Making Everything Easier!™

Qorvo® 专版

物联网

FOR DUMMIES®

学习目标：

- 认清物联网和智能家居的机遇
- 了解不同的物联网通信标准
- 善用小型数据和云中的自学算法

洞悉新知尽在

qorvo

Lawrence Miller, CISSP

关于 Qorvo

Qorvo（纳斯达克代码：QRVO）长期坚持提供创新的射频解决方案以实现更加美好的互联世界。我们结合产品和领先的技术优势、以系统级专业知识和全球性的制造规模，快速解决客户最复杂的技术难题。Qorvo 服务于全球市场，包括先进的无线设备、有线和无线网络和防空雷达及通信系统。我们在这些高速发展和增长的领域持续保持着领先优势。我们还利用我们独特的竞争优势，以推进 5 G 网络、云计算、物联网和其他新兴的应用市场以实现人物、地点和事物的全球互联。访问 www.qorvo.com 了解 Qorvo 如何创造美好的互联世界。

物联网

FOR

DUMMIES®

Qorvo® 专版

作者：Lawrence Miller，CISSP

WILEY

物联网傻瓜书®，Qorvo® 专版

出版商：
约翰·威利父子公司
111 River St.
Hoboken, NJ 07030 - 5774
www.wiley.com

ISBN 978-1-119-40326-5 (pbk)；ISBN 978-1-119-40327-2 (ebk)

美国制造

10 9 8 7 6 5 4 3 2 1

关于我们其他产品和服务的一般信息，或者如何为您的企业或组织定制*傻瓜版*书籍，请联系我们在美国的业务发展部，电话：877-409-4177，电子邮件：info@dummies.biz，网址：www.wiley.com/go/custompub。关于如何为产品或服务申请*傻瓜版*品牌许可的信息，请联系：BrandedRights&Licenses@Wiley.com。

出版商鸣谢

为本书上市做出贡献的部分人员有：

项目编辑：Elizabeth Kuball
排印编辑：Elizabeth Kuball
购置编辑：Katie Mohr
编辑经理：Rev Mengle
业务开发代表：Karen Hattan
生产编辑：Kumar Chellappan
特别援助：Cees Links、Kristien Lippens、Elly Schietse

引言

物联网 (IoT) 正在创造一个新的世界，一个可量化、可测量的世界。在这个世界里，人们可以更好地管理自己的生活，公司可以更好地管理其业务。这个新的“智能”互连世界将从根本上改变社会和消费者，并使所有企业和工业发生深刻变革。物联网的兴起将为我们提供及时且质量更高的信息，帮助我们更快地作出更好的决策，从而实实在在地大幅改善我们的世界和日常生活。

关于本书

本书解释物联网到底是什么，它对不同的行业意味着什么（第 1 章）；当前已有或正在开发的哪些物联网的通信标准和协议（第 2 章）；重要的物联网数据挑战，包括大数据和小数据、数据分析以及安全（第 3 章）；必须知道的关于物联网业务的要点（第 4 章）。

傻瓜式假设

之前提到，大多假设已不再关乎使用，尽管如此，我仍然做出以下假设。

我假设您对互联网和技术的未来产生的兴趣不是过眼烟云。也许您是为消费电子公司、电信服务提供商、移动或有线运营商、房屋建造承包商、医疗设备制造商或其他行业的科技公司工作的设备或产品开发人员、营销或销售经理、工程师。也许您是探索新商机或做研发的企业家或学生。我还假设您不一定是技术人员，所以，本书主要是针对不懂技术的读者而撰写。当然，我同样欢迎懂技术的读者！

如果我果真猜对的话，本书正适合您！如果都没猜中，您也要读下去！这本书很有用，读完后，当谈到物联网时，您不再会觉得自己像个傻瓜！

书中符号

在书中，我偶尔会使用一些特殊符号，以引起读者注意一些重要信息。这些符号如下：

这个符号指示的信息可能值得您牢记——就像记住某些周年纪念日和某人生日一样重要！

您不会在这里看到人类基因图谱，不过这个符号解释术语中的术语——所谓“技术宅”或“传奇”就是靠它炼成的。这个符号会在术语下方解释术语！

感谢您的阅读，希望您能喜欢本书，还请照顾一下作者！严格来说，这个符号所指的是一些有帮助的建议和实用内容。

这个符号表示妈妈的忠告。好吧，也许不是。但最好留意，说不定会帮您节省时间，减少麻烦！

书本之外

短短的24页中，我所能涵盖的内容只有这么多。所以，当你读完本书，在想：“老天，这本书棒极了，我哪里才能学到更多？”您只需要访问网站 www.qorvo.com/iot。

