



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



Université Hadj Lakhder - Batna
Faculté des Sciences de l'Ingénieur
Département d'Informatique

Mémoire de Magistère

Thème :

Protocole de sécurité Pour les Réseaux de capteurs Sans Fil

Préparé par : **Samir ATHMANI**

Proposé et dirigé par : **Dr. Azeddine BILAMI**

Pour l'obtention du **Magistère en Informatique**

Option : Ingénierie des **Systèmes d'Informations**

Soutenue publiquement le : 15/07/2010 devant le jury composé de :

Pr. Mohammed BENMOHAMMED	Professeur	Président	Université de Constantine
Dr. Azeddine BILAMI	M.C.	Rapporteur	Université de Batna
Dr. Abdelmadjid ZIDANI	M.C.	Examineur	Université de Batna
Dr. Okba KEZZAR	M.C.	Examineur	Université de Biskra

Sommaire

SOMMAIRE	2
LISTE DES FIGURES.....	4
LISTE DES TABLEUX	5
RESUME	6
ABSTRACT.....	6
INTRODUCTION GENERALE	7
CHAPITRE 1 : INTRODUCTION AU RESEAU DE CAPTEUR SANS FIL	8
1. INTRODUCTION :	9
2. RESEAU INFORMATIQUE :	9
3. RESEAUX SANS FIL :	10
3.1 Définition :	10
3.2 Les catégories des réseaux sans fil :	11
3.2.1 Le réseau personnel sans fil (WPAN) :	11
3.2.2 Le réseau local sans fil (WLAN) :	12
3.2.3 Le réseau métropolitain sans fil (WMAN) :	13
3.2.4 Le réseau étendu sans fil (WWAN) :	13
4. RESEAUX DE CAPTEURS SANS-FIL	13
4.1 Les capteurs « traditionnels »	13
4.2 Les capteurs dans les réseaux de capteur sans fil	15
4.3 La mise en réseau	18
5. LES PRINCIPALES CARACTERISTIQUES DES RCSF	19
6. ARCHITECTURE DES RESEAUX DE CAPTEURS	22
6.1 Architecture de communication.....	22
6.2 Architecture protocolaire.....	23
6.3 Couches de la pile protocolaire [18, 19].....	24
7. COMPARAISON ENTRE LES RCSF ET LES RESEAUX SANS FIL CLASSIQUES.....	25
8. DOMAINES D'APPLICATION DES RESEAUX DE CAPTEURS SANS FIL	26
8.1 Applications militaires.....	26
8.2 Applications liées à la sécurité	27
8.3 Applications environnementales.....	27
8.4 Applications médicales	28
8.5 Applications écologiques	29
8.6 Applications de traçabilité et de localisation	29
8.7 Applications commerciales :	29
9. LES CHALLENGES/LES BESOINS	30
10. LE SYSTEME D'EXPLOITATION POUR RCSF : TINYOS	32
11. CONCLUSION	34
CHAPITRE 2 : LA SECURITE DANS LES RESEAUX DE CAPTEURS SANS-FIL	35
1 INTRODUCTION	36
2 CONDITIONS DE SECURITE.....	36
2.1 Confidentialité Des Données.....	36
2.2 Intégrité des données.....	36

