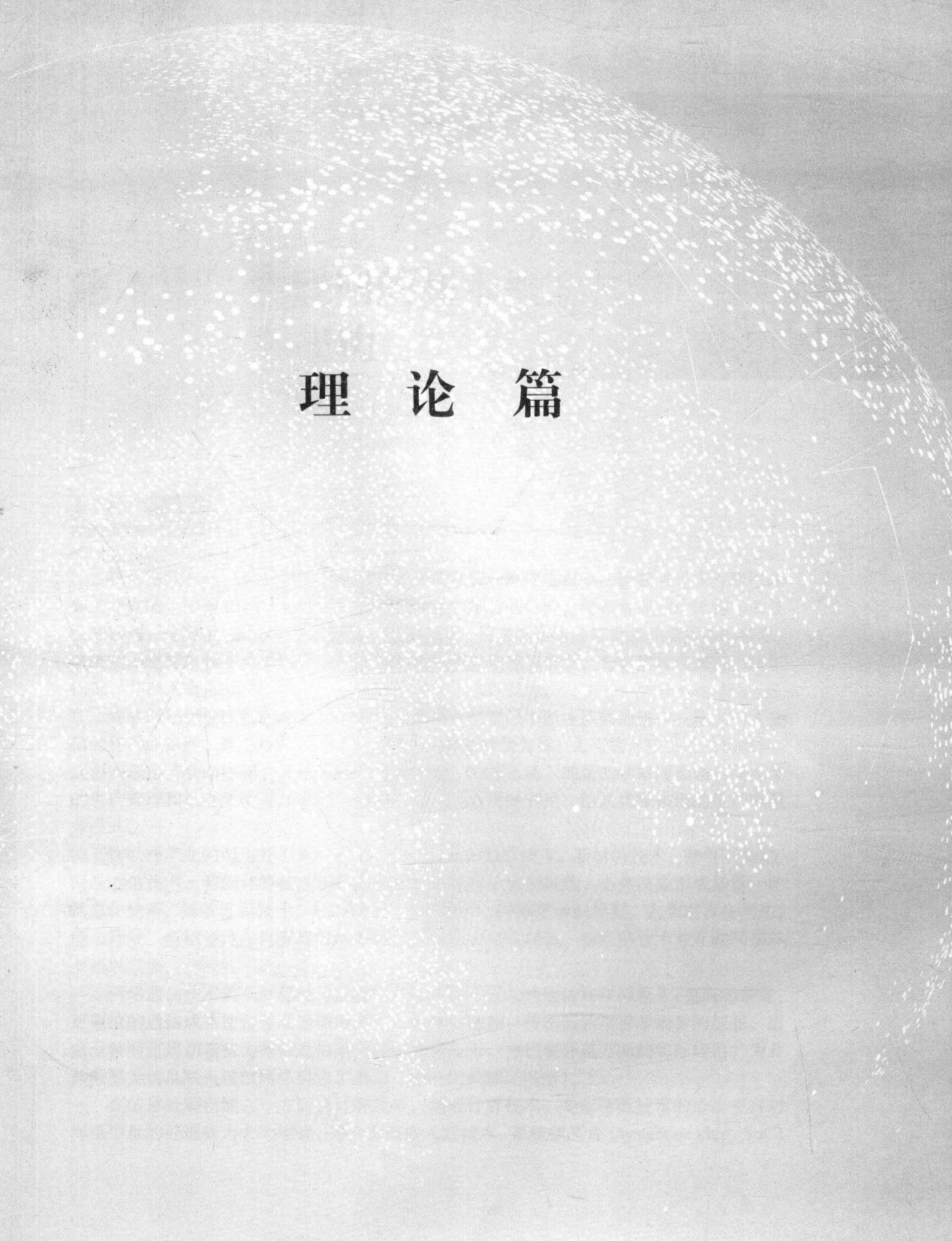
|                       |            |
|-----------------------|------------|
| 6.8.2 NB-IoT 网络的安全技术  | 100        |
| 6.9 小结                | 101        |
| 习题                    | 101        |
| <b>第7章 处理应用层安全技术</b>  | <b>102</b> |
| 7.1 引言                | 102        |
| 7.2 处理应用层的安全威胁        | 103        |
| 7.3 数据库安全技术           | 104        |
| 7.3.1 数据库安全标准简介       | 105        |
| 7.3.2 访问控制            | 107        |
| 7.3.3 安全审计            | 109        |
| 7.3.4 安全数据库实例         | 111        |
| 7.4 云平台安全             | 115        |
| 7.4.1 安全云平台的构建        | 115        |
| 7.4.2 虚拟化安全           | 117        |
| 7.4.3 云数据安全           | 120        |
| 7.5 云平台实例：Hadoop      | 122        |
| 7.6 小结                | 125        |
| 习题                    | 126        |
| <b>第8章 隐私保护技术</b>     | <b>127</b> |
| 8.1 引言                | 127        |
| 8.2 基于身份匿名技术的隐私保护     | 128        |
| 8.2.1 身份匿名的基本概念和技术    | 128        |
| 8.2.2 基于身份隐私保护的原型系统   | 131        |
| 8.2.3 身份匿名的应用场景       | 133        |
| 8.3 基于数据关联的隐私保护       | 134        |
| 8.3.1 数据挖掘带来的隐私泄露挑战   | 134        |
| 8.3.2 面向数据收集的隐私保护技术   | 136        |
| 8.3.3 面向数据传输的隐私保护技术   | 137        |
| 8.3.4 数据关联隐私保护的评估指标   | 138        |
| 8.4 基于位置的隐私保护         | 138        |
| 8.4.1 基于位置的服务         | 138        |
| 8.4.2 基于用户身份标识的位置隐私保护 | 140        |
| 8.4.3 基于位置信息的位置隐私保护   | 140        |
| 8.4.4 轨迹隐私保护          | 142        |
| 8.5 小结                | 146        |

