

Contents

Preface	xi
Chapter 1. Service Level Management in the Internet of Things (IoT)	1
Ahmad KHALIL, Nader MBAREK and Olivier TOGNI	
1.1. Introduction.	1
1.2. IoT: definitions.	2
1.3. IoT: an overview.	3
1.3.1. IoT architectures	3
1.3.2. Application fields of the IoT	6
1.4. Security management and privacy protection in the IoT	8
1.4.1. Motivations and challenges	8
1.4.2. Security services in the IoT environment	10
1.4.3. Privacy protection and trust in the IoT	18
1.5. QoS management for IoT services	21
1.5.1. Motivations and challenges	21
1.5.2. Guaranteeing QoS in IoT	22
1.6. QBAIoT: QoS-based access method for IoT environments	28
1.6.1. Service level guarantee in the IoT	28
1.6.2. The QBAIoT process in the IoT	31
1.6.3. QBAIoT performance evaluation.	36
1.7. Conclusion	38
1.8. References	39

Chapter 2. Service Level Management in the Cloud	45
Nader MBAREK	
2.1. Introduction.	45
2.2. The Cloud environment.	46
2.2.1. Cloud Computing	46
2.2.2. Cloud Networking	50
2.2.3. Inter-Cloud.	52
2.3. Service level and self-management in the Cloud.	54
2.3.1. Quality of Service in a Cloud environment.	54
2.3.2. Security in a Cloud environment	57
2.3.3. Self-management of Cloud environments.	60
2.4. QoS guarantee in Cloud Networking.	63
2.4.1. Cloud Networking architectures	63
2.4.2. Performance evaluation	68
2.5. Conclusion	75
2.6. References	75
Chapter 3. Managing Energy Demand as a Service in a Smart Grid Environment	83
Samira CHOUIKHI, Leila MERGHEM-BOULAHIA and Moez ESSEGHIR	
3.1. Introduction.	83
3.2. The Smart Grid environment	84
3.2.1. Smart microgrids	85
3.2.2. Information and communication infrastructure	86
3.3. Demand management: fundamental concepts.	87
3.3.1. Predicting loads	87
3.3.2. DR – demand response.	88
3.4. Demand-side management	89
3.4.1. The architectures and components of DSM platforms	90
3.4.2. Classifying DSM approaches	91
3.4.3. Deterministic approaches for individual users	92
3.4.4. Stochastic approaches for individual users	93
3.4.5. Deterministic approaches for consumer communities	94
3.4.6. Stochastic approaches for consumer communities.	94
3.5. Techniques and methods for demand scheduling.	96
3.5.1. Game theory	97
3.5.2. Multiagent systems	98
3.5.3. Machine learning	99
3.6. Conclusion	100
3.7. References	101

Chapter 4. Managing Quality of Service and Security in an e-Health Environment. 107

Mohamed-Aymen CHALOUF

4.1. Introduction.	107
4.2. e-health systems	109
4.2.1. Architecture	110
4.2.2. Characteristics	111
4.3. QoS in e-health systems	114
4.3.1. e-health services and QoS	114
4.3.2. QoS management in e-health systems	117
4.4. Security of e-health systems	124
4.4.1. Threats and attacks specific to e-health systems	124
4.4.2. Security management in e-health systems	127
4.5. Conclusion	130
4.6. References	131

Chapter 5. Quality of Service Management in Wireless Mesh Networks 139

Hajer BARGAOUI, Nader MBAREK and Olivier TOGNI

5.1. Introduction.	139
5.2. WMNs: an overview	140
5.2.1. Definition of a WMN.	140
5.2.2. Architecture of a radio mesh wireless network.	140
5.2.3. Characteristics of a WMN environment.	142
5.2.4. Standards for WMNs.	143
5.2.5. Domains of applications	144
5.3. QoS in WMNs	146
5.3.1. QoS in networks.	146
5.3.2. QoS constraints in WMNs.	146
5.3.3. QoS mechanisms in WMNs.	147
5.3.4. Research projects on QoS in WMNs.	150
5.4. QoS-based routing for WMNs.	152
5.4.1. Routing requirements in WMNs	152
5.4.2. Routing metrics in WMNs.	153
5.4.3. QoS-based routing protocols in WMNs.	154
5.5. HQMR: QoS-based hybrid routing protocol for mesh radio networks	157
5.5.1. Description of the HQMR protocol	157
5.5.2. How the HQMR protocol works	160
5.5.3. Validation of the HQMR protocol	162
5.6. Conclusion	168
5.7. References	168

Chapter 6. Blockchain Based Authentication and Trust Management in Decentralized Networks	175
Axel MOINET and Benoît DARTIES	
6.1. Introduction.	175
6.1.1. Challenges and motivations, the state of the art	177
6.1.2. Blockchain, a support for authentication and trust.	181
6.2. The Blockchain Authentication and Trust Module (BATM) architecture.	184
6.2.1. Context and development	184
6.2.2. Managing identities and authentication	185
6.2.3. Calculating trust and reputation using the MLTE algorithm.	188
6.3. Evaluating BATM.	197
6.3.1. Simulation plan	197
6.3.2. Results and interpretation	198
6.4. Conclusion	201
6.5. References	202
Chapter 7. How Machine Learning Can Help Resolve Mobility Constraints in D2D Communications	205
Chérifa BOUCETTA, Hassine MOUNGLA and Hossam AFIFI	
7.1. Introduction.	205
7.2. D2D communication and the evolution of networks.	207
7.2.1. The discovery phase in D2D communications	208
7.2.2. The data exchange phase in D2D communications	209
7.2.3. Investigations into future mobile networks	210
7.3. The context for machine learning and deep learning.	210
7.3.1. Overview of deep learning and its application	212
7.3.2. Types of machine learning	213
7.3.3. Linear regression and classification	213
7.4. Dynamic discovery	215
7.4.1. Real-time prediction of user density	216
7.4.2. The dynamic discovery algorithm	217
7.5. Experimental results.	218
7.5.1. General hypotheses	218
7.5.2. Traffic with low user density	219
7.5.3. Traffic with high user density	219
7.6. Conclusion	222
7.7. References	222

Chapter 8. The Impact of Cognitive Radio on Green Networking: The Learning-through-reinforcement Approach	227
Mohammed Salih BENDELLA and Badr BENMAMMAR	
8.1. Introduction	227
8.2. Green networking	228
8.2.1. Why should we reduce energy consumption?	228
8.2.2. Where can we reduce energy consumption?	228
8.2.3. Definition and objectives of green networking	229
8.3. Green strategies	230
8.3.1. Consolidation of resources	230
8.3.2. Selective connectivity	231
8.3.3. Virtualization	231
8.3.4. Energy-proportional computing	231
8.4. Green wireless networks	233
8.4.1. Energy efficiency in wireless networks	235
8.4.2. Controlling transmission power	236
8.5. How CR contributes to green networking	238
8.5.1. The principle behind CR	238
8.5.2. The cognition cycle	238
8.5.3. Green networking in CR networks	240
8.6. Learning through reinforcement by taking into account energy efficiency during opportunistic access to the spectrum	243
8.6.1. Formulating the problem	245
8.6.2. Comparison between CR and Q_learning enabled CR	247
8.7. Conclusion	248
8.8. References	249
List of Authors	253
Index	255