9. Annexe

état de l'art de la liste exhaustive des technologies considérées

9.1.1. La norme IEEE 802.15.1

La norme IEEE 802.15.1 spécifie les couches physiques et MAC pour des connexions sans fil avec des équipements fixes ou mobiles autour de la personne ou d'un objet. Elle vise des solutions peu chères, robustes, efficaces en énergie, supportées par une large gamme d'équipements. Cette norme est basée sur la technologie initialement développée par le groupe BlueTooth Special Interest Group.

9.1.1.1. Architecture

Au niveau physique, la norme IEEE 802.15.1 utilise la bande des 2.4GHz. Les 79 canaux RF sont numérotés de 0 à 78 et séparés par 1 MHz en commençant par 2 402 MHz. Le codage de l'information se fait par sauts de fréquence. Le saut de fréquence (technique utilisée FHSS, frequency hopping spread spectrum) permet de résister aux interférences et à l'atténuation. Pour réduire la complexité du transceiver, une modulation de fréquence binaire est utilisée. Le débit supporté est de 1Mbit/s. En fonctionnement normal, un canal radio est partagé par un groupe d'équipements synchronisés sur une horloge commune et une séquence de saut de fréquence. L'équipement qui fournit la référence de synchronisation est appelé *maître*, les autres équipements ses *esclaves*. Un tel groupe forme un *piconet*. Un maître peut gérer jusqu'à sept esclaves actifs et 255 esclaves parqués. La séquence de saut de fréquence est déterminée par certains champs de l'adresse du maître et son horloge. C'est une séquence pseudo-aléatoire des fréquences disponibles dans la bande ISM. Il est ainsi possible d'exclure les fréquences faisant l'objet d'interférences causées par d'autres réseaux à proximité. Le canal physique est subdivisé en slots de 625 microsecondes. Les paquets transmis entre équipements sont transmis dans ces slots. Un paquet peut occuper plusieurs slots. Le saut de fréquence n'est effectué qu'entre la transmission et la réception d'un paquet. Plusieurs piconets peuvent être interconnectés, formant alors un scatternet. La seule condition est qu'un nœud passerelle n'est maître d'aucun piconet.

Dans un piconet, la communication est effectuée sur un canal physique selon le mode TDD (Time Division Duplex). Il existe un lien physique entre le maître et chaque esclave, mais pas de lien physique direct entre deux esclaves. Les types de trafic supportés sont les trafics unicast synchrones, asynchrones ou isochrones ainsi que les trafics broadcast. Dans tous les cas, le trafic est soit émis par le maître, soit à destination du maître. L'accès au médium se fait sous le contrôle du maître. Chaque équipement dispose d'une adresse sur 48 bits, appelée *BD_ADDR* (*Bluetooth Device Address*) . Ces adresses sont gérées par la *IEEE Registration Authority*. Il existe trois classes de modules radio *Bluetooth*, sur le marché ayant des puissances différentes et donc des portées différentes :

Classe	Puissance	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	10 à 20 mètres
3	1 mW (0 dBm)	Quelques mètres

La plupart des fabricants d'appareils électroniques utilisent des modules de classe 2.

La figure 1 illustre l'architecture faisant apparaitre l'interface standardisée, appelée HCI, Host Controller Interface, entre le contrôleur qui implémente les trois couches les plus basses (radio, bande de base et gestion de liaison) et l'hôte qui implémente la couche L2CAP et les couches supérieures. Comme le contrôleur est limité en buffers, la couche L2CAP doit se charger de la segmentation des unités de données utilisateur en unités de données protocole pouvant être elles-mêmes fragmentées en paquets.

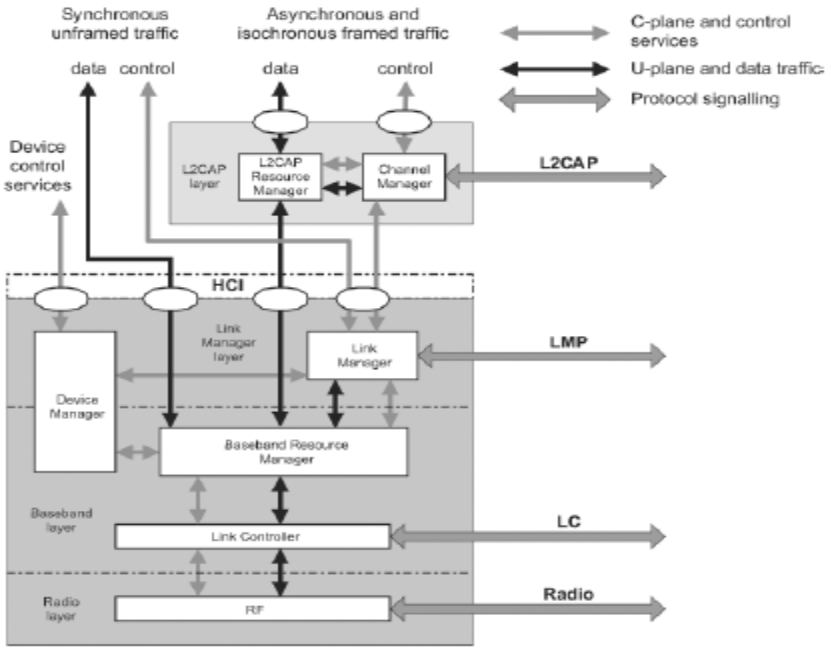

Figure 1 : Architecture avec séparation possible du contrôleur et de l'hôte.

9.1.1.2. La couche L2CAP

La couche L2CAP implémente le L2CAP Manager et le Channel Manager. Elle peut sur option fournir une fonctionnalité de détection/retransmission pour les données utilisateur demandant une certaine fiabilité. De même un mécanisme de contrôle de flux peut être utilisé pour contrôler la disponibilité des buffers chez le récepteur.

Le Channel Manager est responsable de la création, gestion et destruction des canaux L2CAP pour le transfert des messages. Il utilise L2CAP pour interagir avec le Channel Manager d'un équipement distant pour créer les canaux L2CAP demandés. Le Channel Manager interagit avec son local Link Manager pour créer les nouveaux liens logiques nécessaires et les configurer selon la qualité de service demandée par ce type de données à transférer.

Le L2CAP Resource Manager est chargé de veiller à ce que les canaux L2CAP avec des engagements de QoS (qualité de service) puissent accéder à un canal physique malgré les ressources limitées du contrôleur. Il est responsable de l'ordre dans lequel sont soumis les fragments d'unités de données de protocole à la couche bande de base. Il peut également se charger de la politique de mise en conformité des trafics.

9.1.1.3. Le Device Manager

Le Device Manager contrôle le comportement de l'équipement. Il se situe à la fois dans la couche Link Manager et dans la couche BaseBand. Il est responsable de toute opération non directement liée au transfert de données telle que la détection de la présence d'équipement voisin, la gestion du nom local de l'équipement, la gestion des clés des liens. Pour ce faire, il demande l'accès au médium au Baseband Resource Manager.

9.1.1.4. La couche Link Manager :

Elle comprend le Link Manager (LM).

Le Link Manager est responsable de la création, modification, et libération des liens logiques ainsi que la mise à jour des paramètres associés aux liens physiques. Pour ce faire, il communique avec un LM distant en utilisant le protocole LMP.

LMP permet la création de nouveaux liens logiques entre équipements. Initialement, seul un lien de type ACL est créé entre un esclave et le maître du piconet, les autres liens sont créés à la demande. LMP permet également de contôler les paramètres des liens logiques (données cryptées, adaptation de la puissance de transmission, paramètres de QoS).

9.1.1.5. La couche Baseband

La couche BaseBand regroupe le BaseBand Resource Manager et le Link Controller.

Le BaseBand Resource Manager gère l'accès au medium physique. Il gère l'accès au médium dans les slots temporels conformément au type d'accès qui a été négocié.

Le Link Controller est chargé d'encoder et décoder les paquets qui lui sont soumis. Il véhicule la signalisation utilisée pour le contrôle de flux, les acquittements et retransmissions. L'interprétation et le contrôle de cette signalisation sont à la charge du BaseBand Resource Manager.

9.1.1.6. La couche Radio: Radio Frequency (RF)

Le bloc RF est chargé de transmettre et recevoir des paquets sur le canal physique. La couche Baseband peut contrôler le timing et la fréquence de la porteuse. Quatre canaux physiques sont définis :

- deux canaux physiques, le canal basique et le canal adapté, sont associés à un piconet et utilisés pour communiquer entre équipements connectés à ce piconet ;
- un canal physique pour découvrir les équipements : inquiry scan channel ;
- un canal physique pour connecter les équipements : page scan channel.

9.1.1.7. Les services de transfert offerts à l'utilisateur

Nous distinguons les services de transfert suivants, illustrés par la figure 2 :

- ACL : Asynchronous Connection-Oriented utilisés pour un transfert point-à-point, bidirectionnel, fiable ou temps contraint. C'est le lien par défaut qui est créé lors de la connexion de l'équipement au piconet. C'est aussi sur ce lien qu'est véhiculée la signalisation LMP. Si l'équipement est parqué, il perd tous ses liens et en particulier

son lien ACL par défaut. Il demeure cependant synchronisé au piconet. Les données utilisateur sont découpées en paquets de 1, 3 ou 5 slots.

- SCO : Synchronous Connection-Oriented utilisés pour un transfert point-à-point, bidirectionnel audiovisuel, symétrique et à débit constant de 64 kbit/s ; des slots fixes et réservés sont utilisés pour transmettre des paquets de taille fixe périodiquement sans retransmission possible.

