

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

**Ecole nationale Supérieure d'Informatique (E.S.I)**

**Oued-Smar, Alger**

## **Projet Fin d'Etude**

Mémoire présenté pour l'obtention du diplôme d'

**INGENIEUR D'ETAT EN INFORMATIQUE**

Option : Systèmes d'informatiques (SIQ)

# **Thème :**

**Sécurisation du protocole de routage hiérarchique**

**LEACH dans les réseaux de capteurs sans fil**

### **Réalisé par :**

Mlle. BERRACHEDI Amel

Mlle. DIARBAKIRLI Amina

### **Encadré par :**

M. KHELLADI Lyes

Attaché de recherche

CERIST, Alger

Mme. YAHIAOUI Chafia

Maître de conférence

ESI, Alger

Promotion : 2008/2009

## Résumé

Les progrès récents dans les communications sans fil et le domaine de l'électronique ont permis le développement des micro-capteurs, moins coûteux et multifonctionnels. Ces caractéristiques ont permis de se projeter dans la naissance des réseaux de capteurs sans fil (RCSF), et de favoriser leur utilisation dans une multitude d'applications. Celles-ci nécessitent souvent un déploiement dans des environnements hostiles, où les nœuds ainsi que les liens de communication sont continuellement exposés à des menaces importantes.

Par conséquent, les services offerts par les RCSF doivent garantir le niveau de sécurité requis par l'application. Cet objectif est compliqué d'avantage à cause de l'absence d'infrastructure de communication fixe, en plus de limitations matérielles imposées par la taille miniaturisée des capteurs.

Dans cette optique, nous nous sommes intéressés à la sécurisation du protocole LEACH, l'un des protocoles de routage hiérarchiques les plus répandus dans les RCSF. Pour atteindre cet objectif, nous avons étudié les différentes attaques pouvant le menacer. Cela a permis de mettre en place notre protocole AIF-LEACH (*Authenticated sources, data Integrity and Freshness LEACH*) qui intègre les mécanismes de sécurité permettant d'atténuer les vulnérabilités les plus importantes.

**Mots clés:** Réseaux de capteurs sans fil, sécurité, routage, LEACH.

## Abstract

Recent advances in wireless communications and electronics have enabled the development of tiny, low-cost, and multifunctional sensor nodes. These characteristics have contributed to the design of Wireless Sensor Networks (WSNs) and promoted their use in a multitude of applications. These applications often require deployment in hostile environments, where nodes and communication links are continually exposed to important threats.

Hence, the services offered by WSNs must guarantee the security level required by the application. This goal is complicated because of the lack of fixed communication infrastructure, in addition to the hardware limitations imposed by the miniaturized size of sensors.

In this work, we are interested in securing the LEACH protocol, one of the most widespread hierarchical routing protocols for WSNs. To attain this objective, we studied the various attacks that can threaten it. This helped us to propose a new secure protocol that we called AIF-LEACH (*Authenticated sources, data Integrity and Freshness LEACH*), which incorporates security mechanisms to mitigate the most important vulnerabilities that have been explored.

**Key words:** Wireless Sensor Networks, security, routing, LEACH.

# Table des matières

<b>LISTE DES TABLEAUX</b> .....	XIV
<b>LISTE DES FIGURES</b> .....	XV
<b>LISTE DES SIGLES ET D'ABREVIATIONS</b> .....	XVII
<b>LISTE DES GRAPHES</b> .....	XX
<b>INTRODUCTION GENERALE</b> .....	<b>01</b>
<b>I. CHAPITRE I</b> .....	<b>03</b>
<b>PRESENTATION DES RCSF</b> .....	<b>03</b>
I.1. INTRODUCTION .....	03
I.2. LES RESEAUX SANS FIL .....	03
I.2.1. Définition .....	03
I.2.2. Caractéristiques des réseaux sans fil .....	04
I.2.3. Classes des réseaux sans fil .....	04
I.3. LES RESEAUX CELLULAIRES .....	05
I.4. LES RESEAUX AD HOC .....	06
I.4.1. Définition .....	06
I.4.2. Caractéristiques des réseaux Ad Hoc .....	07
I.5. LES RESEAUX DE CAPTEURS SANS FIL .....	08
I.5.1. Définitions .....	08
a) Un capteur .....	08
b) Un réseau de capteurs .....	08
I.5.2. Technologies des capteurs .....	09
I.5.3. Architecture des capteurs .....	09
I.5.4. Caractéristiques des réseaux de capteurs .....	11
I.5.5. Applications des réseaux de capteurs .....	12
I.5.5.1. Applications militaires .....	12
I.5.5.2. Applications à la sécurité .....	13
I.5.5.3. Applications environnementales .....	13
I.5.5.4. Applications médicales .....	13
I.5.5.5. Projets d'applications en cours.....	13
I.5.6. Architectures des réseaux de capteurs .....	15
I.5.6.1. Architecture de communication .....	15
I.5.6.2. Architecture protocolaire.....	16
I.5.6.3. Couches de la pile protocolaire .....	17
I.6. CONCLUSION .....	18

