Technologie ZigBee / 802.15.4
Protocoles, topologies et domaines d'application

par **Thierry VAL**
Professeur des universités.
Université de Toulouse ; UTM ; LATTIS IUT de Blagnac

Eric CAMPO
Université de Toulouse ; UTM ; LATTIS IUT de Blagnac

et **Adrien VAN DEN BOSSCHE**
Post-doctorant.
Université de Toulouse ; UTM ; LATTIS IUT de Blagnac

Après l'arrivée sur le marché depuis quelques années des réseaux locaux sans fil WiFi et Bluetooth, une nouvelle technologie semble, elle aussi, promise à un bel avenir commercial, aussi bien pour des applications grand public telles que celles liées à la domotique, que pour des domaines plus liés aux communications sans fil en milieu industriel : il s'agit du réseau ZigBee. Ce réseau personnel sans fil ou Wireless Personal Area Network (WPAN) se démarque de ses deux principaux concurrents précédemment cités par sa ***simplicité d'implémentation*** *et par* ***ses modes de faible consommation énergétique****. La technologie ZigBee, associée à la norme IEEE 802.15.4, propose une pile protocolaire légère, déclinable sous plusieurs versions en fonction des besoins et de la topologie souhaitée, pour des objectifs de transferts de données à faibles débits et de faibles taux d'utilisation du médium.*

Tableau des sigles	
Abréviation	**Définition**
AODV	Ad hoc On demand Distance Vector
APL	Application Support Layer
APS	Application Support Sub-Layer
BO	Beacon Order
CAP	Contention Access Period
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CFP	Contention Free Period
CRC	Code de Redondance Cyclique
FFD	Full Function Device
GTS	Guaranted Time Slot
LIFS	Long Inter-Frame Spacing
LLC	Logical Link Control
MAC	Medium Access Control
MFR	MAC FootR
MHR	MAC HeadeR
MSDU	MAC Service Data Unit
OSI	Open Systems Interconnection
PAN	Personal Area Network
RFD	Reduced Function Device
RTS/CTS	Ready To Send / Clear To Send
SDP	Service Discovery Protocol
SIFS	Short Inter-Frame Spacing
SO	Superframe Order
SSP	Security Service Provider
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
ZC	ZigBee Coordinator
ZDO	ZigBee Device Object
ZED	ZigBee End Device
ZR	ZigBee Router

1. Présentation générale

1.1 Le projet ZigBee

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. Après une soumission à l'IEEE mi-2001, la ZigBee Alliance [13] a été créée pour développer et promouvoir la norme IEEE 802.15.4 ratifiée en mai 2003. La production de modules compatibles fut alors prévue et les premiers produits (puces radio, piles protocolaires, modules intégrés, kits de développement, etc.) sont apparus ; ils sont disponibles depuis début 2005.

Le protocole ZigBee s'appuie sur ce standard IEEE 802.15.4 [9] [2] pour les couches physique et liaison (cf. paragraphe 2.1), qui sont les couches 1 et 2 du modèle OSI ainsi que sur le développement des couches réseau et applicative par la ZigBee Alliance.

1.2 Objectifs et domaines d'application

ZigBee est un LP-WPAN (*Low Power – Wireless Personal Area Network*) : c'est un réseau sans fil à bas débit et 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** (maximum 250 kbits/s). La différence entre ZigBee et la plupart des autres réseaux locaux et personnels sans fil (WiFi, Bluetooth) se situe au niveau de l'utilisation du médium hertzien : **ZigBee est optimisé pour une faible utilisation du médium partagé par tous**, par exemple 0,1 % du temps [14]. Typiquement, un module ZigBee occupera le médium 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. 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 peuvent dès lors être alimentées pendant plusieurs mois par des piles classiques.

1.3 Consommation énergétique

Le point fort de ZigBee est en effet 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 (100 µW) tout en permettant de passer en mode opérationnel en très peu de temps (300 µs, cf. tableau **1**), 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 à son 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 autre réseau sans fil classique, à puissance d'émission équivalente !

À titre d'**exemple**, la consommation énergétique d'un modem ZigBee type fabriqué par Freescale [4] est donnée dans le tableau **1**. Le modem considéré est le MC13192 [5] [6]. Notons que le mode de fonctionnement normal du module est le mode repos, et de ce fait, les temps de basculement sont donnés par rapport à cet état de référence. La consommation très faible dans le mode « somnolence » (de 40 µA), et le temps de basculement rapide (de seulement 332 µs) vers le mode « repos » sont des atouts indéniables de la technologie ZigBee (notés par des ☺ dans le tableau **1**).