- eSCO : Extended Synchronous Connection-Oriented utilisés pour un transfert point-à-point, bidirectionnel, symétrique ou asymétrique, avec des données régulières et des retransmissions limitées pour des données à débit constant synchronisées sur l'horloge du maître ; ce service est plus flexible que le précédent (ex. : possibilité de retransmission)

- ASB : Active Slave Broadcast utilisés pour des diffusions non fiables aux seuls équipements synchronisés sur le canal physique du piconet dans les groupes L2CAP ;

- PSB : Parked Slave Broadcast utilisés pour des diffusions non fiables à tous les équipements du piconet. ils véhiculent le trafic LMP et L2CAP destiné aux équipements parqués et par les demandes d'accès provenant des équipements parqués.

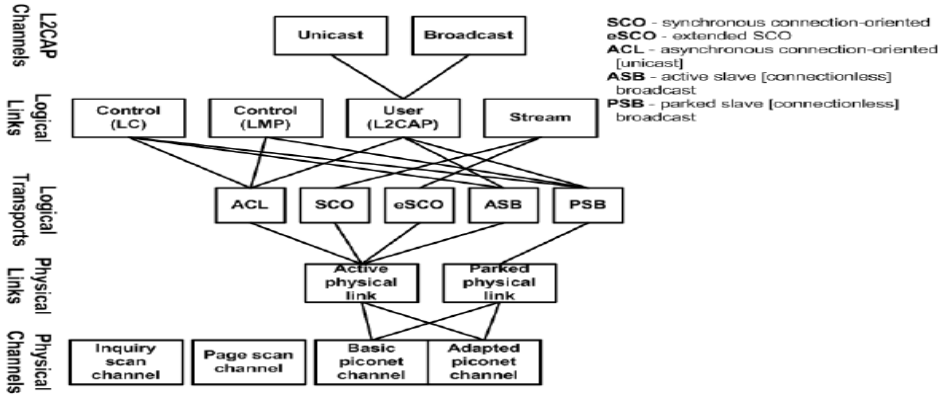

Figure 2: Hiérarchie des entités chargées d'assurer les différents services.

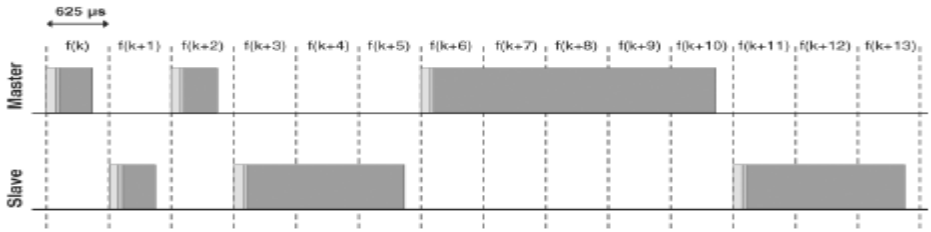

Figure 3 : Succession de paquets émis par le maître et un esclave.

La taille des paquets émis sur un lien ACL est de 1, 3 ou 5 slots ; les slots sont de 625us.

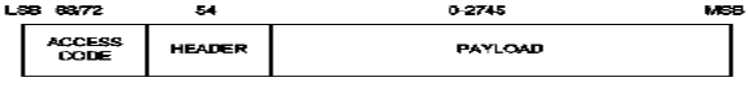

Figure 4 : Format d'un paquet de taille maximum 2745 bits.

9.1.2. La norme IEEE 802.15.3

La norme IEEE 802.15.3 spécifie les couches MAC et physique pour des réseaux radio sans fil de type WPAN (équipements fixes ou mobiles autour de la personne ou d'un objet) à haut débit (11 à 55 Mbit/s). Elle a été conçue pour le transfert de fichiers audio et vidéo en streaming. Cette norme dispose de capacités accrues en termes de portée, de bande passante et de débit de connexion. Elle est compatible avec les autres normes 802.15 pour réseaux WPAN (réseaux personnels sans fil).

9.1.2.1. Description

En se basant sur les précédents appels pour applications collectés pour le groupe 802.15, un nombre significatif d'applications ne peut pas être adressé par le 802.15.1. Des débits élevés sont nécessaires pour des applications dépendant du temps ou des applications de transfert de fichiers volumineux sans sacrifier les critères de simplicité d'implémentation, de coût bas et d'une faible consommation d'énergie.

Un débit minimal de 20Mbit/s a été proposé pour ce type d'applications.

Cette norme vient pallier les insuffisances de partage de la bande passante des précédentes normes. Le 802.15.3 peut en effet admettre jusqu'à 245 connexions simultanées et procure un débit de 55 Mbps (contre 1 Mbps auparavant) pour une distance de connexion de 100 mètres environ. Diffusée sur la fréquence 2,4 GHz, cette norme semble d'autant plus performante qu'elle assure l'immunité aux interférences causées par les autres types de réseaux, ce qui lui permettra de coexister avec les normes de type Wi-Fi (802.11x), 802.15x et Bluetooth.

Il est possible, par exemple, que plusieurs débits soient supportés pour différentes applications utilisateurs. Par conséquent, les notions de coût, de bande de fréquence, de performance, d'énergie et de débit ont été prises en compte lors du développement de ce standard.

9.1.2.2. Architecture du réseau

L'IEEE 802.15.3 définit un réseau avec une architecture en piconets.

Un piconet est un système de communication sans fil en mode ad hoc permettant à un certain nombre de nœuds (*Independent Data Devices* (DEVs)) de communiquer entre eux. Un piconet se distingue des autres types d'architecture réseau dans le fait que les communications sont normalement confinées à une petite zone autour d'une personne ou d'un objet. Cette zone couvre, typiquement, une distance maximale de 10 mètres dans toutes les directions et couvre la personne ou l'objet qu'il soit stationnaire ou en mouvement. Un piconet 802.15.3 consiste en plusieurs composants comme illustré dans Figure 5.

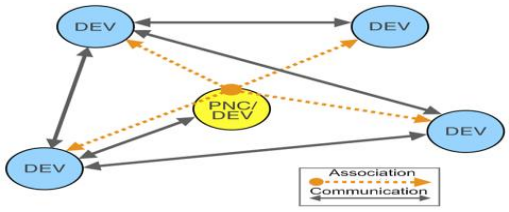

Figure 5 : Type de liaison dans un piconet.

Le composant basique est le DEV. Dans chaque piconet, un DEV est amené à assumer le rôle de coordinateur de piconet (PNC). Le PNC fournit le timing de référence pour le piconet grâce aux transmissions de la trame beacon. De plus, le PNC gère les besoins de QoS, le mode d'économie d'énergie ainsi que le contrôle d'accès au piconet.

Etant donné que les piconets 802.15.3 se forment sans planification préalable et seulement pour un temps limité, ce type de réseau est considéré comme un réseau ad hoc.

Le standard permet à un DEV de demander la formation d'un piconet subsidiaire. Le piconet initial est référencé comme le piconet parent et le piconet subsidiaire est référencé comme le piconet fils ou le piconet voisin selon la méthode utilisée par le DEV pour s'associer avec le PNC. Le piconet fils ou voisin peut être référencé aussi comme un piconet dépendant puisque il se base sur le PNC du piconet initial pour l'allocation du temps d'accès au canal. Un piconet indépendant est un piconet qui ne possède pas de piconets dépendants.

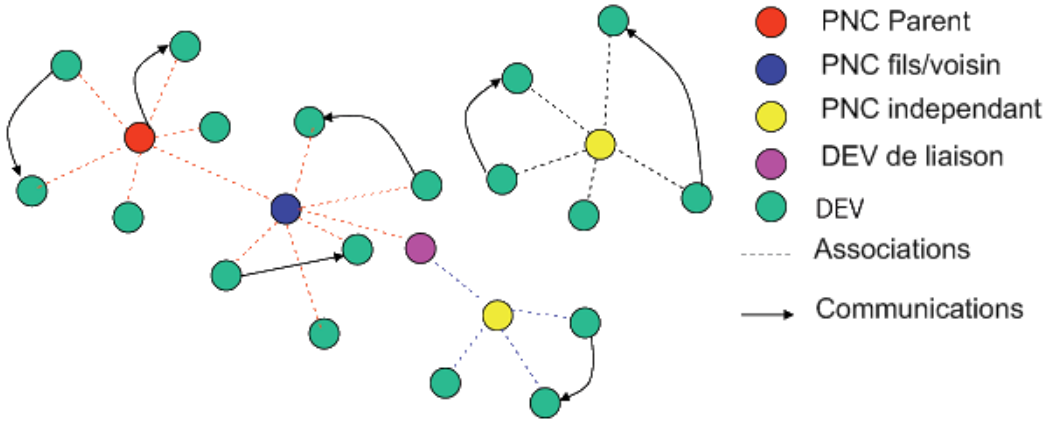

Figure 6 : Architecture en piconets.

9.1.2.3. L'accès au canal de communication

Le temps du canal est divisé en une succession de Supertrames commençant chacune par une trame beacon.

Une Supertrame est composée de 3 parties majeures: le beacon, la CAP (Contention Access Period) et la CTAP (Channel Time Allocation Period).