<b>II. CHAPITRE II .....</b>	<b>19</b>
<b>LA SECURITE DANS LES RCSF .....</b>	<b>19</b>
II.1. INTRODUCTION .....	19
II.2. LES MENACES CONTRE LES RCSF .....	19
II.2.1. Les mauvais comportements .....	19
II.2.2. Les attaques .....	19
II.2.2.1. Classification des attaques .....	20
II.2.2.2. Types d'attaques.....	20
II.3. OBJECTIFS ET SERVICES DE BASE DE LA SECURITE .....	24
II.3.1. L'authentification .....	24
II.3.2. L'intégrité de données .....	24
II.3.3. La confidentialité .....	24
II.3.4. La fraîcheur .....	24
II.3.5. La non-répudiation .....	25
II.3.6. Le contrôle d'accès .....	25
II.3.7. La disponibilité.....	25
II.4. MECANISMES DE SECURITE .....	25
II.4.1. Définition de la cryptographie .....	25
II.4.2. Les outils cryptographiques .....	26
II.4.2.1. Le chiffrement .....	26
II.4.2.2. La signature digitale .....	28
II.4.2.3. La fonction de hachage .....	28
II.4.2.4. Le code d'authentification de message MAC .....	29
II.4.3. La gestion de clés .....	30
II.5. VULNERABILITES DE LA SECURITE DANS LES RCSF .....	30
II.6. CONCLUSION .....	32
<b>III. CHAPITRE III .....</b>	<b>33</b>
<b>LE ROUTAGE DANS LES RCSF.....</b>	<b>33</b>
III.1. INTRODUCTION .....	33
III.2. FACTEURS DE CONCEPTION DE PROTOCOLES DE ROUTAGE .....	33
III.2.1. Tolérance aux pannes .....	33
III.2.2. Consommation d'énergie .....	34
III.2.3. Limitations de capacités des nœuds .....	34
III.2.4. Scalabilité .....	34
III.2.5. Connectivité .....	34
III.2.6. Modèles de transmission de données .....	34

III.2.7. Hétérogénéité .....	35
III.3. METRIQUES DE ROUTAGE .....	35
III.3.1. Métriques pour la consommation énergétique .....	35
III.3.1.1.Par considération de puissance.....	36
III.3.1.2.Par considération du coût .....	36
III.3.1.3.Par considération de puissance et du coût .....	36
III.3.2. Nombre de sauts .....	36
III.3.3. Perte de paquets .....	36
III.3.4. Délai de bout-en-bout EED .....	36
III.4. TAXONOMIE DES PROTOCOLES DE ROUTAGE .....	37
III.4.1. Classification selon les paradigmes de communication .....	37
III.4.1.1. Centré-nœuds.....	37
III.4.1.2. Centré-données.....	37
III.4.1.3. Basé-localisation .....	38
III.4.1.4. Basé-QoS .....	38
III.4.2. Classification selon la topologie du réseau.....	38
III.4.2.1.Topologie plate.....	39
III.4.2.2.Topologie hiérarchique.....	39
III.4.3. Classification selon la méthode d'établissement de routes .....	40
III.4.3.1.Protocoles proactifs .....	40
III.4.3.2.Protocoles réactifs .....	41
III.4.3.3.Protocoles hybrides .....	41
III.5. CONCLUSION .....	41
<b>IV. CHAPITRE IV .....</b>	<b>42</b>
<b>PROTOCOLE DE ROUTAGE LEACH : FONCTIONNEMENT ET SECURITE.....</b>	<b>42</b>
IV.1. INTRODUCTION .....	42
IV.2. PROTOCOLES MAC UTILISES PAR LEACH.....	42
IV.2.1. Accès aléatoire .....	42
IV.2.2. Allocation fixe .....	43
IV.2.2.1.TDMA.....	43
IV.2.2.2.CDMA.....	44
IV.3. ARCHITECTURE DE COMMUNICATION DE LEACH.....	44
IV.4. ALGORITHME DETAILLE DE LEACH.....	45
IV.4.1. Phase d'initialisation .....	45
IV.4.1.1.Phase d'annonce.....	46
IV.4.1.2.Phase d'organisation de groupes.....	47

