Ecole d'ingénieurs
du Canton de Vaud

Tél. : + 41 21 316 98 11
Fax : + 41 21 626 04 67

info@eivd.ch
http://www.eivd.ch

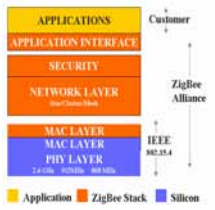
Travail de diplôme 2004
Département Electricité et Informatique

Ecole d'ingénieurs du Canton de Vaud
Rue de Genève 55, CP 59
CH - 1000 Lausanne 20

La sécurité dans le standard 802.15.4 / Zigbee

Introduction

L'entité 802.15.4/Zigbee a été conçue pour répondre au besoin du marché dans le cadre d'applications sans fil avec un faible débit et une basse consommation, telles que :



- l'électronique de loisir,
- le contrôle de processus industriels,
- l'automation de bâtiments,
- l'informatique domestique,
- la surveillance médicale…

Figure 1 – la pile de communication

La sécurité dans le standard 802.15.4

De part la nature des réseaux sans fil, leur sécurisation relève de la plus haute importance. Le standard 802.15.4 ne fait pas exception à cette nécessité et spécifie selon les besoins de l'application trois modes de sécurité différents au niveau de la couche MAC :

- le mode non sécurisé,
- le mode contrôle des accès,
- le mode sécurisé.

Dans le mode sécurisé il existe différentes approches sécuritaires : AES-CTR, AES-CCM et AES-CBC-MAC qui combinent plusieurs fonctions sécuritaires :

- ***le contrôle des accès*** maintient une liste des autres dispositifs avec lesquels un dispositif peut échanger des données.
- ***le cryptage des données*** utilise un algorithme de chiffrement symétrique par bloc afin d'éviter la lecture des données par des dispositifs tiers.
- ***l'intégrité de la trame*** ajoute un code d'intégrité de 32, 64 ou 128 bits, qui assure l'impossibilité de modification et l'authentification des données.
- ***la fraîcheur séquentielle*** permet de détecter et de rejeter des trames qui ont été répliquées et réémises.

Nom de l'approche sécuritaire	Fonctions sécuritaires			
	Contrôle des accès	Cryptage des données	Intégrité de la trame	Fraîcheur séquentielle
Aucune				
AES-CTR	X	X		X
AES-CCM-128	X	X	X	X
AES-CCM-64	X	X	X	X
AES-CCM-32	X	X	X	X
AES-CBC-MAC-128	X		X	
AES-CBC-MAC-64	X		X	
AES-CBC-MAC-32	X		X	

Tableau 1 – les approches sécuritaires sous 802.15.4

L'algorithme AES-128

Toutes ces différentes approches sécuritaires utilisent l'algorithme AES-128 qui réalise un chiffrement des données par bloc de 128 bits à l'aide d'une clé symétrique de 128 bits.
Chaque bloc subit quatre transformations :

- l'addition de la clé de tour,
- la substitution non-linéaire,
- le décalage de lignes,
- Le brouillage de colonnes.

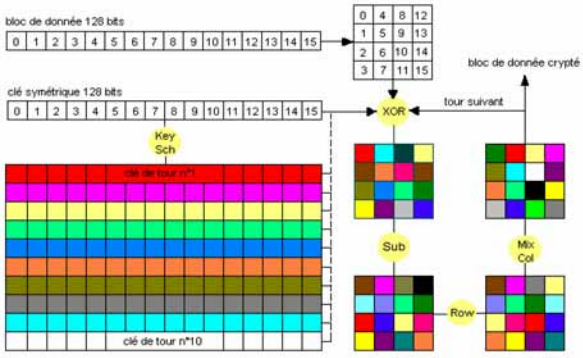


Figure 2 - schéma de principe AES-128

L'implémentation en langage ANSI C

Le but de ce projet est d'intégrer la partie sécurité de 802.15.4 sur une plate-forme de test équipée du microcontrôleur MSP430 de Texas Instruments. Cette implémentation en langage C est réalisée à l'aide de l'environnement de développement de IAR.

Auteur: **Burri Pierre-Alain**
Répondant externe: **C.Kassapoglou, A.Hutter**
Prof. responsable: **Pollini Alexandre**
Sujet proposé par: **CSEM**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale