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 : **I**ngénierie des **S**ystèmes d'**I**nformations

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.	**Examinateur**	Université de Batna
Dr. Okba KEZZAR	M.C.	**Examinateur**	Université de Biskra

Sommaire

Liste des Figures

Liste des tableaux

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 Authentification 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, transceiver 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.