

RÉSEAUX
ET TÉLÉCOMS

Information - Commande - Communication

**La sécurité dans les réseaux
sans fil et mobiles 3**
technologies émergentes

sous la direction de

Hakima Chaouchi

Maryline Laurent-Maknavicius

Hermès

Lavoisier



La sécurité dans les réseaux sans fil et mobiles 3

technologies émergentes

sous la direction de

Hakima Chaouchi

Maryline Laurent-Maknavicius

hermes
Science
— PUBLICATIONS —

Lavoisier

Table des matières

Introduction	15
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
Chapitre 1. La sécurité dans les réseaux mobiles de nouvelle génération	21
Jérôme HÄRRI et Christian BONNET	
1.1. Introduction	21
1.2. <i>Session initiation protocol</i> (SIP)	24
1.2.1. Généralités SIP	24
1.2.2. Failles sécuritaires SIP	25
1.2.3. Sécuriser SIP	26
1.3. Voix par paquets (VoIP)	29
1.3.1. Failles sécuritaires VoIP	31
1.3.2. Sécurisation de VoIP	32
1.4. <i>IP multimedia subsystem</i> (IMS)	32
1.4.1. Architecture IMS	33
1.4.2. Sécurité dans IMS	35
1.4.3. Failles sécuritaires dans IMS	40
1.5. Sécurité 4G	40
1.6. Confidentialité	42
1.6.1. Terminologie	43
1.6.2. Protection des mécanismes d'interception	43
1.7. Conclusion	44
1.8. Bibliographie	45

Chapitre 2. Sécurité des réseaux mobiles IP	47
Jean-Michel COMBES, Daniel MIGAULT, Julien BOURNELLE, Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
2.1. Introduction	47
2.2. Problématique de sécurité liée à la mobilité	48
2.2.1. Vulnérabilités propres aux réseaux mobiles IP	49
2.2.2. Mécanismes de découvertes (éléments réseau comme routeur d'accès...)	50
2.2.3. Authenticité de la localisation du mobile	51
2.2.4. Protection des données (tunnels...)	52
2.3. La mobilité avec MIPv6	52
2.3.1. Fonctionnement de la mobilité IPv6 (MIPv6, HMIPv6, FMIPv6)	52
2.3.2. Initialisation de MIPv6	59
2.3.3. Mobilité des réseaux	63
2.3.4. Problèmes de sécurité ouverts	64
2.4. La mobilité avec Mobile IPv4	66
2.4.1. Le protocole	66
2.4.2. La sécurité	68
2.5. La mobilité avec MOBIKE	69
2.6. La mobilité avec HIP et NetLMM	72
2.6.1. HIP	72
2.6.2. NetLMM	74
2.7. Conclusion	76
2.8. Glossaire	77
2.9. Bibliographie	79
Chapitre 3. Sécurité des réseaux <i>ad hoc</i>	83
Jean-Marie ORSET et Ana CAVALLI	
3.1. Introduction	83
3.2. Motivations et domaines d'application	83
3.2.1. Motivations	83
3.2.2. Applications	86
3.3. Les protocoles de routage	87
3.3.1. Les protocoles proactifs	87
3.3.2. Les protocoles réactifs	89
3.3.3. Les protocoles hybrides	92
3.3.4. Performances	92
3.4. Les attaques sur le protocole de routage	92
3.4.1. Caractéristiques des réseaux <i>ad hoc</i>	93
3.4.2. Description des attaques	94

3.5. Les mécanismes de sécurité	99
3.5.1. Protections basiques	100
3.5.2. Les outils existants	102
3.5.3. Les architectures de gestion de clés	104
3.5.4. Protections utilisant la cryptographie asymétrique	110
3.5.5. Protections utilisant la cryptographie symétrique	115
3.5.6. Protections contre la modification des données	119
3.5.7. Protections contre les attaques de type « tunnel »	121
3.5.8. Mécanismes basés sur la réputation	122
3.6. L'autoconfiguration	126
3.6.1. Protocoles avec détection de conflits	128
3.6.2. Protocoles avec évitement de conflits	130
3.6.3. Autoconfiguration et sécurité	131
3.7. Conclusion	132
3.8. Bibliographie	133

Chapitre 4. Gestion de clés dans les réseaux *ad hoc* 139

Mohamed SALAH BOUASSIDA, Isabelle CHRISMENT et Olivier FESTOR

4.1. Introduction.	139
4.2. Etablissement de confiance dans les réseaux <i>ad hoc</i>	140
4.2.1. La technique de cryptographie à seuil	141
4.2.2. L'infrastructure à clé publique auto-organisée	143
4.2.3. L'accord de clé (<i>key agreement</i>) dans les Manet	145
4.2.4. Les identificateurs cryptographiques	147
4.2.5. La technique du <i>resurrecting duckling</i>	148
4.2.6. Synthèse	148
4.3. Gestion de clé de groupes dans les réseaux <i>ad hoc</i>	149
4.3.1. Les services de sécurité pour les communications de groupe.	151
4.3.2. Les défis de sécurité des communications de groupe dans les Manet	152
4.3.3. Métriques de comparaison.	154
4.3.4. Approche centralisée	154
4.3.5. Approche distribuée	161
4.3.6. Approche décentralisée	165
4.4. Discussions	170
4.4.1. Contraintes et prérequis	170
4.4.2. Services de sécurité.	171
4.4.3. Surcoût de calcul	174
4.4.4. Surcoût de stockage.	175
4.4.5. Surcoût de communications.	176
4.4.6. Vulnérabilités et faiblesses	176