2.3 Fraîcheur De Données	37
2.4 Auto-Organisation	37
2.5 La Localisation	37
2.6 Authentification	38
3 VULNERABILITES DE LA SECURITE DANS LES RCSF	38
4 BLOQUES FONCTIONNELS DE LA SECURITE DANS LES RCSF	40
5. MECANISMES DE SECURITE	40
5.1. Définition de la cryptographie	40
5.2. Les outils cryptographiques	41
5.2.1. Le chiffrement	41
5.2.2. La signature digitale.....	43
5.2.3. La fonction de hachage.....	44
5.2.4. Le code d'authentification de message MAC.....	45
6. LA GESTION DE CLES DANS LES RCSF	46
6.1. La fonction de gestion de clés dans les RCSF	46
6.1.1 Définition	46
6.1.2 Pourquoi la gestion de clés dans les RCSF ?.....	46
6.1.3 Contraintes de conception	47
6.1.4 Systèmes asymétriques ou symétriques ?.....	48
6.2 Schéma aléatoire de pré-distribution de clés de L.ESCHENAUER et D.GLIGOR.....	49
6.2.1 Phase de pré-distribution de clés	49
6.2.2 Phase de découverte de clés partagées.....	50
6.2.3 Phase d'établissement de chemin de clé.....	50
6.2.4 La révocation de clés	51
6.2.4 Schéma q-composite de H.CHAN, A.PERRIG et D.SONG	52
6.3 LEAP.....	53
6.3.1 Hypothèse de fonctionnement.....	53
6.3.2 Chargement de la clé initiale	53
6.3.3 Découverte des voisins	53
6.3.4 Etablissement de la clé par-paire.....	54
6.3.5 Effacement des clés	54
6.3.6 Sécurité de LEAP	54
7. SECURITE DU ROUTAGE DANS LES RCSF	54
7.1. Attaques sur les protocoles de routage dans les RCSF.....	55
7.1.1 Attaques actives	55
7.1.2 Attaques passives	57
7.2 Types de solutions.....	58
7.3 INSENS (Intrusion-tolerant routing for wireless sensor networks).....	58
7.3.1 Initiation authentifiée de la construction de l'arbre.....	59
7.3.2 Construction de l'arbre par relayage de la requête.....	60
7.3.3 Route feedback.....	60
7.3.4 Construction des tables de routage.....	61
7.4 SecRoute	62
7.4.1 Propriétés du SecRoute	63
7.4.2 Découverte des chemins	63
7.4.3 Relais de la réponse.....	64
7.4.4 Relais des données	64
7.5 Sécurité de l'agrégation dans les RCSF	65
7.5.1 Attaques sur l'agrégation de données dans les RCSF	65
7.5.2 SAWN (Secure Aggregation for Wireless Networks)	68
7.5.3 Protocoles basés sur le cryptage de bout en bout.....	71

8 CONCLUSION	72
CHAPITRE 3: APPROCHE DE SÉCURITÉ PROPOSÉE.....	73
1. INTRODUCTION	74
2. APPROCHE DE SECURITE PROPOSEE	74
2.1 Principe de base du protocole de sécurité proposée.....	74
3. LES GRANDES ETAPES DE NOTRE APPROCHE.....	76
3.1 Création des tableaux TN et TC.....	76
3.2 Création de la table de confiance	79
4. CONCEPT DE BASE DU PROTOCOLE DE ROUTAGE HEEP.....	79
5. ANALYSE DE SECURITE	81
5.1 Confidentialité de données et authentification des paquets	81
5.2 Intégrité des données.....	81
5.3 La Localisation	81
6. IMPLEMENTATION	82
6.1 Choix du langage et de l'environnement d'implémentation.....	82
6.2 Etapes d'implémentation de notre protocole	83
6.2.1 Préparation de l'environnement d'implémentation.....	83
6.2.2 Implémentation de notre protocole	84
7. CONCLUSION	85
CHAPITRE 4 : SIMULATION	86
1. INTRODUCTION	87
2. PRESENTATION DU SIMULATEUR NS2.....	87
3. ENVIRONNEMENT DE SIMULATION	87
4. RESULTATS DE SIMULATION	88
5. CONCLUSIONS	92
CONCLUSION GENERALE	93
REFERENCES.....	94

