IEEE STANDARDS ASSOCIATION

Published by Standards Information Network IEEE Press

THE WIRELESS INTERNET OF THINGS

A GUIDE TO THE LOWER LAYERS

DANIEL CHEW

IEEE PRESS

WILEY

The Wireless Internet of Things

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

The Wireless Internet of Things

A Guide to the Lower Layers

Daniel Chew

Published by
Standards Information Network

IEEE PRESS

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

ISBN: 9781119260578

Cover Design: Wiley
Cover Image: iStock.com/monsitj

Set in 10/12pt WarnockPro by Aptara Inc., New Delhi, India

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Preface

While the current state of the IoT market is fragmented across manufacturers and product lines, the future of IoT lies in interoperability. This interoperability will be enabled and communicated through easy access to technology standards developed by the IEEE and others.

This book provides an overview of several wireless standards for connectivity in the Internet of Things (IoT) and then addresses relevant wireless communications theory to help elucidate those standards. The book details the lower layers of a protocol stack in describing the wireless IoT from the bottom-up. In doing so, the book decomposes the issues to be addressed into smaller subsets.

Chapter 1 introduces the concept of the wireless internet of things, detailing background information and giving a few examples of applications. Those applications drive the requirements for the wireless links that enable the wireless IoT. The book then introduces the concept of protocol stacks, such that the wireless links can be decomposed into layers with specific responsibilities. The book gives several examples of protocol stacks and the slight differences in functional decomposition across layers. The fact that the lower layers, physical and media access, are generally covered by independent standards bodies is addressed. This book then sets its scope on those lower layers used for link establishment, channel access, error detection, and modulation. This is done by following a unified lower layer model with three layers, radio, Modem, and Media Access Control.

Chapter 2 outlines physical and media access layers for several popular open wireless standards used by IoT applications. This book focuses on open standards defined by independent standards bodies. Several popular wireless IoT protocols are referenced in a nominative sense in order to link the open standards to applications with which the reader may be more familiar. Those popular protocols are Bluetooth (formerly IEEE 802.15.1), IEEE 802.15.4, and ITU G.9959. This book focuses on low-power wireless links for the IoT; however, this chapter also briefly discusses Wi-Fi as Wi-Fi is important to many IoT applications. Wi-Fi appears again in later chapters as Wi-Fi interacts with the standards identified. This chapter can be used as a quick reference guide for the various protocols. This chapter also introduces concepts that will be explored in the later chapters, and informs the reader as to where in the book more information on that topic can be found.

Chapter 3 is dedicated to the aforementioned Radio layer. Radio front-ends are explored in this chapter. There is a slant toward software-defined radio implementations of IoT protocols, but multiple radio hardware topologies are explored. This chapter reviews the concept of link budgets and goes through examples. This chapter also addresses complex channel models employing both large and small-scale fading.

Chapter 4 focuses on the MODEM. This chapter covers the concepts of the complex-envelope signal model, modulation, demodulation, synchronization, and spread spectrum. Linear and angular modulation schemes as used in the identified open standards are explored, both in terms of background theory and also as to why a particular standard would choose a particular modulation scheme. Synchronization techniques for carrier and symbol recovery are discussed. The chapter ends with a discussion on the various spread spectrum techniques employed in the physical layers of the wireless IoT.

Chapter 5 describes the Media Access Control layer. Channel access schemes commonly employed by the wireless IoT standards, such as CSMA, are detailed. The chapter describes the different bands used by the wireless IoT standards. In particular, the 2.4 GHz Industrial, Scientific, and Medical band, and the congestion therein, is detailed. The chapter describes various interference and interference mitigation techniques employed in wireless IoT standards. The chapter concludes with a discussion on error correction and detection.

A recurring theme in this book has been that no one book can cover all of wireless system design. There are many books relevant to this course of study, on topics ranging from antenna design to symbol synchronization. This book provides background material in relevant theory, analysis of design choices, and numerous citations to aid the reader interested in learning more on a given subject. Each of the chapters in this book provides a list of references such that the interested reader can research the topic in more detail than can be covered in this limited scope.

