MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II académique en Electronique

Option : Réseaux et télécommunication

Thème :

Etude de la sécurité des données dans les réseaux de capteurs sans-fil (ZigBee).

Proposé et dirigé par :

Mr. LAGHROUCHE Mourad.

Présenté par :

Mr. ZIANI Ammar.

Année universitaire 2011/2012

REMERCIEMENTS

En premier lieu je remercie mon **DIEU** le tous puissant de m'avoir donné la foi, la santé et m'a permit de bien mener ce travail.

Avant d'entreprendre la rédaction de mémoire, je souhaite vivement remercier et exprimer mes gratitude à :

Mon promoteur **M. LAGHROUCH Mourad,** à qui je suis très reconnaissant pour le sujet proposé et pour son aide et ses conseils.

Je tiens également à exprimer mes reconnaissances et mon sincère gratitude à tous les enseignants de bonne foi qui nous ont accompagnés tout au long de notre formation et en particulier le chef de département d'électronique

M. Rezki ZIANI.

Un grand merci à mon ami Merzouk et à tous ceux qui ont contribués de prêt ou de loin à la réussite de ce mémoire et en particulier a C.Said.

Ammar.

Dédicaces

Je dédie ce modeste travail à :
Mes très chers parents qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie.
Mes petits frères Massi, Ghiles et Kamel que j'aime beaucoup et à qui je souhaite une bonne réussite dans leurs études et dans leurs vie.
Toute ma famille et mes amis.
Tous ceux qui m'aime et que j'aime que je n'ai pas cité, mais que je n'ai pas oublié.

Sommaire.

Sommaire

Chapitre II : La sécurité dans les réseaux de capteurs sans-fil

Chapitre III : Présentation des normes IEEE 802.15.4 / ZigBee

Chapitre IV : La sécurité dans les normes IEEE 802.15.4 /ZigBee

Sommaire

Liste des figures.

Liste des figures

Liste des figures

Introduction générale.

Introduction générale

La convergence de la micro-électronique et des technologies de communication sans-fil a permis la création d'une combinaison entre les systèmes embarqués et les systèmes distribués ayant engendré les Réseaux de Capteurs Sans-Fil ou RCSFs (Wireless Sensor Networks). Les capteurs apparaissent comme des systèmes autonomes miniaturisés, équipés d'une unité de traitement et de stockage de données, d'une unité de transmission sans-fil et d'une batterie. Organisés sous forme de réseau, les capteurs (ou nœuds) d'un RCSF, malgré la limitation de leurs ressources de calcul, de stockage et d'énergie, ont pour mission de récolter des données et les faire parvenir à une station de base. Par principe, les nœuds du réseau ont un mode d'organisation spontané (ils forment donc un réseau ad hoc) car ils sont prévus pour être déployés rapidement et arbitrairement.

Les réseaux de capteurs sans-fil sont de plus en plus utilisés dans des applications de surveillance de grands systèmes dans une variété de domaines : le militaire, l'environnement, la santé, l'habitat, l'éthologie, etc. Leur remarquable essor est dû à leur taille de plus en plus réduite, leurs prix de plus en plus faible ainsi que leur support de communication sans-fil attrayant peu encombrant mais également peu sécurisant.

La sécurité est une nécessité pour la majorité des applications qui utilisent les RCSFs, notamment si les nœuds capteurs sont déployés dans des endroits peu sûrs, tels que les champs de bataille, les lieux stratégiques (aéroports, bâtiments critiques, etc.). Ces nœuds capteurs qui opèrent dans des lieux difficiles d'accès, sans protection et sans possibilité de rechargement de batterie, peuvent être soumis à des actions perturbatrices et malveillantes susceptibles de compromettre l'essence même d'un RCSF. C'est pourquoi, il est primordial de pouvoir leur assurer un niveau de sécurité acceptable. Compte tenu de leurs spécificités contraignantes, la sécurité dans ce type de réseaux relève d'un véritable challenge. Comme l'objectif premier des nœuds d'un RCSF est de rassembler des donnés de surveillance et de les transmettre à un lieu de décision, cette opération doit se faire sans interférences malicieuses et avec un niveau de sécurité approprié.

Ce travail est réalisé au sein du département d'électronique, de l'université MOULOUD MAMMERI de Tizi-Ouzou, il est organisé en quatre chapitres.

Le premier chapitre traite des notions générales sur les réseaux de capteurs sans-fil.

Le deuxième chapitre est consacré à la sécurité dans les réseaux de capteurs sans-fil.

Dans le troisième chapitre nous allons décrire les normes IEEE 802.15.4 et le protocole de transmission ZigBee.

Et enfin, nous terminerons notre travail par l'étude de quelques méthodes utilisé pour la sécurité du protocole ZigBee.

Chapitre I

Les réseaux de capteurs sans-fil.

I.1. Introduction

Les technologies actuelles en matière de réalisation de composants électronique, et en particulier de microprocesseurs, permettent de développer des équipements de taille et de poids de plus réduits. Cela a permis l'apparition d'objets informatique portables de plus en plus puissants, tels que les ordinateurs portables et les assistants personnels(PDA), ainsi que la communication entre ces équipements qui est de type sans-fil.

L'utilisation d'une interface sans-fil introduit des différences par apport à la communication par câble.

Tout d'abord, le spectre radio, et donc la capacité disponible pour le transfert de données, est limité par la réglementation. Là où un ajout de câble suffit pour augmenter le nombre d'utilisateurs pouvant être satisfait sur un réseau fixe, la bande de fréquence occupée par un réseau mobile ne peut être étendue. Cette restriction limite aussi le débit disponible imposant la nécessité d'une utilisation efficace du canal.

En suite, la qualité des liens radio peut varier avec le temps au gré des diverses interférences et de la mobilité des nœuds. Cette situation mène donc à un taux d'erreur de transmission plus important que sur un réseau filaire et surtout à un taux très fluctuant.

Les avancées faites dans la miniaturisation des systèmes électromécaniques (MEMS) ont permis l'apparition d'un nouveau type de réseaux sans-fil : les réseaux de capteurs. Ces réseaux sont un type particulier de réseaux ad hoc. Ils utilisent un grand nombre de dispositifs appelés nœuds. Ces objets peuvent recueillir et transmettre des données environnementales de manière autonome.

Il n'y a pas si longtemps, la seule solution pour acheminer les données du capteur jusqu'au contrôleur central était le câblage qui avait comme principaux défauts d'être coûteux et encombrant.

I.2. Historique des télécommunications

La télécommunication est toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de touts nature, par fil, radioélectricité, optique ou autres systèmes électromagnétiques.

I.2.1. La communication avec les liaisons filaires

Dans les années 1840, l'américain Samuel Morse invente un télégraphe électrique simple : des piles, un interrupteur, un électro-aimant et des fils suffisent.

L'appareil de Morse, qui transmit le premier télégramme public en 1844, ressemblait à un prédéfinie puis l'interrompait, le tout étant commandé avec la pression d'un doigt. Le premier récepteur Morse était équipé d'un crayon contrôlé électro-magnétiquement. Ce crayon imprimait des marques sur une bande de papier, fixée sur un cylindre animé par un mouvement d'horlogerie. Les marques variaient en longueur suivant la durée des impulsions du courant électrique passant à travers les fils d'un électro-aimant et prenaient la forme visuelle de points et de traits. Par la suite, les opérateurs apprirent à reconnaître directement à l'oreille les traits et les points qui leur étaient transmis. Son appareil fut adopté par la plupart des pays européens et des réseaux nationaux basés sur le télégraphe de Morse virent le jour aux états Unis, en France, en Angleterre... En 1866, après plusieurs essais infructueux, le premier câble transatlantique fut installé et avec lui, le premier véritable réseau mondial de télécommunication se développa. Aux environs de 1940, la première de l'informatique moderne fit son apparition. Rapidement, l'adaptation des technologies de télécommunications à l'informatique fut rapidement incontournable. En 1957, le ministère de la défense américain crée l'agence pour les projets de recherche avancée (ARPA). Dans ce cadre, le besoin de faire communiquer les différentes équipes de recherche aux quatre coins des états Unis se fait ressentir. Ce besoin a mené les chercheurs de l'ARPA à créer l'ARPANET, réseau destiné à relier entre elles les différentes universités du pays, qui grâce à la standardisation du modèle TCP/IP, évoluera vers l'Internet que nous connaissons actuellement.

I.2.2. La communication sans-fil

Depuis peu, les systèmes de communication sans-fil offrent aux utilisateurs la possibilité de profiter des joies des télécommunications quelle que soit leur localisation géographique. Pourtant, la communication sans-fil est presque aussi vieille que la communication filaire...

En 1887, Heinrich Hertz vérifie par l'expérience les théories de Maxwell. Ces dernières, établies de façon mathématique par James Maxwell, nous disent que toute

perturbation électrique donne naissance à des oscillations électromagnétiques. Ces oscillations seront amenées à êtres connues sous le nom d'ondes hertziennes. En 1890, Edouard Branly découvre le premier récepteur sensible aux ondes hertziennes. A partir des travaux de Branly, l'italien Gugliemo Marconi invente le premier appareil de télégraphie sans-fil en 1895. Puis, Marconi va de succès en succès en augmentant les distances de transmission pour atteindre, en 1903, la transmission complète d'un message sur une distance de 3400 km !

Jusqu'à la fin des années 1980, la technologie sans-fil a surtout été utilisée dans le cadre de la radio, de la télévision ou des communications réservées à d'importants organismes comme l'armée. L'arrivée des téléphones cellulaires GSM (Global System for Mobile communication) a offert à tous la possibilité de communiquer de n'importe où, avec n'importe qui. Cependant, un tel dispositif nécessite le déploiement d'une infrastructure coûteuse devant assurer le relais entre les téléphones portables et le réseau téléphonique filaire.

I.3. Les réseaux sans-fil

I.3.1. Les réseaux ad hoc [1]

Un réseau sans-fil ad hoc (ou MANET, pour Mobile Ad hoc NETwork) est formé par un ensemble d'hôtes qui s'organisent seuls et de manière totalement décentralisée, formant ainsi un réseau autonome et dynamique ne reposant sur aucune infrastructure filaire. Ces hôtes peuvent être fixes ou mobiles. Selon ces hypothèses, tout ensemble d'objets munis d'une interface de communication adéquate est susceptible de spontanément former un tel réseau.

Aucune infrastructure n'étant disponible, ces objets ont donc à découvrir dynamiquement leur environnement. Un réseau ad hoc étant avant tout un réseau sans-fil, les objets communiquent entre eux par le biais d'une interface radio. Ces communications sont donc soumises aux phénomènes physiques qui régissent les ondes radio, telle qu'une forte atténuation du signal avec la distance. Ainsi, seuls les hôtes suffisamment proches les uns des autres sont capables de communiquer directement ensemble, et les communications de longue distance doivent s'effectuer par le biais d'un mécanisme nommé multi-sauts : cela signifie simplement que certains objets doivent relayer les messages de proche en proche jusqu'à ce que leur acheminement soit effectué. L'utilisation d'une antenne radio omnidirectionnelle implique également qu'un message envoyé par un émetteur quelconque est reçu par tous les récepteurs suffisamment proches de lui.

La figure 1 illustre un réseau sans-fil classique tel que l'on peut par exemple en trouver dans les gares et les aéroports. L'infrastructure y est composée de deux points d'accès P1 et P2 reliés grâce à une liaison filaire classique, et qui servent de points d'entrée aux hôtes du réseau. Lorsque l'objet a désire communiquer avec l'objet d, il envoie les messages à P1 qui les fait suivre à P2, ce dernier les envoyant à d.

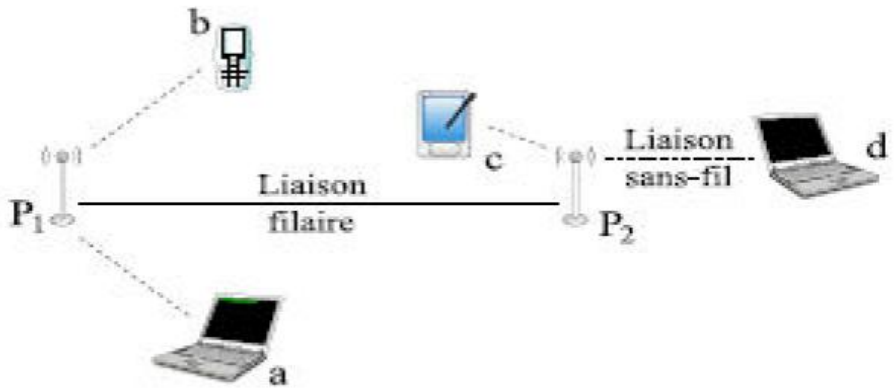

Figure 1 : Réseau sans fil classique.

La figure 2 illustre un réseau ad hoc pour lequel aucune infrastructure n'est nécessaire pour que les hôtes puissent communiquer ensemble. L'objet c doit donc servir de relais afin que a puisse communiquer avec d.

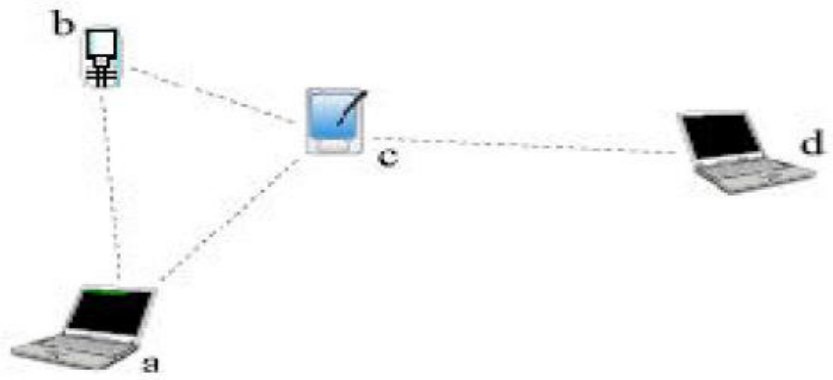

Figure 2 : Réseau sans fil ad hoc.

Les applications de ces réseaux sont multiples, et concernent principalement les zones où une infrastructure filaire est indisponible ou non désirable. C'est par exemple le cas dans les zones sinistrées par un désastre naturel, où les secours ont un grand besoin de communication.

C'est aussi le cas lorsque la rapidité et la discrétion sont des facteurs déterminants : on ne peut raisonnablement imaginer le déploiement d'une infrastructure de communication complète lors de manœuvres militaires en territoire ennemi. D'autres cas plus légers d'utilisation peuvent également survenir. Ainsi, pour des raisons de coût, il n'est, par exemple, pas possible de mettre en place une infrastructure filaire le temps d'une réunion en plein air. Dans tous ces exemples, l'utilisation d'un réseau ad hoc peut s'avérer indispensable.

La conception de protocoles de communication pour les réseaux ad hoc est principalement soumise à trois facteurs, qui peuvent être résumés comme suit :

- **Energie limitée :** Les hôtes fonctionnent grâce à une batterie, dont la durée de vie est généralement limitée à quelques heures d'utilisation ; les communications doivent donc être réduites au strict minimum.
- **Autonomie de décision :** Aucune autorité centrale n'est présente pour gérer les opérations des différents hôtes, le réseau est donc entièrement décentralisé.
- **Topologie dynamique :** Les hôtes sont mobiles et peuvent être connectés entre eux de manière arbitraire. Les liens radio changent régulièrement, lorsque les objets se déplacent, s'éteignent, ou lorsque des obstacles apparaissent ou disparaissent.

I.3.2. Réseaux de capteurs sans-fil (RCSF) [2-3]

I.3.2.1. définition d'un capteur

C'est un système qui sert à détecter, sous forme de signal souvent électrique, un phénomène physique afin de le représenter.

Les capteurs sont des petits appareils dotés d'une batterie, capables de communiquer entre eux et de détecter des événements s'ils se trouvent à l'intérieur de leur rayon de perception.

Un capteur est un petit appareil doté de mécanismes lui permettant de relever des informations sur son environnement. La nature de ces informations varie très largement selon l'utilisation qui est faite du capteur : ce dernier peut tout aussi bien faire des relevés de

température, d'humidité ou d'intensité lumineuse. Un capteur possède également le matériel nécessaire pour effectuer des communications sans-fil par ondes radio.

I.3.2.2. définition d'un RCSF

Les réseaux de capteurs sans-fil sont considérés comme un type spécial des réseaux ad hoc où l'infrastructure fixe de communication et l'administration centralisée sont absentes et les nœuds jouent, à la fois, le rôle des hôtes et des routeurs. Les nœuds capteurs sont des capteurs intelligents « smart sensors », capables d'accomplir trois tâches complémentaires : le relevé d'une grandeur physique, le traitement éventuel de cette information et la communication avec d'autres capteurs. L'ensemble de ces capteurs, déployés pour une application, forme un réseau de capteurs. Le but de celui-ci est de surveiller une zone géographique, et parfois d'agir sur celle-ci (il s'agit alors de réseaux de capteurs-actionneurs).

On peut citer comme exemples un réseau détecteur de feu de forêt, ou un réseau de surveillance de solidité d'un pont après un tremblement de terre. Le réseau peut comporter un grand nombre de nœuds (des milliers). Les capteurs sont placés de manière plus ou moins aléatoire (par exemple par largage depuis un hélicoptère) dans des environnements pouvant être dangereux. Toute intervention humaine après le déploiement des nœuds capteurs est la plupart du temps exclue, le réseau doit donc s'autogérer. Afin que les nœuds capteurs travaillent d'une façon coopérative, les informations recueillies sont partagées entre eux par voie hertzienne. Le choix du lien radio plutôt que du lien filaire permet un déploiement facile et rapide dans un environnement pouvant être inaccessible pour l'être humain.

I.3.2.3. Objectif de la base des RCSFs

Les objectifs de base des réseaux de capteurs sans-fil dépendent généralement des applications, cependant les tâches suivantes sont communes à plusieurs applications :

- Déterminer les valeurs de quelques paramètres suivant une situation donnée. Par exemple, dans un réseau environnemental, on peut chercher à connaître la température, la pression atmosphérique, la quantité de la lumière du soleil, et l'humidité relative dans un nombre de sites, etc.
- Détecter l'occurrence des événements dont on est intéressé et estimer les paramètres des événements détectés. Dans les réseaux de contrôle de trafic, on peut vouloir détecter le mouvement de véhicules à travers une intersection et estimer la vitesse et la

direction du véhicule.

- Classifier l'objet détecté. Dans un réseau de trafic, un véhicule est-il une voiture, un bus, etc.

I.3.2.4. Types de réseaux

Les RCSFs peuvent être classifiés selon deux points de vue :

a) Le model dynamique de réseau

- Soit le réseau est constitué d'un ensemble de capteurs mobiles évoluant dans un environnement statique. Le but de tels réseaux est la plupart du temps l'exploration de zones inaccessibles ou dangereuses. Les travaux de recherche sont souvent orientés robotique, les nœuds jouant à la fois le rôle de capteur et d'actionneur.
- Soit le réseau est constitué de capteurs fixes servant à la surveillance d'occurrence d'évènements sur une zone géographique. Ici, le réseau n'effectue que la surveillance, les données mesurées sont transmises en mode multi-sauts à un nœud spécifique appelé « puits » qui est chargé, après réception, de mettre en œuvre les actions nécessaires. Ce puits peut être connecté, de manière filaire par exemple, à un autre réseau.

b) Le model de délivrance de données

- Soit les capteurs transmettent périodiquement les informations recueillies (délivrance de données continue).
- Soit le capteur transmet des informations à la détection d'un évènement (délivrance de données basée évènement en anglais « event-driven »).
- C'est à l'utilisateur de lancer une requête pour avoir l'information (en anglais « observer-initiated »).
- Délivrance de données hybride où on trouve les différentes délivrances citées avant au même temps.

I.3.3. Comparaison réseaux de capteur et réseaux ad hoc

Le tableau 1 illustre la différence entre un RCSF et un réseau ad hoc

Senseur ou capteur	Ad hoc
Objectif ciblé	Générique / communication
Nœuds collaborent pour remplir un objectif	Chaque nœud a son propre objectif
Très grand nombre de nœuds n'ayant pas tous un identificateur ID	Notion d'ID
Énergie est un facteur déterminant, nœud capteur sujet aux pannes	Débit est majeur

Tableau 1 : Comparaison senseur / ad hoc.

I.4.Architecture de base d'un capteur [2]

Un capteur est composé de quatre éléments principaux :

- Un élément qui se charge de mesurer l'environnement extérieur (unité de capture),
- Une unité de calcul,
- Un élément émetteur / récepteur,
- Une alimentation.

Trois composants additionnels peuvent être implantés dans un capteur :

- Un système de recherche d'emplacement,
- Un générateur d'alimentation,
- Une unité mobile (permettant de faire bouger le capteur).

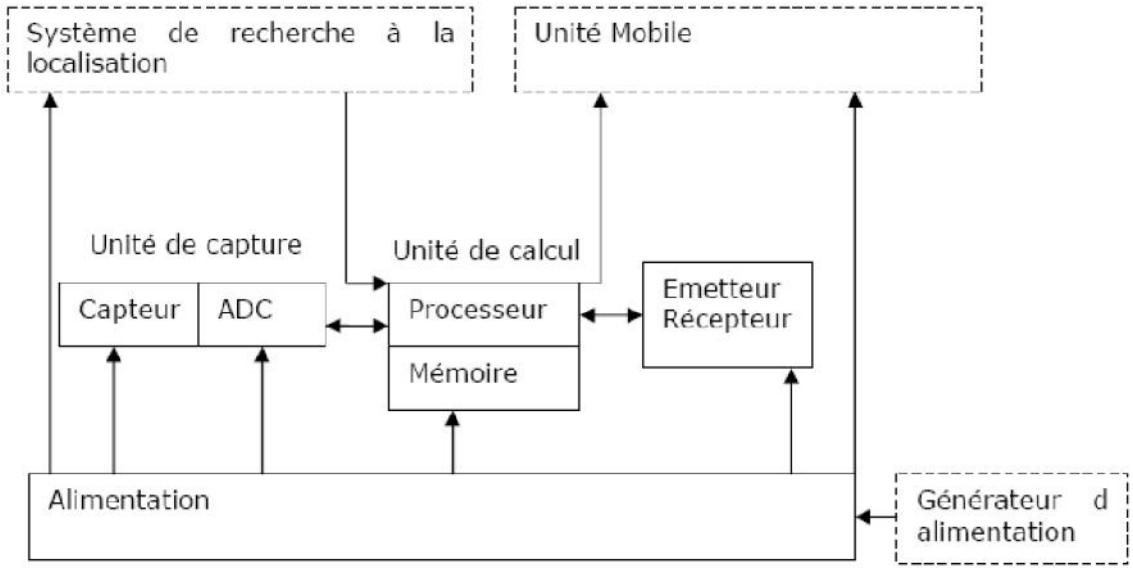

Figure 3 : Architecture de base d'un capteur.

. Capteur : L'unité de capture où élément capteur est composée de deux sous éléments :

- Le capteur récupérant des données analogiques,
- Un convertisseur faisant passer les données analogiques du capteur à des données numériques (appelée ADC pour analog to digital convertor) envoyées à une unité de calcul.

. Unité de calcul : Le composant regroupe :

- Un processeur,
- Une unité de mémoire réduite.

Il permet de stocker les données, exécute les taches de perception qui lui sont assignées.

. Émetteur/Récepteur : élément permettant de connecter le capteur au réseau.

. Alimentation : la source d'énergie pour le capteur, comme tout dispositif embarqué, ils disposent d'une alimentation autonome telle qu'une batterie.

I.5. Architecture d'un RCSF [3]

L'architecture du réseau de capteurs est montrée dans la figure suivante (Figure 4).

L'utilisateur accède à distance aux données capturées à travers un nœud appelé le nœud directeur de tâche « Task Manager Node ». Le nœud directeur de tâche est relié à l'Internet ou au satellite à travers un nœud destinataire « puits » (sink en anglais). Ce dernier

agit en tant que passerelle pour le réseau de capteurs, c'est-à-dire qu'il relie des réseaux de capteurs à d'autres réseaux. Ce nœud est responsable, en plus de la collecte des rapports, de la diffusion des demandes sur les types de données requises aux capteurs via des messages de requêtes. Il a également d'autre capacité de traitement de l'information pour une transformation ultérieure s'il y a lieu. Les nœuds capteurs sont habituellement dispersés dans une zone de capture appelée champ de captage. Les nœuds capteurs rassemblent les données et les conduisent au destinataire. De cette manière, les utilisateurs peuvent rechercher l'information dans les nœuds destinataires pour surveiller et commander l'environnement à distance. Notons qu'un réseau de capteurs peut contenir plusieurs nœuds puits diffusant des intérêts (ce sont la description des données requises par le nœud destinataire en utilisant une appellation combinée attribut-valeur) différents. Par exemple, un nœud puits peut demander à tous les capteurs se trouvant dans la région nord du champ de captage d'envoyer un rapport de température chaque 1 minute, pendant qu'un autre peut être intéressé seulement par les hautes températures (> 40°C) dans la région sud. Par conséquent, un capteur doit pouvoir stocker toutes les requêtes reçues, et les traiter séparément.

