Making Everything Easier!™

Qorvo Special Edition

Internet of Things For Dummies®

A Wiley Brand

Learn to:

- **Identify IoT and smart home market opportunities**
- **Make sense of different IoT communications standards**
- **Leverage small data and self-learning in the cloud**

Brought to you by

qorvo®

®

Lawrence Miller, CISSP

About Qorvo

Qorvo (NASDAQ: QRVO) makes a better world possible by providing innovative RF solutions at the center of connectivity. We combine product and technology leadership, systems-level expertise and global manufacturing scale to quickly solve our customers' most complex technical challenges. Qorvo serves diverse high-growth segments of large global markets, including advanced wireless devices, wired and wireless networks and defense radar and communications. We also leverage our unique competitive strengths to advance 5G networks, cloud computing, the Internet of Things, and other emerging applications that expand the global framework interconnecting people, places, and things. Visit www.qorvo.com to learn how Qorvo connects the world.

Internet of Things FOR DUMMIES

A Wiley Brand

Qorvo Special Edition

by Lawrence Miller, CISSP

FOR DUMMIES
A Wiley Brand

Internet of Things For Dummies®, Qorvo Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-34992-1 (pbk); ISBN 978-1-119-34989-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Elizabeth Kuball

Copy Editor: Elizabeth Kuball

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative:
Karen Hattan

Production Editor: Kumar Chellappan

Special Help: Cees Links,
Kristien Lippens, Elly Schietse

Introduction

The Internet of Things (IoT) is creating a new world — a quantifiable and measurable world — in which people can better manage their lives and companies can better manage their businesses. This new "smart," connected world will offer fundamental changes both to society and to consumers and will profoundly transform entire businesses and industries. The rise of the IoT will create many practical and significant improvements in our world and our daily lives by helping us make better decisions faster with timely, higher-quality information.

About This Book

This book explains what the IoT is all about and what it means for businesses in different industries (Chapter 1); what communications standards and protocols currently exist or are in development for the IoT (Chapter 2); key IoT data challenges, including big and small data, analytics, and security (Chapter 3); and some important takeaways about the IoT for businesses (Chapter 4).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

I assume you have more than a passing interest in the future of the Internet and technology. Perhaps you're a device or product developer, a marketing or sales manager, or an engineer working for a consumer electronics firm, a telecommunications service provider, a mobile or cable operator, a home construction contractor, a medical device manufacturer, or a technology company in some other industry. Or perhaps you're an entrepreneur or student exploring new business opportunities or research and development. I also assume that you are not necessarily a technical person, so I've written this book primarily for nontechnical readers. Of course, technical readers are also welcome!

If these assumptions describe you, this book is for you! If none of these assumptions describes you, keep reading anyway. It's a great book, and when you finish reading it you won't feel like an I-D-10-T when talking about the IoT!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information that you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

TIP

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

WARNING!

This icon points out the stuff your mother warned you about. Okay, probably not. But you should take heed nonetheless — you may just save yourself some time and frustration!

Beyond the Book

There's only so much I can cover in 24 short pages, so if you find yourself at the end of this book thinking, "Gosh, this was an amazing book, where can I learn more?," just go to `www.qorvo.com/iot`.

Where to Go from Here

Chapter 1 might be a good place to start! But if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so you can start reading anywhere and skip around to your heart's content! Read this book in any order that suits you (though I don't recommend upside down or backward).

Chapter 1

Recognizing IoT and Smart Home Opportunities

In This Chapter

- Differentiating between "smart" and "connected"
- Exploring the IoT market opportunity
- Transforming your business for the IoT future

In this chapter, you learn about the Internet of Things (IoT): what it is, how big it is for business and industry, and how it will transform business models and competitive strategies of the future.

Defining the Internet of Things

If you're wondering exactly what the "Internet of Things" is, you're not alone. The term itself is somewhat ambiguous and, at the same time, all-inclusive. Dictionary.com defines the Internet as "a vast computer network linking smaller computer networks worldwide" and a "thing" as "some entity, object, or creature that is not or cannot be specifically designated or precisely described" (yes, I used that Internet thing to look up those definitions).

In a November 2014 *Harvard Business Review* article, Michael Porter and James Heppelmann describe IoT devices as "smart, connected products [that] have three core elements:

> - **Physical** components [that] comprise the product's mechanical and electrical parts.

