Inside Bluetooth Low Energy

Naresh Gupta
CHAPTER 1

Introduction

1.1 Introduction to Wireless Communication

1.2 Data Rates and Coverage
   1.2.1 Wide Area Network
   1.2.2 Metropolitan Area Network
   1.2.3 Local Area Network
   1.2.4 Personal Area Network
   1.2.5 Body Area Network

1.3 Why Have Standards?

1.4 Introduction to Bluetooth and Bluetooth Low Energy

1.5 Applications
   1.5.1 Finding and Alerting Devices
   1.5.2 Proximity and Presence Detection
   1.5.3 Health Care
   1.5.4 Sports and Fitness Equipment
   1.5.5 Mobile Payments

1.6 Competing Technologies
   1.6.1 ANT and ANT+
   1.6.2 ZigBee
   1.6.3 Near Field Communication (NFC)

1.7 Summary

References

CHAPTER 2

Background of Bluetooth

2.1 Introduction

2.2 Ad Hoc Networks—Why?
   2.2.1 Printing Documents, Photos
   2.2.2 Exchanging Business Cards, Photos, Music, Files
# Contents

2.3  What is Bluetooth?  
2.4  Bluetooth SIG  
2.5  History of the Bluetooth Specification  
2.6  IEEE 802.15 Family of Specifications  
2.7  Bluetooth Basics  
2.8  Bluetooth Architecture Overview  
2.9  Basic Terminology  
  2.9.1  Host, Host Controller, and Host Controller Interface (HCI)  
  2.9.2  Device Address (BD_ADDR) and Device Name  
  2.9.3  Class of Device (CoD)  
  2.9.4  Bluetooth Clock  
  2.9.5  Protocol Data Unit (PDU)  
2.10  Data Rates  
2.11  Connection Setup and Topology  
2.12  IEEE Word Usage  
2.13  Summary  

References

---

# Chapter 3

Bluetooth Lower Layers  

3.1  Introduction  

3.2  Bluetooth Radio  
  3.2.1  Frequency Band and Hopping  

3.3  Baseband Controller  
  3.3.1  Topology—Piconet and Scatternet  
  3.3.2  Time Division Duplex  
  3.3.3  Adaptive Frequency Hopping (AFH)  
  3.3.4  Master, Slave Roles and Role Switch  
  3.3.5  Channel, Transport and Links  
  3.3.6  Packet Format  
  3.3.7  Packet Types  
  3.3.8  Link Controller States  

3.4  Link Manager (LM)  
  3.4.1  Connection Control  
  3.4.2  Security  

3.5  Host Controller Interface (HCI)  
  3.5.1  HCI Packet Types  
  3.5.2  HCI Commands and Events  
  3.5.3  Buffers  
  3.5.4  HCI Flow Control  
  3.5.5  Connection Handle  
  3.5.6  HCI Transport Layer  

3.6  Security—Secure Simple Pairing (SSP)  
  3.6.1  Passive Eavesdropping Protection  
  3.6.2  Man-in-the-Middle (MITM) Attack Protection  
  3.6.3  Association Models
CHAPTER 6
Bluetooth Low Energy—Fundamentals

6.1 Introduction
6.2 Single Mode versus Dual Mode Devices
6.3 Bluetooth Smart Marks
   6.3.1 Bluetooth Smart (Sensor-Type Devices)
   6.3.2 Bluetooth Smart Ready (Hubs)
6.4 LE Fundamentals
   6.4.1 Frequency Bands
   6.4.2 Mostly Off Technology
   6.4.3 Faster Connections
   6.4.4 Reduced Functionality
   6.4.5 Shorter Packets
   6.4.6 Reduced Dynamic Memory Footprint
   6.4.7 Optimized Power Consumption of Peripherals
   6.4.8 No Need for Continuous Polling
   6.4.9 Backward Compatibility With BR/EDR
6.5 LE Architecture
6.6 Comparison between BR/EDR and LE
6.7 Summary
   Bibliography