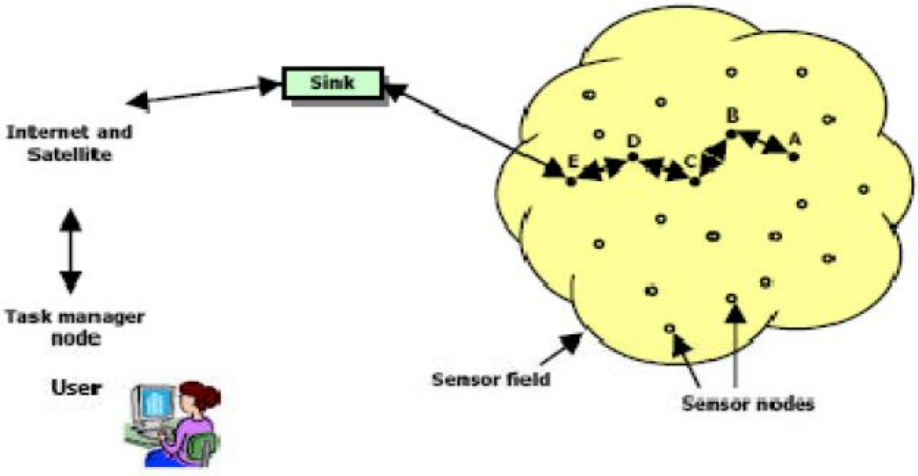

Figure 4 : Architecture d'un réseau de capteurs.

I.6. La pile protocolaire dans un RCSF [2,4]

Le rôle de cette pile consiste à standardiser la communication entre les participants afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles.

Ce modèle comprend 5 couches qui ont les mêmes fonctions que celles du modèle OSI ainsi que 3 couches pour la gestion de la puissance, la gestion de la mobilité et la gestion des tâches.

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction.

Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur.

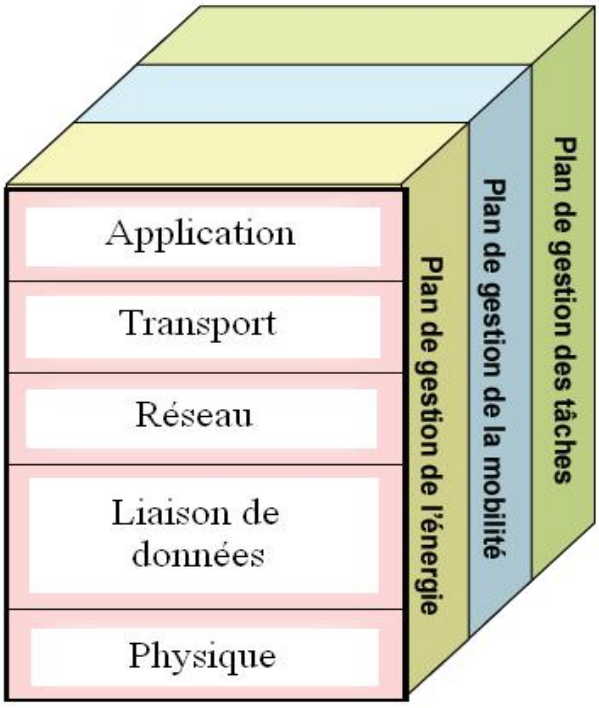

Figure 5 : Pile protocolaire d'une architecture de réseau de senseurs.

I.6.1. La couche physique

Elle s'occupe de la spécification du câblage, des fréquences porteuses, etc. …

Cette couche doit assurer des techniques d'émission, de réception et de modulation de données d'une manière robuste.

I.6.2. La couche liaison

Elle spécifie comment les données sont expédiées entre deux nœuds/routeurs dans une distance d'un saut. Elle est responsable du multiplexage des données, du contrôle d'erreurs, de l'accès sur le media, …

Elle assure la liaison point à point et point à multipoint dans un réseau de communication.

Elle est composée de la couche de contrôle de liaison logique (LLC pour Logical Link Control) qui fournit une interface entre la couche liaison et la couche réseau en encapsulant les segments de messages de la couche réseau avec des informations d'entête additionnelles, et la couche de contrôle d'accès au médium (MAC pour Medium Access Control) qui contrôle la radio.

Comme l'environnement des réseaux de capteurs est bruyant et les nœuds peuvent être mobiles, la couche de liaison de données doit garantir une faible consommation d'énergie et minimiser les collisions entre les données diffusées par les nœuds voisins.

I.6.3. La couche transport

Cette couche est chargée du transport des données, de leur découpage en paquets, du contrôle de flux, de la conservation de l'ordre des paquets et de la gestion des éventuelles erreurs de transmission.

I.6.5. La couche application

Cette couche assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

I.6.6. Le niveau de gestion d'énergie

Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs. Dès lors, un capteur peut par exemple éteindre son interface de réception dès qu'il reçoit un message d'un nœud voisin afin d'éviter la réception des messages dupliqués. De plus, quand un nœud possède un niveau d'énergie faible, il peut diffuser un message aux autres capteurs pour ne pas participer aux tâches de routage, et conserver l'énergie restante

aux fonctionnalités de capture.

I.6.7. Le niveau de gestion de mobilité

Ce niveau détecte et enregistre tous les mouvements des nœuds capteurs, de manière à leur permettre de garder continuellement une route vers l'utilisateur final, et maintenir une image récente sur les nœuds voisins. Cette image est nécessaire pour pouvoir équilibrer l'exécution des tâches et la consommation d'énergie.

I.6.8. Le niveau de gestion de tâches

Lors d'une opération de capture dans une région donnée, les nœuds composant le réseau ne doivent pas obligatoirement travailler avec le même rythme. Cela dépend essentiellement de la nature du capteur, son niveau d'énergie et la région dans laquelle il a été déployé. Pour cela, le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau afin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, et par conséquent, prolonger la durée de vie du réseau.

I.7. Caractéristique d'un capteur

Un capteur est doté des caractéristiques suivantes :

- Capable de calculer
- Capable de communiquer
- Capte toujours
- Préposition / déploiement aléatoire
- Limitation de la durée de vie des batteries
- Densité (petit / grand nombre)
- La rapidité : c'est le temps de réaction d'un capteur entre la variation de la grandeur physique qu'il mesure et l'instant où l'information prise en compte par la partie commande.
- L'étendue de la mesure : c'est la différence entre le plus petit signal détecté et le plus grand perceptible sans risque de destruction pour le capteur.

- La sensibilité : c'est la plus petite variation d'une grandeur physique que peut

détecter un capteur.

I.8. Application concrète d'un RCSF [5]

Les RCSF peuvent avoir beaucoup d'applications (voir la figure 6). Parmi elles, nous citons :

- **Applications militaires**
- **Applications liées à la sécurité**
- **Applications environnementales**
- **Applications médicales**
- **Applications écologiques**
- **Applications de traçabilité et de localisation**
- **Applications commerciales**

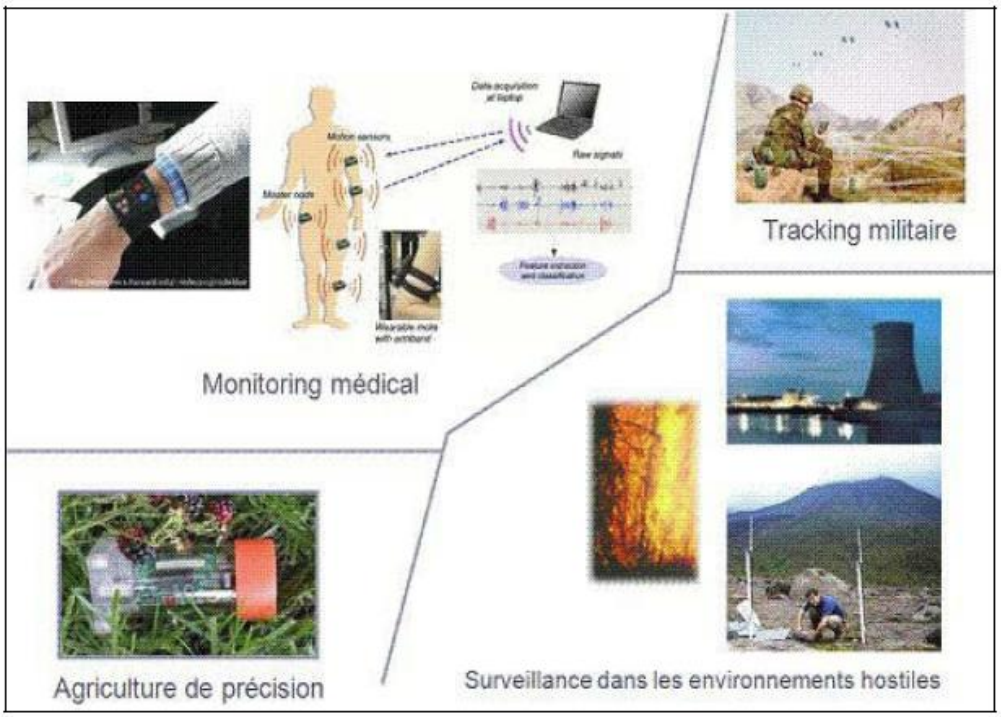

Figure 6 : Applications des RCSF.

I.9. Les réseaux de capteurs standards [6]

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation proviennent de l'IEEE aux États-Unis et de l'ETSI en Europe. La figure 7 décrit les différentes catégories de réseaux suivant leur étendue et la figure 8 les normes existantes.

Les principales normes sont IEEE 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée, IEEE 802.11, ou Wi-Fi (Wireless-Fidelity), pour les réseaux WLAN(Wireless Local Area Network), IEEE 802.16, pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres, et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network), c'est-à-dire les très grands réseaux.

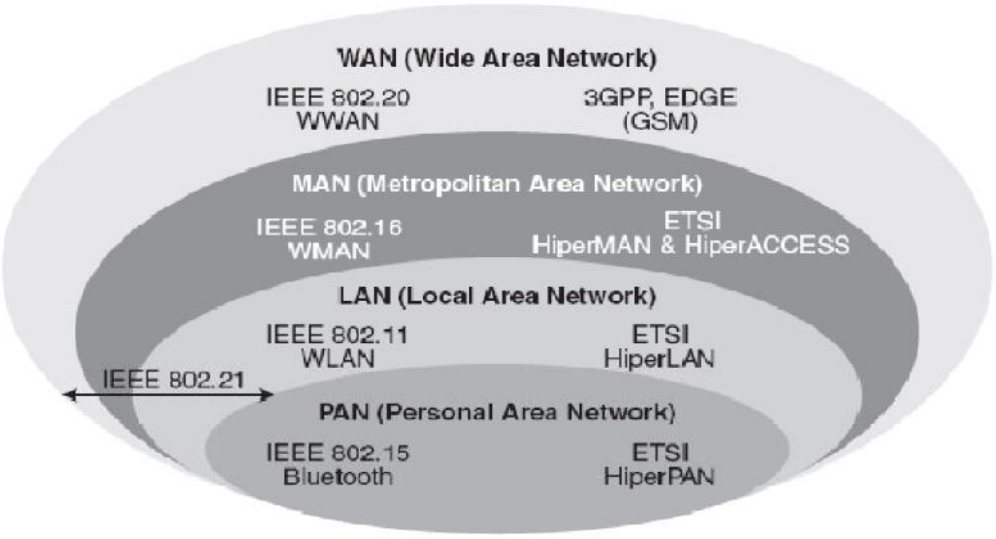

Figure 7 : Catégories des réseaux sans-fil.

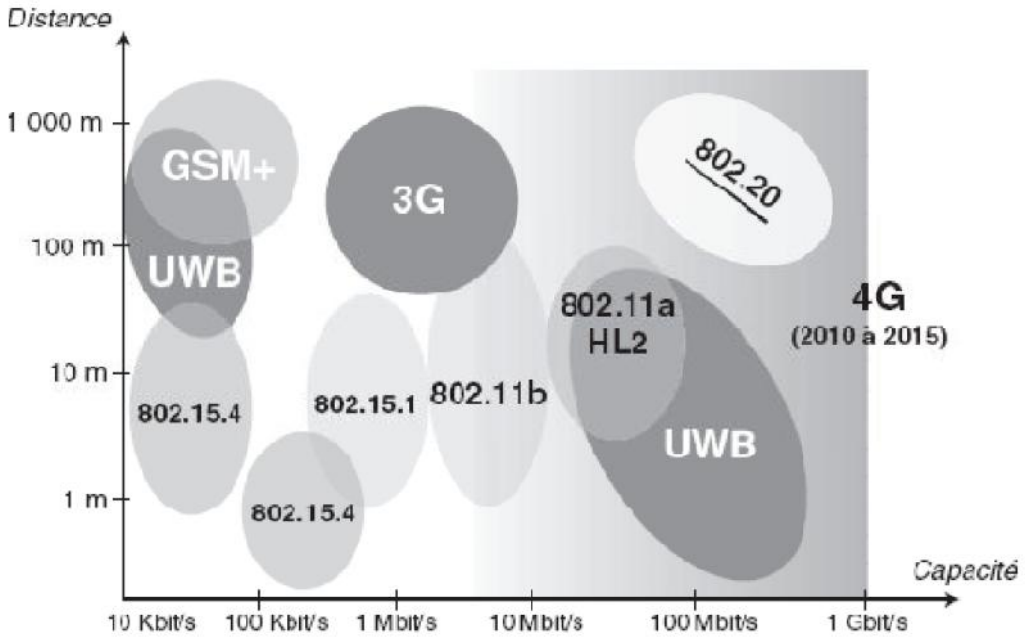

Figure 8 : Principales normes des réseaux sans-fil.

Dans ce qui suit, nous allons présenter les RCSFs standards qui ont été étudiés dans la littérature.

I.9.1. IEEE 802.15.1

IEEE 802.15.1, le plus connu, prend en charge la norme Bluetooth, aujourd'hui largement commercialisée. Mais cette norme est rarement utilisée dans RCSFs à cause de sa consommation importante d'énergie.

I.9.2. IEEE 802.15.3

IEEE 802.15.3 définit la norme UWB (Ultra-Wide Band), qui met en œuvre une technologie très spéciale, caractérisée par l'émission à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio (entre 3,1 et 10,6 GHz). Les débits atteints sont de l'ordre du gigabit par seconde sur une distance de 10 mètres.

I.9.3. IEEE 802.15.4

Les réseaux micro-capteurs sans-fil ont été l'objet de recherches intensives ces dernières années, ils émergent maintenant dans des applications industrielles. Une étape importante dans cette transition a été le dégagement de la norme d'IEEE 802.15.4 qui indique l'interopérabilité dans la couche physique et la couche MAC (Medium Access Control) visant

la radio de transmission du nœud capteur. L'IEEE 802.15.4 standard supporte différentes topologies de réseaux. Dans cette norme, deux types de topologies sont discutés : la topologie en étoile "Star" et la topologie paire à paire "Peer-to-peer". La norme d'IEEE802.15.4 présente deux types de nœuds : un nœud avec une charge complète (Full Function Device (FFD)) et un nœud avec une charge réduite (Reduced Function Device (RFD)).

La norme indique que le réseau soit coordonné par un des FFDs, ce dernier peut router des données (contrairement au RFD). Dans cette norme, la topologie en étoile met l'accent sur la durée de vie des batteries puisque chaque RFD est relié directement au coordonnateur. Par contre la topologie paire à paire s'intéresse à la fiabilité et à la scalabilité puisque tous les nœuds sont des FFDs et peuvent donc être reliés ensemble. La norme IEEE 802.15.4 peut supporter d'autres topologies, par exemple la topologie arbre de cellules "Cluster tree" qui combine les deux topologies précédentes (étoile et paire à paire ou maillé "Mesh"). Les différentes topologies du réseau supportées par IEEE 802.15.4 sont montrées dans la figure suivante :

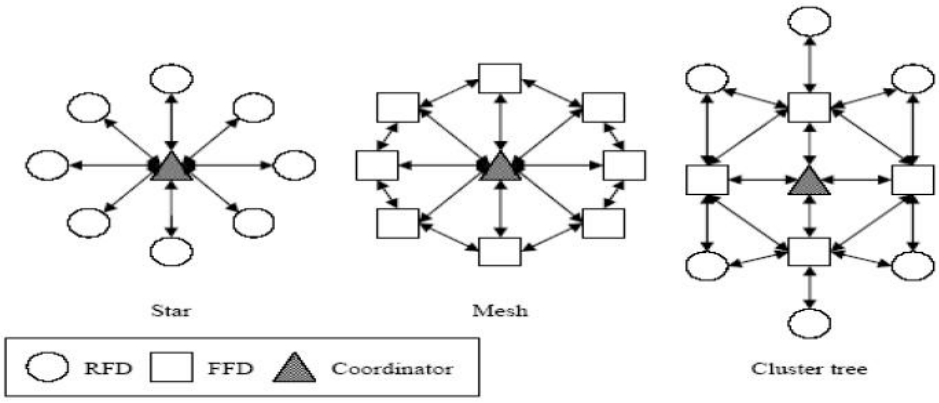

Figure 9 : Les topologies du réseau supportées par IEEE 802.15.4

I.9.4. ZigBee Alliance

En 2002, ZigBee Alliance a été constituée par une association d'entreprises. Le but de ZigBee Alliance est de développer des produits de contrôle fiable avec un coût réduit et qui ne demandent pas beaucoup d'énergie. Ces produits doivent pouvoir être gérés par un réseau sans-fil en utilisant une norme standard globale. Zigbee Alliance fonctionne globalement sur

la bande de fréquences des 2,4 GHz mais également à 915 MHz en Amérique et à 868 MHz en Europe. Les débits offerts sont : 250 Kbits/s à 2.4 GHz (10 canaux), 40 Kbits/s à 915 MHz (6 canaux) et 20 Kbits/s à 868 MHz (1 canal). ZigBee Alliance permet de connecter jusqu'à 255 matériels par réseau sur une portée allant jusqu'à 100 mètres. ZigBee Alliance a été ratifiée en Août 2003 sous la norme IEEE 802.15.4.

I.9.5. IEEE 1451.5

La famille des normes IEEE 1451.5 est prise en charge par le comité technique de la technologie d'instrumentation de capteurs IEEE (Institute of Electrical and Electronics Engineers) de la société de mesure. L'IEEE 1451.5 a été lancé afin de développer une norme pour les méthodes de communication sans-fil ainsi que le format de données des transducteurs (Un transducteur : est un moyen qui permet la conversion de l'énergie d'un type à un autre par exemple, l'énergie magnétique en énergie électronique et vice versa). Le but de ce standard est de développer des transducteurs intelligents "smart transducer" pour les capteurs. Plusieurs interfaces et protocoles de communication sans-fil sont développés pour les réseaux de capteurs par de différents fabricants. Ces interfaces et protocoles de communication sont spécifiés par des fournisseurs. L'IEEE 1451.5 qui accepte les diverses technologies existantes augmentera l'acceptation sur le marché et permettra la connectivité entre les dispositifs de différents fournisseurs.

I.10. Conclusion

Les réseaux de senseurs restent une nouvelle technologie peu accessible au grand publique. Elle est principalement répandue dans les laboratoires de recherches.

Des progrès sont encore à réaliser dans ce domaine. Néanmoins ils correspondent à une certaine vision du futur et permettront des améliorations dans d'innombrables domaines de la vie quotidienne.

Chapitre II

La sécurité dans les réseaux de capteurs sans-fil.

II.1. Introduction

Le degré d'utilisation des systèmes et réseaux d'information et l'environnement des technologies de l'information dans son ensemble ont évoluée de façon spectaculaire depuis1992. Ces évolutions offrent des avantages significatifs mais requirent également que le gouvernement, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'informations, portent une bien plus grande attention à la sécurité.

La sécurité est un enjeu majeur des technologies numériques modernes. Infrastructure de télécommunication (GSM, GPRS, UMTS), réseau sans fils (Bluetooth, WiFi, WiMax), Internet, systèmes d'informations, routeurs, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates, des cybercriminels.

II.2. Conditions de sécurité [7]

Un réseau de capteur est un type spécial de réseaux. Il partage quelques vulgarisations avec un réseau informatique typique, mais pose également des conditions uniques de ses propres caractéristiques. Par conséquent, un protocole de sécurité pour un RCSF, doit satisfaire une ou plusieurs conditions de sécurité, à savoir :

II .2.1. Confidentialité des données

La confidentialité des données est la question la plus importante dans la sécurité de réseau. L'approche standard pour sécuriser le transfert des données est de crypter les données avec une clef secrète connue par l'émetteur et le récepteur.

II .2.2 Intégrité des données

Un nœud intrus (adversaire) peut modifier les données transférées. Par exemple, un nœud malveillant peut ajouter quelques fragments ou manœuvrer les données dans un paquet. Ce nouveau paquet peut alors être envoyé au récepteur original. La perte ou les dommages de données peut même se produire sans présence d'un nœud malveillant dû à l'environnement dur de communication. Ainsi, l'intégrité des données s'assure qu'aucune donnée reçue n'a été

changée en transit.

II.2.3. Fraîcheur de données

Même si la confidentialité et l'intégrité des données sont assurées, nous devons également assurer la fraîcheur de chaque message. Officieusement, la fraîcheur de données suggère que les données soient récentes, et elles s'assurent qu'aucun vieux message n'a été rejoué. Cette condition est particulièrement importante quand il y a des stratégies de partager-clef utilisées dans la conception. Des clefs typiquement partagées doivent être changées avec le temps.

Cependant, cela prend du temps pour de nouvelles clefs partagées d'être propagées au réseau entier. Dans ce cas-ci, il est facile pour l'adversaire d'employer une attaque de rejouer. Pour résoudre ce problème un compteur relatif au temps différent, peut être ajouté dans le paquet pour assurer la fraîcheur de données.

II. 2.4. Auto-Organisation

Un réseau de capteur sans fil est typiquement un réseau adhoc, qui exige chaque nœud capteur soit indépendant et assez flexible à l'auto organisation. Il n'y a aucune infrastructure fixe disponible pour la gestion de réseau dans un réseau de capteurs. L'auto organisation apporte un grand défi à la sécurité du réseau de capteurs sans fil.

II. 2.5. La localisation

Souvent, l'utilité d'un réseau de capteur se fondera sur ses capacités de localiser automatiquement chaque capteur dans le réseau. Un réseau de capteurs conçu pour détecter des anomalies aura besoin de l'information précise d'endroit afin d'indiquer exactement l'endroit d'un défaut.

II. 2.6. Authentification

Un adversaire n'est pas limité simplement à modifier le paquet de données. Il peut changer le jet entier de paquets en injectant les paquets additionnels. Ainsi le récepteur doit s'assurer que les données utilisées dans n'importe quel processus décisionnel proviennent de la source correcte.

D'autre part, en construisant le réseau de capteurs, l'authentification est nécessaire pour beaucoup de tâches administratives (coefficient de reprogrammation ou de contrôle). D'après ce qui précède, nous pouvons voir que l'authentification de message est importante pour beaucoup d'applications dans les réseaux de capteurs. Officieusement, l'authentification de données permet à un récepteur de vérifier que les données sont vraiment envoyées par l'expéditeur réclamé.

Dans le cas de communication bipartite, l'authentification de données peut être réalisée par un mécanisme purement symétrique : l'expéditeur et le récepteur partagent une clef secrète pour calculer le code d'authentification de message (IMPER) de toutes les données communiquées.

II. 3. Vulnérabilités de la sécurité dans les RCSF [8]

Les principaux problèmes de sécurité dans les RCSF émergent à partir des propriétés qui les rendent efficaces et attrayants, qui sont:

Limitation de ressources: l'énergie est peut-être la contrainte la plus forte aux capacités d'un nœud capteur. La réserve d'énergie de chaque nœud doit être conservée pour prolonger sa durée de vie et ainsi que celle de l'ensemble du réseau. Dans la plupart du temps, l'information transmise est redondante vus que les capteurs sont généralement géographiquement co-localisés.

