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

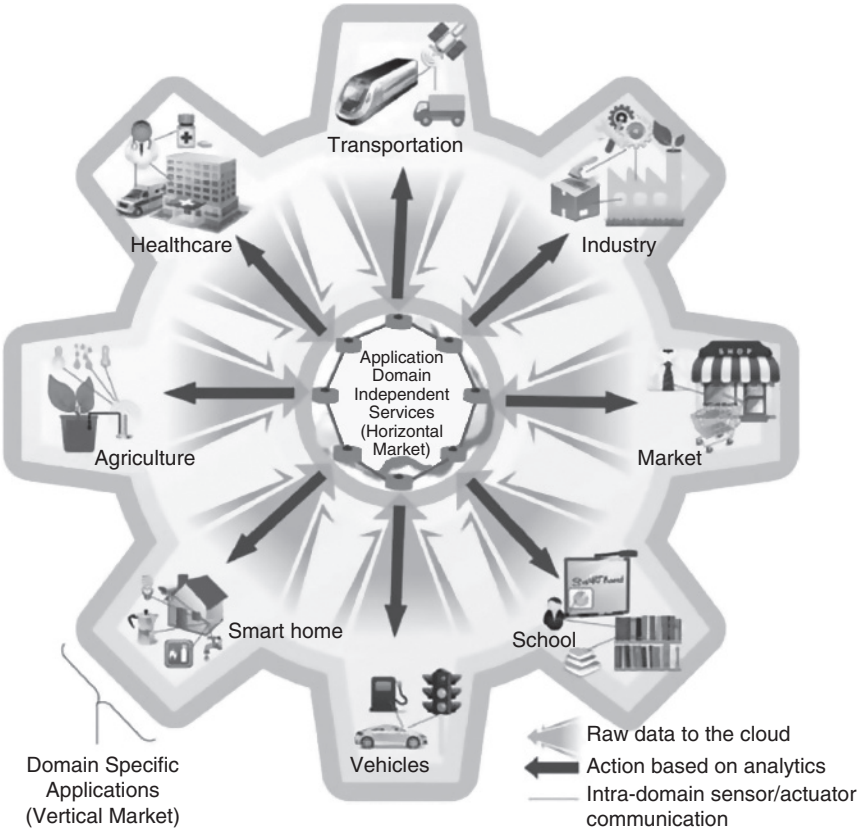

Figure 1.1 The IoT Across Vertical and Horizontal Markets [5]

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

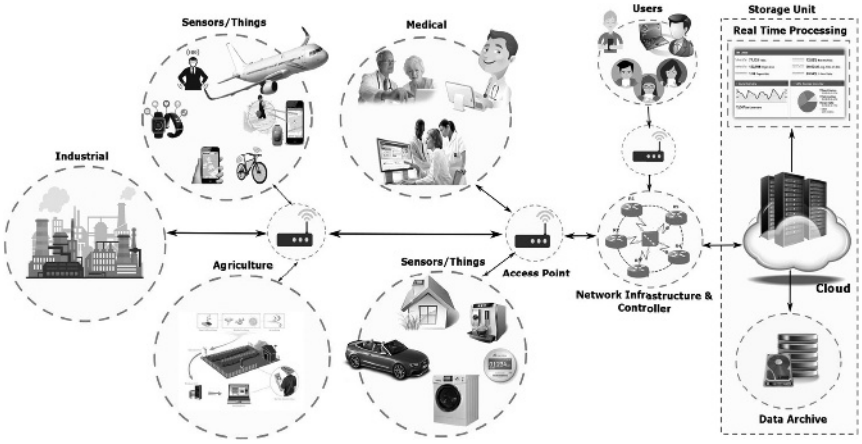

Figure 1.2 The IoT Application Areas and Wireless Connectivity [8]