IV.4.1.3.Phase d'ordonnancement .....	47
IV.4.2. Phase de transmission.....	48
IV.5. AVANTAGES ET INCONVENIENTS DE LEACH .....	49
IV.5.1. Avantages .....	49
IV.5.2. Inconvénients.....	50
IV.6. ATTAQUES ET CONTREMESURES POUR LEACH.....	50
IV.6.1. Inhibiting Node Discovery .....	50
IV.6.2. Cluster set-up Channel Blocking .....	51
IV.6.3. Forged Base Station .....	51
IV.6.4. Spoofed Cluster Head.....	51
IV.6.5. Supported Cluster Head.....	52
IV.6.6. Ghost Nodes .....	52
IV.6.7. Brute-force jamming attack .....	52
IV.6.8. Neighbors Interference .....	53
IV.7. CONCLUSION .....	53
<b>V. CHAPITRE V .....</b>	<b>54</b>
<b>SECURISATION DU PROTOCOLE DE ROUTAGE LEACH .....</b>	<b>54</b>
V.1. INTRODUCTION .....	54
V.2. OBJECTIFS VISES PAR LA SECURISATION DE LEACH .....	54
V.3. SERVICES DE SECURITE POUR LEACH .....	55
V.3.1. Authentification de sources de messages.....	55
V.3.1.1. Différents types de transmissions à sécuriser .....	55
V.3.1.2. Différents liens de communication à sécuriser.....	56
V.3.2. Intégrité de messages échangés .....	57
V.3.3. Fraîcheur de données .....	57
V.3.4. Confidentialité .....	57
V.4. MECANISMES DE SECURITE POUR LE PROTOCOLE AIF-LEACH .....	57
V.4.1. Mécanismes nécessaires pour l'authentification de sources de messages.....	58
V.4.1.1. Protocoles de gestion de clés.....	58
V.4.1.1.1. Protocoles basés sur la pré-distribution de clés .....	58
A. Protocoles de gestion de clés probabilistes.....	58
B. Protocoles de gestion de clés déterministes .....	58
V.4.1.1.2. Protocoles de gestion de clés déterministes étudiés .....	59
A. Low-Energy Key Management Protocol (LEKMP).....	59
B. Survivable and Efficient Clustered Keying (SECK).....	60
C. A*-based Logical Key Hierarchy (A*-LKH) .....	61

D. Hierarchical KEy management and authentication Scheme (HIKES) .....	62
V.4.1.2. Choix du mécanisme de gestion de clés pour AIF-LEACH.....	63
V.4.2. Mécanismes nécessaires pour l'intégrité de données .....	63
V.4.3. Mécanismes nécessaires pour la fraîcheur de données .....	64
V.5. SCHEMA DE SECURITE PROPOSE DANS AIF-LEACH .....	64
V.5.1. Authentification et intégrité de données dans AIF-LEACH.....	64
V.5.1.1. Format des paquets à envoyer .....	64
V.5.1.2. Gestion de clés proposée dans AIF-LEACH.....	65
V.5.2. Fraîcheur de données dans AIF-LEACH.....	68
V.6. DEROULEMENT DU PROTOCOLE AIF-LEACH .....	69
V.7. CONCLUSION .....	75
<b>VI. CHAPITRE VI .....</b>	<b>76</b>
<b>REALISATION .....</b>	<b>76</b>
VI.1. INTRODUCTION .....	76
VI.2. ENVIRONNEMENT DE SIMULATION .....	76
VI.2.1. TinyOS .....	76
VI.2.1.1. Pourquoi TinyOS ?.....	77
VI.2.1.2. Notions principales.....	77
VI.2.2. NesC .....	78
VI.2.3. TOSSIM .....	78
VI.2.3.1. TinyViz .....	79
VI.2.3.2. PowerTOSSIM.....	79
VI.3. IMPLEMENTATIONS ET DEROULEMENTS.....	79
VI.3.1. Implémentation du protocole LEACH.....	79
VI.3.1.1. Structures de données .....	79
VI.3.1.2. Evénements et commandes.....	80
VI.3.1.3. Déroulement .....	81
VI.3.2. Implémentation du protocole AIF-LEACH.....	83
VI.3.2.1. Structures de données .....	83
VI.3.2.2. Evénements et commandes.....	84
VI.3.2.3. Services de sécurité .....	85
VI.3.2.4. Les modules.....	85
VI.3.3. Implémentation des attaques .....	86
VI.3.3.1. Spoofed Cluster Head .....	86
VI.3.3.2. Modification d'un paquet de température captée .....	89
VI.3.3.3. Réinjection d'une donnée interceptée vers le CH .....	90

VI.4. SIMULATION ET EVALUATION DE PERFORMANCES .....	90
VI.4.1. Métriques à évaluer .....	90
VI.4.1.1. Consommation énergétique.....	91
VI.4.1.2. Perte de paquets .....	91
VI.4.1.3. Délai de bout-en-bout.....	91
VI.4.2. Paramétrage de la simulation .....	91
VI.4.3. Résultats et interprétations .....	92
VI.4.3.1. Consommation énergétique.....	92
VI.4.3.2. Perte de paquets .....	94
VI.4.3.3. Délai de bout-en-bout.....	95
VI.4.3.4. Simulation de l'attaque Spoofed cluster head.....	96
VI.5. CONCLUSION .....	98
<b>CONCLUSION GENERALE .....</b>	<b>99</b>
<b>LISTE DES REFERENCES .....</b>	<b>101</b>
<b>ANNEXE .....</b>	<b>110</b>