



BLUETOOTH LOW ENERGY

THE DEVELOPER'S HANDBOOK

ROBIN HEYDON

Bluetooth Low Energy

Bluetooth Low Energy: The Developer's Handbook

Table of Contents

Cover

Half Title

Title Page

Copyright Page

Contents

Preface

Acknowledgments

About the Author

Part I: Overview

Chapter 1 What Is Bluetooth Low Energy?

1.1 Device Types

1.2 Design Goals

1.3 Terminology

Chapter 2 Basic Concepts

2.1 Button-Cell Batteries

2.2 Time Is Energy

2.3 Memory Is Expensive

2.4 Asymmetric Design

2.5 Design For Success

2.6 Everything Has State

2.7 Client-Server Architecture

2.8 Modular Architecture

Table of Contents

2.9 One Billion Is a Small Number

2.10 Connectionless Model

2.11 Paradigms

2.11.1 Client-Server Architecture

2.11.2 Service-Oriented Architecture

Chapter 3 Architecture

3.1 Controller

3.1.1 Physical Layer

3.1.2 Direct Test Mode

3.1.3 Link Layer

3.1.4 The Host/Controller Interface

3.2 The Host

3.2.1 Logical Link Control and Adaptation Protocol

3.2.2 The Security Manager Protocol

3.2.3 The Attribute Protocol

3.2.4 The Generic Attribute Profile

3.2.5 The Generic Access Profile

3.3 The Application Layer

3.3.1 Characteristics

3.3.2 Services

3.3.3 Profiles

3.4 Stack Splits

3.4.1 Single-Chip Solutions

3.4.2 Two-Chip Solutions

3.4.3 Three-Chip Solutions

Chapter 4 New Usage Models

4.1 Presence Detection

4.2 Broadcasting Data

4.3 Connectionless Model

4.4 Gateways

Part II: Controller

Table of Contents

Chapter 5 The Physical Layer

- 5.1 Background
- 5.2 Analog Modulation
- 5.3 Digital Modulation
- 5.4 Frequency Band
- 5.5 Modulation
- 5.6 Radio Channels
- 5.7 Transmit Power
- 5.8 Tolerance
- 5.9 Receiver Sensitivity
- 5.10 Range

Chapter 6 Direct Test Mode

- 6.1 Background
- 6.2 Transceiver Testing
 - 6.2.1 Test Packet Format
 - 6.2.2 Transmitter Tests
 - 6.2.3 Receiver Tests
- 6.3 Hardware Interface
 - 6.3.1 UART
 - 6.3.2 Commands and Events
- 6.4 Direct Testing by Using HCI

Chapter 7 The Link Layer

- 7.1 The Link Layer State Machine
 - 7.1.1 The Standby State
 - 7.1.2 The Advertising State
 - 7.1.3 The Scanning State
 - 7.1.4 The Initiating State
 - 7.1.5 The Connection State
 - 7.1.6 Multiple State Machines
- 7.2 Packets
 - 7.2.1 Advertising and Data Packets

