CONTENTS

List of Figures xix
List of Tables xxiii
Preface xxvii
Acknowledgments xxix
Biographical Sketches of the Authors xxxi

1 Introduction 1
  1.1 HomePlug AV and Its Relationship to IEEE 1901, 2
  1.2 Focus of the Book, 3
  1.3 The HomePlug Powerline Alliance, 4
    1.3.1 HomePlug Specifications, 4
    1.3.2 How the HomePlug AV Specification Was Developed, 5
    1.3.3 The Regulatory Working Group, 6
      1.3.3.1 The United States and the FCC, 6
      1.3.3.2 Europe, CISPR, and CENELEC, 7
      1.3.3.3 Rest of the World, 8
  1.4 The Role of PLC in Multimedia Home Networking and Smart Energy Applications, 8
  1.5 Book Outline, 9
2 The HomePlug AV Network Architecture 12

2.1 Introduction, 12
2.2 Protocol Layers, 12
2.3 Network Architecture, 14
   2.3.1 Station Roles, 16
   2.3.2 Bridging, 16
   2.3.3 Channel Access, 16
2.4 Summary, 17

3 Design Approach for Powerline Channels 18

3.1 Introduction, 18
3.2 Channel Characteristics, 19
3.3 Frequency Band, 21
   3.3.1 Tone Mask, 22
   3.3.2 Amplitude Map, 22
3.4 Windowed OFDM, 23
3.5 Turbo Convolutional Code, 24
3.6 Channel Adaptation, 25
   3.6.1 Bit-Loading, 27
3.7 Beacon Period Synchronized to AC Line Cycle, 27
   3.7.1 AC Line Cycle Synchronization for TDMA Allocations, 28
3.8 TDMA with Persistent and Nonpersistent Schedules, 29
3.9 Data Plane: Two-Level Framing, Segmentation, and Reassembly, 30
3.10 PHY Clock Synchronization, 30
3.11 Summary, 31

4 Physical Layer 32

4.1 Introduction, 32
   4.1.1 Transceiver Block Diagram, 33
4.2 PPDU, 34
   4.2.1 PPDU Formats, 35
   4.2.2 PPDU Structure, 36
   4.2.3 Symbol Timing, 36
4.3 Preamble, 37
4.4 Frame Control, 38
4.5 Payload, 39
   4.5.1 Scrambler, 40
   4.5.2 Turbo Convolutional Encoder, 41
      4.5.2.1 Constituent Encoders, 41
      4.5.2.2 Termination, 41
      4.5.2.3 Puncturing, 42
      4.5.2.4 Turbo Interleaving, 42
4.5.3 Channel Interleaver, 44
4.5.4 ROBO Modes, 46
  4.5.4.1 ROBO Interleaver, 46
4.5.5 Mapping and Tone Maps, 49
  4.5.5.1 Empty Tone Filling, 50
  4.5.5.2 Last Symbol Padding, 50
  4.5.5.3 Mapping Reference, 51
  4.5.5.4 Mapping for BPSK, QPSK, 8 QAM, 16 QAM, 64 QAM, 256 QAM, 1024 QAM, 51
  4.5.5.5 Mapping for ROBO-AV, 53
4.5.6 Payload Symbols, 54
4.5.7 Windowed OFDM and Symbol Shaping, 55
4.6 Priority Resolution Symbol, 56
4.7 Transmit Power, Tone Mask, and Amplitude Map, 56
  4.7.1 Relative Power Levels, 56
  4.7.2 Tone Mask, 57
  4.7.3 Amplitude Map, 58
4.8 Summary, 60

