Contents

Chapter 1. Multicriteria Selection of Transmission Parameters in the IoT 1
Sinda BOUSSEN, Mohamed-Aymen CHALOUF and Francine KRIEF

1.1. Introduction 1
1.2. Changing access network in the IoT 2
1.3. Spectrum handoff in the IoT 3
1.4. Multicriteria decision-making module for an effective spectrum handoff in the IoT 4
1.4.1. General architecture 4
1.4.2. Decision-making flowchart 9
1.4.3. Performances evaluation 15
1.5. Conclusion 22
1.6. References 22

Chapter 2. Using Reinforcement Learning to Manage Massive Access in NB-IoT Networks 27
Yassine HADJADJ-AOUL and Soraya AIT-CHELLOUCHE

2.1. Introduction 27
2.2. Fundamentals of the NB-IoT standard 29
2.2.1. Deployment and instances of use 29
2.2.2. Transmission principles 30
2.2.3. Radio resource random access procedure 33
2.3. State of the art 37
2.4. Model for accessing IoT terminals 39

2.5. Access controller for IoT terminals based on reinforcement learning . . . 42
2.5.1. Formulating the problem. . . . 42
2.5.2. Regulation system for arrivals . . . 44
2.6. Performance evaluation. . . . 46
2.7. Conclusion . . . 51
2.8. References . . . 51

Chapter 3. Optimizing Performances in the IoT: An Approach Based on Intelligent Radio . . . 57
Badr BENMAMMAR

3.1. Introduction. . . . 57
3.2. Internet of Things (IoT) . . . 58
3.2.1. Definition of the IoT . . . 58
3.2.2. Applications of the IoT. . . . 59
3.2.3. IoT challenges . . . 60
3.2.4. Enabling technologies in the IoT . . . 61
3.3. Intelligent radio . . . 64
3.3.1. Definition of intelligent radio . . . 64
3.3.2. Motivations for using intelligent radio in the IoT . . . 66
3.3.3. Challenges in using intelligent radio in the IoT . . . 68
3.4. Conclusion . . . 71
3.5. References . . . 73

Chapter 4. Optimizing the Energy Consumption of IoT Devices . . . 77
Ahmad KHALIL, Nader MBAREK and Olivier TOGNI

4.1. Introduction. . . . 77
4.2. Energy optimization. . . . 78
4.2.1. Definitions . . . 78
4.3. Optimization techniques for energy consumption . . . 79
4.3.1. The A* algorithm . . . 79
4.3.2. Fuzzy logic. . . . 80
4.4. Energy optimization in the IoT . . . 82
4.4.1. Characteristics of the IoT . . . 82
4.4.2. Challenges in energy optimization . . . 84
4.4.3. Research on energy optimization in the IoT . . . 84
4.5. Autonomous energy optimization framework in the IoT . . . 86
4.5.1. Autonomous computing . . . 86
4.5.2. Framework specification. . . . 89

4.6. Proposition of a self-optimization method for energy consumption in the IoT. 90
4.6.1. Fuzzy logic model 91
4.6.2. Decision-making algorithm 95
4.6.3. Evaluating energy self-optimization in the IoT 97
4.7. Conclusion 101
4.8. References 101

Chapter 5. Toward Intelligent Management of Service Quality in the IoT: The Case of a Low Rate WPAN 105
Guillaume LE GALL, Georgios Z. PAPADOPOULOS, Mohamed-Aymen CHALOUF and Olivier TOGNI

5.1. Introduction. 106
5.2. Quick overview of the IoT 108
5.2.1. The micro-IPv6 stack. 108
5.2.2. Technologies for the IoT. 110
5.2.3. IoT and quality of service 114
5.3. IEEE 802.15.4 TSCH approach 115
5.4. Transmission scheduling 117
5.4.1. General considerations. 117
5.4.2. Scheduling in the literature 118
5.5. Routing and RPL 120
5.5.1. Routing 120
5.5.2. RPL 121
5.5.3. Multipath 122
5.6. Combined approach based on 802.15.4 TSCH and multipath RPL 123
5.6.1. Automatic Repeat reQuest. 125
5.6.2. Replication and Elimination. 125
5.6.3. Overhearing 127
5.7. Conclusion 127
5.8. References 128

Chapter 6. Adapting Quality of Service of Energy-Harvesting IoT Devices 133
Matthieu GAUTIER and Olivier BERDER

6.1. Toward the energy autonomy of sensor networks 135
6.1.1. Energy harvesting and management 135
6.1.2. State-of-the-art energy managers. 138

6.2. Fuzzyman: use of fuzzy logic 141
6.2.1. Design of Fuzzyman 141
6.2.2. Evaluating Fuzzyman 145
6.2.3. Conclusion 146
6.3. RLMan: using reinforcement learning 148
6.3.1. Formulating the problem of managing the harvested energy 148
6.3.2. RLMan algorithm 150
6.3.3. Evaluation of RLMan 153
6.3.4. Conclusion 155
6.4. Toward energy autonomous LoRa nodes 155
6.4.1. Multisource energy-harvesting architecture 157
6.4.2. Applying energy management to LoRa nodes 157
6.5. Conclusion 157
6.6. References 160