It is the hope of the author that this book is useful to a variety of readers. Developers of platforms and applications of IoT will benefit from this book that provides a practical survey of standards relevant to the lightweight and low-cost needs of IoT platforms. This book will be useful for a variety of engineers involved in Digital Signal Processing (DSP), network implementation, and wireless communication, but could also be useful to the entrepreneur or hobbyist looking to understand the technology and develop the next big Thing.

Daniel Chew

Acknowledgments

I would like to acknowledge the people who helped make this book a reality. I would like to thank the series editors Jack Burbank and Bill Kasch for giving me the opportunity to write this book. I would like to thank Andrew Adams and Joseph Bruno for their review of my earliest material. I would like to thank Ken McKeever and Ryan Mennecke for their assistance and expertise in this field.

I also want to thank my family and friends who supported me through this process. Without them, this book could not have been possible.

I would like to dedicate this book to my wife, Lleona, and to my children, Marin, Everett, and Theodore.

About the Author

Daniel Chew is a member of the Senior Professional Staff at The Johns Hopkins University Applied Physics Laboratory and teaches in the Engineering for Professionals program at Johns Hopkins University. He received a Bachelor's of Electrical Engineering from the University of Delaware in 1998 and a Master's of Science in Electrical and Computer Engineering from Johns Hopkins University in 2008. His professional interests are in the Internet of Things, Wireless Communication Systems, Digital Signal Processing, and Software-Defined Radios.

1

Introduction

This book began as a collection of observations and implementation experience that the author accumulated while researching wireless links used to enable the "Internet of Things" (IoT). Wireless communications engineers approach the challenge as a stack of layers, where the system has been decomposed into a stacked series of functions. Approaching the various wireless links used for IoT in this layered fashion helps cultivate an appreciation for the various standards that enable interoperability. This book will approach several standards for the wireless IoT from the layered perspective as found in a protocol stack. Organizing this book in the manner of a protocol stack will help the reader better navigate this book, and hopefully, shed some light on the purpose of the specifics within the different wireless standards that empower the IoT.

Let's begin with a question: What is the Internet of Things?

1.1 What is the Internet of Things?

The term "Internet of Things" has been around since the early 2000s [1]. This term refers to autonomous computing devices being networked together to perform various tasks. The term was coined by Kevin Ashton of the MIT Auto-ID center and was originally in reference to Radio Frequency Identifier (RFID) information being made available on the Internet [2]. RFID is a technology that allows objects to be tagged with devices that transmit identification information. RFID allows for the automatic identification and tracking of those tagged objects. This information can be sensed, gathered, parsed, and posted to the internet by way of automated and interconnected computing devices. The term "Internet of Things" has since grown to encompass far more applications and technologies than the original RFID reference.

There are a number of application areas that have either been adopted into or have grown from the Internet of Things, including:

- home automation
- medical devices

The Wireless Internet of Things: A Guide to the Lower Layers, First Edition. Daniel Chew.

- industrial control
- smart grid
- distributed sensor networks
- and others

The Internet of Things is not a new concept, technology, or set of products, but is rather a natural evolution of networked computing technology, enabled primarily through affordable processing and connectivity. IoT is an extension of the "ubiquitous computing" concept popularized by Mark Weiser [3,4]. The size and cost of computing power is and has been decreasing for decades. This decrease in size and cost has resulted in small, inexpensive embedded devices, which are ideal for sensor and interface applications. Combined with the ease of connectivity provided by a robust and varied infrastructure consisting of wired, terrestrial cellular, satellite, and local wireless communication technologies, the rise of the Internet of Things is the natural consequence. While all of the technologies that comprise the Internet of Things are important, it is connectivity, particularly wireless connectivity, that is a fundamental component shaping many of the choices made in the implementation of IoT devices.

Figure 1.1 [5] illustrates the wide reach of this technology in both "vertical" and "horizontal" markets. The "vertical markets" address the needs of a specific group of consumers, and "horizontal markets" seek to address the needs of a wide group of consumers. By making use of technologies such as ubiquitous computing and wireless communications, the IoT transforms objects from being "traditional" to "smart." In Figure 1.1, these smart objects are grouped into domain-specific applications (vertical markets) while network-computing services form domain-independent services (horizontal markets).