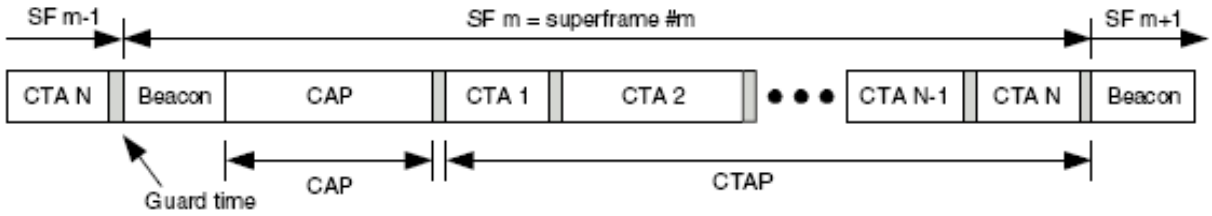

Figure 7 : Structure d'une Supertrame.

La CTAP est utilisée pour les flux de données asynchrone ou isochrone alors que la CAP peut être utilisée pour transmettre des commandes ou des données (*non-stream data*).

Durant la CAP les nœuds sont en compétition pour accéder au canal en utilisant l'algorithme CSMA/CA. Cependant, durant la CTAP, le PNC contrôle l'accès au canal en assignant des CTAs (Channel Time Allocation) à un nœud (DEV) ou à un group de nœuds, chaque CTA possède un temps de début et une durée fixe.

Le PNC contrôle le type de données ou commandes transmises durant la CAP grâce à une information transmise dans la trame beacon.

Un DEV ne doit transmettre, pour la Supertrame en cours, que des trames du type spécifié par le PNC dans la trame beacon. Le PNC peut changer le type de trames pouvant êtres transmises durant la CAP d'une Supertrame à une autre.

Afin de minimiser les collisions, avant de transmettre un DEV doit effectuer une écoute du canal (CCA) afin de détecter si le canal est libre ou non. Durant la CAP, un DEV n'est autorisé à transmettre qu'une seule trame à la fois, avec une écoute du canal avant chaque transmission de trame.

L'IEEE 802.15.3 offre de plus une qualité de service accrue, puisqu'il inclut le protocole TDMA (*Time Division Multiple Access*). Ce dernier permet de gérer les connexions simultanées en fonction de la bande passante disponible afin d'optimiser les transferts et d'éviter les encombrements de réseau. En effet, durant la CTAP l'accès au canal se base sur une technique TDMA dans laquelle chaque CTA possède un début et une durée garanties, ce qui permet de réduire la consommation d'énergie ainsi que garantir de bonnes caractéristiques de QoS.

Un DEV possédant un CTA peut ou non utiliser tout le temps qui lui est alloué. La sélection du flux, commande ou données asynchrone à transmettre localement par le DEV, est fonction du nombre de trames en attente dans la file et de leur priorité.

Il existe deux types de CTA: dynamique et pseudo statique. Le PNC a la possibilité de bouger un CTA dynamique à l'intérieur de la Supertrame permettant ainsi de réarranger les CTAs afin d'optimiser leur assignation.

9.1.2.4. La communication entre nœuds

Afin de pouvoir manipuler des trames volumineuses des couches supérieures, la couche MAC a la possibilité de fragmenter et défragmenter ces trames ce qui permet de réduire le FER (*Frame Error Rate*) en réduisant la taille des trames.

Si un nœud (DEV) veut vérifier la bonne réception d'une trame, l'une des trois politiques d'acquittement est utilisée :

- Pas d'acquittement (No-ACK policy) : pas de garantie de bonne réception de la trame.
- Acquittement immédiat (Imm-ACK policy) : chaque trame est acquittée séparément.
- Acquittement retardé (Dly-ACK policy) : Permet à la source de transmettre plusieurs trames sans recevoir d'acquittement. Les acquittements individuels sont groupés en une seule trame d'acquittement envoyée à la demande de la source. Ce type d'acquittement permet de réduire le trafic sur le canal tout en permettant à la source de vérifier la bonne réception des trames transmises.

Si le DEV source ne reçoit pas d'acquittement alors il a la possibilité de retransmettre la trame ou d'abandonner la transmission de la trame.

La décision de retransmettre ou d'abandonner la transmission d'une trame dépend du type de données transmises, du type de commande, du nombre de retransmissions, du temps d'attente dans la file…etc.

9.1.2.5. La couche physique

La couche physique 802.15.3 opère sur la bande entre 2.4 GHz et 2.4835 GHz, généralement qualifiée de bande libre (émission/réception sans licence). Deux plans de canaux ont été définis, le premier plan comporte 4 canaux pour des applications à haute densité et le deuxième plan comporte 3 canaux permettant une meilleure coexistence avec les réseaux IEEE 802.11b.

Puisque deux canaux des deux plans se chevauchent, il y a au total 5 canaux de communication.

Id du canal	Fréquence centrale	Haute densité	Coexistence 802.11b
1	2.412 GHz	X	X
2	2.428 GHz	X	
3	2.437 GHz		X
4	2.445 GHz	X	
5	2.462 GHz	X	X

La couche physique supporte 5 débits différents allant de 11 à 55 Mbit/s. Une transmission en débit de base (22 Mbit/s) n'est pas codée alors que les transmissions en débits de 11, 33, 44 et 55 Mbit/s sont codées grâce à une modulation codée en treillis.

Type de modulation	Codage	Débit (Mbit/s)
QPSK	TCM à 8 états	11
DQPSK	Pas de codage	22
16-QAM	TCM à 8 états	33
32-QAM	TCM à 8 états	44
64-QAM	TCM à 8 états	55

9.1.3. La norme IEEE 802.15.4

IEEE 802.15.4 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).

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 2.4 GHz.

IEEE 802.15.4 prévoit une portée classique de quelques dizaines de mètres. La puissance maximale émise par un module 802.15.4 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 d'autonomie énergétique. 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 %).

Le couche liaison spécifié par le standard IEEE 802.15.4 décrit un format de trame générique 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), 127 octets au maximum;
- la séquence de contrôle (2 octets) : un CRC (Code de Redondance Cyclique)

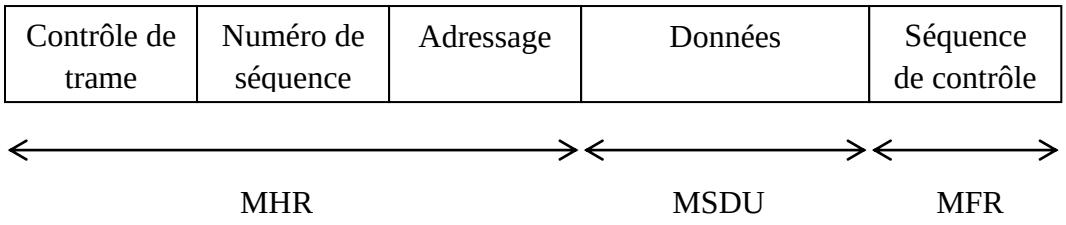

Figure 8: Format d'une trame MAC IEEE 802.15.4.

9.1.4. La famille de norme IEEE 802.11

La famille IEEE 802.11 spécifie un contrôle d'accès au médium et plusieurs couches physiques pour pouvoir connecter en sans fil des équipements fixes, portables ou mobiles dans une zone locale donnée. Elle utilise des techniques de modulation qui utilisent le même protocole de base. Les plus populaires sont les protocoles 802.11b, et 802.11g qui utilisent la bande de fréquence des 2,4GHz. C'est pourquoi les nœuds 802.11 peuvent parfois souffrir des interférences causées par les fours micro-ondes, les téléphones sans fil et les équipements BlueTooth. Alors que BlueTooth utilise le saut de fréquence FHSS, le 802.11b et le 802.11g utilisent respectivement, la signalisation DSSS, direct sequence spread spectrum signaling et la méthode OFDM, orthogonal frequency division multiplexing. Le 802.11a utilise la bande des 5GHz, offrant 19 canaux distincts. La sécurité a été renforcée dans le 802.11i. Le 802.11n propose une nouvelle technique de modulation multi-streaming. Les autres standards de la famille (c-f, h, j) sont des amendements.

Les principaux amendements qui modifient de manière significative les techniques de transmission utilisées sont les suivants :

Protocole	Date de normalisation	Fréquence	Débit max	Portée en intérieur	Portée en extérieur	
Legacy	1997	2.4-2.5 GHz	2 Mbit/s			
802.11a	1999	5.15-5.35/ 5.47-5.725/ 5.725-5.875 GHz	54 Mbit/s	~25 m	~75 m	Permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Spécifie 8 canaux radio dans la bande des 5 GHz.
802.11b	1999	2.4-2.5 GHz	11 Mbit/s	~35 m	~100 m	La norme la plus répandue. Propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée ≤ 300 m en extérieur. 3 canaux radio dans la bande des 2.4 GHz
802.11g	2003	2.4-2.5 GHz	54 Mbit/s	~25 m	~75 m	Offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4

						GHz. Compatibilité ascendante avec la norme 802.11b : des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11n	2009	2,4GHz ou 5GHz	540 Mbit/s	~50 m	~125 m	
802.11y	2008	3.7 GHz	54Mbit/s	~50 m	~5000 m	

Il existe aussi des amendements concernant principalement la couche MAC du standard:

Amendement	**Date de publication**	**Description**
802.11c		Modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	2001	Supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	2005	Vise à donner des possibilités en matière de qualité de service (QoS) au niveau de la couche *liaison de données*. Permet de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f		Recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming)*

802.11h	2003	Décrit des mécanismes permettant de mesurer et d'abandonner les canaux afin de respecter leurs conditions d'utilisations locales (notamment nécessaires pour l'utilisation de la bande ISM à 5 GHz en Europe).
802.11i	2004	Améliore la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11j	2004	Décrit les modifications nécessaires à l'utilisation des bandes de fréquences à 4.9 GHz et 5 GHz en conformité avec la régulation japonaise. Est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

En 2007, la plupart des principaux amendements à la norme 802.11 (a,b,d,e,g,h,i,j) ont été directement intégrés dans la norme et sont disponibles sous la forme d'un unique document .

