Etude du protocole, de la sécurité et création d'une application ZigBee

Anthony AMBROGI, Jérémy THIMONT

Master SSIC, 2010 - 2011, Metz University,
Ile du Saulcy, 57045 Metz, France
anthony.ambrogi@umail.univ-metz.fr
jeremy.thimont@umail.univ-metz.fr

Résumé ZigBee est une technologie sans-fil à courte portée et à faible consommation énergétique. Dans un contexte actuel d'économies d'énergies et de développement durable, l'utilisation d'un tel procédé peut s'avérer bénéfique afin de permettre de réduire les consommations de courant. Nous nous servirons donc de cette base afin de créer une application destinée à réduire les dépenses électriques inutiles.

Mots-clés : Réseaux sans fil, Domotique, ZigBee, Consommation électrique, Protocole, Sécurité, 802.15.4

1 Spécifications ZigBee

1.1 Généralités

Qu'est-ce que ZigBee ?

ZigBee est un LP-WPAN (*Low Power-Wireless Personal Area Network*). Autrement dit, il s'agit d'une technologie sans-fil à courte portée et à faible consommation énergétique. C'est un protocole de communication sans fil conçu par la ZigBee Alliance basé sur la norme IEEE 802.15.4.

FIGURE 1. Logo de la ZigBee Alliance

Cette technologie a pour but la communication à courte distance (quelques centaines de mètres) entre les différents noeuds du réseau. On pourra aussi remarquer que ZigBee a un débit faible (moins de 0.1 Mbps). La figure 2 nous présente les deux dernières

caractéristiques et compare les différentes technologies sans fil actuelles. Il faudra tenir compte de ces spécifications lors de la conception d'applications basées sur la technologie ZigBee. Par exemple, il serait impensable de remplacer la technologie Wifi des box internet actuelles par la technologie ZigBee étant donné que le débit est beaucoup trop faible pour transporter les données actuelles.

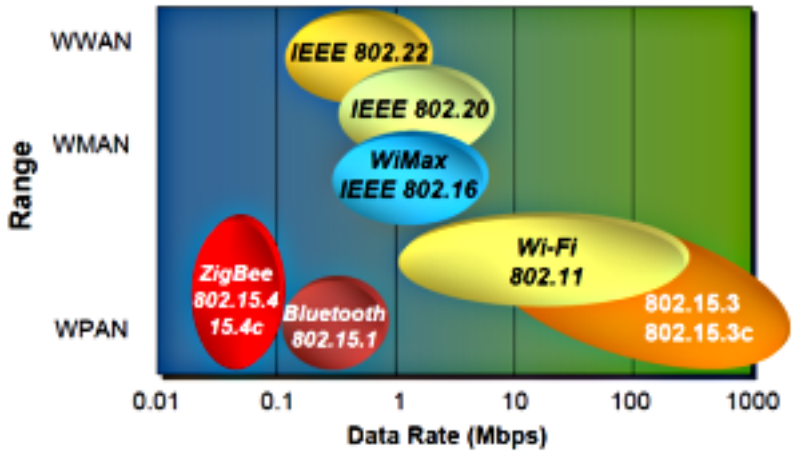

FIGURE 2. Graphique comparatif de différents protocoles sans fil

D'autres caractéristiques remarquables de ZigBee sont :

- le faible besoin de mémoire en comparaison à d'autres technologies sans-fil.
- la consommation réduite pour les systèmes fonctionnants sur batterie (se compte en années avec des piles AA).
- le coût réduit de l'infrastructure (équipements et installation) et la faible complexité.
- le grand nombre de noeuds adressables pour un seul réseau, permettant une zone de couverture étendue.
- le fonctionnement autonome, sûr et sécurisé pendant des années sans intervention.
- le protocole standardisé, qui permet à plusieurs vendeurs de rendre leurs produits interopérables sur le marché.

La différence entre ZigBee et la plupart des autres WPAN se situe au niveau du temps d'utilisation du média. ZigBee est optimisé pour une faible utilisation du médium partagé par tous, (0,1% du temps). En effet, un module émetteur-récepteur occupera le médium pendant quelques millisecondes pour l'émission des données, attendra éventuellement une réponse ou un acquittement, puis se mettra en veille pendant une certaine période avant l'émission suivante.

Market Name	ZigBee®	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA/1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

FIGURE 3. Tableau comparatif de différents protocoles sans fil

ZigBee prévoit deux types d'objets :

- les **FFD** (Full Function Device) : qui implémentent la totalité de la spécification. Ils ont 3 rôles possibles : coordinateur PAN, routeur ou dispositif terminal et peuvent communiquer avec FFD et RFD. Généralement, le FFD sera alimenté par une source non contrainte énergiquement.
- les **RFD** (Reduce Function Device) : entités allégées dans un objectif de moindre consommation énergétique et d'utilisation mémoire. Ils n'ont que le rôle de dispositif terminal car la pile réduite n'implémente pas le mécanisme de routage.

La ZigBee Alliance

La ZigBee Alliance, dont le slogan est "Wireless Control That Simply Works", a été formée en 1997 par huit compagnies et a pour but de standardisé le protocole ZigBee. Elle comprend maintenant plus de 200 entreprises et continue de s'étendre. Etre membre de la ZigBee Alliance signifie rejoindre le réseau de développeurs de la technologie ZigBee afin d'étendre le champ d'action, le nombre d'applications basées sur ce type de réseau, avoir une application certifiée ZigBee et être compétitif au niveau du marché.

Pour être membre de la ZigBee Alliance, il suffit de remplir un formulaire, accepter la licence et payer une certaine somme d'argent. Cette somme dépend du rang de membre souhaité : promoteur, participant ou adoptif. Être membre de l'Alliance est requis pour vendre des produits comportant la technologie ZigBee cependant ce n'est pas utile dans un but universitaire et toutes utilisations à but non-lucratif.

Grâce à ses avantages la ZigBee Alliance est présente sur de nombreux domaines en expansion, notamment la domotique (contrôle des volets, de la lumière...). Avoir des maisons entièrement automatisées représente aujourd'hui une certaine utopie mais ZigBee espère fournir l'avancée technologique afin de répondre à ce problème. Nous trouvons aussi ZigBee dans le domaine de la santé (bracelets pour malades), la gestion de l'énergie (capteurs de courant, gestion du chauffage), le contrôle à distante (télécommandes uniques pour divers équipements) et la télécommunication (paiement avec téléphones portables).

FIGURE 4. Le marché couvert par ZigBee

1.2 L'Architecture ZigBee

Comme le montre la figure 4, l'architecture ZigBee est composée de 4 couches sur les 7 du modèle OSI : Physique (*PHY*), Liaison (*MAC*), Réseau (*NWK*) et Application (*APL*). Entre ces couches se trouve les points d'accès aux services (*SAP*), ces SAP offrent les API pour permettre aux couches de communiquer tout en isolant le travail interne à chacune des couches. ZigBee utilise deux types de SAP par couches : un pour les données, et un pour le management.

Les deux couches inférieures (*PHY et MAC*) sont définies par les spécifications de l'IEEE 802.15.4, et les couches supérieures sont proposées directement par la norme.

La couche **PHY** traduit simplement les trames en bits qu'elle peut transmettre et recevoir par transmission radio. Conformément à IEEE 802.15.4, ZigBee peut travailler sur trois bandes de fréquences : 868MHz (Europe), 915MHz (Amérique du nord) et 2,4GHz (Mondial). La norme prévoit deux couches physiques différentes, une pour le 868/915MHz (*PHY868/915*) et une seconde pour le 2,4GHz (*PHY2450*) mettant en oeuvre une modulation à spectre étalé. Les principales fonctions remplies par cette couche sont les suivantes :

- l'activation et la désactivation de la transmission radio
- la communication des canaux
- l'évaluation de la qualité du canal

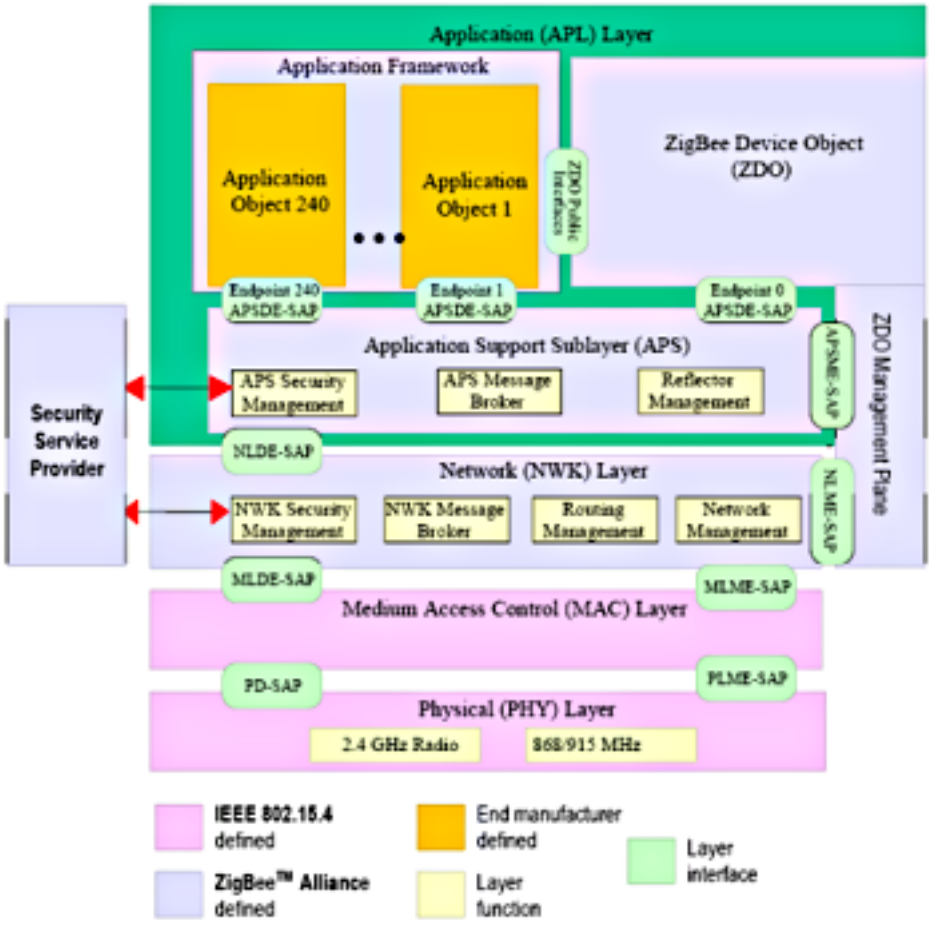

FIGURE 5. Architecture du protocole ZigBee

La couche **MAC** utilise le concept de réseau délivrant des services pour la formation ou la découverte des réseaux et la possibilité d'en rejoindre. Elle donne également un identifiant de PAN. Cette norme prévoit deux topologies différentes :

- Topologie étoile (*star*) : la communication est établie via un commutateur central (le coordinateur PAN) qui peut initier, terminer ou router les communications.
- Topologie point à point (*peer-to-peer*) : la communication se fait entre tous les noeuds à portée ensemble sans hiérarchie.

Les principales fonctions remplies par cette couche sont les suivantes :

- l'accès au canal physique pour les transferts (CMSA-CA)
- l'ordonnancement des données
- la délivrance de trames d'acquittement (ACK)

- la garantie de l'intégrité des données

La couche **NWK** est responsable de la topologie maillée (*mesh networking*) permettant à un noeud de communiquer à un autre grâce à un routage automatique. Cette technique permet aussi de recréer des chemins entre les noeuds même si des noeuds intermédiaires deviennent inaccessibles. La couche inclut aussi la diffusion des paquets, et permet l'envoi sûr d'un paquet vers un noeud. Tous les réseaux ZigBee sont sécurisés à la couche NWK et les données transmises sont encryptées. Les principales fonctions remplies par cette couche sont les suivantes :

- la responsabilité de la topologie (construction et maintenance)
- la possibilité d'adresser 65536 noeuds par PAN
- l'interconnexion possible de réseaux
- fournir les mécanismes pour joindre, quitter et former un réseau
- la gestion de l'adressage, du routage et de la sécurité
- la gestion des types de services applicatifs

La sous-couche APL, support d'application (**APS**), est utilisée comme un filtre. Elle comprend la signification des données reçues, vérifie si la source est reliée à l'application en question, filtre les éventuels doublons, et maintient une table de correspondance qui indique les noeuds ou groupes auxquels on souhaite s'adresser.

La sous-couche ZigBee Device Object (**ZDO**), est responsable de la gestion du réseau en local et via le médium d'accès. Il offre des services pour la découverte d'autres noeuds et services dans le réseau, et est définit l'état courant et le rôle de l'objet dans le réseau.

La partie **Application Framework** contient la ZigBee Cluster Library et fournit un framework dans lequel chaque application tourne. Les clusters sont des collections de commandes et attributs pour un certain comportement.