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

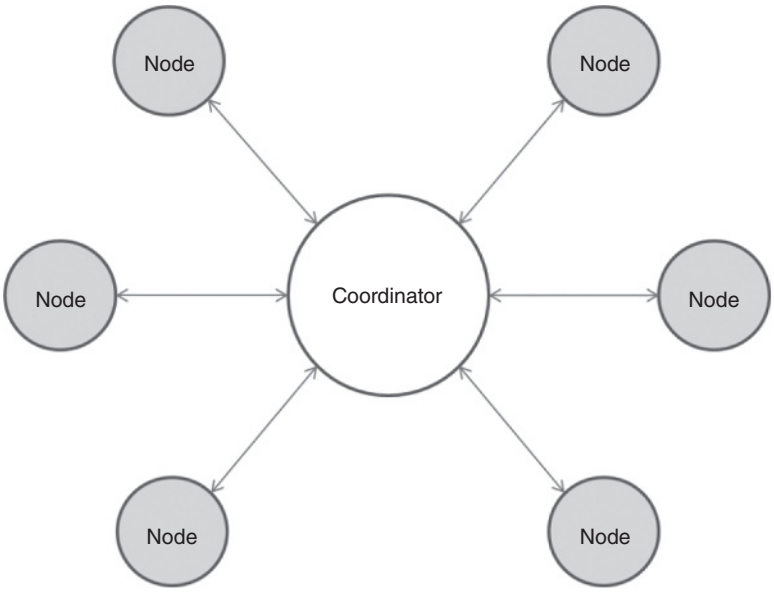

Figure 1.3 Star Topology

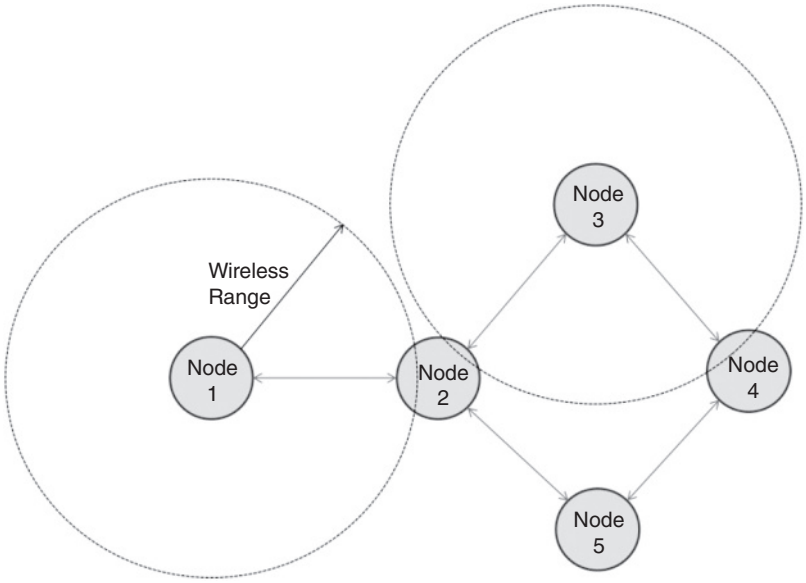

Figure 1.4 Mesh Topology

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.

1.3.2 Types of Networks

In addition to topologies, there are different types of networks designed for different scales and uses. For example, a Local Area Network (LAN) is a network intended for a single building or campus [10]. A Wide Area Network (WAN) is a network intended for an entire country or continent [10]. The Internet is an example of a WAN. A local wireless Internet connection, such as the type one might have at home with a Wi-Fi router, is referred to as a Wireless LAN (WLAN). The wireless router also provides a "gateway" for all the computing devices in your home to access the Internet. This concept is illustrated in Figure 1.5. Several personal computers and a smart phone are connected to a WLAN. The WLAN is established by a Wi-Fi router that also provides a gateway for Internet access.

A Wireless Personal Area Network (WPAN) is a network formed for data flow between the user's own personal devices. A WPAN is therefore smaller in scale than a WLAN. An example is illustrated in Figure 1.6. In this example, a wireless PAN is formed as a star topology where the central node, a smart phone, takes the role of coordinator. Figure 1.6 illustrates how a Bluetooth connection between a user's smart phone and associated peripherals such as wireless headphones is an example of a WPAN [11].

Gateways play an important part in many IoT applications. The concept is illustrated in Figure 1.7 and Figure 1.8 for the star and mesh topologies, respectively.

In Figure 1.7, a wireless "device network" connects various devices to a coordinating node in a star topology. This coordinating node then accesses a Wi-Fi router to send data to a cloud server. The Wi-Fi router serves as a "gateway."