9.1.4.1. Topologie

La figure ci- après illustre les différents composants 802.11. On distingue deux types de nœuds :

- les points d'accès, notés PA sur la figure, gère l'association des autres nœuds ;
- les nœuds autres, encore appelés stations, notées STA sur la figure.

Un BSS, Basic Service Set comprend un point d'accès éventuel (i.e ; pas de point d'accès en mode ad hoc) et les stations qui lui sont associées. Le Distribution System, DS, est chargé d'interconnecter différents points d'accès et de former ainsi un réseau étendu.

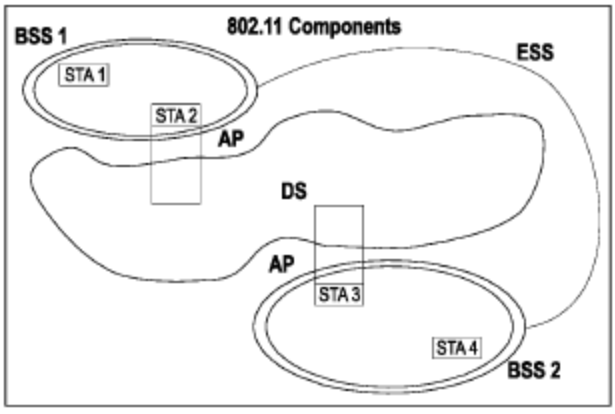

Figure 9 : Les différents composants d'un réseau 802.11.

9.1.4.2. Services offerts

Les services offerts permettent de :

- transférer des données utilisateur entre nœuds : ces services sont :
    - service de distribution invoqué à chaque émission/réception de données ;
    - service d'association permet à un nœud de connaître son point d'accès ;
    - service de réassociation, utilisé en cas de mobilité ou changement de topologie ;
    - service de désassociation pour terminer une association existante ;
- contrôler l'accès au médium et assurer la confidentialité ; ces services sont :
    - l'authentification utilisée pour remplacer la connexion filaire, est fournie au niveau deux entre deux nœuds voisins ;
    - la confidentialité des données.
- gérer la bande de fréquence ; ces deux services utilisés avec la bande des 5GHz sont :
    - transmit power control (TPC)
    - dynamic frequency selection (DFS).
- supporter des applications avec des contraintes de QoS par le biais de la différentiation de services au niveau de l'accès au médium et la spécification des types de trafic avec leurs contraintes de QoS ;
- offrir une synchronisation temporelle précise aux applications (ex. flux audio ou vidéo).

9.1.4.3. Les trames 802.11

Pour fournir ces services, différents types de trame sont utilisés :

- les trames de données qui contiennent des données fournies par la couche supérieure. Une trame MAC peut avoir jusqu'à 4 champs d'adresse. L'adresse 1 est celle du récepteur, l'adresse 2 de l'émetteur, l'adresse 3 est utilisée comme filtre par le récepteur.

- les trames de contrôle facilitent l'échange de trames de données entre nœuds. Citons à titre d'exemple:
    - les trames d'acquittement (ACK) : après avoir reçu une trame de données, le récepteur acquitte l'émetteur s'il n'a détecté aucune erreur. Si l'émetteur ne reçoit pas un acquittement dans un intervalle de temps donné, il retransmit sa trame jusqu'à concurrence d'un nombre maximum de transmissions.
    - les trames Request to Send (RTS): les trames RTS et CTS sont utilisées pour réduire les collisions causées par les nœuds caches. L'envoi du RTS est la première étape avant l'envoi des données.
    - les trames Clear to Send (CTS): Un nœud répond à une trame RTS par une trame CTS. Il permet ainsi au noeud émetteur du RTS d'envoyer ses données. Le CTS inclut une durée Durant laquelle toute station hormis le destinataire du CTS s'abstient de transmettre.
- Les trames de gestion assurent la maintenance. Citons à titre d'exemple :
    - les trames d'authentification où un nœud envoie une demande d'authentification à son point d'accès. La procédure dépend du type d'authentification utilisé. A l'issue de cette procédure, le point d'accès accepte ou refuse.
    - les trames de demande d'association émises par un nœud pour permettre au point d'accès d'allouer les ressources et synchroniser le nœud.
    - les trames de réponse d'association émises par un point d'accès vers un nœud pour indiquer l'acceptation ou le refus d'association.
    - la trame de beacon émise périodiquement par le point d'accès pour annoncer sa présence et fournir divers paramètres du réseau.
    - la trame de désauthentification émise par un nœud voulant terminer sa connexion.
    - la trame de désassociation émise par un nœud voulant terminer sa connexion.
    - la trame de demande de sonde émise par un nœud demandant des informations à un autre nœud.
    - la trame de réponse de sonde émise par un point d'accès en réponse à une demande d'un autre nœud.
    - la trame de demande de réassociation émise par un nœud qui n'est plus à portée de son point d'accès courant.
    - la trame de réponse de réassociation émise par un point d'accès contenant l'acceptation ou le rejet de la réassociation demandée par un autre nœud .

9.1.5. Le standard ZigBee

ZigBee cible les réseaux sans fil utilisés pour la télé-surveillance et les applications de contrôle. Il se veut offrir une solution simple, fiable, et de faible coût pour des réseaux à faible débit et faible consommation énergétique. ZigBee est promu par la ZigBee Alliance, une alliance d'industriels. La technologie ZigBee vise une très large gamme d'équipements (i.e. tout équipement usuel susceptible de communiquer en sans fil) ainsi que plus généralement les marchés industriels, commerciaux et gouvernementaux.

ZigBee s'appuie sur le standard IEEE 802.15.4 pour les couches physique et MAC. Il propose une couche réseau qui offre le routage multisaut et une couche application.

9.1.5.1. Topologies

Selon les spécifications MAC IEEE 802.15.4, il existe trois types d'équipements qui sont spécifiés dans ZigBee:

- ZigBee Coordinateur (MAC Network Coordinator). Maintient la connaissance globale du réseau; le plus sophistiqué des trois types et donc celui qui consomme le plus de mémoire et d'énergie ;
- ZigBee Routeur (MAC Full Function Device): supporte la fonctionnalité complète spécifiée dans IEEE 802.15, peut router des paquets pour les autres noeuds.
- ZigBee Terminal (MAC Reduced Function Device): ne supporte qu'une fonctionnalité limitée pour réduire le coût et la complexité. Cet équipement ne peut pas router des paquets pour d'autres.

Les différentes topologies rencontrées dans ZigBee sont au nombre de trois : mesh, étoile et cluster tree. Elles sont illustrées dans la figure suivante.

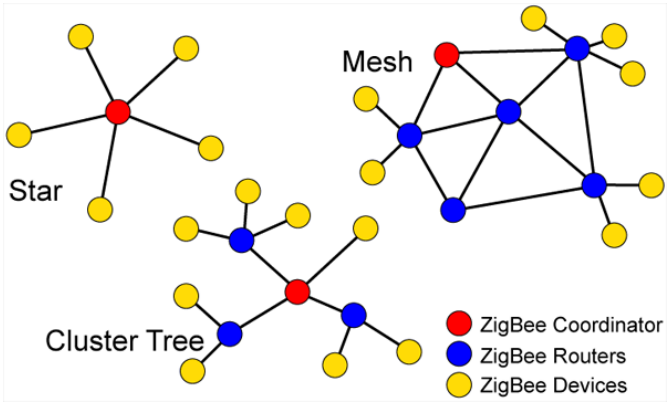

Figure 10 : Topologies ZigBee.

Pour des réseaux en étoile, ZigBee peut fournir une latence de l'ordre de 16ms dans un réseau avec beacon en utilisant des timeslots garantis pour se protéger des interférences pouvant être créées par d'autres capteurs.

L'espace d'adressage permet d'atteindre jusqu'à:

- 2^64 équipements en mode étendu, chacun disposant d'une adresse sur 64 bits;
- 2^16 équipements en mode local, chacun disposant d'une adresse sur 16 bits.

La norme IEEE 802.15.4 fournit des services d'authentification, cryptage, et intégrité permettant aux développeurs d'appliquer les niveaux de sécurité requis: pas de sécurité, listes de contrôle d'accès, et chiffrement AES 32-bit à 128-bit avec authentification. C'est au développeur que revient le choix du meilleur compromis : niveau de sécurité versus consommation énergétique, et capacité de traitement. La sécurité ZigBee permet de gérer à distance la sécurité du réseau sans fil (ex. gestion des clés de sécurité).

9.1.5.2. Stack ZigBee

La stack ZigBee est représentée sur la figure 11 On retrouve au niveau des deux premières couches la norme IEEE 802.15.4. La ZigBee Alliance a ajouté une couche Réseau et une couche Application incluant le support de l'application, l'objet ZigBEE (ZigBee Device Object) et les objets application définis par le constructeur.