> - **"Smart"** components [that] comprise the sensors, microprocessors, data storage, controls, software, and, typically, an embedded operating system and enhanced user interface.
> - **Connectivity** components [that] comprise the ports, antennae, and protocols enabling wired or wireless connections with the product."

The "physical" part of IoT devices and components include lots of different "things" — for example, the engine, air conditioner, and navigation system in a smart car; smoke alarms, thermostat, and refrigerator in a smart home; and watches, fitness trackers, and insulin pumps in wearable technology.

What makes IoT devices and components "smart" are the various sensors and microprocessors that enable advanced functionality — for example, the electronic control units in a smart car; motion-activated cameras in a home security system; and wearable hypoglycemia sensors that automatically alert diabetic patients when their blood sugar levels are dangerously low.

Finally, IoT devices are "connected" to the Internet and other systems for different purposes — for example, to provide location tracking and real-time traffic information for a vehicle's navigation system; to alert a security company when a home intrusion is detected; and to store detailed health information, collected by a wearable medical device, in a secure, private cloud where it can be downloaded by a patient's physician during a routine exam.

REMEMBER

Smart and *connected* aren't the same thing. Connecting a device or component to the Internet doesn't necessarily make it smart — case in point, a person texting on his smartphone while driving a car is connected to the Internet, but definitely not smart! To truly be smart, an IoT device or component must be able to gather and analyze data and automatically perform intelligent actions based on its analysis — without necessarily requiring human involvement.

Looking at IoT Market Potential

For many, the IoT is the "next big thing." But, in reality, the IoT is already here — simply consider the smart car, smart home, and wearable technology examples described in the preceding section.

If you're wondering whether you're late to the IoT party, relax! Today's IoT devices are still in their introduction and early growth stages. You might consider IoT devices in the current market to be the first generation of IoT innovation — and we still have a long way to go. To paraphrase the great American philosopher Jeff Foxworthy: Today's IoT devices aren't much "smarter than a fifth grader"!

Consider the following analogy: A small child who touches a hot stove might instinctively:

- ✓ Pull his hand away from the stove.
- ✓ Scream in agony.
- ✓ Put his hand in his mouth to soothe it.

Note that these steps have to be performed in the above order; otherwise, the child might also burn his tongue on the stove and his scream will be muffled by his hand! As the child matures, he becomes smarter (except for that brief period of years known as adolescence!). For example, in the future he may

- ✓ Learn not to touch a hot stove in the first place.
- ✓ Recognize the severity of a burn (first, second, or third degree).
- ✓ Determine the appropriate first-aid or medical treatment.

Similarly, today's IoT devices are in their early development stages. For example, a smart home (or building) today might

- ✓ Sound an alarm to alert the occupants of a fire in the home or building.
- ✓ Activate emergency exit lights.
- ✓ Notify the fire department.
- ✓ Actuate a sprinkler system.

Future IoT smart homes (or buildings) might also

- Proactively detect, alert, and even prevent hazardous conditions (such as faulty electrical wiring, an unattended stove or iron, or a dangerous buildup of combustible or toxic fumes in a closed space).
- Interactively direct occupants along the safest and most expedient escape route, while also venting smoke away from the escape route.
- Shut down electrical, ventilation, and gas systems that might otherwise provide additional fuel and oxygen to the fire.
- Instantaneously transmit home or building schematics to a heads-up display in every emergency responder's helmet, complete with real-time information about hot spots, environmental conditions, and structural damage, as well as the location of occupants collected by home/building sensors.
- Securely send information about any special health conditions or injuries of individuals in the home or building to emergency responders, collected by personal wearable devices that are geographically fenced so that only data about individuals who are in the home or building is sent.
- Automatically transmit all pertinent health and injury information about victims, and route paramedics along the most expedient route to the nearest hospital or trauma center based on its current triage capabilities and load.
- Proactively reroute civilian traffic away from the route to the emergency scene and to the hospital, by sending detour alerts to smartphones and vehicle navigation systems in the area and changing traffic signals and lane directions as appropriate.

These examples are just a few of the virtually limitless possibilities for innovation and opportunity in the IoT market. The IoT will enable better decisions to be made faster, supported by timely, higher-quality real data, instead of intuition.