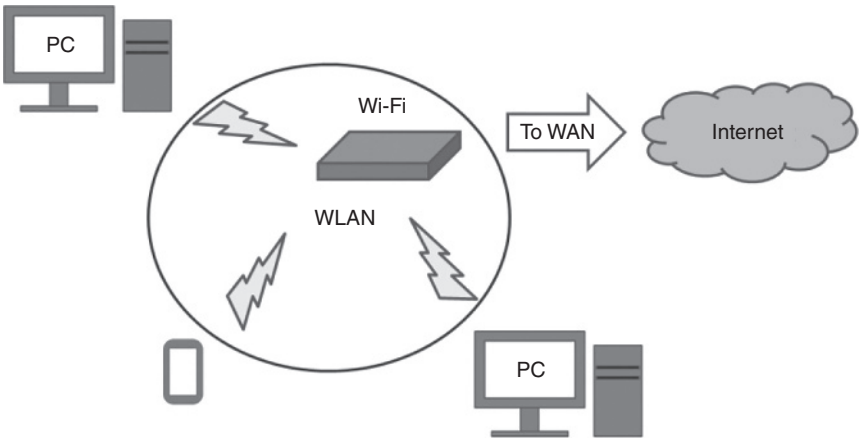

Figure 1.5 WLAN and Gateway to WAN

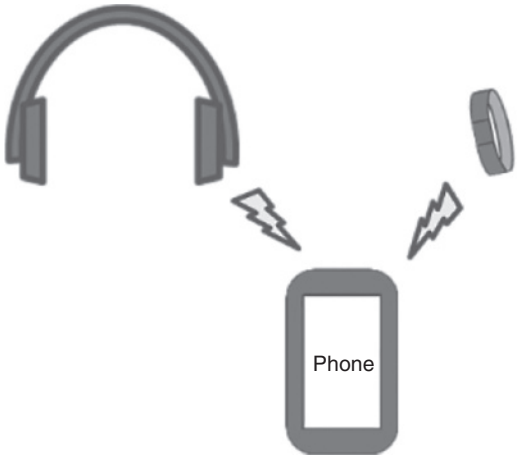

Figure 1.6 Wireless PAN

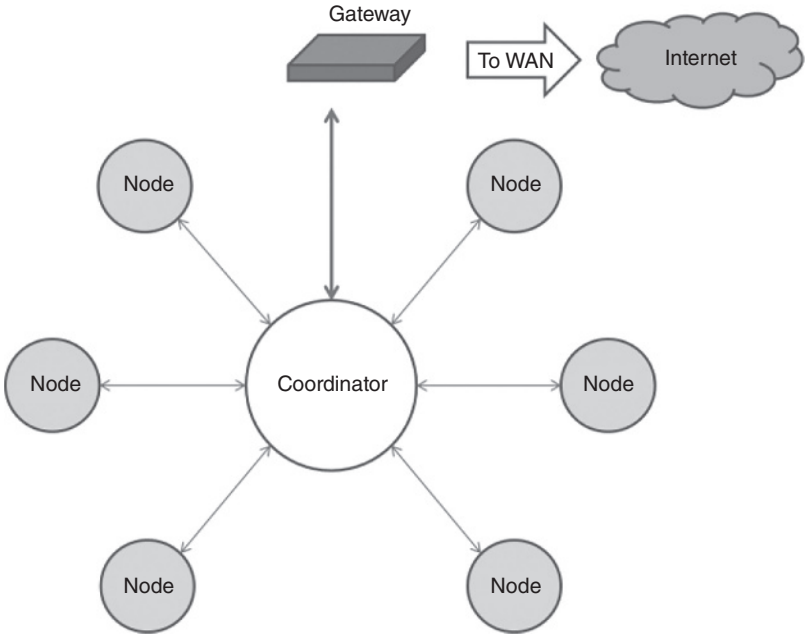

Figure 1.7 Star Device Network

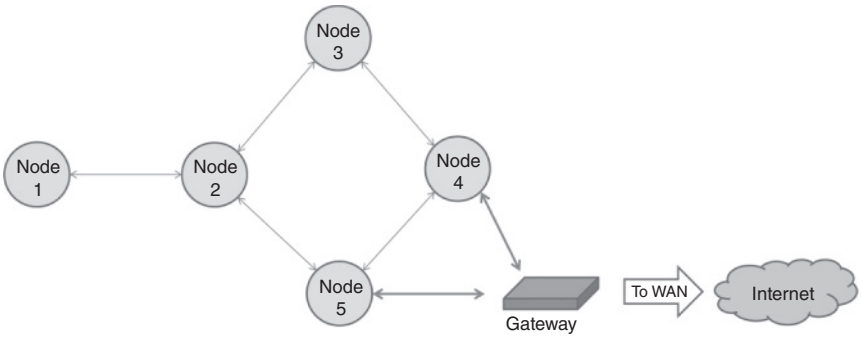

Figure 1.8 Mesh Device Network

Data from the device network is funneled to the coordinating node, which then passes the data to the gateway where it will be sent into the larger Internet.

In Figure 1.8, a number of nodes are configured in a mesh network that exists at the periphery of the larger Internet. Data from the furthest nodes must be routed and the funneled to the gateway in order to export data to the Internet.

Reference [12] provides an example use-case for a wireless device network configured in mesh topology. The use-case is illustrated in Figure 1.9. Figure 1.9 shows a wireless device (sensor) network designed to track cattle position and health. Node 1 is composed of multiple sensors and two transceivers. This node serves as the coordinator. The coordinator bridges between the device network and a WLAN. The other nodes are composed of multiple sensors and one transceiver. That one transceiver processes a low power communications protocol, ZigBee, and sends data through the network to the coordinator.

