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