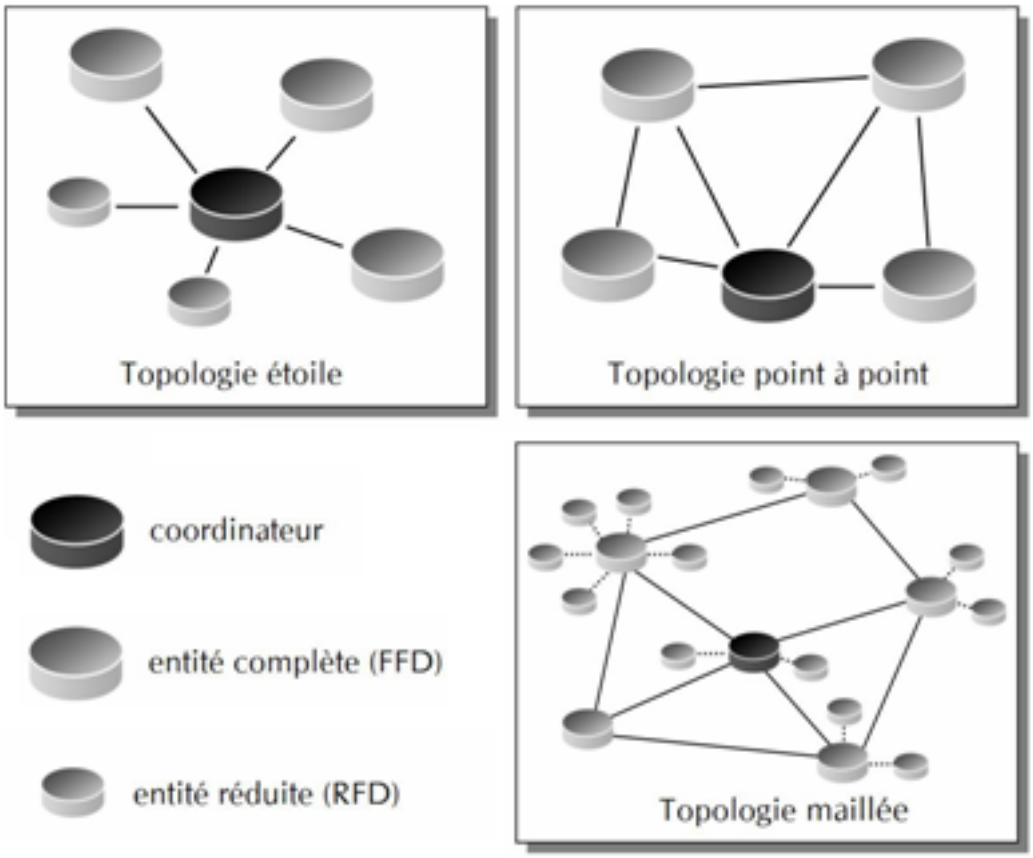

FIGURE 6. Les différentes topologies prises en compte par ZigBee

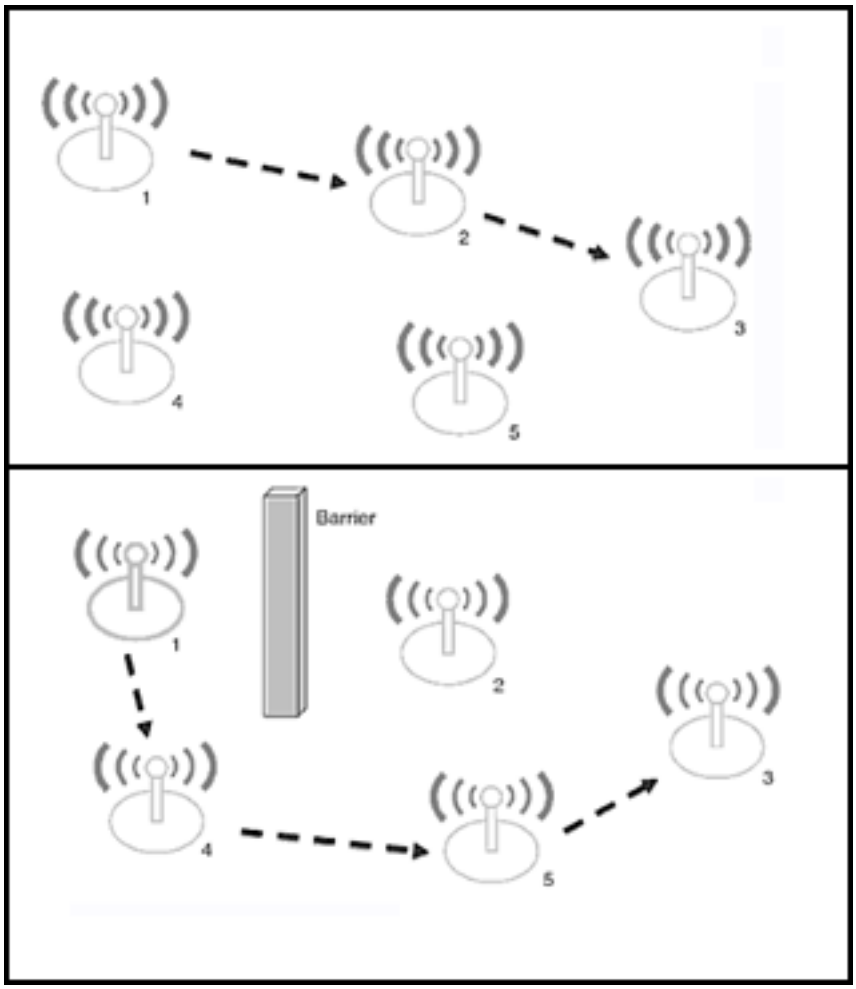

FIGURE 7. Les avantages du réseau maillé
(au dessus :1 peut communiquer avec 3 grâce à 2 ; en dessous : malgré la barrière 1 peut toujours communiquer avec 3 grâce au routage automatique qui a recréé un chemin passant par 4 et 5)

1.3 Etat de l'art : *Une méthode d'accès totalement déterministe pour un réseau personnel sans fil - Adrien Van Den Bossche, 2007*

La première partie du document présente la norme IEEE 802.15.4/ZigBee. De nombreuses choses évoquées plus tôt dans cet article sont dans ce document. De plus, ils expliquent que 802.15.4 a deux méthodes d'accès au médium :

- **un mode non coordonné (CSMA/CA)**, dont le principe, non expliqué dans le document, est le suivant : le noeud voulant émettre écoute le réseau. S'il est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé Distributed Inter Frame Space (DIFS)), alors la station peut émettre.
- **un mode coordonné (beacon mode)**. Ce dernier n'est disponible que pour topologie en étoile et voici le principe : le coordinateur envoie périodiquement des trames balises sur lesquelles peuvent se synchroniser les noeuds et s'en servir comme relais. Les supertrames correspondent à l'espace entre deux balises et comportent une partie active où les noeuds peuvent émettre et recevoir et une partie inactive où les noeuds somnolent. Deux méthodes d'accès au sein de la supertrame sont possibles :
  * La première partie est de type **avec contention**. Les accès au médium se font de façon " classique ", en best-effort, selon le protocole CSMA/CA.
  * La seconde, optionnelle, est dite **sans contention**. Dans ce mode, le coordinateur pourra allouer un ou plusieurs slots à un noeud en particulier s'il en fait la demande. On parle de Guaranteed Time Slots (GTS).

Ils montrent ensuite une série de failles comme, par exemple, le fait que l'obtention d'une réservation du médium est conditionnée par 2 points : le réseau ne doit pas être saturé et les premiers demandeurs sont les premiers servis et la demande de réservation utilise le protocole CSMA/CA qui ne permet pas d'avoir la certitude qu'il n'y aura pas de collision.

Ils proposent certaines améliorations incluant ces possibilités :

- *Mécanisme de demande de réservation du médium* : leur mécanisme prévoit la présence d'un supercoordinateur si plusieurs réseaux se chevauchent et alors un coordinateur doit d'abord envoyer une demande au supercoordinateur pour réserver le médium à un de ces noeuds, cette demande sera aussi faite de manière déterministe.
- *Mécanisme d'allocation au préalable pour les arrivées dans le réseau* : le supercoordinateur peut attribuer un GTS à un noeud avant son arrivée dans le réseau.
- *Mécanisme d'accès par défaut* : un slot qui n'est pas annoncé comme GTS n'est pas considéré comme librement utilisable, contrairement à 802.15.4, car il peut être réservé dans une autre étoile.

Dans le cadre d'une application de domotique, il ne faut pas que les commandes de l'utilisateur soient retardées ou impossibles du au nombre de noeuds trop important.
Ces failles ne sont obtenues que lors de l'accès au support avec l'utilisation de beacons, ceux-ci ne pouvant être mis en place que dans un réseau en étoile. La technologie ZigBee permet de créer des réseaux maillés et les mécanismes mis en place dans les couches supérieurs permettent d'éviter d'utiliser une topologie en étoile.

2 La sécurité ZigBee

2.1 Généralités

Les services de sécurité mis en place pour ZigBee se chargent de l'établissement et du transport des clés, de la protection des frames (paquets) et du management des équipements.

Chaque couche prend en charge le mécanisme de sécurité (*PHY*, *MAC*, *NWK* et *APL* [*APS* contient des services pour l'établissement et la maintenance des relations sécurisées et *ZDO* s'occupe de la politique de sécurité et de la configuration pour un équipement]) La spécification est basée sur un modèle, où chaque couche de la pile de protocoles se fait mutuellement confiance.

Comme nous l'avons dit plus tôt dans cet article, ZigBee est basé sur la norme IEEE 802.15.4 pour sa gestion des couches physique et liaison. Donc la sécurité pour ces couches est aussi assurée par cette norme. D'autre part la figure 5, nous montre la présence du "Security Service Provider" qui fournit la sécurité pour les couches NWK et APL.

2.2 La sécurité de la norme IEEE 802.15.4

La sécurité des trames

La couche IEEE MAC implémente de nombreuses caractéristiques qui sont utilisées dans le protocole ZigBee dans les couches réseau et application, dont le service de sécurité.

La norme IEEE 802.15.4 utilise l' algorithme de cryptage standard Advanced Encryption Standard (AES) avec une clé de 128bits (= 16 octets). Cette clé peut être préinstallée sur les noeuds, partagée hors bande (via un autre canal que celui d'envoi ou de réception de message), ou grâce à cette voie. Il faut noter que le standard IEEE 802.15.4 ne donne pas de schéma précis pour l'établissement de cette clé.
Le cryptage permet de cacher le message mais aussi de valider les données transmises (intégrité des données ou confiance accordée à l'émetteur).

Dans les trames IEEE 802.15.4, trois champs sont relatifs à la sécurité (représentés en rouge dans la figure 8). Une application qui utilise le standard IEEE 802.15.4 peut choisir différents types de protection en mettant en place différents paramètres de contrôle.

FIGURE 8. Le format des trames 802.15.4

Le champ "Auxiliary Security Header" présenté par la figure 9, est utilisé uniquement dans le cas lorsque l'on active le bit "Security Enabled" contenu dans la "Frame Control". Il est composé de 3 champs principaux : "Security Control" (protection utilisée) , "Frame Counter" (identifiant de compteur unique protégeant la duplication du message) et "Key Identifier" (informations indiquant la clé).

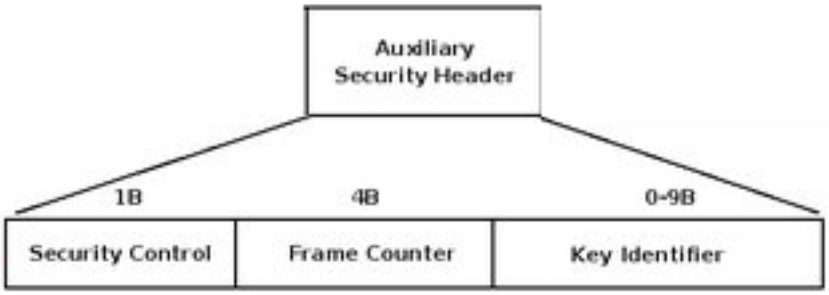

FIGURE 9. Le format du champ Auxiliary Security Header

Le champ " Security Control " est lui-même composé de 3 parties : " Security Level ", " Key Identifier Mode " et " Reserved ". La figure 9 nous montre la décomposition de ce champ.

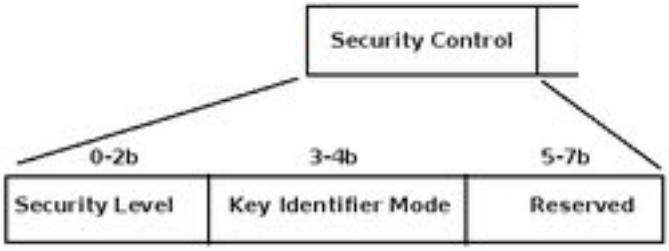

FIGURE 10. Le format du champ Security Control

Le champ " Security Level " indique quelle politique de sécurité est déterminée selon le tableau 1 :

TABLE 1. Différentes polices de sécurité des trames

Valeurs bits	Police de sécurité	Signification
000 (0x00)	Pas de sécurité	Pas de cryptage ni d'authentification des données
001 (0x01)	AES-CBC-MAC-32	Pas de cryptage
010 (0x02)	AES-CBC-MAC-64	mais l'authentification des
011 (0x03)	AES-CBC-MAC-128	données est garantie
100 (0x04)	AES-CTR	Cryptage mais pas d'authentification des données
101 (0x05)	AES-CCM-32	Cryptage
110 (0x06)	AES-CCM-64	et authentification
111 (0x07)	AES-CCM-128	des données

Le champ "Key Identifier", présenté dans la figure 11, permet de mettre en place le genre de clé qui doit être utilisé. Le tableau 2 représente les différentes valeurs et leurs correspondances.