Tableau 1 – Consommation typique d'un modem 802.15.4 avec temps de basculement entre chaque état (source Freescale)

Mode	Consommation	Temps vers « repos »
Off		23 ms
Hibernation	3 µA	18 ms
Somnolence	☺ 40 µA ☺	☺ 332 µs ☺
Repos	**1 mA**	
Émission	34 mA	144 µs
Réception	37 mA	144 µs

1.4 Implémentations

La technologie ZigBee prévoit deux types d'entités :
1. les entités complètes, ou FFD (*Full Function Device*) ;
2. les entités réduites, ou RFD (*Reduce Function Device*).

Les FFD implémentent la totalité de la spécification ZigBee alors que les RFD sont des entités allégées dans un objectif de moindre consommation énergétique et de moindre utilisation mémoire pour le microcontrôleur associé. Les entités RFD sont nécessairement des nœuds terminaux du réseau ; un tel nœud ne saura pas router un paquet sur le réseau. Typiquement, un capteur embarqué sera RFD et alimenté sur batteries, alors qu'une unité centrale de traitement, alimentée par une source non contrainte énergétiquement, sera FFD avec une fonction de coordination du réseau, comme nous le verrons dans le paragraphe suivant.

1.5 Topologies

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 (*Personal Area Network*). Ces deux topologies sont représentées dans les figures **1** et **2**. Au-dessus de 802.15.4, la couche réseau de ZigBee (cf. paragraphe 2.4) 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).

Topologie étoile

Dans la topologie étoile présentée en figure **1**, 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 [16] 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 à fortes capacités, secteur...) [10].

Topologie point à point

Dans la topologie point à point (*peer-to-peer*) présentée en figure **2**, un FFD peut communiquer directement avec tout autre FFD à la condition qu'ils soient 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 des adresses courtes (cf. paragraphe 1.6).

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 tree* (arborescence de cellules) ou les réseaux maillés *mesh*. Nous aborderons ces techniques plus loin dans cet article, dans la partie consacrée à la couche réseau (cf. paragraphe 2.4).

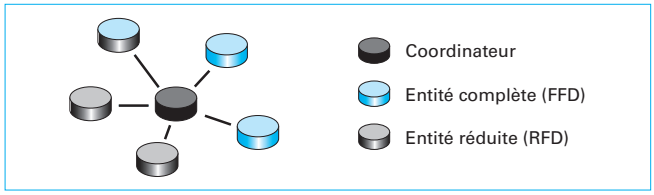

Figure 1 – Représentation de la topologie en étoile

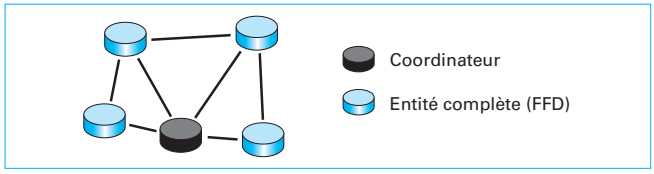

Figure 2 – Représentation de la topologie point à point

1.6 Adressage

Au niveau 802.15.4

Toute entité 802.15.4 possède une adresse unique appelée adresse MAC (*Medium Access Control*). À la différence de 802.3, une adresse MAC 802.15.4 est codée sur 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, à cause des débits de transmission, relativement faibles. L'adresse courte est attribuée par le coordinateur du PAN au moment de l'association au réseau.

Au niveau ZigBee

La norme 802.15.4 ne prévoit pas de règle pour le choix de ces adresses, cette tâche est laissée au libre arbitre des couches supérieures, en particulier à la couche 3 de ZigBee (cf. figure **3**). Nous verrons au paragraphe 2.4.2 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. En d'autres termes, il existe dans la couche 3 de ZigBee un mécanisme de configuration des adresses de niveau 2 !

1.7 Valeurs typiques

Pour conclure la présentation générale de ce WPAN, voici en résumé les valeurs typiques caractérisant IEEE 802.15.4 et ZigBee (certaines de ces valeurs ont été détaillées dans le tableau **1**) :

– Débit : 250 kbits/s sur le médium physique pour PHY2450 (cf. paragraphe 2.2).
– Puissance d'émission typique : entre 0 et 3 dBm.
– Portée radio : quelques centaines de mètres en espace libre.
– Consommation 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) :
  • inférieure à 20 ko pour une entité réduite (RFD),
  • entre 40 à 60 ko pour une pile complète (FFD).
– Nombre d'entités connectables au réseau :
  • 2^8 dans une étoile,
  • 2^{16} dans un PAN maillé,
  • 2^{64} adresses MAC disponibles.
– Accès au médium : pur CSMA/CA (sans RTS/CTS) ou organisé (mode balisé avec slots dédiés).
– Détection / correction d'erreurs : CRC 16 bits dans la trame MAC.