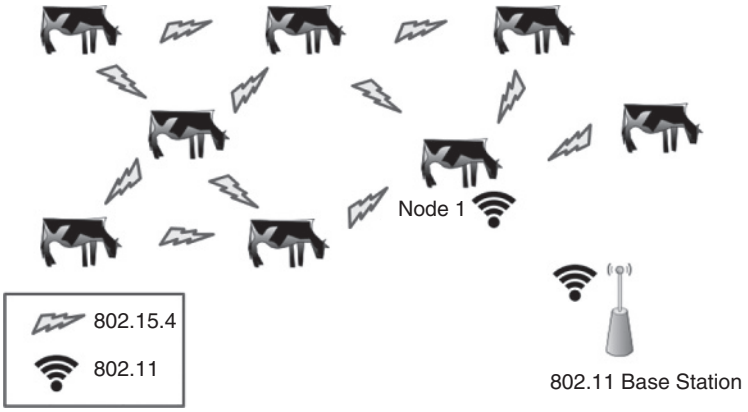

Figure 1.9 Mesh Topology of a Device Network in eAgriculture [12]

The devices in the device network are expected to operate on battery for extended periods of time. This means that the devices must be low power in order to extend battery life. The preference for low power wireless links is common in wireless sensor networks and the wireless IoT in general. This book shall focus on the standards that define the wireless links between low power devices in the wireless IoT.

1.4 What is the Role of Wireless Standards in the Internet of Things?

Wireless standards specify features for a shared wireless link such as the modulation scheme, bands of operation, and data rate, among others. Having a standard set of features in the wireless link allows for interoperability between devices created by different vendors.

Standardized wireless protocols provide a means of interoperability such that data can be exchanged between remote nodes and computing devices inside an IoT network. Wireless IoT devices conform to one of these standards and then the device can join an IoT network defined by that protocol.

The interoperability of devices utilizing these protocols rests upon conformance to a wireless standard. The standards themselves are written in such a way that a design can be tested for conformity. The standards offer little in the way of justification for the limits imposed or choices made for that standard. One of the primary goals of this book is to elucidate wireless standards pertaining to the IoT. To that end, this book approaches wireless IoT standards as "protocol stacks." A theoretical background for the wireless IoT must be provided from the ground-up. From there, the pieces can be tied together to describe in detail some of the most common wireless IoT protocols.

1.5 Protocol Stacks

A "protocol stack" is a series of layers of processing, each "stacked" upon the other. This concept is illustrated in Figure 1.10. In this example, the middle layer is labeled "Layer N" and the layers immediately above and below are labeled "Layer N + 1" and "Layer N-1," respectively. This is to demonstrate the sequential nature of the layers in data processing. Received data comes up from the physical medium and is processed sequentially by each layer from lowest to highest. The higher layers send data down to the lower layers to be transmitted across the physical medium.

Most communication systems, including the protocols for the wireless IoT, are organized into a protocol stack [13]. Such a layered architecture provides

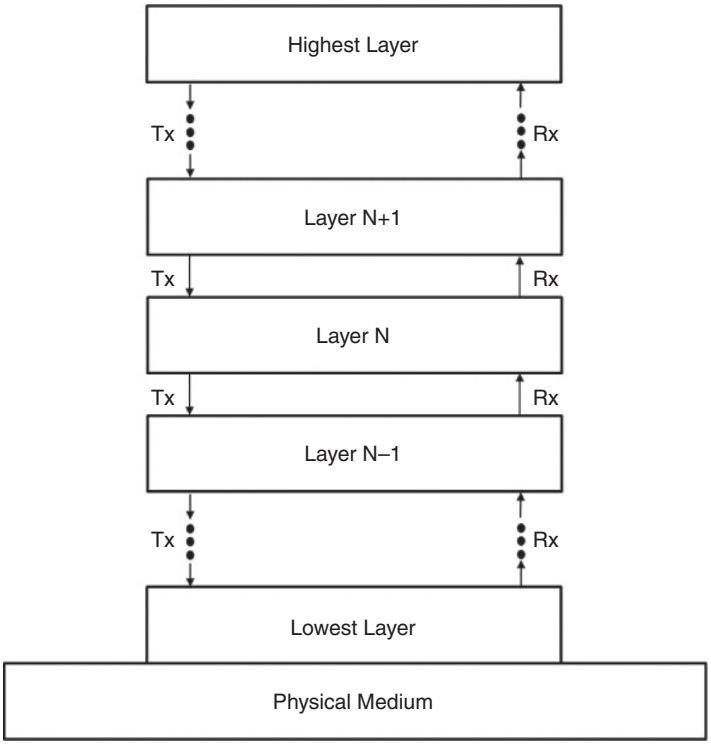

Figure 1.10 Example Protocol Stack

a natural means to decompose the various functions within a communications system.

