République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Ecole Doctorale d'Informatique

Thèse de Doctorat

En Informatique

Option

Réseaux et Systèmes Distribués

Thème

Gestions de Clés dans les Réseaux de Capteurs Sans-Fil

Présenté par

Mohamed Lamine MESSAI

Devant le jury composé de :

Président :	Djamil AISSANI, Professeur, Université de Béjaïa, Algérie
Rapporteur :	Makhlouf ALIOUAT, Professeur, Université de Sétif 1, Algérie
Rapporteur :	Hamida SEBA, Maître de Conférences HDR , Université Claude Bernard Lyon 1, France
Examinateur :	Nadjib BADACHE, Professeur, CERIST, Algérie
Examinateur :	Abdellah BOUKERRAM, Professeur, Université de Béjaïa, Algérie
Examinateur :	Mohamed BENMOHAMED, Professeur, Université de Constantine 2, Algérie
Examinateur :	Zibouda ALIOUAT, Maître de Conférences A, Université de Sétif 1, Algérie

Résumé

Jour après jour, les réseaux de capteurs sans-fil (RCSFs) s'intègrent dans les domaines nécessitant l'observation du monde physique. Cette intégration a fait l'émergence des RCSFs qui a ouvert la voie à une multitude de domaines de recherche. L'intérêt suscité par cette effervescence d'investigation préconise de larges champs d'application dans un avenir proche. Toutefois, beaucoup d'obstacles inhérents à leurs spécificités doivent être surmontés avant de pouvoir atteindre leur maturité. Parmi ces entraves, le problème de sécurité se pose avec acuité et doit être solutionné de manière appropriée et en conformité avec les caractéristiques particulières des RCSFs. Ces caractéristiques contraignantes s'observent dans la limitation des ressources telles que : l'énergie, la puissance de calcul, la bande passante et l'espace mémoire. En raison de ces contraintes et de leur déploiement dans des environnements sans surveillance et hostiles, les différents nœuds capteurs d'un RCSF sont vulnérables à la compromission et susceptibles d'une violation physique. De plus, l'utilisation des transmissions sans-fil rend les RCSFs perméables à des malveillances de toutes sortes, et constitue un véritable chalenge de sécurité à relever. Notre thèse contribue au domaine de gestion de clés dans les RCSFs, qui est le cœur de tout système de sécurité : nous présentons en premier lieu un état de l'art des RCSFs et des protocoles de gestion de clés proposés pour ces réseaux. Comme conséquence, nous proposons un nouveau protocole de gestion de clés appelé STKM (Tree-Based Protocol for Key Management in Wireless Sensor Networks), et un autre nommé SKM (Sequence Based Key Management in Wireless Sensor Networks). La dernière contribution concerne la proposition d'un protocole appelé SEAC (a Self-Stabilizing Energy Aware Clustering Scheme for Sensor Networks) pour l'organisation du RCSF en *clusters*. Notre idée est de concevoir un schéma de gestion de clés sur cette organisation des noeuds capteurs .
Mots clés : Conservation d'énergie, Réseaux de capteurs sans-fil, Sécurité, Cryptographie, Gestion de clés.

Abstract

During the last few years, wireless sensor networks (WSNs) are integrated in areas that necessitate the observation of physical world. This integration maked the emergence of WSNs, and paved the way for a variety of research domains. WSNs consist of small nodes with sensing, computation, and wireless communication capabilities and expected to play an essential role in the upcoming age of pervasive computing. However, many obstacles inherent to their specificities must be overcome before reaching thier maturity. Among these obstacles, the security problem is acute and needs to be addressed appropriately and according to characteristics of WSNs. These characteristics are observed in the limited resources such as energy, computing power, bandwidth and storage space. WSNs are generally deployed in hostile environments and sensor nodes are prone to node compromise attacks and physical violation. In addition, the use of wireless transmissions makes WSNs permeable to malware of all kinds, and security a real challenge. This thesis contributes to the field of key management in WSNs, which is the heart of every security system : first we present a state of the art of WSNs and

key management protocols proposed for these networks. As a consequence, we propose a new key management protocol called STKM (Tree-Based Protocol for Key Management in Wireless Sensor Networks), and another named SKM (Sequence Based Key Management in Wireless Sensor Networks). The last contribution relates to the use of the clustering technique to organize the WSN for energy saving problem. We propose a new clustring scheme ; SEAC (Self-Stabilizing Energy Aware Clustering Scheme for Sensor Networks), our idea is to design a key management scheme adapted to SEAC.

Keywords **:** Wireless sensr networks, Security, Cryptography, Key management, energy saving.

Table des matières