Table of Contents

7.2.2 Whitening

7.3 Packet Structure

7.3.1 Bit Order and Bytes

7.3.2 The Preamble

7.3.3 Access Address

7.3.4 Header

7.3.5 Length

7.3.6 Payload

7.3.7 Cyclic Redundancy Check

7.4 Channels

7.4.1 Frequency Hopping

7.4.2 Adaptive Frequency Hopping

7.5 Finding Devices

7.5.1 General Advertising

7.5.2 Direct Advertising

7.5.3 Nonconnectable Advertising

7.5.4 Discoverable Advertising

7.6 Broadcasting

7.7 Creating Connections

7.7.1 Access Address

7.7.2 CRC Initialization

7.7.3 Transmit Window

7.7.4 Connection Events

7.7.5 Channel Map

7.7.6 Sleep Clock Accuracy

7.8 Sending Data

7.8.1 Data Header

7.8.2 Logical Link Identifier

7.8.3 Sequence Numbers

7.8.4 Acknowledgement

7.8.5 More Data

7.8.6 Examples of the Use of Sequence Numbers and More Data

7.9 Encryption

Table of Contents

7.9.1 AES

7.9.2 Encrypting Payload Data

7.9.3 Message Integrity Check

7.10 Managing Connections

7.10.1 Connection Parameter Update

7.10.2 Adaptive Frequency Hopping

7.10.3 Starting Encryption

7.10.4 Restarting Encryption

7.10.5 Version Exchange

7.10.6 Feature Exchange

7.10.7 Terminating Connections

7.11 Robustness

7.11.1 Adaptive Frequency Hopping

7.11.2 Strong CRCs

7.12 Optimizations for Low Power

7.12.1 Short Packets

7.12.2 High Bit Rate

7.12.3 Low Overhead

7.12.4 Acknowledgement Scheme

7.12.5 Single-Channel Connection Events

7.12.6 Subrating Connection Events

7.12.7 Offline Encryption

Chapter 8 The Host/Controller Interface

8.1 Introduction

8.2 Physical Interfaces

8.2.1 UART

8.2.2 3-Wire UART

8.2.3 USB

8.2.4 SDIO

8.3 Logical Interface

8.3.1 HCI Channels

8.3.2 Command Packets

8.3.3 Event Packets

Table of Contents

8.3.4 Data Packets

8.3.5 Command Flow Control

8.3.6 Data Flow Control

8.4 Controller Setup

8.4.1 Reset the Controller to a Known State

8.4.2 Reading the Device Address

8.4.3 Set Event Masks

8.4.4 Read Buffer Sizes

8.4.5 Read Supported Features

8.4.6 Read Supported States

8.4.7 Random Numbers

8.4.8 Encrypting Data

8.4.9 Set Random Address

8.4.10 White Lists

8.5 Broadcasting and Observing

8.5.1 Advertising

8.5.2 Passive Scanning

8.5.3 Active Scanning

8.6 Initiating Connections

8.6.1 Initiating Connection to White List

8.6.2 Initiating a Connection to a Device

8.6.3 Canceling Initiating a Connection

8.7 Connection Management

8.7.1 Connection Update

8.7.2 Channel Map Update

8.7.3 Feature Exchange

8.7.4 Version Exchange

8.7.5 Starting Encryption

8.7.6 Restarting Encryption

8.7.7 Terminating a Connection

Part III: Host

Chapter 9 Logical Link Control and Adaptation Protocol

Table of Contents

9.1 Background

9.2 L2CAP Channels

9.3 The L2CAP Packet Structure

9.4 The LE Signaling Channel

9.4.1 Command Reject

9.4.2 Connection Parameter Update Request and Response

Chapter 10 Attributes

10.1 Background

10.1.1 Protocol Proliferation Is Wrong

10.1.2 Data, Data, Everywhere

10.1.3 Data and State

10.1.4 Kinds of State

10.1.5 State Machines

10.1.6 Services and Profiles

10.2 Attributes

10.2.1 Attribute

10.2.2 The Attribute Handle

10.2.3 Attribute Type

10.2.4 Attribute Value

10.2.5 Databases, Servers, and Clients

10.2.6 Attribute Permissions

10.2.7 Accessing Attributes

10.2.8 Atomic Operations and Transactions

10.3 Grouping

10.4 Services

10.4.1 Extending Services

10.4.2 Reusing Another Service

10.4.3 Combining Services

10.4.4 Primary or Secondary

10.4.5 Plug-and-Play Client Applications

10.4.6 Service Declaration

10.4.7 Including Services

Table of Contents