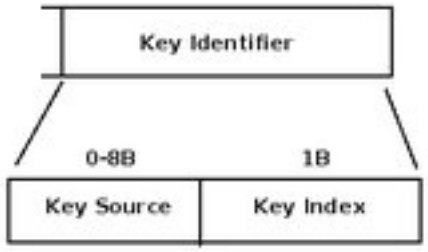

FIGURE 11. Le format du champ Key Identifier

TABLE 2. Identification de clé utilisée

Valeurs bits	Correspondance
00 (0x00)	L'identification de la clé est connue implicitement par l'émetteur et le récepteur
01 (0x01)	L'identification de la clé est déterminée explicitement par l'octet "Key Index" et de la macDefaultKeySource
10 (0x02)	L'identification de la clé est déterminée explicitement par l'octet "Key Index" et des 4 octets "Key Source"
11 (0x03)	L'identification de la clé est déterminée explicitement par l'octet "Key Index" et les 8 octets "Key Source"

Comme nous pouvons le constater sur le schéma 12. Les différentes techniques de cryptage permettent de déterminer le format de la trame " Data Payload ".
Nous aurons le cryptage des données via une clé 128bits ainsi que l'ajout de deux champs avant les données cryptées :

- " Frame Counter " qui va servir à éviter les attaques par réplications
- " Key Control " qui sera utilisé par la couche application si la valeur maximale de "Frame Counter" est atteinte.

D'autre part nous aurons aussi l'authentification qui va ajouter 4,8 ou 16 octets après les données pour le MAC (Message Authentification Code). Plus le nombre d'octets alloués pour ce message est important, plus la sécurité d'authentification est améliorée et plus il est difficile à un attaquant de casser cette sécurité. Cependant, cette amélioration donne un paquet plus lourd, ce qui peut s'avérer gênant.

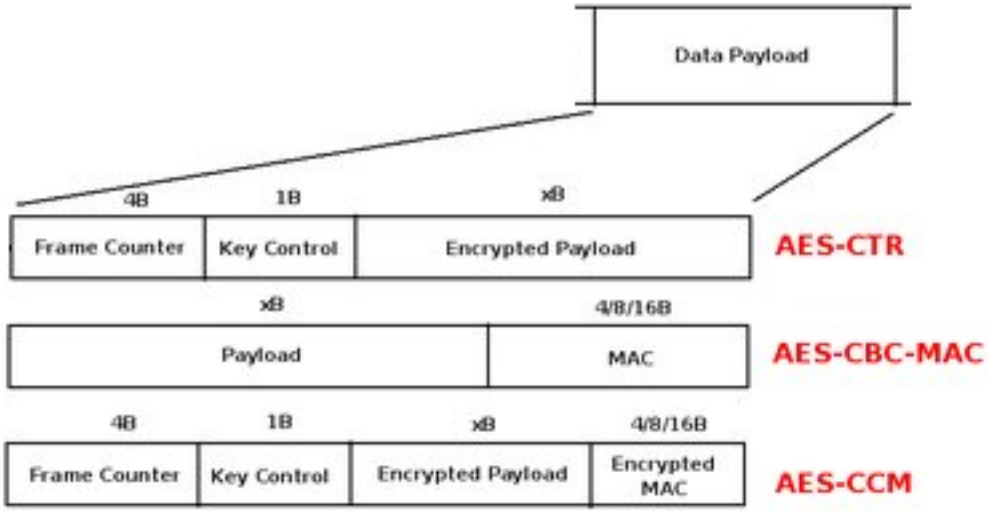

FIGURE 12. Le format du champ Data Payload

La sécurité des noeuds

En plus de la sécurité des trames, les noeuds se protègent de leurs voisins au niveau de la couche MAC. Pour cela chaque émetteur-récepteur traite sa liste de contrôle des noeuds de confiance. Cette liste de contrôle d'accès(*ACL*) contient les champs suivants :

- "Address" : Adresse du noeud voisin en communication
- "Security Suite" : Niveau de sécurité associé pour l'échange des messages. Voir le tableau 1
- "Key" : Clé de 128 bits utilisé pour l'algorithme AES
- "Last Initial Vector (IV) and Replay Counter"' : Last IV est utilisé par la source et Replay Counter par le destinataire comme identification de message, afin de lutter contre les attaques extérieures.

2.3 La sécurité des couches supérieures

Les clés de sécurité

Principe général

ZigBee est basé sur le chiffrement symétrique donc les deux équipements d'une communication protégée ont besoin de partager la même clé. C'est cette clé qui sera directement utilisée pour le chiffrement des données. La question est de savoir comment cette clé est distribuée à chaque équipement. Il y a trois méthodes :

- La préinstallation : Il s'agit de placer les clés dans l'équipement grâce à une méthode hors bande, via un équipement spécial comme un clavier par exemple.
- Le transport : C'est le centre de confiance qui envoie la clé, de la façon la plus sécurisée possible, aux deux équipements
- L'établissement : Il s'agit d'une méthode où les équipements négocient séparément avec le centre de confiance pour établir les clés sans qu'elles soient transportées en utilisant une de ces trois techniques :

  SKKE (*Symmetric-Key Key Establishment*)

  CBKE (*Certificate-based Key Establishment*)

  ASKE (*Alpha-secure Key Establishment*)

Il faut savoir que ZigBee utilise trois types de clés :

- Les communications de pair à pair sont protégées par des clés 128 bits (les "clés de liaison" ou "link keys") partagées par les 2 équipements pour la sécurité de la couche APS. Le plus souvent, un des deux équipement est le centre de confiance et c'est lui qui s'occupe de la création et l'établissement de la clé.
- Les communications broadcast sont protégées par des clés 128 bits (les "clés de réseau" ou "network keys") partagées par tous les équipements du réseau. Un jeu de clés est tenu par le centre de confiance du réseau et la clé de réseau courante est identifiée par un numéro de séquence de clé. Cette clé est généralement transportée par le Centre de confiance, mais peut aussi être préinstallée. La mise à jour se fait en deux étapes :

  Mise à jour de la nouvelle clé et du numéro clé de séquence associée

  Passer à nouveau numéro de la séquence de la clé
- Une "clé maître" ou "master key" est utilisée pour la génération des clés avec la technique *SKKE*.

Le protocole d'établissement des clés symétriques (SKKE)

Ce protocole étant très utilisé dans l'architecture ZigBee, et pouvant être utilisé aussi pour l'échange d'une clé au niveau de la couche MAC par exemple, nous avons choisit de le détailler dans cette partie spéciale.

Dans ce protocole un équipement est initiateur (nommé U), l'autre est répondeur(nommé V). Chacun des équipements partage une clé commune ("master key"). Cette clé doit être préinstallée, installée par un centre de confiance, ou entrée via mot de passe, code PIN, etc...

Dans cette partie, nous assumerons donc que cette partie du travail est déjà fait et que, par exemple, les " master keys " ont été préinstallées lors de la fabrication. Nous allons cependant mettre un bémol sur cette étape, en effet, si la " master key " partagée est compromise par un pirate, alors l'établissement d'une " link key " peut aussi être compromis. Dans le protocole suivant le symbole || signifie la concaténation

Etape 1 : Initialisation

Dans cette étape, l'initiateur envoie un challenge au récepteur (*QEU*) . Le récepteur va valider le challenge et envoyer à son tour un challenge (*QUV*) pour l'initiateur U. Lui aussi va valider le challenge de *V*.

Etape 2 : Génération du secret partagé

2.1 Chaque noeud va générer un *MACData* en apposant leurs identifiants et challenges respectifs comme suit :

$$MACData = U||V||QEU||QEV$$

2.2 Chaque partie va calculer la signature du *MACData* (que nous appellerons *MACTag*) en utilisant la clé partagée (*Mkey*) comme clé de la fonction de hachage (HMAC) :

$$Z = MAC_{Mkey}MACData$$

Les deux parties partagent donc le même secret, qui n'est pas encore la clé partagée.

Etape 3 : Dérivation de la clé

Chaque partie va dériver Z avec la même fonction de dérivation de manière à obtenir une valeur $KKeyData$ de 256 bits.

$$Hash_1 = H(Z||01_{16})$$
$$Hash_2 = H(Z||02_{16})$$
$$KKeyData = kdf(Z, 256) = Hash_1||Hash_2$$

La valeur $Hash_2$ sera la clé partagée ("link key") entre les deux équipements.
Pour confirmer que les deux parties sont arrivées à la même " link key ", nous utiliserons la valeur de $Hash_1$, comme clé pour notre fonction de hachage pour l'étape de confirmation :

$$MACKey = Hash_1 \text{ (1)}$$
$$KeyData = Hash_2 \text{ (2)}$$

Etape 4 : La confirmation

Pour finir, les équipements ont besoin d'être sûrs qu'ils partagent la même clé sans se l'envoyer. Pour cela, ils vont encore compter sur les fonctions de hachage, et ils vont générer différents *MACTags* basés sur différentes valeurs mais ils vont utiliser la même clé(la *MACKey*) pour générer les hachages avec la clé (*MACTags*).

4.1 La génération des *MACTags* :
U et *V* vont d'abord générer les valeurs *MACData*. Puis, basées sur ces valeurs, *U* et *V* vont générer les *MACTags*. L'initiateur va recevoir le $MACTag_1$ du répondeur et générer $MACTag_2$ pour le renvoyer au répondeur.
Les *MACData* et *MACTags* sont calculés comme cela :

Premièrement, les deux équipements vont calculer les valeurs *MACData*

$$MACData1 = 02_{16}||V||U||QEV||QEU$$
$$MACData2 = 03_{16}||U||V||QEU||QEV$$

A partir de là, les deux équipements vont générer les *MACTags* grâce aux *MACkey*

$$MacTag_1 = MAC_{MacKey}MacData_1$$
$$MacTag_2 = MAC_{MacKey}MacData_2$$

4.2 La confirmation des *MACTags* :
Finalement, l'initiateur U va recevoir le $MacTag_1$ et le répondeur va recevoir le $MACTag_2$. Puis ils vont vérifier que les *MACTags* reçus sont égaux aux *MACTags* calculés par chaque équipement. Si la vérification est un succès, chaque noeud sait que l'autre a calculé la " link key " correctement.

La figure 13 est là pour synthétiser toutes les étapes du protocole SKKE.

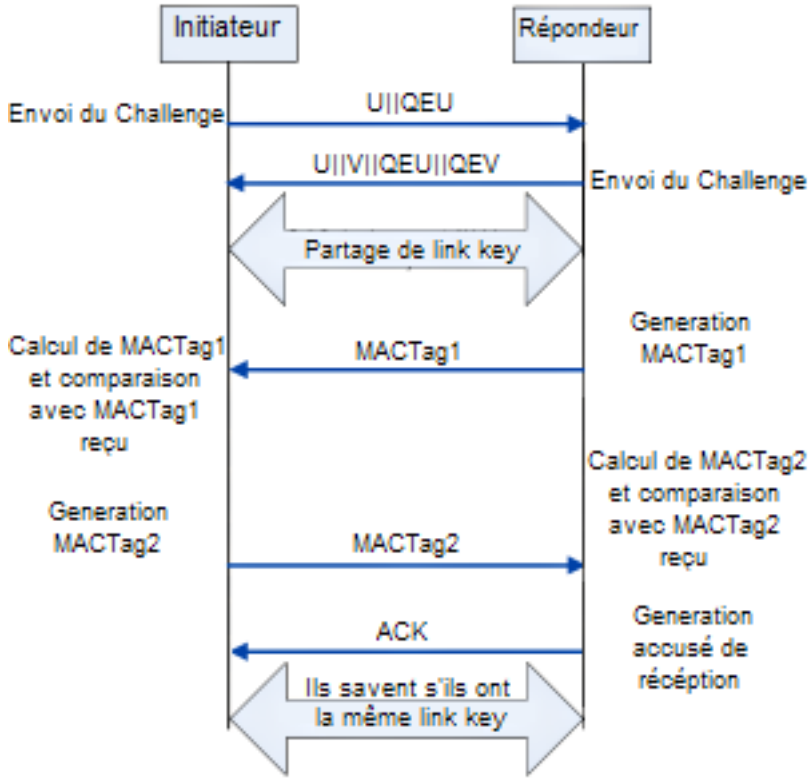

FIGURE 13. Le protocole SKKE

Le Centre de Confiance

Les spécifications ZigBee introduisent le rôle de centre de confiance qui est un équipement auquel les autres équipements du réseau peuvent avoir confiance. C'est celui-ci qui distribue les clés et contrôle les accès. Il y en a un seul par réseau et il s'agit le plus souvent du coordinateur ZigBee.

Il donne les fonctions suivantes :

Identifier et authentifier des équipements qui rejoignent le réseau

Garder et distribuer les clés réseaux aux équipements dont il s'occupe

Relier deux noeuds et d'activer la sécurité entre les équipements dont il s'occupe du début à la fin

Il peut être configuré selon 2 niveaux de sécurité :

- *Commercial mode* : il donne un niveau élevé de sécurité (*High Secure*). Le centre doit maintenir une liste de tous les équipements, link keys, master keys, network keys. Il établit et maintient les clés et compteurs avec tous les éléments. Il devrait également appliquer les politiques nécessaires pour la mise à jour des clés et du contrôle d'accès. Plus il y a d'équipements plus la mémoire requise est importante. Pour ce type de mode les équipements contiennent généralement l'adresse du centre et la master key initiale.
- *Residential mode* : il donne un niveau bas de sécurité (*Standard Secure*). Il peut maintenir une liste de tous les équipements et partage juste la network key. Les équipements ont besoin de la " network key " qui peut être préconfigurée ou envoyée par transport non sécurisé.

La Sécurité des messages

ZigBee permet de protéger les messages non seulement au niveau *MAC* comme nous l'avons vu précédemment mais aussi aux niveaux supérieurs *NWK* et *APS*. Chacun de ces niveaux peut garantir la sécurité et l'intégrité du message.

La couche NWK

Le rôle de cette couche est de donner des fonctionnalités pour assurer les opérations de la couche *MAC* et de donner un service correct pour la couche *APL*. Quand un paquet de cette couche a besoin d'être sécurisé, elle utilise la cryptographie AES comme la couche *MAC*.