Liste des Figures

FIGURE 1 : LES CATEGORIES DES RESEAUX SANS FIL [1].....	11
FIGURE 2 : SCHEMATISATION D'UN CAPTEUR "TRADITIONNEL"	15
FIGURE 3 : SCHEMA D'UN COMPOSANT D'UN RESEAU DE CAPTEURS, INSPIRE DE [10]	17
FIGURE 4 : MODELE DE CAPTEUR VIRTUEL, INSPIRE DE [07]	18
FIGURE 4 : SCHEMATISATION D'UN RESEAU DE CAPTEURS SANS-FIL [16]	19
FIGURE 5 : ARCHITECTURE DE COMMUNICATION D'UN RESEAU DE CAPTEURS. [18]	23
FIGURE 6 : LA PILE PROTOCOLAIRE DANS LES RESEAUX DE CAPTEURS. [18]	24
FIGURE 7 : APPLICATIONS DES RCSF [20]	30
FIGURE 8 : SCHEMA REPRESENTANT L'ARCHITECTURE DU TINYOS[25]	33
FIGURE 9 : SECURITE DANS LES RCSF : PROPRIETES, CHALLENGES ET SOLUTIONS [20]	39
FIGURE 10 : TAXONOMIE DES CHALLENGES ET SOLUTIONS DE SECURITE DANS LES RCSF [20]	40
FIGURE 10 : LE CHIFFREMENT SYMETRIQUE. [33]	42
FIGURE 11 : LE CHIFFREMENT ASYMETRIQUE. [33]	43

FIGURE 12: LA SIGNATURE DIGITALE. [33]	44
FIGURE 13 : LA FONCTION DE HACHAGE. [33].....	45
FIGURE 14 : LE CODE D’AUTHENTIFICATION DE MESSAGE MAC. [33]	45
FIGURE 15 : FONCTIONS DE LA GESTION DE CLES.....	46
FIGURE 16 : POSITIONNEMENT DE LA GESTION DE CLE DANS UN RCSF SECURISE[20]	47
FIGURE 17 : CONTRAINTES DE CONCEPTION DE SOLUTIONS DE GESTION DE CLES	47
FIGURE 18 : TAXONOMIE DE PRE-DISTRIBUTION DE CLES POUR LES RCSF[20]	49
FIGURE 19 : DECOUVERTE DES CLES PARTAGEES[20].....	50
FIGURE 20 : ÉTABLISSEMENT DE CHEMINS SECURISES	51
FIGURE 21 : REVOCATION DE CLES	52
FIGURE 22 : SCHEMA Q-COMPOSITE	53
FIGURE 23 : ATTAQUE DE "JAMMING"	55
FIGURE 24 : ATTAQUE SINKHOLE	56
FIGURE 25 : ATTAQUE WORMHOLE.....	56
FIGURE26 : CATEGORIES DE SOLUTIONS CONTRE LES ATTAQUES SUR LE ROUTAGE.....	58
FIGURE 26 : REQUETE AUTHENTIFIEE DE CONSTRUCTION DE L'ARBRE[20]	60
FIGURE 27 : CONSTRUCTION DE L'ARBRE[20]	60
FIGURE 28 : ROUTE FEEDBACK[20].....	61
FIGURE 28 : CONSTRUCTION ET DISTRIBUTION DES TABLES DE ROUTAGE[20]	62
FIGURE 29 : FORMAT DE LA TABLE DE ROUTAGE DANS SECROUTE	63
FIGURE 30 : FONCTIONNEMENT CORRECTE DE L'AGREGATION[20].....	66
FIGURE 31 : UN MALICIEUX INJECTE UNE FAUSSE DONNEE[20].....	66
FIGURE 32 : UN MALICIEUX FALSIFIE LE RESULTAT D'UNE AGREGATION[20]	67
FIGURE 33 : CLASSIFICATION DES SOLUTIONS D'AGREGATION SECURISEE[33]	68
FIGURE 34 : EXEMPLE D'ARBRE D'AGREGATION SECURISE AVEC SAWN[21]	69
FIGURE 35 : ALGORITHME CMT[21]	71
FIGURE 36 : ALGORITHME ECEG [21]	72
FIGURE 37 : ALGORITHME DE CREATION DES TABLES TC ET TN	77
FIGURE 38 : DU CALCUL DU NOMBRE D’APPARITION DES NŒUDS DANS LA TABLE TN	78
FIGURE 39 : ALGORITHME DE CREATION DU BLACK LISTE	78
FIGURE 40 : ALGORITHME DE CREATION DE LA TABLE DE CONFIANCE	79
FIGURE 41 : ORGANISATION DES NŒUDS DANS LE RESEAU.....	80
FIGURE 39 : RESULTATS DE SIMULATION	89
FIGURE 40 : RESULTATS DE SIMULATION	90
FIGURE 41 : COMPARAISON ENTRE LES PROTOCOLES HEEP, LEACH-C ET NOTRE APPROCHE	91
FIGURE 42 : COMPARAISON DE VIVACITE DES NEUDS ENTRE LES PROTOCOLES HEEP, LEACH-C ET NOTRE APPROCHE	92