CHAPTER 7
Physical Layer

7.1 Introduction
7.2 Frequency Bands
7.3 Transmitter Only, Receiver Only, or Both
7.4 Output Power
7.5 Range
7.6 Modulation Characteristics
7.7 LE Timeline
7.8 Summary
   Bibliography
CHAPTER 8
Link Layer 151
8.1 Introduction 151
8.2 Overview of Link Layer States 151
  8.2.1 Standby State 151
  8.2.2 Advertising State (Advertiser) 152
  8.2.3 Scanning State (Scanner) 153
  8.2.4 Initiating State (Initiator) 153
  8.2.5 Connection State (Master or Slave) 153
8.3 Device Address 153
  8.3.1 Public Device Address 153
  8.3.2 Random Address 154
8.4 Physical Channel 154
8.5 Channel Map 156
8.6 Adaptive Frequency Hopping 156
8.7 Events 157
  8.7.1 Advertising Events 157
  8.7.2 Connection Events 158
8.8 Topology 159
8.9 Packet Format 160
  8.9.1 Preamble 161
  8.9.2 Access Address 161
  8.9.3 CRC 161
  8.9.4 PDU 161
8.10 Bit Stream Processing 165
8.11 Link Layer States 166
  8.11.1 Nonconnected States 167
  8.11.2 Connection State 173
8.12 Link Layer Control Procedures 176
  8.12.1 Connection Update Procedure 176
  8.12.2 Channel Map Update Procedure 177
  8.12.3 Encryption Procedure 178
  8.12.4 Feature Exchange Procedure 180
  8.12.5 Version Exchange Procedure 180
  8.12.6 Termination Procedure 181
  8.12.7 Device Filtering and White List 181
8.13 Practical Examples 183
8.14 Summary 183
  Bibliography 184

CHAPTER 9
Host Controller Interface and Commands 185
9.1 Introduction 185
  9.1.1 HCI Packet Types 186
  9.1.2 HCI Command Packets 186
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Subject</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.3</td>
<td>HCI Event Packet</td>
<td>186</td>
</tr>
<tr>
<td>9.1.4</td>
<td>HCI ACL Data Packet</td>
<td>186</td>
</tr>
<tr>
<td>9.2</td>
<td>HCI Commands and Events</td>
<td>187</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Device Setup</td>
<td>189</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Controller Flow Control</td>
<td>189</td>
</tr>
<tr>
<td>9.2.3</td>
<td>Host Flow Control</td>
<td>191</td>
</tr>
<tr>
<td>9.2.4</td>
<td>Controller Information</td>
<td>191</td>
</tr>
<tr>
<td>9.2.5</td>
<td>Remote Information</td>
<td>192</td>
</tr>
<tr>
<td>9.2.6</td>
<td>Controller Configuration</td>
<td>192</td>
</tr>
<tr>
<td>9.2.7</td>
<td>Device Discovery</td>
<td>193</td>
</tr>
<tr>
<td>9.2.8</td>
<td>Connection Setup</td>
<td>193</td>
</tr>
<tr>
<td>9.2.9</td>
<td>Connection State</td>
<td>193</td>
</tr>
<tr>
<td>9.2.10</td>
<td>Physical Links</td>
<td>194</td>
</tr>
<tr>
<td>9.2.11</td>
<td>Link Information</td>
<td>194</td>
</tr>
<tr>
<td>9.2.12</td>
<td>Authentication and Encryption</td>
<td>194</td>
</tr>
<tr>
<td>9.2.13</td>
<td>Testing</td>
<td>195</td>
</tr>
<tr>
<td>9.2.14</td>
<td>Usage of White Lists</td>
<td>195</td>
</tr>
<tr>
<td>9.3</td>
<td>Practical Sequence Diagrams</td>
<td>196</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Passive Scanning</td>
<td>197</td>
</tr>
<tr>
<td>9.3.2</td>
<td>Typical Sequence for Active Scanning</td>
<td>197</td>
</tr>
<tr>
<td>9.3.3</td>
<td>Connection Establishment</td>
<td>198</td>
</tr>
<tr>
<td>9.3.4</td>
<td>Setting up White list</td>
<td>198</td>
</tr>
<tr>
<td>9.4</td>
<td>Summary</td>
<td>199</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>199</td>
</tr>
<tr>
<td><strong>10.1</strong></td>
<td>Logical Link Control and Adaptation Protocol (L2CAP)</td>
<td>201</td>
</tr>
<tr>
<td>10.1</td>
<td>Introduction</td>
<td>201</td>
</tr>
<tr>
<td>10.2</td>
<td>PDU and SDU</td>
<td>201</td>
</tr>
<tr>
<td>10.3</td>
<td>Basic Assumptions</td>
<td>202</td>
</tr>
<tr>
<td>10.4</td>
<td>Maximum Transmission Unit (MTU)</td>
<td>202</td>
</tr>
<tr>
<td>10.5</td>
<td>L2CAP Features</td>
<td>203</td>
</tr>
<tr>
<td>10.5.1</td>
<td>Fixed Channel Identifiers</td>
<td>203</td>
</tr>
<tr>
<td>10.5.2</td>
<td>Fragmentation and Defragmentation of Data</td>
<td>204</td>
</tr>
<tr>
<td>10.5.3</td>
<td>Channel Multiplexing</td>
<td>204</td>
</tr>
<tr>
<td>10.6</td>
<td>Data Packets</td>
<td>205</td>
</tr>
<tr>
<td>10.7</td>
<td>L2CAP Parameters</td>
<td>205</td>
</tr>
<tr>
<td>10.8</td>
<td>L2CAP Signaling</td>
<td>206</td>
</tr>
<tr>
<td>10.8.1</td>
<td>Command Reject</td>
<td>207</td>
</tr>
<tr>
<td>10.8.2</td>
<td>Connection Parameter Update Request</td>
<td>207</td>
</tr>
<tr>
<td>10.8.3</td>
<td>Connection Parameter Update Response</td>
<td>207</td>
</tr>
<tr>
<td>10.9</td>
<td>Practical Examples</td>
<td>208</td>
</tr>
<tr>
<td>10.10</td>
<td>Summary</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>209</td>
</tr>
</tbody>
</table>
CHAPTER 11

