

IC2

Réseaux et télécoms

Les systèmes embarqués communicants

mobilité, sécurité, autonomie

sous la direction de
Francine Krief

hermes

Lavoisier

Table des matières

Introduction générale	19
Francine KRIEF	
Chapitre 1. Introduction aux systèmes embarqués	25
Patrice KADIONIK	
1.1. Introduction	25
1.2. Système embarqué : une définition	26
1.3. Caractéristiques d'un système embarqué	28
1.4. L'importance de la loi de Moore	30
1.5. Les systèmes embarqués et le système sur silicium	32
1.6. Les systèmes embarqués et les communications	34
1.7. Les systèmes embarqués et la sécurité	35
1.8. Les systèmes embarqués et les contraintes temporelles	36
1.9. Les systèmes embarqués et les logiciels libres	39
1.10. Les systèmes embarqués et leur conception	40
1.11. Un exemple de conception d'un système embarqué multimédia	42
1.12. Conclusion	46
1.13. Bibliographie	46
Chapitre 2. Routage à qualité de service dans les réseaux <i>ad hoc</i> mobiles	49
Zoubir MAMMARI	
2.1. Introduction	49
2.2. Réseaux <i>ad hoc</i> mobiles : concepts, caractéristiques, challenges	51
2.2.1. Concepts et principes de base	51

2.2.2. Limites et challenges	52
2.2.3. Protocoles MAC pour les réseaux <i>ad hoc</i>	54
2.2.4. Mobilité et localisation de nœuds	55
2.2.4.1. Localisation de nœuds mobiles.	55
2.2.4.2. Modèles de mobilité	56
2.3. Routage à QoS : considérations générales.	56
2.3.1. Fonctions d'un protocole de routage.	57
2.3.1.1. Collecte et dissémination des informations d'état.	57
2.3.1.2. Sélection de chemin	58
2.3.1.3. Maintenance et réparation de chemins	58
2.3.2. Classification des protocoles de routage	59
2.3.2.1. Routage par la source, saut par saut et hiérarchique	59
2.3.2.2. Routage <i>unicast</i> , <i>multicast</i> et <i>anycast</i>	60
2.3.2.3. Redondance de chemins et chemins disjoints	60
2.3.2.4. Routage intradomaine et interdomaine	61
2.3.3. Propriétés attendues des protocoles de routage.	61
2.3.4. Problèmes de routage à QoS	62
2.4. Protocoles de routage <i>best effort</i> dans les MANETs.	64
2.4.1. Critères de classification des protocoles de routage.	65
2.4.1.1. Stratégie de découverte et mise à jour des chemins.	65
2.4.1.2. Structure du réseau.	67
2.4.1.3. Utilisation d'informations géographiques	67
2.4.1.4. Utilisation d'informations du passé ou du futur	68
2.4.1.5. Critères de sélection de liens et de chemins	68
2.4.2. Présentation de protocoles de routage	68
2.4.2.1. Protocole DSDV	69
2.4.2.2. Protocole OLSR	69
2.4.2.3. Protocole AODV	70
2.4.2.4. Protocole ZRP	70
2.4.2.5. Protocole HSR	71
2.4.2.6. Protocole LAR	71
2.5. Routage à QoS dans les MANETs	72
2.5.1. Approches pour le routage à QoS	73
2.5.2. Réserveation de ressources	74
2.5.2.1. Routage à QoS avec réserveation de ressources	75
2.5.2.2. Routage à QoS sans réserveation de ressources	75
2.5.3. Exemples de méthodes de réserveation.	76
2.5.3.1. Réserveation synchrone.	76
2.5.3.2. Méthodes de réserveation asynchrone de <i>slots</i>	77
2.5.4. Modèles d'estimation.	80
2.5.4.1. Estimation de bande passante disponible.	81