5 MAC Protocol Data Unit (MPDU) Format 61
5.1 Introduction, 61
  5.1.1 General AV Frame Control, 63
5.2 Beacon, 64
  5.2.1 Beacon Frame Control, 65
    5.2.1.1 Beacon Time Stamp (BTS), 65
    5.2.1.2 Beacon Transmission Offset (BTO), 65
  5.2.2 Beacon Payload, 65
    5.2.2.1 Beacon Type, 65
    5.2.2.2 Addressing, 66
    5.2.2.3 Neighbor Network Coordination, 67
    5.2.2.4 Network Operation Mode, 67
    5.2.2.5 CCo Capability, 68
    5.2.2.6 Participation in Multiple Networks, 68
    5.2.2.7 CCo Handover, 68
    5.2.2.8 Beacon Management Information (BMI), 68
    5.2.2.9 Beacon Payload Check Sequence (BPCS), 77
5.3 Start-of-Frame (SOF), 77
  5.3.1 Start-of-Frame (SOF) Frame Control, 77
    5.3.1.1 Addressing-Related Fields, 78
    5.3.1.2 Queue-Related Fields, 79
    5.3.1.3 Bursting-Related Fields, 79
    5.3.1.4 Payload Demodulation-Related Fields, 80
    5.3.1.5 TDMA Allocation-Related Fields, 81
5.3.1.6 SACK Retransmission-Related Fields, 81
5.3.1.7 Encryption-Related Fields, 82
5.3.1.8 Detection Status-Related Fields, 82
5.3.1.9 Participation in Multiple Networks-Related Fields, 82
5.3.1.10 Convergence Layer SAP Type (CLST), 83
5.3.2 SOF Payload, 83
5.4 Selective Acknowledgment (SACK), 85
5.4.1 Addressing-Related Field, 85
5.4.2 Queue-Related Field, 86
5.4.3 Bursting-Related Field, 86
5.4.4 TDMA Allocation-Related Fields, 87
5.4.5 Detection Status-Related Field, 87
5.4.6 Version-Related Fields, 87
5.4.7 SACK Data, 87
5.5 Request to Send (RTS)/Clear to Send (CTS), 88
5.5.1 Addressing-Related Fields, 88
5.5.2 Queue-Related Fields, 89
5.5.3 TDMA Allocation-Related Fields, 89
5.5.4 Detection Status Fields, 89
5.5.5 Immediate Grant-Related Fields, 90
5.5.6 Virtual Carrier Sense (VCS)-Related Fields, 90
5.5.7 RTS Flag, 91
5.6 Sound, 91
5.6.1 Sound Frame Control, 91
5.6.1.1 Addressing, 91
5.6.1.2 Queue, 92
5.6.1.3 Bursting, 92
5.6.1.4 Payload Demodulation, 92
5.6.1.5 TDMA Allocations, 93
5.6.1.6 Detection Status-Related Field, 93
5.6.1.7 Sound ACK, 93
5.6.1.8 Sound Complete Flag, 93
5.6.1.9 Sound Reason Code, 93
5.6.1.10 Max Tone Maps, 94
5.6.2 Format of Sound MPDU Payload, 94
5.7 Reverse Start-of-Frame (RSOF), 95
5.7.1 Reverse SOF (RSOF) Frame Control, 95
5.7.1.1 Addressing-Related Field, 95
5.7.1.2 Queue-Related Field, 95
5.7.1.3 Bursting-Related Field, 96
5.7.1.4 TDMA Allocation-Related Fields, 97
5.7.1.5 Detection Status-Related Field, 97
5.7.1.6 Version-Related Fields, 97
5.7.1.7 Selective Acknowledgment-Related Field, 97
5.7.1.8 Payload Demodulation-Related Fields, 97
5.8 Summary, 98

6 MAC Data Plane 99

6.1 Introduction, 99
6.2 MAC Frame Generation, 101
6.3 MAC Frame Streams, 102
   6.3.1 Priority of Management Streams, 103
6.4 Segmentation, 104
6.5 Long MPDU Generation, 104
6.6 Reassembly, 106
6.7 Buffer Management and Flow Control, 106
   6.7.1 Transmit Buffer Management, 107
   6.7.2 Receive Buffer Management, 109
6.8 Communication Between Associated but Unauthenticated STAs, 112
6.9 Communication Between STAs not Associated with the
   Same AVLN, 112
   6.9.1 Multinetwork Broadcast (MNBC), 113
6.10 Data Encryption, 114
6.11 MPDU Bursting, 114
6.12 Bidirectional Bursting, 115
   6.12.1 Bidirectional Bursting During CSMA, 116
   6.12.2 Connections and Links During Bidirectional Bursts, 118
   6.12.3 Encryption of RSOF Payload, 118
6.13 Automatic Repeat Request (ARQ), 118
   6.13.1 Request SACK Retransmission, 119
   6.13.2 Broadcast/Multicast and Partial Acknowledgment, 119
6.14 Summary, 120