Creating a New IoT Business Model

The IoT is the catalyst for many companies and entire industries to create new business models and transform their competitive strategies. In their *Harvard Business Review* article "How Smart, Connected Products Are Transforming Competition," Michael Porter and James Heppelmann write "Smart, connected products offer exponentially expanding opportunities . . . and capabilities that cut across and transcend traditional product boundaries. The changing nature of products is also disrupting value chains, forcing companies to rethink and retool nearly everything they do internally."

Forward-looking businesses in practically every industry imaginable see the IoT as the Holy Grail of products and profitability. However, before undertaking this quest, they need to understand that the IoT market is rapidly changing and constantly evolving — especially in the smart home and consumer electronics market. The IoT is a moving target that businesses need to understand. Thus, we shall first answer these questions three:

- What . . . is your name?
- What . . . is your quest?
- What . . . is the airspeed velocity of an unladen swallow?

Wait, not those questions — that's *Monty Python and the Holy Grail!* Companies seeking the IoT Holy Grail should first answer these questions three:

- How do we get there from here?
- What do consumers really want?
- How will business and industry evolve?

Moving beyond the status quo

Although the IoT future is bright, there are some real challenges that must be addressed by businesses and industries in order for the IoT to achieve its full potential. These include

- **Standards and interoperability:** Communications standards need to be defined and interoperability issues resolved. Within the IoT market, many competing industry giants, consortiums, and frameworks are jockeying for primacy. Chapter 2 explains various IoT communications standards and interoperability issues.
- **Security and privacy:** Identity theft and credit card fraud are major security and privacy issues today, but these threats pale in comparison to the potential risk of an IoT attack. A stolen identity or credit card number can be devastating to an individual's financial health — but a hacked pacemaker, insulin pump, smart home, or smart car can be lethal. Chapter 3 covers IoT security and privacy concerns in greater detail.

Providing smart solutions and services

Unfortunately, many businesses today — particularly device manufacturers in the smart home industry — are already heading down the wrong path when thinking about the IoT and their product strategies. Despite its name, the Internet of Things isn't about "things." Things are the necessary enablers, but there is an entire ecosystem at play — Porter and Heppelmann refer to it as a "system of systems" — in which things play a relatively minor role in the IoT.

To be successful in the new and highly competitive IoT market, businesses need to understand the following:

- The IoT (and the smart home) business model isn't about pushing products ("things") out the door in a single sales transaction. It's about reinventing products as recurring services and revenue streams.
- What consumers really want are smart solutions and smart services that will make their lives better, easier, healthier, safer, simpler, more comfortable, more convenient, more efficient, and more enjoyable. They are specifically looking for solutions like "security," "energy efficiency," "assisted living," and others.

TIP

In April 2016, Comcast released a report that provides valuable insight into what consumers really want in the smart home — services, not just a bunch of connected devices that remotely control various widgets and devices in the home. In *Internet of Things Application Fields For Dummies,* I explain the Smart Home as a Service (SHaaS) concept.

REMEMBER

The IoT enables better decisions to be made faster with timely, higher-quality data. Device manufacturers and service providers need to look at the big picture, not just individual components, devices, and machines.

Defining new service roles

Traditional cable and satellite television operators today are facing increasing competition from Internet service providers (ISPs) and over-the-top (OTT) services such as Netflix, Amazon Prime, and others — particularly popular among millennials — that are commoditizing entertainment and delivering streaming media solutions over the Internet.

This evolution in demand, behavior, and demographics is compelling operators to innovate in order to attract and retain customers with new services (and revenue streams). The demand for the IoT and smart home services presents an immense opportunity for operators, who are already uniquely positioned to deliver these services with the following advantages:

- A tremendous worldwide customer base
- Extensive business and residential wired, wireless, and satellite infrastructure
- All the necessary marketing, billing, and customer support systems
- Skilled field service technicians (and vehicle fleets) to install and maintain smart home systems

Many large operators are already rolling out smart home services, such as home security and environmental control. However, there is a much bigger IoT and smart home opportunity that is just starting to emerge.

The smart home is a solution that is seemingly designed for operators to sell, but they aren’t alone. Retailers, insurance companies, and product vendors are experimenting with direct (Internet) sales models as well. There is a window of opportunity for smart operators that recognize it and are expanding into smart home services.

