

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique
Ecole Doctorale d'Informatique



Thèse de Doctorat

En Informatique

Option

Réseaux et Systèmes Distribués

Thème

**Gestions de Clés dans les Réseaux de
Capteurs Sans-Fil**

Présenté par

Mohamed Lamine MESSAI

Devant le jury composé de :

Président : Djamil AISSANI, Professeur, Université de Béjaïa, Algérie
Rapporteur : Makhlouf ALIOUAT, Professeur, Université de Sétif 1, Algérie
Rapporteur : Hamida SEBA, Maître de Conférences HDR , Université Claude Bernard Lyon 1, France
Examineur : Nadjib BADACHE, Professeur, CERIST, Algérie
Examineur : Abdellah BOUKERRAM, Professeur, Université de Béjaïa, Algérie
Examineur : Mohamed BENMOHAMED, Professeur, Université de Constantine 2, Algérie
Examineur : Zibouda ALIOUAT, Maître de Conférences A, Université de Sétif 1, Algérie

Résumé

Jour après jour, les réseaux de capteurs sans-fil (RCSFs) s'intègrent dans les domaines nécessitant l'observation du monde physique. Cette intégration a fait l'émergence des RCSFs qui a ouvert la voie à une multitude de domaines de recherche. L'intérêt suscité par cette effervescence d'investigation préconise de larges champs d'application dans un avenir proche. Toutefois, beaucoup d'obstacles inhérents à leurs spécificités doivent être surmontés avant de pouvoir atteindre leur maturité. Parmi ces entraves, le problème de sécurité se pose avec acuité et doit être solutionné de manière appropriée et en conformité avec les caractéristiques particulières des RCSFs. Ces caractéristiques contraignantes s'observent dans la limitation des ressources telles que : l'énergie, la puissance de calcul, la bande passante et l'espace mémoire. En raison de ces contraintes et de leur déploiement dans des environnements sans surveillance et hostiles, les différents nœuds capteurs d'un RCSF sont vulnérables à la compromission et susceptibles d'une violation physique. De plus, l'utilisation des transmissions sans-fil rend les RCSFs perméables à des malveillances de toutes sortes, et constitue un véritable challenge de sécurité à relever. Notre thèse contribue au domaine de gestion de clés dans les RCSFs, qui est le cœur de tout système de sécurité : nous présentons en premier lieu un état de l'art des RCSFs et des protocoles de gestion de clés proposés pour ces réseaux. Comme conséquence, nous proposons un nouveau protocole de gestion de clés appelé STKM (Tree-Based Protocol for Key Management in Wireless Sensor Networks), et un autre nommé SKM (Sequence Based Key Management in Wireless Sensor Networks). La dernière contribution concerne la proposition d'un protocole appelé SEAC (a Self-Stabilizing Energy Aware Clustering Scheme for Sensor Networks) pour l'organisation du RCSF en *clusters*. Notre idée est de concevoir un schéma de gestion de clés sur cette organisation des noeuds capteurs .

Mots clés : Conservation d'énergie, Réseaux de capteurs sans-fil, Sécurité, Cryptographie, Gestion de clés.

Abstract

During the last few years, wireless sensor networks (WSNs) are integrated in areas that necessitate the observation of physical world. This integration made the emergence of WSNs, and paved the way for a variety of research domains. WSNs consist of small nodes with sensing, computation, and wireless communication capabilities and expected to play an essential role in the upcoming age of pervasive computing. However, many obstacles inherent to their specificities must be overcome before reaching their maturity. Among these obstacles, the security problem is acute and needs to be addressed appropriately and according to characteristics of WSNs. These characteristics are observed in the limited resources such as energy, computing power, bandwidth and storage space. WSNs are generally deployed in hostile environments and sensor nodes are prone to node compromise attacks and physical violation. In addition, the use of wireless transmissions makes WSNs permeable to malware of all kinds, and security a real challenge. This thesis contributes to the field of key management in WSNs, which is the heart of every security system : first we present a state of the art of WSNs and

key management protocols proposed for these networks. As a consequence, we propose a new key management protocol called STKM (Tree-Based Protocol for Key Management in Wireless Sensor Networks), and another named SKM (Sequence Based Key Management in Wireless Sensor Networks). The last contribution relates to the use of the clustering technique to organize the WSN for energy saving problem. We propose a new clustering scheme ; SEAC (Self-Stabilizing Energy Aware Clustering Scheme for Sensor Networks), our idea is to design a key management scheme adapted to SEAC.

Keywords : Wireless sensr networks, Security, Cryptography, Key management, energy saving.

Table des matières

Table des matières	
Liste des figures	iv
Liste des tableaux	v
Introduction générale	1
1 Généralité sur les réseaux de capteurs sans-fil	4
1.1 Introduction	4
1.2 Les réseaux sans-fil	5
1.2.1 Réseaux ad hoc	5
1.2.2 Réseaux de capteurs sans-fil (RCSF)	7
1.2.2.1 Qu'est ce qu'un capteur (senseur) ?	7
1.2.2.2 Définition d'un RCSF	7
1.2.2.3 Objectifs de base des RCSFs	8
1.2.2.4 Types des RCSFs	8
1.3 Architecture de base d'un capteur	9
1.4 Architecture d'un RCSF	10
1.5 La pile protocolaire dans un RCSF	11
1.5.1 La couche physique	12
1.5.2 La couche liaison	12
1.5.3 La couche réseau	13
1.5.4 La couche transport	13
1.5.5 La couche application	13
1.5.6 Le niveau de gestion d'énergie	13
1.5.7 Le niveau de gestion de mobilité	14
1.5.8 Le niveau de gestion des tâches	14
1.6 Application concrète d'un RCSF	14
1.7 Facteurs et contraintes conceptuelles des RCSFs	15
1.7.1 La tolérance aux fautes	15
1.7.2 L'échelle (<i>Scalability</i>)	15
1.7.3 Système d'exploitation	16
1.7.4 Sécurité physique limitée	16
1.7.5 Coût de production	16