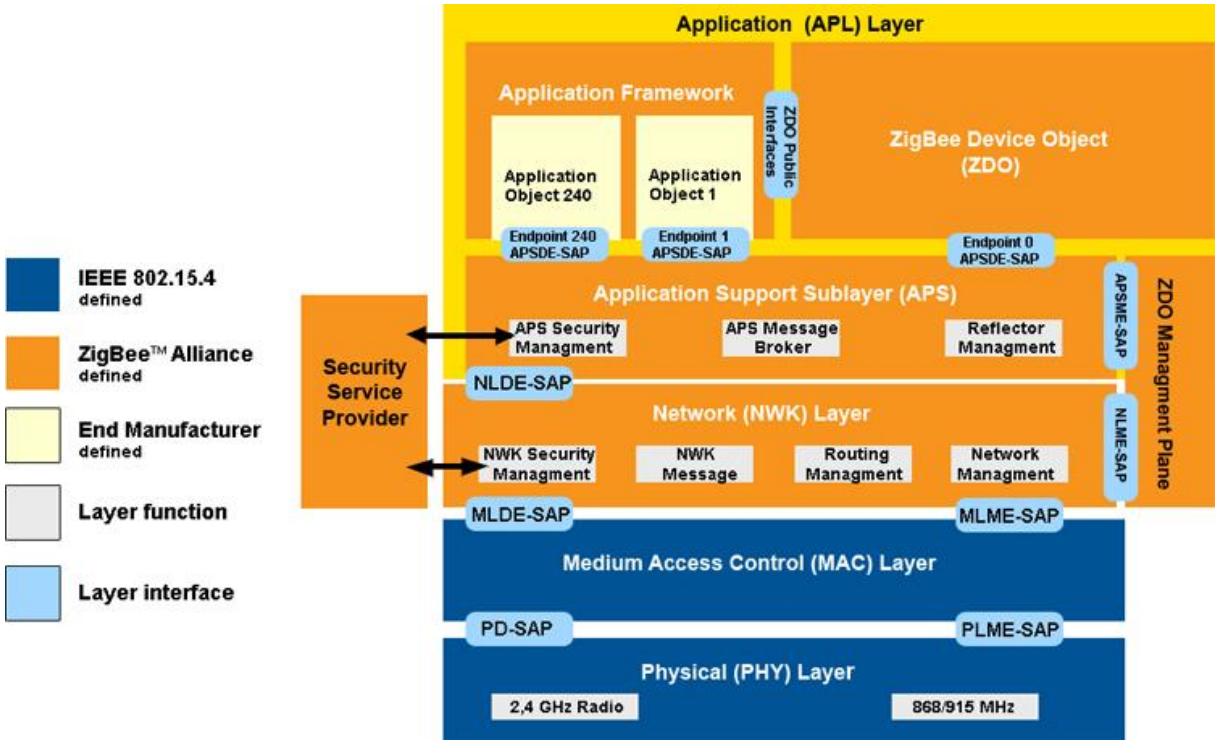

Figure 11 : Stack ZigBee.

La couche Réseau permet à un équipement de joindre/quitter le réseau, appliquer le niveau de sécurité requis aux paquets et de les router vers leur destination finale. De plus, la découverte et la maintenance des routes sont à la charge de cette couche, ainsi que la découverte des voisins à un saut et le stockage d'information pertinente les concernant . C'est la couche Réseau du coordinateur qui est responsable de créer un nouveau réseau et d'assigner de nouvelles adresses aux équipements qui viennent s'associer.

La couche Application inclut la sous-couche APS, le ZDO et les objets application définis par le constructeur. La sous-couche APS maintient les tables pour les associations permettant à deux équipements associés de s'entendre sur leurs besoins et services et d'échanger des messages. Le ZDO définit le rôle des équipements dans le réseau (ex. :, ZigBee coordinateur ou terminal), découvre les équipements présents sur le réseau et determine les services applicatifs qu'ils fournissent, a l'initiative ou répond aux requêtes d'association et établit une relation sécurisée entre équipements.

La pile protocolaire ZigBee est petite en comparaison des autres standards sans fil. Pour des équipements terminaux avec des capacités limitées, la pile protocolaire ne demande que 4Kbits de mémoire. L'implémentation complète de cette pile prend 32Kbits de mémoire. Le coordinateur du réseau a besoin de davantage de mémoire pour gérer Tla base de données des équipements et les tables d'association.

9.1.5.3. Profils ZigBee

Un profil d'équipement ZigBee, ou profil d'application, est un ensemble de descripteurs d'équipements décrivant la vue que l'application a de ces équipements. Les profils sont développés par les vendeurs de la technologie ZigBee pour adresser des besoins technologiques spécifiques. Ils sont un moyen pour d'une part unifier des solutions techniques interopérables au sein du standard ZigBee et pour d'autre part focaliser sur un marché donné.

Les Profils de pile protocolaire désignent un ensemble de valeurs de paramètres utilisées dans la pile protocolaire et agréées pour fournir l'interopérabilité dans des marchés spécifiés. Dans la version v1.0, les profils de pile protocolaire identifies étaient:

- Domotique – application pour éteindre/allumer l'éclairage.
- Automatisme.
- Contôle industriel.

Si l'on désire mettre en place un équipement pouvant se connecter à un réseau ZigBee, il y a trois possibilités :

- Soit faire partie de la ZigBee Alliance et donc bénéficier de ses apports technologiques, notamment concernant cette pile protocolaire de communication.
- Soit reprendre un produit développé par l'un des membres de la ZigBee Alliance et disposer de la stack, spécifique à ce produit, développée par le constructeur choisi.
- Soit développer sa propre stack en accord avec les dernières spécifications disponibles. Si ce développement est effectué à des fins commerciales, il devra être validé par la ZigBee Alliance.

9.1.6. Le standard BlueTooth

BlueTooth est une technologie sans fil standardisée pour échanger des données à courte distance entre équipements fixes ou mobiles dans le cadre des réseaux personnels sans fil (WPAN) avec de hauts niveaux de sécurité. Créée par Ericsson en 1994, elle se voulait une alternative aux cables RS-232. Le standard BlueTooth est géré par le BlueTooth Special Interest Group.

Afin d'assurer une compatibilité entre tous les périphériques *Bluetooth*, la majeure partie de la pile de protocoles est définie dans la spécification. La figure suivante illustre la pile protocolaire BlueTooth. Il est à noter que les couches basses sont développées en hardware, tandis que les couches hautes sont développées en software. L'interface HCI fournit une méthode uniforme pour accéder aux couches matérielles. Son rôle de *séparation* permet un développement indépendant du matériel et du logiciel. HCI permet un transfert de données à débit maximum, soit 720 kbit/s pour la norme 1.2, et un débit trois fois plus élevé pour la norme 2.0+EDR.

Les protocoles de transport suivants sont supportés :

- *Universal Serial Bus* (USB) ;
- PC-Card ;
- RS-232 ;
- UART.

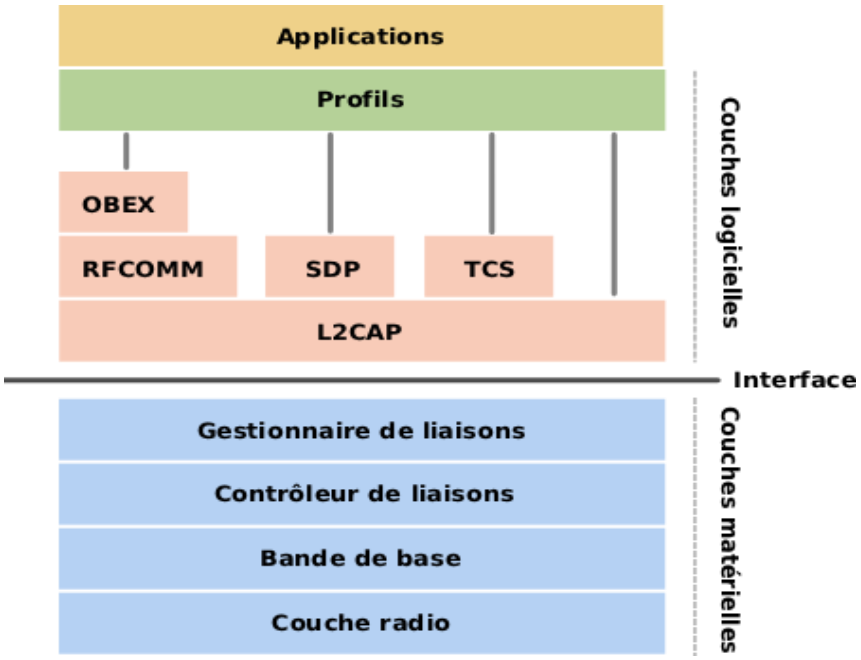

Figure 12 : La pile protocolaire BlueTooth.

9.1.6.1. Les profils

Un profil correspond à une spécification fonctionnelle d'un usage particulier. Les profils peuvent également correspondre à différents types de périphériques. Les profils ont pour but d'assurer une **interopérabilité** entre tous les appareils *Bluetooth*. Ils définissent :

- la manière d'implémenter un usage défini
- les protocoles spécifiques à utiliser
- les contraintes et les intervalles de valeurs de ces protocoles

Les différents profils sont :

1. GAP : *Generic Access Profile*
2. SDAP : *Service Discovery Application Profile*
3. SPP : *Serial Port Profile*
4. HS Profile : *Headset Profile*
5. DUN Profile : *Dial-up Networking Profile*
6. LAN Access Profile : ce profil est maintenant obsolète ; il est remplacé par le profil PAN
7. Fax Profile
8. GOEP : *Generic Object Exchange Profile*
9. SP : *Synchronization Profile*
10. OPP : *Object Push Profile*
11. FTP : *File Transfer Profile*
12. CTP : *Cordless Telephony Profile*
13. IP : *Intercom Profile*
14. A2DP : *Advanced Audio Distribution Profile* (profil de distribution audio avancée)
15. AVRCP : *Audio Video Remote Control Profile* (Commande à distance)
16. HFP : *HandsFree Profile*
17. PAN : *Personal Area Network Profile*
18. VDP : *Video Distribution Profile*
19. BIP : *Basic Imaging Profile*
20. BPP : *Basic Printing Profile*
21. SYNC : *Synchronisation Profile*
22. SAP : *SIM Access Profile*
23. PBAP : *PhoneBook Access Profile*
24. HIDP : *Human Interface Device Profile*

Deux types d'implémentation BlueTooth peuvent être distingués:

- Les implémentations générales qui mettent l'accent sur la flexibilité et la richesse des possibilités visent les PCs. Le support de profils BlueTooth supplémentaires est possible par l'ajout de drivers.
- Les implémentations pour systèmes embarqués qui sont contraintes par des ressources limitées. Des exemples sont fournis par les périphériques BlueTooth.