La plupart de cette énergie peut donc être économisée par agrégation de données. Cela exige une attention particulière à détecter l'injection de fausses données ou la modification défectueuse de données, lors des opérations d'agrégation au niveau des nœuds intermédiaires.

La communication sans fils multi-sauts: en plus de fournir un déploiement simple, la communication sans fil a l'avantage d'offrir l'accès à des endroits difficilement accessibles tels que des terrains désastreux et hostiles. Malheureusement, la portée de la communication radio des "mots" est limitée en raison de considérations énergétiques. La communication multi-sauts est donc indispensable pour la diffusion des données dans un RCSF. Cela introduit de nombreuses failles de sécurité à deux niveaux différents: attaque de la construction et maintenance des routes, et attaque des données utiles par injection, la modification ou la

suppression de paquets. En outre, la communication sans fil introduit d'autres vulnérabilités à la couche liaison en ouvrant la porte à des attaques de brouillage et de style déni de service par épuisement des batteries.

Couplage étroit avec l'environnement: la plupart des applications de RCSF exigent un déploiement étroit des nœuds à l'intérieur ou à proximité des phénomènes à surveiller. Cette proximité physique avec l'environnement conduit à de fréquentes compromissions intentionnelles ou accidentelles des nœuds. Comme le succès des applications RCSF dépend également de leur faible coût, les nœuds ne peuvent pas se permettre une protection physique inviolable.

Par conséquent, un adversaire "bien équipé" peut extraire des informations cryptographiques des nœuds capteurs. Comme la mission d'un RCSF est généralement sans surveillance, le potentiel d'attaquer les nœuds et de récupérer leur contenu est important. Ainsi, les clefs cryptographiques et informations sensibles devraient être gérées d'une manière qui augmente la résistance à la capture des nœuds.

La figure 10 résume les problèmes de sécurité émergeant des caractéristiques d'un RCSF et les solutions à entreprendre :

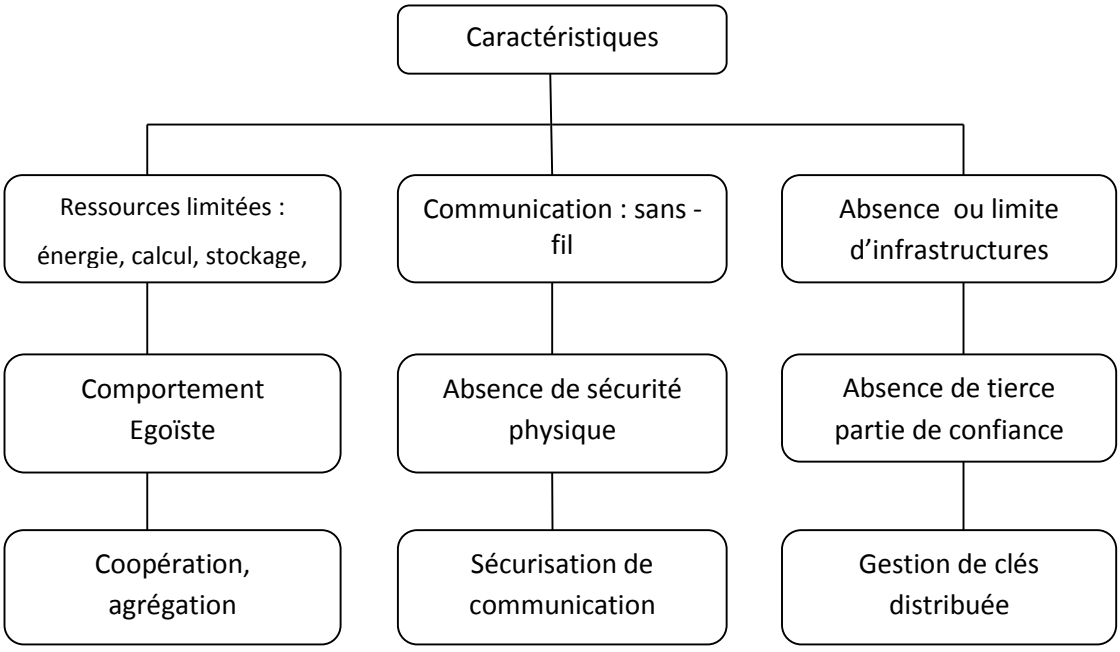

Figure 10 : Sécurité dans les RCSF : propriétés, challenges et solutions.

II. 4. Bloques fonctionnels de la sécurité dans les RCSF [8]

Comme illustré à la figure 11, on distingue quatre blocks fonctionnels des solutions de sécurité dans les RCSF : la gestion de clés, la sécurité du routage, la sécurité de l'agrégation de données, et la sécurité de l'accès au canal.

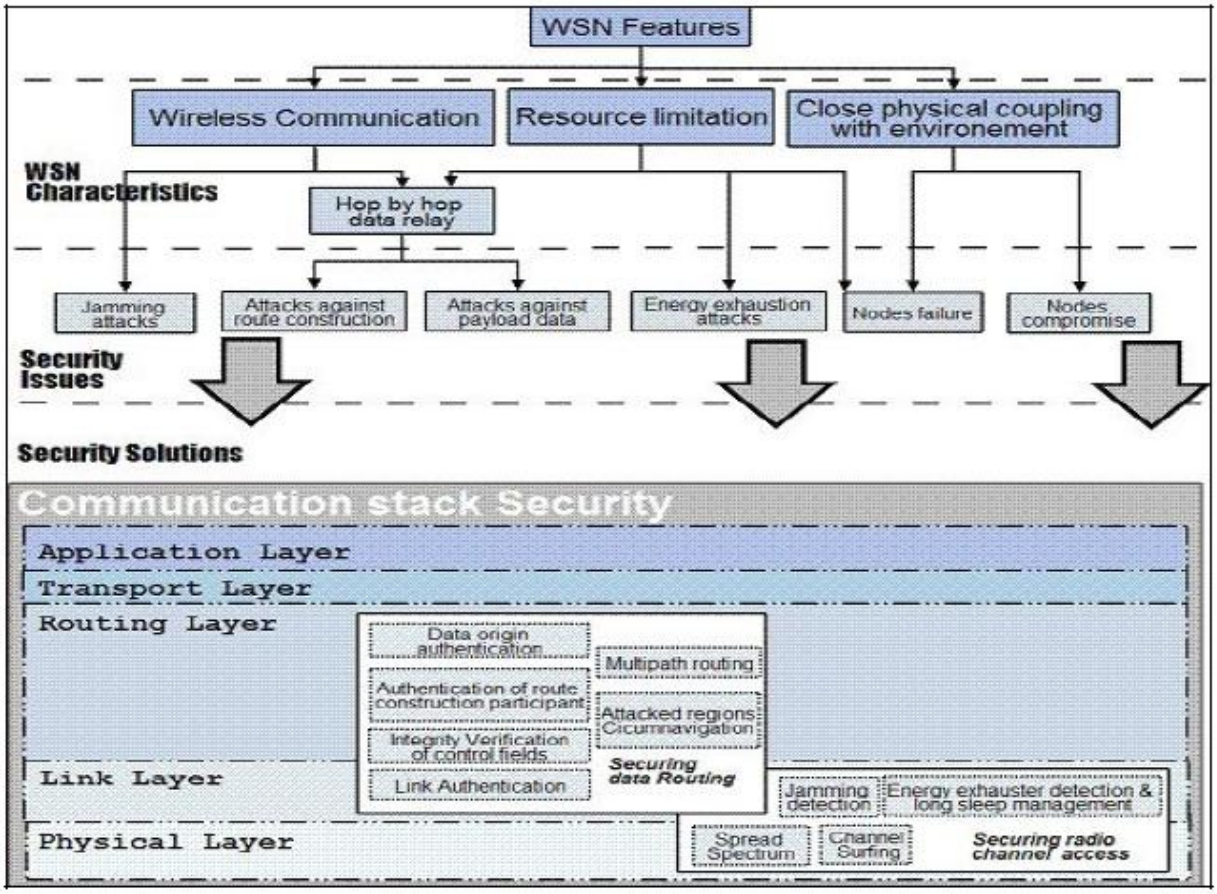

Figure 11 : Taxonomie des challenges et solutions de sécurité dans les RCSF.

II. 5. Mécanismes de sécurité

Plusieurs mécanismes, basés généralement sur la notion de cryptographie, sont mis en place afin de répondre à la question de la sécurité dans les RCSF.

II. 5.1. Définition de la cryptographie [9-11]

Le mot « cryptographie » est composé des mots grecs:

« Crypto » signifie caché,

«graphy » signifie écrire.

C'est donc l'art de l'écriture secrète.

La cryptographie est l'étude des techniques mathématiques qui permettent d'assurer certains services de sécurité. Elle est définie comme étant une science permettant de convertir des informations "en clair" en informations cryptées (codées), c'est à dire non compréhensibles, et puis, à partir de ces informations cryptées, de restituer les informations originales.

La cryptographie est réalisée selon certains outils. Avant de les aborder, il est commode de définir la notion de clé qui sera utilisée tout au long de cette partie.

Une clé : Dans la cryptographie moderne, l'habilité de maintenir un message crypté secret, repose non pas sur les algorithmes, mais sur une information secrète dite clé qui est un paramètre utilisé en entrée d'une opération cryptographique et qui doit être utilisée avec les algorithmes pour produire le message crypté.

II. 5.2. Les outils cryptographiques [9,12-14]

II. 5.2.1. Le chiffrement

Le chiffrement est le système cryptographique assurant la confidentialité. Pour cela, il utilise des clés. Selon cette utilisation, on distingue deux classes de primitives : symétrique ou asymétrique.

- **Le chiffrement symétrique** Une même clé est utilisée entre deux nœuds communicants pour chiffrer et déchiffrer les données en utilisant un algorithme de chiffrement symétrique. Les algorithmes de chiffrement symétriques sont décomposés en deux catégories :
    - Le chiffrement en chaîne est fait bit à bit sans attendre la réception entière des données. L'algorithme le plus connu est : RC4 (Rivest Cipher 4).
    - Le chiffrement par bloc consiste à fractionner les données en blocs de taille fixe (64 bits, 128 bits). Chaque bloc sera ensuite chiffré une fois qu'il atteint a taille envisagée. Les algorithmes les plus utilisés sont : DES (Data Encryption Standard), AES (Advanced Encryption Standard).

La figure 12 illustre la méthode de cryptographie par un chiffrement symétrique :

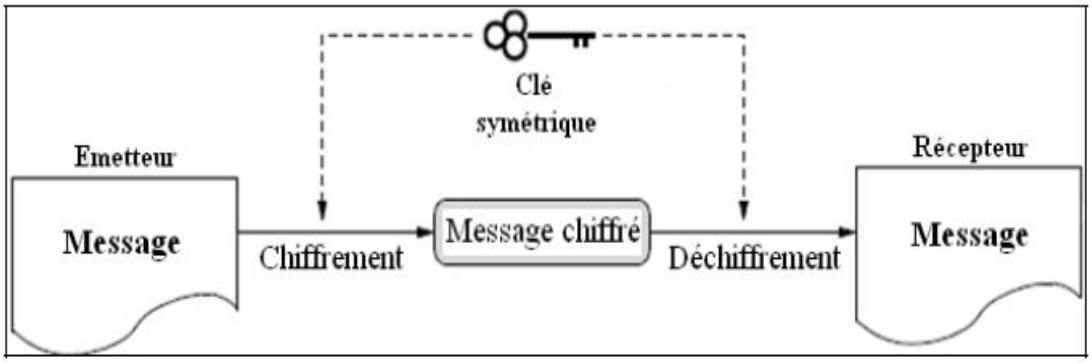

Figure 12 : Le chiffrement symétrique.

Bien que l'on connaisse des algorithmes de chiffrement symétriques rapides et efficaces (comme RC4), ils peuvent exposer un grand contraste dans l'énergie dissipée pendant la construction et la distribution de clés. En effet, la distribution de clés est difficile car dans un système symétrique, chaque nœud a besoin d'une clé partagée avec chaque autre nœud du réseau. Donc on aura à gérer n*(n-1)/2 clés si on considère que le nombre de nœuds dans le réseau est égal à n.

Cependant, de tels algorithmes cryptographiques pourraient être les plus appropriés pour les applications des RCSF. En effet, ils ne requièrent pas d'opérations mathématiques complexes pour crypter ou décrypter les données. Par conséquent, ils n'exigent pas de grandes dissipations énergétiques durant les phases de chiffrement et de déchiffrement.

- **Le chiffrement asymétrique**: Deux clés différentes sont générées par le récepteur: une clé publique diffusée à tous les nœuds servant au chiffrement de données qu'ils vont émettre au récepteur, et, une clé privée maintenue secrète chez le récepteur servant pour le déchiffrement de ces données lorsque ce dernier les reçoit. Le point fondamental sur lequel repose la sécurité du chiffrement asymétrique est l'impossibilité de déduire la clé privée à partir de la clé publique. L'algorithme de chiffrement asymétrique le plus connu est : RSA (Rivest Shamir Adleman).

La figure 13 illustre la méthode de cryptographie par un chiffrement asymétrique :

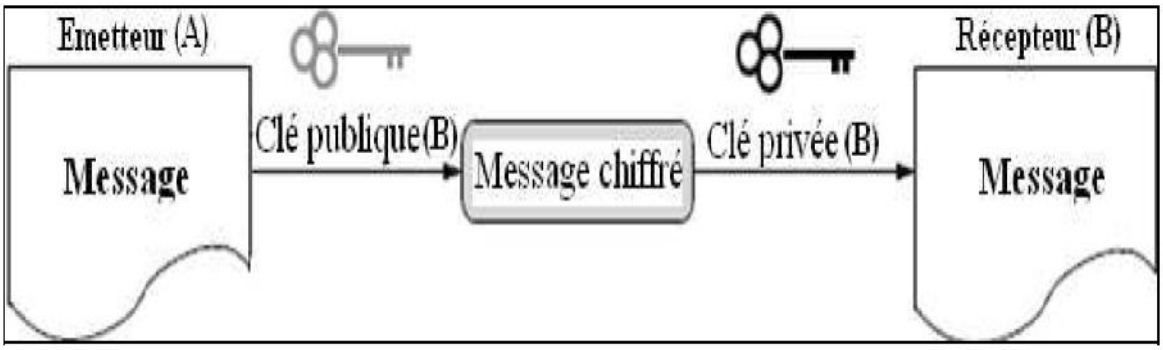

Figure 13 : Le chiffrement asymétrique.

Dans ces algorithmes, différents problèmes mathématiques se présentent à cause des calculs utilisés pour déchiffrer les données reçues. La complexité de telles opérations est très importante parce que les nœuds capteurs exigent une capacité de traitement plus levée et une dissipation d'énergie plus haute. En utilisant le chiffrement asymétrique, chaque nœud capteur souffre d'un autre problème dû au stockage de clés publiques de tous les nœuds restant du réseau.

Cela provoque une forte occupation des mémoires de chaque nœud. Cependant, la distribution de clés est moins pénible car leur échange est fortement simplifié. En effet, avec un système asymétrique, chaque nœud a besoin d'une paire de clés. Si on considère que le nombre de nœuds dans le réseau est égal à n, il faudra donc gérer 2.n clés.

Bien que le chiffrement asymétrique comporte des avantages, il est inutilisable dans les RCSF. Cela est dû à sa lenteur d'exécution et son coût en termes de capacité des ressources.

L'utilisation du chiffrement symétrique dans les RCSF possède quant à elle des inconvénients. Son problème majeur est de pouvoir trouver une méthode qui facilite l'établissement des clés entre les nœuds.

II. 5.2.2. La signature digitale

La signature digitale est un système cryptographique assurant la non-répudiation de la source. Elle repose sur les clés asymétriques. L'émetteur (A) signe les données à transmettre avec sa clé privée (A) en produisant une signature digitale (1). Ce dernier est par la suite envoyé avec les données (2). Si elle peut être déchiffrée avec la clé publique (A) par le récepteur (B) et si son résultat est identique aux données reçues alors la signature est valide4), c'est-à-dire, les données proviennent bien de leur émetteur légitime qui ne pourra pas nier l'émission de ces données dans le futur.

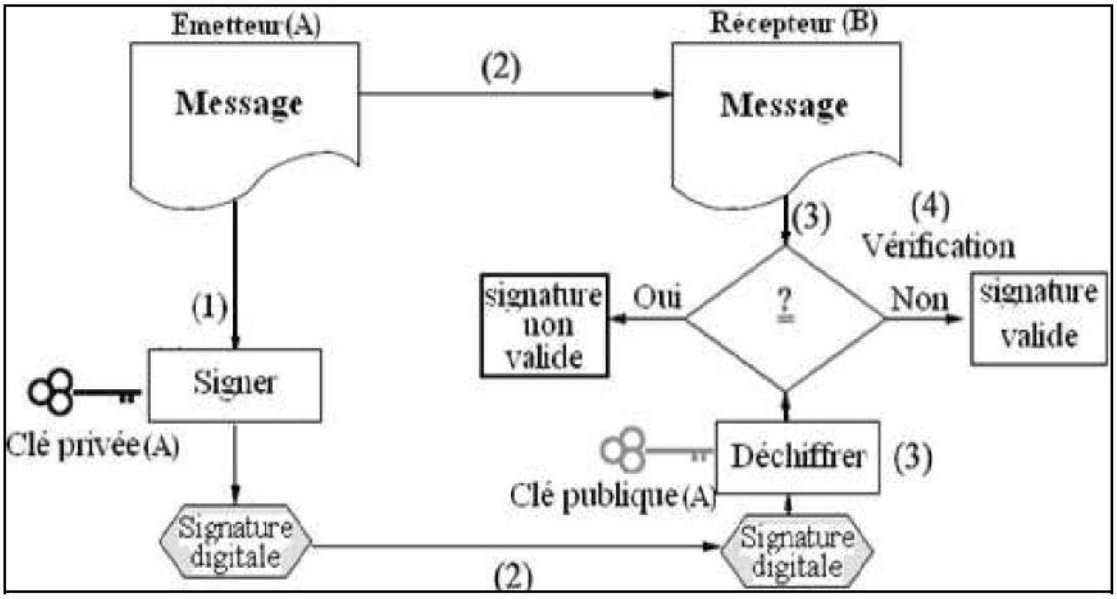

Figure 14: La signature digitale.

II. 5.2.3. La fonction de hachage

C'est le mécanisme qui assure l'intégrité de données. Cette fonction calcule une courte empreinte de taille fixe à partir d'une donnée de taille arbitraire (1). Etant donnée une fonction de hachage f, et un message à transmettre m. La fonction f doit remplir ces conditions:

- Il est facile de calculer f(m), c'est-à-dire, de calculer l'empreinte à partir du contenu du message.
- Il est difficile de calculer m tel que f(m) = f, c'est-à-dire, de trouver le contenu du message à partir de l'empreinte. C'est pourquoi la fonction f est dite « à sens unique ».

- Il est difficile de trouver un autre message m2 tel que f(m) = f(m2), c'est-à-dire, il est difficile de trouver deux messages aléatoires qui donnent la même empreinte et cela mène à la résistance aux collisions. Cette empreinte est recalculée par le récepteur (2) afin qu'il la compare à celle calculée par l'émetteur. Si elles sont différentes (3), alors les données ont été altérées pendant leur transmission. Les fonctions de hachage les plus courantes sont: MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm).

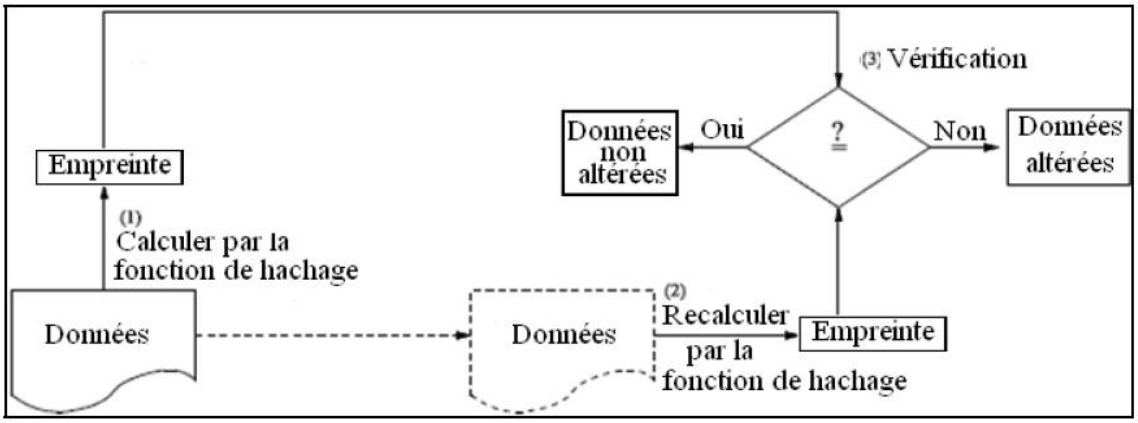

Figure 15: La fonction de hachage.

II. 5.2.4. Le code d'authentification de message MAC

Le code d'authentification de message MAC (Message Authentification Code) fait partie des fonctions de hachage à clé symétrique assurant l'intégrité de données comme toute autre fonction de hachage, en plus, l'authenticité de la source de données. Cette clé est utilisée pour calculer le code MAC par l'émetteur (1). Ce code est par la suite envoyé avec les données (2).

Le récepteur calcule à son tour le code MAC avec cette même clé et le compare au code qu'il a reçu (3). S'ils sont bien identiques (4), alors la source est authentique et les données n'ont pas été altérées. Dans la pratique, HMAC (keyed-Hash Message Authentication Code) est utilisé.

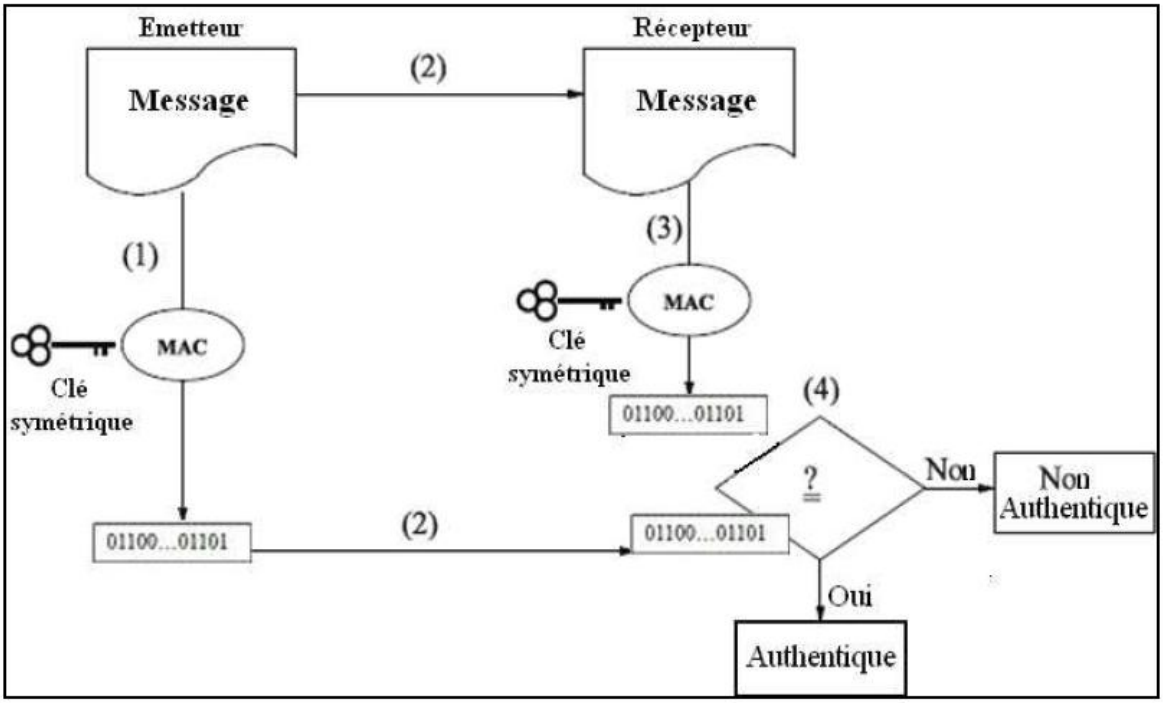

Figure 16 : Le code d'authentification de message MAC.

II. 6. La gestion de clés dans les RCSF

La gestion de clés fournit des mécanismes efficaces, sécurisés et stables de gestion de clés utilisées dans les opérations cryptographiques. Par conséquence, la gestion de clés est un service primordial pour la sécurité de n'importe quel système basé sur la communication. Sous les contraintes des RCSF, la conception d'un système de gestion de clés est un grand défi. Sélectionner une solution cryptographique appropriée pour les RCSF est un autre défi.

