REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

N° d'ordre : .....

UNIVERSITE MOHAMED BOUDIAF-M'SILA
FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE
Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux
Par : ZIAZIA Zeid

SUJET

Sécurité de l'agrégation dans les réseaux de capteurs sans fil

Soutenu publiquement le : / / 2015 devant le jury composé de :

.....	**Université de M'sila**	**Président**
Mr. ATHMANI Samir	**Université de M'sila**	**Rapporteur**
.....	**Université de M'sila**	**Examinateur**
.....	**Université de M'sila**	**Examinateur**

Promotion : 2014/2015

Table des matières

CHAPITRE 3

ELABORATION DE LA SOLUTION

CHAPITRE 4

IMPLEMENTATION EVALUATION DES PERFORMANCES A TRAVERS LA SIMULATION

INTRODUCTION GENERAL

Les avancées technologiques réalisées dans les domaines de la microélectronique et de la communication sans fil ont permis de concevoir et de fabriquer des composants miniaturisés, autonomes et fiable tels que les capteurs. En effet, ces composants électroniques classés parmi les systèmes embarqués, déployés sur une surface géographique importante formant un réseau de nœuds capteurs afin de collecter des informations sur des événements bien définis, et de les acheminer vers un nœud particulier de traitement, appelé puits (Sink) ou bien station de base (BS). Les informations collectées servent à construire une vision globale de la zone couverte pour prendre des décisions.

Les nœuds capteurs composant le réseau sont conçus pour être déployés d'une manière dense dans des endroits hostiles et difficiles d'accès, d'où la nécessité de limiter au maximum leurs dimensions physiques qui s'obtiennent impérativement au détriment des capacités de calcul, de traitement et de ressources énergétiques. Mais l'absence de sécurité physique, et la nature vulnérable des communications radios sont des caractéristiques qui augmentent les risques d'attaque.[12]

Les réseaux de capteur sans fil sont sujets à différents types de menaces telles que l'interception des données envoyées et reçues par un support sans fil permet de les modifier ou de les rejouer. L'intrus peut également injecter, saturer ou endommager les équipements du réseau. Dans cette optique, un protocole de sécurité doit pouvoir être établi avec peu d'influence sur la performance globale du réseau, tout en fournissant les différents services de sécurité pour chaque type d'application.

L'agrégation des données est une approche très intéressante pour réduire la charge des communications. Elle consiste à traiter les données recueillies par chaque capteur au niveau d'un nœud appelé agrégateur. Seulement le résultat produit sera transmis à la station de base. De cette manière la quantité de données communiquées dans le réseau peut être diminuée, ce qui réduit par conséquent la consommation de la bande passante et l'épuisement d'énergie des capteurs. Cependant, garantir la sécurité conjointement à des techniques d'agrégation est très.

Dans ce mémoire, nous allons nous intéressées aux problèmes de confidentialité et d'authentification pour lequel nous pensons qu'il manque encore des solutions efficaces. Nous avons proposé un algorithme d'agrégation très semble est efficace. Le but de notre travail est que la station de base pout être récupère les lectures individuel de tout les nœuds participant dans l'opération d'agrégation après il peut être vérifie les services de sécurité.

Le présent document est organisé en trois chapitres

Le premier chapitre présente une introduction aux réseaux de capteurs sans fil ainsi que leur fonctionnement, leurs applications potentielles et aussi leurs principales caractéristiques.

Le second chapitre survole les problèmes de sécurités des données agrégées dans les réseaux de capteurs sans fil, les solutions proposées et leurs classifications avec la description des publications existantes.

Le dernier chapitre constitue le cœur de notre travail. Nous proposons un nouvel algorithme pour renforcer l'authentification des données agrégées dans les réseaux de capteurs clustérisés.

Et enfin, nous terminons notre mémoire par une conclusion générale.

CONCLUSION GENERALE

Les RCSFs constituent des sujets de recherche innovants pour diverses disciplines des sciences et techniques de l'information et de la communication mais avec toutefois des contraintes spécifiques s'érigeant en défis certains à relever. Parmi les problèmes poses a l'heure actuelle dans ce type de réseaux, la sécurité en est un véritable et auquel une solution adéquate doit être apportée.

Dans notre projet de fin d'études, nous nous sommes intéressés à la sécurité de l'agrégation de donne. Pour cela, il nous étudier les différentes attaques qui ciblent l'agrégation de donne et les solutions propose sur ce Protocol Ceci nous a permis de proposer une solution efficace en terme d'authentification

Nous avons simulé le fonctionnement de notre algorithme avec le simulateur NS2 version 2.34 et comparé les résultats fournis avec ceux du protocole LEACH,

Enfin, comme perspectives nous envisageons d'améliorer les performances de notre protocole d'agrégation que ce soit au niveau de taille de paquet.