Chapter 2

IoT Communications and Interoperability Challenges

In This Chapter

- Identifying and connecting IoT devices with IPv6 and 6LoWPAN
- Using Wi-Fi for high-speed data networks
- Getting smart about Bluetooth
- Stirring up the IoT nest with Thread
- Keeping the IoT hive alive with ZigBee
- Joining AllJoyn and IoTivity together

In this chapter, you learn about several important communications standards and technologies and their role in the IoT and smart home solutions.

Addressing IP Shortages with IPv6 and 6LoWPAN

Originally developed by the U.S. Defense Advanced Research Projects Agency (DARPA), the Internet Protocol (IP) is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol suite.

IPv4 is commonly used to address devices/nodes in computer networks and on the Internet today. However, IPv4 addresses consist of only 32 bits and are thus limited to only 4.3 billion unique addresses. Every device/node communicating on the Internet requires a unique address. IPv4 was adopted by the Internet Engineering Task Force (IETF) at a time when it seemed like 4.3 billion unique addresses would be plenty.

After all, IBM's Thomas Watson had predicted in 1943 that there be "a world market for maybe five computers" and Ken Olsen of Digital Equipment Corporation predicted in 1977 that "There is no reason anyone would want a computer in their home." Perhaps the IETF was relying upon 3Com's Robert Metcalfe's prediction in 1995 that "the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse."

Fortunately, none of these predictions came to pass. Today, there are many times more than 4.3 billion unique devices/ nodes connected to the Internet.

In 1998, the IETF formally defined IPv6 as the replacement protocol for IPv4, primarily to address IPv4's address space limitations. IPv6 consists of 128-bit hexadecimal addresses that provide 3.4 x 10^{38} unique addresses — that's a really big number (340 hundred undecillion or so)! I (rather boldly) predict that IPv6 will provide enough unique IP addresses for IoT devices to last at least a few years — you read it here first!

Are standards a blessing or a curse?

This seems like a fair question, deserving of a simple and straightforward answer: Standards are both a blessing *and* a curse!

First, let's address the curse: It usually takes an interminable amount of time to define a new standard and, once defined, the standard often feels like a compromise that has been begrudgingly adopted, but doesn't fully serve the varied interests of all the different industry players.

But standards are clearly a blessing as well. Without standards, it would be exponentially more difficult and expensive to develop components, devices, equipment, software, machines, and systems — "things" — that integrate and interoperate with other things. Every element of a large system that can be standardized essentially removes a significant uncertainty factor from the overall complexity of the entire system — or, at least, isolates it and makes it more manageable.

Thus, one of the main blessings of standards is the enormous peace of mind that it provides for businesses and consumers alike, who can develop, build, and purchase solutions with confidence.

The key characteristics of standards are that they must be

- **Open** rather than closed (proprietary) to realize the advantages of low-cost, multivendor adoption, and peace of mind
- **International** to avoid complexity due to different regional requirements and settings

The main IPv6 challenge for IoT devices is that IPv6 addresses are very long (128 bits to be exact) — and long addresses are hard to remember! So, IPv6 devices require more memory which, in turn, reduces their battery life.

REMEMBER

IPv6 is a key enabling protocol that allows every IoT device in the world to have a unique address on the Internet.

TIP

In case you're wondering, the IETF doesn't count IP versions the same way I count burpees at the gym! They didn't skip versions 0 through 3 and 5 — those were all experimental versions. There are currently only two relevant versions of IP: 4 and 6.

The IETF has also produced a standard called 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), which essentially allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications requiring wireless Internet connectivity at relatively low data rates, such as smart light bulbs and smart meters.

Wi-Fi: Can't We All Just Get Along?

The Institute of Electrical and Electronics Engineers (IEEE) 802.11x standard (Wi-Fi) is an extremely popular choice for wireless home and business networks. Capable of high-speed throughput of several hundred megabits per second, the main disadvantage of Wi-Fi for IoT devices is that the data transfer rate is too fast. What?! ***Remember:*** Speed kills . . . battery life.

Many IoT devices, particularly in the smart home, are low-power, small-form-factor devices with very tiny batteries that are designed to last for years. These devices transmit lots of "small data" (discussed in Chapter 3) packets and, thus, do not require high data transfer rates. By comparison, battery-operated Wi-Fi devices typically need to be charged every day or so because they require reliable ("connection-oriented") high-speed data transfer rates.