II. 6.1. La fonction de gestion de clés dans les RCSF [8]

II. 6.1.1 Définition

La gestion des clés est un des aspects les plus difficiles de la configuration d'un système cryptographique de sécurité. Pour qu'un tel système fonctionne est soit sécurisé, chacun des utilisateurs doit disposer d'un ensemble de clés secrètes (dans un système à clés secrètes) ou de paire de clés publiques/privés (dans un système à clés publiques). Cela implique de générer les clés et de les distribuer de manière sécurisée aux utilisateurs ou d'offrir à l'utilisateur le moyen de les générer. Il doit aussi pouvoir enregistrer et gérer ses clés publiques et privées de manière sure. Dans les systèmes à clés publiques, la gestion des clés

comprend la capacité à vérifier et à gérer les clés publiques des autres utilisateurs qui sont signées sous formes de certificats numériques.

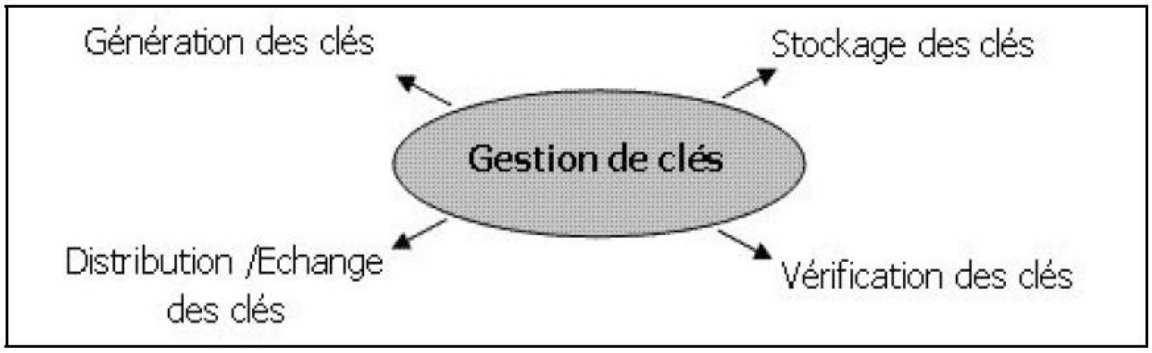

Figure 17: Fonctions de la gestion de clés

II. 6.1.2 Pourquoi la gestion de clés dans les RCSF ?

Après leur déploiement, les capteurs ont besoin d'établir des clés cryptographiques avec leurs voisins pour assurer des services de sécurité:

- ✓ Sécuriser le routage
- ✓ Sécuriser l'agrégation
- ✓ Coopération (authentification), etc.

II. 6.1.3 Contraintes de conception

La figure 18 résume les contraintes découlant des propriétés des RCSF, à prendre en compte dans la conception d'une solution de gestion de clés pour les RCSF.

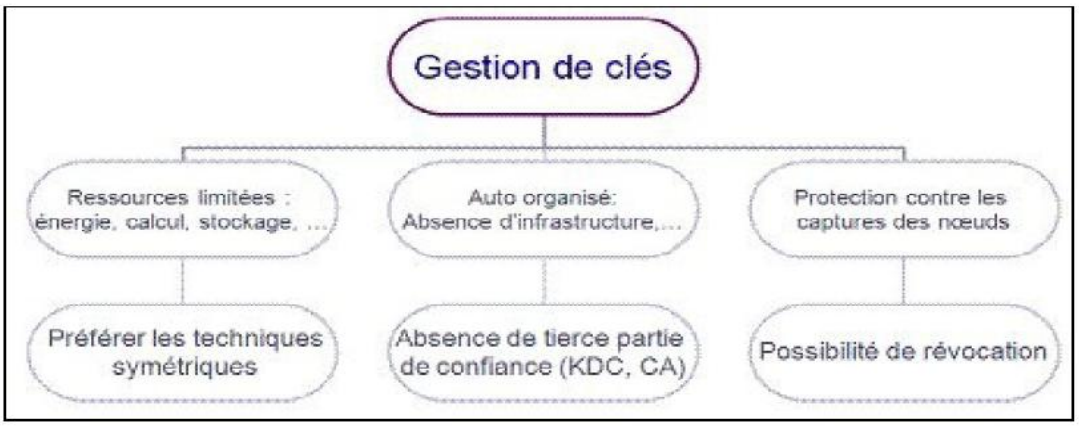

Figure 18 : Contraintes de conception de solutions de gestion de clés

II. 6.1.4 Systèmes asymétriques et symétriques

Dans les systèmes à clés publiques, l'échange de clé est fortement simplifié. Chaque partie communicante publie sa clé publique. Les clés publiques sont habituellement distribuées en utilisant des certificats numériques, utilisés par le destinataire pour authentifier la clé publique reçue ; toutes les communications avec cette partie seront alors cryptées avec cette clé. L'avantage principal d'utiliser des algorithmes à clés publiques est la facilité de gestion des clés et leur fiabilité.

Les inconvénients de cette approche incluent la consommation d'énergie due au calcule des algorithmes à clé publiques, la consommation d'énergie due à la transmission des certificats, et le stockage des clés connues pour être plus grandes que les clés symétriques. Employer des mécanismes de clés symétriques pour l'établissement de la confiance réduit considérablement la consommation d'énergie des nœuds capteurs et l'espace de stockage réservé pour accueillir ces clés.

Cependant, l'échange de clés dans les systèmes à clés symétriques est beaucoup plus compliqué. Habituellement, une seule clé symétrique est utilisée entre deux parties communicantes, sur une seule session ou sur une période limitée.

Bien que la cryptographie à clé publique comporte des avantages certains par rapport à la cryptographie à clé symétrique et malgré les recherches qui visent à les appliquer aux RCSF, la cryptographie à clé symétrique possède ses propres qualités qui la rend toujours la plus préférée pour les RCSF. Pour cette raison la plupart des schémas de gestion de clés proposés pour les RCSF sont basés sur la cryptographie symétrique.

Le problème majeur avec la cryptographie symétrique est de pouvoir trouver une méthode qui facilite l'établissement des clés entre les nœuds. La solution commune est d'utiliser une méthode de pré-distribution, dans laquelle les clés sont chargées dans les nœuds capteurs avant le déploiement.

La figure 19 illustre une taxonomie des solutions de gestion de clés basée sur la pré-distribution. Dans cette taxonomie, les protocoles sont classés selon la façon avec laquelle es nœuds voisins partagent des clés communes (probabiliste ou déterministe), et selon la

topologie du réseau (hiérarchique ou plate).

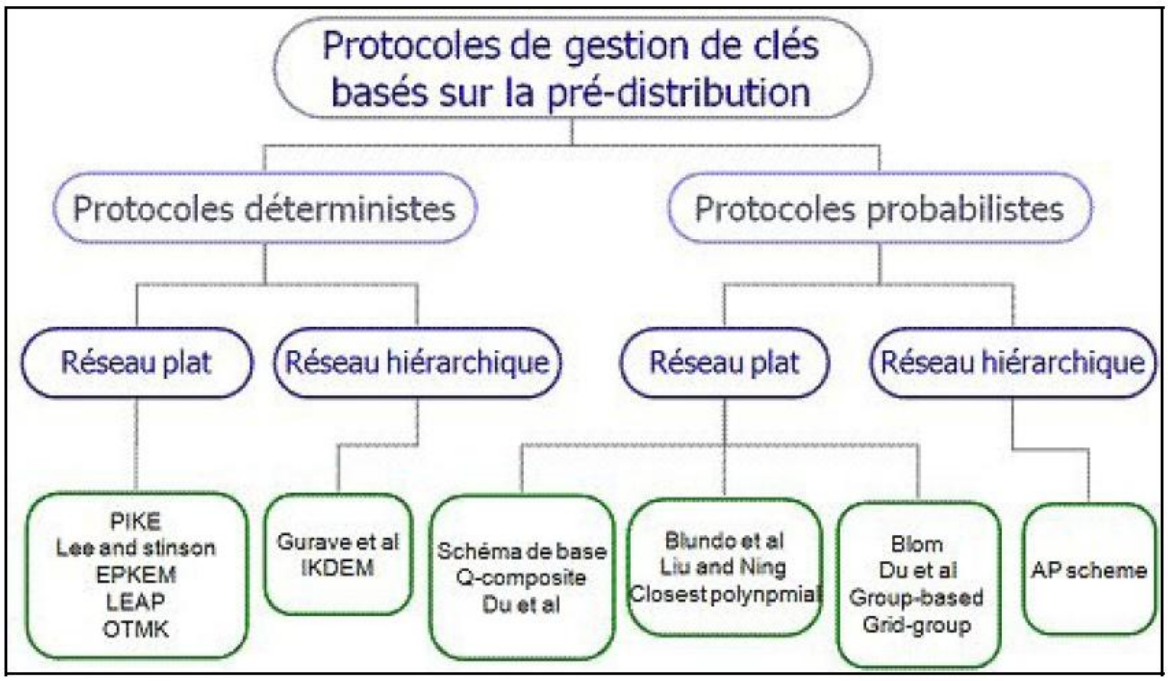

Figure 19 : Taxonomie de pré-distribution de clés pour les RCSF.

II. 6.2 Schéma aléatoire de pré-distribution de clés de L.ESCHENAUER et D.GLIGOR

Eschenauer et Gligor ont proposé un schéma de gestion de clé basé sur la probabilité de partager une clé entre les nœuds d'un graphe aléatoire. Il fournit des techniques pour la pré-distribution de clé, la découverte de la clé partagée, l'établissement de chemin de clé, et la révocation de clé.

L'idée maîtresse de ce schéma, est de distribuer aléatoirement un certain nombre de clés, issues d'un ensemble fini à chaque nœud du réseau avant son déploiement. Deux nœuds quelconques seront en mesure de s'échanger des messages sécurisés s'ils possèdent une clé commune.

II. 6.2.1 Phase de pré-distribution de clés

Un grand ensemble S de clés est générée (217-220 Clés). Pour chaque nœud, m clés sont choisies au hasard de l'ensemble S (S= {(kid1, key1), (kid2, key2),....}). Ces m clés sont stockées dans la mémoire du nœud et forment le trousseau de clés du nœud. Le nombre de

clés |S| de l'ensemble est choisi de telle manière que deux sous-ensembles aléatoires de S de taille m auront une certaine probabilité p d'avoir au moins une clé en commun, par exemple pour une probabilité p=0.5 on a besoin d'un sous ensemble de taille m=75 clés de l'ensemble S de taille |S|=10,000 clés.

II. 6.2.2 Phase de découverte de clés partagées

Les nœuds découvrent leurs voisins et plus particulièrement ceux avec qui ils sont en mesure de communiquer de façon sécurisée car ils possèdent une clé identique dans leur trousseau de clés respectif. Le protocole peut être de diffuser la liste des identités kidi des clés possédées. La clé partagée devient la clé de session du lien entre les deux nœuds. La figure 20 illustre cette phase :

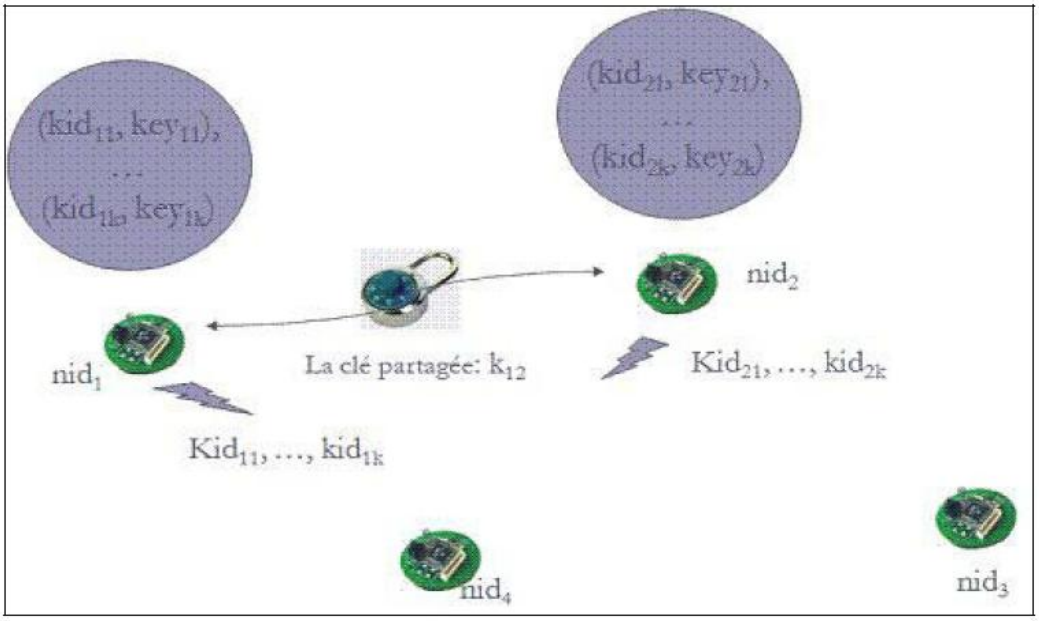

Figure 20 : Découverte des clés partagées.

II. 6.2.3 Phase d'établissement de chemin de clé

Après la phase de découverte de clés partagées, le réseau devient un graphe connecté formé de quelques liens sécurisés. Les nœuds peuvent alors utiliser les liens existants pour mettre en place des clés partagées avec leurs voisins qui ne partageaient pas de clé en commun avec eux. La figure 21 illustre cette phase :

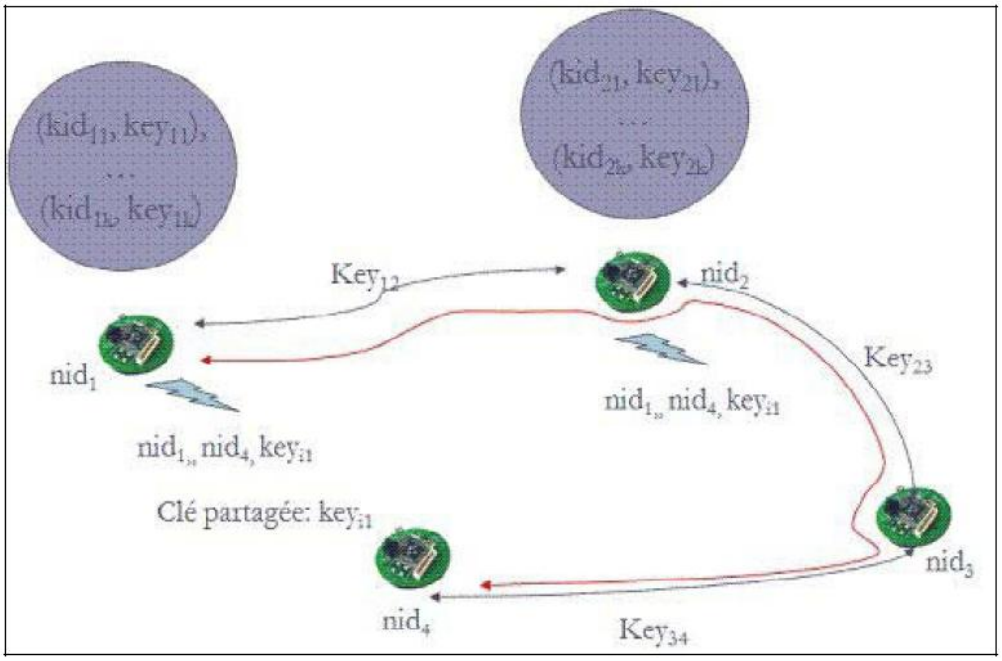

Figure 21: Etablissement de chemins sécurisés.

II. 6.2.4 La révocation de clés

La révocation d'un nœud compromis se fait par l'élimination de leur trousseau de clés. Pour cela, un nœud contrôleur (qui a une grande connectivité et peut être mobile) annonce un message simple de révocation contenant une liste signée de k identificateurs des clés (kidi) pour que ces clés soient retirées des trousseaux de clés des autres nœuds.

La liste des identités est signée par une clé de signature Ke générée par le nœud contrôleur et envoyée en unicast à chaque nœud i en la chiffrant avec la clé Kci (la clé Kci est partagée entre le contrôleur et le ième nœud pendant la phase de pré- distribution de clés). Quelques liens seront disparus à cause de la suppression de clés du nœud compromis ce qui nécessite une reconfiguration de ces liens (par la découverte de clés partagées ou l'établissement de chemin de clé). La figure 22 illustre cette phase :

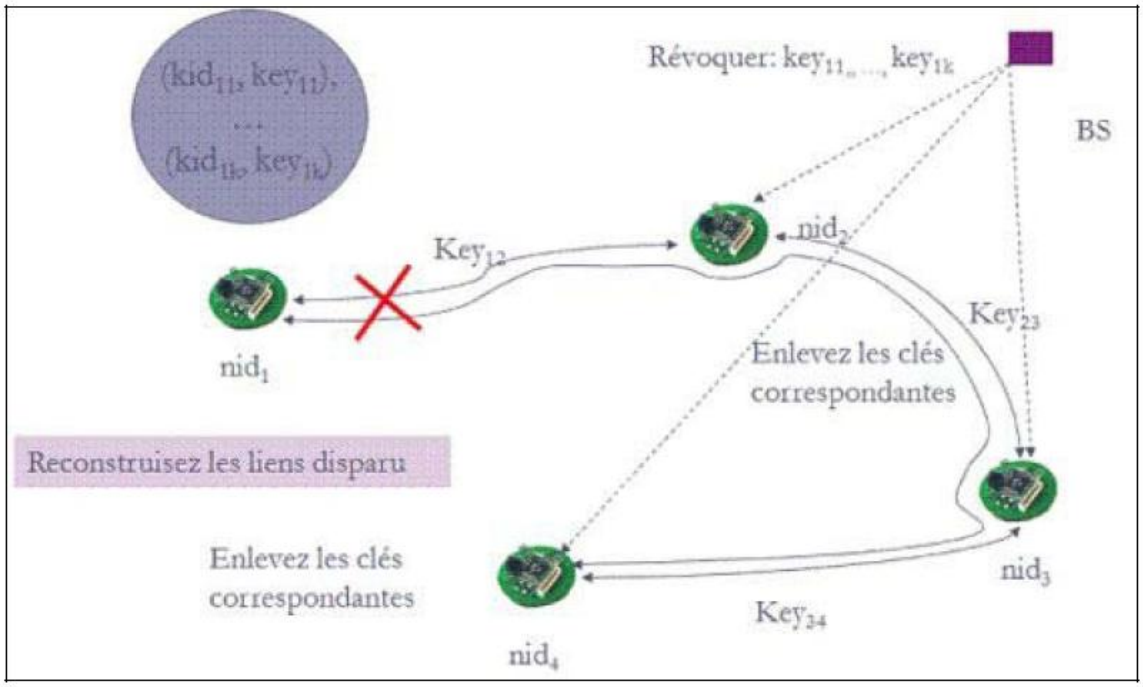

Figure 22 : Révocation de clés

II. 6.2.4 Schéma q-composite de H.CHAN, A.PERRIG et D.SONG

Ce schéma est identique à celui de Eschenaur et Gligor sauf qu'au lieu d'exiger le partage d'une clé commune pour sécuriser un lien, une paire de nœud doit partager q clés avec q > 1 pour établir un lien sécurisé. La nouvelle clé utilisée pour la communication entre ces deux nœuds est le hash de toutes les clés partagées, par exemple pour deux nœuds quelconque qui partage q' clés (q'≥q) la clé utilisée pour la communication est K = hash (k1 || k2 || ... || kq'). Plus le nombre de clé partagées augmente plus la résilience contre la capture du nœud augmente.

Autrement, lorsque le nombre, exigé, de clés partagées augmente, il devient plus difficile à un attaquant avec un ensemble donné de clés de casser un lien.

Cependant, pour préserver une probabilité donnée p que deux nœuds partageant des clés suffisantes pour établir un lien sécurisé, il est nécessaire de réduire la taille de l'ensemble de clés S. Ceci permet à un attaquant de gagner un plus grand échantillon de S en cassant peu de nœuds. La figure 23 illustre un exemple de partage de clés avec q=2.

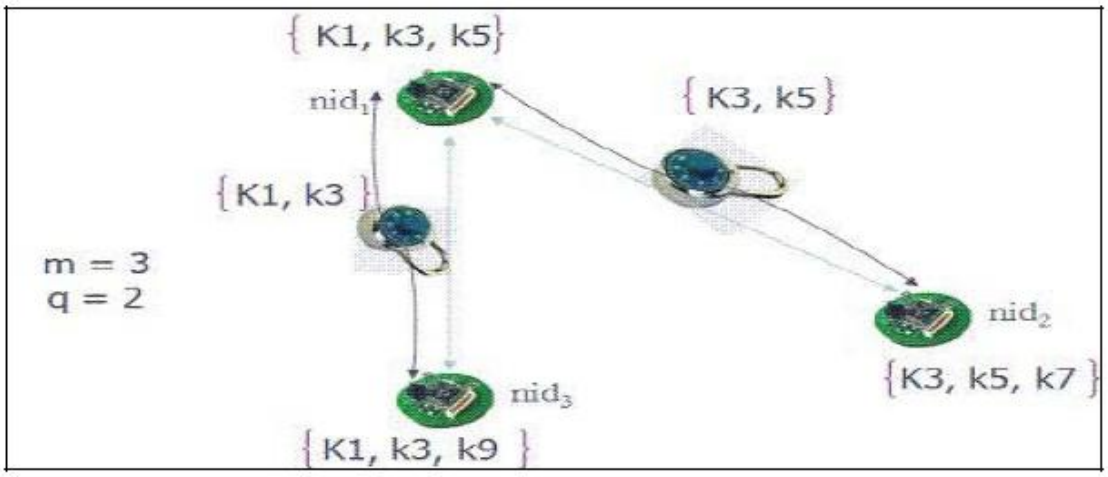

Figure 23 : Schéma q-composite

II. 7. Sécurité du routage dans les RCSF [8]

La couche de routage est le module responsable d'acheminer correctement une donnée d'un point du réseau vers un autre. Pour assurer ce rôle, la couche de routage est composée de deux blocs fonctionnels : la construction de routes et le relais des données. Le premier composant permet de construire un backbone connectant les nœuds aux destinations désirées via un ensemble de chemins.

Le deuxième composant quant à lui utilise ce backbone afin d'acheminer les données captées vers les utilisateurs finaux. Un adversaire désirant attaquer les réseaux peut alors s'en prendre à l'un des deux composants qu'il faudra protéger.

II. 7.1. Attaques sur les protocoles de routage dans les RCSF

Vus les contraintes des RCSF, la plus part des protocoles de routage sont assez simple, et par conséquent assez vulnérables aux attaques. Un nœud malicieux peut opérer sur deux niveaux :

- Les données échangées entre les nœuds.
- La topologie du réseau créée par le protocole.

Ces attaques peuvent être classées en deux catégories : actives et passives.

II. 7.1.1 Attaques actives

.Attaque de "jamming"

Vu la sensibilité du média sans fil au bruit, un nœud peut provoquer un déni de service en émettant des signaux à une certaine fréquence. Cette attaque peut être très dangereuse car elle peut être menée par une personne non authentifiée et étrangère au réseau.