7 Central Coordinator 121

7.1 Introduction, 121
7.2 CCo Selection, 122
   7.2.1 CCo Selection for a New AVLN, 122
   7.2.2 Auto-Selection of CCo, 122
   7.2.2.1 CCo Capability, 123
   7.2.3 User-Appointed CCo, 124
7.3 Backup CCo and CCo Failure Recovery, 125
   7.3.1 Backup CCo, 125
   7.3.2 CCo Failure Recovery, 125
7.4 Transfer/Handover of CCo Functions, 125
7.5 CCo Network Management Functions, 127
   7.5.1 Network Time Base Synchronization, 127
7.5.1.1 Arrival Time Stamp for MSDU Jitter and Delay Control, 129
7.5.1.2 PHY Clock Correction When Participating in More Than One Network, 129
7.5.2 Discover Process, 130
7.6 Summary, 132

8 Channel Access

8.1 Introduction, 133
8.2 Beacon Period and AC Line Cycle Synchronization, 135
  8.2.1 Line Cycle Synchronization, 135
8.3 Beacon Period Structure, 135
  8.3.1 Beacon Period Structure in CSMA-Only Mode, 139
  8.3.2 Beacon Period Structure in Uncoordinated Mode, 141
  8.3.3 Beacon Period Structure in Coordinated Mode, 142
8.4 CSMA Channel Access, 143
  8.4.1 Carrier Sense Mechanism, 144
    8.4.1.1 MAC-Level Acknowledgments, 144
    8.4.1.2 Setting of Virtual Carrier Sense (VCS) Timer, 145
    8.4.1.3 RTS/CTS, 146
  8.4.2 Contention Procedure, 146
    8.4.2.1 Priority Contention, 148
8.5 TDMA Channel Access, 148
  8.5.1 Admission Control and Scheduling (Persistent and Nonpersistent), 148
8.6 Summary, 149

9 Connections and Links

9.1 Introduction, 150
9.2 Packet Classification, 151
9.3 Connection Specification (CSPEC), 152
9.4 Connections and Links, 154
  9.4.1 Link Identifiers, 156
    9.4.1.1 Assignment of LIDs, 157
  9.4.2 Connection Identifiers, 157
9.5 Connection Services, 157
  9.5.1 Connection Setup, 159
  9.5.2 Connection Monitoring, 161
  9.5.3 Connection Teardown, 161
  9.5.4 Connection Reconfiguration, 164
  9.5.5 Global Link Reconfiguration Triggered by CCo, 167
    9.5.5.1 Squeeze and De-Squeeze, 167
9.6 Bandwidth Management by CCo, 168
  9.6.1 Scheduler and Bandwidth Allocation, 168
  9.6.2 Connection Admission Control, 171
  9.6.3 Beacon Period Configuration, 171
9.7 Summary, 171

10 Security and Network Formation 172

10.1 Introduction, 172
10.2 Power-on Network Discovery Procedure, 172
  10.2.1 Unassociated STA Behavior, 174
  10.2.2 Unassociated CCo Behavior, 175
  10.2.3 Behavior as an STA in an AVLN, 176
  10.2.4 Behavior as a CCo in an AVLN, 177
10.3 Forming or Joining an AVLN, 178
  10.3.1 AVLN Overview, 178
    10.3.1.1 Network Identification, 178
    10.3.1.2 Human-Friendly Station and AVLN Names, 178
    10.3.1.3 Get Full AVLN Information, 178
    10.3.1.4 Get Full STA Information, 178
  10.3.2 Association, 179
    10.3.2.1 TEI Assignment and Renewal, 179
  10.3.3 Method for Authentication, 181
  10.3.4 Forming a New AVLN, 181
    10.3.4.1 Two Unassociated STAs with Matching NIDs, 183
    10.3.4.2 Two Unassociated STAs Form an AVLN Using a DAK-Encrypted NMK, 183
    10.3.4.3 Two Unassociated STAs: One in SC-Add and One in SC-Join, 186
    10.3.4.4 Two Unassociated STAs: Both in SC-Join, 186
  10.3.5 Joining an Existing AVLN, 188
    10.3.5.1 Matching NIDs, 189
    10.3.5.2 DAK-Encrypted NMK, 189
    10.3.5.3 SC-Join and SC-Add, 190
  10.3.6 Leaving an AVLN, 192
  10.3.7 Removing a Station from an AVLN, 193
10.4 Security Overview, 193
  10.4.1 Encryption Keys, Pass Phrases, Nonces, and Their Uses, 194
    10.4.1.1 Device Access Key (DAK), 194
    10.4.1.2 Device Password (DPW), 194
    10.4.1.3 Network Membership Key (NMK), 194
    10.4.1.4 Network Password (NPW), 194
    10.4.1.5 Network Encryption Key (NEK), 194
10.4.1.6 Temporary Encryption Key (TEK), 195
10.4.1.7 Nonces, 195