从哪里开始

从第 1 章开始可能是不错的起点。尽管如此，如果您觉得哪一章让您兴趣大增，您也可直接跳读该章。每章自成一体，所以从哪里开始都无妨。只要您觉得合心意，您可按照任何顺序阅读本书（不过，我不建议反着或倒着阅读本书）。

第1章

认清物联网和智能家居的机遇

内容提要

- 区分“智能”与“互连”
- 发现物联网市场机遇
- 转变业务以迎接物联网的未来发展

在本章中，您将了解到关于物联网 (IoT) 的一些事情：什么是物联网；对企业和工业而言，物联网有多重要；以及它将如何转变未来的业务模式和竞争战略。

物联网定义

很多人想知道“物联网”(Internet of Things) 到底是什么。这个术语本身就有点模棱两可，同时又无所不包。Dictionary.com 将“互联网”(Internet) 定义为“一个连接全球较小计算机网络的巨大计算机网络”，将“物件”(thing) 定义为“某个没有或无法明确指出或精确描述的实体、对象或生物”（是的，我使用互联网上的物件来查找一些定义）。

在 2014 年 11 月《哈佛商业评论》的一篇文章中，Michael Porter 和 James Heppelmann 将物联网设备描述为“拥有以下三个核心元素的智能互连产品：

- **物理**部分，包括产品的机械和电气部件。
- **“智能”**部分，包括传感器、微处理器、数据存储器、控制器、软件，通常还有嵌入式操作系统和增强型用户界面。
- **连接**部分，包括支持与产品进行有线或无线连接的端口、天线和协议。”

物联网设备和组件的“物理”部分包括大量不同的物件，例如：智能汽车中的发动机、空调和导航系统；智能家居中的烟雾报警器、恒温器和冰箱；可穿戴技术中的手表、健身追踪器和胰岛素泵。

让物联网设备和组件拥有“智能”的是各种支持高级功能的传感器和微处理器，例如：智能汽车中的电子控制单元；家庭安保系统中的动作感应摄像头；以及可穿戴低血糖传感器，当糖尿病患者的血糖水平低到危险程度时，它会自动发出提醒。

最后，物联网设备“连接”到互联网和其他系统以实现各种各样的目的，例如：为车辆导航系统提供位置追踪和实时交通信息；当检测到有人侵入住宅时向安保公司发出报警；将可穿戴医疗设备收集到的详细健康信息存储在安全私有云中，患者的主治医生在例行检查时可以下载。

*智能*和*互连*不是一回事。设备或组件接入互联网并不一定就能让它变“聪明”。举一个恰当的例子，一个人边开车边在智能手机上发消息，他尽管接入了互联网，但显然没有变“聪明”！要真正拥有智能，物联网设备或组件必须能够收集和分析数据，并根据分析自动执行明智的操作，不一定需要人工干预。

审视物联网市场潜力

对许多人来说，物联网是“下一个大热门”。但实际上，物联网已经到来，只需想想上一节提到的智能汽车、智能家居和可穿戴技术例子。

如果您想知道现在加入物联网盛会是否有点晚，请放心，机会还多得是！当今的物联网设备仍处于导入和早期发展阶段。您可以把当前市场中的物联网设备看作第一代物联网创新，我们还有很长的路要走。借用美国伟大哲学家 Jeff Foxworthy 的话说：当今的物联网设备并不比“五年级小朋友聪明多少”！

考虑下面的类比：小孩子碰到热火炉时可能会本能地做出如下动作：

- 把手从火炉拿开。
- 痛苦地尖叫。
- 把手放到嘴里以减轻疼痛。

注意，这些动作必须按照以上顺序完成；否则，孩子的舌头可能会被火炉烧伤，而他的尖叫声可能会被手捂住！当孩子长大后，他会变得更聪明（除了短暂的所谓青春期）。例如，将来他可能会