Chapter 7. Adapting Access Control for IoT Security 163
Ahmad KHALIL, Nader MBAREK and Olivier TOGNI

7.1. Introduction. 163
7.2. Defining security services in the IoT 164
7.2.1. Identification and authentication in the IoT. 164
7.2.2. Access control in the IoT 165
7.2.3. Confidentiality in the IoT 166
7.2.4. Integrity in the IoT 166
7.2.5. Non-repudiation in the IoT 167
7.2.6. Availability in the IoT 167
7.3. Access control technologies 168
7.4. Access control in the IoT. 172
7.4.1. Research on the extension of access control models for the IoT 172
7.4.2. Research on adapting access control systems and technologies for the IoT 173
7.5. Access control framework in the IoT. 176
7.5.1. IoT architecture 177
7.5.2. IoT-MAAC access control specification 179
7.6. Conclusion 193
7.7. References 194

Chapter 8. The Contributions of Biometrics and Artificial Intelligence in Securing the IoT 197
Amal SAMMOUD, Omessaad HAMDI, Mohamed-Aymen CHALOUF and Nicolas MONTAVONT

8.1. Introduction. 197
8.2. Security and privacy in the IoT 198
8.3. Authentication based on biometrics 199
8.3.1. Biometrics 199
8.3.2. Biometric techniques 199
8.3.3. The different properties of biometrics 200
8.3.4. Operating a biometric system 201
8.3.5. System performances. 202
8.4. Multifactor authentication techniques based on biometrics. 202
8.4.1. Multifactor authentication 203
8.4.2. Examples of multifactor authentication approaches for securing the IoT 204
8.4.3. Presentation of the approach of Sammoud et al. (2020c). 205
8.5. Authentication techniques based on biometrics and machine learning 213
8.5.1. Machine learning algorithms 213
8.5.2. Examples of authentication approaches based on biometrics and machine learning. 214
8.5.3. Authentication approaches based on ECG and machine learning 215
8.6. Challenges and limits 217
8.6.1. Quality of biometric data 217
8.6.2. Non-revocability of biometric data. 218
8.6.3. Security of biometric systems. 218
8.7. Conclusion 218
8.8. References 218

Chapter 9. Dynamic Identity and Access Management in the IoT: Blockchain-based Approach. 223
Léo MENDIBOURE, Mohamed-Aymen CHALOUF and Francine KRIEF

9.1. Introduction. 223
9.2. Context 224
9.2.1. Intelligent identity and access management 225
9.2.2. Blockchain 226

9.3. Blockchain for intelligent identity and access management 227
9.3.1. A new architecture integrating blockchain 228
9.3.2. The different benefits. 229
9.4. Challenges 234
9.4.1. Scaling up 235
9.4.2. Blockchain security. 235
9.4.3. Energy consumption 236
9.4.4. Definition of consensus algorithms based on artificial intelligence. 236
9.5. Conclusion 237
9.6. References 237

Chapter 10. Adapting the Security Level of IoT Applications 243
Tidiane SYLLA, Mohamed-Aymen CHALOUF and Francine KRIEF

10.1. Introduction 243
10.2. Definitions and characteristics 244
10.2.1. Definitions 244
10.2.2. Characteristics 244
10.3. IoT applications 246
10.4. IoT architectures 246
10.5. Security, trust and privacy protection in IoT applications. 247
10.5.1. General remarks 248
10.5.2. Security services. 248
10.5.3. Communication security 251
10.5.4. Trust 252
10.5.5. Privacy 253
10.6. Adapting the security level in the IoT 254
10.6.1. Context-awareness 255
10.6.2. Context-aware security 256
10.6.3. Context-aware security architecture and privacy protection designed using the “as a service” approach 258
10.7. Conclusion 261
10.8. References. 261

Chapter. 11 Moving Target Defense Techniques for the IoT. 267
Renzo E. NAVAS, Laurent TOUTAIN and Georgios Z. PAPADOPOULOS

11.1. Introduction 268
11.2. Background 269

11.2.1. Brief chronology of Moving Target Defense 269
11.2.2. Fundamental technical and taxonomic principles of MTD 270
11.3. Related works. 271
11.3.1. Surveys on MTD techniques. 271
11.3.2. Frameworks for IoT systems linked to the concept of MTD. 271
11.4. LMTD for the IoT: a qualitative survey 272
11.4.1. Data: MTD mechanism against side-channel channel attacks based on renegotiating cryptographic keys 272
11.4.2. Software. 272
11.4.3. Runtime environment. 273
11.4.4. Platform: diversifying by reconfiguring the IoT node firmware. 275
11.4.5. Networks 275
11.4.6. Section summary 278
11.5. Network components in the IoT: a vast domain for MTD. 279
11.5.1. Physical layer 280
11.5.2. Link layer. 281
11.5.3. OSI network layer. 281
11.5.4. Transport layer. 282
11.5.5. Application layer 283
11.5.6. Section summary 284
11.6. An MTD framework for the IoT. 284
11.6.1. Proposition: components. 284
11.6.2. Instantiation: UDP port hopping 286
11.7. Discussion and avenues for future research 287
11.8. Conclusion 288
11.9. References. 288

List of Authors 293

Index 295