Ce sont les couches supérieures qui s'occupent d'installer les clés de sécurité, les compteurs de paquets et les niveaux de sécurité. Si celle-ci n'est pas disponible, la couche *NWK* peut utiliser la clé réseau active pour émettre le message, et la clé active ou alternative pour les messages entrants. Elle utilise le *MIC* (Message Integrity Code) pour déterminer le niveau de sécurité. Comme le montre la figure 14, un paquet qui a besoin d'être sécurisé est un paquet comprenant le champ " Auxiliary Header " (d'une longueur de 14 octets).

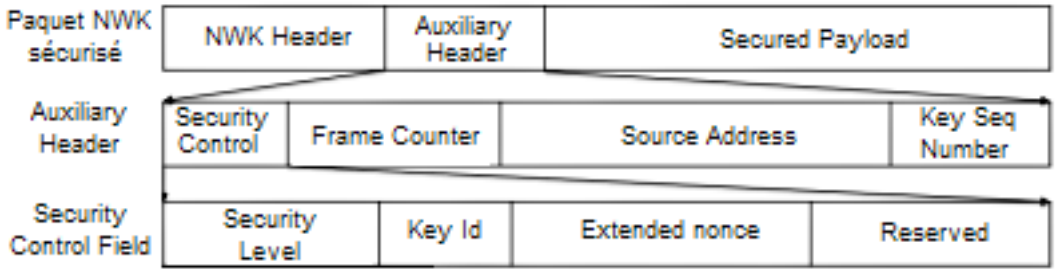

FIGURE 14. Le format des trames NWK

Puis le " Frame Counter " permet de donner un numéro à la trame pour, notamment, éviter les duplications. Ainsi chaque noeuds va garder un compteur de paquets reçus ("Frame Count") avec chaque autre noeud dans la Network Information Base (NIB). Donc lors de la réception, si ce le Frame Counter reçu est inférieur au Frame Count alors on abandonne. Sinon on met à jour le Frame Count avec " Frame Counter reçu + 1 "

A savoir que les données transportées par la trame respectent les principes de sécurité du tableau 1. La sécurité des données n'est pas que dans le fait du cryptage des données mais aussi du contrôle de l'intégrité.

La couche APL

Comme nous le montre la figure 5, la couche *APL* est composée des sous couches *APS* et *ZDO*. *ZDO* définit les objets de l'application et est responsable de l'initialisation de la sous couche *APS*, la couche *NWK*, du Security Service Provider et de l'assemblage des informations de l'application. Quand la couche application a besoin d'être sécurisée, c'est la sous couche *APS* qui s'occupe de la sécurité. Donc, la sécurité de la couche application est en fait entièrement prise en charge par la sous couche *APS*.

La sous-couche APS

C'est elle qui donne l'interface entre la couche *NWK* et *APL*. Elle traite les paquets (entrants et sortants) pour les envoyer et les recevoir de façon sécurisée. De plus elle établit et s'occupe des clés. Elle utilise les fonctions de sécurité, basées sur la " link key " ou la " network key " pour sécuriser les trames émises par la couche *APL*. Elle utilise aussi le MIC (Message Integrity Code) pour déterminer le niveau de sécurité. Elle fournit des services pour :

- L'établissement des clés : C'est le mécanisme pour créer la " link key ". Les deux équipements partagent une " master key " qui sera utilisée pour la génération. Dans la spécification de 2007 la méthode employée est la SKKE (Symmetric-Key Key Exchange). Récemment, PKKE (Public-Key Key Establishement) est inclus dans le profil de l'application.

- Le transport des clés : Elle ne peut pas se faire via un système de sécurisation avec cryptographie étant donné que le receveur ne pourra pas la décoder. Un moyen pour faire un tel échange de clé est de faire la transmission par un canal hors bande. Mais ce service va permettre l'échange (un minimum sécurisé ou non) des clés.
- La mise à jour des équipements : C'est le mécanisme qui permet au centre de confiance de maintenir une liste à jour des équipements. Le principe est qu'un premier équipement prévient un deuxième qu'un troisième change de statut (joindre ou quitter le réseau)
- Suppression d'équipement : Principe par lequel un équipement informe un autre équipement pour supprimer un équipement connecté au réseau qui ne respecte pas les principes de sécurité du réseau
- Changement de clé : Moyen sécurisé pour un équipement d'informer un autre équipement qu'il devrait passer à un autre réseau actif
- Demande de clé : Moyen sécurisé pour demander la "clé réseau" courante, ou la "clé maître" à un autre équipement
- La table de configuration des permissions : Elle contient les informations sur les équipements qui ont les autorisations pour réaliser telles ou telles commandes. De plus, la PCT (Permission Configuration Table) détermine si une sécurité basée sur une " link key " est requise ou non avec l'autre équipement. Le maintien d'une telle table est optionnel.

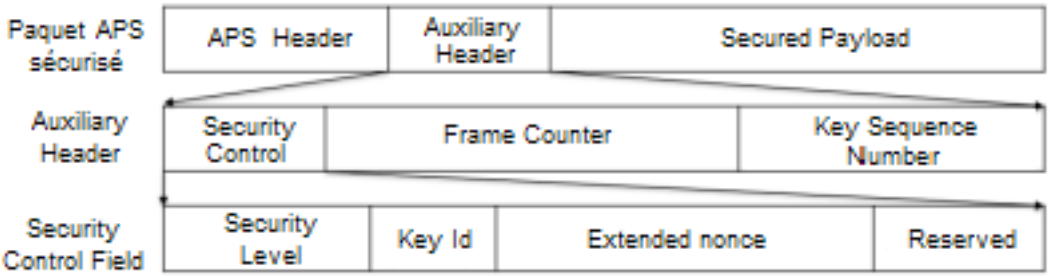

FIGURE 15. Le format des trames APS

La structure du paquet APS est donnée par la figure 15. Encore une fois on constate la présence d'un champ " Frame Counter ". Les données transportées comprennent un premier champ de un octet correspondant à un identificateur de commande APS afin de donner le type de commande (SKKE, Transport de clé, Mise à jour des équipements, ...) du paquet. Il y a quelques points importants à noter dans ces commandes. L'établissement des clés (comme SKKE) se fait de façon non sécurisée.
Nous noterons que le principe de sécurisation est quasiment équivalent à la couche NWK. En effet APS détient aussi une liste indiquant les liens (différentes informations) et principes de sécurité (" link keys " / " network key ") à utiliser avec chaque noeud.

Rejoindre un réseau ZigBee

Principe

Lors de cette étude, nous notons que les réseaux ZigBee ont tendance à être très axés sur la sécurité. Les messages sont sécurisés, plusieurs clés sont mises en place, des algorithmes complets peuvent être instanciés, etc... Mais encore faut il qu'il n'y ai pas de faille dans les équipements d'un réseau. Imaginons qu'un équipement soit compromis ou arrive à entrer dans le réseau sans aucune autorisation, alors la mise en place de tous ces principes de sécurité deviendrait complètement inutile. C'est pourquoi le moyen de rejoindre un réseau ZigBee est aussi soumis à des algorithmes de sécurité.

Comme nous l'avons dit plus tôt il y a dans tout réseau un Centre de Confiance. Généralement c'est le coordinateur qui joue le rôle de Centre de Confiance. C'est à travers lui que les messages vont transiter et que la décision va être prise pour inclure un équipement au réseau. Les équipements initialement présents dans le réseau mais ayant manqué une mise à jour de la "network key" vont devoir refaire le scénario pour réintégrer le réseau.

Scénario

La jointure non sécurisée via un routeur Cette partie dépend de la couche MAC qui est définie dans les spécifications de IEEE 802.15.4 et pas dans les spécifications ZigBee. Nous remarquerons qu'elle est très peu sécurisée avec généralement des envois de trames non cryptées.
Nous pourrons noter que ces échanges peuvent être cryptés si l'on procède à un préinstallation des clés au niveau de la couche *MAC* entre le premier routeur et l'équipement qui veut rejoindre le réseau. Cependant les spécifications ne le prennent pas en compte et nous constaterons que c'est inutile de suivre une telle procédure, étant donné que l'échange des clés finales sera sécurisé. Selon nous, ça ne ferait que réduire les performances du réseau.

- Tout d'abord le noeud (routeur ou équipement final) qui veut rejoindre un réseau (nous l'appellerons X), envoie une demande non sécurisée. Les routeurs dans la zone d'émission ayant reçus la requête renvoie une réponse et X choisit le réseau à rejoindre par la suite.
- X envoie ensuite la demande d'association avec ce routeur (R).
- R va répondre, connaissant l'adresse de X et les principes de sécurité dans le cas d'une réassociation. C'est le seul point où on peut avoir de la sécurité. R peut refuser si X est dans une blacklist par exemple.
- Si X reçoit une réponse positive alors il est déclaré comme *joint mais non authentifié*. Il va devoir donc passé à l'authentification.

L'authentification via le Centre de Confiance Cette procédure est lancée une fois qu'un équipement est *joint mais non authentifié*. L'authentification dépend de plusieurs paramètres comme le niveau de sécurité (Haut ou Standard), la présence de routeur(s) intermédiaire(s) avec le Centre de Confiance, le niveau de sécurité, les pré configurations, etc...
Nous remarquerons que dans les spécifications de 2007, les routeurs voisins du nouvel équipement doivent aussi l'authentifier via un protocole d'authentification mutuelle. Ce protocole est basé sur un challenge, un secret partagé (la "network key"), et la vérification.

Nous avons choisi de décrire le scénario du modèle de sécurité commun de la ZigBee Alliance : La "link key" préconfigurée sur X et pour étendre notre exemple à un cas plus complexe, R n'est pas le Centre de Sécurité (TC)

- Une fois la jointure réalisée (couche 2), R va donc envoyer la mise à jour à TC pour l'autorisation. Ces communications entre R et TC sont sécurisées au niveau de la sous couche APS en utilisant la "link key" entre R et TC.
- TC crypte le transport de la "network key" pour X grâce à la "link key" partagée entre TC et X, préconfigurée sur X et l'envoie via un tunnel à R.
- R récupère donc la "network key" transportée et l'envoie à X de manière non sécurisée au niveau de R. Cependant seul un équipement avec la "link key" partagée entre X et TC pourra décrypter le message.
- X reçoit donc la "network key" grâce à sa "link key" préconfigurée.
- X établit une procédure d'authentification avec R via l'authentification mutuelle afin de voir s'il a reçu la bonne "network key", et finir la procédure totale.

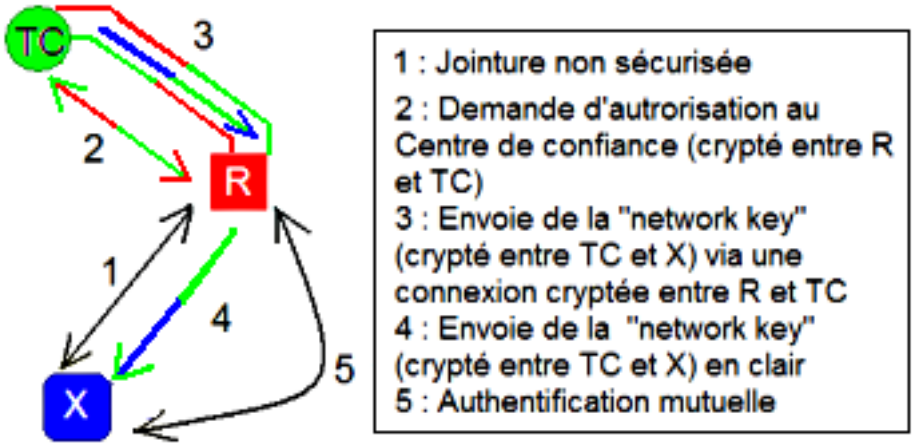

FIGURE 16. Le mécanisme de jointure dans un réseau ZigBee

2.4 Etat de l'art - Travaux existants

2.4.1. Towards security issues in ZigBee architecture - Pavel Ocenasek, 2009

Dans cet article, l'auteur étudie deux points importants pour évaluer la sécurité des réseaux ZigBee. Le premier point est le standard 802.15.4 définit par l'IEEE. Il s'intéresse particulièrement aux services de sécurité fournit par la couche MAC :

- *Le contrôle d'accès et l'intégrité des messages* qui a pour but d'empêcher des tiers d'accéder au réseau et de détecter et rejeter des messages venant d'eux.
- *La confidentialité* doit permettre de garder les informations secrètes aux parties non autorisées. Pour cela, la couche MAC utilise généralement le cryptage
- *La protection contre la réémission (ou le rejeu)*. Une personne non autorisée qui arrive à intercepter un message peut effectuer une attaque par répétition.

Le deuxième point exposé concerne l'architecture ZigBee. Celle-ci fournit une sécurité au niveau de l'authentification, du cryptage, de l'intégrité des messages et une protection contre la réémission de messages.

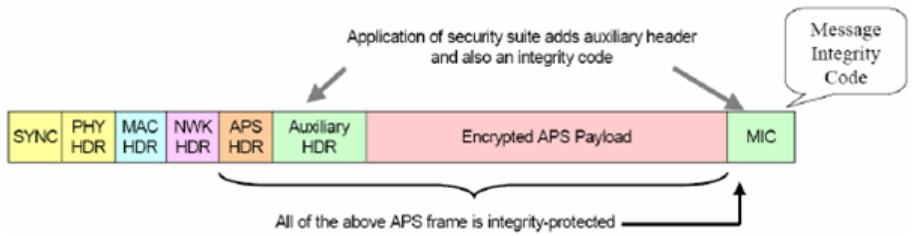

FIGURE 17. Différents en-têtes pour assurer la sécurité des produits ZigBee

L'architecture offre deux modes d'opérations :

- *Le mode résidentiel* est le mode prévu pour les néophytes en termes de sécurité. Tout ce fait automatiquement et ils ne jouent aucun rôle dans la maintenance de la sécurité. On utilise seulement les clés de réseaux pour protéger l'installation. Le centre de confiance résidentiel ne stocke que les clés réseaux, donc n'importe quel capteur peut servir de centre de confiance. Ce dernier fournit une sécurité du point de vue authentification, intégrité et cryptage des messages. Cependant, d'après Pavel, le réseau est vulnérable aux attaques d'initiés.
- *Le mode commercial* permet au réseau de contrôler les applications critiques (alarmes, surveillances ...). Le réseau est activement surveillé et maintenu (mise à jour des clés, ajout contrôlé des nouveaux appareils). Dans ce mode, les nouveaux appareils ne sont admis que manuellement. Le centre de sécurité met à jour les clés réseaux périodiquement. Celles-ci ne sont utilisées que par la couche réseau, ce qui empêche les attaquants de prendre le contrôle d'un appareil.