9.1.7. BlueTooth basse énergie

En juillet dernier, Bluetooth SIG a formellement annoncé l'adoption de *Bluetooth* Core Specification Version 4.0 incluant la technologie *Bluetooth* basse énergie. Cette nouvelle technologie, consommant beaucoup moins d'énergie (voir le tableau ci-après) est particulièrement adaptée aux équipements disposant de batterie bouton tels que les montres et les jouets. Il existe deux implémentations possibles de BlueTooth basse énergie :

- en mode dual, la fonctionnalité BlueTooth basse énergie est intégrée dans un contrôleur BlueTooth classique.
- en mode unique pour des équipements fortement intégrés et compacts fonctionnant sur batterie, dont la durée de vie visée est d'un an. Elle offre alors un mode idle consommant très peu, une découverte simple des équipements, un transfert point à multipoint fiable à faible consommation et des connexions sécurisées à moindre coût.

Les premiers produits BlueTooth basse énergie seront disponibles d'ici la fin de l'année.

Le tableau ci-dessous compare les versions classique et basse énergie de Bluetooth.

	BlueTooth classique	BlueTooth basse énergie
Fréquence radio	2,4GHz	2,4GHz
Portée radio	200m	100m
Débit max	1-3Mb/s	1Mb/s
Esclaves actifs	7	Non défini; depend de l'implémentation
Sécurité	64/128-bit et définie par l'utilisateur	128-bit AES with Counter Mode CBC-MAC et définie par l'utilisateur
Robustesse	Saut de fréquence rapide, FEC et Fast ack	Saut de fréquence rapide, Lazy Ack, 24-bit CRC, 32-bit Message Integrity Check
Latence (à partir d'un état non connecté)	100ms	6ms
Temps total pour émettre données	100ms	3ms
Certification	SIG Bluetooth	SIG Bluetooth
Transfert de voix	Oui	Non

Topologie	Scatternet	Etoile-Bus
Consommation énergétique	1 comme référence	0.01 to 0.5
Pic de consommation	<30 mA	<20 mA
Découverte de service	Oui	Oui
Concept de profil	Oui	Oui
Exemples d'utilisation	Téléphones mobiles, jeux, PCs, streaming audio, santé, sport, sécurité, industrie, etc	Téléphones mobiles, jeux, PDAs, santé, sport, domotique, automatisme, industrie, etc.

9.1.8. Le standard ISA100

ISA100 est un standard ouvert de technologies réseaux sans fil [ISA100.11a, 2009]. Il concerne les systèmes sans fil pour l'automatisation industrielle, et plus particulièrement le contrôle de process et les applications qui y sont liées.

L'objectif principal d'ISA100 est de fournir un standard unique pour les réseaux sans fil, permettant d'utiliser plusieurs protocoles et plusieurs applications. Le domaine d'ISA100 est le niveau terrain au travers d'un LAN. Le champ applicatif visé concerne surtout les applications non critiques de surveillance (de type alerte, ou de type monitoring), et dans une moindre mesure les applications de contrôle ou de sûreté. ISA100 est particulièrement adapté aux applications de monitoring périodique, et au contrôle de process lorsque des délais de 100 ms sont tolérables.

De manière générale, ISA100 offre les caractéristiques suivantes : des temps de latence supérieurs à 100 ms, la possibilité pour certains équipements d'avoir une faible consommation énergétique, le passage à l'échelle des équipements, la robustesse et la résistance aux interférences en environnement industriel sévère. ISA100 assure la coexistence avec de nombreux protocoles sans fil tels que WiFi (802.11x), WiMAX (802.16x), Bluetooth, WirelessHART, etc. ISA100 fournit aussi des services de sécurité.

9.1.8.1. Architecture et topologie

ISA100 possède une architecture comportant un réseau filaire appelé l'épine dorsale, et un (ou plusieurs) réseau(x) sans fil. ISA100 utilise plusieurs types d'entités : les routeurs de l'épine dorsale, les passerelles, les équipements sur piles avec possibilités de routage (que nous nommerons FFD), les équipements sur piles sans possibilité de routage (que nous nommerons RFD), et les capteurs sur piles. Les équipements sur piles peuvent être fixes ou mobiles.

Les routeurs de l'épine dorsale sont interconnectés entre eux et avec les passerelles au travers de l'épine dorsale. Parmi les routeurs de l'épine dorsale (ou les passerelles), se trouvent des routeurs ayant les fonctionnalités de gestion du système et de gestion de la sécurité. Toutes les autres entités sont des équipements sans fil et sur piles. Ces équipements s'auto-organisent

selon les deux topologies permises dans ISA100 : la topologie en étoile et la topologie maillée.

Dans une topologie en étoile, tous les équipements sont associés à un FFD ou à une passerelle, via un seul saut. Cette topologie est privilégiée lorsque le délai est la métrique principale.

Dans une topologie maillée, les RFD et les capteurs s'associent chacun à un ou plusieurs FFD. Les FFD s'associent chacun à d'autres FFD et à des passerelles. Cette topologie est privilégiée lorsque la fiabilité est la métrique principale. En effet, les données peuvent suivre plusieurs chemins, ce qui permet de lutter contre les ruptures de liens sans fil.

9.1.8.2. Couches basses (physique et MAC)

ISA100 se base sur les couches basses définies dans 802.15.4 (norme 2006) à 2.4 GHz. Cette couche physique offre un débit théorique de l'ordre de 250 kbps. Comme 802.15.4, ISA100 utilise un mécanisme d'acquittements et de retransmissions pour lutter contre les pertes, et un mécanisme d'écoute du canal pour éviter les collisions.

ISA100 construit une nouvelle couche liaison de données au-dessus de la couche MAC de 802.15.4. Cette couche liaison de données est responsable de la gestion de la topologie, du saut de fréquences, et de la sécurité à un saut.

Le saut de fréquences est utilisé pour lutter contre les interférences, et pour favoriser la coexistence avec d'autres protocoles fonctionnant dans la même bande de fréquences.

La sécurité à un saut permet d'éviter les attaques venant d'agents extérieurs au réseau. Elle est réalisée au moyen de clés qui peuvent être symétriques ou asymétriques. La sécurité à un saut fournit des services de confidentialité, d'intégrité et d'authentification. Ces services peuvent être fournis indépendemment.

9.1.8.3. Couches intermédiaires (réseau et transport)

ISA100 se base sur le protocole réseau IPv6, et sur les protocoles de transport TCP et UDP.

ISA100 fournit un mécanisme de sécurité de bout en bout, permettant de garantir l'authentification, la confidentialité et l'autorisation. Ces services peuvent être réalisés indépendemment. Ils protègent contre les agents internes disposant des clés du système, et pouvant donc intercepter les communications sécurisées à un saut.

9.1.8.4. Couches hautes (application)

ISA100 permet le déploiement de plusieurs applications et profils applicatifs. ISA100 définit une unique couche applicative supportant le tunneling. ISA100 présente aux applications supérieures des points d'entrée applicatifs auxquels il est possible de se connecter.

En pratique, les informations qui parviennent à la couche transport sont démultiplexées au niveau de la couche applicative d'ISA100, qui les redirige vers le point d'entrée applicatif correspondant.

9.1.9. Le standard WirelessHart

WirelessHart est un standard industriel qui vise à assurer une solution sans fil pour les réseaux de capteurs sans fil utilisés dans des applications ayant de fortes contraintes temporelles. WirelessHart a adopté un mécanisme de sauts de fréquences qui lui permet de résister aux interférences et aux effets des obstacles qui sont deux caractéristiques essentielles d'un environnement industriel.

La pile protocolaire d'un réseau WirelessHart est constituée de 5 couches : une couche physique, une couche MAC, une couche réseau, une couche transport et une couche application. Une entité spécifique appelée *Network Manager* prend en charge la constitution des tables de routage des nœuds du réseau et le séquencement des échanges TDMA.

Un réseau WirelessHart est constitué essentiellement de 4 éléments : Les entités capteurs ou actionneurs, une entité mobile appelée *Handheld* responsable de la configuration et du calibrage des autres entités, une passerelle qui connecte les entités du réseau de capteurs aux postes de contrôle et de surveillance, et le *Network Manager* qui est responsable de la configuration du réseau, de son séquencement et de la gestion des communications entre les différentes entités.

9.1.9.1. La couche physique :

La couche physique est celle de la norme IEEE 802.15.4. Le débit est de 250 kbits/s dans la bande de fréquences ISM 2400-2483,5 MHz. Ceci permet d'utiliser 16 canaux différents séparés de 5 MHz entre eux.

9.1.9.2. La couche MAC :

Par-dessus cette couche physique, contrairement à ZigBee, WirelessHart a défini la couche MAC en adoptant une méthode TDMA et un mécanisme de sauts de fréquences qui nécessitent une synchronisation globale du réseau. L'accès TDMA assure des envois déterministes et sans collision. Des slots de temps de 10 ms chacun sont regroupés en *superframes* périodiques.