- 首先知道绝不能触碰热火炉。
- 分辨烧伤程度（一级、二级或三级）。
- 确定适当的急救或治疗方法。

与此相似，当今的物联网设备尚处于早期发展阶段。例如，如今的智能家居（或楼宇）可能会

- 当房屋或楼宇发生火灾时，发出警报声以提醒居住者。
- 开启紧急逃生指示灯。
- 通知消防部门。
- 启动喷淋系统。

将来的物联网智能家居（或楼宇）可能还会：

- 主动检测、报警甚至预防危险状况（例如：电线故障、无人照看的火炉或熨斗，或者封闭空间中可燃或有毒烟气的积聚达到危险程度）。
- 交互式引导居住者沿着最安全、最快捷的路线逃生，同时排出逃生路径中的烟雾。
- 关闭电气、通风和煤气系统以防止向火源输送更多燃料和氧气。
- 即时将家庭或楼宇示意图传输到每位应急响应人员头盔的平视显示屏上，并提供关于热点、环境状况和结构损害的实时信息，以及家居/楼宇传感器收集到的居住者位置。
- 将可穿戴式设备收集到的房屋或楼宇中人员的特殊健康状况或受伤情况安全地发送给应急响应人员；对这些设备进行位置识别，从而仅发送位于房屋或楼宇中的人员的数据。
- 自动传输受灾人员的所有相关健康和伤害信息，并根据附近医院的当前分流能力和负荷，引导医护人员沿最快捷路线将伤者送往最近的医院或创伤中心。
- 向相关区域中的智能手机和车辆导航系统发送绕行提示，并酌情改变交通信号灯和行驶方向，从而主动引导民用车辆绕开通往事故现场和医院的路线。

以上只是说明物联网市场无限创新可能性和机遇的几个例子。有了物联网，人们将能在及时且更高质量的真实数据的支持下更快做出更好的决策，而不是依赖直觉。

创建新的物联网业务模式

对许多公司和所有行业来说，物联网是创建新的业务模式和变革竞争战略的催化剂。在《哈佛商业评论》的“智能互连产品如何改变竞争”一文中，Michael Porter 和 James Heppelmann 写道：“智能互连产品将提供爆发式扩大的机遇 . . . 和能力，切断并超越传统的产品边界。产品不断变化的特点也会打断价值链，迫使公司重新思考并改组内部的几乎一切事务。”

在几乎所有能想象到的行业中，高瞻远瞩的企业都把物联网视为产品和盈利的“圣杯”。然而，踏上这一征途之前，必须明白物联网市场正在迅速变化且不断发展，尤其是智能家居和消费电子市场。物联网是企业需要了解的一个移动靶标。因此，首先应当回答以下三个问题：

- 你 . . . 叫什么？
- 你 . . . 寻求的是什么？
- 空载飞行器 . . . 的气流速度是多少？

等等，搞错了，这是电影《巨蟒与圣杯》中的问题。追寻物联网圣杯的公司首先应当回答以下三个问题：

- 我们如何从此岸到达彼岸？
- 消费者真正想要什么？
- 企业和行业将如何演变？

超越现状

虽然物联网前途是光明的，但要发挥其全部潜能，企业和行业必须应对一些真正的挑战，其中包括：

- **标准和互操作：**需要制定通信标准并解决互操作问题。在物联网市场，有许多行业巨头、联盟和框架组织在争夺主导权。第 2 章介绍了各种物联网通信标准和互操作问题。
- **安全和隐私：**身份盗窃和信用卡欺诈是当今的重大安全和隐私问题，但与物联网攻击的潜在风险相比，这些威胁可谓小巫见大巫。身份或信用卡号码失窃可能会破坏个人财务状况，但起搏器、胰岛素泵、智能家居或智能汽车遭到攻击则可能会致命。第 3 章详细讨论了安全和隐私问题。

提供智能解决方案和服务

不幸的是，当今许多企业——尤其是智能家居行业的设备制造商——在思考物联网及其产品战略时已经步入歧途。尽管名叫物联网，但“物”并不是最重要的。物件固然是必不可少的，但这里有一整套生态系统（Porter 和 Heppelmann 称之为“由系统组成的系统”）在运行，物件在其中的作用相对较小。

为了在竞争激烈的物联网新大陆取得成功，企业需要明白以下几点：

- 物联网（以及智能家居）业务模式并不是在一次交易中将产品（“物”）推销出去就万事大吉，而是要重塑产品，使之成为定期服务和收入流。
- 消费者真正需要的是智能解决方案和智能服务，以便让人们的生活更美好、更轻松、更健康、更安全、更简单、更舒适、更便利、更高效、更愉快。人们特别需要“安保”、“提高能效”、“辅助生活”之类的解决方案。