These network-computing services are sometimes called "The Cloud." What is "The Cloud"? There is a humorous answer to that question: "There is no cloud, just someone else's computer."

"The Cloud" is a collection of computation and data storage resources made available to end-consumers by a service provider. End-consumers gain access to these resources through the Internet. This collection of computation and data storage resources is shared across the large number of end-consumers with whom the service provider has some contract.

"Cloud Computing" is where computational tasks are offloaded from local devices and executed on remote, presumably larger and more powerful, devices. The local devices make requests of the remote, more powerful, "cloud" devices. The cloud devices execute the request and provide the results to the local, smaller, devices that directly interface with the end-user.

Wireless IoT technology interfaces with "The Cloud" and "Cloud Computing" to provide many different end-user applications. For example, an end-user may use their smart phone to access a cloud data center that is updated with the status of various sensors. In that example, the wireless IoT devices form a "device

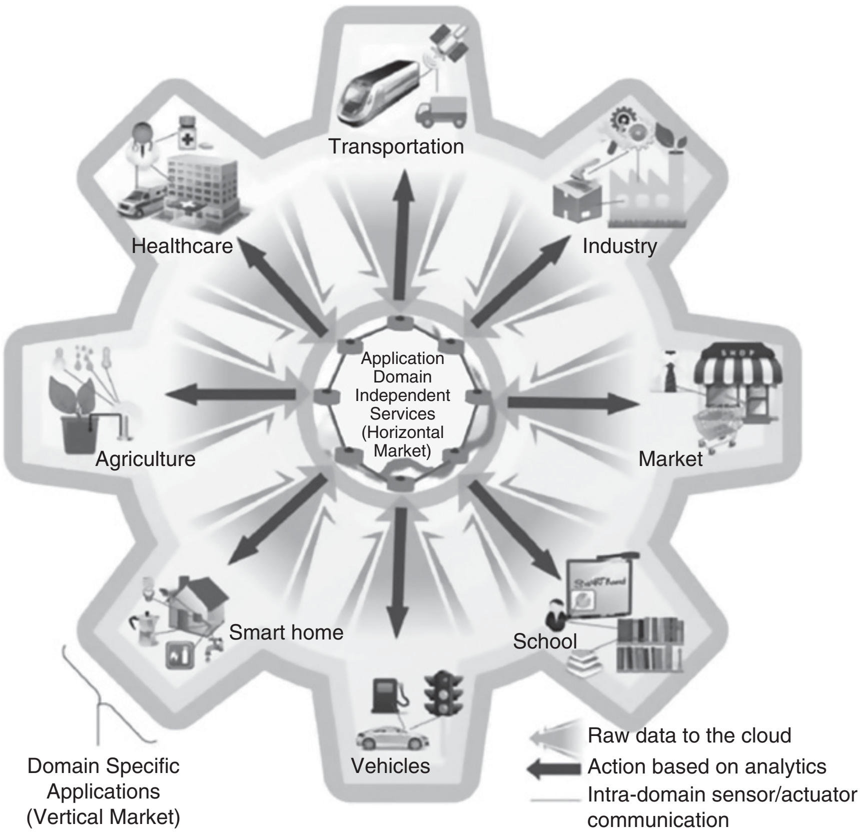

Figure 1.1 The IoT Across Vertical and Horizontal Markets [5]

network" that sends information through a gateway to a server "in the cloud." The end-user can then access that information by using a personal wireless data device to log into the repository of sensor data stored on the remote server.

While the specific implementations of each of these application areas may be quite different, they all rely on the ability to remotely monitor, manage, and actuate distributed devices. IoT technology has enabled a wide variety of applications and is already deployed across markets as disparate as health care and power grids. World market analyses have made forecasts predicting the continuing rise of IoT applications and significant contributions to the world GDP [6].