Le network manager envoie à tous les nœuds du réseau un tableau qui leur donne la fréquence à utiliser durant un slot donné. L'administrateur du réseau est capable d'interdire l'utilisation des fréquences affectées par de fortes interférences, cette liste de fréquences s'appelle *blacklist*.

9.1.9.3. Les couches réseau et transport :

Au niveau 3, WirelessHart assure un routage mesh qui tente d'éviter les obstacles. Le network manager envoie à l'ensemble des nœuds du réseau un graphe qui indique tous les liens possibles dans le réseau. Chaque nœud du réseau est capable de jouer le rôle d'un routeur.

Deux protocoles de routage sont définis dans WirelessHart : Un routage par graphe où chaque nœud sur le chemin vers la destination finale calcule le prochain saut, et un routage par source où la source du paquet spécifie le chemin complet dans l'entête.

9.1.9.4. La couche application :

Le rôle de la couche application est essentiellement de définir les différentes commandes, réponses et les différents types de données. A la réception d'une commande durant une communication entre la passerelle et une autre entité, la couche application récupère le contenu et génère une réponse.

9.1.9.5. La sécurité :

WirelessHart emploie 2 niveaux de sécurité : une sécurité saut par saut au niveau de la couche MAC en utilisant les MIC *(Message Integrity Code)* basé sur CCM* *(Counter with CBC-MAC)* mode avec AES 128, et une sécurité de bout en bout au niveau de la couche réseau en utilisant 4 types de clés :

- les clés publiques, utilisées par les entités souhaitant rejoindre le réseau pour générer les MIC.
- les clés de réseau, partagées par toutes les entités déjà associées au réseau pour générer les MIC.
- les clés de *Join*, uniques par entité et utilisées par les nouvelles entités pour s'authentifier auprès du Network Manager.
- les clés de session, uniques par communication de bout en bout et générées par le Network Manager pour assurer la confidentialité et l'intégrité des données.

9.1.10. La norme 6LowPan

Jusqu'à peu, l'utilisation du protocole IP sur des réseaux sans fil embarqué était considérée comme non viable. En effet, il était très difficile d'adapter le protocole IP pour opérer sur des microcontrôleurs et sur des liaisons à basse consommation d'énergie.

L'émergence du standard 6LoWPAN de l'IETF pour des communications IP sur des liaisons radio à faible puissance a changé la donne.

9.1.10.1. Le besoin d'une alternative IP:

Un des avantages du protocole IP est qu'il est fortement adopté dans le milieu commercial, possède un cycle de développement assez rapide et assure une interopérabilité entre les équipements des différents constructeurs.

IP est facile à intégrer et assure une interopérabilité mondiale, cependant, le protocole suscite des interrogations concernant les failles de sécurité qu'il pourrait comporter. De plus, IP était considéré comme inapproprié pour une utilisation dans des réseaux embarqués sans fil parce que la taille du protocole ne pouvait pas être réduite pour opérer sur des microcontrôleurs ou des liaisons à faible puissance tel que l'IEEE 802.15.4.

Les paquets IEEE 802.15.4 sont de petite taille et la pile protocolaire entière doit tenir dans un espace mémoire assez réduit (architecture embarquée). Cependant, le bénéfice d'opérer sur un protocole IP au lieu d'opérer directement sur un type de lien particulier devient apparent lorsqu'on s'intéresse à l'interconnexion des réseaux et à leur interopérabilité.

De plus, le WiFi (IEEE 802.11) s'est imposé comme le réseau sans fil dominant pour les ordinateurs, les ordinateurs portables, les PDA…etc. Une fois la sécurisation de la liaison sans

fil mise en place grâce au WPA (*WiFi Protected Access*), cette technologie a connu une forte pénétration dans les environnements industriels. Cependant, en raison de sa consommation d'énergie très élevée, le WiFi a été adopté pour des équipements alimentés en électricité ou rechargeables quotidiennement.

En 2007, l'IETF a complété le standard 6LoWPAN (RFC 4944) pour des communications IPv6 sur un lien IEEE 802.15.4. Ce standard permet d'étendre les communications IP à des équipements à faible consommation d'énergie et géographiquement dispersés.

6LoWPAN est un standard qui fournit un schéma de compression des entêtes IP afin de permettre l'encapsulation d'un paquet IP dans la trame de la couche MAC.

9.1.10.2. Architecture protocolaire

L'architecture protocolaire est définie en couches. Le protocole IP réside au niveau de la couche 3 permettant à une variété d'applications d'utiliser une variété de liens de communication pouvant être offerts par différentes technologies physiques et MAC.

Les applications se trouvent à un niveau très élevé d'abstraction et utilisent des protocoles de transport (principalement TCP ou UDP) afin d'acheminer leurs données et ce, sans se préoccuper du type de liaison utilisée.

Cette indépendance du lien physique offerte par le protocole IP est la raison principale de sa pertinence et de son taux de pénétration.

Afin de migrer les réseaux de capteurs des PAN (*Personal Area Network*) vers LoWPAN (*Low-power Wireless Personal Area Network*) l'IEEE a défini en 2003 le standard 802.15.4. Ce standard spécifie la couche MAC et physique pour la création de réseaux personnels sans fil à faible débit et à faible consommation d'énergie.

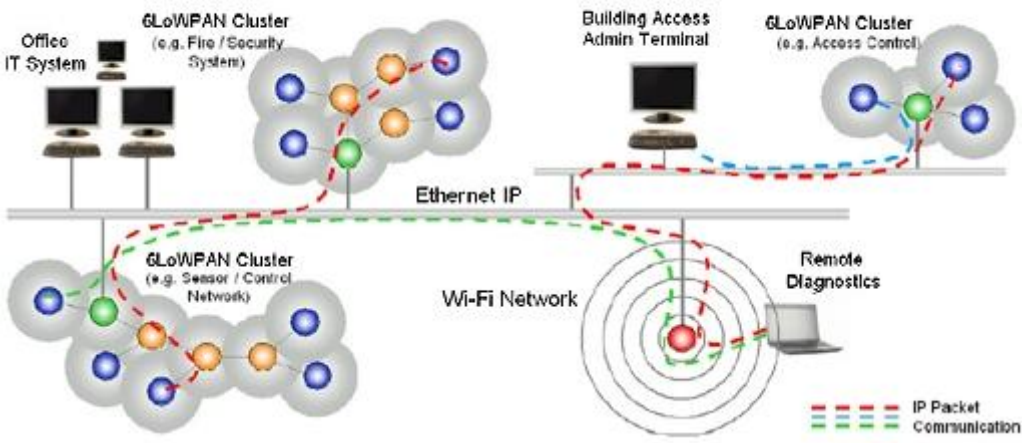

Figure 13 : Intégration des réseaux 6LoWPAN avec les réseaux existants.

Actuellement, il existe des réseaux de capteurs sans fil mais qui ne se basent pas sur le protocole IP tel que ZigBee. 6LoWPAN permet à un nœud capteur de communiquer en IP en

plaçant une couche d'adaptation au dessus de la couche MAC IEEE 802.15.4 afin de réaliser des fonctions de fragmentation/défragmentation, compression des entêtes IP, TCP et UDP.

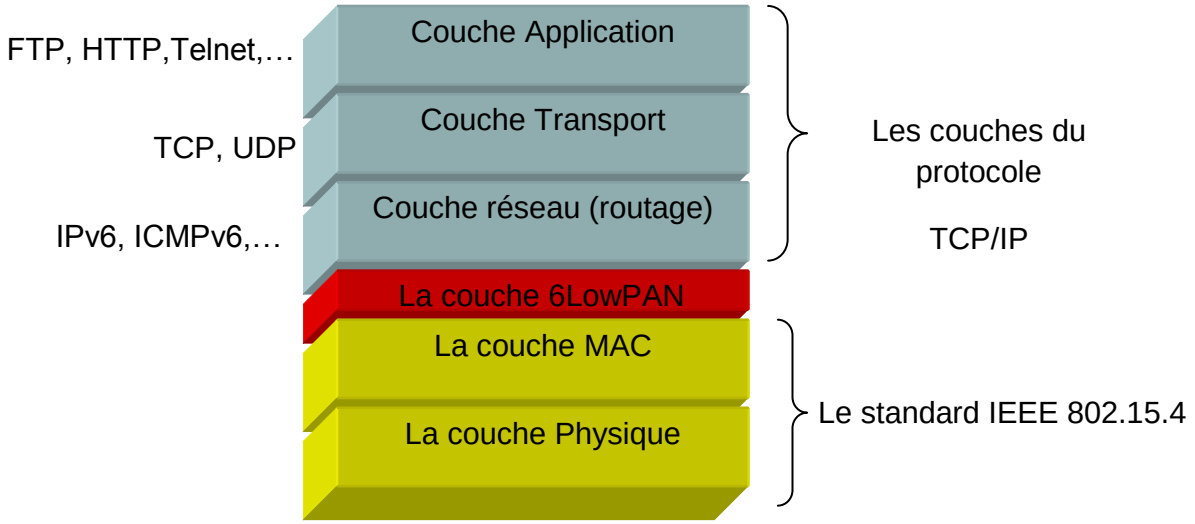

Figure 14: Position de la couche d'adaptation 6LoWPAN.

Le groupe 6LoWPAN de l'IETF a été chargé de définir la façon de transporter des paquets IP sur des trames IEEE 802.15.4 tout en assurant une interopérabilité avec les autres réseaux IP existants.