|                         |            |
|-------------------------|------------|
| 习题                      | 146        |
| <b>第9章 RFID系统及其安全技术</b> | <b>147</b> |
| 9.1 引言                  | 147        |
| 9.2 RFID技术简介            | 148        |
| 9.2.1 RFID系统的工作原理       | 148        |
| 9.2.2 RFID标准            | 149        |
| 9.2.3 RFID的典型应用         | 151        |
| 9.3 RFID的安全威胁           | 153        |
| 9.4 RFID隐私保护协议          | 155        |
| 9.4.1 物理方法              | 155        |
| 9.4.2 基于密码算法的方法         | 156        |
| 9.5 RFID距离限定协议          | 158        |
| 9.6 RFID距离限定协议的安全威胁     | 160        |
| 9.7 小结                  | 160        |
| 习题                      | 160        |

## 实 践 篇

|                              |            |
|------------------------------|------------|
| <b>第10章 针对物联网安全等级保护的安全测评</b> | <b>163</b> |
| 10.1 传统安全标准对物联网的不适应性         | 164        |
| 10.1.1 物理和环境安全方面的不适应性        | 164        |
| 10.1.2 网络和通信安全方面的不适应性        | 164        |
| 10.1.3 设备和计算安全方面的不适应性        | 165        |
| 10.1.4 应用和数据安全方面的不适应性        | 165        |
| 10.2 物联网安全的等级保护标准            | 165        |
| 10.2.1 物理和环境安全标准             | 166        |
| 10.2.2 网络和通信安全标准             | 166        |
| 10.2.3 设备和计算安全标准             | 166        |
| 10.2.4 应用和数据安全标准             | 167        |
| 10.3 针对物联网安全等级保护标准的测评方法      | 167        |
| 10.3.1 物理和环境安全测评方法           | 167        |
| 10.3.2 网络和通信安全测评方法           | 168        |
| 10.3.3 设备和计算安全测评方法           | 169        |
| 10.3.4 应用和数据安全测评方法           | 169        |
| 10.4 身份认证、数据机密性和数据完整性的测评技术   | 170        |
| 10.4.1 身份认证测评技术              | 170        |
| 10.4.2 数据机密性测评技术             | 171        |