With the basic concept of a protocol stack in mind, two of the most famous protocol stacks will now be discussed. Those are the Open Systems Interconnection reference model and the TCP/IP reference model.

1.5.1 The Open Systems Interconnection Reference Model

One of the most common protocol stacks used as a template for layered design is arguably the seven-layer Open Systems Interconnection (OSI) reference model defined by the International Standardization Organization (ISO) [14]. The seven-layer OSI model is illustrated in Figure 1.11. This stack is often used as a guide to understanding other protocol stacks.

Each layer in the seven layer OSI reference model has a specific function:

- Application: This is the process that is ultimately producing and consuming data.

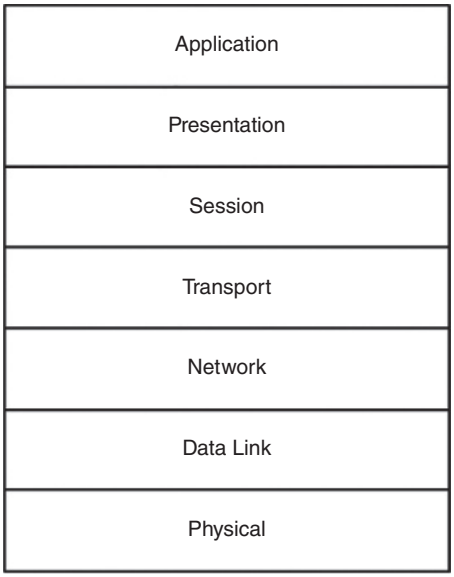

Figure 1.11 Seven-Layer OSI Reference Model

- Presentation: Provides independence to application processes by structuring the data.
- Session: Provides control and synchronization between application processes communicating across the network (e.g., starting a "session," ending a "session").
- Transport: Packetizes the data, sequences the data, and handles connection-oriented or connectionless delivery.
- Network: Routes the data across the network.
- Data Link: Controls access to the physical medium. Corrects for errors in received data.
- Physical: Transmits and receives data across the physical medium.

1.5.2 The TCP/IP Reference Model

The TCP/IP reference model is the stack upon which the Internet rests. While the OSI reference model is popular for academic study or a common point of reference to compare other protocol stacks, it has not gained popularity in actual implementation. The OSI reference model and the "TCP/IP" reference model were competing protocol stacks for what was to become the Internet [15,16]. To summarize the result of years of publications and debate, the TCP/IP model won.

The TCP/IP reference model is illustrated in Figure 1.12 [17]. The corresponding layers in System A and System B interact by way of transmitting data through the lower layers and processing data received from the lower layers.

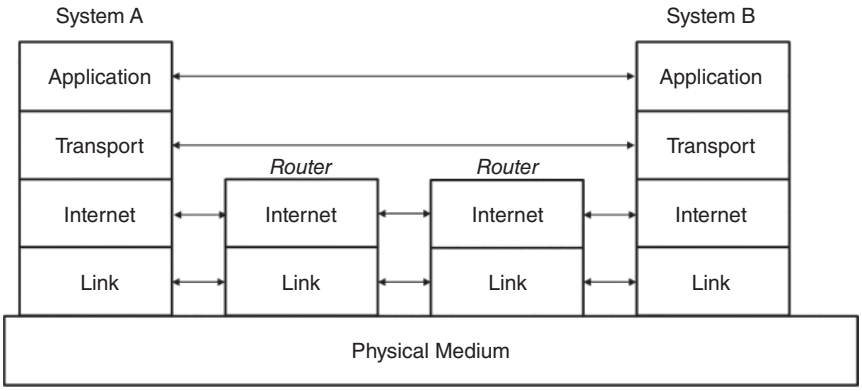

Figure 1.12 TCP/IP with Routers

Routers in the network between System A and System B are represented by the two partial stacks. The routers do not need to parse the whole stack, only enough to route packets between System A and System B.

Each layer in the TCP/IP four-layer stack has a specific function:

- Application: This is the process that is ultimately producing and consuming data.
- Transport: Packetizes the data, sequences the data, and handles connection-oriented or connectionless delivery.
- Internet: Routes the data across the network.
- Link: Controls access to the physical medium. Corrects for errors in received data. Transmits and receives data across the physical medium.

The layers of the TCP/IP reference model and the layers of the OSI reference model can be mapped as shown in Figure 1.13. As can be seen, the TCP/IP reference model is much simpler than the OSI reference model. Functions placed by the OSI reference model into the Presentation and Session layers are left solely to the Application layer in the TCP/IP reference model.