2. Étude protocolaire de ZigBee / 802.15.4

2.1 Une pile protocolaire en couches

La pile protocolaire ZigBee est représentée en figure **3**. On y retrouve le découpage classique en couches recommandé par l'OSI (*Open Systems Interconnection*). Nous détaillons par la suite les couches implémentées : PHY, LNK, NWK et APL.

2.2 La couche physique PHY de 802.15.4

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 868/915 MHz (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).

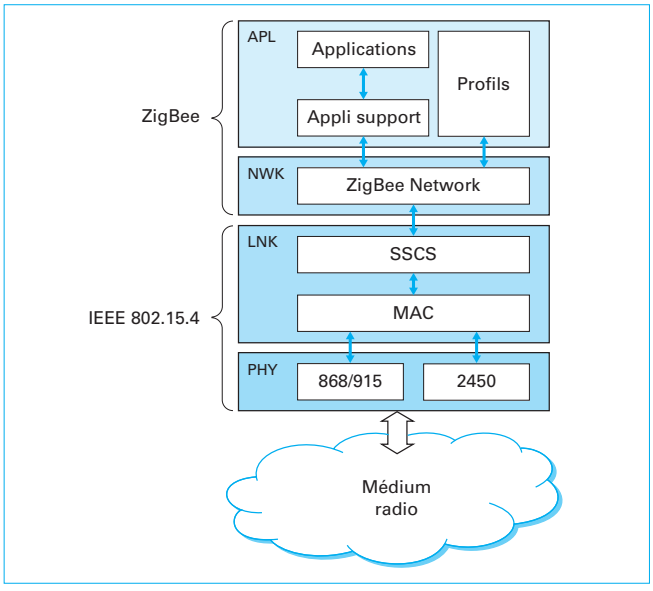

Figure 3 – La pile protocolaire 802.15.4 / ZigBee

Au total, 27 canaux (numérotés de 0 à 26) sont répartis sur ces trois bandes. Cette diversité en terme d'utilisation du spectre radiofréquence permet à la technologie de répondre aux nombreuses réglementations et d'être utilisable sur toutes les régions du globe mais aussi de s'adapter aux environnements pollués (fours à micro-onde, appareils RF, WiFi, Bluetooth...). Actuellement, les premiers produits disponibles utilisent majoritairement la bande PHY2450.

2.2.2 Modulations et étalement de spectre

Comme beaucoup d'autres technologies WLAN/WPAN, 802.15.4 met en œuvre une modulation à spectre étalé [17]. Une modulation utilisant une méthode unique d'étalement de spectre séquentiel (DSSS) permet d'améliorer l'immunité aux interférences et aux multi-trajets, en sacrifiant quelque peu les performances en terme de débit. De plus, grâce au codage réalisé par la séquence pseudo-aléatoire, aussi appelée *PN-codes*, qui permet de réaliser l'étalement, la confidentialité des échanges est améliorée. Cette technique ne garantit pas néanmoins des propriétés optimales de confidentialité et d'authentification ; une partie de la couche liaison effectuera cette tâche.

La couche PHY868/915 est relativement simple et basique : les symboles sont binaires, grâce à l'emploi d'une modulation BPSK et un débit peu élevé (20 kbits/s pour le 868 MHz, 40 kbits/s pour le 915 MHz). En revanche, la couche PHY2450 propose une modulation à codage orthogonal plus complexe, O-QPSK, qui permet une efficacité plus élevée et un débit plus intéressant.

2.2.3 Portée, puissance d'émission et sensibilité du récepteur

IEEE 802.15.4 prévoit une portée classique de quelques dizaines de mètres. La puissance maximale émise par un module 802.15.4 ou ZigBee n'est pas définie par la norme ; celle-ci est laissée d'une part à l'appréciation de l'autorité de régulation de la zone où est effectuée la transmission, et d'autre part au constructeur pour des questions évidentes d'autonomie énergétique du système dans lequel il est implanté. Néanmoins, la puissance typique recommandée est de 1 mW, soit 0 dBm et la sensibilité du récepteur doit être meilleure que – 85 dBm à 2,4 GHz (pour un taux d'erreur paquet meilleur que 1 %).

En pratique, un nœud ZigBee a une portée de quelques dizaines de mètres, jusqu'à une centaine de mètres en extérieur et sans obstacle. Notons que, de par la robustesse de la couche physique, les portées d'un *transceiver* 802.15.4 sont comparables à celle d'un *transceiver* 802.11, mais avec une puissance d'émission plus faible : à rapport signal sur bruit SNR égal, 802.15.4 dispose d'un taux d'erreur bit (BER) meilleur que les autres technologies sans fil proposées par l'IEEE.