Pour finir, l'auteur met en avant les différentes vulnérabilités et problèmes de l'architecture ZigBee et donnent quelques recommandations pour améliorer le réseau. Il identifie trois types de vulnérabilités et problèmes :

- **Problèmes de gestion** tels que le problème de clé identique dans les entrées multiples de la liste de contrôle d'accès
- **Problèmes d'intégrité** tels que les modes de cryptage sans authentification
- **Problèmes de la gestion des clés** tels que les clés de réseau partagées incompatibles avec la protection à la réémission

Les problèmes de la gestion des clés sont dus en partie aux " nonce ". En effet, ceux-ci ont deux rôles : ils fournissent une valeur de non-répétition pour assurer la confidentialité et il fournit un compteur monotone croissant pour empêcher la réémission. L'expéditeur doit donc s'assurer qu'il n'utilise jamais le même nonce deux fois pour un même message.

Cependant, Etant donné que l'auteur ne cite pas ses sources, nous ne savons pas clairement si tous ces problèmes sont exploitables en pratique. N'offrant pas d'idées d'implémentation, des recherches futures devront être effectuées pour permettre une évolution rapide des services de sécurité ZigBee.

2.4.2. An Identity-Based Auth Protocol for Clustered ZigBee Network - Wei Chen, Xiaoshuan Zhang,Dong Tian and Zetian Fu, 2010

Ce document traite de la sécurité des réseaux ZigBee et stipule qu'il est vulnérable à différentes attaques. Les auteurs proposent un protocole d'authentification identitaire pour clustériser un réseau ZigBee et un protocole sécurisé pour l'échange de paramètres publics entre deux clusters.

Avec la diversité des applications dans lesquelles ZigBee peut être utilisé, ils expliquent qu'il est nécessaire que le protocole d'authentification doit sécuriser les communications et résister à diverses attaques. Cependant il y a deux problèmes aux normes définit par ZigBee Alliance. Le premier est le nombre de clés utilisées dans le réseau. En effet, chaque paire de noeuds partagent une clé unique. Le nombre de clés maîtres dans le mode commercial est de l'ordre de n^2 avec n étant le nombre de périphériques du réseau. Le deuxième problème est la vulnérabilité du protocole d'échange de clé à clés symétriques. Dans ce protocole, le coordinateur ne peut pas rejeter un appareil avant d'avoir reçu le message SKKE-4 (Symmetric-Key Key Exchange). Il s'expose donc à des attaques de type déni de service (DoS attack) qui va consommer la batterie des noeuds et surcharger le réseau.

Les auteurs définissent les trois types de clés utilisées par ZigBee :

- La **master key** qui est une clé à long-terme utilisé pour la livraison des clés de cryptage.
- La **link key** qui assure la sécurité sur un lien spécifique entre 2 noeuds.
- La **network key** qui assure la sécurité dans le réseau.

Un dispositif peut acquérir une clé de liaison et une clé de réseau via la clé de transport ou la préinstallation. La norme ZigBee contient le protocole SKKE qui empêche les dispositifs malveillants de se joindre au réseau.

A la suite d'un état de l'art sur la cryptographie identitaire et de quelques explications sur la cryptographie identitaire et bilinéaire, les auteurs établissent un modèle du système et du réseau utilisés.

- **Modèle du système**

  Les auteurs utilisent un réseau ZigBee à grande échelle pour pouvoir utiliser plusieurs clusters. Un cluster contient un coordinateur et plusieurs appareils. Chaque cluster est connecté par une Autorité d'Identification (AI) via son coordinateur. La clé publique de l'AI est connue de tous les coordinateurs. Dans ce schéma, les coordinateurs utilisent une cryptographie basée sur les certificats et les appareils finaux utilisent une cryptographie identitaire.

  Les coordinateurs obtiendraient leur certificat à la configuration du réseau et les appareils finaux obtiendraient leur clé privée par un mécanisme d'accès direct (out-of band). Désormais, lorsque les coordinateurs ne sont pas connectés à l'AI ils peuvent s'authentifier mutuellement grâce aux certificats et les appareils finaux grâce à la cryptographie identitaire. Périodiquement, les coordinateurs se connecteront à l'AI grâce à un mécanisme d'accès direct (out-of-band) et l'AI pourra détecter les coordinateurs compromis, les réinitialiser ou les remplacer.

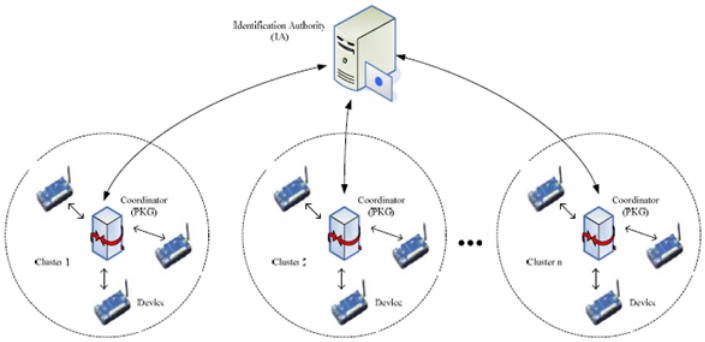

FIGURE 18. Modèle du système utilisé avec différents clusters et une autorité d'identification

- Modèle du réseau

Les auteurs supposent que le réseau ZigBee a les caractéristiques suivantes :

1. Les coordinateurs sont plus puissants que les appareils finaux et peuvent effectuer à la fois l'authentification basée sur les certificats et l'authentification identitaire.

2. Les appareils ont la puissance de calcul nécessaire pour calculer les cartes bilinéaire, et seulement effectuer une authentification identitaire.

3. L'adversaire n'a pas pu trouver la clé privée correspondant à une clé publique donnée. L'adversaire a une capacité de temps de calcul polynomial et ne peut pas résoudre les problèmes difficiles bien connus, tels que le problème du logarithme discret...

4. L'adversaire pourrait obtenir des messages en passant par le réseau.

De plus, les auteurs établissent les hypothèses suivantes :

- Lorsque les deux noeuds appartiennent au même cluster, ils partagent un ensemble de paramètres identitaires du système, et ils peuvent calculer une clé partagée en utilisant des cartes bilinéaires directement pour s'authentifier mutuellement.
- Lorsque les deux noeuds appartiennent à différents clusters qui ont différents paramètres identitaires du système, il est nécessaire d'échanger des paramètres système entre ces groupes pour mettre en oeuvre l'authentification identitaire. Pour cela, ils utiliseront l'authentification basée sur les certificats pour assurer la sécurité de la procédure d'échange.

Leur proposition se compose de l'association de deux algorithmes disponibles dans leur article. Le premier est utilisé pour établir une clé partagée entre deux noeuds qui appartiennent au même cluster, le second est utilisé pour les paramètres systèmes à échanger entre deux noeuds qui appartiennent à différents clusters.

2.4.3. ZigBee-2007 Security Essentials - Ender Yüksel, Hanne Riis Nielson and Flemming Nielson, 2008

Dan cet article, qui est un document fondateur de ZigBee de part sa complétude et sa bibliographie, les auteurs présentent les éléments essentiels de la sécurité de la spécification ZigBee-2007. Ils expliquent les différents concepts de clés, de protocoles et de calculs mis en oeuvre. De plus, ils expliquent les protocoles utilisant les standards puis finissent par identifier les principaux défis à prendre en considération pour consolider les réseaux ZigBee.

Certains points de l'article ayant déjà été traités plus tôt dans ce rapport (comme la spécification ou l'architecture ZigBee), nous ne reviendrons pas dessus et nous nous intéresserons particulièrement aux points non soulevés ou beaucoup plus complets.

les auteurs étudient les différentes clés de sécurité et le centre de confiance de ZigBee. La clé de liaison (LK) est partagée entre deux appareils et est utilisée pour sécuriser les communications de couche Application. Elle est utilisée comme sécurité de base en mode Haute Sécurité (HS). La clé réseau (NK) est partagée entre tous les appareils du réseau et est utilisée pour sécuriser les diffusions au sein d'un réseau. Elle est utilisée comme sécurité de base en mode Sécurité Standard (SS). Pour finir, la clé maître (MK) est utilisée pour crée une clé partagée entre deux appareils ZigBee. Il existe trois méthodes différentes pour acquérir des clés :

Méthode d'acquisition/Type de clé	NK	MK	LK
Transport de clé (via le centre de confiance)	Oui	Oui	Oui
Etablissement d'une clé (via MK)	Non	Non	Oui
Pré-installation (avant de rejoindre le réseau)	Oui	Oui	Oui

FIGURE 19. Méthode d'acquisition et type de clé utilisé

Les clés réseaux disposent de deux modes différents (sécurité standard et haute) et dans certains modes, les clés peuvent être optionnelles. Il existe 2 types de clés NK en fonction du mode de sécurité SNK pour le standard et HSNK pour l'haute.

Clés	Couches		Modes	
	Réseau	Application	SS	HS
NK	Oui	Oui	Oui	Oui
MK	Non	Oui	Non	Oui (Optionnelle)
LK	Non	Oui	Oui (Optionnelle)	Oui (Optionnelle)

FIGURE 20. Différents modes de fonctionnement

Il est possible de dériver des clés à partir de la "link key" pour différentes méthodes d'acquisition. Pour calculer ces clés, il faut utiliser une fonction de hachage de clés pour le code d'authentification de message (HMAC).

Type de clé	Calcul en hexadecimal	Explications
Clé pour le transport de clé	$HMAC(0x00)_{LK}$	Protège le transport de la NK
Clé pour le chargement de clé	$HMAC(0x02)_{LK}$	Protège le transport de la MK et de la LK
Clé de données	LK	Equivalente à LK

FIGURE 21. Calcul du HMAC

Il existe trois types d'appareils ZigBee : les appareils terminaux, les routeurs et les coordinateurs. Le coordinateur sert de centre de confiance (TC) dans un réseau. C'est avec lui que se fera l'échange de clés pour un appareil désirant entrer dans le réseau. En mode SS (résidentiel) ils échangeront une NK tandis qu'en mode HS (commercial) ils échangeront une MK. Dans les réseaux vulnérables, il est nécessaire que ces clés s'obtiennent par préinstallation. Le TC peut se configurer soit en mode SS où il maintient à jour le SNK et il contrôle les politiques d'admission soit en mode HS où il maintient une liste de tous les périphériques du réseau. Dans le mode HS, les protocoles d'échange de clé à clé symétrique et d'authentification mutuelle sont obligatoirement utilisés.

Différents protocoles et services sont utilisés pour assurer la sécurité des appareils ZigBee :

- Le protocole **AES-CCM* mode de fonctionnement** est utilisé par la couche NWK et les trames APS. C'est une extension de l'AES-CCM et fournit des fonctions pour l'authentification et le chiffrement.
- La sous-couche **APS** inclut beaucoup de services de sécurité tels que la mise à jour de l'appareil, le transport de clé, etc...
- Le protocole **d'authentification mutuelle (MEA)** permet à un émetteur et à un receveur de s'authentifier mutuellement à l'aide d'une clé secrète NK. Les appareils s'authentifient à l'aide de challenges aléatoires qu'ils se soumettent.
- Le protocole **d'établissement de clés à clés symétriques** un dispositif émetteur veut établit une LK avec un receveur en partageant une MK.

Par la suite, les auteurs définissent différentes procédures de base pour un réseau ZigBee :

- L'adhésion à un réseau
- L'authentification de l'appareil
- La mise à jour de la clé réseau
- L'établissement des clés d'application de terminaux à terminaux
- Le retrait d'un appareil du réseau

Pour finir, les auteurs un état de l'art sur les travaux existants et liés à leurs recherches tels que des travaux sur les fonctions de cryptographie symétrique, les vulnérabilités décelées dans la norme IEEE 802.15.4, une comparaison avec la sécurité d'autres réseaux à faible consommation, une politique de sécurité contre le cambriolage etc...

3 Développement du projet

3.1 Contexte du projet

La domotique

Généralités

La domotique est "l'ensemble des techniques visant à intégrer à l'habitat tous les automatismes en matière de sécurité, de gestion de l'énergie, de communication, etc... ". Il s'agit donc d'avoir toutes des fonctions permettant d'automatiser sa maison selon ses besoins et ses envies.

