mobile communications series

NARESH GUPTA

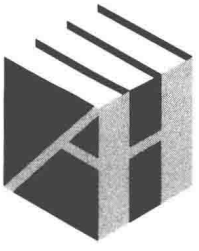
INSIDE BLUETOOTH LOW ENERGY

Second Edition

Inside Bluetooth Low Energy

Second Edition

Naresh Gupta



ARTECH
HOUSE
BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data
A catalog record for this book is available from the British Library.

ISBN-13: 978-1-63081-089-4

Cover design by John Gomes

This book is in no way affiliated with SIG. The author is writing as an individual interested in the technology.

10 9 8 7 6 5 4 3 2 1

Inside Bluetooth Low Energy

Second Edition

For a listing of recent titles in the
Artech House Mobile Communications Series,
turn to the back of this book.

To my respected parents, my dear wife, and my naughty kids.

You are always there for me, and have never doubted my dreams, no matter how crazy they may sound.

I know I stole countless hours that I should have spent with you in writing this book but you never complained...

Preface to the First Edition

The idea for writing this book was sparked by a former colleague over a cup of coffee a couple of years ago when he said, "Naresh, why don't you write a book on Bluetooth Low Energy?" At that time I brushed off that idea, saying that I was too busy in implementing Bluetooth Low Energy features and writing a book was not a piece of cake. Later that year I kept realizing that, since the technology is very new, the amount of available reading material is very limited and it's not too easy to understand the technology, especially for newbies. In the winter of 2011, I finally decided to try my hand at explaining this technology to people who were eager to understand but did not have a good starting point.

Objectives of This Book

This book covers the concepts of Bluetooth and Bluetooth Low Energy. It introduces the reader to the history of the technology, terminology, use cases, architecture, and details of how it works, along with some hands-on examples. It's not intended to cover everything down to the minute detail that is written in the Bluetooth specification because that is already done well by the specification. Rather, it's expected to be a working companion to the specification. Instead of diving directly into the full specification, the user can first understand the technology at a broad level from this book and then dive deeper into the relevant sections of the specification.

This book does not assume prior knowledge of Bluetooth or other wireless protocols, though knowing them would certainly be a plus. Most of the new terminology used in this book is also explained within this book. A lot of practical examples are provided so that the concepts can be correlated to the real-world applications. Some sample programs are also provided that can be used to gain understanding and as a starting point of a full-fledged implementation. Screenshots of air logs and message sequence charts are also provided to give a good view of how things actually work.

It will be good if the reader is familiar with the Unix or Linux operating systems to understand the sample programs provided in this book. Some basic knowledge of any scripting language would also be helpful. The commands and programs provided in this book have been written directly on the Linux shell prompt or using very basic features of Perl or C language. It's expected that these programs could be adapted easily to any other language as well.

Intended Audience

This book is meant for engineering students, software and hardware engineers, architects, and engineering and business managers.

This book serves the purpose of introducing engineering students to the concepts of Bluetooth and Bluetooth Low Energy. It helps them to understand the "what" and "how" parts, including a broad view of the technology, the various building blocks, and how they come together. It also has practical exercises to get a first-hand feel for how the technology works. Once they understand the concepts, users can dig into the specification for an in-depth understanding of their area of interest.

For software engineers, hardware engineers, and architects, this book helps them to understand the architecture of the Bluetooth Low Energy Stack and the functionality provided by each of the layers. The book also discusses the enhancements that have been made in Bluetooth Low Energy compared to previous versions of Bluetooth so that readers can appreciate why this technology leads to such huge savings in power consumption. It guides them on setting up their own system in a quick and efficient manner with inexpensive, easily available hardware, and a couple of PCs running Linux. The sample programs help users understand the "how" part of the technology. The book then builds further on the concepts by going from simple operations and programs to more complex programs that can be used as a starting point for the reader's own implementation.

For engineering and business managers, this book helps them to understand the "why" part. Why should they choose this particular technology? What does it offer them as a USP (Unique Selling Proposition)? Is it the right technology to solve their business problem? They may not have the time to dig into the deep technical intricacies of the technology before making a decision. This book aids them by quickly introducing them to the technology and providing them sufficient information to make an informed decision.