Tableau 2 – Caractéristiques des couches physiques proposées par IEEE 802.15.4

PHY	Bande (MHz)	Nbre canaux (n°)	Région	Étalement 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	2 000	O-QPSK	250	62.5	16-ary orthogonal

Remarquons également que comme pour toutes les technologies de réseau sans fil, la portée effective d'un *transceiver* 802.15.4 est très liée à sa puissance d'émission. Certains modules sont dotés d'un étage amplificateur HF en sortie et/ou d'un amplificateur à faible bruit en entrée, ce qui permet d'étendre considérablement la portée radio.

À titre d'**exemple**, les modules XBeePro fabriqués par la société MaxStream [19] sont vendus pour une portée supérieure à 1 km en ligne de vue.

L'étendue d'un réseau ZigBee peut être largement supérieure à la portée effective de deux modules grâce à la topologie maillée (multi-sauts), comme nous le verrons plus loin. Enfin, comme c'est le cas dans tous les réseaux hertziens, la portée est largement conditionnée par la présence d'obstacles ou par la pollution du spectre radiofréquence. À ce titre, le coordinateur du réseau peut décider d'effectuer un changement de canal à titre exceptionnel si le taux d'erreur sur le réseau est trop important.

2.3 La couche liaison LNK de 802.15.4

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).

2.3.1 Format de trame

Le niveau liaison spécifié par le standard IEEE 802.15.4 décrit un format de trame générique (présentée en figure **4**) et les champs qui la composent : en-tête MAC (MHR, *MAC HeadeR*), données MAC (MSDU : *MAC Service Data Unit*) et pied de trame MAC (MFR : *MAC FootR*). Les champs sont les suivants :

– le **contrôle de trame** (2 octets) : permet d'identifier le type de trame (donnée, balise acquittement ou commande), le mode d'adresse, la demande ou non d'acquittement, etc. ;

– le **numéro de séquence** (1 octet) : octet permettant la numérotation de chaque trame ;

– l'**adressage** (1 à 20 octets) : contient les adresses source et destination de la trame ;

– les **données** : les données utiles (typiquement un datagramme réseau) ;

– la **séquence de contrôle** (2 octets) : un CRC (Code de Redondance Cyclique) normalisé ITU-T sur 16 bits ($x^{16} + x^{12} + x^5 + x^1$).

2.3.2 La sous-couche MAC

2.3.2.1 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 mode*, 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 dès 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 unité temporelle discrète appelée *période de backoff* pour pouvoir retarder plus ou moins l'émission d'une trame et éviter les collisions.

Contrôle de trame	Numéro de séquence	Adressage	Données (Network Level PDU)	Séquence de contrôle
MHR			MSDU	MFR

Figure 4 – Trame MAC générique IEEE 802.15.4

L'implémentation du CSMA/CA dans 802.15.4 est très proche de celle de 802.11, à deux exceptions près :

1. Absence de RTS/CTS : à la différence de 802.11, la méthode d'accès avec contention de 802.15.4 ne prévoit pas de mécanisme pour réserver le médium avant de commencer à émettre les données. Ceci s'explique par le fait que, dans un réseau 802.15.4, les trames DATA sont très courtes et le débit très faible et, de fait, l'utilisation d'un protocole de type RTS/CTS serait très coûteuse. Après avoir attendu un nombre aléatoire de périodes de *backoff*, si le médium est libre, la trame de données est émise.

2. Gestion des temps inter-trames : 802.15.4 en prévoit trois, du plus court au plus long :

– t_{ACK} est le délai imposé entre une trame de donnée et son acquittement. Il doit être le plus court possible, mais dans tous les cas supérieur à 92 µs ;

– SIFS, pour *Short Inter-Frame Spacing*, suit les trames dites « courtes », c'est-à-dire d'une longueur inférieure ou égale à 18 octets ;

– LIFS, pour *Long Inter-Frame Spacing*, suit les trames dites « longues », c'est-à-dire d'une longueur strictement supérieure à 18 octets.

Dans un objectif d'économie d'énergie, cette gestion des temps inter-trames en fonction de la longueur de la trame est nécessaire compte tenu des faibles ressources de traitement (CPU) des nœuds récepteurs : plus le volume des données est important, plus le temps de traitement nécessaire est grand.

Le mode coordonné, ou balisé

Dans le mode coordonné, une ou plusieurs entité(s) du réseau 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'étoile.