4.5. Conclusion	177
4.6. Bibliographie	178
Chapitre 5. Sécurité dans les réseaux de capteurs sans fil	183
José-Marcos NOGUEIRA, Hao-Chi WONG, Antonio A.F. LOUREIRO, Chakib BEKARA, Maryline LAURENT-MAKNAVICIUS, Ana Paula RIBEIRO DA SILVA, Sérgio DE OLIVEIRA et Fernando A. TEIXEIRA	
5.1. Introduction.	183
5.2. Attaques sur les réseaux de capteurs sans fil et contre-mesures	185
5.2.1. Différentes formes d'attaques.	185
5.2.2. Mécanismes préventifs.	187
5.2.3. Détection d'intrus	187
5.2.4. Tolérance à l'intrusion	188
5.3. Mécanismes de prévention : authentification et protection des échanges	189
5.3.1. Notations des protocoles de sécurité.	189
5.3.2. Coût des protocoles de sécurité dans les capteurs	190
5.3.3. Protocole de sécurité SNEP	192
5.3.4. Protocole de sécurité μ TESLA	194
5.3.5. Protocole TinySec	196
5.3.6. Protocole de Zhu <i>et al.</i>	198
5.3.7. Synthèse des protocoles de sécurité	200
5.4. Etude de cas : détection d'intrus centralisée et passive	201
5.4.1. Stratégie de détection d'intrus	201
5.4.2. Modèle d'information	202
5.4.3. Stratégie d'analyse des informations.	203
5.4.4. Architecture du système de détection d'intrus	205
5.4.5. Un prototype d'IDS.	206
5.5. Etude de cas : détection d'intrus décentralisée	208
5.5.1. Modélisation des IDS distribués pour différentes configurations de RCSF	209
5.5.2. Algorithme utilisé.	210
5.5.3. Prototype utilisé dans la validation de la solution	211
5.5.4. Le simulateur	212
5.5.5. Expériences	213
5.5.6. Résultats	214
5.6. Etude de cas : tolérance à l'intrusion avec routes multiples	217
5.6.1. Routes alternatives	218
5.6.2. Algorithme de détection d'intrus	220
5.6.3. Evaluation de la solution.	223
5.7. Conclusion	227
5.8. Bibliographie.	229

Chapitre 6. Gestion de clés dans les réseaux de capteurs	233
Chakib BEKARA et Maryline LAURENT-MAKNAVICIUS	
6.1. Introduction	233
6.2. Introduction à la gestion de clés	234
6.3. Besoins en sécurité des RCSF	236
6.4. Problématique de gestion de clés dans les RCSF	237
6.5. Métriques pour l'évaluation des protocoles de gestion de clés dans les RCSF	240
6.6. Classification des protocoles de gestion de clés dans les RCSF	241
6.7. Notations et suppositions	242
6.8. Protocoles d'authentification d'une source de diffusion	243
6.8.1. Protocole de Perrig <i>et al.</i> μ TESLA	244
6.9. Protocoles probabilistes de gestion de clés	247
6.9.1. Protocole d'Eschenauer <i>et al.</i>	247
6.9.2. Autres approches	251
6.10. Protocoles déterministes de gestion de clés	251
6.10.1. Protocole de Dutertre <i>et al.</i>	251
6.10.2. Protocole de Bhuse <i>et al.</i>	254
6.10.3. Autres protocoles	257
6.11. Protocoles de gestion de clés hybrides	258
6.11.1. Protocole de Price <i>et al.</i>	258
6.11.2. Autres protocoles	261
6.12. Comparaison entre les protocoles de gestion de clés dans les RCSF	261
6.12.1. Type de clés gérées	261
6.12.2. Connectivité du réseau résultant	262
6.12.3. Coût en calcul	262
6.12.4. Coût en stockage	263
6.12.5. Coût en transmission	264
6.12.6. Analyse de la sécurité	264
6.12.7. Passage à l'échelle (<i>scalability</i>)	266
6.13. Conclusion	267
6.14. Bibliographie	268
Conclusion	271
Hakima CHAOUCHI et Maryline LAURENT-MAKNAVICIUS	
Index	273

Le traité Information, Commande, Communication répond au besoin de disposer d'un ensemble complet des connaissances et méthodes nécessaires à la maîtrise des systèmes technologiques.

Conçu volontairement dans un esprit d'échange disciplinaire, le traité IC2 est l'état de l'art dans les domaines suivants retenus par le comité scientifique :

- Réseaux et télécoms
- Traitement du signal et de l'image
- Information et science du vivant
- Informatique et systèmes d'information
- Systèmes automatisés et productique
- Management et gestion des STICS
- Cognition et traitement de l'information.

Chaque ouvrage présente aussi bien les aspects fondamentaux qu'expérimentaux. Une classification des différents articles contenus dans chacun, une bibliographie et un index détaillé orientent le lecteur vers ses points d'intérêt immédiats : celui-ci dispose ainsi d'un guide pour ses réflexions ou pour ses choix.

Les savoirs, théories et méthodes rassemblés dans chaque ouvrage ont été choisis pour leur pertinence dans l'avancée des connaissances ou pour la qualité des résultats obtenus dans le cas d'expérimentations réelles.