Prerequisite Knowledge

Bluetooth Low Energy is expected to be the next inflection point for Bluetooth technology and is expected to pave the way for billions of devices in the future. These devices will need software and hardware implementation, a variety of applications to realize the full potential of the devices, tools to support the implementation, tools to test the implementation, and several more building blocks. It is expected that many of the people who are implementing these building blocks would be exposed directly to Bluetooth Low Energy without having previously worked on Bluetooth.

This book does not assume prior knowledge of Bluetooth or any other wireless technology. Rather, it has a dedicated set of four chapters to explain Bluetooth technology before moving on to Bluetooth Low Energy technology. So it should serve both as a good starting point to people new to Bluetooth and a good refresher for people already familiar with Bluetooth who are seeking to understand what is new in Bluetooth Low Energy.

The book also contains several programming examples. All programs illustrated in this book have been tested on a Linux system using the BlueZ protocol

stack. BlueZ is the "official Linux Bluetooth protocol stack." Support for BlueZ can be found in many Linux distributions, and in general it is compatible with any Linux system in the market. As far as possible, these examples are written using very simple commands and scripts that can be executed with the bash shell. Some familiarity with Linux and shell commands will help the reader in understanding these programs faster.

Organization of This Book

This book is organized into five parts:

Part 1 starts with the background of wireless technologies and then introduces Bluetooth and Bluetooth Low Energy. It then illustrates some of the use case scenarios of Bluetooth Low Energy and introduces some of the competing technologies. It comprises the following chapter:

Chapter 1: Introduction

Part 2 sets the ball rolling by explaining the Bluetooth technology. It serves as a good introduction for readers who are not familiar with Bluetooth. It serves as a refresher to readers who have some familiarity with Bluetooth but not a full understanding of how it works. It may be skipped by people who are Bluetooth experts. This part explains the fundamentals of Bluetooth and the architecture. It then moves on to explaining the Bluetooth protocol stack from bottom to top, including the profiles and use cases. Practical examples, message sequence charts, and air sniffer logs have been provided to give a view of how each component works and to show how the various components work together to support end-to-end real-world scenarios. This part concludes with a practical chapter on setting up the Bluetooth development environment and step-by-step development of a Bluetooth real-world application. The application, fictitiously named Café Bluebite, illustrates how simple Bluetooth commands can be used to implement very powerful uses. It comprises the following chapters:

Chapter 2: Background of Bluetooth

Chapter 3: Bluetooth Lower Layers

Chapter 4: Bluetooth Upper Layers and Profiles

Chapter 5: Getting the Hands Wet

Part 3 focuses on the lower layers of Bluetooth Low Energy. It starts with an introduction of Bluetooth Low Energy, and then explains single- and dual-mode devices followed by some of the fundamental concepts of Bluetooth Low Energy. It moves on to explain the Bluetooth Low Energy architecture. Here again a bottom to top approach is taken and the protocol stack is explained starting from the lowest layers. During the explanation of each layer, the main enhancements (compared to Bluetooth) are explained along with how the technology leads to drastic reductions in power consumption. This part contains a good number of sequence diagrams, air sniffer captures, and examples of how the various layers work together. It comprises the following chapters:

Chapter 6: Bluetooth Low Energy—Fundamentals

Chapter 7: Physical Layer

Chapter 8: Link Layer

Chapter 9: Host Controller Interface and Commands

Part 4 focuses on the upper layers of Bluetooth Low Energy. It continues where Part 3 left off and starts with a discussion of the L2CAP layer and the main differences from the L2CAP layer of prior Bluetooth versions. Security is an important part of any wireless system and can be a major criterion behind the success or failure of any wireless technology. This part explains the Security Manager in detail and how Bluetooth helps to prevent various possible security breaches. This part moves on to explaining the concept of attributes and Attribute Protocol. Attribute Protocol provides the building blocks for profiles and services that are explained in the chapter related to Generic Attribute Profile. This part then explains the Generic Access Profile. It is one of the basic profiles in the Bluetooth world and provides services to all other profiles. Bluetooth Low Energy defines a very simple architecture for GATT-based profiles. This part explains the GATT-based profiles in detail along with an end-to-end explanation of what happens behind the scenes when a profile is active. It finally includes a chapter on how to develop basic Bluetooth Low Energy applications. This chapter starts with some basic LE operations and then goes on to discuss the development of interesting and useful programs to understand the different concepts that were explained earlier. Finally, it provides some tips and tricks on how to debug LE applications. It comprises the following chapters:

Chapter 10: Logical Link Control and Adaptation Protocol (L2CAP)

Chapter 11: Security Manager (SM)

Chapter 12: Attribute Protocol (ATT)

Chapter 13: Generic Attribute Profile (GATT)

Chapter 14: Generic Access Profile (GAP)

Chapter 15: GATT-Based Profiles

Chapter 16: Developing LE Applications

Part 5 provides an introduction to the Bluetooth testing and qualification process. It introduces the various tools that are available from the Bluetooth SIG for testing. It also gives an overview of the various events organized from time to time by the Bluetooth SIG and other organizations where engineers get an opportunity to test their implementations. Such events are very useful from an interoperability perspective to ensure that the device works seamlessly with other devices that are currently available in the market as well as with future devices. The overview of qualification helps the reader to understand the mandatory requirements that any Bluetooth device has to comply with before it can be sold in the market. It comprises the following chapter:

Chapter 17: Testing and Qualification

In addtion a complete glossary of acronyms and important terms is provided to serve as a quick reference.

Preface to the Second Edition

In the three years since the first edition of the book was published, I have received several messages from readers commenting on the book and providing excellent suggestions on how to improve it. I have also assimilated the new learning and experiences that I've had while developing innovative technology products into this new edition. Newer versions of the specifications have been ratified, which have introduced landmark changes in how this technology can be more effective and how it can address to a larger number of use-case scenarios.

The first edition of this book was based on Bluetooth Core Specifications 4.0. This second edition explains the main changes introduced by Bluetooth Core Specifications 4.1 and Bluetooth Core Specifications 4.2.

The most notable changes explained in this book are:

- The *Internet of Things (IoT)* space has been growing exponentially. The Bluetooth SIG has introduced a new profile called Internet Protocol Support Profile (IPSP), which is geared towards providing IPv6 Internet connectivity to Bluetooth devices. The Bluetooth sensors can access the Internet and send and receive messages through gateway devices like smartphones, tablets, and home routers. Chapter 15 introduces a new section that explains how this works and the key technology ingredients required from various protocol stack layers in order to make it work.
- Faster Connections: One of the radical changes brought in by specifications 4.0 was extremely short packets in order to keep the power consumption low. While this proved to be very useful, it also led to some constraints in scenarios where large amounts of data were to be transferred (i.e., in situations like uploading log files to the Internet and firmware upgrade of the devices). Most users don't upgrade the firmware frequently, but when they do, they would not expect the firmware upgrade to take several minutes. The newer versions of the specifications introduced LE Data extensions which improved the packet size by almost ten times in order to provide an effective increase in the overall data throughput. Chapter 8 explains these changes in detail.
- Enhanced Power Efficiency: New enhancements have been made to make the devices more power efficient. For example, some of the functionality (i.e., address resolution of the remote devices) has been moved to lower layers of the stack so that the upper layers need not be involved in such activities. These are also explained in Chapter 8.

- Privacy Enhancements: Privacy has always been one of the key concerns with wearable devices since tracking a wearable device (such as a watch) effectively means tracking the person wearing it. Newer enhancements have been made to enhance the privacy when wearing such devices. This is termed LE Privacy 1.2. The details are explained in Chapters 8 and 14.
- Enhanced Security: Bluetooth Core Specifications 4.2 introduced FIPS compliant encryption and an entirely new feature called LE Secure Connections, which is geared towards higher security. This provides much better security as compared to what is now termed as *LE Legacy Pairing*. This is explained at length in Chapter 11.

Acknowledgments

First and foremost, I would like to thank my former colleagues at ST-Ericsson. It was a great opportunity to learn, experiment, and innovate during almost 9 years with ST-Ericsson. Along with my team members, I would like to thank my former supervisors, Davy Jacops and Dr. Aloknath De. Under their able guidance I was able to grow my team from a handful of people to a reasonably large team working on the latest evolutions in various connectivity areas.

I would like to thank my former colleague Balvinder Pal Singh for being a critical reviewer of my work. His eye for detail and out-of-the-box thinking always amazed me. He gave several excellent suggestions to make this book much more useful to newbies as well as Bluetooth experts.

Next, I would like to thank Frontline, in particular Tomas O'Raghallaigh, for allowing me to use the screenshots captured from the Frontline ComProbe Protocol Analysis System software and sharing some of the sample air logs for Bluetooth transactions. Information about Frontline products related to Bluetooth Low Energy may be found at http://www.fte.com/lowenergy.