Bibliographie

[1] CHALLALYacine, «Réseaux de Capteurs Sans Fils», support-SIT60, Vol. 103, pp. 14, 17, Novembre 2008,

[2] Ramdani mohamed «problémes de sécurité dans les réseaux dev capteurs avac prise en charge de l'énergie», MÉMOIRE DE MAGISTER, Blida, Novembre 2013, SAAD DAHLAB

[3] Claude Castelluccia, « La Sécurité des Capteurs et Réseaux de Capteurs », PLANETE, INRIA, Juin 2008.

[4] XUE Yong, AGUILARAndres [et al.], « Agrégation de données dans les réseaux de capteurs », Projet SR04, Rapport final, Vol. 21, pp. 3-9, 13-14, 16, 2010.

[5] BOUNEGTA, « Réseaux de capteurs sans fil », Université de Bechar, Ingénieur d'état en informatique, 2010.

[6] LABRAOUI Nabila, Mourad Guerroui [et al.], « Data Aggregation Security Challenge in Wireless Sensor Networks », A Survey, Published by licenseunder the OCP Science imprint, Vol. 324, pp. 304-305, 311, October 2010.

[7] LABRAOUI Nabila, «La sécurité dans les réseaux de capteurs sans fil», Thèse pour l'obtention du diplôme de doctorat, 2012.

[8] MERAD Omar, « la sécurité des données agrégées dans les réseaux de capteurs sans fil », mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique, 2010.

[9] Hani Alzaid, Ernest Foo et Juan Gonzalez Nieto, «Secure Data Aggregation in Wireless Sensor Network», A Survey, vol. 13, pp. 3, 2011.

[10] N.Labraoui, M.Gueroui, T.Zia, «Data Aggregation Security Challenges in Wireless Sensor Networks», in the proceeding soft he 9th International Symposium on Programming and Systems (ISPS 2009), May25-27, 2009, Algiers, Algeria.

[11] Claude Castelluccia et Aurélien Francillon, « Protéger les réseaux de capteurs sans fil », Actes du symposium SSTIC08, vol. 11, pp. 8, 2005.

[12] MERAD BOUDIA Omar Rafik «agrégation des données et sécurité des réseaux de capteurs sans fil », Thèse pour l'obtention du diplôme de doctorat, 2014, L'UNIVERSITE DE TLEMCEN.

ملخص

شبكات الاستشعار اللاسلكية كثيرا ما تنشر في بيئات معادية، فتكون عرضة للعديد من الهجمات . بسبب الموارد الذاكرة المحدودة وقيود الطاقة لا يمكن استعمال خوارزميات معقدة أمنية في شبكات الاستشعار.

في هذا االبحث اقترحنا خوارزمية لتأمين تجميع البيانات في شبكات الاستشعار اللاسلكية، مبدأه هو أن المحطة الأساسية يمكن أن تستعيد القراءة الفردية لكل عقدة للتحقق من الخدمات الأمنية.

الكلمات المفتاح : شبكات الاستشعار اللاسلكية ,تجميع المعطيات ,أمن المعطيات المجمعة , الموثوقية ,التشفير.

Abstract

The Wireless Sensor Networks (WSN) is often deployed in hostile environments, which makes them very vulnerable and increase the risk of attacks. Due to limited memory resources and energy constraints, complex security algorithms cannot be used in sensor networks.

In this work we proposed an algorithm to secure data aggregation in wireless sensor networks; its principle is that the base station could Retrieves Individual reading for each node to check the security services.

Key words: Wireless sensor networks, aggregation data, secure aggregated data, Authentication, and encryption.

Résumé

Les Réseaux de capteurs sans fil (WSN) sont souvent déployés dans des environnements hostiles, ce qui les rend très vulnérables et augmente le risque d'attaques.

En raison des ressources mémoires limitées et des contraintes d'énergie, des algorithmes complexes de sécurité ne peuvent pas être utilisés dans les réseaux de capteurs.

Dans ce mémoire nous avons proposé un algorithme pour sécuriser l'agrégation de donnée dans les réseaux de capteur sans fil, Son principe est que la station de base put récupère les lectures individuelle pour chaque nœud, afin de vérifier les services de sécurité.

Mots clés : Réseaux de capteurs sans fil, agrégation des données, sécurité des données agrégées, l'authentification, chiffrement.