2016 年 4 月，Comcast 发布的一份报告中提供了一项有价值的发现：消费者在智能家居中真正需要的是服务，而不是远程控制家里各种工具和设备的一堆联网设备。我在《物联网应用领域傻瓜书》中解释了“智能家居即服务 (SHaaS)”这一概念。

有了物联网，人们将能利用及时且更高质量的数据更快地做出更好的决策。设备制造商和服务提供商需要着眼全局，而不是个别组件、设备和机器。

定义新的服务角色

当今的传统有线和卫星电视运营商面临着来自互联网服务提供商 (ISP) 和 OTT 服务商（尤其受到千禧一代的欢迎的如 Netflix、Amazon Prime 等）日趋激烈的竞争，它们将娱乐变成商品，通过互联网提供流媒体解决方案。

这种需求、行为和人群的演变，迫使运营商必须通过创新服务（和收入流）来吸引并留住客户。对物联网和智能家居服务的需求为运营商提供了大好机会，它们占据着有利地位，并拥有如下独特的优势来提供这些服务：

- 庞大的全球客户群
- 广泛的企业和住宅有线、无线、卫星基础设施
- 所有必需的营销、计费和客户支持系统
- 熟练的现场服务技术人员（和车队）可安装并维护智能家居系统

许多大型运营商已经推出智能家居服务，例如家庭安保和环境控制。然而，更大的物联网和智能家居机会正在蓬勃兴起。

智能家居解决方案似乎是运营商的专利，但觊觎者甚众。零售商、保险公司和产品供应商也都在试验（互联网）直销模式。机灵的运营商抓住这个时机进入智能家居服务领域。

第 2 章

物联网通信和互操作挑战

内容提要

- 利用 IPv6 和 6LoWPAN 识别并连接物联网设备
- Wi-Fi 用于高速数据网络
- 巧妙使用蓝牙
- 利用 Thread 激起物联网巢
- 利用 ZigBee 使物联网巢保持有效
- AllJoyn 和 IoTivity 结合

在本章中，您将了解到几种重要通信标准和技术，以及其在物联网和智能家居解决方案中的作用。

利用 IPv6 和 6LoWPAN 解决 IP 地址短缺问题

互联网协议 (IP) 最初由美国国防高级研究计划局 (DARPA) 开发，现已是传输控制协议/互联网协议 (TCP/IP) 通信协议套件的一部分。

IPv4 常用来为当今计算机网络和互联网中的设备/节点寻址。然而，IPv4 地址只有 32 位，最多只能提供 43 亿个唯一地址。互联网上的每一设备/节点都需要一个唯一地址。互联网工程任务小组

(IETF) 当初采纳 IPv4 时，43 亿唯一地址似乎非常充裕。毕竟，IBM 的 Thomas Watson 于 1943 年预言“世界市场可能只需要 5 台计算机”，Digital Equipment Corporation 的 Ken Olsen 于 1977 年预言“没有理由每个家庭都想要一台计算机”。也许 IETF 倚重的是 3Com 公司 Robert Metcalfe 1995 年的预言：“互联网很快就会地址枯竭，像炫目的超新星爆发一样，1996 年就会灾难性崩溃。”

幸运的是，上述预言都没有成真。如今，连接到互联网的唯一设备/节点已经比 43 亿多出好几倍。

1998 年，IETF 正式将 IPv6 规定为 IPv4 的替代协议，主要目的是解决 IPv4 地址空间有限问题。IPv6 十六进制地址包括 128 位，可提供 3.4×10^{38} 个唯一地址，堪称天文数字！我（相当大胆地）预测 IPv6 提供的唯一 IP 地址至少够物联网设备使用好几年——不信咱们等着瞧！

标准是福还是祸?

这是一个合理的问题，值得用简单直接的语言来回答：标准是福*也*是祸！

先谈不好的一面。制定新标准通常需要花上不计其数的时间，而一旦制定完成，标准常常像一个折中产物被各方不情愿地采纳，并不能完全服务于所有行业参与者的不同利益。

但标准显然也有它的好处。没有标准的话，开发组件、设备、装置、软件和系统（即所谓“物件”，它们与其他东西集成并进行互操作）的难度与成本会大幅增加。一个大系统中每一个能够标准化的元件，都会降低整体系统的不确定性和总复杂度，或者至少能将其隔离，从而更易管理。