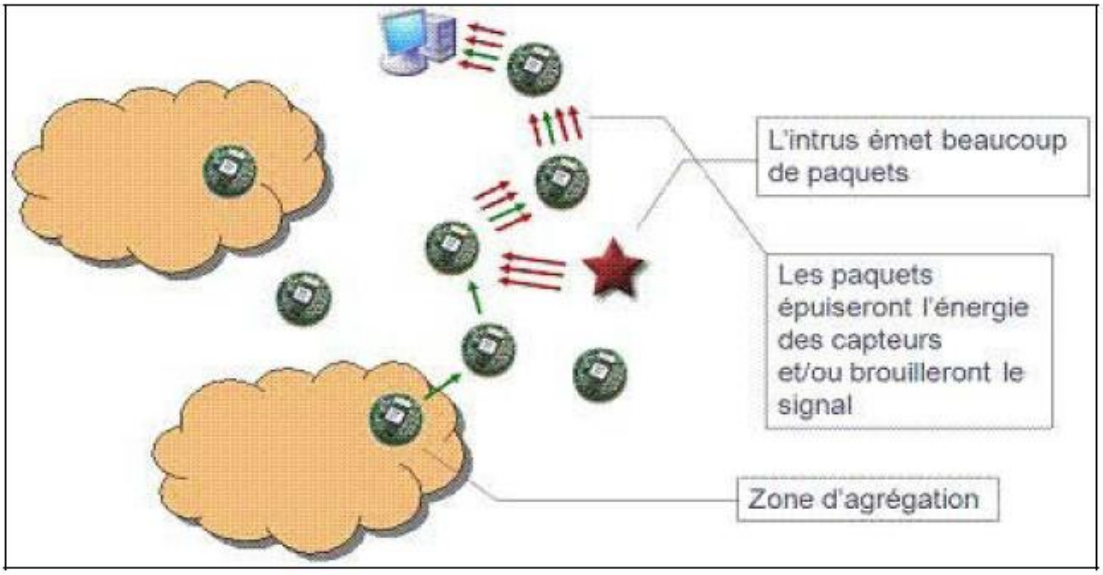

Figure 24 : Attaque de "jamming"

.Attaque Sink hole

Dans une attaque sinkhole, le nœud essaye d'attirer vers lui le plus de chemins possibles permettant le contrôle sur la plus part des données circulant dans le réseau. Pour ce faire, l'attaquant doit apparaître aux autres comme étant très attractif, en présentant des routes optimales.

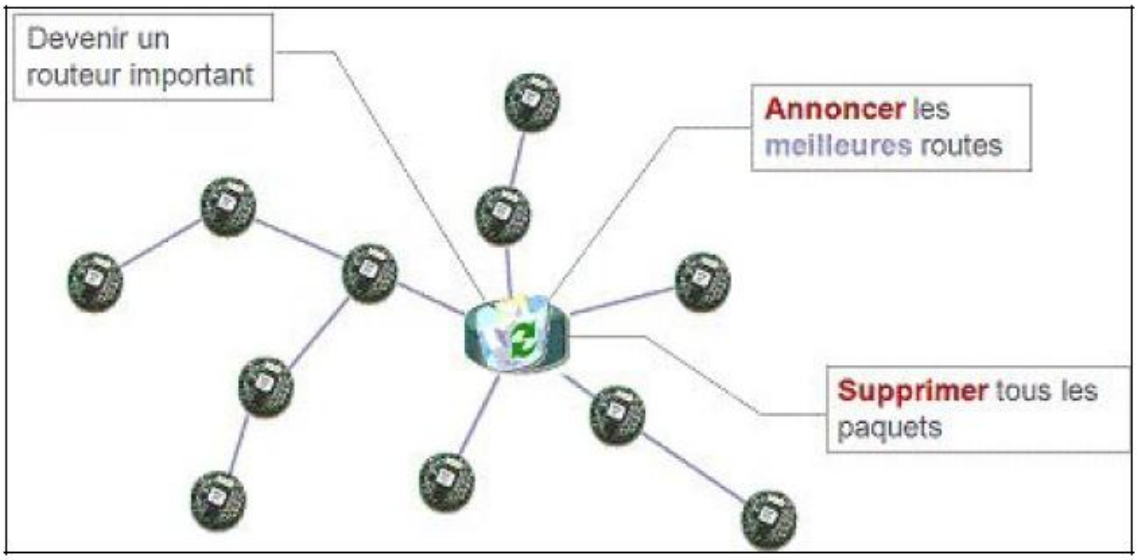

Figure 25: Attaque sink hole.

. Attaque Wormhole

Dans une attaque wormhole, un attaquant reçoit des paquets dans un point du réseau, puis les encapsule vers un autre attaquant pour les réintroduire dans le réseau. La figure 26 illustre un exemple d'une attaque Wormhole :

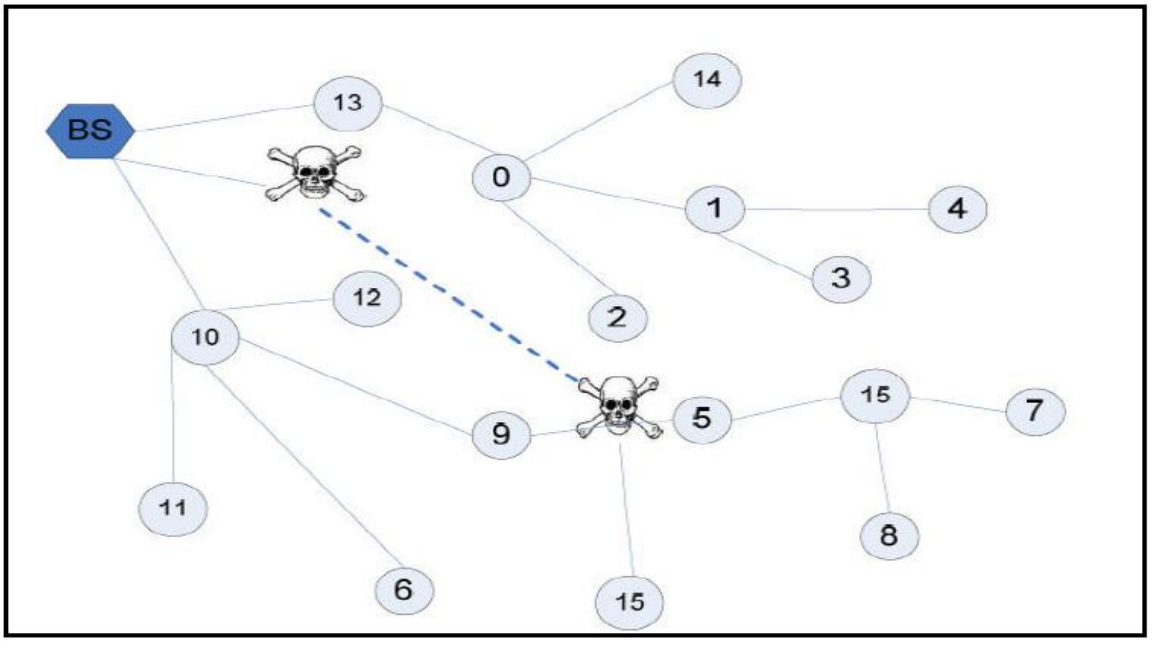

Figure 26 : Attaque Wormhole.

. Routing table poisoning

Certaines optimisations ont été développées afin d'augmenter la connaissance des chemins. Lorsqu'un nœud entend (en mode promiscues) une information de routage, il met à jour sa table de routage locale en conséquence. Un nœud malicieux peut émettre un nombre important de fausses informations, remplissant ainsi les tables de routage des nœuds. Comme ces tables possèdent des tailles limitées, cela va engendrer un débordement, et les tables ne contiendront que de fausses routes.

. Attaque Sybil

Dans certains algorithmes, la fiabilité du routage est implémentée par l'instauration d'une redondance de chemins. Un attaquant peut altérer ce genre de systèmes en "endossant" plusieurs identités, ce qui permet de créer plusieurs routes passant par le nœud malicieux, qui ne sont en réalité qu'un seul chemin.

. Attaque Hello flooding

La faible portée de capteurs et la présence d'attaquant de classe laptop ont permis l'introduction d'une nouvelle attaque : hello flooding. Cette attaque se base sur le fait que la plus part des liens entre l'attaquant laptop et les capteurs sont unidirectionnels. Donc, un attaquant peut diffuser l'information d'une route optimale vers tous les nœuds du réseau en émettant avec un signal puissant, et tous les nœuds mettront à jour leurs tables locales. Lorsqu'un nœud veut communiquer, il ne pourra pas utiliser cette route car le prochain saut, qui est l'attaquant, est hors portée.

II. 7.1.2 Attaques passives

. Selective Forwarding

Tous les protocoles de routage supposent que les nœuds sont "honnêtes" et vont relayer normalement les paquets qui transitent par eux. Cependant, un attaquant peut violer cette règle en supprimant la totalité ou une partie de ces paquets. De plus, si l'attaquant au paravent utilisé une attaque sinkhole, il devient un routeur important dans le réseau. Donc, en abandonnant son rôle de routeur, les performances du système seront gravement dégradées.

.Eavesdropping

Comme le média sans fil est un média ouvert, un nœud peut entendre toutes les

communications de ses voisins. Cela peut divulguer d'importantes informations, comme la localisation d'un nœud important. La combinaison avec une attaque sinkhole aggrave d'avantage l'impact de cette attaque.

II. 7.2 Types de solutions

Nous distinguons trois niveaux de solutions aux attaques sur le routage de données dans les RCSF :

La prévention contre les attaques actives: dans cette catégorie on utilise généralement des mécanismes cryptographiques pour protéger la signalisation qui sert à la construction de routes. C'est généralement des mécanismes d'authentification et de contrôle d'intégrité qui sont utilisés pour empêcher un nœud malicieux d'injecter, de modifier et/ou de supprimer une information qui servira pour la découverte, la construction ou la maintenance d'une route.

La détection de comportements suspects: dans cette catégorie on tente de déceler des comportements qui témoignent d'une attaque passive (manque de coopération, refus de relais de paquets, etc...).

La tolérance : dans cette catégorie, on introduit des mécanismes de tolérance de défaillance de nœuds à cause d'attaques ou de pannes. Le routage multi-chemin en est un exemple typique.

La figure 27 résume les catégories de solutions à préconiser pour faire face à différents types d'attaques :

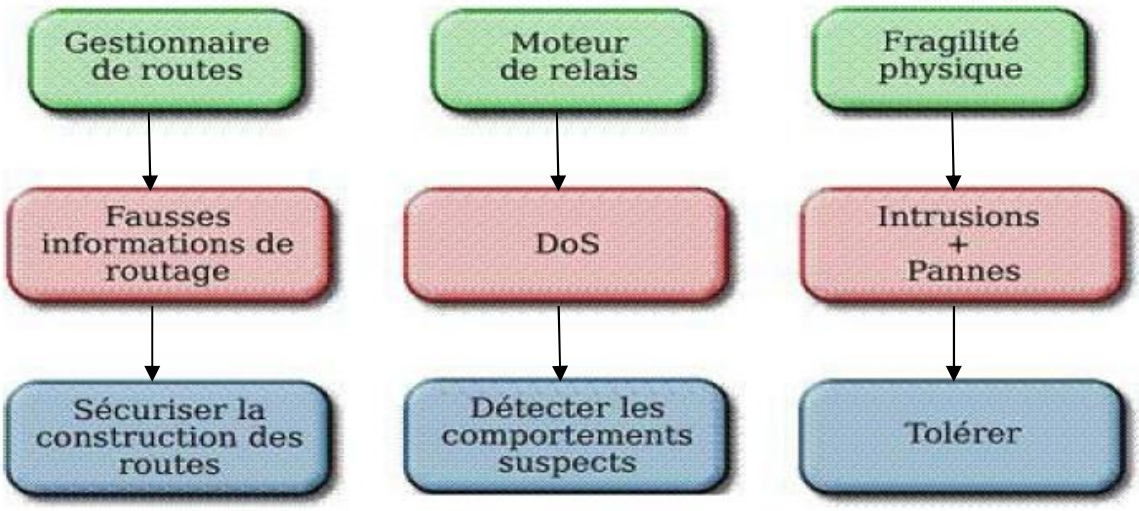

Figure 27: Catégories de solutions contre les attaques sur le routage.

II. 8 Conclusion

Nous avons abordé dans ce chapitre l'aspect de sécurité dans les RCSF et les contraintes de ces derniers qui rendent impossible l'application des méthodes classiques de sécurité dans de tels réseaux. Nous avons aussi introduit les différents protocoles et solutions de gestion de clés proposés pour les RCSF. Nous avons vu que les protocoles basés sur la méthode de pré-distribution sont les plus appropriés aux RCSF, pour leur faible coût.

L'inadaptation de la cryptographie asymétrique a conduit les recherches dans la gestion de clés vers la cryptographie symétrique et ainsi aux méthodes de pré-distribution de clés. Nous croyons que cette situation peut changer dans l'avenir. Des méthodes de cryptographie asymétriques à faible coût comme la ECC ont un avenir prometteur pour sécurisé les RCSF et méritent des études plus approfondies.

Chapitre III

Présentation des normes IEEE 802.15.4 / ZigBee.

III.1. Généralités

ZigBee est une technologie de réseau sans fil personnel (WPAN) destinée à l'électronique embarquée à très faible consommation énergétique. Elle propose une pile propriétaire et légère, déclinable dans plusieurs versions plus ou moins complètes, pour des applications de transferts de données faibles débits et de faibles taux d'utilisation du medium.

III.1.1. Le projet ZigBee [15]

L'idée initiale du projet ZigBee date de 1998 ; une première proposition (v0.1) a été présentée courant 2000 puis rapidement une seconde (v0.2) à la fin de la même année. Apres une soumission à l'IEEE mi 2001, la ZigBee Alliance a été créée pour développer et promouvoir la norme. La production de modules compatibles fut alors prévue et les premiers produits (puces radio, piles protocolaires, modules intégrés, kits de développement, etc.) sont apparus et sont disponibles depuis la fin de l'année 2004.

ZigBee s'appuie sur la norme IEEE 802.15.4 (que nous désignerons par la suite par « 802.15.4 ») pour les couches physique et liaison, qui sont les couches 1 et 2 du modèle OSI. ZigBee propose ensuite ses propres couches supérieures (réseau, etc.) qui doivent faire l'objet d'une demande auprès de la ZigBee Alliance pour être utilisées. A ce titre, des droits sont perçus par la ZigBee Alliance pour tout emploi d'une pile ZigBee dans le cadre d'une application industrielle.

III.1.2. Objectifs et domaine d'application [16]

ZigBee est un réseau sans fil à courte portée qui utilise les ondes hertziennes pour transporter des messages entre deux ou plusieurs entités réseaux. Il est caractérisé par une portée comprise entre quelques mètres et quelques centaines de mètres et un débit faible (max. 250kbits/s). La différence entre ZigBee et la plupart des autres WPAN existants se situe au niveau de l'utilisation du médium hertzien ; ZigBee est optimisé pour une faible utilisation du médium partage par tous, par exemple 0.1% du temps. Typiquement, un module ZigBee occupera le medium pendant quelques millisecondes en émission, attendra éventuellement une

réponse ou un acquittement, puis se mettra en veille pendant une longue période avant l'émission suivante, qui aura lieu à un instant prédéterminé. Cette nécessité introduit des problématiques de recherche intéressantes, notamment au niveau des couches Liaison (temporisation et stockage des messages, accès original au médium) et Réseau (routage avec respect de contraintes énergétiques).

ZigBee est conçu pour interconnecter des unités embarquées autonomes comme des capteurs/actionneurs, à des unités de contrôle ou de commande. De telles entités embarquées pouvant dès lors entre alimentées pendant plusieurs mois par des piles standards.

III.1.3. Consommation énergétique [17]

Le point fort de ZigBee est sa très faible consommation énergétique, grâce à un mode de fonctionnement appelé *doze* ou somnolence. Ce mode permet à une entité communicante ZigBee de consommer très peu d'énergie (100µW) tout en permettant de passer en mode opérationnel en très peu de temps (300 µs), contrairement à d'autres WPAN comme Bluetooth par exemple.

Bien que les progrès de l'électronique en terme de consommation énergétique soient sensibles ces derniers temps (possibilités accrues et rapides de mise en veille, baisse significative des courants de fuites dans le silicium, etc.), les bonnes performances de ZigBee sur ce plan sont essentiellement dues au mode somnolence, qui implique par conséquent une faible utilisation protocolaire du médium. Un réseau ZigBee utilisé en continu, par exemple pour une application de type streaming audio consommera autant d'énergie que tout réseau sans fil classique, à puissance d'émission et débit équivalents.

III.1.4. Topologies [18]

Selon les besoins de l'application, la norme IEEE 802.15.4 prévoit deux topologies : étoile (star) ou point à point (peer to peer). Le réseau formé est appelé PAN. Ces deux topologies sont représentées en figures 28 et 29 Au dessus de 802.15.4, la couche réseau de ZigBee permet la création de réseaux plus complexes comme les réseaux maillés (mesh) ou arborescents (tree) grâce à un routage automatique des paquets de niveau 3 (niveau réseau).

III.1.4.1 Topologie étoile

Dans la topologie étoile, les entités RFD sont connectées à un nœud FFD central appelé coordinateur; dans cette topologie, tous les messages sont relayés par le coordinateur, comme dans un Piconet Bluetooth avec le maître ou dans un réseau Wifi en mode infrastructure avec le point d'accès. Les communications directes entre entités RFD sont impossibles. Notons que le rôle central du coordinateur implique de plus fortes dépenses énergétiques ; un coordinateur devra donc généralement prévoir une source d'alimentation non contrainte (batteries conséquentes, secteur).

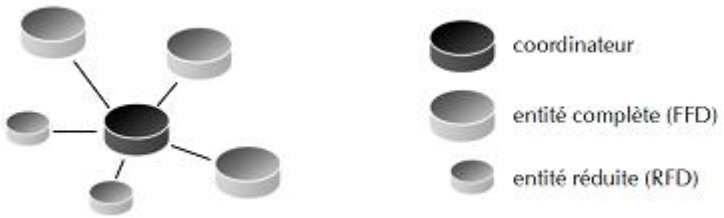

Figure 28: Représentation de la topologie en étoile.

III.1.4.2. Topologie point à point

Dans la topologie point à point (peer-to-peer), un FFD peut communiquer directement avec tout autre FFD s'ils sont à portée radio l'un de l'autre. Dans cette topologie, on retrouve un coordinateur unique comme dans la topologie étoile. Son rôle est de tenir à jour une liste des participants au réseau et de distribuer les adresses courtes.

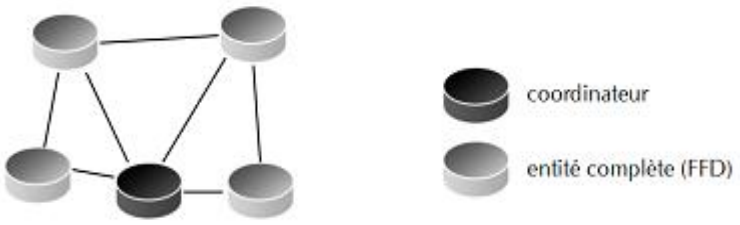

Figure 29 : Représentation de la topologie point à point.

III.1.4.3. Topologies plus complexes

Avec l'aide d'une couche réseau et d'un système de routage des paquets de données, il est possible d'élaborer des topologies plus complexes. La technologie ZigBee propose une couche réseau permettant de créer facilement de telles topologies grâce à des algorithmes de routage automatique tels que le *cluster trée* (arborescence de cellules) ou les réseaux maillés *mesh*. Nous aborderons ces techniques dans la partie consacrée à la couche réseau.

III.1.5.Adressage

Toute entité 802.15.4 possède une adresse unique appelée adresse MAC. A la différence de 802.3, une adresse MAC 802.15.4 a une longueur de 64 bits, soit 8 octets, contre 6 dans 802.3 ou 802.11. Dans 802.15.4, cette adresse est également appelée adresse étendue. Elle peut être utilisée dans les dialogues au sein du PAN, mais une seconde adresse appelée adresse courte, sur 16 bits, sera préférée dans la plupart des cas compte tenu des débits de transmission, relativement faibles. L'adresse courte est attribuée par le coordinateur du PAN au moment de l'association au réseau. La norme 802.15.4 ne prévoit pas de règle pour le choix de ces adresses, cette tache est laissée au libre arbitre des couches supérieures. Nous verrons plus loin que dans la spécification de sa couche réseau, ZigBee propose un algorithme de distribution d'adresses automatique et décentralisé. Notons d'ores et déjà que ZigBee propose l'utilisation d'un adressage commun pour les couches 2 et 3, mais, à la différence d'autres protocoles comme IPv6, c'est la couche 3 qui impose son adresse à la couche 2.

III.1.6. Valeurs typiques

Pour conclure cette partie sur les généralités des deux normes, voici en résumé les valeurs typiques caractérisant IEEE 802.15.4 et ZigBee :

• Débit : 250 kbits/s sur le médium physique pour PHY2450.

• Puissance d'émission typique : entre 0 et 3 dBm.

• Portée radio : quelques centaines de mètre en espace libre.

• Consommation énergétique du composant d'émission / réception (hors traitement CPU) :

◦ 3 µA en hibernation (*hibernate mode*).

◦ 40 µA en somnolence (*doze mode*).

◦ 1 mA au repos (*idle mode*).

◦ 30 mA en émission.

◦ 40 mA en réception.

• Taille de la pile protocolaire (code + mémoire) :

◦ Inferieure à 20 ko pour une entité réduite (RFD).

◦ Entre 40 à 60 ko pour une pile complète (FFD).

• Nombre d'entités connectables au réseau :

◦ 256 dans une étoile (2^8).

◦ 65536 dans un PAN maillé (2^{16}).

◦ 18446744073709551616 adresses MAC disponibles (2^{64}).

• Accès au médium : pur CSMA/CA3 (sans RTS/CTS) ou organisé (mode balisé avec slots dédiés).

• Détection / correction d'erreurs : FCS3 16 bits dans la trame MAC.

III.2. Présentation de la pile protocolaire ZigBee [19]

III.2.1. Quelques notions fondamentales

Comme la plupart des technologies réseaux, l'ensemble des protocoles décrits par la norme ZigBee est représentable sous la forme d'une pile protocolaire découpée en plusieurs couches. Ce découpage permet de séparer clairement les différentes tâches; l'identification des spécialités des différents acteurs et des différents métiers de la conception réseau est ainsi rendue plus claire.

III.2.1.1. Le découpage en différentes couches

La pile proposée par l'IEEE et la ZigBee Alliance suit les recommandations de l'ISO en terme de séparation des rôles attribués aux différentes couches. Comme cela a été dit

précédemment, cette pile reprend les couches 1 et 2 normalisées dans la norme 802.15.4 et ajoute ses propres couches supérieures.

La couche 1 (couche physique) décrit les caractéristiques de l'interface radio (fréquences, largeur de bande, modulation, débit binaire, etc.) ; la couche 2 (couche liaison) décrit les caractéristiques de la sous- couche MAC (gestion des accès au médium) et la sous-couche SSCS3 (formation de trame, convergence des données) ; la couche 3 (couche réseau) décrit le processus de routage des données sur le réseau ; enfin, la couche la plus haute (couche application) décrit le système élaboré de profils, à l'instar de Bluetooth ou IrDA, qui permet la normalisation du niveau application directement dans la pile protocolaire, au même titre que les couches basses.

III.2.1.2. Le principe de l'encapsulation

Rappelons tout d'abord le principe générique de l'encapsulation : lorsque deux entités d'une même couche s'échangent des messages, les données sont de fait véhiculées par les couches inferieures. Les couches les plus hautes auront généralement une bonne connaissance de la raison de la communication, mais une piètre idée de ce qui se passe réellement sur le médium (le chemin emprunté par l'information, etc.). A l'opposé, les couches les plus basses auront une connaissance très précise sur la manière dont les données sont gérées et transportées, mais très peu d'informations sur le contenu réel et ce qu'elles représentent. Cependant, c'est le système dans son ensemble qui va permettre de transmettre des informations de manière fiable sur un réseau étendu et hétérogène.

Le rôle d'un réseau est bel et bien de transmettre des données ; les données que reçoit une couche N par la couche N+1 sont appelées les données de service. On parlera d'une unité de données de service, ou SDU3, pour designer un ensemble de données passées par la couche supérieure. Lorsqu'une couche veut transmettre un message, elle le transmet à la couche immédiatement inferieure en y ajoutant des informations que son homologue, l'entité de même couche à l'autre bout du réseau, saura comprendre pour traiter les données reçues. Ces informations ajoutées peuvent précéder les données à transmettre – on parlera alors d'entête, ou header, HR – ou bien les succéder – on parlera alors de *postambule*. L'ensemble passé à la couche inférieure (en-tête, données de service, postambule) formera l'unité de données du

protocole, ou PDU. La couche inferieure traitera le PDU de la couche supérieure comme son SDU. Généralement, on ajoute la première lettre du nom de niveau pour designer un HR, un PDU ou un SDU. Par exemple, un PDU de niveau MAC sera désigné par MPDU (MacPDU) et un SDU de niveau Physique sera désigné par PSDU (PhySDU). Notons qu'un MPDU est équivalent au PSDU, puisque les niveaux PHY et MAC sont mitoyens dans une pile protocolaire classique comme celle de ZigBee.

