

# Table des matières

<b>Chapitre 1. Sélection multicritère des paramètres de transmission dans l’IoT</b> . . . . .	1
Sinda BOUSSEN, Mohamed-Aymen CHALOUF et Francine KRIEF	
1.1. Introduction. . . . .	1
1.2. Changement de réseau d’accès dans l’IoT. . . . .	2
1.3. Transfert de spectre dans l’IoT . . . . .	3
1.4. Module de décision multicritère pour un transfert de spectre efficace dans l’IoT . . . . .	4
1.4.1. Architecture générale. . . . .	4
1.4.2. Organigramme de prise de décision . . . . .	9
1.4.3. Évaluation des performances . . . . .	15
1.5. Conclusion . . . . .	22
1.6. Bibliographie. . . . .	22
<b>Chapitre 2. Utilisation de l’apprentissage par renforcement pour la gestion des accès massifs dans les réseaux NB-IoT.</b> . . . . .	27
Yassine HADJADJ-AOUL et Soraya AIT-CHELLOUCHE	
2.1. Introduction. . . . .	27
2.2. Fondamentaux de la norme NB-IoT . . . . .	29
2.2.1. Déploiement et cas d’usage . . . . .	29
2.2.2. Principes de transmissions. . . . .	30
2.2.3. Procédure d’accès aléatoire à la ressource radio . . . . .	33
2.3. État de l’art . . . . .	37
2.4. Modèle pour l’accès des terminaux IoT . . . . .	39
2.5. Contrôleur d’accès pour les terminaux IoT basé sur l’apprentissage par renforcement . . . . .	42

2.5.1. Formulation du problème . . . . .	43
2.5.2. Système de régulation des arrivées. . . . .	44
2.6. Évaluation des performances . . . . .	46
2.7. Conclusion . . . . .	50
2.8. Bibliographie. . . . .	51

### **Chapitre 3. Optimisation des performances de l'IoT : une approche basée sur la radio intelligente . . . . . 57**

Badr BENMAMMAR

3.1. Introduction. . . . .	57
3.2. <i>Internet of Things</i> (IoT). . . . .	58
3.2.1. Définition de l'IoT . . . . .	58
3.2.2. Applications de l'IoT. . . . .	59
3.2.3. Défis de l'IoT . . . . .	60
3.2.4. Technologies habilitantes de l'IoT. . . . .	61
3.3. Radio intelligente . . . . .	64
3.3.1. Définition de la radio intelligente . . . . .	64
3.3.2. Motivations de l'utilisation de la radio intelligente dans l'IoT . . . . .	66
3.3.3. Défis de l'utilisation de la radio intelligente dans l'IoT . . . . .	68
3.4. Conclusion . . . . .	73
3.5. Bibliographie. . . . .	73

### **Chapitre 4. Optimisation de la consommation énergétique des dispositifs IoT . . . . . 79**

Ahmad KHALIL, Nader MBAREK et Olivier TOGNI

4.1. Introduction. . . . .	79
4.2. L'optimisation énergétique. . . . .	80
4.2.1. Définitions . . . . .	80
4.3. Techniques d'optimisation de la consommation énergétique. . . . .	81
4.3.1. L'algorithme A étoile . . . . .	81
4.3.2. La logique floue. . . . .	83
4.4. Optimisation énergétique dans l'IoT . . . . .	85
4.4.1. Caractéristiques de l'IoT. . . . .	85
4.4.2. Challenges de l'optimisation énergétique. . . . .	87
4.4.3. Travaux de recherche concernant l'optimisation énergétique dans l'IoT . . . . .	87
4.5. <i>Framework</i> d'optimisation énergétique autonome dans l'IoT . . . . .	89
4.5.1. Gestion autonome. . . . .	89
4.5.2. Spécification du <i>framework</i> . . . . .	92

4.6. Proposition d'une méthode d'auto-optimisation de la consommation énergétique dans l'IoT . . . . .	93
4.6.1. Modèle de logique floue . . . . .	94
4.6.2. Algorithme de prise de décision . . . . .	98
4.6.3. Évaluation de l'auto-optimisation énergétique dans l'IoT . . . . .	100
4.7. Conclusion . . . . .	104
4.8. Bibliographie . . . . .	104

## **Chapitre 5. Vers une gestion intelligente de la qualité de service dans l'IoT : cas d'un réseau *Low Rate WPAN* . . . . .** 107

Guillaume LE GALL, Georgios Z. PAPAPOPOULOS,  
Mohamed-Aymen CHALOUF et Nicolas MONTAVONT