Liste des tableaux

TABLE1 : COMPARAISON ENTRE LES RCSF ET LES RESEAUX SANS FIL	26
TABLE 2. PARAMETRES DE SIMULATION.	88
TABLE 3: RESULTATS DE SIMULATION.	89
TABLE 4: POURCENTAGE DE NOMBRE DES PAQUETS MODIFIES	90

Résumé

Le domaine d'application des réseaux de capteurs ne cesse d'accroître avec le besoin d'un mécanisme de sécurité efficace. Le fait que les RCSF traitent des données très souvent sensibles, opérant dans des environnements hostiles et inattendus, la notion de sécurité est considérée comme indispensable. Cependant, à cause de la limitation des ressources et la faible capacité de calcul d'un nœud capteur, le développement d'un mécanisme garantissant une sécurité pose de vrais défis de conception.

Dans ce mémoire nous avons essayé de proposer un nouveau mécanisme de sécurité dédié aux RCSF. Notre objectif principal est de sécuriser le processus de transfert des données vers la station de base. Le protocole proposé protège les données transférées contre les attaques des nœuds intrus en utilisant un mécanisme de sécurité basé sur l'utilisation de message de contrôle MAC (Message Authentication Code) pour l'authentification. Les performances de notre protocole sont évaluées à l'aide du simulateur NS2.

Abstract

The sensor networks application domain continues to increase with the need for an effective security mechanism. The fact that WSN often deal with sensitive data operating in hostile and unexpected environments, makes the concept of security considered essential. However, because of limited resources and low computing capacity of a sensor node, the development of a mechanism that ensures security is a real design challenges.

In this report we have tried to propose a new security mechanism dedicated to WSN. Our main objective is to secure the process of transferring data to the base station. The proposed protocol protects transferred data against intruder nodes attacks, using a security mechanism based on the use of control message MAC (Message Authentication Code) for authentication. Our protocol performances are evaluated using the simulator NS2.

Introduction générale

L'essor des technologies sans fil offre aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. En comparaison avec l'environnement filaire, l'environnement sans fil permet aux utilisateurs une souplesse d'accès et une facilité de manipulation des informations à travers des unités de calcul mobiles (PC portable, PDA, capteur...).

Les réseaux sans fil peuvent être classés en deux catégories : les réseaux avec infrastructure fixe préexistante, et les réseaux sans infrastructure. Dans la première catégorie, une importante infrastructure logistique et matérielle est nécessaire pour le déploiement du réseau ; le modèle de la communication utilisé est généralement le modèle cellulaire (les réseaux GSM par exemple). La deuxième catégorie est celle des réseaux ad hoc.

Un réseau ad hoc peut être défini comme un ensemble d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de tout support fixe.

Avec les avancées techniques en terme de performances et de miniaturisation, réalisées dans les microsystèmes électromécaniques (MEMS: microcontrôleur, trancheiver RF...) et les communications sans fil, une nouvelle variante de réseaux ad hoc s'est créée afin d'offrir des solutions économiquement intéressantes pour la surveillance à distance et le traitement des données dans les environnements complexes et distribués : Les réseaux de capteurs sans fil.