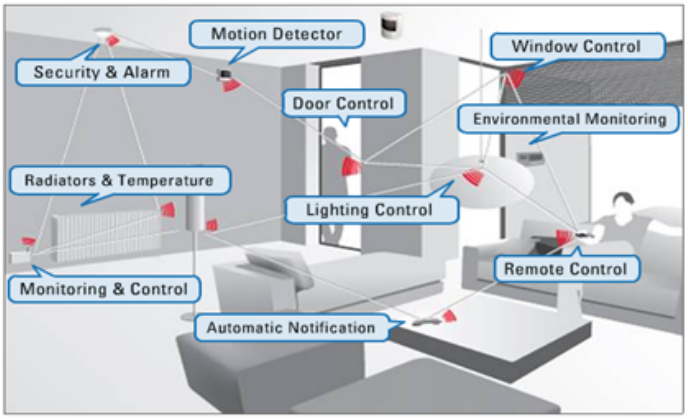

FIGURE 22. Exemple de domotique présente dans une maison

Actuellement, la domotique ne rencontre pas encore un réel un succès. Il n'existe pas ou très peu d'habitations ou lieux de travail où la technologie automatique s'est installée pour régir les règles de l'habitat. Pour investir dans une telle technologie, il faut que l'utilisateur trouve un système complet, peu cher, très facile d'utilisation et utile auquel il peut avoir entièrement confiance. Typiquement personne ne choisira une solution qui prendra le contrôle de sa maison s'il ne sait pas parfaitement comment il fonctionne, qu'il n'est pas sûr ou qu'il est beaucoup trop complexe d'utilisation. Au contraire, l'Homme doit dominer la situation surtout lorsqu'il s'agit de tous les équipements de sa propre maison.

Par ailleurs, nous noterons aussi que l'Homme aime automatiser les tâches qu'il réalise quotidiennement. C'est sur ce point qu'il faut se baser en respectant les autres contraintes pour permettre de développer, petit à petit, la domotique dans les environnements résidentiels, commerciaux et industriels. Au fur et à mesure de ce développement, il prendra confiance et sera incité à vouloir de plus en plus de facilité au quotidien.

La domotique pourrait aussi être considérée comme un luxe. Il serait bon de développer des applications et des technologies requérant un faible coût à l'achat, lors de l'installation et avec très peu de management.

Les caractéristiques de ZigBee (sans fil, sécurisé, sûr, standardisé, faible coût, marchés...) en font un prétendant de choix pour résoudre ses problèmes d'automatisation.

Etat de l'art : *Smart Home Challenges and Approaches to Solve Them - Roland Eckl and Asa MacWilliams, 2009*

Ce papier est basé sur le développement de la domotique sans se focaliser sur ZigBee. Les auteurs font tout d'abord un état de l'art des technologies domotiques actuelles et notent les limites de ces équipements :

- Soit les applications sont **trop simples avec un rayon d'action trop limité**.
- Soit les applications sont **trop complexes et trop dures à utiliser** qui vont entrainer l'abandon de la technologie par l'utilisateur.
- Soit les applications sont **trop intelligentes** et essayent d'en savoir plus que l'utilisateur.

Suite à cet état de l'art, ils proposent dans ce papier six approches pour résoudre ces problèmes :

1. Centraliser l'application pour faciliter le développement des modules et avoir un accès à l'internet, par exemple pour les modifications à distance.

2. Disposer d'interfaces ouvertes au niveau réseau et logiciels pour fournir plus d'interopérabilité envers les équipements.

3. Avoir une réponse instantanée lors d'un choix de l'utilisateur. Typiquement, l'utilisateur ne doit pas avoir à attendre une seule seconde lors de l'extinction d'une ampoule.

4. Invoquer des scénarios avec un contexte. Par exemple "‘ diner ", " coucher ", " travail " pour faciliter la mise en place et synchronisation de tous les équipements à telle ou telle moment de la journée.

5. Séparer les équipements de contrôle avec leurs différentes possibilités et modalités, en fonction de l'expérience de l'utilisateur et des besoins à couvrir.

6. Trouver un ou plusieurs business qui aurait besoin de nos solutions et s'adapter parfaitement à celui-ci.

Ces 6 points semblent très pertinents pour créer une réelle interaction entre l'utilisateur et la domotique. Ces points serviront de base pour le développement de notre application car , les utilisateurs vont rechercher la simplicité et la modernité du sans fil et de la domotique, faire confiance à la sécurité mis en place, apprécier le fait que l'énergie utilisée soit faible, etc...

L'économie d'énergie

Contexte actuel

Le fait que ZigBee soit un protocole utilisant très peu d'énergie et basé sur la domotique nous a poussé à faire une étude sur les réelles dépenses énergétiques actuelles en France. Le rapport Technologie de l'Information et Communication (TIC) et Développement durable (décembre 2008) du ministère de l'Ecologie, de l'Energie, du Développement Durable et de l'Aménagement du Territoire, témoigne du trop haut taux d'utilisation de l'électricité en France. Nous pourrons extrapoler ces résultats pour les pays développés économiquement voisins de La France.

Celui-ci nous montre qu'au cours des dernières années, la consommation électrique des appareils dédiés à l'audio-visuel a doublé en à peine dix ans et que l'informatique est apparu pour atteindre déjà une consommation plus que significative (un peu moins de 500kWh/an).

La majeure partie de la dépense énergétique des foyers s'ordonne comme suit :

1. Les PC et écrans.
2. Les serveurs et les moyens de télécommunications.
3. Les imprimantes.

Dans le même temps les autres équipements de la maison ont vu leur consommation se stabiliser ou se réduire légèrement comme, par exemple, la consommation des équipements de réfrigération qui a été diminuée de moitié. On en vient à se poser la question suivante : " comment faire pour arrêter cette augmentation sachant que l'informatique est en pleine expansion depuis des années ?"

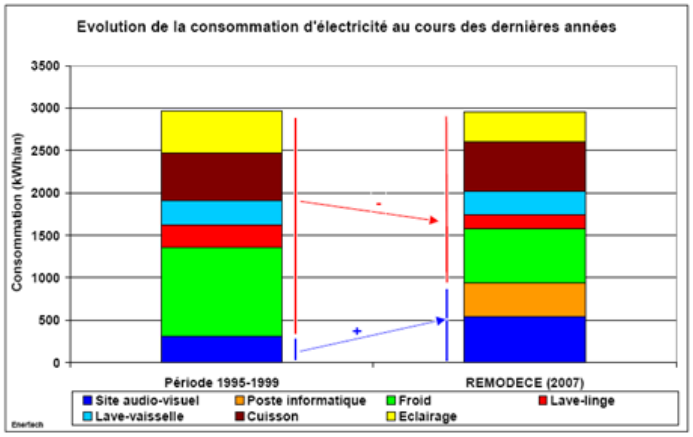

FIGURE 23. Evolution de la consommation électrique

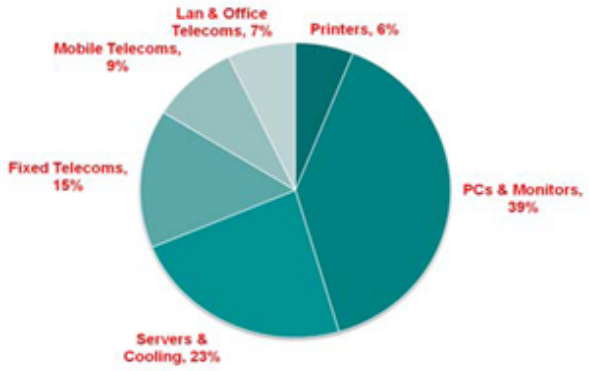

FIGURE 24. Répartition de la consommation électrique

De plus, ce rapport apporte des précisions sur l'importante évolution des systèmes de veille : " Il convient de souligner la consommation de plus en plus significative des systèmes de veille dans la consommation totale : 200 à 500 kWh/an/ménage soit environ 5 à 10 TWh, soit encore 10% de la consommation d'électricité spécifique et l'équivalent d'une à deux tranches nucléaires. Or ces dispositifs concernent principalement les matériels informatiques et audiovisuels : un démodulateur fonctionne en moyenne 13h/jour contre 6h pour une télévision, un magnétoscope est 90% du temps en veille... ".

Enfin il est important de noter que tout équipement branché consomme de l'énergie et ce, même s'il est éteint. Certains équipements consomment ont quasiment la même consommation d'énergie éteints qu'allumés.

D'après ce rapport, on voit qu'il est important de faire un progrès dans ce domaine. Il nous est venu l'idée d'orienter notre projet dans ce domaine de l'écologie afin de résoudre ces problèmes dans le futur.

Etat de l'art

Durant toutes nos recherches concernant la domotique et l'économie d'énergie, nous avons trouvé plusieurs systèmes permettant de contrôler nos dépenses d'énergie. Le premier est un outil proposé par Google pour suivre ses dépenses énergétiques. Le second, quant à lui, est une branche de la ZigBee Alliance nommée ZigBee Smart Energy qui propose des produits permettant la gestion de l'énergie et certifiés ZigBee. Les deux derniers systèmes n'entrent pas dans la cadre de la domotique mais sont des solutions existantes de mise hors tension automatique.

Google Power Meter

Google Power Meter est un outil gratuit de suivi de consommation énergétique dans un but d'économie d'énergie, d'économie financière ainsi que de protection d'environnement. Ce logiciel permet de suivre les graphiques de consommation électrique d'un habitat à chaque instant. Ceux-ci permettent de retourner les résultats par jour, semaine et mois. On peut ainsi voir les pics de consommation et essayer de les résoudre. De plus Google Power Meter fournit une prédiction du coût de la facture électrique et de la comparer au budget que l'on souhaite allouer aux dépenses énergétiques.

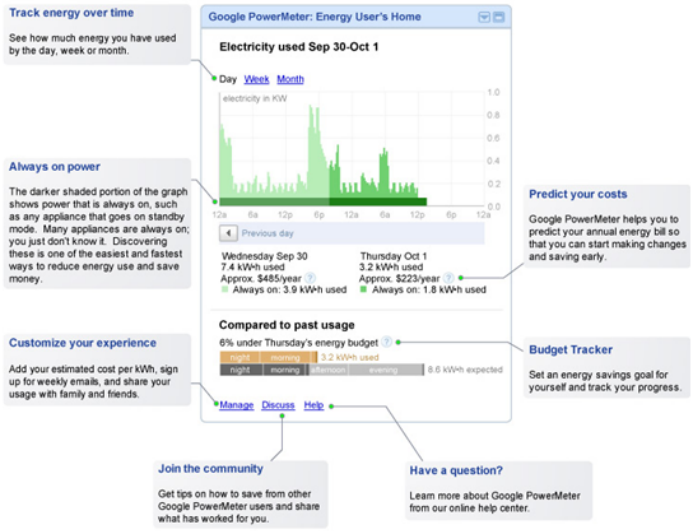

FIGURE 25. Graphique et statistiques de Google Power Meter

Ce logiciel a pour but d'aider le client à visualiser concrètement ses consommations électriques et lui faire prendre conscience de la dépense énergétique pour qu'il fasse son possible pour la réduire. Dans cette optique, les baisses de consommations électriques vont aider à construire un futur avec des énergies plus écologiques.

Le protocole ZigBee, est axé sur une utilisation réduite de l'énergie. En effet un noeud ZigBee est prévu pour fonctionner plusieurs années avec une batterie. On pourrait donc envisager de réduire des consommations excessives grâce des objets ZigBee, ou alors utiliser cette technologie dans un but de centraliser aussi les données et permettre à l'utilisateur d'agir dans un but écologique.

ZigBee Smart Energy

La branche ZigBee Smart Energy permet l'utilisation de la technologie ZigBee dans le cadre de l'écologie avec la gestion de l'énergie. ZigBee Smart Energy s'adresse aux compagnies d'énergies, fournisseurs de services énergétiques et à leurs clients afin de pouvoir communiquer directement avec des thermostats et autres appareils intelligents.

Ces différents appareils offrent plusieurs possibilités telles que :

- Des capteurs permettant l'affichage de la consommation moyenne énergétique d'une habitation avec l'affichage du prix équivalent. Ex : Aztech's In-Home Display d'Aztech
- Des contrôleurs de charge qui permettent de contrôler des pompes de piscines et autres charges de forte puissance. Ils peuvent aussi mesurer la consommation en énergie via un compteur d'énergie intégré. Ex : ZBMLC30-SE de SimpleHomeNet
- Des capteurs qui agissent comme un routeur maillé qui permettent d'étendre la portée d'un réseau. Ex : ZOE-RE de SimpleHomeNet
- Des capteurs qui permettent l'affichage de la consommation d'électricité et de gaz. Ex : Customer Information Panel de PRI
- Des Modules pour les compteurs de chaleur, de refroidissement, et d'eau Ex : ZigBee for MULTICAL de Kamstrup

FIGURE 26. Exemples d'appareils ZigBee Smart Energy

Coupe-veille informatique

FIGURE 27. Système de mise hors tension pour installation informatique

Cet outil détecte la mise en veille ou la mise hors tension du produit maître tel qu'un ordinateur et coupe automatiquement l'alimentation des périphériques reliés. Il permet de brancher jusqu'à 6 appareils : 1 équipement central (ordinateur), 4 périphériques et 1 appareil nécessitant d'être alimenté en permanence (téléphone, modem).

Coupe-veille multimédia

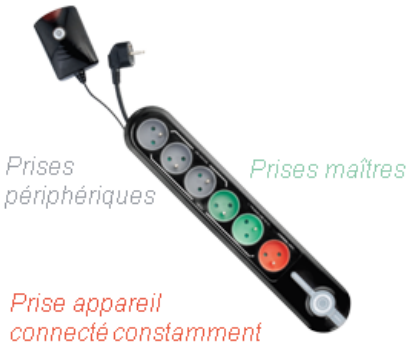

FIGURE 28. Système de mise hors tension pour installation informatique ou audio-vidéo

Cet outil détecte la mise en veille ou la mise hors tension de l'appareil connecté à l'une des 2 prises maître (TV, Home cinéma, ordinateur). Il coupe alors automatiquement l'alimentation des équipements reliés aux prises contrôlées et aux prises maîtres. Il permet de brancher jusqu'à 6 appareils : 2 équipements centraux (Home cinéma, TV, ordinateur...) sur les 2 prises maîtres, 3 périphériques sur les 3 prises contrôlées et 1 appareil nécessitant d'être alimenté en permanence (décodeur, box, fax) sur la prise d'alimentation permanente.