10.4.2 Methods for Authorization (NMK Provisioning), 195
10.4.2.1 Security Level, 196
10.4.2.2 Preloaded NMK, 198
10.4.2.3 Direct Entry of the NMK, 198
10.4.2.4 Distribution of NMK Using DAK, 199
10.4.2.5 Distribution of NMK Using Unicast Key Exchange (UKE), 200
10.4.2.6 Distribution of NMK Using Other Key Management Protocols, 202
10.4.2.7 Changing the NMK, 203

10.4.3 NEK Provisioning, 203
10.4.3.1 Provisioning NEK for New STA, 203
10.4.3.2 Provisioning NEK for Part or All of the AVLN, 203

10.4.4 Encryption Key Uses and Protocol Failures, 204

10.4.5 AES Encryption Algorithm and Mode, 207
10.4.5.1 PHY Block-Level Encryption, 207
10.4.5.2 Payload-Level Encryption, 207

10.4.6 Generation of AES Encryption Keys, 208
10.4.6.1 Generation from Passwords, 208
10.4.6.2 Automatic Generation of AES Keys, 208
10.4.6.3 Generation of Nonces, 208

10.4.7 Encrypted Payload Message, 209
10.4.8 User Interface Station (UIS), 210

10.5 Summary, 210

11 Additional MAC Features

11.1 Introduction, 211

11.2 Channel Estimation, 211
11.2.1 Channel Estimation Procedure, 212
11.2.2 Initial Channel Estimation, 213
11.2.3 Dynamic Channel Adaptation, 214
11.2.4 Maintenance of Tone Maps, 217
11.2.5 Tone Map Intervals, 218
11.2.6 Priority of Channel Estimation Response, 219
11.2.7 Channel Estimation with Respect to the AC Line Cycle, 219

11.3 Bridging, 219
11.3.1 Acting as an AV Bridge, 220
11.3.2 Communicating Through an AV Bridge, 221
11.3.2.1 Communication with a Known DA, 222
11.3.2.2 Communicating with an Unknown DA, 222
11.4 HomePlug 1.0.1 Coexistence, 223
   11.4.1 HomePlug AV Coexistence Modes, 223
   11.4.2 Detection and Reporting of Active HomePlug 1.0.1, 224
   11.4.3 HomePlug 1.0.1/1.1 Coexistence Mode Changes, 224
   11.4.4 HomePlug 1.0.1-Compatible Frame Lengths, 225
11.5 Proxy Networking, 225
   11.5.1 Identification of Hidden Stations, 227
   11.5.2 Association of Hidden Station, 227
   11.5.3 Instantiation of Proxy Network, 229
   11.5.4 Proxy Beacons, 229
   11.5.5 Provisioning the NMK to Hidden Stations, 229
   11.5.6 Provisioning NEK for Hidden Stations (Authenticating the HSTA), 230
   11.5.7 Exchange of MMEs Through a PCo, 230
   11.5.8 Transitioning from Being a STA to Being an HSTA, 231
   11.5.9 Transitioning from Being an HSTA to Being a STA, 231
   11.5.10 Recovering from the Loss of a PCo, 232
   11.5.11 Proxy Network Shutdown, 232
11.6 Summary, 232

12 Neighbor Networks
   12.1 Introduction, 233
      12.1.1 CSMA-Only Mode, 233
      12.1.2 Uncoordinated Mode, 234
      12.1.3 Coordinated Mode, 234
   12.2 Transition Between Neighbor Network Operating Modes, 234
   12.3 Coordinated Mode, 236
      12.3.1 Interfering Network List, 237
      12.3.2 Group of Networks, 237
      12.3.3 Determining a Compatible Schedule, 237
         12.3.3.1 Computing the INL Allocation, 238
      12.3.4 Communication Between Neighboring CCos, 239
      12.3.5 Neighbor Network Instantiation, 240
         12.3.5.1 Procedure to Establish a New Network in Coordinated Mode, 240
         12.3.5.2 Changing the Number of Beacon Slots, 242
         12.3.5.3 Setting the Value of SlotUsage Field, 244
      12.3.6 Procedure to Share Bandwidth in Coordinated Mode, 244
      12.3.7 Bandwidth Scheduling Rules, 246
      12.3.8 Procedure to Shut Down an AVLN, 246
      12.3.9 AC Line Cycle Synchronization in Coordinated Mode, 247
   12.4 Passive Coordination in CSMA-Only Mode, 248
   12.5 Neighbor Network Bandwidth Sharing Policy, 248
   12.6 Summary, 249
13 Management Messages