Figure 1.13 demonstrates that there are functions common between ostensibly different designs of protocol stacks. These stacks can often be mapped or translated between one another. The fact that mapping is often possible provides a mechanism such that concepts common to different stacks for different applications can be discussed in the abstract.

1.5.3 The IEEE 802 Reference Model

IEEE has published a family of standards for personal, local, and metropolitan area networks. These are the IEEE 802 set of standards. The protocol stack of

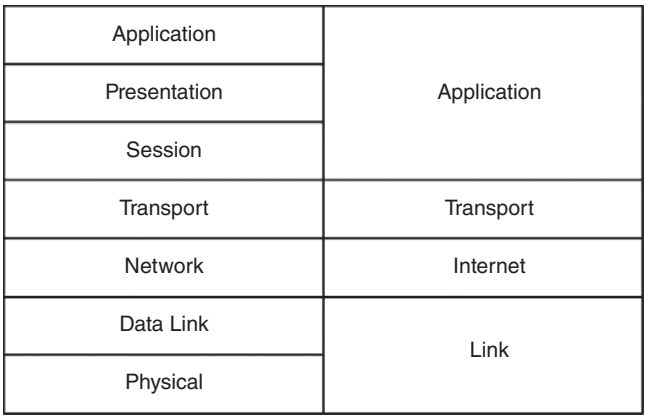

Figure 1.13 Mapping TCP/IP to OSI

the reference model for these standards is derived from the OSI model, and maps to the OSI model as shown in Figure 1.14. The IEEE 802 standards only define the physical and data link layer. The data link layer is broken into two sub layers, the Media Access sublayer and the logical link control sublayer. The definitions of the upper layers are left to other standards.

The Logical Link Control layer (LLC) for all IEEE 802 standards is defined in IEEE 802.2. The relationship between these standards is shown in Figure 1.15. Only Ethernet (802.3), 802.15.4, 802.15.1 (formerly Bluetooth), and Wi-Fi (802.11) are shown in Figure 1.15 for the sake of brevity. These various protocols share a common definition for LLC layer, that being IEEE 802.2.

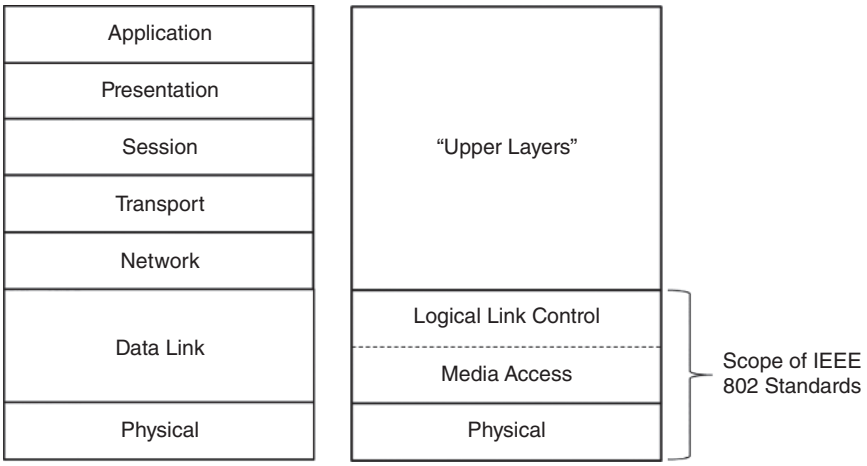

Figure 1.14 The IEEE 802 Reference Model

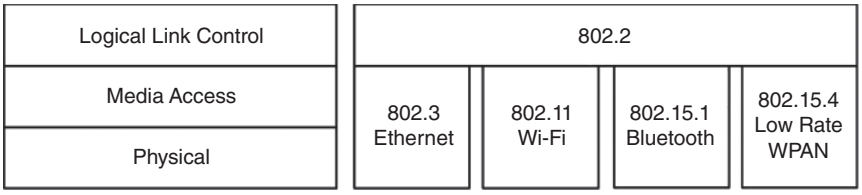

Figure 1.15 The Relationship Between IEEE 802 Standards

The physical (PHY) and media access control (MAC) layers are defined for each different standard. Therefore, the PHY and MAC deserve some special attention.

1.5.4 A Layered Model for IoT Operations

Layered models can be used to describe systems other than wireless links. Numerous articles and papers have employed layered models to describe IoT operations in the abstract. Such a layered model encompasses all of the IoT, from the small sensing device through the wireless protocol to the cloud operations. There are several different layered models employed in literature to describe the operation of the IoT. One of the most common of these is the "three-layer model" [18–20]. The "three-layer model" shall be used here for its simplicity. This model is illustrated in Figure 1.16.