La figure **5** illustre le fonctionnement de transfert de données dans une étoile ou cellule gérée par un coordinateur (cf. paragraphe 2.4.1) unique :

– 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).

2.3.2.2 Notion de supertrame

L'espace temporel entre deux trames balises est appelé supertrame. Une supertrame est toujours divisée en 16 slots temporels de durées égales, la trame balise occupe toujours le premier slot ; elle permet donc 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 **6**.

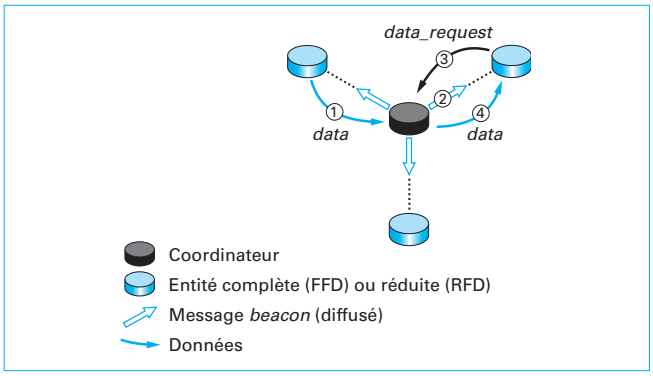

Figure 5 – Principe du transfert de données dans une étoile

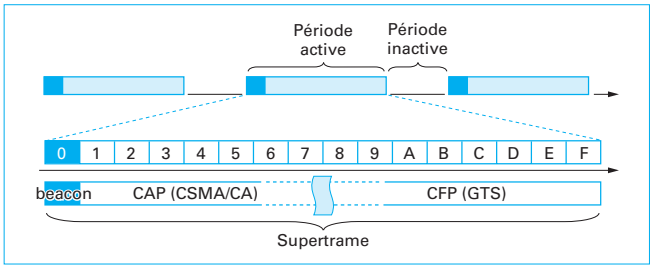

Figure 6 – Structure de la supertrame

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 ;
– SO (*Superframe Order*), qui fixe la durée active de la supertrame.

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. À 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. Si les nœuds 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 sont les économies sur le plan énergétique. Il faudra donc trouver un compromis entre ces deux constantes selon l'application.

Le mode coordonné de 802.15.4 propose deux méthodes d'accès au sein de la supertrame :

• **Un mode avec contention** avec lequel les accès se font de façon classique selon le protocole CSMA/CA slotté. Cependant, les trames balises sont toujours émises périodiquement en début de supertrame, pour assurer la synchronisation entre les entités du réseau. Ce mode d'accès au médium est toujours possible et une partie de la supertrame doit être systématiquement dédiée par le coordinateur aux accès se faisant dans ce mode. Cette partie de la supertrame est appelée CAP.

• **Un mode sans contention**, « *contention free* », optionnel, avec lequel les accès au médium sont maîtrisés par le coordinateur. Ce mode peut être utilisé par les nœuds qui en font la demande. Si la capacité du réseau le permet, le coordinateur pourra choisir d'honorer la demande du nœud en lui allouant un ou plusieurs slots dans la direction (émission ou réception) qui a été demandée ; on parle de GTS. Les GTS sont toujours placés en fin de supertrame, dans les derniers slots. On appelle cette partie de la supertrame CFP. Dans cette période, l'accès au médium est donc organisé et réparti par le coordinateur et les collisions sont rendues plus rares.

Ce mode sans contention rend possible une réservation de bande passante et peut offrir une certaine garantie sur le plan temporel. Pour se faire, le coordinateur peut attribuer jusqu'à 7 GTS, alors qu'un GTS peut occuper un ou plusieurs des 16 slots que comporte la supertrame ; le début de la supertrame, via la CAP, reste toujours en accès libre par CSMA/CA pour permettre l'accès aux transports ne nécessitant pas ou peu de garantie de ne pas être bloqués par un nombre trop important de GTS. Les demandes de GTS ainsi que les demandes d'association au réseau ne peuvent se faire que dans la CAP. Il est donc primordial, pour ne pas bloquer le réseau, de limiter la taille de la CFP au sein la supertrame.

2.3.3 La sous-couche LLC

Conformément à la famille des standards IEEE 802, 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 **vérification 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 qu'il faut effectuer entre les adresses de niveau 3 (au niveau réseau, l'adressage est généralement globalisé sur tout le réseau) et les adresses de niveau 2 (au niveau liaison, l'adressage est parfois local et spécifique à un seul brin filaire ou à la zone de couverture radio de chaque cellule utilisée...). La convergence d'adressage permet également la gestion des procédés de diffusion (*broadcast*) et de diffusion limitée ou diffusion dirigée (*multicast*).