Security Manager (SM) 211

11.1 Introduction 211
11.2 Security in Host Instead of Controller 211
11.3 Asymmetrical Architecture 212
11.4 Security Breaches 212
  11.4.1 Passive Eavesdropping 212
  11.4.2 MITM (Active Eavesdropping) 213
  11.4.3 Tracking 214
11.5 Pairing Methods 214
  11.5.1 Just Works 214
  11.5.2 Passkey Entry 214
  11.5.3 Out of Band 215
11.6 Security Properties 215
  11.6.1 Authenticated MITM Protection 215
  11.6.2 Unauthenticated no MITM Protection 215
  11.6.3 No Security 216
11.7 Cryptographic Functions 216
  11.7.1 Security Function e 216
  11.7.2 Random Address Function ah 216
  11.7.3 Confirm Value Generation Function c1 216
  11.7.4 Key Generation Function s1 216
11.8 Pairing 217
  11.8.1 Phase 1: Pairing Feature Exchange 217
  11.8.2 Phase 2: Short Term Key (STK) Generation 219
  11.8.3 Phase 3: Transport Specific Key Distribution 220
11.9 Security Manager Protocol 222
  11.9.1 Commands Used During Phase 1 (Pairing Feature Exchange) 222
  11.9.2 Commands Used During Phase 2 (STK Generation) 224
  11.9.3 Commands Used During Phase 3 (Transport Specific Key Distribution) 226
11.10 Practical Examples 227
11.11 Summary 230

Bibliography 231

CHAPTER 12

Attribute Protocol (ATT) 233

12.1 Introduction 233
12.2 Attribute 233
  12.2.1 Attribute Type 234
  12.2.2 Attribute Handle 235
  12.2.3 Attribute Permissions 235
  12.2.4 Attribute Value 236
  12.2.5 Control Point Attributes 236
12.2.6 Grouping of Attribute Handles 237
12.2.7 Atomic Operations 237
12.3 Attribute Protocol 237
12.3.1 PDU Format 238
12.3.2 Sequential Transactions 239
12.4 Methods 240
12.4.1 Request and Response Type Methods 240
12.4.2 Command Type Methods 250
12.4.3 Notification Type Methods 252
12.4.4 Indication and Confirmation Type Methods 252
12.5 Practical Examples 253
12.5.1 Exchange MTU 253
12.5.2 Reading Primary Services of a Device 254
12.6 Summary 257
Bibliography 258

CHAPTER 13
Generic Attribute Profile (GATT) 259
13.1 Introduction 259
13.1.1 Profile Dependencies 260
13.1.2 GATT-Based Profile Architecture 261
13.2 Roles 266
13.3 Attributes 267
13.3.1 Attribute Caching 269
13.3.2 Attribute Grouping 270
13.3.3 Notification and Indication 270
13.4 Service Definition 271
13.4.1 Service Declaration 271
13.4.2 Include Definition 271
13.4.3 Characteristic Definition 271
13.5 Configured Broadcast 275
13.6 GATT Features 275
13.6.1 Server Configuration 275
13.6.2 Primary Service Discovery 276
13.6.3 Relationship Discovery 280
13.6.4 Characteristic Discovery 281
13.6.5 Characteristic Descriptor Discovery 286
13.6.6 Characteristic Value Read 288
13.6.7 Characteristic Value Write 292
13.6.8 Characteristic Value Notification 297
13.6.9 Characteristic Value Indication 297
13.6.10 Characteristic Descriptors 298
13.7 Timeouts 301
13.8 GATT Service 301
13.8.1 Service Changed Characteristic 302
13.9 Security Considerations 304
   13.9.1 Authentication and Authorization Requirements 304
13.10 Summary 304
Bibliography 304