Thus, other technologies, such as Bluetooth and ZigBee (discussed later in this chapter), complement Wi-Fi in the smart home and other IoT applications.

TECHNICAL STUFF

Wi-Fi meshing (IEEE 802.11s) was defined in the early 2000s but has not been widely adopted due to serious challenges in overcoming latency issues in connection-oriented protocols.

Making a Mesh Out of Bluetooth

Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. In 1999, Bluetooth openly challenged Wi-Fi on the wireless battlefield. Despite its weak WEP-onry, Wi-Fi prevailed in this conflict and Bluetooth found its own solid application space in personal technologies, such as smartphones, headsets, and cordless keyboards and mice.

More recent developments have been focused on making Bluetooth “networking capable” and have included Bluetooth Low-Energy (BLE, also known as Bluetooth Smart or Bluetooth 4.0+) and Bluetooth Mesh. BLE/Smart/4.0+ devices consume significantly less power than current Bluetooth devices and can access the Internet directly through 6LoWPAN connectivity (discussed earlier in this chapter). Bluetooth Mesh is an extension of BLE/Smart/4.0+ that enables connectivity to a larger set of independent devices (such as smart light bulbs in a smart home) working together in a mesh network.

WARNING!

Bluetooth Mesh, like IEEE 802.11s Wi-Fi meshing (discussed earlier in this chapter) is a connection-oriented protocol and must, therefore, overcome some of the same latency challenges as Wi-Fi meshing. It is therefore unlikely that Bluetooth Mesh will be widely adopted in the IoT.

Searching for a Common Thread

The Thread Group is an alliance created by Google/Nest, Samsung, ARM Holding, and others to create a wireless mesh networking protocol for the IoT — specifically, smart home solutions. The Thread stack is an open standard, but paid membership in the Thread Group is required for access to the full Thread specification.

The Thread protocol leverages various standards, including IPv6, 6LoWPAN, and IEEE 802.15.4 (all discussed in this chapter) to create an IP-addressable, local mesh wireless network of up to 250 devices. Thread is essentially the commercial version of 6LowPAN, in much the same way that Wi-Fi is the commercial version of IEEE 802.11 (for some reason, consumers prefer catchy names like “Thread” and “Wi-Fi” over “6LowPAN” and “IEEE 802.11”). Thread adds some security features and an application layer interface to 6LowPAN. Thread provides secure, low-power, redundant mesh networking with direct connectivity to the Internet and cloud services for smart home devices.

TIP

ZigBee can run on top of Thread and the next version of ZigBee IP will essentially be Thread.

Keeping Up with the ZigBee Buzz

ZigBee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. ZigBee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products. Important ZigBee specifications include

- **ZigBee PRO:** Provides the foundation for the IoT and smart home solutions including redundant, low-cost, ultra-low-power (even battery-free) devices and nodes with a full wireless mesh networking capability that is scalable to hundreds of nodes on a single network.
- **ZigBee GreenPower (GP):** Minimizes power demands with self-powered, energy harvesting devices and battery-powered devices that require ultra-long battery life, such as switches, panic or emergency buttons, and various sensors.
- **ZigBee RF4CE (Radio Frequency for Consumer Electronics):** Defines a robust low-power, low-latency radio frequency (RF) remote control network for two-way, device-to-device control applications that don’t require a full-featured wireless mesh network. ZigBee RF4CE supports multivendor interoperable devices such as remote controls, home entertainment systems, keyless entry, and garage door openers.

- **ZigBee IP:** The standard for a scalable IPv6-based (discussed earlier in this chapter) full wireless mesh network. ZigBee IP enables control of low-power, low-cost devices over the Internet and includes robust networking and security features. It's focused on — and in practice, limited to — Smart Energy solutions.
- **ZigBee Consolidation Application Layer (ZCAL):** Formerly known as the ZigBee Cluster Library (ZCL), ZCAL is the application layer language used to describe the functionality of IoT devices (for example, on-off control and temperature readings). ZCAL contains data models for the different device types used in home automation, building automation, and retail services, and it is continuously expanded to cover additional devices and functionality.
- **ZigBee 3.0:** Combines ZigBee Pro, GreenPower, and ZCAL, and includes a set of harmonized methods for commissioning nodes on a network to yield fully interoperable IoT products in the smart home.

Oh, I See — It's the OCF!