Le principe générique de l'encapsulation est illustré par la figure 30 Un exemple applique à 802.15.4

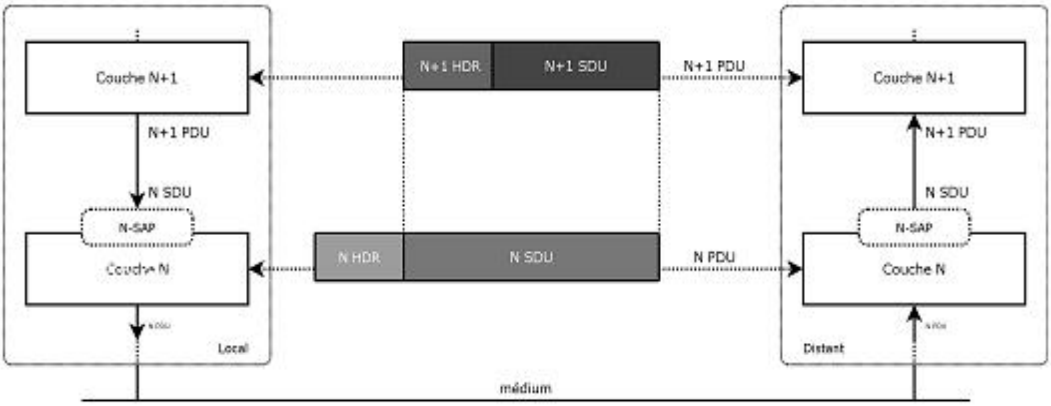

Figure 30 : Le principe générique de l'encapsulation.

III.2.1.3 Protocole d'échange entre deux couches voisines

Les échanges de messages entre deux couches mitoyennes se font selon le principe classique du service de niveau n, service assuré par la nième couche de la pile. Pour accéder à ce service, la couche immédiatement supérieure (n + 1) peut accéder au Point d'Accès de Service (SAP) de niveau n.

Pour être accessible, un SAP propose un jeu de primitives propre à ses capacités (par exemple : scanner le médium radio 2,4GHz, créer une connexion au réseau, envoyer des données, etc.). Selon ses besoins, la couche supérieure appelle les primitives qu'elle souhaite dans l'ordre imposé par son protocole.

Pour s'échanger des messages, deux couches mitoyennes disposent de quatre types de primitives :

1. ***Request*** : demande effectuée par le service local de niveau n + 1 au SAP de niveau n.

2. ***Indication*** : la demande qui vient d'être faite par le *request* est acheminée jusqu'au nœud destinataire par le réseau ; le SAP distant de niveau n le transmet à la couche n + 1.

3. ***Response*** : la couche distante de niveau n + 1 répond en envoyant un message à son entité paire.

Pour être acheminé par le réseau, le message est passé au SAP de niveau n.

4. ***Confirm*** : le SAP local de niveau n transmet cette réponse au service de niveau n + 1, qui avait initié la requête.

La figure 31 illustre ce fonctionnement.

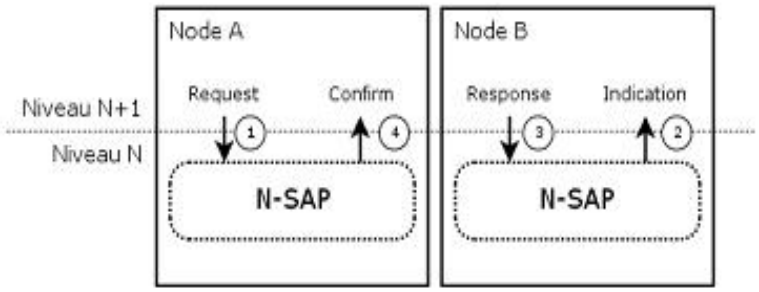

Figure 31 : communication respectant le protocole normalisé.

III.2.1.4 Représentation de la pile protocolaire ZigBee

La pile protocolaire ZigBee est représentée sur la figure 32 :

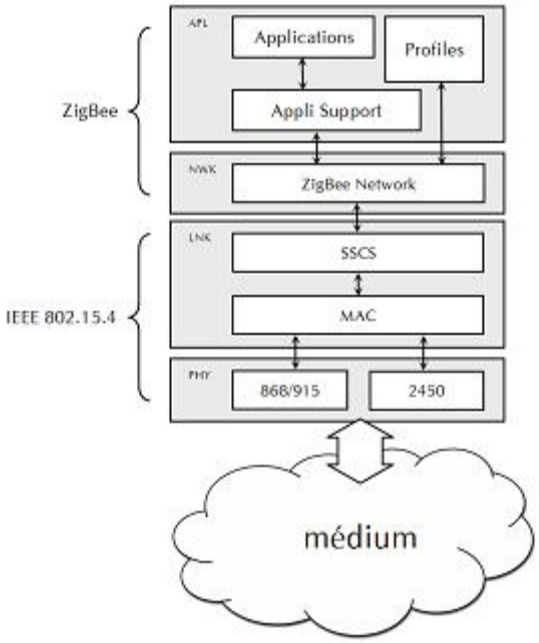

Figure 32: La pile protocolaire 802.15.4 /ZigBee.

III.2.1.5 Les interfaces de communication entre couches

La norme ZigBee prévoit plusieurs interfaces pour la communication entre couches. Ces interfaces sont les Points d'Accès de Service (SAP) vus précédemment. La figure 33 représente cet interfaçage protocolaire.

A l'instar des autres piles protocolaires comme 802.11 chaque couche de la pile protocolaire ZigBee compte deux entités, chacune ayant sa propre interface :

- Une entité dédiée aux transferts de données. Cette entité est sollicitée lorsque la couche supérieure veut envoyer ou recevoir des données sur le réseau. Les primitives présentes sur cette interface sont généralement peu nombreuses (envoyer des données, recevoir des données) et elles se retrouvent à chaque niveau de la pile, pour chaque couche.
- Une entité dédiée à la gestion de la couche. Cette entité sert à commander toutes les taches propres à la couche. Elle dispose généralement d'un jeu de primitives plus étoffé que l'interface dédiée aux transferts de données. Chaque couche ayant un rôle bien précis, chaque niveau dispose d'un jeu qui lui est propre. Voici quelques exemples de primitives :

- pour le niveau Physique :

  – changer de canal radio.

  – passer en émission.

  – détecter l'énergie sur le médium.

- pour le niveau Liaison :

  – rechercher un coordinateur.

  – se synchroniser sur une autre entité.

  – notifier que l'on quitte le réseau.

  – demander de la bande passante à un coordinateur (plus de droit à la parole).

- pour le niveau Réseau :

  – diffuser les routes connues,

  – demander une route.

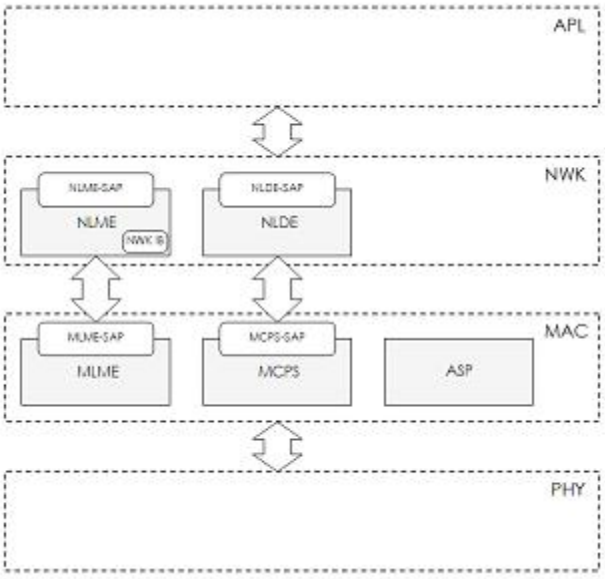

Figure 33 : Principe d'interfaçage entre couches et SAP pour ZigBee.

III.2.2. La couche Physique

III.2.2.1. Bandes de fréquences et canaux

Conformément à IEEE 802.15.4, ZigBee peut travailler sur trois bandes de fréquences différentes : 868 MHz pour la région Europe, 915 MHz pour l'Amérique du nord, et 2,4 GHz pour une couverture mondiale. La norme prévoit deux couches physiques différentes (PHY), une pour le 868/915MHz (PHY868/915) et une seconde pour le 2,4 GHz (PHY2450). Le tableau 2 résume les caractéristiques et les paramètres des deux couches physiques proposées (PHY868/915 et PHY2450).

PHY	Bande (MHz)	Nbre canaux (n°)	Région	Etalement de spectre		Données		
				Débit Chip (kChip/s)	Modulation	Débit binaire (kbit/s)	Débit Symboles (kSymb/s)	Symboles
868/915	868 ~ 868.6	1 (0)	Europe	300	BPSK	20	20	Binaires
	902 ~ 928	10 (1~10)	USA	600	BPSK	40	40	Binaires
2450	2400 ~ 2483.50	16 (11~26)	Toutes	2000	O-QPSK	250	62.5	16-ary orthogonal

Tableau 2 : Caractéristiques des deux couches physiques proposées (PHY868/915 et PHY2450).

III.2.2.2. Le paquet de niveau physique

La norme prévoit un paquet de niveau physique représenté sur la figure 34.

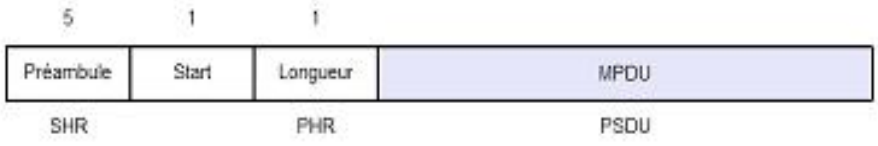

Figure 34: Structure d'un paquet de niveau physique.

Ce paquet comprend un en-tête de synchronisation, un en-tête PHY et les données PHY. L'en-tête de synchronisation comprend 6 octets : un préambule d'une longueur de 5 octets qui permet au récepteur de parfaire sa synchronisation et un fanion de START sur 1 octet. Ce fanion rompt l'alternance des bits transmis lors du préambule, indiquant ainsi l'imminence de la transmission de données. Après l'entête de synchronisation vient l'en-tête PHY dont le rôle est de spécifier la longueur du paquet. Les données suivent cet entête, 127 octets maximum par paquet, soit une durée de transmission maximum de 4,256 ms par paquet sur la couche PHY2450 (250 kbits/s).

La couche PHY de 802.15.4 rend deux services :

- un service de données PHY (PHY data service), qui permet l'´emission et la réception de PPDU3 sur le médium radio.
- un service de gestion PHY (PHY management service), qui permet l'interfaçage entre le logiciel et l'entité de gestion de la couche physique.

III.2.3. La couche Liaison

De façon très similaire au modèle défini par le groupe 802 de l'IEEE, le niveau liaison de 802.15.4 (Niveau 2 OSI) comprend une sous-couche d'accès au médium (MAC) et une sous-couche de convergence (SSCS).

III.2.3.1. La sous-couche MAC

III.2.3.1.1. Types d'accès au médium

La sous-couche MAC gère les accès au médium radio, résolvant notamment les problèmes d'accès concurrents. 802.15.4 propose deux modes pour l'accès au médium : un mode non coordonné (totalement CSMA/CA, sans RTS/CTS) et un mode coordonné, ou *beacon mod*e, disponible uniquement dans une topologie étoile où le coordinateur de cette étoile envoie périodiquement des trames balises (*beacon*) pour synchroniser les nœuds du réseau. L'emploi du mécanisme CSMA/CA dans le mode non coordonné est relativement classique et 802.15.4 n'offre que peu d'innovations par rapport aux autres technologies sans fil dans ce mode ; en

revanche, le mode coordonné permet d'entrevoir des applications intéressantes mettant en œuvre une Qualité de Service.

- **Le mode non coordonné**, totalement CSMA/CA

Dans le mode non coordonné, il n'y a pas d'émission de *beacon* donc pas de synchronisation entre les différents nœuds du réseau. Les nœuds voulant émettre des données doivent utiliser le protocole CSMA/CA «non slotté », c'est-à-dire que le début d'une émission se fait d`es que le médium est jugé libre, sans attendre le début d'un éventuel slot. Cependant, même si l'algorithme est dit « non slotté », il se base tout de même sur une unit´e temporelle discrète appelée période de *backoff* pour pouvoir retarder plus ou moins l'émission d'une trame et éviter les collisions.

- **Le mode coordonné**, ou balisé

Dans le mode coordonné, une ou plusieurs entité(s) du reseau diffuse(nt) périodiquement des trames appelées balises, ou *beacon*. Tout membre du réseau qui entend cette balise peut utiliser la réception de cette trame pour se synchroniser avec son émetteur et se servir de lui comme relais. Ce mode de fonctionnement permet les meilleures performances sur le plan énergétique car une fois l'information transmise au relais, le nœud communicant peut somnoler ; de plus, les messages en attente étant stockés dans la mémoire du relais, un nœud peut choisir de se réveiller selon ses besoins, et demander alors les données en attente. On parle alors de transfert de données indirect dans une topologie en étoile, car tout échange sur le réseau passe par le relais. On appellera par la suite ce relais le coordinateur d'´etoile. La figure 35 illustre le fonctionnement de transfert de données dans une étoile.

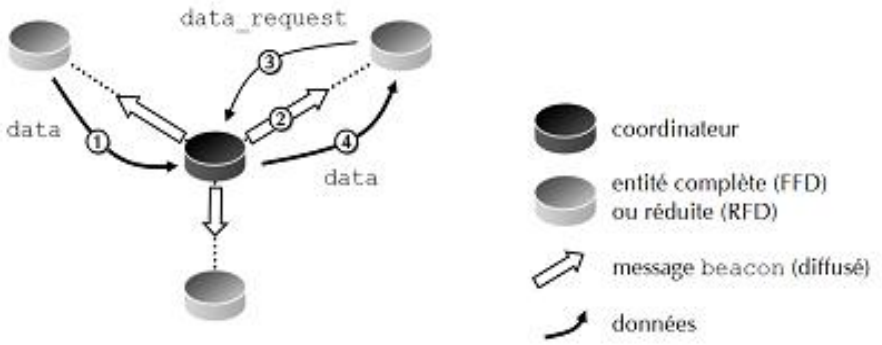

Figure 35 : Principe du transfert de données dans une étoile.

- Le transfert de données direct est illustré par l'envoi du message (1) de type data. Le nœud envoie directement ses données au coordinateur de l'étoile puis se rendort.
- Le nœud de destination récupère ses données de manière indirecte : le message *beacon* (2) annonce les données en attente pour tous les nœuds ; le nœud de destination écoute le *beacon*, constate que des données sont en attente et les réclame par le message *data_request* (3). Le coordinateur peut alors transmettre les données en attente en envoyant le message data (4).

III.2.3.1.2 Notion de supertrame

L'espace temporel durant lequel les communications prennent part est appelé supertrame. Une supertrame est toujours divisée en 16 slots temporels de durées égales, la trame balise occupant le premier slot ; cette trame permet de diffuser la synchronisation pour tous les nœuds à portée radio, mais également l'identifiant du PAN et la structure dynamique de la présente supertrame, en fonction des demandes qui ont été faites par les nœuds membres de l'étoile. La structure d'une supertrame est représentée figure 36.

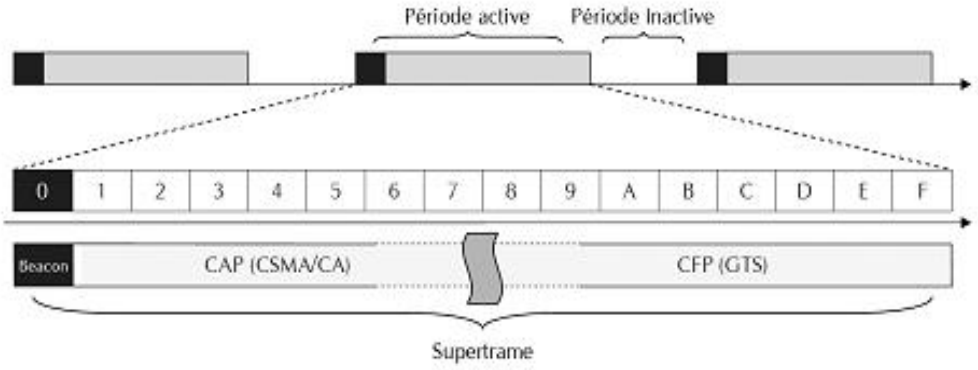

Figure 36 : Représentation d'une supertrame IEEE 802.15.4.

La supertrame possède deux paramètres fondamentaux :

- BO (*Beacon Order*), qui fixe l'intervalle de temps entre l'envoi de deux messages *beacon* par le coordinateur. On déduit de BO le paramètre BI3 (*Beacon Interval*), selon la loi :

$$BI = 2^{BO} * 15,36 \text{ ms avec } 0 \leq BO \leq 14$$

- SO (*Superframe Order*). Ce paramètre fixe la durée active de la supertrame selon la loi :

$$D_{active} = 2^{SO} * 15,36 \text{ ms avec } 0 \leq SO \leq BO$$

L'organisation de l'accès au médium par supertrame permet les meilleures économies sur le plan énergétique. Les nœuds du réseau se réveillent juste avant le slot 0 et se mettent à l'écoute. A la réception du *beacon*, ils prennent connaissance de la structure de la supertrame qui débute : valeurs de BO et SO, présence de données en attente, etc. S'ils n'ont de données ni à émettre, ni à recevoir, ils peuvent somnoler jusqu'au *beacon* suivant.

Notons que plus BO et SO sont faibles, plus la fréquence des supertrames est élevée, donc plus le réseau est réactif (latence faible). En revanche, plus la différence entre BO et SO est grande, meilleures ont les économies sur le plan énergétique. Il faudra donc trouver un compromis entre ces deux constantes selon l'application.

III.2.3.2. La sous-couche LLC

Conformément à la plupart des standards 802.n, IEEE 802.15.4 propose une sous-couche de convergence de type LLC pour normaliser l'interfaçage des couches décrites par le standard

avec une couche de niveau supérieur, typiquement une couche de niveau 3 compatible LLC. Cette convergence est assurée par la sous-couche SSCS qui est décrite par le standard.

Une couche de convergence typique doit jouer plusieurs rôles :

1. La vésication de l'intégrité des données reçues avant la remise à la couche supérieure, par exemple par utilisation conjointe d'un Code de Redondance Cyclique (CRC) et d'un mécanisme d'acquittement.
2. Le contrôle de flux, afin d'éviter la saturation des tampons de réception et la perte éventuelle de données ou les débordements de mémoire,
3. La convergence d'adressage, c'est-à-dire la correspondance des adresses de niveau 3 (niveau réseau, l'adressage est généralement globalisé sur tout le réseau) avec les adresses de niveau 2 (niveau liaison, l'adressage est généralement local et limité au médium utilisé). La convergence d'adressage permet également la gestion des procédés de diffusion (*broadcast)* et de diffusion par classes (*multicast*).

III.2.3.3 Structures de trames

802.15.4 propose 4 types de trames :

1. Trame de données (Data Frame) : transfert de données.
2. Trame d'acquittement (Acknowledgment Frame) : confirmation de données bien reçues.
3. Trame beacon (Beacon Frame) : émise par le coordinateur de réseau en mode beacon.
4. Trame de commande MAC (MAC Command Frame) : pour le contrôle des nœuds.

Ces quatre types de trames ont une structure commune : un champ contrôle de trame (f*rame control*), un champ numéro de séquence (*sequence number*), un ou plusieurs champs propres au type de la trame puis une séquence de contrôle sur 16 bits (*Frame Check Sequence*).

Le format général d'une trame MAC est montré à la figure 37.

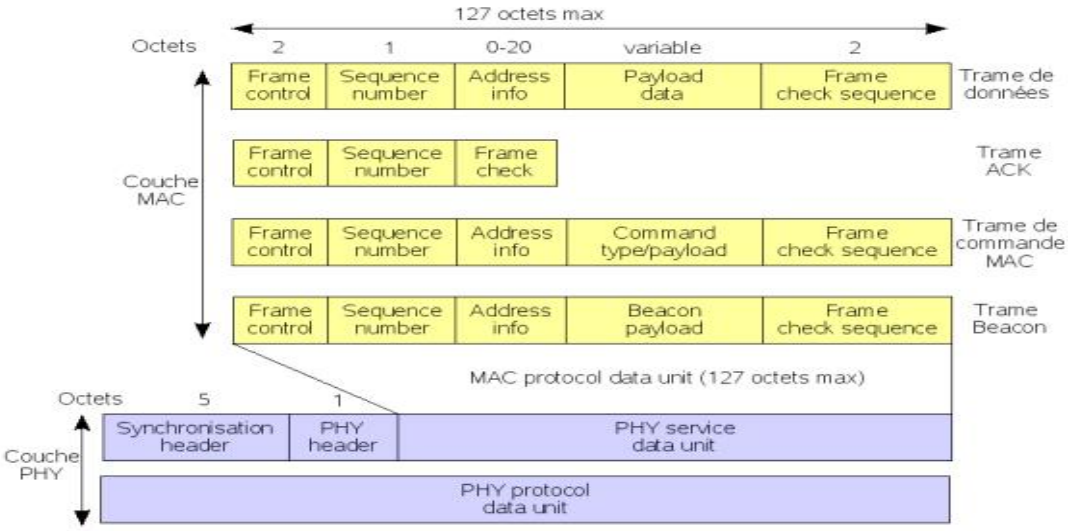

Figure 37 : Format général de la trame MAC.

La trame générale MAC est composée d'un entête MAC (MHR : MAC Header), d'une unité de données de service MAC (MSDU : MAC Service Data Unit) et pied de page MAC (MFR : MAC Footer).

- ✓ L'entête MAC (MAC Header) est composé d'un champ de contrôle de trame qui indique le type de trame MAC transmise, spécifie le format du champ adresse et contrôle l'acquittement. Le champ d'adresse est variable de 0 à 20 octets en fonction du type de trame, et le champ du numéro de séquence assure l'ordre à la réception et permet l'acquittement de la trame MAC.
- ✓ MSDU (MAC service data unit) (payload) est de longueur variable. Cependant, la trame MAC complète ne doit pas dépasser 127 octets de long, et les données contenues dans le champ de données « payload » dépendent du type de trame.
- ✓ MFR (MAC FooteR) contient Le champ de la séquence de contrôle de trame FCS (Frame Check Sequence) qui aide à vérifier l'intégrité de la trame MAC. Dans les trames MAC IEEE 802.15.4 le FCS est un control de redondance cyclique CRC (Cyclic Redundancy Check) sur 16 bits de l'Union des Télécommunications Internationales-secteur standardisation des télécommunications ITUT (International Télécommunication Union). Seules les trames de données et de balisage contiennent réellement des données envoyées par les couches supérieures, les trames d'acquittement et de commande MAC

proviennent de la couche MAC et sont utilisées pour les communications MAC point à point.

Enfin, la norme IEEE 802.1.5.4 définit 3 types d'équipements (nœuds du réseau) :

- Le coordinateur du réseau.
- L'équipement à fonctionnalités complètes FFD (Full Function Device).
- L'équipement à fonctionnalités réduites RFD (Reduced Function Device).

L'équipement FFD peut être soit un coordinateur, soit un routeur, soit un équipement terminal (capteur).

L'équipement RFD est un équipement simplifié comme un équipement terminal (End Device) muni de capteurs.

Pour communiquer au sein d'un même réseau, au moins un équipement FFD et des équipements RFD utilisent de concert le même canal radio parmi ceux définis dans la norme.

Un équipement FFD peut dialoguer avec des équipements RFD ou FFD, mais un équipement RFD ne peut dialoguer qu'avec un équipement FFD.

III.2.4. La couche Réseau

Nous l'avions vu au début de ce chapitre, ZigBee recommande l'utilisation de la technologie proposée par le standard IEEE 802.15.4 pour les deux premières couches du modèle OSI (couche physique et couche liaison). Pour les couches supérieures, la ZigBee Alliance propose sa propre spécification, et notamment, sa propre couche Réseau (niveau 3 OSI).

III.2.4.1. Eléments de la topologie du réseau

ZigBee définit trois types d'éléments pour constituer un réseau.

1. Le Coordinateur ZigBee, ou ZigBee Coordinator, ZC :

- il est unique pour tout le réseau ZigBee et il est à l'origine de la création du réseau,
- il reprend les tâches du PAN *Coordinator* décrit dans le standard IEEE 802.15.4,
- il agit comme simple routeur (ZR, voir point suivant) une fois le réseau crée.

2. Le Routeur ZigBee, ou ZigBee Router, ZR :
   - il doit d'abord s'associer avec le ZC ou un autre ZR,
   - il accepte que d'autres éléments du réseau s'associent à lui,
   - il reprend les tâches du coordinateur 802.15.4,
   - il relaie les messages selon un protocole de routage qui sera pr´esent´e plus bas,
   - il est optionnel.