CHAPTER 14

Generic Access Profile 305
14.1 Introduction 305
14.2 Roles 306
   14.2.1 Broadcaster Role 306
   14.2.2 Observer Role 306
   14.2.3 Peripheral Role 306
   14.2.4 Central Role 307
14.3 Representation of Bluetooth Parameters 307
   14.3.1 Bluetooth Device Address 307
   14.3.2 Bluetooth Device Name 308
   14.3.3 Bluetooth Passkey 308
   14.3.4 Bluetooth Class of Device 308
   14.3.5 Pairing—Authentication and Bonding 308
14.4 Advertising and Scan Response Data Format 309
   14.4.1 Local Name (AD Type = 0x08 or 0x09) 310
   14.4.2 Flags (AD Type = 0x01) 310
   14.4.3 Manufacturer Specific Data (AD Type = 0xFF) 310
14.5 GAP Characteristics 311
   14.5.1 Device Name Characteristic 311
   14.5.2 Appearance Characteristic 312
   14.5.3 Peripheral Privacy Flag Characteristic 313
   14.5.4 Reconnection Address Characteristic 313
   14.5.5 Peripheral Preferred Connection Parameters Characteristic 314
14.6 Operational Modes and Procedures 315
   14.6.1 Broadcast Mode and Observation Procedure 315
   14.6.2 Discovery Modes and Procedures 316
   14.6.3 Connection Modes and Procedures 319
   14.6.4 Bonding Modes and Procedures 325
14.7 Security 327
   14.7.1 LE Security Mode 1 328
   14.7.2 LE Security Mode 2 328
   14.7.3 Authentication Procedure 328
   14.7.4 Authorization Procedure 329
   14.7.5 Encryption Procedure 329
   14.7.6 Data Signing 329
   14.7.7 Privacy Feature 329
   14.7.8 Random Device Address 331
14.8 Summary 331
Bibliography 332
CHAPTER 15

GATT-Based Profiles

15.1 Introduction 333
15.2 Profile, Services, and Characteristics 333
15.3 Immediate Alert Service (IAS)
   15.3.1 Service Declaration 335
   15.3.2 Service Characteristics 335
15.4 Find Me Profile (FMP)
   15.4.1 Roles 336
15.5 Link Loss Service (LLS)
   15.5.1 Service Declaration 337
   15.5.2 Service Characteristics 337
15.6 Transmit Power Service (TPS)
   15.6.1 Service Declaration 338
   15.6.2 Service Characteristics 339
15.7 Proximity Profile (PXP)
   15.7.1 Roles 339
15.8 Battery Service (BAS)
   15.8.1 Service Declaration 340
   15.8.2 Service Characteristics 340
15.9 Device Information Service (DIS)
   15.9.1 Service Declaration 340
   15.9.2 Service Characteristics 341
15.10 Current Time Service (CTS)
   15.10.1 Service Declaration 341
   15.10.2 Service Characteristics 341
15.11 Health Thermometer Service (HTS)
   15.11.1 Service Declaration 341
   15.11.2 Service Characteristics 341
15.12 Health Thermometer Profile (HTP)
   15.12.1 Roles 343
15.13 Blood Pressure Service (BPS)
   15.13.1 Service Declaration 343
   15.13.2 Service Characteristics 343
15.14 Blood Pressure Profile (BLP)
   15.14.1 Roles 344
15.15 Health, Sports and Fitness Profiles
15.16 Other Services and Profiles
15.17 Practical Examples
15.18 Summary
Bibliography

CHAPTER 16

Developing LE Applications

16.1 Introduction 349
16.2 Ingredients

16.2.1 Installing hcidump
16.2.2 Basic Bluetooth operations

16.3 Advertising and Scanning

16.4 Creating a Connection

16.5 GATT Operations

16.5.1 Enable GATT Functionality on Server
16.5.2 Execute GATT Procedures from the Client
16.5.3 Reading and Writing Characteristics

16.6 Disconnecting

16.6.1 Disconnecting the GATT Connection
16.6.2 Disconnecting the LE Connection

16.7 Real-World Application—Find Lost Keys

16.8 Debugging LE Applications

16.8.1 Logging the HCI Interface
16.8.2 Air Sniffer
16.8.3 Peer Devices and Interoperability Testing
16.8.4 Profile Tuning Suite (PTS)

16.9 Disclaimer

16.10 Summary

References

CHAPTER 17

Testing and Qualification

17.1 Introduction

17.2 Need for Bluetooth Qualification

17.3 What Is Interoperability?

17.4 Development Resources and Events

17.4.1 UnPlugFest (UPF)
17.4.2 Automotive Events
17.4.3 SIG Device Library
17.4.4 Profile Tuning Suite (PTS)

17.5 Bluetooth Qualification Program

17.6 Test Categories

17.6.1 BQTF, BRTF
17.6.2 BQE
17.6.3 Test Documents
17.6.4 Prequalification

17.7 Summary

Bibliography

Glossary of Acronyms and Important Terms

About the Author

Index