The Open Connectivity Foundation (OCF), formerly the Open Interconnect Consortium (OIC), was created in February 2016 and is one of the largest standards organizations for IoT connectivity. The OCF currently has more than 170 member companies, including Cisco, Electrolux, Intel, Microsoft, Qualcomm, and Samsung Electronics, among others.

OCF is bringing together earlier initiatives from Intel (IoTivity from the OIC) and Qualcomm (AllJoyn from the AllSeen Alliance), both of which are largely complementary and overlapping open-source projects under the Linux Foundation. Both IoTivity and AllJoyn enable seamless discovery and device-to-device (D2D) connectivity to an IoT network.

Despite some competition for market share and overlap between technologies, Wi-Fi, Bluetooth, Thread, ZigBee, and OCF all seem to have found a core application space and will, thus, have important complementary roles in the IoT for the foreseeable future: Wi-Fi for content sharing and distribution, Bluetooth for cable replacement and wearables, Thread and ZigBee for low-power sense and control networking, and OCF at the Application Layer.

Chapter 3

It's a Small (Data) World!

In This Chapter

- Collecting data — about big and small data
- Getting smart in the IoT cloud
- Recognizing the changing nature of cyberthreats in the IoT

In this chapter, you learn about the various IoT data, analytics, and security/privacy challenges that must be addressed.

Big Data Is Big, and Small Data Will Be Massive

Digital data is everywhere. EMC's seventh annual *Digital Universe Study* estimates that the total amount of digital data created, replicated, and consumed worldwide is doubling every two years and predicts that it will reach 40,000 exabytes by 2020. To put that in context, it would take almost 2.2 quadrillion trees to print 40,000 exabytes of data — nearly 700 times more than the estimated 3 trillion trees on the entire planet!

TECHNICAL STUFF

A terabyte is equal to 1,024 gigabytes, a petabyte is equal to 1,024 terabytes, and an exabyte is equal to 1,024 petabytes.

However, according to the EMC study, "only 22 percent of the information in the digital universe [is] considered useful data, [and] less than 5 percent of the useful data is actually analyzed." Data generated by the IoT is expected to increase useful data to more than 35 percent of the digital universe by 2020.

Much of this “useful data” is what many businesses today refer to as “big data” — extremely large (sometimes multiple petabytes) datasets of structured and unstructured data collected from numerous sources and analyzed for various patterns, trends, and behaviors using advanced technology frameworks such as Hadoop and MapReduce.

But there is another facet of IoT data that is equally important — and potentially useful — in the digital universe: small data. Small data is generated as very small datasets containing very limited or specific attributes, such as temperature readings in a smart home, speed in a smart car, or heart rate in a smart pacemaker. These datasets can be collected at periodic intervals — for example, every 5 seconds — and over time the data collected becomes quite massive.

TIP

St. Jude Children’s Research Hospital founder Danny Thomas famously said, “I’d rather have a million people give me a dollar than one [person] give me a million [dollars]. That way, you’ve got a million people involved.” The IoT is taking a cue from Danny Thomas with billions of devices and trillions of sensors contributing small data to a massive digital universe!

Small data is typically used in IoT devices in near real-time to determine current states or operating conditions and trigger appropriate actions or events. For example:

- ✓ Making a minor temperature adjustment in a smart home to maintain a comfortable environment
- ✓ Changing certain engine parameters to improve a smart car’s fuel efficiency and safety at a given speed
- ✓ Administering a small electrical charge to properly regulate a person’s heartbeat

Both big and small data will play important roles in the IoT, and it should be readily apparent from the few examples described in this section that security and privacy are extremely critical in the smart, connected world. I cover these topics in the following sections.

Data Analytics and Self-Learning in the Cloud

Much of the work that has already been done in the field of data analytics is focused on surfacing patterns and trends in big data so that organizations can make informed decisions using predictive analytics. For example, businesses make strategic decisions that impact future profitability based on financial data or use data about consumer preferences to positively influence the customer experience. Government organizations may use financial data to identify fraud in social programs or use various sociological data to identify potential "hot spots" for crime and proactively police those areas.

Significant work has also been done to develop algorithms to "understand" and interpret small data collected in the cloud, as well as to identify exception conditions. This requires processing massive amounts of small data from a near continuous stream of data from perhaps as many as 100 IoT devices in a smart home of the future.