Ces systèmes orientés vers les installations informatiques et audio-vidéo, nous offrent de bonnes possibilités concernant la conception et la programmation d'un système écologique utilisé dans le cadre de la domotique et fonctionnant pour type d'appareil branché.

3.2 Vision globale du projet

Présentation de ZigBeecolo

Spécifications

Il fallait garder à l'esprit que nous devions utiliser la technologie sans fil ZigBee. Il fallait assimiler toutes les caractéristiques de ce réseau afin de développer un projet où nous pourrions tirer le meilleur de cette technologie.

Développer quelque chose dans la domotique nous paraissait indispensable. C'est un point très intéressant et nous sommes sûrs que l'étendue de ZigBee dans ce domaine peut être immense. De plus, l'idée de développer une application écologique dans un contexte d'économie d'énergie, d'automatisation et de contrôle à distance nous paraissait une nécessité.

Pour cela nous avons réfléchi à de nombreuses situations de la vie quotidienne où nous pouvions constater les pertes énergétiques d'un foyer. Nous avons donc construit un scénario d'une journée type d'un étudiant en informatique et nous avons trouvé des points faibles qui nous serviraient de base pour le développement de notre projet.

Le scénario est le suivant :

> *Monsieur Dupond est un jeune informaticien et vit dans un appartement en France.*
>
> *Comme la majorité des étudiants, et des jeunes en règles général, il est en possession de plusieurs équipements électroménagers, télévision, poste informatique, téléphone portable, etc...*
>
> *Lorsque cet étudiant n'est pas chez lui ou lorsqu'il dort, par exemple, il n'a aucun besoin de dépenser du courant (mise à part pour quelques cas particuliers comme le frigidaire, le téléphone-répondeur, etc...). Et pourtant : son radio- réveil, son micro-onde, son magnétoscope et sa chaîne hifi lui donneront toujours l'heure, et dépenseront donc du courant.*
>
> *De plus, sa cafetière ne fonctionne pas, tout comme son chargeur de mobile et son ordinateur, mais ils sont branchés sur secteur et donc ils consomment inutilement.*

D'après ce scénario, il nous est venu l'idée de créer des prises qui s'intercaleraient entre l'équipement et la prise secteur, permettant d'arrêter complètement le courant grâce à des appareils de contrôle à distance. Bien entendu ces prises seraient des équipements finaux utilisants la technologie ZigBee, la consommation ne serait donc pas nulle mais très faible. Tous ces éléments seraient régis par un coordinateur central.

Les différents points autour desquels notre application sera développée nous ont été inspirés par l'article d'Eckl et MacWilliams et sont les suivants :

- Centralisation des données sur un équipement spécifique (coordinateur central) et si possible permettre à cet équipement d'aller sur Internet et de transmettre des données, d'avoir des rapports de consommation électrique ou encore d'avoir un control à distance.
- Une automatisation possible avec par exemple la désactivation de la prise lorsqu'un portable est chargé, l'utilisation du lave-linge est achevée ou plus généralement après une longue période (préalablement déterminée) d'inactivité.
- Un arrêt manuel des prises (choix des différents appareils à gérer) avec un outil de contrôle à distance.
- L'introduction de différents modes de fonctionnement comme le mode *Sommeil* où tous les équipements mise à part le radio réveil seraient arrêtés, *Longue absence* où tout serait arrêté, ou le fait de désactiver certaines pièces avec encore la possibilité de créer des modes personnalisables.
- L'introduction d'une alarme en cas de trop forte consommation électrique et prévoir pourquoi pas l'arrêt de certains appareil avant que l'ensemble de l'installation disjoncte.
- La détection du mode *Veille* des appareils afin d'arrêter complètement la venue du courant.

Démarches effectuées

Au début de nos recherches et découvertes de l'architecture ZigBee, nous imaginions que le réseau allait ressembler au schéma suivant :

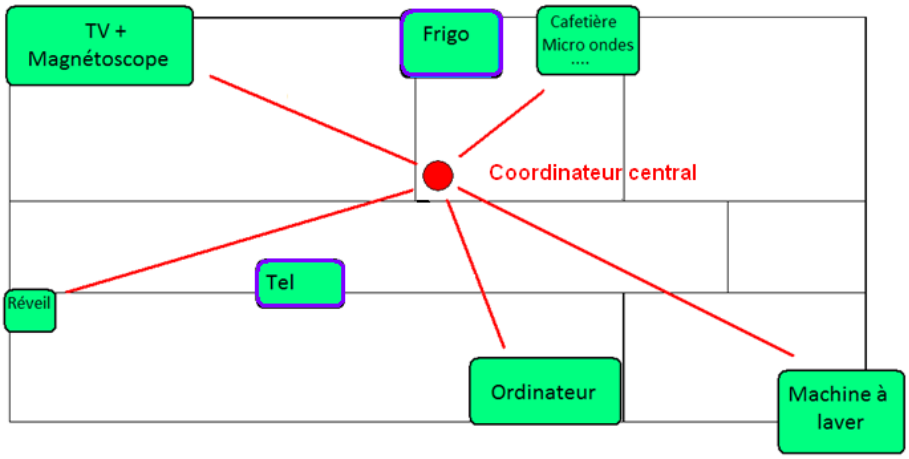

FIGURE 29. Schéma simplifié du réseau

Dans ce schéma, les appareils entourés de violet (Frigidaire et Téléphone) ne dispose pas d'équipement ZigBee leur permettant de gérer le courant. En effet, ces appareils ont un besoin constant de courant et leur mise hors tension sera fait de manière manuelle de la part de l'utilisateur pour éviter tout problème lié à la mise hors tension de ceux-ci. En ce qui concerne les autres appareils, ils disposent tous d'une connexion sans fil au coordinateur central.

De plus, le réseau utilisé est un réseau maillé, d'où, si les dispositifs terminaux sont trop éloignés du concentrateur, il est possible d'ajouter des routeurs ou de laisser le soin à certains dispositifs terminaux d'agir comme tel. Certains des dispositifs proposés par ZigBee joue un double rôle. L'un pour fonctionner comme dispositif terminal et l'autre pour servir de routeur. De cette manière, tous les appareils pourront être synchronisés au coordinateur central directement ou indirectement.

D'après ces schémas simplifiés, le réseau devrait fonctionner comme suit :

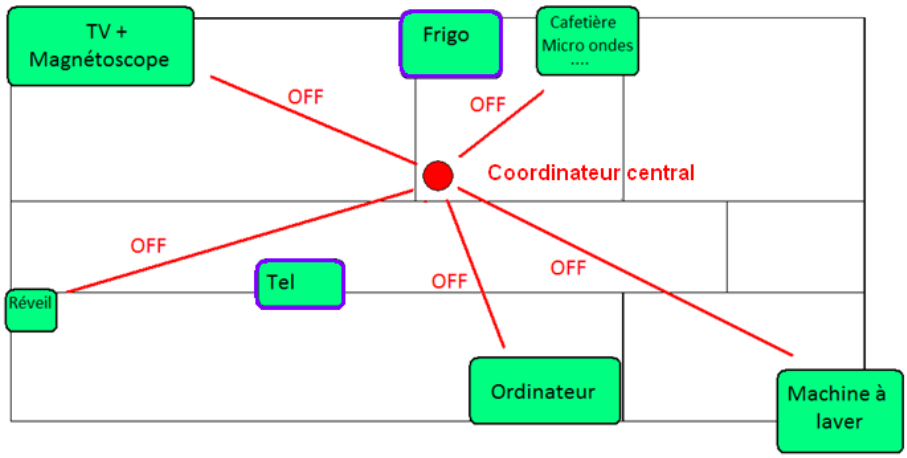

FIGURE 30. Schéma simplifié de l'extinction des appareils

Dans cette configuration, sur les ordres de l'utilisateur, le coordinateur envoie un signal d'extinction à toutes les prises permettant de couper la perte de courant.

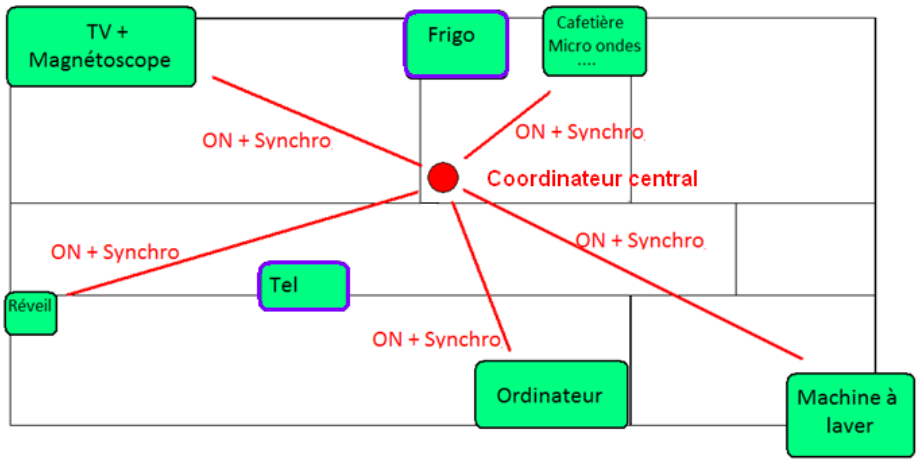

FIGURE 31. Schéma simplifié de synchronisation des appareils

Dans cette configuration, sur les ordres de l'utilisateur, le coordinateur envoie un signal de démarrage à toutes les prises permettant d'allumer les appareils et leur syn-

chronisation avec le coordinateur central (pour gérer un affichage correct de l'heure par exemple).

Partant de ce principe, nous avons effectué plusieurs recherches pour trouver des dispositifs modulables et reprogrammables (ainsi que le logiciel et l'API) pour permettre ce genre d'innovation.

Première recherche

Tout d'abord, nous avons découvert qu'il existait plusieurs APIs disponibles pour développer des applications ZigBee. La lecture d'une partie du livre *"ZigBee Wireless Networking"* de Drew Gislason, nous a permis de découvrir qu'il n'existe pas d'API standard pour un protocole ZigBee. ZigBee nécessite une seule chose : la correction du comportement des ondes telles que les ondes Wifi et toutes les autres améliorations sont effectuées par l'éditeur.

Dans ce contexte, l'API utilisé dépend de la pile du vendeur. En effet, chaque vendeur offre les fonctionnalités standards de ZigBee. Cependant, chaque éditeur peut ajouter différentes optimisations et fonctionnalités en fonction de ses besoins. Un produit certifié ZigBee signifie que, peu importe l'API utilisée ou l'éditeur choisi pour chaque composant, le réseau fonctionnera parfaitement. Ainsi, ZigBee possède une liste de plate-forme attestée ZigBee dont 4 principaux éditeurs se distinguent :

- **Texas Instruments** utilise l'USB pour la connexion du PC au kit de développement. Offre 2 types d'interfaces : une complète et une simple.
- **Ember** offre un concept d'améliorations des fonctionnalités existantes. Il utilise Ethernet pour la connexion du PC au kit de développement et les prix sont généralement plus élevés que les concurrents.
- **Integration Associates** utilise l'USB pour la connexion du PC au kit de développement. Il utilise la norme 802.15.4 et place directement la MAC dans le matériel pour accélérer certains processus tel que le chiffrement et le déchiffrement.
- **Freescale** est l'éditeur préféré de l'auteur. Il offre un outil de configuration qui rend la construction des réseaux plus faciles. Il offre une gamme de protocoles pour les réseaux ZigBee ainsi que d'autres qui peuvent s'incorporer avec un réseau ZigBee.

Après avoir pris connaissances des différentes possibilités des 4 plus grands éditeurs certifiés ZigBee, nous avons opté pour une pile Texas Instruments qui nous paraissait être un compromis idéal en terme de prix et de possibilités de programmation avec les deux différentes interfaces.

Deuxième recherche

Tout d'abord, nous nous sommes orientés vers les produits vendus par Texas Instruments. Pour commencer, nous avons eu beaucoup de mal à comprendre les différences entre les différents kits proposés. Dans un premier temps, nous nous sommes concentrés sur la partie logicielle nous permettant de reprogrammer les futurs composants de notre

réseau. Ainsi, nous avons trouvé le CCDEBUGGER 2530 et le module IAR EW8051. Après plusieurs recherches, nous avons constaté que ces produits pourraient s'intégrer parfaitement au développement envisagé. Il ne nous restait plus qu'à trouver les composants de notre réseau.

Par la suite, nous avons donc étudié différents produits compatibles avec cette interface logicielle et notamment les produits vendus par Cleosys, une société française, et dont la pile utilisée était celle de Texas Instruments. Cette société proposait un kit de développement contenant un coordinateur central, une télécommande, une prise ainsi que le logiciel permettant de reprogrammer les appareils comme souhaité. Ce kit était idéal pour l'usage souhaité aussi bien en terme de possibilités de reprogrammation que de prix. Il n'était donc plus utile de disposer du CCDEBUGGER ainsi que du module IAR étant donné que le kit offert par cette société nous apportait tout ce dont nous avions besoin.