The "Perception" layer is called such because this is the layer where information is gathered. This layer handles any sensor that is attached to the wireless IoT links. The data gathered could be from any source relevant to the application. The sensors could be any number of things from vibration sensors for a security system to sensors used to gather data on soil conditions for agricultural applications.

The "Network" layer handles all transportation of data. This is the layer that encapsulates much of what this book will discuss. The operation of the wireless links between sensors and network coordinators are encapsulated here. Routing between the network nodes is encapsulated here. Funneling information to a gateway and sending that information to remote servers is encapsulated here.

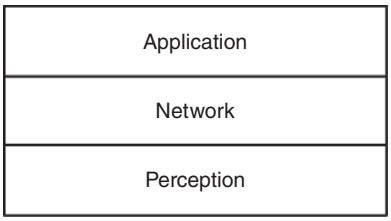

Figure 1.16 Three-Layer Model for Wireless Sensor Networks

The "Application" layer represents the desired application. This layer handles the user interface and decisions made at the top of the stack. The application is the layer that might exist in "the cloud."

The operation of the wireless link that empowers the device network is encapsulated in the "Network" layer of the model in Figure 1.16. This book will focus on that wireless interoperability.

1.6 Introduction to the Protocols for the Wireless Internet of Things

This book will delve into concepts that help define the lower layers of wireless IoT. Specific protocols that will be explored will include:

- IEEE 802.15.4,
- Bluetooth (previously standardized as IEEE 802.15.1),
- and ITU-T G.9959.

The IEEE 802.15.4 provides standards for PHY and MAC layers for low-rate wireless personal area networks. A subset of the PHY and MAC layers defined therein are used by wireless IoT protocols.

The Bluetooth standard is maintained by the Bluetooth Special Interest Group (SIG). The lower layers of Bluetooth, PHY, and MAC were once standardized as IEEE 802.15.1. Now those lower layers are maintained by the Bluetooth SIG.

ITU-T G.9959 provides a standard for the PHY and MAC layers for short range narrow-band digital radio communication transceivers. The Z-Wave protocol for the wireless IoT uses the ITU-T G.9959 standard for its lower layers. The upper layers are maintained by the Z-Wave Alliance.

Each protocol has a stack, and there are many features common to these stacks. One common theme is that the lower two layers, PHY and MAC, are maintained by neutral standards bodies whereas the upper layers are maintained by an industry group. The details of the upper layers of these wireless IoT protocols may not be free for a developer to use. A developer must check with the specific industry alliance before publishing information on those upper layers or developing solutions using those upper layers.

Wi-Fi, which follows the IEEE 802.11 standards, will also be discussed. This book focuses on the standards for low power wireless IoT protocols. Wi-Fi does not fit that criteria; therefore, a detailed discussion on Wi-Fi is beyond the scope of this book. While the focus of this book is on IoT devices and the wireless protocols between them, Wi-Fi plays an important role in the wireless IoT and some discussion is necessary.

1.7 The Approach of this Book

Chapter 2 will provide background and operational information on the protocols identified in Section 1.6. The remainder of this book will follow a layered approach to providing an in-depth analysis of the lower layers of the wireless IoT standards. To accomplish this, a hybrid model of IoT protocols stacks will be followed charting a path through the lower layers of the protocol stacks.

As will be shown in Chapter 2, the protocol stacks for the wireless IoT can be simplified to fewer layers than that shown in Section 1.5. This hypothetical stack is illustrated in Figure 1.17. There are only two layers that will be covered in this book: Physical and MAC.

The physical layer is split into two hypothetical sublayers, "Radio" and "MODEM." These two sublayers will be covered in Chapters 3 and 4, respectively.

The Radio layer will be defined as encapsulating the physical interface to the spectrum. The Radio layer chapter will cover the theory and technology behind the wireless links described in the wireless standards of interest. This will include topics such as radio hardware and channel effects.

The Modem layer will be defined as encapsulating the modulation and demodulation algorithms necessary to convert bits into waveforms and vice versa. The Modem layer chapter will cover the theory and algorithms behind the wireless standards of interest. This will include topics such as modulation, demodulation, and spread spectrum.

Chapter 5 will focus on the MAC layer. The "Media Access Control layer" (MAC) is a common name for the layer that manages and controls access to limited Physical layer resources. The OSI model considers MAC to be a "sublayer" of the larger "Data Link" layer. The standards defined under IEEE 802 also identify a MAC sublayer. Within the IEEE 802 literature, the MAC "sublayer" is sometimes referred to simply as the MAC "layer." Some other protocols, such as Z-Wave, specifically delineate a MAC layer within the standard.