This "self-learning" capability in the cloud is critical to future IoT applications, such as family and senior lifestyle systems (discussed in Chapter 2 of *Internet of Things Applications For Dummies*), which rely upon fuzzy logic and other artificial intelligence (AI) technologies to perform intelligent actions without a constant need for human intervention.

Keeping Small Data Private and Secure Is a Big Deal

Privacy and security are key to the IoT, but they also require tradeoffs. People, by their nature take risks — for example, as a matter of convenience — which potentially compromises their security and privacy. These issues are not unique to the IoT — they exist in the Internet of today as well. However, the nature of the threat changes with the IoT. Today, identity theft and credit card fraud are the prevalent motivators for cyberattacks. With the IoT, extortion, hacktivism, and cyberterrorism can become increasingly prevalent cyberattack threats.

The value of small data to a cybercriminal may not be readily apparent. After all, threatening to expose how many steps a person takes during the day or the temperature in her smart home is unlikely to extract a hefty extortion payment. But threatening to expose explicit images stolen from various cameras in a smart home or causing a pacemaker or insulin pump to malfunction is far more serious.

Likewise, hacktivist groups motivated by political or social causes might target a utility company's smart grid system, causing billing errors that will potentially bankrupt the company.

Finally, cyberterrorists might target these same IoT medical devices and simply forgo the extortion demands, killing unsuspecting patients on a random and large scale. Smart cars may similarly be targeted to cause death and injury, and smart grids may be targeted to cause widespread outages or manmade environmental disasters.

The big challenge for security in the IoT is that it should not interfere with ease of use and comfort. For example, having to enter a passcode to turn a light on or off is unrealistic. The future of the IoT will most likely be a hybrid security solution combining familiar, legacy mechanisms with more advanced technical solutions, much like the keyless entry systems on many cars today — despite being able to unlock and even start these cars without a key, most cars also still unlock and start with keys, just in case the owner feels a bit nostalgic.

Another IoT security challenge is the lack of a direct user interface for many IoT devices and sensors. A computer or smartphone has a keyboard and screen that allows a user to enter a security passcode, for example. A smart lamp or smoke detector doesn't have a direct interface, although a smartphone application may help.

To properly secure the IoT, device manufacturers, developers, and service providers must work together to ensure that access to IoT applications, systems, devices, sensors, networks, and connectivity, as well as the data that they generate, is properly secured with strong encryption and secure key management. However, encryption alone isn't enough. IEEE 802.15.4, for example, uses 128-bit Advanced Encryption System (AES) for security, but additional measures, such as increasing counters and randomization to prevent man-in-the-middle and replay attacks, are also necessary.

Chapter 4

Eight Key IoT Takeaways

In This Chapter

- Creating smart solutions and services, not just connected things
- Working together for a brighter (and interoperable) IoT future
- Addressing data, security, and privacy challenges

You know 'em, you love 'em. Here's a list of eight IoT connectivity takeaways, presented in classic *For Dummies* style!

- **Smart and connected aren't the same thing.** A "smart" IoT device or component must be able to automatically perform intelligent actions based on analysis of data that is collected by the device or component. Simply connecting some "thing" to the Internet isn't enough.
- **Consumers want solutions, not things.** Despite the "coolness" factor of many of the latest gadgets and gizmos, the overwhelming majority of consumers aren't looking for a bunch of cool things. They want smart solutions and services that will make their lives better, easier, healthier, safer, simpler, more comfortable, more convenient, more efficient, and more enjoyable.
- **Smart businesses will offer smart services for recurring revenues "from the cradle to the grave."** Consumers are increasingly shifting from buying things ("ownership") to buying services ("usership"). Smart businesses will look beyond an initial product purchase to a recurring revenue model that provides consumers with value-added services (not an "extended warranty") throughout the life of the IoT solutions they use.

