CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

Contents

1 Introduction *page* 1
1.1 The growth of standards 1
1.2 Markets 4
1.2.1 Games controllers 4
1.2.2 Voice 5
1.2.3 Internet access 5
1.2.4 Internet connected devices 5
1.3 What is a standard? 7
1.4 Choosing a wireless standard 10
1.5 Wireless application areas 11
1.5.1 Standard vs proprietary wireless 11
1.5.2 The importance of topology 12
1.5.3 The 'Internet of things' 13
1.6 Using this book 15
1.7 References 16

2 Fundamentals of short-range wireless 17
2.1 Basics 17
2.1.1 The connection model and topology 18
2.1.2 Latency, range and throughput 18
2.1.3 Security 18
2.2 Wireless architecture 19
2.2.1 The radio 19
2.2.2 Baseband: media access control (MAC) 20
2.2.3 Higher-layer stacks 22
2.2.4 Profiles 22
2.3 Wireless parameters 24
2.3.1 Range 25
2.3.2 Throughput 34

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

2.3.3 Interference and coexistence 36
2.3.4 Topology 42
2.3.5 Security – authentication and encryption 48
2.3.6 Power consumption 49
2.3.7 Profiles and interoperability 52
2.3.8 Voice and latency (quality of service and synchronous transmission) 53
2.3.9 Reliability 55
2.3.10 Audio and video 56
2.3.11 Usability and commissioning 57
2.4 Conclusion 58
2.5 References 59

3 Wireless security 60
3.1 Security attacks 62
3.1.1 Discovery 62
3.1.2 Eavesdropping (interception) 62
3.1.3 Denial of service 62
3.1.4 Man-in-the-middle attacks, spoofing and bluejacking 63
3.1.5 Address tracking 66
3.2 Security features 66
3.2.1 Authorisation 66
3.2.2 Authentication 67
3.2.3 Encryption 68
3.2.4 Other features 69
3.3 Generation and distribution of link keys 70
3.4 Comparison of security procedures 70
3.4.1 Susceptibility to attack 71
3.4.2 Security implementations 75
3.5 Testing security – in praise of hacking tools 79
3.6 References 80

4 Bluetooth 81
4.1 Background 81
4.2 The radio 84

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

4.3 Topologies 87
4.4 Connections 91
4.4.1 Making connections 92
4.5 Transferring data 97
4.5.1 Asynchronous links (ACL) 97
4.5.2 Synchronous links (SCO and eSCO) 98
4.5.3 Voice codecs 99
4.6 The lower-layer stack (the controller) 99
4.7 The higher-layer stack (the host) 100
4.7.1 Logical link control and adaptation protocol (L2CAP) 101
4.7.2 Service discovery protocol (SDP) 101
4.7.3 Generic access profile (GAP) 102
4.7.4 Bonding and pairing 102
4.8 Transport protocols 104
4.9 Profiles 104
4.9.1 Serial port profile (SPP) 105
4.9.2 Handsfree profile (HFP) 105
4.9.3 Generic object-exchange profile (GOEP / OBEX) 106
4.9.4 Personal area networking profile (PAN) 108
4.9.5 Health device profile (HDP) 109
4.9.6 Human interface device profile (HID) 109
4.9.7 Advanced audio distribution profile (A2DP) 110
4.10 Power consumption 111
4.11 Bluetooth 3.0 112
4.12 References 114

5 IEEE 802.11abgn/Wi-Fi 115
5.1 Introduction 115
5.1.1 The difference between 802.11 and Wi-Fi 117
5.1.2 Bluetooth 3.0 121
5.1.3 Alphabet soup 121
5.2 802.11 topology 121

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

5.2.1 Bridging with access points 125
5.2.2 802.11 services 127
5.3 The 802.11 radio 130
5.4 Framing 134
5.5 Modulation 137
5.6 5.1 GHz – 802.11a 140
5.7 MIMO – 802.11n 141
5.8 Making connections 143
5.9 Power management 144
5.9.1 Wireless multimedia power save 145
5.10 References 145

6 IEEE 802.15.4, ZigBee PRO, RF4CE, 6LoWPAN and Wireless HART 147
6.1 IEEE 802.15.4 148
6.1.1 The MAC 152
6.1.2 Topologies 153
6.1.3 Framing 154
6.1.4 802.15.4 security 156
6.2 ZigBee 156
6.2.1 ZigBee and ZigBee PRO 160
6.2.2 The ZigBee network 162
6.2.3 ZigBee profiles and applications 167
6.3 ZigBee RF4CE 171
6.4 6LoWPAN 172
6.5 WirelessHART 173
6.6 References 174

7 Bluetooth low energy (formerly Wibree) 176
7.1 Basic tenets 178
7.1.1 Small packet size 178
7.1.2 Autonomous controller 178
7.1.3 Duty cycle and latency 179
7.1.4 Asymmetry 179
7.1.5 Range 179
7.1.6 Ease of use 179

