# Sécurité des communications dans les réseaux de capteurs sans fil (RCSF)

Ismail Mansour[1], Gérard Chalhoub[2], Michel Misson[3]

*Clermont université/LIMOS CNRS, Complexe scientifique des Cézeaux, 63177 Aubière cedex, France*

[1]mansour@isima.fr, [2,3](chalhoub,misson)@sancy.univ-bpclermont.fr

***Résumé*— L'aspect sécurité des réseaux de capteurs occupe de plus en plus de chercheurs au cours de ces dernières années. Il a été récemment prouvé que l'utilisation de la cryptographie à clé publique dans les RCSF était une chose faisable. Cependant elle consomme encore beaucoup d'énergie, de temps de calcul et de capacité de mémoire. Nous proposons l'utilisation des clés publiques ECC dans le but d'échanger des clés symétriques. Ces clés sont utilisées pour chiffrer les communications, elles sont révoquées en cas de captures physiques des nœuds et renouvelées périodiquement. Conjointement, nous proposons une approche basée sur le saut de fréquences qui permet aux nœuds du réseau de se défendre contre les attaques comme le *jamming* et aux communications d'être plus robustes contre les interférences.**

## I. INTRODUCTION

Un RCSF est composé de nœuds limités en énergie, en capacités mémoire et de calcul. Le fait d'utiliser l'air pour communiquer, permet à un adversaire de facilement intercepter, injecter ou modifier des paquets échangés sur le réseau en utilisant des nœuds communicants plus performants que les nœuds capteurs.

Un RCSF est un réseau ad hoc particulier. Les nœuds du RCSF peuvent communiquer entre eux sans passer par une infrastructure. Ils possèdent tous les clés symétriques de chiffrement des voisins. Lorsqu'un nœud est capturé physiquement, la récupération des clés stockées dans ce nœud peut amener à des graves conséquences : un adversaire peut déchiffrer les communications sur plusieurs liens à l'aide de ces clés. Dans ce cas, on ne peut pas assurer l'intégrité et la confidentialité des messages ni l'authentification de l'entité expéditrice.

Un RCSF sécurisé a besoin d'une architecture qui est capable à la fois (i) d'assurer la distribution authentifiée des clés aux nœuds grâce à une politique de gestion de clés (*key mangement*) pour le chiffrement des communications, (ii) d'arrêter les menaces provoquées par un vol de clés stockées dans un nœud lorsqu'il est capturé par un adversaire, (iii) et de se défendre contre les attaques connues dans les réseaux sans fil comme le déni de service par *jamming*.

## II. PROPOSITION

Pour assurer la sécurité des communications entre les nœuds d'un RCSF contre l'interception, l'injection et la modification des échanges d'une part, et contre les captures des nœuds d'une autre part, nous proposons une solution basée sur :

### *A. Les opérations cryptographiques*

Le but est d'utiliser une technique hybride des systèmes symétriques et asymétriques. Le réseau est initialement déployé avec une pré-distribution d'une paire de clés asymétriques ECC (*Elliptic Curve Cryptography*) [1] pour chaque nœud. Ces clés, stockées dans les nœuds avant le déploiement, servent à établir des liens sécurisés. Ces liens assurent l'authentification de la source et l'intégrité des données et permettent aux nœuds d'échanger des clés symétriques en toute sécurité. Le chiffrement symétrique entre les nœuds du réseau assure la confidentialité des données échangées.

### *B. La révocation et le renouvellement des clés du réseau*

En proposant un protocole qui empêche des nœuds capturés de continuer à faire partie du réseau et cela en révoquant leurs clés. Un renouvellement de clés symétriques est fait périodiquement pour éviter qu'elles soient trouvées facilement. Ce renouvellement est basé sur l'utilisation d'une liste des clés (*key-chain*), une technique utilisée souvent dans les RCSF comme méthode efficace pour l'authentification des clés [2].

### *C. La technique de saut de fréquences*

Cette technique utilisée dans les RCSF contre l'attaque de déni de service. Elle permet aux nœuds d'utiliser les fréquences disponibles du médium dans le but de rendre le réseau plus robuste et de détecter une telle attaque.

## III. CONCLUSION

Dans ce papier nous avons présenté une solution complète pour sécuriser les communications dans un RCSF. Un travail en cours consiste à évaluer les différents algorithmes de cryptographie et les mécanismes de mise à jour des clés sur les cartes TelosB.

Ce travail est financé partiellement par FEDER (*European Fund for Regional Development*).

## REFERENCES

[1] J. Lopez and R. Dahab, "An overview of elliptic curve crytography," University of Campinas, Tech. Rep., May 2000.

[2] G. Dini and M. Savino, "S2RP: a Secure and Scalable Rekeying Protocol for Wireless Sensor Networks," *In Proc. Of 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS,06)*, pp.457-466, 2006.