5.1. Introduction . . . . .	108
5.2. Rapide tour d'horizon de l'IoT . . . . .	110
5.2.1. La pile micro-IPv6 . . . . .	110
5.2.2. Les technologies pour l'IoT . . . . .	112
5.2.3. IoT et qualité de service . . . . .	117
5.3. Approche IEEE 802.15.4 TSCH . . . . .	118
5.4. Ordonnancement des transmissions . . . . .	120
5.4.1. Considérations d'ordre général . . . . .	120
5.4.2. L'ordonnancement dans la littérature . . . . .	121
5.5. Routage et RPL . . . . .	123
5.5.1. Routage . . . . .	123
5.5.2. RPL . . . . .	124
5.5.3. Multichemin . . . . .	125
5.6. Approche combinée basée sur 802.15.4 TSCH et RPL multichemin . . . . .	126
5.6.1. <i>Automatic Repeat reQuest</i> (ARQ) . . . . .	128
5.6.2. <i>Replication and Elimination</i> (RE) . . . . .	128
5.6.3. <i>Overhearing</i> (OH) . . . . .	130
5.7. Conclusion . . . . .	131
5.8. Bibliographie . . . . .	132

## **Chapitre 6. Adaptation de la qualité de service dans les dispositifs IoT à récupération d'énergie . . . . .** 137

Matthieu GAUTIER et Olivier BERDER

6.1. Vers une autonomie énergétique des réseaux de capteurs . . . . .	139
6.1.1. Récupération et gestion d'énergie . . . . .	139
6.1.2. État de l'art des gestionnaires d'énergie . . . . .	143

6.2. Fuzzyman : utilisation de la logique floue . . . . .	145
6.2.1. Conception de Fuzzyman . . . . .	145
6.2.2. Évaluation de Fuzzyman . . . . .	150
6.2.3. Conclusion . . . . .	151
6.3. RLman : utilisation de l'apprentissage par renforcement . . . . .	153
6.3.1. Formulation du problème de gestion de l'énergie récupérée. . . . .	153
6.3.2. Algorithme de RLMan . . . . .	155
6.3.3. Évaluation de RLMan . . . . .	158
6.3.4. Conclusion . . . . .	160
6.4. Vers des nœuds LoRa autonomes en énergie . . . . .	160
6.4.1. Architecture de récupération d'énergie multisource. . . . .	162
6.4.2. Application de la gestion d'énergie à des nœuds LoRa. . . . .	162
6.5. Conclusion . . . . .	163
6.6. Bibliographie. . . . .	165

## **Chapitre 7. Adaptation du contrôle d'accès pour la sécurité de l'IoT.**

<b>Chapitre 7. Adaptation du contrôle d'accès pour la sécurité de l'IoT.</b> . . . . .	<b>169</b>
Ahmad KHALIL, Nader MBAREK et Olivier TOGNI	
7.1. Introduction. . . . .	169
7.2. Définition des services de sécurité dans l'IoT . . . . .	170
7.2.1. Identification et authentification dans l'IoT . . . . .	170
7.2.2. Contrôle d'accès dans l'IoT. . . . .	171
7.2.3. Confidentialité dans l'IoT . . . . .	172
7.2.4. Intégrité dans l'IoT . . . . .	173
7.2.5. Non-répudiation dans l'IoT . . . . .	173
7.2.6. Disponibilité dans l'IoT . . . . .	174
7.3. Technologies de contrôle d'accès. . . . .	174
7.4. Contrôle d'accès dans l'IoT . . . . .	178
7.4.1. Travaux de recherche concernant l'extension des modèles de contrôle d'accès pour l'IoT . . . . .	178
7.4.2. Travaux de recherche concernant l'adaptation des systèmes et des technologies de contrôle d'accès pour l'IoT . . . . .	180
7.5. <i>Framework</i> de contrôle d'accès dans l'IoT . . . . .	183
7.5.1. Architecture IoT. . . . .	184
7.5.2. Spécification du contrôle d'accès IoT-MAAC. . . . .	186
7.6. Conclusion . . . . .	201
7.7. Bibliographie. . . . .	202

## **Chapitre 8. Apports de la biométrie et de l'intelligence artificielle dans la sécurisation de l'IoT . . . . . 205**

Amal SAMMOUD, Omessaad HAMDI, Mohamed-Aymen CHALOUF  
et Nicolas MONTAVONT

8.1. Introduction. . . . .	205
8.2. Sécurité et vie privée dans l'IoT . . . . .	206
8.3. Authentification basée sur la biométrie . . . . .	207
8.3.1. La biométrie . . . . .	207
8.3.2. Les techniques de la biométrie . . . . .	208
8.3.3. Les différentes propriétés de la biométrie. . . . .	209
8.3.4. Fonctionnement d'un système biométrique. . . . .	210
8.3.5. Performances des systèmes . . . . .	210
8.4. Techniques d'authentification multifacteur basées sur la biométrie. . . . .	211
8.4.1. Authentification multifacteur . . . . .	211
8.4.2. Exemples d'approches d'authentification multifacteur pour la sécurisation de l'IoT . . . . .	213
8.4.3. Présentation de l'approche de Sammoud <i>et al.</i> . . . . .	214
8.5. Techniques d'authentification à base de biométrie et d'apprentissage automatique . . . . .	222
8.5.1. Algorithmes d'apprentissage automatique . . . . .	222
8.5.2. Exemples d'approches d'authentification à base de biométrie et d'apprentissage automatique. . . . .	223
8.5.3. Approches d'authentification à base d'ECG et d'apprentissage automatique. . . . .	224
8.6. Enjeux et limites . . . . .	227
8.6.1. Qualité des données biométriques . . . . .	227
8.6.2. Non-révocabilité des données biométriques . . . . .	227
8.6.3. Sécurité des systèmes biométriques . . . . .	227
8.7. Conclusion . . . . .	227
8.8. Bibliographie. . . . .	228