2.5.4.2. Estimation de délai	83
2.5.5. Présentation des principaux protocoles de routage à QoS	84
2.6. Conclusion	85
2.7. Bibliographie	88
Chapitre 3. La gestion autonome des réseaux de capteurs <i>ad hoc</i>	93
Francine KRIEF	
3.1. Introduction	93
3.2. Les réseaux de capteurs sans fil	94
3.2.1. Les domaines d'application des réseaux de capteurs	94
3.2.2. Les principaux constituants d'un capteur	95
3.2.3. L'importance de l'énergie dans les réseaux de capteurs	96
3.2.4. Les technologies de transmission	97
3.2.5. Les algorithmes de routage	98
3.2.6. Les principales offres commerciales	102
3.2.7. Les principaux enjeux	103
3.2.8. Les projets portant sur les réseaux de capteurs	104
3.3. Les réseaux de capteurs autonomes	105
3.3.1. Les réseaux autonomes	105
3.3.2. L'autoconfiguration des réseaux de capteurs	106
3.3.3. L'autoréparation des réseaux de capteurs	107
3.3.4. L'auto-optimisation des réseaux de capteurs	108
3.3.5. L'autoprotection des réseaux de capteurs	109
3.3.6. Les projets portant sur l'autonomie dans les réseaux de capteurs	111
3.4. Un exemple d'autoconfiguration	112
3.4.1. L'optimisation de l'énergie et la classification numérique	112
3.4.2. L'algorithme d'optimisation de l'énergie LEA2C	114
3.4.3. L'évaluation de performance de l'algorithme LEA2C	115
3.4.4. Les évolutions de l'algorithme LEA2C	117
3.5. Conclusion	117
3.6. Bibliographie	118
Chapitre 4. La technologie RFID.	121
Vincent GUYOT	
4.1. Introduction	121
4.2. Les systèmes d'identification automatiques	121
4.2.1. Le code-barres	121
4.2.2. Les systèmes optiques de reconnaissance des caractères (OCR)	122
4.2.3. L'identification biométrique	122

4.2.3.1. L'identification vocale	122
4.2.3.2. Les empreintes digitales	123
4.2.4. Les cartes à puce	123
4.2.5. Les systèmes RFID	124
4.3. Les composants d'un système RFID	124
4.4. Les différents types de systèmes RFID	125
4.4.1. Les systèmes RFID bas de gamme	125
4.4.2. Les systèmes RFID milieu de gamme	126
4.4.3. Les systèmes RFID haut de gamme	127
4.5. Les gammes de fréquences radio	127
4.6. La sécurité des informations	127
4.6.1. Authentification mutuelle symétrique	128
4.6.2. Authentification à l'aide de clefs dérivées	129
4.6.3. Le chiffrement du transfert	130
4.7. Les normes en vigueur	131
4.7.1. L'identification animale	131
4.7.2. Les cartes à puce sans contact	132
4.7.3. L'identification de container	132
4.7.4. La gestion des marchandises	132
4.7.4.1. Les normes ISO	132
4.7.4.2. L'initiative GTAG	133
4.8. Exemples de réalisations	133
4.8.1. Les cartes à puce sans contact	133
4.8.2. Accès aux transports publics	134
4.8.3. Accès aux pistes de ski	135
4.8.4. Contrôle d'accès	136
4.8.4.1. Les systèmes connectés	136
4.8.4.2. Les systèmes déconnectés	136
4.8.4.3. Les transpondeurs	137
4.8.5. Les systèmes de transport	138
4.8.5.1. Eurobalise S21	138
4.8.5.2. Le transport de containers internationaux	138
4.8.6. L'identification animale	139
4.8.6.1. Gérer le cheptel	139
4.8.6.2. Les courses de pigeons voyageurs	140
4.8.7. Les évènements sportifs	140
4.9. Conclusion	141
4.10. Bibliographie	141