|        |                             |     |
|--------|-----------------------------|-----|
| 10.4.3 | 数据完整性测评技术 .....             | 172 |
| 10.5   | 小结 .....                    | 173 |
|        | 习题 .....                    | 174 |
| 第 11 章 | 感知层的安全指标和测评方法 .....         | 175 |
| 11.1   | 感知层安全指标 .....               | 175 |
| 11.1.1 | 物理安全指标 .....                | 176 |
| 11.1.2 | 运行环境安全指标 .....              | 178 |
| 11.1.3 | 网络安全指标 .....                | 181 |
| 11.1.4 | 数据安全指标 .....                | 182 |
| 11.1.5 | 密钥管理测评指标 .....              | 184 |
| 11.1.6 | 可用性测评指标 .....               | 185 |
| 11.2   | 感知层安全实现技术与测评方法 .....        | 186 |
| 11.2.1 | 物理安全实现技术与测评方法 .....         | 186 |
| 11.2.2 | 运行环境安全实现技术与测评方法 .....       | 191 |
| 11.2.3 | 网络安全实现技术与测评方法 .....         | 193 |
| 11.2.4 | 数据安全实现技术与测评方法 .....         | 195 |
| 11.2.5 | 密钥管理实现技术与测评方法 .....         | 198 |
| 11.2.6 | 可用性测评技术与测评方法 .....          | 199 |
| 11.3   | 小结 .....                    | 200 |
|        | 习题 .....                    | 200 |
| 第 12 章 | 物联网感知层的安全实现实例 .....         | 201 |
| 12.1   | 初始信任的建立 .....               | 201 |
| 12.2   | 基于公钥证书的身份认证协议 .....         | 202 |
| 12.3   | 基于共享密钥的轻量级安全数据传输协议 .....    | 202 |
| 12.3.1 | 协议的身份认证和密钥协商 (AKA) 功能 ..... | 203 |
| 12.3.2 | 协议的数据完整性保护功能 .....          | 203 |
| 12.3.3 | 协议的数据机密性保护功能 .....          | 203 |
| 12.3.4 | 对协议的进一步轻量化设计 .....          | 203 |
| 12.4   | 数据新鲜性保护技术 .....             | 204 |
| 12.4.1 | 基于时间戳的数据新鲜性保护 .....         | 204 |
| 12.4.2 | 基于计数器的数据新鲜性保护 .....         | 204 |
| 12.5   | 小结 .....                    | 205 |
|        | 习题 .....                    | 205 |
|        | 参考文献 .....                  | 206 |



# 理 论 篇





# 第1章 物联网的基本概念和架构

## 1.1 引言

物联网概念从最初产生时便一直处于逐渐发展和演变过程中。物联网是在互联网基础上建立的，以射频识别标签等信息感知设备为核心的架构，能够实现对全球物品的连接和跟踪；逐渐地，更多的传感器嵌入到物品中，用来感知物品自身或环境状态的信息；这类物品也越来越具有智能性，能够协同获取和处理感知信息，为管理和控制提供决策依据，并在人类直接干预或无人工干预的情况下进行联动。

物联网已经被应用到社会经济领域。随着大量物品不断连接到网络中，从人与人通信的移动通信网、机器与机器连接的互联网，发展到物与物、人与物连接互动的物联网，逐渐表现出“全面感知、无缝互联、高度智能、协同互动”的新的物联网形态，使人类的生产管理和社会生活更加高效，资源得到更加合理的利用，给人类带来新的生产和服务模式。

物联网产业的诞生并不是一时兴起的，而是在纳米技术、新材料技术、微电子技术、网络通信技术、智能计算技术和自动化技术发展h到一定阶段后，必然演变形成的新一轮信息化变革。随着标识技术、定位技术、传感技术、网络技术的发展，人类对自身状态、周边环境、所辖资产、世界局势的感知需求和能力日益增强，物联网技术在互联网基础上得以发展。