- **Adopting standards is critical for the success of the IoT.** The IoT is a rapidly changing and constantly evolving frontier. Without standards, device manufacturers will rush to market with the latest "thing" in order to exploit short-term competitive advantages and fast profits, without regard to interoperability or long-term sustainability. To make the IoT a truly smart, connected universe rather than an Internet of random "stuff," standards need to be adopted.
- **Significant confusion and overlap exists in the IoT industry.** Many large alliances, consortiums, and industry players are jockeying for position and leadership in the IoT. Many of these alliances compete with and overlap each other, while at the same time cooperating in some instances!
- **ZigBee is the smart choice for the smart home.** The ZigBee Consolidated Application Library (ZCAL) is an excellent choice for the Application Layer language because it's a market-proven solution and fully integrated in ZigBee 3.0. It's expected to become the Application Layer language of choice for other IoT communication standards as well.
- **Think big when it comes to small data.** Businesses have been focused on the opportunities and challenges of big data for many years. With the IoT, small data — very small datasets containing limited or specific attributes collected by sensors — will complement big data to create even greater opportunities . . . and challenges.
- **Security and privacy become a matter of life or death.** Identity theft and credit card fraud are the preeminent forms of cybercrime today. IoT applications such as smart cars, smart homes, smart utilities, and smart wearables and medical devices will open up a Pandora's box of new threats that will increasingly become the cyberattacks of choice, including ransomware, hacktivism, and cyberterrorism. Security and privacy must be top of mind for everyone in the IoT industry.

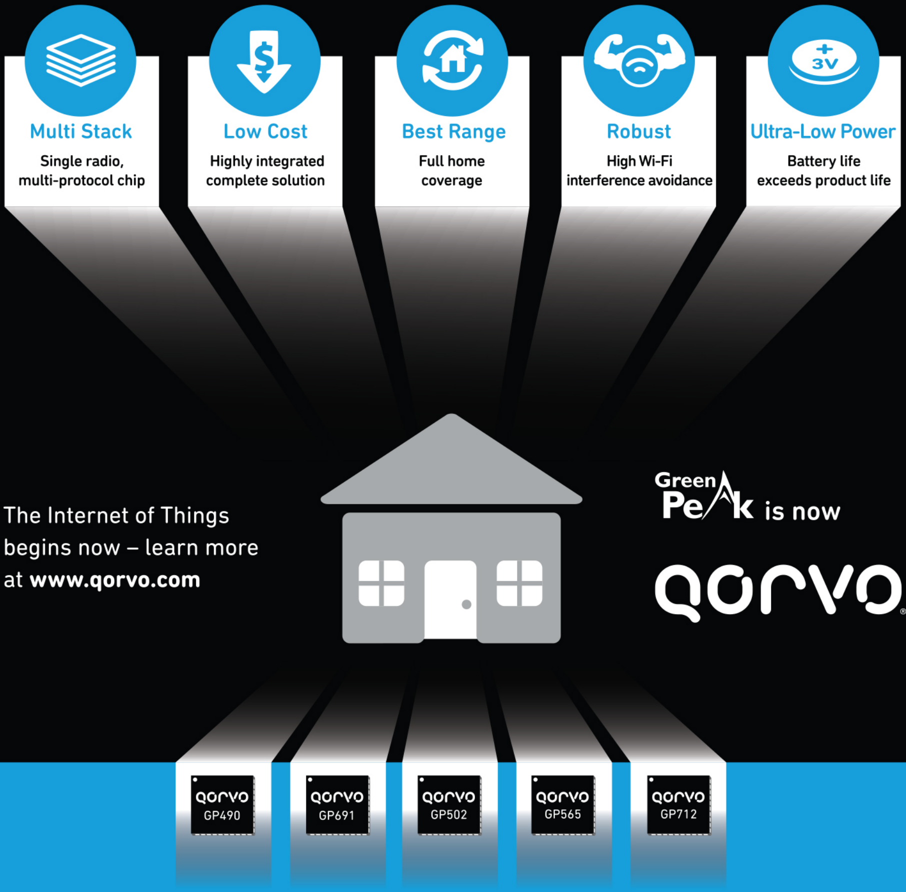
REMEMBER

The IoT enables better decisions to be made faster with timely, higher-quality data.

Futureproofing the wireless smart home.

Consumers worry the smart home products they buy today won't talk to next year's gadgets. Qorvo's ultra-low power IEEE 802.15.4 solutions solve compatibility issues and support the multiple home networking standards of today and tomorrow, with a single chip.

Qorvo's key RF differentiators



Multi Stack
Single radio, multi-protocol chip

Low Cost
Highly integrated complete solution

Best Range
Full home coverage

Robust
High Wi-Fi interference avoidance

Ultra-Low Power
Battery life exceeds product life

The Internet of Things begins now – learn more at **www.qorvo.com**

GreenPeak is now qorvo®