Dans le cadre de 802.15.4, la sous-couche de convergence proposée est très simple, et ce pour plusieurs raisons :

1. Tout d'abord, et c'est le cas avec la plupart des technologies sans fil, dans IEEE 802.15.4, le mécanisme d'acquittement sert non seulement à assurer à un émetteur que le destinataire a reçu correctement les données envoyées, mais aussi à détecter que la transmission sur le médium partagé n'a pas subi de collision (CSMA/CA). De ce fait, l'acquittement est pris en charge par le processus de gestion d'accès au médium et le standard ne prévoit pas de le faire remonter jusqu'à la sous-couche SSCS ; la gestion de ce dernier reste cantonnée à la sous-couche MAC. De plus, la présence d'un système évolué de gestion de la couche MAC nécessite l'intégrité des messages de gestion à ce niveau : cette vérification est donc assurée par un processus qui se situe en dessous de la couche liaison. La sous-couche de convergence n'a donc pas à assurer cette tâche une seconde fois.

2. Dans IEEE 802.15.4, le contrôle de flux est implicite et réalisé très simplement car, étant donné le faible volume de données échangées et la faible capacité mémoire des nœuds, le système d'envoi des paquets de données est de type *send & wait*, c'est-à-dire que la couche supérieure attend le traitement intégral du paquet de données avant l'envoi du paquet suivant (pas d'anticipation).

3. Dans IEEE 802.15.4, la gestion d'adressage est simplifiée dans la mesure où il n'y a pas de conversion à réaliser. Le plan d'adressage est le même entre la couche liaison et la couche réseau, les nœuds utilisent leur adresse MAC pour s'associer au réseau puis ils se voient attribués une adresse courte par le coordinateur du PAN.

2.4 La couche réseau NWK de ZigBee

Comme nous l'avions évoqué au début de cet article, 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 [13], et

notamment, sa propre couche réseau (niveau 3 OSI). Elle permet de définir précisément les règles d'établissement d'un réseau, de l'association et de l'interconnexion des nœuds ainsi que le format des trames échangées. Évoquons tout d'abord les topologies possibles ayant une influence sur le travail de la couche 3.

2.4.1 Éléments de la topologie du réseau

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

1. Le nœud le plus important est 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 et il agit comme simple routeur (ZR, voir point suivant) une fois le réseau créé.

2. Le nœud intermédiaire est le routeur ZigBee, ou *ZigBee Router*, ZR. Celui-ci doit d'abord s'associer avec le ZC ou un autre ZR. Il accepte ensuite que d'autres éléments du réseau s'associent à lui, et reprend les tâches du coordinateur 802.15.4. Le ZR relaie les messages selon un protocole de routage qui sera présenté plus loin. Le routeur ZC est optionnel dans un réseau simple.

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

Ces trois types d'éléments sont très semblables à ce que propose le standard IEEE 802.15.4 vu précédemment. Nous pouvons constater, comme nous l'évoquions précédemment, 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. Ce processus nécessite une connaissance du réseau qui est réalisée par un algorithme de découverte automatique que nous décrirons par la suite.

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. 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, comme nous le verrons plus loin.

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 **7**. Un processus de routage doit être mis en place pour relayer les paquets de bout en bout du réseau ; nous verrons ce processus dans le paragraphe 2.4.3.

2.4.2 Adressage

La spécification ZigBee autorise deux types d'adressage : un adressage libre laissé à la convenance de la couche supérieure et un adressage de type hiérarchique en arbre. Dans ce dernier cas, les adresses sont distribuées suivant un algorithme hiérarchique ayant la structure arborescente. L'avantage de cette distribution est qu'elle est totalement décentralisée tout en garantissant l'unicité des adresses distribuées, car chaque routeur ZigBee dispose d'un certain nombre d'adresses qu'il peut distribuer aux nœuds qui s'associent à lui. Pour réaliser cette distribution d'adresses, chaque routeur doit connaître en particulier sa profondeur dans l'arbre, c'est-à-dire le nombre de sauts à effectuer pour atteindre le coordinateur. Le principe de l'adressage en arbre est très intéressant, car il permet de distribuer automatiquement des adresses de façon décentralisée et déterministe, ce qui minimise les échanges de messages de gestion. Cette économie de messages échangés va dans le sens de l'économie d'énergie. De plus, cet adressage permet un routage automatique en se basant sur les adresses ; là encore, nul besoin d'échange de messages pour déterminer quelle route emprunter ! En terme d'économie d'énergie, un réseau ZigBee a tout intérêt – si possible, par rapport à la géométrie des liens, les portées des nœuds et la présence d'obstacles – à utiliser ce type d'adressage car il va de pair avec une limitation des requêtes des demandes de route et une réduction de la mémoire utilisée pour le processus de routage.