Chapitre 5. La sécurité matérielle des systèmes embarqués	143
Lilian BOSSUET et Guy GOGNIAT	
5.1. Introduction.	143
5.2. Systèmes embarqués et problématique de sécurité.	144
5.2.1. Contraintes de conception des systèmes embarqués.	144
5.2.2. La problématique de sécurité des systèmes embarqués.	146
5.2.3. Les principales menaces de sécurité	147
5.3. Sécurité des systèmes et des données.	150
5.3.1. Principe de sécurité en profondeur (projet ICTER)	150
5.3.2. Caractéristiques d'un système matériel embarqué sécurisé	152
5.3.3. Solutions matérielles de sécurité	153
5.3.3.1. Solutions matérielles de sécurité au niveau système	153
5.3.3.2. Solutions matérielles de sécurité au niveau architecture	154
5.3.3.3. Solutions matérielles de sécurité au niveau logique	156
5.3.3.4. Solutions matérielles de sécurité au niveau physique	157
5.4. Architectures matérielles sécurisées pour les systèmes embarqués	158
5.4.1. Architectures de protection du logiciel et des données embarqués	158
5.4.2. Architectures de protection de la propriété intellectuelle.	162
5.4.3. Crypto-architecture pour la protection des communications et les applications de sécurité	165
5.4.4. Un cas d'étude : SANES une architecture matérielle sécurisée reconfigurable.	167
5.5. Conclusion	169
5.6. Bibliographie.	170
Chapitre 6. La sécurité des communications dans les systèmes embarqués	175
Mohamed Aymen CHALOUF	
6.1. Introduction.	175
6.2. Sécurité des communications	176
6.2.1. Attaques de sécurité	176
6.2.1.1. Les attaques passives	176
6.2.1.2. Les attaques actives	177
6.2.2. Services de sécurité.	177
6.2.2.1. Authentification	178
6.2.2.2. Contrôle d'accès	178
6.2.2.3. Confidentialité des données.	178
6.2.2.4. Intégrité des données.	178
6.2.2.5. Non-répudiation	178

6.2.2.6. Disponibilité.	179
6.2.3. Notions de cryptographie	179
6.2.3.1. Confidentialité des messages	179
6.2.3.2. Authentification des messages	182
6.2.4. Techniques de sécurité	183
6.2.4.1. Le protocole IPsec	183
6.2.4.2. Le protocole TLS.	186
6.3. Sécurité des communications dans l'embarqué.	192
6.3.1. Spécificités des systèmes embarqués	192
6.3.2. Problèmes posés lors de l'implémentation de la sécurité dans l'embarqué.	193
6.3.2.1. Génération des valeurs aléatoires	193
6.3.2.2. Cryptographie à clé publique	194
6.3.2.3. Gestion de l'espace mémoire	194
6.3.2.4. Temps de négociation des paramètres de sécurité.	195
6.3.3. Adaptation des techniques de sécurité pour l'embarqué	195
6.3.3.1. Génération des valeurs aléatoires à partir d'un dossier (<i>File-Based</i>)	195
6.3.3.2. Accélération de la cryptographie à clé publique.	195
6.3.3.3. Minimisation de l'espace mémoire utilisé	196
6.3.3.4. Optimiser le temps de négociation des paramètres de sécurité	197
6.3.4. Un mini serveur <i>web</i> implémentant SSL/TLS	198
6.3.4.1. La plate-forme IPC@CHIP.	198
6.3.4.2. Portage de la bibliothèque « OpenSSL » sur la plate-forme.	199
6.3.4.3. Réécriture du code	199
6.3.5. Un exemple d'utilisation de SSL/TLS dans l'embarqué	199
6.4. Conclusion	200
6.5. Bibliographie.	200

Chapitre 7. L'adaptation *Cross-Layer* pour les services multimédias dans les systèmes embarqués communicants de type 802.11.