10.5 Characteristics

10.5.1 Characteristic Declaration

10.5.2 Characteristic Value

10.5.3 Descriptors

10.6 The Attribute Protocol

10.6.1 Protocol Messages

10.6.2 The Exchange MTU Request

10.6.3 The Find Information Request

10.6.4 The Find By Type Value Request

10.6.5 The Read By Type Request

10.6.6 The Read Request

10.6.7 The Read Blob Request

10.6.8 The Read Multiple Request

10.6.9 The Read By Group Type Request

10.6.10 The Write Request

10.6.11 The Write Command

10.6.12 The Signed Write Command

10.6.13 The Prepare Write Request and Execute Write Request

10.6.14 The Handle Value Notification

10.6.15 The Handle Value Indication

10.6.16 Error Response

10.7 The Generic Attribute Profile

10.7.1 The Discovery Procedures

10.7.2 The Discovering Services

10.7.3 Characteristic Discovery

10.7.4 Client-Initiated Procedures

10.7.5 Server-Initiated Procedures

10.7.6 Mapping ATT PDUs to GATT Procedures

Chapter 11 Security

11.1 Security Concepts

11.1.1 Authentication

11.1.2 Authorization

11.1.3 Integrity

Table of Contents

- 11.1.4 Confidentiality
- 11.1.5 Privacy
- 11.1.6 Encryption Engine
- 11.1.7 Shared Secrets

11.2 Pairing and Bonding

- 11.2.1 Pairing
- 11.2.2 Exchange of Pairing Information
- 11.2.3 Authentication
- 11.2.4 Key Distribution
- 11.2.5 Bonding

11.3 Signing of Data

Chapter 12 The Generic Access Profile

12.1 Background

- 12.1.1 Initial Discovery
- 12.1.2 Establishing the Initial Connection
- 12.1.3 Service Characterization
- 12.1.5 Reconnections
- 12.1.4 Long-Term Relationships
- 12.1.6 Private Addresses

12.2 GAP Roles

12.3 Modes and Procedures

- 12.3.1 Broadcast Mode and Observation Procedure
- 12.3.2 Discoverability
- 12.3.3 Connectability
- 12.3.4 Bonding

12.4 Security Modes

- 12.4.1 Security Modes

12.5 Advertising Data

- 12.5.1 Flags
- 12.5.2 Service
- 12.5.3 Local Name
- 12.5.4 TX Power Level

Table of Contents

12.5.5 Slave Connection Interval Range

12.5.6 Service Solicitation

12.5.7 Service Data

12.5.8 Manufacturer-Specific Data

12.6 GAP Service

12.6.1 The Device Name Characteristic

12.6.2 The Appearance Characteristic

12.6.3 The Peripheral Privacy Flag

12.6.4 Reconnection Address

12.6.5 Peripheral Preferred Connection Parameters

Part IV: Application

Chapter 13 Central

13.1 Background

13.2 Discovering Devices

13.3 Connecting to Devices

13.4 What Does This Device Do?

13.5 Generic Clients

13.6 Interacting with Services

13.6.1 Readable Characteristics

13.6.2 Control Points

13.6.3 State Machines

13.6.4 Notifications and Indications

13.7 Bonding

13.8 Changed Services

13.9 Implementing Profiles

13.9.1 Defining a Profile

13.9.2 Finding Services

13.9.3 Finding Characteristics

13.9.4 Using Characteristics

13.9.5 Profile Security

Chapter 14 Peripherals

Table of Contents

- 14.1 Background
- 14.2 Broadcast Only
- 14.3 Being Discoverable
- 14.4 Being Connectable
- 14.5 Exposing Services
- 14.6 Characteristics
- 14.7 Security Matters
- 14.8 Optimizing for Low Power
 - 14.8.1 Discoverable Advertising
 - 14.8.2 Bonding
 - 14.8.3 Connectable Advertising
 - 14.8.4 Directed Advertising
 - 14.8.5 Connected
 - 14.8.6 Stay Connected or Disconnect
- 14.9 Optimizing Attributes

Chapter 15 Testing and Qualification

- 15.1 Starting a Project
- 15.2 Selecting Features
- 15.3 Consistency Check
- 15.4 Generating a Test Plan
- 15.5 Creating a Compliance Folder
- 15.6 Qualification Testing
- 15.7 Qualify Your Design
- 15.8 Declaring Compliance
- 15.9 Listing
- 15.10 Combining Components

Index