因此，标准的一个主要好处是它能让企业和消费者的内心获得巨大的安宁，使他们能放心地开发、构建和购买解决方案。

标准必须具备以下两个主要特点：

- **开放性**（不能是封闭的或专有的），以便实现低成本、多供应商采用、省心的优点
- **国际性**，消除不同地区需求和设置引起的复杂性

对物联网设备而言，IPv6 主要挑战在于 IPv6 地址非常长（准确的说是 128 位），长地址难以记住！因此，IPv6 设备需要更大存储器，而这又会缩短电池续航时间。

IPv6 是一项关键启用协议，可使得世界上的每台物联网设备在互联网上都有一个唯一地址。

有人可能会疑惑为什么IETF 并不像我在健身房计数立卧撑跳次数一样编排 IP 版本！他们并没有跳过版本 0 至 3 和 5，这些都是试验版本。目前只有两个重要的 IP 版本：4 和 6。

IETF 还制定了一项称为 6LoWPAN（低功耗无线个人区域网络上的 IPv6）的标准，它本质上允许 IPv6 流量在低功耗无线网状网络上流通。6LoWPAN 设计用于需要相对较低数据速率的无线互联网连接的节点和应用，比如智能灯泡和智能电表。

Wi-Fi：大家难道不能和睦相处码？

对无线家庭和企业网络而言，电气电子工程师协会 (IEEE) 802.11x 标准 (Wi-Fi) 是极受欢迎的选择。Wi-Fi 支持每秒数百兆比特的高吞吐速率，但对物联网设备来说，数据传输速率过快反倒是其主要缺点。什么？！***记住：***速度会要 . . . 电池的命。

许多物联网设备（尤其是在智能家居领域）是低功耗、小尺寸设备，其电池非常小，设计工作时间为数年。这些设备传输大量“小数据”（详见第 3 章）包，故而不需要高数据传输速率。相比之下，电池供电的 Wi-Fi 设备通常每天都要充电，因为它们需要可靠（“以连接为导向”）的高速数据传输。

因此，在智能家居和其他物联网应用中，蓝牙和 ZigBee（本章稍后讨论）等其他技术是 Wi-Fi 的有效补充。

Wi-Fi 网格化 (IEEE 802.11s) 制定于 2000 年代早期，但由于在解决连接导向协议的延迟问题上遇到严重挑战而未被广泛采用。

蓝牙网格化

蓝牙是一种低功耗、短距离通信技术，主要设计用于中心辐射拓扑中无线设备之间的点到点通信。1999 年，蓝牙在无线战场上公开向 Wi-Fi 发起挑战。尽管武器稍逊一筹（WEP 加密不太安全），Wi-Fi 还是赢得了胜利，而蓝牙则牢牢占据了智能手机、无线键盘和鼠标等个人应用领域的地盘。

最新发展聚焦于让蓝牙“支持联网工作”，包括 Bluetooth Low-Energy（低能耗蓝牙，简称 BLE，也称为 Bluetooth Smart 或 Bluetooth 4.0+）和 Bluetooth Mesh（网格蓝牙）。BLE/Smart/4.0+ 设备的功耗显著低于当前蓝牙设备，并且可通过 6LoWPAN 连接（本章前面已讨论）直接访问互联网。Bluetooth Mesh 是 BLE/Smart/4.0+ 的扩展，实现与更大的独立设备集的连接（比如智能家居中的智能灯泡），使它们在网状网络中共同工作。

像 IEEE 802.11s Wi-Fi 网格化一样，Bluetooth Mesh 也是一种以连接为导向的协议，同样必须克服一些延迟挑战。因此，Bluetooth Mesh 也不大可能被物联网广泛采用。

搜寻通用 Thread

Thread Group 是一个由 Google/Nest、Samsung、ARM Holding 及其他方组成的联盟，旨在为物联网——具体来说是智能家居解决方案——创建一种无线网状网络协议。Thread 协议栈是一个开放标准，但只有 Thread Group 中的付费会员才能获取完整的 Thread 规范。

Thread 协议利用 IPv6、6LoWPAN 和 IEEE 802.15.4（全都在本章中讨论过）等多种标准来创建一个最多包括 250 台设备的 IP 寻址本地无线网状网络。Thread 本质上是 6LowPAN 的商用版本，就像 Wi-Fi 是 IEEE 802.11 的商用版本一样（由于某种原因，消费者更喜欢“Thread”和“Wi-Fi”等朗朗上口的名称，而不喜欢“6LowPAN”和“IEEE 802.11”）。Thread 在 6LowPAN 基础上增加了一些安全特性和一个应用层接口。Thread 提供安全、低功耗、冗余的网状网络，使得智能家居设备可以直接连接互联网和云服务。