3. Le nœud terminal, ou ZigBee End *Device*, ZED :
   - il doit d'abord s'associer avec le ZC ou un ZR,
   - il ne constitue qu'un élément final du réseau : il n'accepte ni association, ni participation au routage des messages.
   - il est lui aussi optionnel.

Ces trois types d'éléments sont très semblables à ce que propose le standard IEEE 802.15.4. Nous pouvons constater, comme nous l'évoquions en début de chapitre, que le réseau ZigBee peut avoir une portée plus étendue que le rayonnement d'un simple nœud 802.15.4 grâce au processus de routage qui permet le relais d'un message par une ou plusieurs entités jusqu'à la destination finale.

III.2.4.1.1. Topologie en arbre

Dans le cadre d'une topologie en arbre, le processus de création du réseau s'articule autour du ZC dont la mise en service marque le début de la phase de création. Par la suite, toutes les entités qui se trouvent à portée radio de ce nœud se rattachent à lui. Les entités qui ne sont pas à portée du ZC se rattachent à l'un des ZR, de proche en proche, jusqu'à la formation totale du réseau, comme l'illustre la figure 38.

Sur l'exemple de la figure, le réseau se forme en trois temps. Cette formation hiérarchisée forme un arbre dont la racine est le ZC ; il convient de lier cette topologie à l'adressage et au routage adéquat.

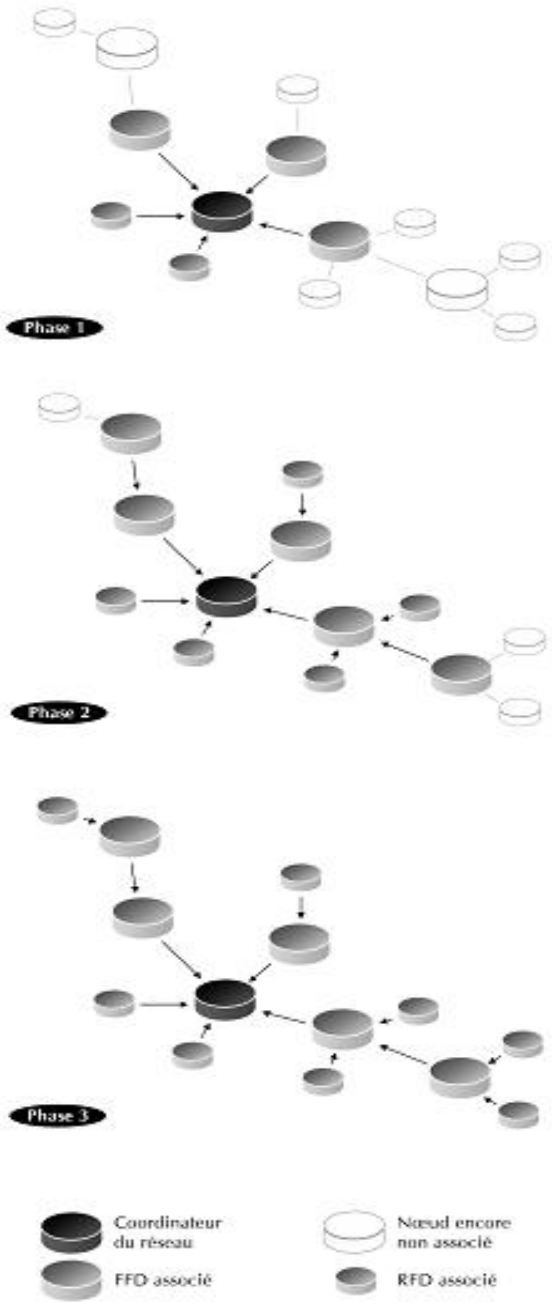

Figure 38 : Exemple de création du réseau ZigBee en arbre.

III.2.4.1.2. Topologie maillée

Avec la topologie maillée, ou *mesh*, tous les ZR à portée radio les uns des autres peuvent dialoguer entre eux, sans structure hiérarchique, comme l'illustre la figure 39. Un processus de routage doit être mis en place pour relayer les paquets de bout en bout du réseau.

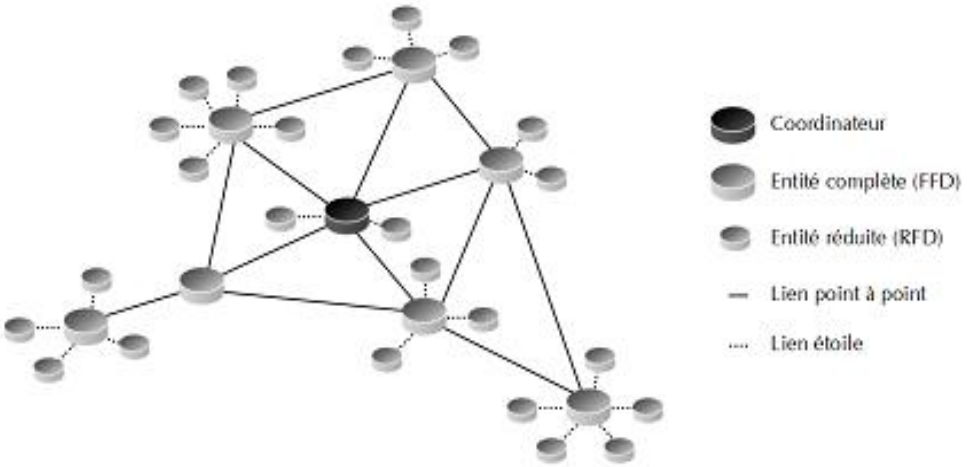

Figure 39 : Exemple de topologie maillée.

III.2.4.2. Architecture de la couche réseau

A l'instar de la couche liaison décrite plus haut par le standard IEEE 802.15.4, la couche réseau proposée par ZigBee se décompose en deux entités : une première entité (NLDE3) traitant l'envoi, la réception des données et éventuellement la réémission de données reçues dans le cadre du routage, et une seconde entité (NLME) chargée de la gestion et de la maintenance du réseau (routage, adressage, etc.). L'entité NLDE communique avec la couche 2 via le point d'accès MCPS-SAP et met à disposition des couches supérieures son propre point d'accès NLDE-SAP3. L'entité NLME communique avec la couche 2 via le point d'accès MLME-SAP et permet au ZDO de pouvoir communiquer avec elle via son point d'accès : NLME-SAP.

La couche réseau contient également une base d'informations appelée NIB. Elle contient les informations sur les nœuds voisins et la table de routage. La structure de la couche réseau proposée par ZigBee est représentée figure 40.

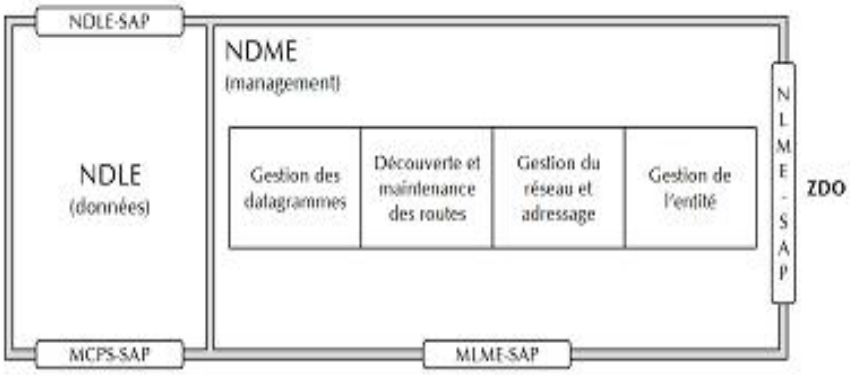

Figure 40 : Structure de la couche réseau proposée par ZigBee.

III.2.4.3. Services rendus

La couche Réseau de ZigBee est en charge des opérations suivantes :

- Création et traitement des PDU de niveau Réseau (NPDU3),
- Participation au routage des paquets,
- Création (Coordinateur ZigBee) ou rattachement à un réseau existant,
- Adressage,
- Découverte du voisinage et stockage des informations li´ees aux nœuds voisins,
- Contrôle du récepteur, économie d'énergie (fonctions liées à la couche MAC).

III.2.5. Principes de base du routage ZigBee

Du fait de la mémoire très limitée des nœuds, le routage ZigBee suit le principe de base suivant :

- si la table de routage contient une entrée qui correspond au routage demandé, il faut router le paquet selon cette entrée,
- si elle ne contient aucune entrée et si la mémoire libre le permet, il faut lancer le processus de découverte de route,
- sinon, il faut router le paquet selon le routage hiérarchique en arbre (*Tree Routing*).

La structure de la table de routage d'un nœud ZigBee est représentée dans le tableau 3.

Nom du champ	Taille	Description
Adresse de destination	2 octets	L'adresse courte du nœud de destination
Statut	3 bits	Le statut de la route
Adresse du prochain saut	2 octets	L'adresse courte de la passerelle

Tableau 3 : Structure de la table de routage d'un nœud ZigBee.

III.2.4.7. Structure du paquet de niveau réseau

Nous concluons cette partie sur le niveau réseau de ZigBee par la structure du paquet de niveau 3, comme l'illustre la figure 41. Sur cette figure, on peut également voir comment le paquet de niveau 3 est encapsulé dans la trame DATA de niveau 2 (802.15.4).

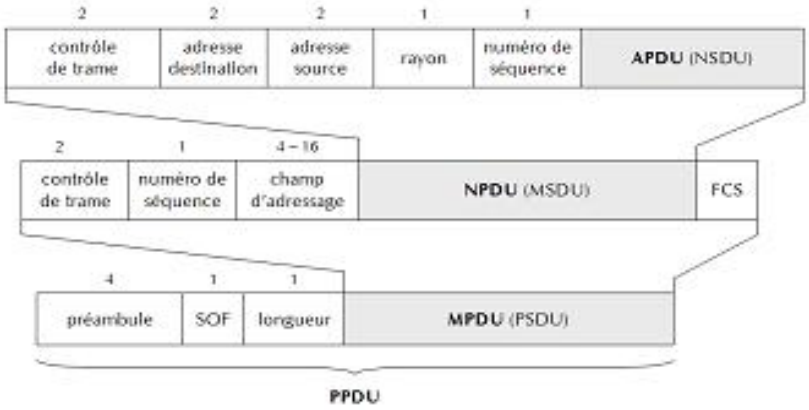

Figure 41 : Structure du paquet de niveau réseau et encapsulation dans une trame de données 802.15.4.

Comme la trame 802.15.4, le paquet ZigBee possède un champ de contrôle et un champ de numéro de séquence propre, ainsi qu'un champ d'adressage (source, destination) pour l'adressage de bout-en-bout du réseau. Notons également la présence du champ rayon qui est modifié à chaque passage dans un routeur.

III.3. Conclusion

A la lumière de ce qu'on a vu dans ce chapitre, on peut dire que le protocole ZigBee est un protocole de haut niveau basé sur la norme IEEE 802.15.4 et conçu par la ZigBee Alliance. Son autonomie importante, sa faible consommation et son faible coût sont ses principaux atouts pour l'utilisation en monde embarqué.

Par comparaison avec les autres protocoles sans-fil comme le Wifi, le ZigBee n'a besoin que d'un faible espace mémoire qui lui permet de déployer un maillage de plus de 65.000 nœuds, là où le Wifi n'en permet que 32, au maximum. Ce maillage à haute densité permet une résilience très importante : si un nœud tombe, le message initial peut arriver à destination via un autre chemin. On reconnaît ici la force d'un système distribué.

Par contre La faible portée de ZigBee - 100m, peut ne pas convenir à certaines configurations géographiques. On remarque ici l'avantage des bandes ISM puisque la portée est 10 fois plus importante (1000 m).

Chapitre IV

La sécurité dans les normes IEEE 802.15.4 /ZigBee.

IV.1. Introduction

ZigBee est un protocole conforme aux normes de l'industrie construit autour du protocole sans fil IEEE 802.15.4, qui fournit l'infrastructure réseau nécessaire aux applications réseau sans fil basse consommation.

Et en vu de l'importance du ZigBee dans les applications de sécurité et dans les stockages et les transmissions des données, il est important de mètre en œuvre des méthodes efficaces pour les sécuriser.

IV.2. Application de la sécurité dans le ZigBee

IV.2.1. Les mesures de sécurité pour le ZigBee

- **La cryptographie** peut protéger la confidentialité.
- **Le hachage et la signature** peuvent assurer l'intégrité. Le hachage est un mécanisme qui vérifie l'intégrité du message.
- **La signature numérique** peut assurer l'authentification et le contrôle d'accès.

IV.2.2. Environnement d'application de la sécurité

Pour appliquer la sécurité dans le protocole ZigBee il faut d'abord savoir quelle est la couche responsable sur la sécurité dans pile protocolaire ZigBee.

La sécurité des données se fait dans la sous couche 'Application Support Sub-Layer' de la couche application définissant les profiles des objets ainsi que les messages d'échange entre les objets et le coordinateur et assure a communication des données et des commandes avec le bloc fonctionnel SSP qui fournit le service 'Sécurité'.

La figure 42 illustre la position de service de sécurité dans la pile protocolaire ZigBee :

Le format général d'une trame ZigBee cryptée est donné dans la figure 43.

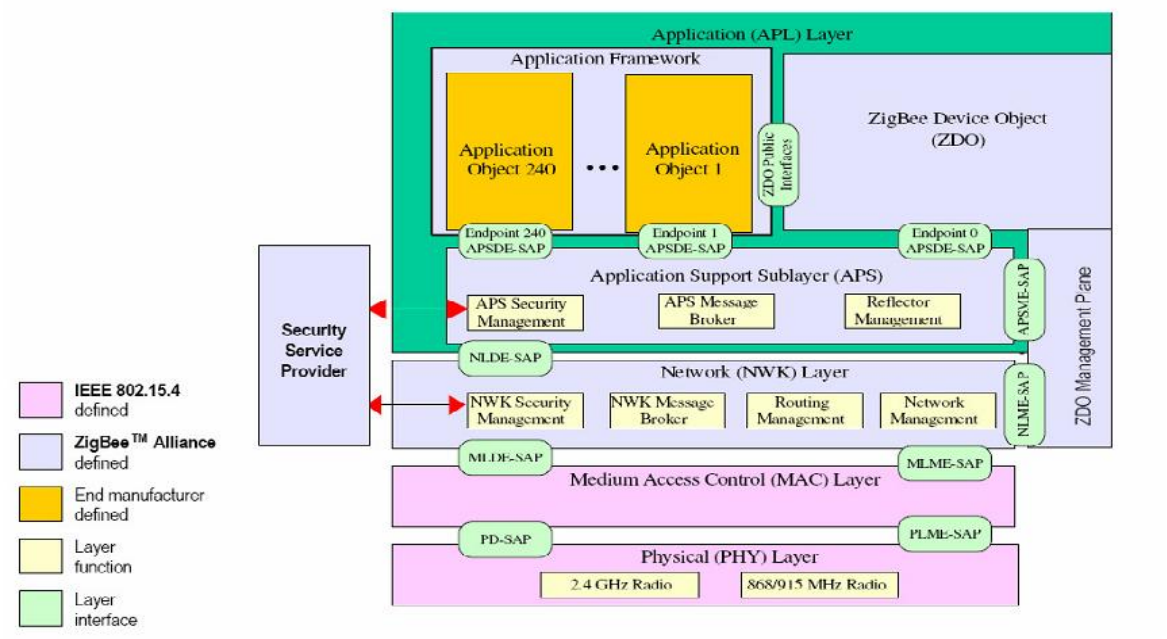

Figure 42 : Présentation détaillée de la pile protocolaire ZigBee.

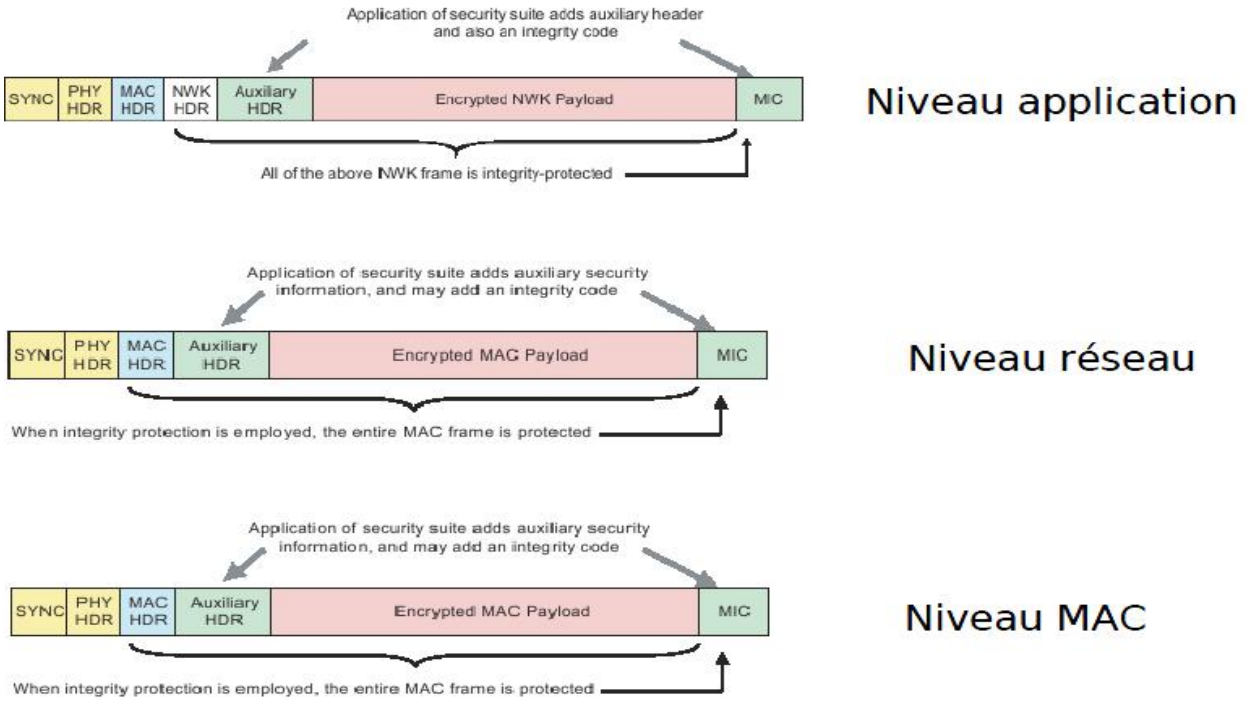

Figure 43 : format général d'une trame ZigBee cryptée.

IV.3. Vue d'ensemble ZigBee cryptographie

IV.3.1. Contenu de la norme 802.15.4/ZigBee cryptographie [20][21][22]

IV.3.1.1. Chiffrement

Le chiffrement est utilisé pour protéger les renseignements devant être lu par un tiers non autorisé, en particulier si un message est envoyé sur un canal non sécurisé. Il devrait y avoir aucun danger si un tiers connaît l'algorithme de mise en œuvre. La sécurité doit être fondée sur une clé secrète seulement. La norme IEEE 802.15.4 utilise le chiffrement AES-128 (Advanced Encryption Standard) avec un cryptage 128 bits longueur de la clé. À la connaissance de la cryptographie recherche, cet algorithme satisfait à toutes les exigences de sécurité modernes.

Toutefois, l'application erronée d'un bon algorithme peut néanmoins détruire la sécurité. Ceci peut être évité par des modes de cryptage soi-disant, à savoir comment un algorithme cryptographique est appliqué.

IV.3.1.2. Protection de l'intégrité

Le cryptage est un moyen de défense contre les attaques passives, c'est à dire contre les intrus. Mais il est souvent plus important de se protéger contre les attaques actives qui envoient des faux renseignements ou malicieusement modifiés messages. Donc, il n'ya généralement pas de secret, si une fenêtre est ouverte ou fermé, c'est à dire par exemple un message n'a pas besoin d'être chiffré. Cependant, il est très important qu'aucun attaquant ne peut envoyer une notification "fenêtre est fermée" pour un système d'alarme lorsque la fenêtre est ouverte.

Tout cela vaut en particulier pour les réseaux de capteurs sans fil, puisque la radio messages est facile à falsifier.

La cryptographie permet de détecter les messages non autorisées envoyés ou modifié par l'ajout de contrôle cryptographiques, MAC soi-disant (Message Authentication Code), avec la connaissance d'une clé secrète comme le montre la figure 44: L'expéditeur calcule le MIC et

l'envoie en même temps que le message. Le récepteur recalcule la MIC du message reçu et le compare avec la MIC dans le message. Si le calcule et MIC reçu coïncident, l'expéditeur doit avoir connu la clé secrète.

Un attaquant qui ne connaît pas cette clé ne serait pas en mesure de modifier le message et pour calculer un MIC valide. Ainsi, le MIC garantit que le message a été généré par l'expéditeur et non pas par certaines attaquant, à condition que la clé secrète n'a pas été divulgué.

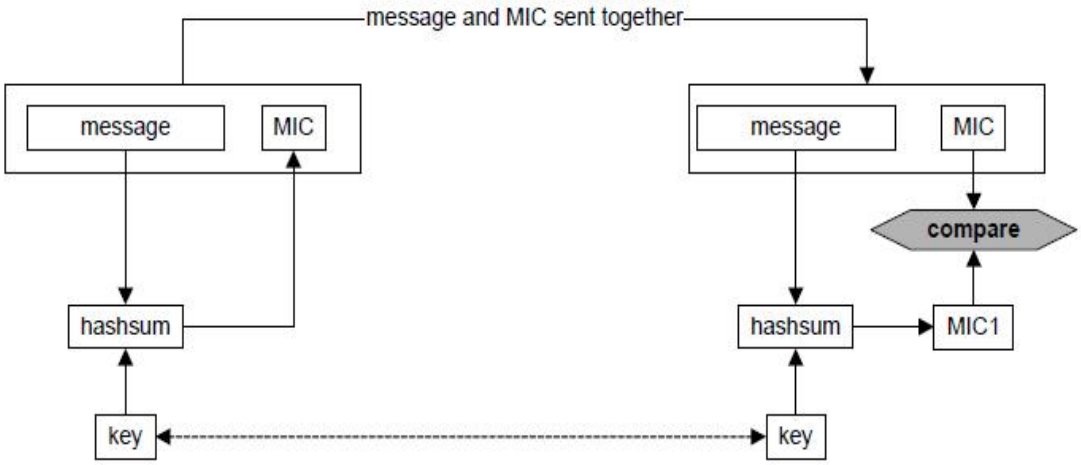

Figure 44 : Un MIC détecte des modifications.

La norme IEEE 802.15.4 (ZigBee) sélectionne le mode de chiffrement CCM * qui permet également à activer la protection de l'intégrité. La protection de l'intégrité a des conséquences importantes:

- La charge utile du message ne peut pas être modifiée par un pirate sans se faire remarquer.
- Si l'ID de l'expéditeur est inclus dans le calcul MIC, le récepteur peut être sûr de qui a envoyé ce message, c'est à dire l'usurpation est exclue.
- Quand un compteur de vues croissante est inclus dans le calcul MIC, les attaques sont exclues. Autrement dit, un message enregistré par un auditeur ne serait pas de nouveau accepté (par exemple, "la fenêtre est fermée").

- Par la même moyenne, le bon ordre des messages envoyés peut être assurée (pensez à «fenêtre ouverte» - «guichet fermé»). Il est possible que l'ordre des messages soit modifié par des problèmes de routage. Pour les applications critiques, aussi «attaques retard" peuvent être évités lorsque l'horodatage sont inclus dans le calcul MIC. Dans un tel scénario, l'attaquant attrape un message et perturbe le récepteur en même temps. Le message est alors envoyé plus tard.

IV.3.2. La cryptographie utilisée dans la norme IEEE 802.15.4 (ZigBee)

IV.3. 2.1. L'algorithme AES [24]

Le chiffrement selon la norme IEEE 802.15.4 est basé sur l'algorithme AES.

Bien que la sécurité des algorithmes utilisables a pas encore prouvé, AES a été choisi comme nouveau norme de cryptage dans une compétition mondiale et a été étudié par les meilleurs crypto-analystes pendant des années, qui n'ont pas trouvé la moindre faiblesse en elle. Donc AES peut être considéré comme l'un des meilleurs algorithmes cryptographiques disponibles. Il remplace le DES qui a été utilisé durant 30 ans qui utilise une clé de 56 bits seulement. Alors que les 56 bits de longues possibles touches peuvent être jugés par matériel spécial aujourd'hui, la clé de 128 bits AES ne peut pas être deviné avec le matériel que nous le connaissons aujourd'hui (et même les ordinateurs quantiques hypothétiques ne pouvait pas rompre au moins une Clefs de 256 bits en utilisant la théorie récente).