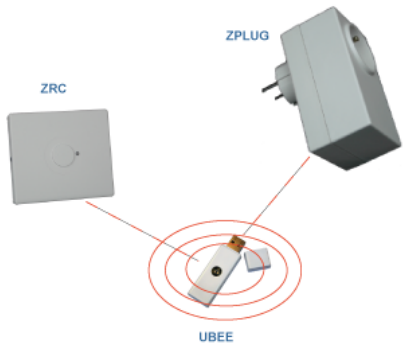

FIGURE 32. Composants utilisés pour le développement de notre application

De par ce fait, le schéma de notre réseau serait comme suit :

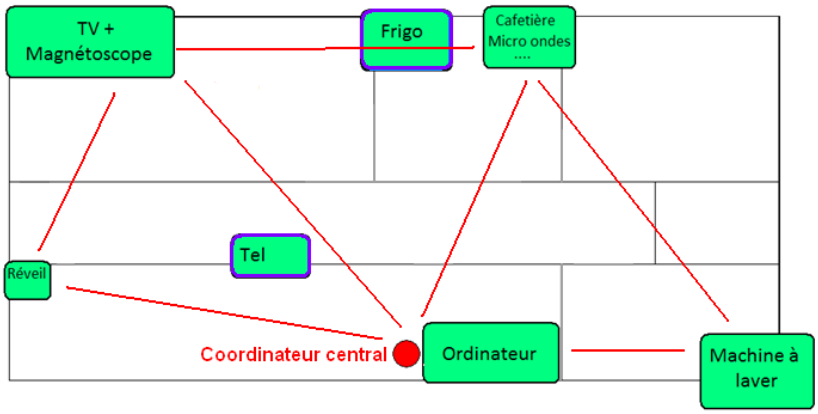

FIGURE 33. Schéma simplifié du réseau maillé en fonction des composants utilisés

La seule différence notable, ce situe au niveau du coordinateur central. En effet, avec ce kit de développement, le coordinateur se trouve directement connecté à l'ordinateur ce qui peut augmenter les distances avec d'autres composants mais qui ne pose aucun problème grâce à l'utilisation du réseau maillé.

Dans le cadre du développement de ce projet, nous appliquons l'utilisation de la technologie ZigBee à une chambre étudiante comme présente dans la plupart des campus universitaire. Ce contexte reprend donc les différents équipements que possède un étudiant. Comme présenté sur le schéma, le coordinateur sera connecté à l'ordinateur, la prise s'intercalera entre la prise murale et l'alimentation d'un équipement (dans notre cas, nous utiliserons un réveil pour la synchronisation des données ainsi qu'un chargeur de téléphone pour contrôler la coupure du courant au moment opportun). Pour finir, la télécommande se chargera d'envoyer des informations d'extinction, de démarrage ou tout autre fonctionnement imaginable sur ordre de l'utilisateur.

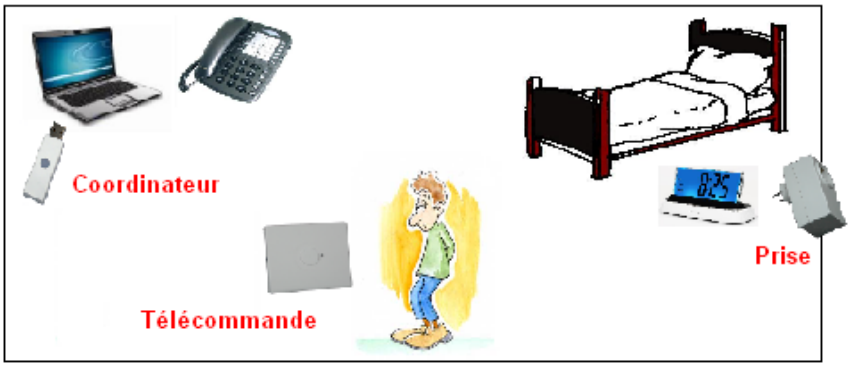

FIGURE 34. Schéma simplifié du réseau appliqué à notre contexte

Design réseau

Spécifications

Pour le développement de notre projet, nous avons donc établi une convention pour le réseau. Etant donné que ZigBee nous donne de nombreuses possibilités nous nous devions de les exploiter. De plus, ZigBee étant étroitement lié à la domotique, le choix de la spécification du type de réseau nous sera donné par ZigBee.

Un réseau ZigBee demande la présence d'un coordinateur. Ce coordinateur est le point ou toutes les données vont converger. Dans notre projet, il s'agira d'un ordinateur avec la clé USB UBee. Généralement, c'est ce coordinateur qui est aussi le Centre de Confiance. Nous allons donc utilisé ce principe de base qui nous permettra de gérer l'intégralité du réseau via ce coordinateur.

Comme nous l'avons vu auparavant, ZigBee met en place un réseau de type maillé. Ce réseau est très pratique étant donné que les routeurs permettent de créer des liens entre eux pour étendre les capacités du réseau. Ainsi ce type de réseau nous permettra donc d'avoir un coordinateur portatif dans tout le réseau. Comme nous l'avons vu plus tôt avec la figure 7, on constate que les connexions se feraient toute seules entre les différents équipements, si elles perdaient le lien direct avec le coordinateur. Ce réseau est beaucoup plus modulable étant donné que les prises ZPlug que nous utilisons sont des routeurs (donc des FFD). Ainsi chaque prise pourra communiquer avec le coordinateur même si elle n'est pas dans son secteur et qu'elle n'y a pas un accès direct, sous condition que les routeurs soient assez proches les uns des autres.

Sécurité du réseau

La domotique en générale et donc ZigBeecolo ne doivent pas être soumis à des problèmes en matière de sécurité. Il est très facilement compréhensible qu'on ne doit pas pouvoir compromettre le moindre équipement d'un système de domotique et donc du réseau. Pour cela, nous mettrons en place un principe de sécurité visant à assurer un fort niveau sécurité.

Etant donné que les spécifications ZigBee proposent deux niveau de sécurité, notre choix se tournera tout simplement vers le niveau le plus sécurisé. Le mode commercial sera alors activé. Ainsi le réseau sera activement surveillé, les ajouts seront contrôlés, les authentifications mutuelles seront effectives et les "network key" seront régulièrement mis à jour.

Les nouveaux équipements (prises ou télécommandes) étants des équipements plus ou moins fixes, leurs ajouts au réseau seront réalisés le plus manuellement possible, par un responsable. Ce responsable établira une clé commune entre la prise à ajouter et le Centre de Confiance, pour que l'authentification soit réalisée de manière sécurisée. Ainsi le scénario décrit dans la partie *Rejoindre un réseau ZigBee* sera mise en oeuvre. Le centre de confiance établira donc les différentes clés et pourra mettre à jour cette "link key" avec la technique d'établissement SKKE.

Les messages au niveau 2, 3 et 4 seront donc tous cryptés avec AES et sa clé de 128 bits et le MIC sera apposé à chaque couche. Le niveau de sécurité maximal étant le AES-CCM-128 ce qui signifie que le MIC sera long de 128 bits également. Ainsi l'intégrité et la confidentialité sera entièrement assuré. Si chaque couche appose son niveau de sécurité, alors un attaquant aura d'autant plus de mal à attaquer le système. De plus, les messages échangés entre le coordinateur et les prises ne devraient pas être trop volumineux, voilà pourquoi le temps de latence ne devrait pas être trop long entre le moment où l'on choisit d'arrêter les prises et où les prises sont vraiment désactivées.

Nous pourrons noter que toutes ces suppositions ne sont que théoriques. En effet, si nous remarquons que le système est beaucoup trop ralenti, du fait des multiples cryptages et tests ou encore que les clés sont trop souvent réactualisées, alors nous pondérerons nos résultats et nous serons plus laxistes sur la sécurité du système.

Design applicatif

Spécifications

Avoir un réseau ZigBee ne suffira pas pour faire fonctionner notre projet. Les utilisateurs devront être conscients du système de domotique mis en place, être au courant des modifications apportées, interagir avec le système, pouvoir gérer le réseau ou simplement visualiser certaines données. Pour cela, seul le niveau applicatif, sera l'interface homme machine.

Comme nous l'avons vu plus tôt, nous seront en présence d'une clé USB branchée sur un ordinateur. Nous avons donc eu l'idée d'une application interagissant avec cet clé. Nous avions pensé avoir un menu qui permettrait de choisir entre plusieurs actions :

- consulter le plan avec les équipements et fonctionnements en place
- changer les différents modes : "Sommeil", "Longue absence", "Désactiver", etc...
- afficher les rapports de consommations électriques
- changer les paramètres : "Date et Heures", "Luminosité/Contraste", "Changer les accès et mots de passe", etc...
- gérer le réseau : "Ajouter/Supprimer équipement", "Changer le réseau", etc...

Encore une fois dans cette partie nous allons émettre un bémol. N'ayant point reçu les équipements et n'ayant pu développer une quelconque application, il ne s'agit ici que d'idées et de suppositions qui nous paraissaient pertinentes. Nous ne savions pas le temps que mettrait ces différents points pour se développer, et quelles entraves pourrions nous rencontrer.

De plus, nous avons eu l'idée d'introduire un mode veille/extinction pour l'application, ce qui serait aussi un bon point sachant que notre but est de réduire les consommations électriques. Cependant nous sommes aujourd'hui en présence d'une clé USB et d'un ordinateur ce qui n'est pas le plus économique en matière d'économie d'énergie. Si cette idée se développe à l'avenir, ce serait intéressant d'avoir un petit moniteur émetteur/récepteur alimenté en guise de coordinateur qui ne consomme pas trop d'énergie. Celui-ci pourrait être facilement mis en veille ou arrêté en cas de non utilisation, et beaucoup plus ergonomique.

Sécurité de l'application

Prévoir une bonne application est une bonne chose mais encore une fois, il ne faut pas négliger le côté sécurité. L'interface avec l'utilisateur sera un point faible pour le réseau complet.

Un mot de passe administrateur devra être mis en place sur le coordinateur, qui est aussi le Centre de Confiance, afin de ne pas permettre à n'importe qui d'accéder à ce coordinateur. C'est le point central du réseau et de la sécurité de ZigBee. Alors si un pirate aurait accès à ce Centre de Confiance, il pourrait accepter n'importe quel équipement, compromettre le réseau, supprimer toute sécurité, etc...

Nous voulons aussi garantir le bon fonctionnement du réseau en mettant des restrictions entre les différents utilisateurs. On ne sait pas qui et où notre projet sera utilisé. Un utilisateur quelconque ne doit pas pouvoir accéder à certaines modifications, pouvoir accéder au relevé des consommations électriques, pouvoir tout désactiver dans le bâtiment complet, etc... Nous prévoyions la mise en place de comptes utilisateurs avec mots de passe.

4 Conclusion

4.1 ZigBee, une technologie d'avenir

ZigBee est une technologie modulable qui permet la construction d'un réseau via la technologie sans-fil. Contrairement à certaines normes comme le Bluetooth ou le Wifi, elle est à très faible consommation d'énergie. Elle est parfaitement adaptée à la domotique, et offre un confort à l'utilisateur, en effet le fait d'utiliser un coordinateur central et un réseau maillé lui permet de tout commander via un seul appareil sans s'occuper de l'emplacement des divers équipements.

Les spécifications ZigBee offrent un niveau de sécurité complet à chaque couche. Nous avons noté la présence d'un module de sécurité directement implémenté dans les couches NWK et APL, de plusieurs modes de sécurité, de cryptographie, d'authentification, etc...

4.2 Bilan personnel

Après plusieurs mois de travail, le résultat obtenu nous satisfait cependant malgré le fait de ne pas avoir pu pratiquer toute la théorie étudiée et envisagée. Nous avions l'envie de développer un projet autour de cette technologie, qui aurait pu être implémenté et testé dans un cas concret d'application. Enfin le fait de pouvoir utiliser ces équipements auraient pu être une plus-value dans notre cursus.

En effet, d'un point de vue recherche, ce sujet nous a permis de progresser avec notamment l'étude de documents scientifiques et de technologies. Elle nous a permis aussi de développer un oeil critique sur un domaine vaste comprenant la domotique, l'écologie, le sans-fil et la sécurité. Ce sujet nous a permis de faire naitre, d'étudier et d'amener à maturité un sujet de développement qui nous était cher.

4.3 Perspectives futures

Ce projet, décrit dans ces quelques pages, n'est donc qu'une esquisse de ce que pourrait être la domotique écologique et économique. A ce stade, une étude assez riche a été réalisée, mais il reste un très gros travail par la suite avec toute la conception de l'application, de la phase de test en matière de sécurité et d'économie, de l'extensibilité pour que ce projet se développe et ait la chance de résoudre le gaspillage électrique à venir.

5 Références

1. ZigBee Specification - ZigBee Alliance (2008)
2. ZigBee Overview - ZigBee Alliance (2009)
3. ZigBee Security - ZigBee Alliance (2009)
4. ZigBee Wireless Networking - Drew Gislason (2008)
5. IEEE Standard for Information technology : Telecommunications and information exchange between systems : Local and metropolitan area networks : Specific requirements : Part 15.4 : Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) - IEEE Computer Society (2006)
6. Technologie de l'Information et Communication (TIC) et Développement durable - Ministère de l'Ecologie, de l'Energie, du Développement Durable et de l'Aménagement du Territoire (2008)
7. Smart Home Challenges and Approaches to Solve Them - Roland Eckl, Asa MacWilliams (2009)
8. Une méthode d'accès totalement déterministe pour un réseau personnel sans fil - Adrien Van Den Bossche (2007)
9. Towards security issues in ZigBee architecture - Pavel Ocenasek (2009)
10. An Identity-Based Auth Protocol for Clustered Zigbee Network - Wei Chen, Xiaoshuan Zhang, Dong Tian, Zetian Fu (2010)
11. ZigBee-2007 Security Essentials - Ender Yüksel, Hanne Riis Nielson, Flemming Nielson (2008)
12. Key Exchange in 802.15.4 Networks and Its Performance Implications - Moazzam Khan, Fereshteh Amini, Jelena $Mišić$ (2006)
13. Google PowerMeter : http ://www.google.com/powermeter (2010)
14. E-boutique EDF : http ://www.eboutiqueedf.com/ (2010)