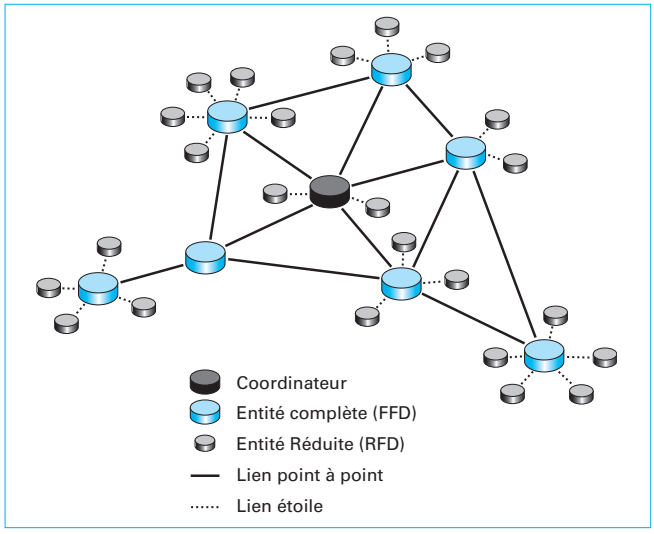

Figure 7 – Exemple de topologie maillée

2.4.3 Principes de base du routage ZigBee

Du fait de la mémoire très limitée des nœuds, le routage ZigBee [3] 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*).

Algorithme de routage à la demande

L'algorithme de routage à la demande proposé par la *ZigBee Alliance* est proche d'AODV [11]. AODV est un protocole de routage purement « à la demande » c'est-à- dire que les nœuds qui participent au routage ne cherchent pas à maintenir des informations sur la topologie du réseau ou sur les routes.

Lorsqu'un nœud veut envoyer un message à un autre nœud et qu'il ne possède pas l'entrée correspondante dans sa table de routage, il lance le processus de recherche de chemin (*Path Discovery*) en diffusant une requête de recherche de route (*route_request*). Cette requête est relayée par les routeurs voisins, et ainsi de suite, par inondation sur tout le réseau. Lorsque le nœud de destination reçoit la requête, il répond en envoyant un message de réponse (*route_reply*) mais à la différence du *route_request* qui avait été envoyé par diffusion, la réponse est envoyée seulement au dernier routeur ayant relayé la diffusion et ainsi de suite, jusqu'au nœud qui avait initialement demandé la route. Pour retrouver le chemin inverse, chaque routeur rediffusant un message *route_request* doit mémoriser par quel voisin ce message lui est parvenu.

Algorithme de routage hiérarchique : *Tree Routing*

Le cas particulier de la topologie en arbre permet de simplifier grandement le routage puisque, dans le cadre de cette topologie hiérarchique, l'adressage est fonction de la topologie. Il suffit donc d'observer l'adresse du nœud de destination pour déterminer à quel voisin envoyer le paquet.

Le problème principal de cet algorithme de routage est que, de part sa structure arborescente, il ne permet pas la redondance des liens comme dans un réseau *mesh*. Si un lien vient à tomber, c'est toute une partie du réseau qui se retrouve isolée. Conceptuellement, sa fiabilité paraît plus faible que celle d'un réseau *mesh*. De plus, cet algorithme de routage n'est pas toujours facilement réalisable, par exemple dans le cas d'un réseau où la mobilité est forte.

2.5 La couche applicative APL et les profils de ZigBee

La couche applicative est la couche de niveau le plus haut. C'est elle qui détermine la façon dont vont être utilisés tous les niveaux inférieurs et ceci pour une application donnée.

La couche APL (*Application Support Layer*) est associée à plusieurs entités protocolaires : le module SSP (*Security Service Provider*) qui peut gérer les fonctions de sécurité (authentification, cryptage), le module APS (*Application Support Sub-Layer*) qui est un soutien aux applications pour la mise en liaison des dispositifs et les services de messagerie, et le module ZDO (*ZigBee Device Object*) qui permet la découverte des dispositifs et des services, au même titre que la couche SDP (*Service Discovery Protocol*) de Bluetooth.

Les profils d'applications définissent quels sont les messages envoyés pour une application donnée. Les dispositifs avec le même profil interopèrent de bout en bout.

ZigBee publie un ensemble de profils publics mais il est possible que des fabricants proposent leurs propres profils. Dans ce cas là, il est nécessaire de leur faire subir des tests de certification permettant de valider leur fonctionnement et le respect des règles protocolaires de ZigBee.