## **Chapitre 9. Gestion dynamique des identités et des accès dans l'IoT : une approche basée sur la *blockchain*. . . . . 231**

Léo MENDIBOURE, Mohamed-Aymen CHALOUF et Francine KRIEF

9.1. Introduction. . . . .	231
9.2. Contexte. . . . .	233
9.2.1. La gestion intelligente des identités et des accès. . . . .	233
9.2.2. La <i>blockchain</i> . . . . .	234

9.3. La *blockchain* au service de la gestion intelligente des identités et des accès. . . . . 236

    9.3.1. Une nouvelle architecture intégrant la *blockchain*. . . . . 236

    9.3.2. De nombreux bénéfiques . . . . . 238

9.4. Enjeux . . . . . 243

    9.4.1. Passage à l'échelle . . . . . 244

    9.4.2. Sécurité de la *blockchain* . . . . . 244

    9.4.3. Consommation énergétique . . . . . 245

    9.4.4. Définition d'algorithmes de consensus propres à l'intelligence artificielle . . . . . 245

9.5. Conclusion . . . . . 246

9.6. Bibliographie. . . . . 247

**Chapitre 10. Adaptation du niveau de sécurité des applications IoT . . . . . 251**

Tidiane SYLLA, Mohamed-Aymen CHALOUF et Francine KRIEF

10.1. Introduction . . . . . 251

10.2. Définitions et caractéristiques . . . . . 252

    10.2.1. Définitions . . . . . 252

    10.2.2. Caractéristiques . . . . . 253

10.3. Applications de l'IoT . . . . . 254

10.4. Architectures de l'IoT . . . . . 255

10.5. Sécurité, confiance et protection de la vie privée dans les applications IoT. . . . . 256

    10.5.1. Généralités . . . . . 256

    10.5.2. Services de sécurité . . . . . 257

    10.5.3. Sécurité des communications . . . . . 259

    10.5.4. Confiance . . . . . 261

    10.5.5. Protection de la vie privée . . . . . 262

10.6. Adaptation du niveau de sécurité dans l'IoT. . . . . 263

    10.6.1. Sensibilité au contexte . . . . . 263

    10.6.2. Sécurité sensible au contexte . . . . . 265

    10.6.3. Architecture de sécurité et protection de la vie privée sensibles au contexte conçue suivant l'approche « as a service ». . . . . 267

10.7. Conclusion . . . . . 270

10.8. Bibliographie . . . . . 271

<b>Chapitre 11. Techniques de <i>Moving Target Defense</i> pour l’IoT . . .</b>	<b>277</b>
Renzo E. NAVAS, Laurent TOUTAIN et Georgios Z. PAPADOPOULOS	
11.1. Introduction . . . . .	278
11.2. Contexte . . . . .	279
11.2.1. Brève chronologie de la <i>Moving Target Defense</i> (MTD) . . . . .	279
11.2.2. Principes fondamentaux de la MTD, techniques et taxonomie . . . . .	280
11.3. Travaux connexes . . . . .	281
11.3.1. Enquêtes sur les techniques de MTD . . . . .	281
11.3.2. <i>Frameworks</i> pour systèmes IoT liés au concept MTD . . . . .	282
11.4. La MTD pour l’IoT : une enquête qualitative . . . . .	282
11.4.1. Data : mécanisme MTD contre les attaques par canal auxiliaires basé sur la renégociation des clés cryptographiques . . . . .	282
11.4.2. <i>Software</i> . . . . .	283
11.4.3. Environnement d’exécution . . . . .	284
11.4.4. Plate-forme : diversification par reconfiguration des micrologiciels des nœuds IoT . . . . .	285
11.4.5. Réseaux . . . . .	286
11.4.6. Résumé de la section . . . . .	289
11.5. Composants de réseau dans l’IoT : un vaste domaine pour la MTD . .	289
11.5.1. Couche physique . . . . .	290
11.5.2. Couche liaison . . . . .	291
11.5.3. Couche réseau OSI . . . . .	292
11.5.4. Couche transport . . . . .	293
11.5.5. Couche application . . . . .	294
11.5.6. Résumé de la section . . . . .	295
11.6. Un <i>framework</i> MTD pour l’IoT . . . . .	295
11.6.1. Proposition : composantes . . . . .	296
11.6.2. Instanciation : <i>UDP Port Hopping</i> . . . . .	297
11.7. Discussion et axes de recherche future . . . . .	298
11.8. Conclusion . . . . .	299
11.9. Bibliographie . . . . .	300
 <b>Liste des auteurs . . . . .</b>	 <b>305</b>
 <b>Index . . . . .</b>	 <b>307</b>