ZigBee 可以在 Thread 上运行，ZigBee IP 的下一版本本质上将是 Thread。

紧跟 ZigBee 潮流

ZigBee 是一种基于 IEEE 802.15.4 标准的低成本、低功耗无线网状网络协议。ZigBee 是低功耗组网市场的主导协议，在工业环境和智能家居产品中拥有很高的采用率。ZigBee 有如下重要规范：

- **ZigBee PRO：**包括冗余、低成本、超低功耗（甚至无电池）设备和节点在内的物联网和智能家居解决方案的基础，拥有完整的无线网状网络功能，单一网络可扩展到包含成百上千的节点。
- **ZigBee GreenPower (GP)：**利用自供电、能量采集设备和需要超长电池寿命的电池供电设备，例如开关、紧急按钮和各种传感器，使功率需求最低化。
- **ZigBee RF4CE（消费电子射频）：**为不需要全功能无线网状网络的双向设备到设备控制应用定义一种强大的低功耗、低延迟射频 (RF) 遥控网络。ZigBee RF4CE 支持多供应商互操作设备，例如：遥控、家庭娱乐系统、无钥门禁和车库开门器。

- **ZigBee IP：**基于 IPv6（本章前面已讨论）的可扩展全无线网状网络标准。ZigBee IP 支持通过互联网控制低功耗、低成本设备，具备强大的组网和安全特性。它专注于（在实践中是局限于）智能能源解决方案。
- **ZigBee 整合应用层 (ZCAL)：**ZCAL 前称为 ZigBee 簇群库 (ZCL)，是一种用于描述物联网设备功能（例如开关控制和温度读数）的应用层语言。ZCAL 包含家庭自动化、楼宇自动化和零售服务所用各类设备的数据模型，并且在持续扩展以容纳更多设备和功能。
- **ZigBee 3.0：**集 ZigBee Pro、GreenPower 和 ZCAL 于一体，包括一组协调一致的方法来调试网络上的节点，从而获得完全可互操作的智能家居物联网设备。

哦，我明白了——它是 OCF!

开放连接基金会（Open Connectivity Foundation，简称 OCF）前身是开放互连联盟（Open Interconnect Consortium，简称 OIC），创建于 2016 年 2 月，是物联网连接领域最大的标准组织。OCF 目前拥有 170 多家会员公司，包括 Cisco、Electrolux、Intel、Microsoft、Qualcomm、Samsung Electronics 等。

OCF 将 Intel（来自 OIC 的 IoTivity）和 Qualcomm（来自 AllSeen Alliance 的 AllJoyn）之前的倡议结合起来，二者均是 Linux 基金会下的开源项目，具有很大的互补性和重叠性。IoTivity 和 AllJoyn 均支持无缝发现和设备到设备 (D2D) 的物联网连接。

虽然各种技术之间存在市场份额竞争和某些重叠，但 Wi-Fi、蓝牙、Thread、ZigBee 和 OCF 似乎都找到了各自的核心应用领域。在可以预见的未来，它们对物联网发展会起到重要的相辅相成作用：Wi-Fi 用于内容共享和分发，蓝牙用于可穿戴设备及取代电线，Thread 和 ZigBee 用于低功耗检测和控制网络；OCF 用于应用层。

第3章

这是一个小（数据）世界！

内容提要

- 收集数据——关于大数据和小数据
- 物联网云变得越来越聪明
- 认清物联网隐患不断变化的特点

在本章中，您将了解到各种物联网数据、分析以及必须应对的安全/隐私挑战。

大数据很大，而小数据会变成海量数据

数字数据无处不在。EMC 第七份年度《数字宇宙研究》估计，全球创造、复制和消耗的总数字数据量每两年翻一番，预计到 2020 年将达到 40,000 EB。如果将这 40,000 EB 数据打印出来的话，将需要大约 2200 万亿棵树，是整个地球上的树木数量（估计有 3 万亿棵）的大约 700 倍！

1 TB = 1,024 GB，1 PB = 1,024 TB，1 EB = 1,024 PB。

然而，根据 EMC 研究，“数字宇宙中仅有 22% 的信息被认为是有用数据，而实际分析的有用数据不到 5%。”到 2020 年，物联网产生的数据有望将有用数据提高到数字宇宙的 35% 以上。