Dès le début de la proposition protocolaire de la pile ZigBee, les concepteurs ont prévu des applications potentielles associées à des profils de communication, à l'instar de IrDA [20] et surtout de Bluetooth [21]. On regroupe généralement les applications de ZigBee en sept grandes catégories :

- L'**automatisation des immeubles** : la sécurité, le contrôle d'accès, l'éclairage, le chauffage...
- Le **médical** : le suivi et la surveillance continue de patients, le monitoring des phases d'efforts lors d'activité physiques et sportives...
- Le **contrôle industriel** : la gestion des biens, des stocks, la gestion de l'énergie, la surveillance des risques et de l'environnement, les applications de contrôle/commande industrielles, les télérelevés...
- Les **services de télécommunications** : le m-commerce (commerce mobile), les infos services, les interactions des objets que l'on appelle souvent « Internet des choses »...
- L'**électronique grand public** : le pilotage et le contrôle à distance des TV, VCR, DVD...
- Le **PC et ses périphériques** : souris, clavier, joysticks...
- La **domotique** : la gestion du chauffage, de l'éclairage, des occultants, des alarmes...

À l'heure actuelle, ce sont les applications de contrôle de l'éclairage ou *lighting* qui ont été en premier développées et soutenues par les industriels concepteurs de composants ZigBee. On peut entrevoir dans cette démarche commerciale la volonté d'offrir enfin des solutions domotiques flexibles sans fil opérationnelles mais également d'élargir l'utilisation de la norme dans des secteurs à très fort potentiel de pénétration (automobile, environnement, agroalimentaire...).

3. Bilan et perspectives

À la lumière des informations techniques qui viennent d'être présentées dans cet article, le lecteur doit maintenant posséder les connaissances de base et pouvoir apprécier les avantages et les limites d'un réseau personnel sans fil comme ZigBee.

Le but principal d'un WPAN ZigBee est d'offrir un moyen de communication radio simple et robuste, entre des équipements électriques et électroniques généralement de petite taille, très souvent autonomes énergétiquement, et ayant des besoins de communication très ponctuels. Le nombre de nœuds dans un réseau ZigBee peut être très grand et dépasser plusieurs milliers d'entités, comme cela peut être le cas dans un réseau de capteurs industriel, domotique ou même militaire ; cependant les débits envisagés s'expriment en quelques dizaines de kbits/s au maximum. Un nœud ZigBee passe une grande partie de son temps en état de somnolence et communique de façon très ponctuelle avec ses interlocuteurs. C'est la faculté de se réveiller très rapidement, envoyer ou recevoir quelques octets, puis se rendormir tout aussi rapidement qui lui confère un avantage majeur face aux autres technologies WPAN plus lentes durant ces phases.

De plus, la technologie radio de ZigBee est très faiblement perturbée par les technologies de mêmes fréquences WiFi et Bluetooth et est très faiblement perturbatrice grâce notamment à la nature des applications visées (taux de transmissions faibles avec des petites quantités de données). La possibilité pour les industriels, laboratoires de recherche, et même organismes de formation, d'appréhender très facilement les couches basses protocolaire de 802.15.4, en font un candidat idéal pour le prototypage rapide d'applications de communication associées à des protocoles spécifiques et novateurs. Les fabricants et principaux acteurs offrent généralement des kits de développement simples d'utilisation, et d'un coût raisonnable.

L'objectif actuel de ZigBee est de définir un **réseau d'usage universel et peu coûteux à configuration automatique**, qui puisse être utilisé aussi bien par des processus de contrôle industriels, des dispositifs médicaux, des détecteurs de sécurité (incendie, intrusion), des systèmes d'automatisme dans le bâtiment et pour la domotique en général. **Les perspectives de développement de ZigBee sont donc nombreuses** et devraient même dépasser le succès commercial de Bluetooth. Enfin, il reste néanmoins beaucoup de points à améliorer dans l'architecture protocolaire de ZigBee, comme ses réelles aptitudes à offrir une QdS (Qualité de Service) plus aboutie, par exemple pour des applications à fortes contraintes temporelles (robotique, capteurs industriels critiques...), ou son interopérabilité avec des protocoles classiques largement utilisés dans l'Internet. Des développements futurs de ZigBee dépendra le succès de ce nouveau LP-WPAN, face à des concurrents tels que 6LowPAN [15], basé lui aussi sur des couches basses 802.15.4 mais permettant l'utilisation directe de communications IPv6, grâce en particulier à une compression des en-têtes IPv6, fortement consommatrices en bande passante, afin que ces en-têtes puissent être insérées dans les petits paquets 802.15.4.