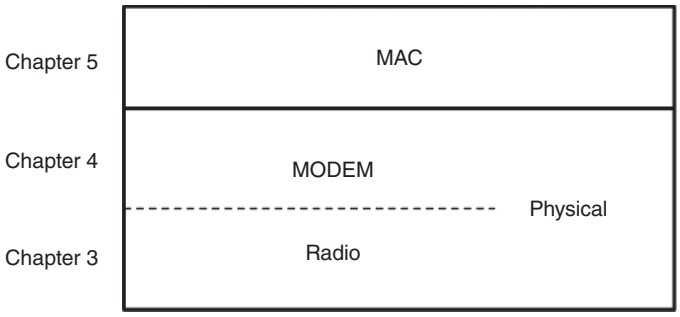

Figure 1.17 Simplified Protocol Stack

Upper layers must send data to the MAC, which then manages transmissions parameters. The MAC manages the reception of data and provides complete packets to upper layers. The MAC coordinates access with other nodes in the system. Spread spectrum techniques are typically discussed as physical layer properties. However, spread spectrum techniques do require some negotiation and coordination at higher layers.

The MAC layer is important to the wireless IoT as it controls access to the physical medium in contentious environments. This chapter will delve into the background theory necessary to understand the operation of media access control and the wireless standards specifying operations thereof. Topics will include multiple access techniques and error correction.

References

1 F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," in *From Active Data Management to Event-Based Systems and More*. Berlin, Heidelberg: Springer, 2010, pp. 242–259.
2 C. R. Schoenberger. (2002, Mar. 18). The internet of things. *Forbes* [Online]. Available: https://www.ieee.org/content/dam/ieee-org/ieee/web/org/conferences/style_references_manual.pdf
3 M. Weiser, "The computer for the 21st century," *Sci. Am.*, vol. 265, no. 9, pp. 66–75, 1991.
4 M. Weiser, R. Gold, and J. S. Brown, "The origins of ubiquitous computing research at PARC in the late 1980s," *IBM Syst. J.*, vol. 38, no. 4, pp. 693–696, 1999.
5 A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.
6 L. Yang, C. Yao, T. Nguyen, S. Gurumani, K. Rupnow, and D. Chen, "System-level design solutions: Enabling the IoT explosion," in *2015 IEEE 11th Int. Conf. ASIC (ASICON)*, Chengdu, China, Nov. 2015, pp. 1–4.
7 K. J. Singh and D. S. Kapoor, "Create your own Internet of Things: A survey of IoT platforms," *IEEE Consum. Electron. Mag.*, vol. 6, no. 2, pp. 57–68, 2017.
8 L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenge and opportunities of the Internet of Things (IoT)," in *2017 IEEE 11th Int. Conf. Sens. Technol. (ICST)*, Sydney, Australia, Dec. 2017, pp. 1–5.
9 J. Misic and V. Misic, *Wireless Personal Area Networks: Performance, Interconnections and Security with IEEE 802.15.4*. West Sussex: John Wiley & Sons Ltd., 2008.
10 A. S. Tanenbaum, *Computer Networks*. Upper Saddle River: Prentice Hall, 2003.

11 P. Johansson, M. Kazantz, and M. Gerla, "Bluetooth: An enabler for personal area networking," *IEEE Netw*., vol. 15, no. 5, pp. 28–37, 2001.
12 P. K. M. Nkwari, S. Rimer, B. S. Paul, and H. Ferreira, "Heterogeneous wireless network based on Wi-Fi and ZigBee for cattle monitoring," in *IEEE IST-Africa Conf*., Lilongwe, Malawi, May 2015, pp. 1–9.
13 M. R. Palattella, M. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) Things," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389–1406, 2013.
14 H. Zimmerman, "OSI reference model—The ISO model of architecture for open systems interconnection," *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 425–432, 1980.
15 A. L. Russell, "The internet that wasn't," *IEEE Spectr*., vol. 50, no. 8, pp. 39–43, 2013.
16 D. Meyer and G. Zobrist, "TCP/IP versus OSI," *IEEE Potentials*, vol. 9, no. 1, pp. 16–19, 1990.
17 R. Braden, "RFC1122: Requirements for Internet hosts – communication layers," The Internet Engineering Task Force, 1989.
18 L. Dan, S. Jianmei, Y. Yang, and X. Jianqiu, "Precise agricultural greenhouses based on the IoT and fuzzy control," in *IEEE Int. Conf. Intell. Transp. Big Data Smart City (ICITBS)*, Changsha, China, Dec. 2016, pp. 580–583.
19 M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *IEEE 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, Chengdu, China, Aug. 2010, pp. V5-484–V5-487.
20 M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," in *IEEE Conf. Stan. for Commun. Netw. (CSCN)*, Helsinki, Finland, Sep. 2017, pp. 246–251.