很多这种“有用数据”就是当今许多企业所称的“大数据”——由结构化和非结构化数据组成的超大型（有时候达到数 PB）数据集，这些数据是从众多来源收集得到的，利用 Hadoop 和 MapReduce 等高级技术框架进行分析以找出不同模式、趋势和行为。

但在数字宇宙中，还有一种物联网数据也同样重要，并且具有潜在使用价值，那就是“小数据”。小数据是作为非常小的数据集而产生的，包含非常有限或特定的属性，例如：智能家庭的温度读数、智能汽车的车速或智能起搏器的心率。这些数据集可以周期式收集，比如每 5 秒收集一次；随着时间推移，收集到的数据量会变得非常庞大。

圣犹达儿童研究医院创始人 Danny Thomas 有一句名言：“我宁愿一百万人每人给我一美元，而不愿一个人给我一百万美元。这样的话，将有一百万人参与进来。”物联网从 Danny Thomas 那里得到了启示，数十亿设备和数万亿传感器为庞大的数字宇宙贡献小数据！

小数据通常是近乎实时地用在物联网设备中，以确定当前状态或工作条件，并触发相应的操作或事件。例如：

- 小幅调节智能家庭的温度以维持一个舒适的环境
- 改变某些发动机参数以提高智能汽车在给定速度下的燃油效率和安全性
- 给予一个小电荷以适当调节某个人的心率

大数据和小数据在物联网中都会发挥重大作用，从本节给出的几个例子很容易看出，安全和隐私对于智能互连世界极端重要。我将在以下几节中讨论这些话题。

数据分析和云中的自学习

数据分析领域完成的很多工作是聚焦于揭示大数据中的模式和趋势，使得组织机构可以根据预测分析作出明智决策。例如，企业基于金融数据作出影响未来盈利能力的战略决策，或使用关于客户偏好的数据来积极影响客户体验。政府组织可以利用金融数据找出社会计划中的欺诈，或使用各种社会学数据识别潜在的犯罪“热点”并主动加以监管。

此外还做了大量工作来开发算法以“理解”并解读云中收集的小数据，以及识别异常状况。这需要处理海量小数据，未来一个智能家庭中可能有 100 台之多的物联网设备会提供几乎连续的数据流。

云中的这种“自学习”能力是未来物联网应用的关键，例如家庭和老人生活方式系统（《物联网应用傻瓜书》第 2 章中做过讨论），这些系统依赖模糊逻辑和其他人工智能 (AI) 技术来执行智能操作，不需要人工持续干预。

保护小数据的隐私和安全至关重要

隐私和安全对物联网非常重要，但也需要权衡。人们天生敢于冒险，比方说为了某种便利，这就可能影响安全性和隐私权。此类问题不是物联网独有的，在当今的互联网中同样存在。然而，就物联网而言，隐患的性质发生了改变。目前，身份盗窃和信用卡欺诈是网络攻击的主要动机。对于物联网，敲诈勒索、黑客主义和网络恐怖主义可能成为日益普遍的网络攻击威胁。

小数据对网络罪犯的价值可能不大明显。毕竟，威胁公开一个人每天走了多少步或其智能家庭的温度是多少，不大可能会敲诈到一大笔钱。但是，威胁曝光从智能家庭中各种摄像头盗取的暴露照片，或让起搏器或胰岛素泵不能正常工作，则要严重得多。

类似地，受政治或社会原因驱动的黑客团体可能会攻击电力公司的智能电网系统，引发可能会使公司破产的计费错误。

最后，网络恐怖分子可能会攻击物联网医疗设备，他们放弃任何勒索要求，仅以随机地大规模残害毫无警惕的患者为目标。智能汽车可能会被攻击而引起伤亡，智能电网可能遭到攻击而导致大规模停电或人为环境灾难。

物联网安全性的重大挑战在于它不应当干扰易用性和舒适性。例如，要求输入密码才能开灯或关灯是不现实的。未来的物联网最有可能采用一种混合安全解决方案，其将熟悉的传统机制与更先进的技术方案融为一体，就像当今很多汽车上的无钥门禁系统——虽然不用钥匙就能解锁甚至启动这些汽车，但万一车主有点怀旧，通过钥匙也能解锁和启动大部分汽车。

物联网安全的另一个挑战是许多物联网设备和传感器没有直接用户接口。计算机或智能手机有键盘和屏幕，用户可以输入安全密码等。智能灯具或烟雾探测器则没有直接接口，尽管智能手机应用可以帮忙。