13.1 Introduction, 250
13.2 Management Message Format, 250
   13.2.1 Original Destination Address (ODA), 250
   13.2.2 Original Source Address (OSA), 251
   13.2.3 VLAN Tag, 251
   13.2.4 MTYPE, 251
   13.2.5 Management Message Version (MMV), 251
   13.2.6 Management Message Type (MMTYPE), 251
   13.2.7 Fragment Management Information, 252
   13.2.8 Management Message Entry Data (MME), 254
   13.2.9 MMEPAD, 254
13.3 Station–Central Coordination (CCo), 254
13.4 Proxy Coordinator (PCO) Messages, 260
13.5 Central Coordinator–Central Coordinator, 260
13.6 Station–Station, 262
13.7 Manufacturer-Specific Messages, 266
13.8 Vendor-Specific Messages, 267
13.9 Summary, 267

14 IEEE 1901

14.1 Introduction, 268
14.2 FFT, 269
   14.2.1 30–50 MHz Frequency Band, 269
   14.2.2 Additional Guard Intervals, 270
   14.2.3 4096 QAM, 271
   14.2.4 16/18 Code Rate, 271
   14.2.5 SNID Reuse, 271
   14.2.6 Repeating and Routing, 272
      14.2.6.1 Repeating and Routing of Unicast MSDUs, 272
      14.2.6.2 Repeating and Routing of Broadcast/Multicast
      MSDUs, 273
14.3 Wavelet, 274
   14.3.1 Baseband PHY, 274
   14.3.2 Bandpass PHY, 274
      14.3.2.1 Wavelet MAC, 274
   14.3.3 Transceiver Block Diagram, 275
   14.3.4 PPDU Format, 276
      14.3.4.1 Overview of the PPDU Encoding/Decoding
      Process, 277
      14.3.4.2 Modulation-Dependent Parameters, 278
   14.3.5 PHY Encoder, 278
      14.3.5.1 Generator for RCE Frame, 278
      14.3.5.2 Scrambler, 278
14.3.5.3 CRC Encoder for FL, 279
14.3.5.4 Concatenated Encoder, 279
14.3.5.5 Convolutional Codes Defined by Low-Density Parity-Check Polynomials (Optional), 280
14.3.5.6 FEC Type Field, 281
14.3.5.7 Interleaver, 281
14.3.5.8 Wavelet Process, 282
14.3.5.9 Major Specifications, 292
14.3.5.10 Notch and Power Control, 293
14.3.5.11 System Clock Frequency Tolerance, 294

14.4 Coexistence, 294
14.4.1 Coexistence Signals, 294
14.4.2 ISP Signaling Scheme, 295
14.4.2.1 ISP Fields, 296
14.4.2.2 Network Status, 298
14.4.3 Coexistence Resources, 298
14.4.3.1 FDM, 298
14.4.3.2 TDM, 298
14.4.4 ISP Resource Allocation, 299
14.4.5 ISP Parameters, 301
14.4.6 Management Messages, 301

14.5 Summary, 301

15 HomePlug Green PHY 302

15.1 Introduction, 302
15.2 Physical Layer, 302
15.3 MAC Layer, 303
15.3.1 Power Save, 304
15.3.1.1 Distribution of Power Save State Information, 306
15.3.1.2 CC0 Power Save, 307
15.3.2 Bandwidth Sharing Between Green PHY and HomePlug AV and IEEE, 307
15.3.2.1 Green PHY Preferred Allocation, 307
15.3.2.2 Distributed Bandwidth Control, 308
15.3.3 PEV–EVSE Association, 309
15.3.3.1 PEV–EVSE Association Procedure, 310

15.4 Summary, 311

16 HomePlug AV2 312

16.1 Introduction, 312
16.2 MIMO, 312
16.3 Extended Frequency Band, 315
16.3.1 Power BackOff, 316
16.4 Efficient Notching, 316
16.5 Short Delimiter and Delayed Acknowledgment, 316
  16.5.1 Short Delimiter, 317
  16.5.2 Delayed Acknowledgment, 320
  16.5.3 TCP and UDP Efficiency Improvements, 320
16.6 Immediate Repeating, 321
16.7 Power Save, 322
16.8 Summary, 323

Appendix A Acronyms 325

Appendix B HomePlug AV Parameter Specification 332

References 334

Index 337