203

Ismaïl DJAMA

7.1. Introduction.	203
7.2. Les limites de la structuration en couche	205
7.2.1. La couche d'accès réseaux	206
7.2.2. La couche réseau	209
7.2.3. La couche transport.	211
7.2.4. La couche application	212

7.3. Le concept de <i>Cross-Layer</i>	213
7.3.1. Les approches ascendantes	215
7.3.2. Les approches descendantes	218
7.3.3. Les approches mixtes	219
7.4. Conclusion	224
7.5. Bibliographie	225
Chapitre 8. Apport de l'architecture DTN pour les réseaux mobiles <i>ad hoc</i>	229
Olfa SAMET	
8.1. Introduction	229
8.2. Les réseaux mobiles <i>ad hoc</i>	230
8.2.1. Définition	230
8.2.2. Les caractéristiques des réseaux mobiles <i>ad hoc</i>	231
8.2.3. Les contraintes des réseaux mobiles <i>ad hoc</i>	231
8.3. <i>Challenged Networks</i>	232
8.3.1. Liens de transmission	233
8.3.2. Architecture du réseau	234
8.3.3. Terminaux utilisateurs	234
8.3.4. Protocoles de communication	234
8.4. Les réseaux tolérants aux délais : DTN	235
8.4.1. Définition et objectifs	235
8.4.2. Spécificités de l'architecture DTN	237
8.4.2.1. La commutation de <i>Bundles</i> : <i>Store and Forward</i>	237
8.4.2.2. Les régions et les nœuds DTN	239
8.4.2.3. Les services de la couche <i>Bundle</i>	241
8.4.2.4. La sécurité	243
8.4.3. Modèle protocolaire d'un réseau DTN	245
8.4.4. Le routage dans un réseau DTN	246
8.4.4.1. Problématique de routage dans un réseau DTN	246
8.4.4.2. Les algorithmes de routage	248
8.4.4.3. Protocoles de routage DTN	250
8.5. Apport des DTN dans les réseaux mobiles <i>ad hoc</i>	255
8.5.1. Liens à délai important	256
8.5.2. Résolution des problèmes liés aux taux de pertes élevés	257
8.6. Conclusion	257
8.7. Bibliographie	257

Chapitre 9. Les interfaces intelligentes et les communications mobiles . . . 259

Badr BENMAMMAR et Zeina JRAD

9.1. Introduction	259
9.2. Assister l'utilisateur dans l'accès aux nouveaux services de l'internet	261
9.2.1. Les interfaces utilisateur intelligentes	261
9.2.2. Caractéristiques générales d'une interface intelligente	262
9.3. Modélisation des comportements utilisateurs	263
9.3.1. Détermination des données contextuelles d'un profil	264
9.3.2. Définition générale des caractéristiques pertinentes	265
9.4. Synthèse sur les réseaux mobiles et sans fil	267
9.4.1. La technologie WiMAX	269
9.4.2. Le WiMAX et la qualité de service	271
9.4.3. Le WiMAX mobile et la 4G.	272
9.5. Références d'interfaces intelligentes pour l'accès aux réseaux mobiles.	275
9.5.1. Prédiction de la mobilité des utilisateurs	275
9.5.2. Négociation de la QoS pour un utilisateur mobile.	277
9.6. Conclusion	282
9.7. Bibliographie	283

**Chapitre 10. Routage et gestion de la mobilité
dans les réseaux personnels** 289

Usman JAVAID et Francine KRIEF

10.1. Introduction	289
10.2. Les environnements personnels	290
10.2.1. Réseaux personnels	291
10.2.2. Fédération de réseaux personnels	292
10.2.3. Environnement personnel ubiquitaire	292
10.3. Le routage dans les environnements personnels	294
10.3.1. Spécificités des réseaux personnels.	294
10.3.2. Le protocole de routage PNRP	295
10.3.3. Simulation	298
10.4. La découverte de passerelles	298
10.4.1. Découverte de passerelles dans les réseaux multisauts	298
10.4.2. Le protocole ADD.	299
10.4.3. Simulations.	300
10.5. Gestion de la mobilité	301
10.5.1. Gestion de la mobilité dans les réseaux personnels	301

10.5.2. Architecture de gestion de la mobilité	301
10.5.2.1. Le gestionnaire ULM.	301
10.5.2.2. Simulations	303
10.5.3. <i>Handover</i> multisauts sans couture	303
10.5.3.1. Le standard 802.21	304
10.5.3.2. Simulations	305
10.6. Conclusion	305
10.7. Bibliographie	306
Index	309