为了保护物联网安全，设备制造商、开发商和服务提供商必须共同努力，确保通过强大的加密方案和安全秘钥管理来保障对物联网应用、系统、设备、传感器、网络、连接以及其所产生数据的安全访问。然而，单凭加密是不够的。例如，IEEE 802.15.4 采用 128 位高级加密系统 (AES) 来保障安全性，但其他措施也是必不可少的，比方说通过提高计数器和随机化来防止中间人和回放攻击。

第4章

物联网的八大要点

内容提要

- 创造智能解决方案和服务，而不只是将物件连接起来
- 协同工作以实现更光明（且可互操作）的物联网未来
- 应对数据、安全和隐私挑战

一旦认识它们，你就会爱上它们。以下是关于物联网连接的八大要点，以经典*傻瓜书*风格呈现！

- **智能和互连不是一回事。**“智能”互联网设备或组件必须能够基于对其收集到的数据进行分析而自动执行智能操作。简单地将某种“物件”连接到互联网是不够的。
- **消费者需要解决方案，而不是物件。**尽管最近的许多器具和玩意儿很酷，但绝大部分消费者渴望的并不是一堆很酷的物件。他们需要的是智能解决方案和服务，以便让人们的生活更美好、更轻松、更健康、更安全、更简单、更舒适、更便利、更高效、更愉快。
- **智能企业将提供“从摇篮到坟墓”的智能服务以获取循环收益。**消费者越来越多地从购买物件（“所有权”）转向购买服务（“使用权”）。智能企业将超越初次产品购买而发展循环收益模式，在物联网解决方案寿命期间为消费者提供增值服务（而非“延长保修”）。

- **采用标准对物联网成功至关重要。**物联网正在迅猛发展，其边界不断拓宽。若无标准，设备制造商将会匆忙向市场推出最新的“物件”以攫取短期竞争优势，挣快钱，而不考虑互操作性或长期可持续性。为使物联网成为一个真正智能化的互连世界，而不是随机的一堆物件拼凑成的网络，必须采用标准。
- **物联网行业存在明显的混乱和重叠。**许多大型联盟、协会和企业在极力争夺物联网的地位和领导权。其中很多联盟相互竞争并有所重叠，但同时在某些情况下又彼此合作！
- **ZigBee 是智能家居的明智选择。**ZigBee 整合应用层 (ZCAL) 是应用层语言的出色选择，该方案已得到市场检验，并已完全集成在 ZigBee 3.0 中。预计它也是其他物联网通信标准的首选应用层语言。
- **对小数据也要从大处着眼。**企业聚焦大数据的机遇和挑战已有很多年。对于物联网，小数据——包含传感器收集到的有限或特定属性的超小数据集——是大数据的有益补充，二者结合将能创造更大的机遇 . . . 和挑战。
- **安全和隐私是攸关生死的大事。**身份盗窃和信用卡欺诈是当今最突出的网络犯罪行为。智能汽车、智能家居、智能电力设施、智能可穿戴装置和医疗设备等物联网应用将开启潘多拉魔盒，新的威胁将成为主要网络攻击方式，包括勒索软件、黑客主义和网络恐怖主义。物联网行业中的每个人都要把安全和隐私作为首要考虑。

有了物联网，人们将能利用及时且更高质量的数据更快做出更好的决策。

让无线智能家居永不过时

消费者担心他们今天买的智能家居产品不能用于下一年的新装置。Qorvo 的超低功耗 IEEE 802.15.4 解决方案借助单芯片便可解决兼容性问题，并支持当前和未来的多个家庭网络标准。

令 Qorvo 射频方案脱颖而出的几大要素

多堆栈
单无线电
多协议芯片

低成本
高度集成的
完整解决方案

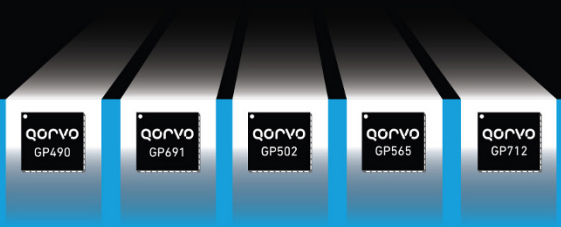
出色的工作范围
全面的家居
覆盖范围

稳定可靠
防 Wi-Fi
干扰性高

超低功耗
电池寿命
超过产品寿命

物联网开始启航——如需
了解更多信息，请访问
www.qorvo.com

GreenPeak 现在属于 qorvo 公司



WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.