网络通信技术的发展已经可以满足世界上数十亿人的通信和联网服务，更高的带宽、更廉价的通信成本使得移动通信网络可以承受如视频、传感器数据等非语音的加载，通信运营商更迫切希望为宽带通信附加新的增值服务，并已展开这方面的实际应用，为业务数据类信息联入通信网络奠定了基础（物联网的神经网络）。

在信息处理领域，一方面云计算技术、超级计算技术、专家智能技术的进步使得对海量信息的处理能力大大增强；另一方面嵌入式技术、系统级芯片（system on chip, SoC）

技术的发展使得很多信息在终端即可进行压缩和预处理, 这些技术为业务数据大量涌入通信网络后面临的海量信息处理问题提供了解决办法 (物联网的大脑)。

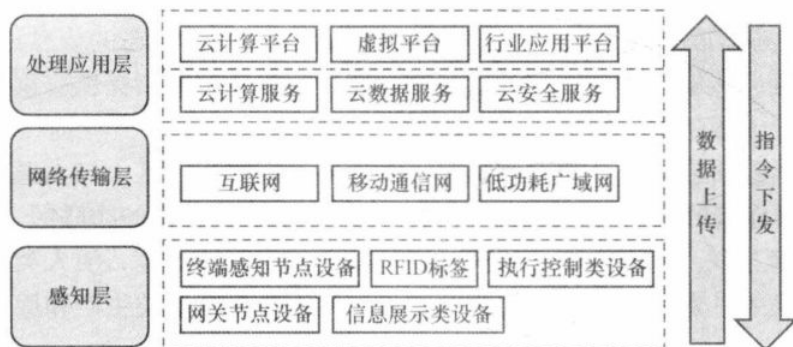
在行业应用方面, 可使用物联网技术的领域非常广泛, 物联网相关产业市场也非常巨大。物联网与云计算、大数据、移动互联网、人工智能等成为近年来的热门技术, 但实际上, 物联网技术是统领云计算、大数据、移动互联网、人工智能等技术的综合技术, 其他技术都是应用于物联网这个大系统中的典型技术。

## 1.2 物联网的架构

基于不同的认识角度, 对物联网架构的描述也有几种不同的表现形式。这里分别进行介绍。

### 1.2.1 按照数据流程定义的物联网架构

按照物联网系统对数据的处理流程, 物联网包含三个逻辑层, 分别为感知层、网络传输层和处理应用层, 如图 1.1 所示。在概念描述上, 存在多种不同的描述方式, 例如



网络传输层有时也被称为网络层或传输层, 处理应用层有时也被称为处理层或应用层。

感知层的功能主要是获取环境感知信息, 这些感知信息经由网络传输层的通信网络传输到处理应用层的数据处理中心, 接

着数据处理中心对这些数据进行统一处理, 然后用于为行业提供应用服务, 从而完成这些数据的生命周期。反过来, 从处理应用层下发的数据 (一般为指令), 经过网络传输层发送到感知层, 然后由感知层的相应设备进行处理。

从图 1.1 所示物联网架构看, 感知层的作用是获取原始数据或标签信息, 或执行指令 (包括操作指令、信息处理指令); 网络传输层的作用是将这些原始数据传输到远程的处理平台进行处理; 处理应用层的作用无疑是对来自不同感知层的数据进行应用。由于对数据的处理和对数据的应用无论在流程上还是在方法上都有很大区别, 为了更清晰地描述完整的物联网架构, 有时将物联网的处理应用层分为处理层和应用层, 形成四个逻辑层的架构, 但两种架构的内涵是一样的。因此, 为了描述方便, 通常将物联网架构描述为三个逻辑层的架构 (简称三层架构)。

物联网的感知层包括如下几类不同的设备: ①终端感知节点设备, 包括各种传感器、