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

7.2 RF 180
7.3 Topology 180
7.3.1 Profile roles 181
7.3.2 Unidirectional devices 181
7.3.3 Bidirectional devices 182
7.4 Advertising and data channels 183
7.4.1 Advertising packets 185
7.4.2 Response packets 186
7.5 The Bluetooth low-energy state machine 188
7.5.1 Advertising 189
7.5.2 Connecting 191
7.5.3 Discovery 193
7.5.4 Bonding 195
7.6 The Bluetooth low-energy protocol stack 195
7.6.1 Attributes – exposing state 197
7.6.2 Attribute PDUs 198
7.6.3 Notifications and indications 199
7.6.4 Characteristics 200
7.6.5 Aggregate characteristics and time stamping 200
7.6.6 Services 201
7.6.7 Configuring attribute servers 202
7.7 Profiles 202
7.7.1 Proximity 203
7.7.2 Gateways 203
7.8 Single-mode chips 205
7.9 Dual-mode chips 206
7.10 References 207

8 Application development – configuration 208
8.1 Topology 209
8.1.1 Cable replacement 209
8.1.2 Reconnection 214
8.1.3 Multipoint 215
8.1.4 Infrastructure (network connectivity) 218

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

8.1.5 Cluster tree 220
8.1.6 Mesh 220
8.2 Data protocols 221
8.2.1 Profile or proprietary 221
8.2.2 Interfacing with external protocols 222
8.2.3 Voice, audio and codecs 223
8.2.4 Latency and time synchronisation 226
8.3 Set-up and commissioning 227
8.3.1 Pairing, bonding, association 227
8.3.2 Promiscuity 228
8.3.3 The initial connection 229
8.3.4 Out-of-band techniques 230
8.3.5 Disconnecting 231
8.3.6 Limiting broadcasts 232
8.4 Feature creep 232
8.5 Security 233
8.6 Upgrading 233
8.6.1 Upgrading mesh and cluster-tree networks 237
8.7 References 238

9 Application development – performance 239
9.1 Range and throughput 239
9.1.1 Power amplifiers and low noise amplifiers 239
9.1.2 Power control 243
9.1.3 Filtering 244
9.1.4 RF matching, tuning and PCB design 244
9.2 Choice of antenna 246
9.2.1 Gain 246
9.2.2 Directionality 246
9.2.3 Construction (technology) and size 247
9.2.4 Detuning 247
9.2.5 Polarisation and antenna radiation characteristics 248
9.2.6 Ground planes 249
9.2.7 Antenna types 250

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

9.2.8 Diversity and multiple antennae 252
9.2.9 One last point on antennae 253
9.3 Coexistence 253
9.3.1 Interference mitigation 253
9.3.2 Colocation 255
9.4 Power consumption 256
9.4.1 Duty cycle 257
9.4.2. Sleep modes 259
9.4.3 Functional circuitry 259
9.5 Topology effects 260
9.6 Ultra-low power and energy harvesting 261
9.7 Temperature 261
9.7.1 Working below 0 °C 262
9.7.2 Working above 50 °C 263
9.8 References 263

10 Practical considerations – production, certification and IP 264
10.1 Regulatory approval 264
10.1.1 Modular approval 266
10.1.2 Other considerations 267
10.1.3 The Radio and Telecommunications Terminal Equipment directive (R&TTE) 267
10.2 Specific absorption rate – SAR 268
10.3 Medical, automotive and aviation 268
10.4 Export controls 269
10.5 Standards-based approvals and IP licences 270
10.5.1 Standards approval hierarchies 274
10.5.2 Specific requirements 275
10.6 Open-source protocol stacks 279
10.7 OUI – the device address 280
10.8 Production test 281
10.9 References 282

11 Implementation choices 284
11.1 Assessing the options 284

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

11.2 The design architecture 284
11.2.1 Chip-based designs 286
11.2.2 Reference designs 287
11.2.3 Modules 288
11.3 Development tools 289
11.4 Stack integration tools 289
11.5 Deciding on an implementation strategy 290
11.5.1 Bill of material cost 290
11.5.2 Development cost 290
11.5.3 Integration cost 291
11.5.4 RF design 291
11.5.5 Approvals 291
11.5.6 Time to market 291
11.5.7 Production test 291
11.5.8 Size 292
11.6 Comparison of costs 292
11.7 Longevity 294

12 Markets and applications 296
12.1 Growing the market 298
12.2 Healthcare, wellness, sports and fitness 299
12.2.1 The Continua Health Alliance 301
12.2.2 Health 2.0 302
12.2.3 Clinical asset management and lone workers 302
12.2.4 Assisted living 303
12.2.5 Sports and fitness 304
12.3 The telematics and automotive markets 305
12.3.1 Vehicle-to-vehicle communications 306
12.3.2 Vehicle and driver monitoring 308
12.4 Smart energy 309
12.4.1 The key opportunities 312
12.5 Home automation 314
12.6 Consumer electronics 316
12.6.1 Internet connected devices 316

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-76069-0 - Essentials of Short-Range Wireless
Nick Hunn
Table of Contents
More information

12.7 Fashion wireless 318
12.7.1 Tags 318
12.7.2 Watches 318
12.7.3 Bracelets – the new watches 319
12.8 Industrial and automation 319
12.9 Self-powered sensors 320
12.10 Privacy concerns 320
12.11 Conclusion 321
12.12 References 322

Glossary of acronyms and abbreviations 324

Index 329

© in this web service Cambridge University Press www.cambridge.org