AES est un matériel facile: Il faut relativement peu de ressources, et il est rapide. Donc, c'est le meilleur choix pour la cryptographie symétrique dans les dispositifs de faible puissance. AES pouvez utiliser 128, 192 et 256 bits clés longues. Même les clés de 128 bits ne peuvent pas être brisée; les clés les plus longues sont une précaution si des faiblesses encore inconnues de l'algorithme serait être trouvée. IEEE 802.15.4 utilise le chiffrement AES-128 (clés de 128 bits).

AES est un chiffrement par blocs: le chiffrement et le déchiffrement sont faits sur des portions de la même longueur seulement, ici 128 bits (16 octets), ce qui donne un résultat de 128

bits - pour toutes les tailles de clé. Le seul problème se pose avec des longueurs de plaine ou de texte chiffré qui ne sont pas des multiples de 16, c'est une question de modes de chiffrement.

En outre, AES est un algorithme de chiffrement produit soi-disant (voir Figure 45):

- La première étape est l'initialisation clé: Basé sur la clé, 10 touches rondes sont calculées.
- Après cela, le cryptage / décryptage se fait en 10 étapes presque identiques (tours), chaque fonction de la touche correspondante à une ronde. Chaque tour se compose de simples transformations comme XOR par octet, 'octet' et l'octet de substitution permutation. Contrairement à certains autres algorithmes, la procédure de déchiffrement différente de cryptage.

Pour IEEE 802.15.4, ce n'est pas grave puisque en mode CCM *, le décryptage utilise uniquement le cryptage AES. Néanmoins, l'émetteur-récepteur radio du module de sécurité offre également une fonctionnalité de décryptage AES. À cette fin, la dernière touche ronde doit être calculée avant et ensuite utilisé comme clé.

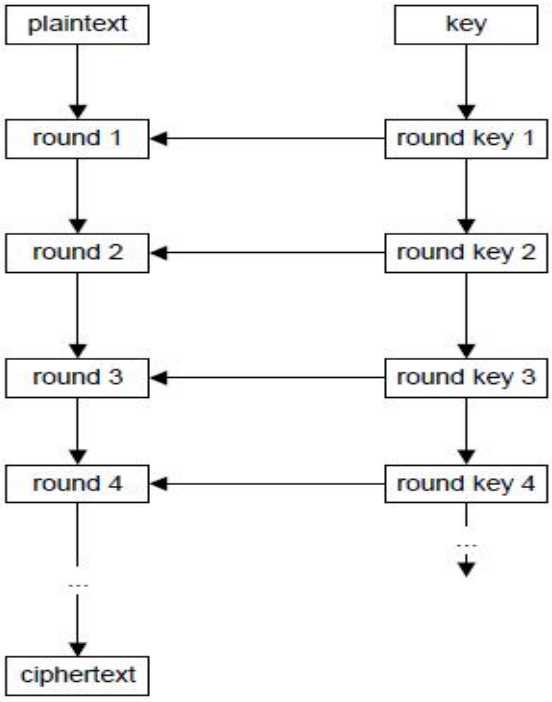

Figure 45 : Structure d'un algorithme produit.

IV.3.2.2. Les modes de cryptage, CBC-MAC, rembourrage [25]

Un algorithme cryptographique peut chiffrer ou déchiffrer un bloc seulement. Les modes de chiffrement traitent de la façon d'appliquer un algorithme du bloc de messages de longueurs arbitraires. Ce n'est pas seulement une question technique, mais il a aussi une grande influence sur la sécurité. Seuls les sujets d'importance à la norme ZigBee sont discutés dans ce qui suit.

IV.3.2.2.1. Mode ECB

Le mode le plus simple est le mode ECB (Electronic Code Book) : Chaque bloc clair ou chiffré (dans notre cas, 16 octets) est respectivement déchiffré séparément avec la même clé, comme le montre la figure 46.

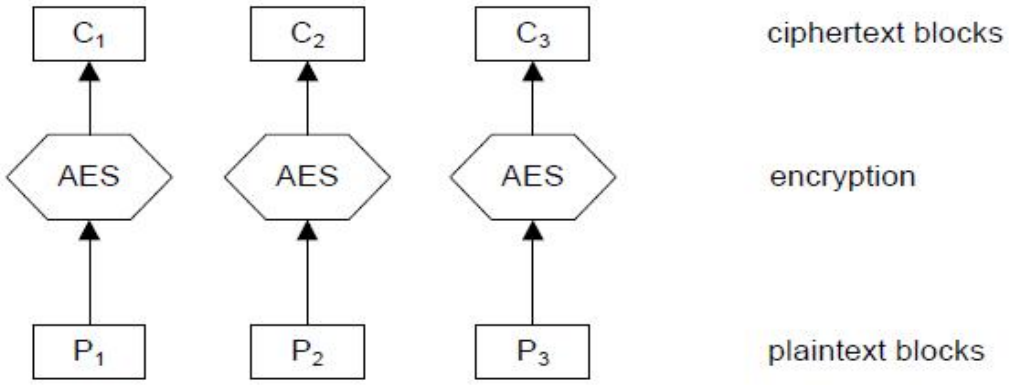

Figure 46 : mode ECB.

Ce mode est facile à mettre en œuvre et permet la parallélisassions. Cependant, la structure de texte en clair n'est pas entièrement masquer. En particulier, le plain texte identiques le rendement les cryptogrammes et mêmes ce qui peut permettre des attaques pratiques: supposons qu'un capteur a deux états "on" et "off", c'est-à-dire, il génère deux types de messages seulement. Si les messages sont crypté simple, c'est à dire en mode ECB, un attaquant observe également deux types de messages cryptés (chiffrés) seulement. Il n'est généralement pas difficile de deviner à partir du contexte qui appartient à un texte chiffré qui message. Par conséquent ECB est appliquée que dans des cas particuliers, par exemple pour crypter d'autres (au hasard) touches. En général, un mode plus sécurisé doit être appliquée, comme le mode CBC expliqué dans le paragraphe suivant.

IV.3.2.2.2. Mode CBC

Le mode le plus important dans la pratique est le mode CBC (Cipher Block Chaining), comme il est montré dans la Figure 47. Lors de cryptage, le dernier bloc de texte chiffré est calculé en utilisant la fonction logique XOR avec le bloc de texte en clair réel et ensuite il sera crypté. Le premier bloc, dit vecteur d'initialisation (IV), est pseudo-aléatoire et la fonction XOR est utilisée en premier avec le bloc de texte en clair avant le cryptage.

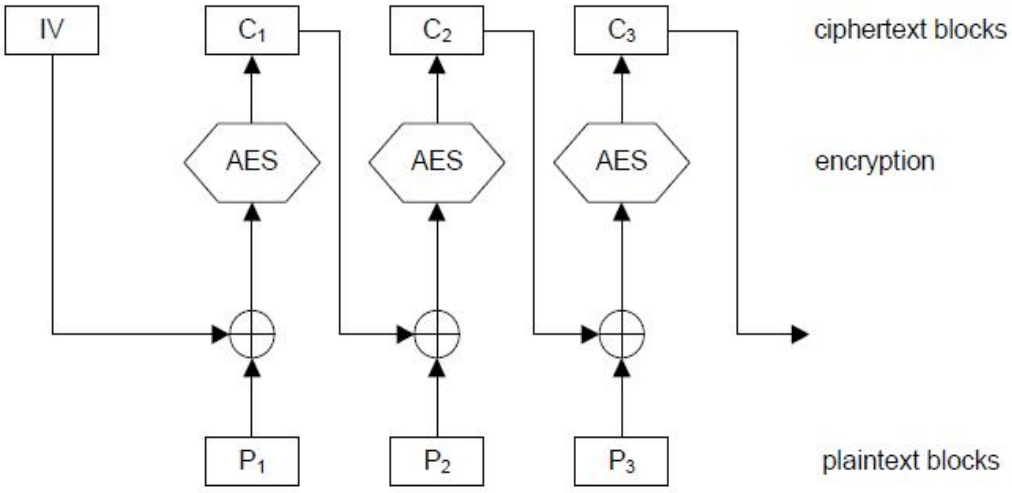

Figure 47 : Mode CBC.

CBC cache complètement des informations concernant le texte clair (à l'exception de la longueur, bien sûr), même les deux cryptogrammes fait partie du même texte en clair à condition que des vecteurs d'initialisation différents sont utilisés pour les différents messages cryptés.

IV.3.2.2.3 CBC-MAC

Le mode CBC peut être utilisé pour calcul du MAC: le dernier cryptogramme calculé dépend de tous les blocs de texte en clair, il convient que la somme de contrôle cryptographique (MAC) ne peut être calculée que si la clé secrète est connue. Habituellement, le vecteur d'initialisation a la valeur « 0 » dans ce cas. Pour les messages de longueur fixe, le CBC-MAC est sécurisée.

IEEE 802.15.4(ZigBee) utilise le mode CCM *, et ce calcule CBC-MAC de longueur variable des messages. Cependant, le bloc de message est un premier nonce contenant la longueur du message ce qui implique que la CBC-MAC calculé (appelé MIC dans le CCM *) est également sécuriser.

IV.3.2.2.4 Le mode compteur

Le mode compteur (CTR) fonctionne comme le montre la figure 48: Une séquence de nonces (unique des blocs de contenu connus) est généralement construit en réservant une partie d'une partie fixe nonce et remplir cette partie avec une suite croissante de nombres. Ce flux est un ensemble de nonces chiffrés par bloc, et le flux résultant est chiffré au niveau du bit en utilisant la fonction logique XOR avec le texte en clair qui nous donne à la fin le texte chiffré.

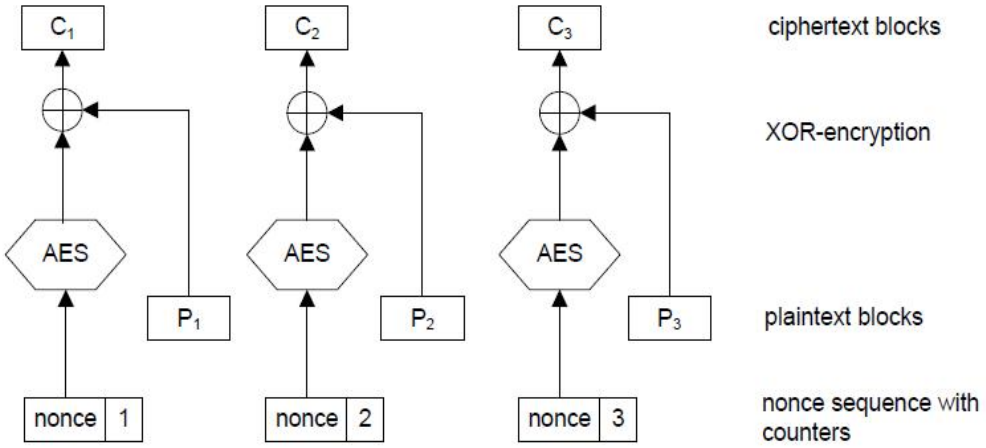

Figure 48 : Mode compteur (CTR)

En dépit de sa simplicité de construction, le mode CTR est sécurisé si la protection de l'intégrité s'applique, et si aucune combinaison de valeur à usage unique avec le compteur n'est répétée pour la même touche. Le mode offre quelques fonctionnalités utiles:

- Il peut être parallélisée.
- Le déchiffrement est exactement la même opération que le cryptage.
- Pas de remplissage est requis (voir ci-dessous).
- Le chiffrement dépend de nonces, c'est-à-dire, les messages peuvent être chiffrés par des différents cryptogrammes.

- Les messages peuvent être modifiés par un attaquant actif, même si il ne peut pas les décrypter.

IV. 3.2.2.5. Remplissage [23-24]

Tous les modes expliqué jusque-là s'appliquent aux messages avec des multiples de longueur de bloc (pour AES-128: 16 octets) seulement. Il existe des différentes méthodes pour contourner ce problème. Le Rembourrage est la méthode la plus simple, c'est-à-dire, l'ajout le plus grand nombre (éventuellement aucune) octets pour le message jusqu'à ce que un multiple de la longueur de bloc est atteinte. Habituellement, les octets nuls sont pris. En général, le décryptage ne sera pas unique si le dernier octet du texte en clair peut être un octet nul (depuis la fin du texte en clair il ne peut pas être déterminé de façon unique). Le mode CCM * décrit dans IEEE 802.15.4 contient la longueur du message dans le nonce (qui est contenue dans le bloc de message authentifié première) et résout donc ce problème.

IV.3.2.2.6. Les modes CCM, CCM * [26-28]

Le mode CCM est une combinaison entre le mode CBC-MAC et le mode CTR. Son principe est de combiner un texte clair tête avec une charge utile cryptée où en-tête et la charge utile ainsi que devrait être intégrité protégée.

La sécurité peut être attestée pour tout chiffrement par bloc (on supposon que le chiffrement par bloc est sécurisée).

Le CCM * diffère de CCM que le cryptage et l'authentification ne sont autorisés.

Le CBC-MAC utilisée dans CCM / CCM * peut avoir réduit la longueur et est appelé MIC là.

Une CCM assure que celui utilisé dans la norme IEEE 802.15.4 se fait comme suit (voir aussi la figure 49):

- Un nonce est construite contenant des longueurs d'en-tête et la charge utile en texte en clair et ajouté au début du message. Un nonce est une partie d'un bloc AES qui doit contenu être unique sur l'ensemble des messages sécurisés avec la même clé.
- Après cela, la tête en clair (contenant le nonce) et la charge utile sont rembourrées avec un octet nul séparément.
- Ensuite, un CBC-MAC (MIC) est calculé sur l'ensemble du message à l'initialisation du vecteur à « 0 » et annexé à la concaténation.
- Ensuite, le nonce utilisé pour la CBC-MAC (MIC) de calcul est modifiée.
- Ensuite, la charge utile et MIC sont cryptés en mode CTR avec le nouveau nonce où la valeur Compteur pour le chiffrement MIC est 0, et les compteurs de début de chiffrement de charge utile a la valeur « 1 ».
- Enfin, le MIC peut être réduit en longueur. MIC longueurs de bit 0, 32, 64 ou 128 sont autorisés (la longueur de bit « 0 » signifie: pas d'authentification, le MIC n'est pas calculé).

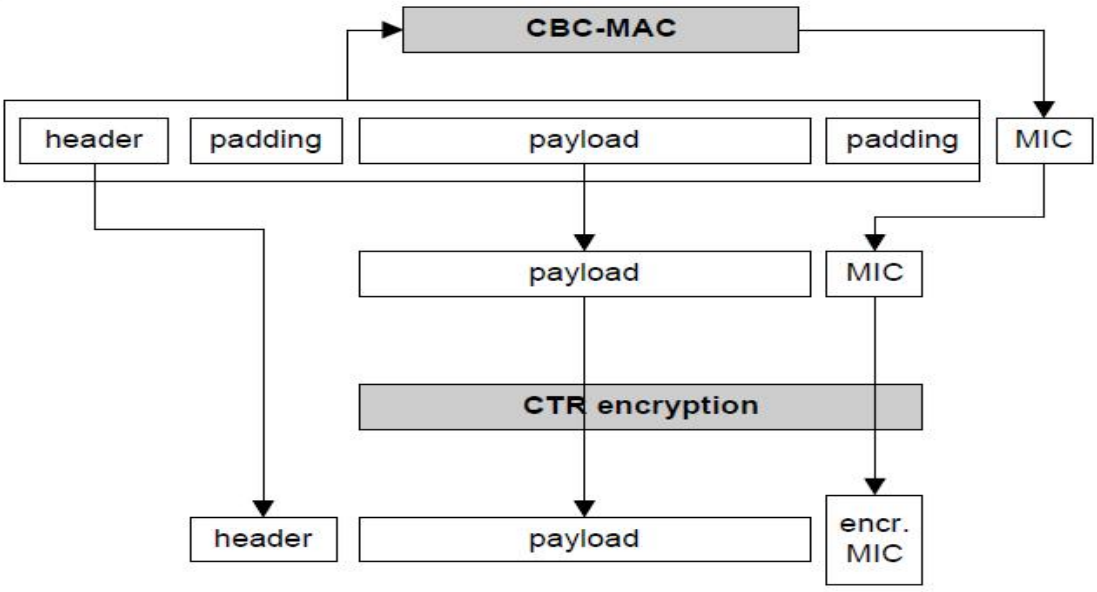

Figure 49: CCM mode.

IV.3.3. Avantages et inconvénients de la cryptographie ZigBee

Avantages:

1. Seule la cryptographie symétrique est utilisée ce qui est beaucoup plus rapide, plus facile à mettre en œuvre et plus facile à manipuler que la cryptographie asymétrique (cryptographie à clé publique).

2. En mode CCM *, on utilise seulement le cryptage AES, aucun décryptage AES n'est nécessaire. Cela permet ma réduction de matériel de décryptage.

3. La même clé est utilisée pour l'authentification et de chiffrement, sans compromettre la sécurité. Ainsi initialisation clé est rare, devient firmware petite et plus rapide. Même en mode ZigBee commerciale, la clé ne doit pas être réinitialisée tant que le dispositif communique avec un partenaire fixe.

4. La partie cryptographie de la norme est plutôt simple. Ce n'est pas seulement agréable pour développement du *firmware*, mais aussi pour la sécurité: Une bonne sécurité doit être compacte et faciles à consulter.

5. L'algorithme et le mode de cryptage sont à la fois libre de brevets.

Inconvénients:

1. Le transfert de clé est risqué: Pour transférer une clé secrète sur l'air, il n'y a pas d'autre moyen que de le chiffrer par une clé principale qui doit être distribué lors de l'initialisation par l'extérieur. Si cette clé maître est compromise (par exemple depuis un appareil a été volé et analysés), la sécurité risquent d'être perdues.

2. Le mode CCM* permet le cryptage sans authentification. Ce mode ne doit jamais être utilisé car il n'est pas sûr. Il aurait dû être écartée en CCM*.dans le cas de ZigBee, ce mode n'est pas utilisé.

3. Pour calculer un MIC et chiffrer un message, le message doit être chiffré deux fois: une fois pour le calcul MIC, et une fois pour le chiffrement proprement dit (le MIC et cryptage nécessite un bloc plus d'être cryptées). Il ya près de deux fois plus rapides modes de combiner l'authentification des messages avec chiffrement de charge utile, mais ils ne sont pas libre de tout brevet.

4. Le cryptage MIC n'est pas nécessaire - en raison de la structure nonce, un auditeur ne peut recueillir des informations sur les charges utiles peut-être identiques, ce qui peut produire une attaque de collision possible.

5. En règle générale, CCM * est considéré comme mauvaises destinées d'autres modes comme le mode EAX.

IV.4. Conclusion

ZigBee protège les messages transmis de nœuds en nœuds en utilisant la sécurité fournie par la couche MAC, mais pour les messages qui doivent passer plusieurs nœuds, ZigBee s'appuie sur les couches supérieures (comme la couche NWK).

La couche MAC utilise un algorithme de cryptage avancé de type AES, qui protège la confidentialité, l'intégrité, et l'authenticité des trames MAC.

La couche MAC fournie donc le processus de sécurité, mais les couches supérieures déterminent les clés de cryptage et le niveau de sécurité à appliquer.

Quand un nœud reçoit ou émet une trame sécurisée, la couche MAC regarde la destination (source), détermine la clé de cryptage associée à cette destination puis utilise cette clé pour traiter la trame.

On détermine l'emploi de la sécurisation ou non grâce à un bit dans l'en-tête MAC de la trame.

Conclusion générale.

Conclusion générale :

Dans ce mémoire, nous avons mis en avant les caractéristiques essentielles des réseaux de capteurs sans-fil, ainsi que les besoins et les défis de la sécurité dans ces derniers. Nous avons étudié aussi quelques schémas de gestion de clés qui permettent d'offrir le service de sécurité de base pour n'importe quel système basé sur la communication. L'ensemble des protocoles de gestion de clés proposés pour les RCSF, se basent principalement sur la cryptographie à clé symétrique et la méthode de pré-distribution de clés afin d'achever l'établissement de clés entre les entités communicantes dans le réseau.

La norme ZigBee se base sur la norme IEE 802.15.4, il est utilisé dans plusieurs domaines comme la surveillance médicale, le transport, et le domaine militaire...etc. Sa sécurité est assuré par le codage AES-128 bits qui n'a montré la moindre défaillance jusqu'à aujourd'hui. Ce type de codage assure la sécurité grâce à l'utilisation d'une clé de chiffrement secrète qui répond bien aux besoins de la sécurité dans le ZigBee comme l'intégrité et l'authentification.

Le codage AES-128 bits est l'un des moyens les plus fiable pour assurer la sécurité dans la transmission et le stockage des données, il est utilisés par des grandes compagnies mondiales comme Interpole et NSA.

Bibliographie.

Bibliographie:

[1] Internet Engineering Task Force (IETF). Groupe de travail MANET (mobile ad hoc network). http://www.ietf.org

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. l. Cayirci. "A survey on sensor networks". IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-116, August 2002.

[3] Equipe de Get 2005 Capt'Ad-hoc. "Sensor networks: State of the art". Technical Report, Telecom Paris, ENST Br, INT, INRIA, Mars 2006.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: a survey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.

[5] I. Khemapech, I. Duncan and A. Miller. "A survey of wireless sensor networks technology". In PGNET, Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, June 2005.

[6] Guy Pujolle. "Les Reseaux". 5eme edition, 2006, ISBN : 2-212-11987-9.

[7] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey ", Department of Computer Science Wayne State University.

[8] Yacine Challal, « Réseaux de Capteurs Sans Fils », Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

[9] Hatem Bettahar, Yacine Challal, « Introduction à la sécurité informatique », Supports de cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 15 Octobre 2008.

[10] www.securiteinfo.com, « Le Grand Livre de SecuriteInfo.com », 19 Février 2004.

[11] Mohamed-El-Amine Chetibi, Souad Djerroud, « Sécurisation des échanges sur les réseaux Wifi », Thèse d'ingéniorat, Institut National de formation en informatique INI, Algérie, Juin 2008.

[12] Emmanuel. Bresson, «Cryptographie: chiffrement par flot», Séminaire de la cryptographie, Page(s): 22-34, Laboratoire de cryptographie, Université de Paris XII, 2001/2002.

[13] D.Baker, H.X.Mel, «La cryptographie décryptée», Livre, Nombre de Pages: 413, Edition Campus Press, 2001.

[14] A.Bachir, A. Ouadjaout, L. Khelladi, M. Bagaa, N. Lasla, Y.Challal, « Information Security in Wireless Sensor Networks», Handbook/Encyclopedia on Ad Hoc and Ubiquitous Computing, edited by: Agrawal Dharma P., and Xie Bin., World Scientific, 2009.

[15] LAN-MAN Standards Committee of the IEEE Computer Society– 802.15.4 IEEE Standard for Information technology, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) – IEEEStd 802.15.4-2003 (2003).

[16] J. Zheng et M. J. Lee – Will IEEE 802.15.4 make ubiquitous networking a reality ? : A discussion on a potential low power, low bit rate standard – IEEE Communications Magazine, vol.27, no. 6, pp. 23-29 (2004).

[17] T. Khoutaif et F. Peyrard – Performances evaluation of the asynchronous Bluetooth links in a real time environment – IEEE Personal Wireless Communications (PWC'2005), Colmar, France (Aout 2005).

[18] J.F. Llibre, P. Pinel et E. Campo – Dimensionnement d'un générateur photo voltaïque pour un système communicant autonome – XII ieme Colloque National de la Recherche dans les IUT, Brest, France (2006).

[19] A. VAN DEN BOSSCHE « Proposition d'une nouvelle méthode d'accès déterministe pour un réseau personnel sans fil à fortes contraintes temporelles », Thèse Doctorat, Université de Toulouse 2, France (juillet 2007).

[20] www.nist.gov /aes (AES development, historical site).

[21] http://csrc.nist.gov /publications/fips/fips197/fips-197.pdf (AES standard and test vectors).

[22] http://csrc.nist.gov/groups /ST/toolkit/block_ciphers.html (overview over block ciphers, key handling and test vectors).

[23] Schneier, B.: Applied Cryptography, 2nd ed., 1996.

[24] Wobst, R.: Cryptology Unlocked, 2007.

[25] http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

[26] http://en.wikipedia.org/wiki/CCM_mode

[27] http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[28] http://tools.ietf.org/html/rfc3610