An interesting trend within the IoT is the accessibility of development to individuals, which is a by-product of low-cost processing [7]. The availability of inexpensive general purpose embedded processing devices means that device and application development is no longer limited to companies with substantial development and manufacturing budget. Hobbyists and members of the Maker community are able to make use of these platforms to create their own devices for their own unique applications.

With so much development in this field, it is clear there is a risk of fragmentation and a lack of interoperability. Without interoperability, nothing in Figure 1.1 would function. Therefore, the future of IoT lies in interoperability. It is this interoperability that makes connectivity possible. This interoperability will be enabled and communicated through easy access to technology standards developed by the IEEE and others.

This book will focus on the wireless aspects of the IoT, and the standards that enable the necessary interoperability. To that end, there must be provided a disambiguation in what is being referred to as the "wireless" Internet of Things in this book.

1.2 What is the Wireless Internet of Things?

For applications of the IoT, as networks of increasingly autonomous computing devices performing some task, wireless connectivity is often essential. Consider Figure 1.2 [8]. Figure 1.2 shows disparate applications, all connecting to the internet by way of wireless access points. Those wireless access points alone demonstrate the importance of wireless connectivity to the IoT.

Moreover, many of those application areas shown in Figure 1.2 would not be possible without locally networked devices. Wireline connectivity can establish a network of automated computing devices and connect those devices to cloud-based services. Wireless connectivity provides benefits in deployment that are unmatched by wireline solutions. Numerous sensor applications simply will not

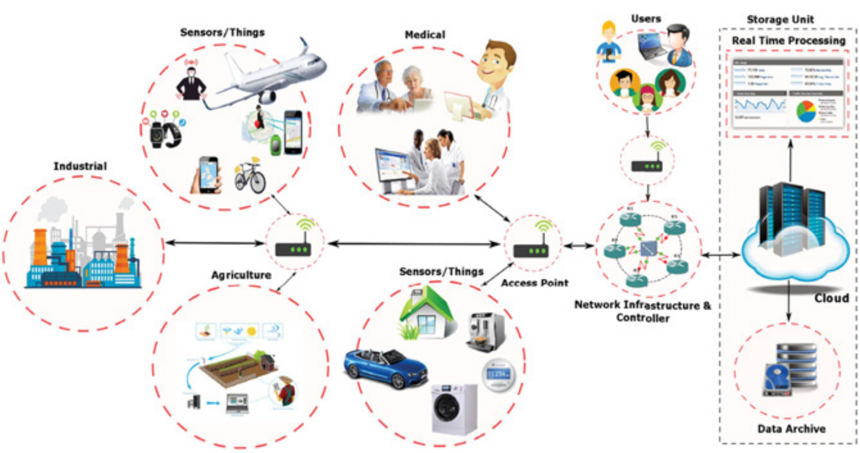

Figure 1.2 The IoT Application Areas and Wireless Connectivity [8]

function without mobility, which requires wireless connectivity. For these reasons and others, wireless connectivity is a key element to the success of IoT.

Using the term "wireless Internet of Things" narrows the conversation to focus on that wireless connectivity as opposed to cloud-based services and other aspects of popular IoT applications.

1.3 Wireless Networks

Networking is essential for the wireless IoT. Different types of networks exist to satisfy the needs of different end-user applications. Therefore, while not the focus of this book, a brief discussion of the various types of wireless IoT networks is necessary to better understand the functions of the lower layers that will be covered in the subsequent chapters.

1.3.1 Network Topologies

A network topology is the organization of nodes in a given network of nodes. A common network topology for the wireless IoT is the "star" topology [9]. The star topology is illustrated in Figure 1.3. The star topology is called such because all network traffic converges onto a single point. If any data is intended