1.7.6	L'environnement	17
1.7.7	La topologie du réseau	17
1.7.8	Les contraintes matérielles	17
1.7.9	Média de transmission	18
1.7.10	La connectivité	18
1.7.11	La consommation d'énergie	19
	1.7.11.1 Energie de capture	20
	1.7.11.2 Energie de traitements	20
	1.7.11.3 Energie de communication	20
1.8	Capteurs en images	21
1.9	Conclusion	21
2	La gestion de clés dans les RCSFs	23
2.1	Introduction	23
2.2	Analyse de vulnérabilité	24
	2.2.1 Vulnérabilité physique	24
	2.2.2 Vulnérabilité technologique	24
2.3	Contraintes influençant la sécurité dans un RCSF	25
2.4	Energie pour la sécurité	25
2.5	Défis de sécurité	25
2.6	Buts de sécurité	26
	2.6.1 Disponibilité	26
	2.6.2 Intégrité des données	26
	2.6.3 Confidentialité	26
	2.6.4 Fraîcheur	27
	2.6.5 Authentification	27
	2.6.6 Non répudiation	27
	2.6.7 Contrôle d'accès	27
2.7	Les attaques dans les RCSFs	27
2.8	Modèle de l'attaquant	31
	2.8.1 Attaquant puissant (<i>Strong attacker</i>)	31
	2.8.2 Un modèle réaliste d'attaquant	31
2.9	Problèmes de sécurité dans chaque couche [27]	31
	2.9.1 Couche physique	31
	2.9.2 Couche liaison	32
	2.9.3 Couche réseau	32
	2.9.4 Couche transport	33
2.10	La Gestion de clés dans les RCSFs	33
	2.10.1 But des protocoles de gestion de clés	34
2.11	Phases de la gestion de clés	35
2.12	Métriques d'évaluation	36
2.13	Classification	37
2.14	Utilisation de la cryptographie asymétrique	38
	2.14.1 TinyPK (Tiny Public Key) [35]	39
	2.14.2 TinyECC [36]	40

2.15	Utilisation de la cryptographie symétrique	41
2.15.1	Absence de pré-distribution de clés (<i>No key pre-distribution</i>)	41
2.15.1.1	<i>Key Infection</i> [42]	42
2.15.2	<i>Master key based pre-distribution</i>	42
2.15.2.1	<i>Broadcast session key negotiation protocol (BROSK)</i> [44]	43
2.15.2.2	<i>Lightweight Key Management System</i>	44
2.15.3	<i>Paire-wise key pre-distribution</i>	44
2.15.3.1	<i>Schéma de Blom</i>	45
2.15.3.2	Mécanisme de distribution de clés polynomiale	46
2.15.4	Participation de la station de base (<i>Base station participation</i>)	47
2.15.4.1	<i>SPINS : Security Protocols for Sensor Networks</i>	47
2.15.5	Pré-distribution probabiliste des clés (<i>Probabilistic key pre-distribution</i>)	50
2.15.5.1	Pré-distribution aléatoire de clés [56]	50
2.15.5.2	<i>key management using deployment knowledge</i> [53]	51
2.15.6	Gestion de clés dynamiques (<i>Dynamique key management</i>)	52
2.15.7	Gestion de clés hiérarchique (<i>Hierarchical key management</i>)	53
2.15.8	<i>Location-based keys</i>	54
2.16	Conclusion	55
3	Tree Based Protocol for Key Management in Wireless Sensor Networks [63]	56
3.1	Introduction	56
3.2	<i>STKM : A Spanning Tree-Based Key Management Solution for WSNs</i>	57
3.3	Hypothèses	57
3.4	Notation	59
3.5	Schéma proposé	59
3.5.1	Pré-distribution de clés	60
3.5.2	Construction de l'arbre	61
3.5.3	Maintenance de l'arbre et rafraîchissement de clés	62
3.6	Exemple applicatif	62
3.7	Evaluation	64
3.7.1	Complexité en mémoire	64
3.7.2	Complexité en communication	65
3.7.3	Capture de nœuds et passage à l'échelle	65
3.8	Simulation	65
3.9	Analyse de sécurité	71
3.10	Conclusion	72
4	A Lightweight Key Management Scheme for Wireless Sensor Networks [65]	73
4.1	Introduction	73
4.2	<i>SKM : Sequence-based Key Management for Wireless Sensor Networks</i>)	74
4.2.1	Schéma proposé	75
4.2.2	Etablissement de clés	76
4.2.3	Rafraîchissement de clés	78

4.2.4	L'ajout de nouveaux nœuds capteurs	79
4.3	Evaluation de performances	80
4.4	Analyse de sécurité	85
4.5	Conclusion	86
5	SEAC : a Self-Stabilizing Energy Aware Clustering Scheme for Sensor Networks [67]	87
5.1	Introduction	87
5.2	Travaux antérieurs	89
5.3	Self-stabilizing Energy-Aware Clustering Approach (SEAC)	91
5.3.1	Alliances basées énergie dans les graphes	92
5.3.2	L'algorithme SEAC	93
5.3.3	Formation de <i>clusters</i>	95
5.4	Evaluation	95
5.4.1	Modèle d'énergie	95
5.4.2	Résultats des simulations	96
5.5	Conclusion	100
	Conclusion Générale et Perspectives	101
	Bibliographie	103