I would also like to thank Artech House for their support during the whole process. Special thanks to Aileen Storry for constantly reminding me of the schedule and responding so promptly to my e-mails.

On the personal side, I would like to thank Ekta, my wife, for her unwavering support. Almost all my weekends and vacation time for more than a year went into writing, rewriting, revising, and then re-revising the book. She was always understanding and the one who would quietly set the 4:00 AM alarm without telling me so that I could finish the book as soon as possible. She was also the one who motivated and supported me while writing the second edtion of the book after looking at the response that the first edition has received.

Thanks as well to Vishesh and Twinkle. I never realized before I started this book that they have grown old enough to actually edit and put final touches to some of the figures in this book. Thanks to them, I had to spend less time on refining the figures and could focus on getting the material organized. Thanks as well to sweet little Onashi for not pressing the only button on my laptop that she likes—the shutdown button. Next, I would like to thank my mother, Ms. Saroj Gupta, for making me who I am today. She was the one who encouraged me to think big, take on new challenges in life, and then work sincerely towards achieving them.

My father, Mr. A. K. Gupta, is an avid computer and Bluetooth user but not a wireless expert. For him technologies like Bluetooth should just work intuitively without knowing the technical jargon. He read the book cover-to-cover several times. He helped me to add sufficient background information for people new to wireless technologies and Bluetooth to help them understand the technical jargon and what is happening behind the scenes when they trigger a Bluetooth operation. I would like to thank my father for his very useful comments on how to make this book more readable and understandable for all.

Special thanks to my late father-in-law, Mr. Uttam Prakash Gupta. The most imporant value that I learned from him was about giving back to society. He devoted his entire life to the betterment of society and saving the lives of thousands of living beings. This book is my attempt to give something back to society.

Foreword to the First Edition

Bluetooth (BT) technology has become all-pervasive, with attach rates close to one hundred percent for mobiles and laptops. Bluetooth Low Energy (BLE) is the next growth area that leverages on the success of BT but caters to the applications where frequent battery charging is not an option. The lower power consumption in BLE is not achieved by the nature of the active radio transport, but by the design of the protocol to allow low duty cycles with burst transmission and by the use cases envisaged.

Many features of classic BT are inherited in BLE technology, including the broad architecture of the protocol stack. Data transfer rates for BLE technology are below 100 kbps, and also many profiles (including object exchange and audio/video distribution) are not offered in BLE in order to keep the power consumptions low. On the positive side, a master device could support a large number of slave devices, and the connection setup is pretty fast. Because a BLE device is in sleep mode the majority of the time and the communication is "bursty," the average power consumption is reduced to significantly low levels.

This book unravels the beauty and subtlety of BLE technology and contrasts this technology vis-a-vis classic BT technology. Naresh has been working on BT and short-range connectivity area for close to ten years; his vast developmental experience has a footprint throughout the book. He has a focused approach in discussing BLE profiles, ATT, GATT, GAP, security aspects, HCI commands, development tools, and debugging and testing mechanisms. At the same time, he has captured well the BLE architectural aspects and reference design relating to standard specifications.

The book serves as a practical guide to promising BLE technology that is well-suited for sensors, actuators, and other small devices with ultra low power consumption. BT 4.0 with low energy technique paves the way for BT connected devices and the Internet of Things. Opening a garage wirelessly, receiving alerts to watch for incoming calls, or finding lost keys (and even cats)—any of these applications could easily be built with BLE technology. The book provides many such application examples and the underlying working principles so that practicing engineers could learn how to build innovative applications on BT-smart and smart-ready devices.

It has been a pleasure for me to pen this foreword to this book on BLE authored by Naresh. This is particularly so, as I hired Naresh to build the Bluetooth team, and the team increased both in mandate and strength under my guidance in ST-Ericsson, where I was serving as Country Director until recently. Naresh and his colleagues have filed three patents from their inventive work. A good deal of this material has also been presented as classroom lectures to Masters degree students at Jaypee University, as well as at the Indian Institute of Technology-Delhi, where I served as Adjunct Professor. I sincerely believe that this timely book will immensely help students and engineers alike to get a holistic view of this promising technology.

Aloknath De, Ph.D.
Fellow-Indian National Academy of Engineering