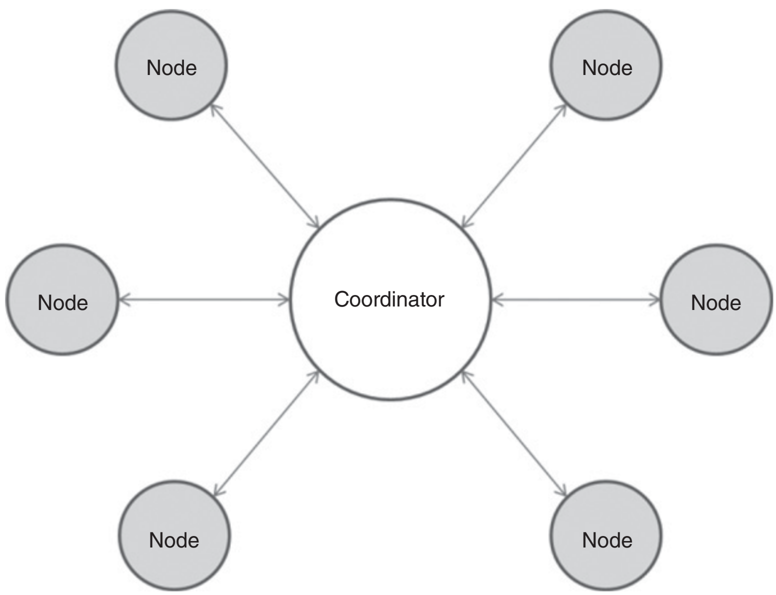

Figure 1.3 Star Topology

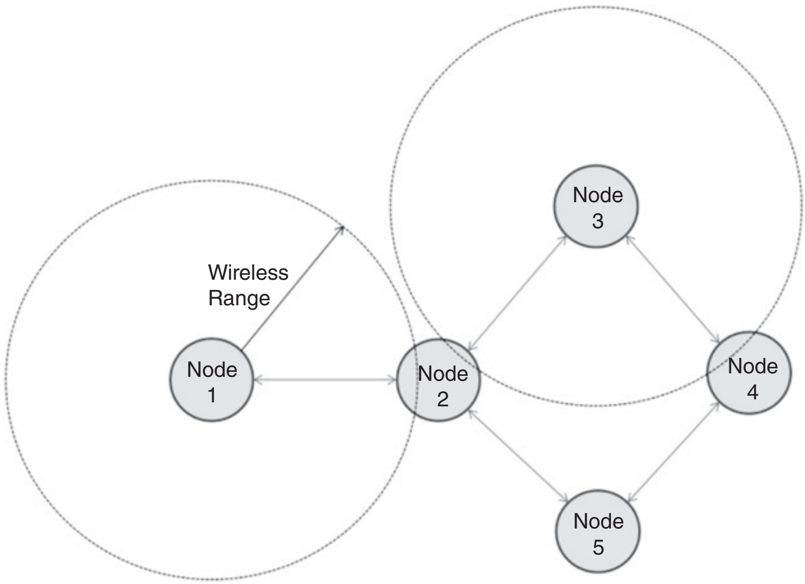

Figure 1.4 Mesh Topology

to travel from one node to another, that data must still travel through the central point of the star topology. Under the star topology, the central point serves as a coordinator for all other nodes in the wireless IoT network.

Wireless IoT networks can also be organized into "mesh" networks [9]. These mesh networks are sometimes called "peer-to-peer" networks. The mesh topology is illustrated in Figure 1.4. The nodes in the mesh network can establish links to other nodes within wireless range. Only the wireless ranges for nodes 1 and 3 are shown in in Figure 1.4 to avoid clutter. In order to propagate data from one node to another, routing must be established between the nodes. In Figure 1.4, Node 1 can only communicate with Node 2. Node 2 can see Nodes 1, 3, and 5. Node 3 can see Nodes 2 and 4. In order for Node 1 to send a message to Node 4, the message must be routed from Node 2 to either Node 3 or Node 5 and then routed again to Node 4.

Figure 1.4 shows the complexity of routing in the mesh network topology as compared to the simplicity of the star topology in Figure 1.3. The star topology requires that one coordinator node keep contact with all subordinate nodes. The mesh network topology allows for a more flexible structure to take shape, but requires routes to be in place for nodes to communicate. The exact method of establishing routing between nodes for a given wireless IoT system is specific to the wireless IoT protocol. A discussion on algorithms for routing data between nodes exceeds the scope of this one book.