Ce standard permet aux nœuds 6LoWPAN, en plus de communiquer entre eux, de communiquer avec les ordinateurs et les périphériques IP déjà existants. Ainsi, le besoin de passerelles complexes et spécifiques aux applications est éliminé. De plus, les standards basés sur le protocole IP qui ont été développés durant des années afin de fournir des communications sécurisées peuvent être réutilisés.

Malheureusement, l'utilité du protocole IP n'est pas totalement gratuite, les paquets IP contiennent des adresses longues, des entêtes trop volumineux pour être contenues dans une trame IEEE 802.15.4 de 127 octets. Afin de rendre possible les communications IPv6 sur des liaisons 802.15.4, le groupe de travail 6LoWPAN a suggéré l'ajout d'une couche d'adaptation entre la couche IP et la couche MAC et qui permet d'effectuer une compression des entête IP, TCP et UDP et la fragmentation des paquets IP.

Pour la compression de l'entête IP, 6LoWPAN définit un schéma de compression pour les communications IPv6 de type lien local. Les informations pouvant êtres déduites de l'entête de la couche liaison sont tout simplement supprimées de l'entête IP, par exemple : les adresses source et destination. Les champs ne pouvant pas être déduits sont compressés en quelques bits afin de réduire au maximum la taille de l'entête.

La fragmentation est un autre mécanisme fourni par la couche d'adaptation 6LoWPAN. Quand le paquet IPv6 dépasse la taille du champ donnée de la trame MAC, les paquets sont fragmentés à la source et réassemblés à la destination.

Dans le but de supporter la transmission de paquets IPv6 sur la couche liaison, la couche d'adaptation peut utiliser des adresses du niveau liaison. Alternativement, la couche IPv6 peut se baser sur cette capacité pour réaliser un routage intra-PAN.

Pour accomplir une transmission multi sauts, 6LoWPAN définit l'entête Mesh. L'entête Mesh est utilisé afin de standardiser la façon d'encoder le champ « hop limit » ainsi que les adresses MAC source et destination du paquet.

Le standard 6LoWPAN permet d'insérer des entêtes à la demande selon les besoins. La figure ci-dessous présente les entêtes pouvant êtres insérés par la couche d'adaptation.

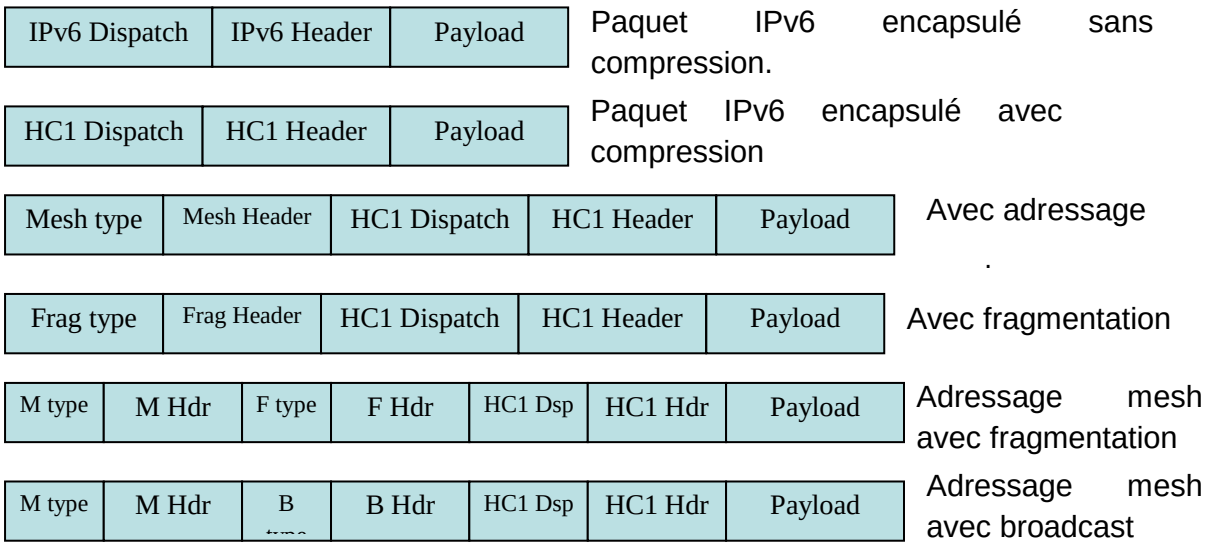

Figure 15 : ***Formats de paquets 6LoWPAN.***

9.1.11. WiFi Low Power

WiFi désigne aujourd'hui une solution « Réseau Local Sans Fil » (WLAN) qui a évolué selon différentes versions depuis une vingtaine d'années. Si l'on retient le débit, la portée et la consommation comme paramètres essentiels pour parler des différentes étapes de cette évolution, nous pouvons constater certaines tendances, celles qui nous intéressent le plus ici sont relatives à la consommation.

A l'origine, cette gamme de solutions réseau est née de la norme IEEE 802.11 qui a évolué par amendements ou a été remplacée par de nouvelles versions comme 802.11a, 802.11b, 802.11n… WiFi représente à l'origine une certification d'interopérabilité, avec le temps ce mot désigne plus globalement ce type de réseaux.

9.1.11.1. Concernant le débit :

A l'origine le débit instantané était de 1 et 2 Mbits/s, la version 802.11b a permis dans la même bande de fréquences de passer à 11 Mbits/s ce qui reste une grandeur représentative de l'offre, ce débit est toujours pratiqué aujourd'hui. La version 802.11n est beaucoup plus ambitieuse à ce niveau car le débit instantané s'exprime en centaine de Mbits/s. Rappelons que d'une part le débit peut s'adapter aux conditions de propagation (Notamment chuter quand la distance entre les stations augmente) et que d'autre part, les chiffres donnés ici pour

le débit instantané servent à définir une bande passante qui est partagée entre les stations (Ainsi pour un réseau à 11 Mbits/s une station ne dispose au mieux que de la moitié de ce débit et beaucoup moins si ce réseau est chargé). La tendance est donc d'aller vers des débits de plus en plus importants notamment en changeant le mode de modulation.

9.1.11.2. Concernant la portée.

Si nous laissons à la solution la capacité d'adapter son débit aux circonstances, les deux grandeurs typiques à retenir sont jusqu'à 300 m en extérieur non obstrué et de l'ordre de quelques dizaines de mètres en intérieur (50 m par exemple). Les conditions de propagations en intérieur étant à la fois variables et complexes, exprimer une limite représentative n'a pas de sens : l'environnement peut se comporter comme un guide pour l'onde radio (effet de canyon, pour un couloir par exemple) ou comme un écran (effet d'ombre, pour une machine outil en métal). Sauf aménagements particuliers, ces deux chiffres restent représentatifs à travers les évolutions des solutions WiFi. Ceci s'explique par le fait que ces normes supportent une couverture cellulaire (3 canaux indépendants pour 802.11b, 8 pour 802.11a qui offre 54 Mbits/s mais moins de portée). Dans ce cas, des cellules trop grandes offriraient moins de bande passante aux stations du réseau. La portée n'est donc généralement pas un véritable objectif.

9.1.11.3. Concernant la consommation.

C'est le paramètre critique dès qu'il s'agit de considérer WiFi comme une solution potentielle pour des réseaux de capteurs.

Il est possible de distinguer aujourd'hui trois tendances quand il s'agit de juger des progrès dans ce domaine. Rappelons qu'un des principes des télécommunications peut se résumer à : La capacité de décodage d'une information reçue d'une onde radio est fonction du rapport de l'énergie reçue par bit (ou par symbole) sur l'énergie du bruit dans la bande passante considérée. Il est rare de pouvoir agir sur le bruit radio ambiant, une augmentation de débit se traduit donc le plus souvent par une augmentation de la puissance émise donc de la consommation de la solution.

9.1.11.4. Tendance impulsée par les smartphones

Une tendance forte vient du marché très tonic des smartphones. Dans ce domaine le challenge de la consommation est couplé avec celui de l'encombrement de la solution. Il faut à la fois réduire les puissances manipulées et le nombre de composants. Pour ce faire Broadcom a mis au point un composant composite (a combo device) qui, par le biais de mise en commun de modules, est capable de supporter soit LP WiFi soit BT (Bluetooth). Il s'agit du BCM4329. Cette stratégie a été aussi suivie par Atheros, qui a une solution combo équivalente avec son composant AR9002WB-1NGB.

Les chiffres sur la consommation ne sont pas facilement accessibles, néanmoins le challenge n'étant pas d'offrir du bas débit avec une autonomie exprimée en années. Cette piste n'a pas beaucoup d'intérêt dans l'univers des réseaux de capteurs.

9.1.11.5. Tendance impulsée par la version n

Les objectifs et les innovations de la version n de 802.11 sont composites. Cette version intègre à la fois de nouvelles modulations, des optimisations protocolaires (Technologie MIMO, concaténation de trames,..) et l'économie d'énergie n'est pas la principale priorité. Il est évoqué à plusieurs reprises dans la littérature qu'un point d'accès 80211 n consomme plus qu'un a/b/g. Les efforts de consommation sont là pour amortir le surcoût en énergie demandé par les innovations en débits, portée, etc.

Nous pouvons retenir l'idée qu'il s'agit de consommer, avec cette nouvelle version, pas plus qu'avec les anciennes moins performantes selon d'autres critères. Là encore, l'objectif ne coïncide pas avec les ambitions généralement associées aux réseaux de capteurs.

9.1.11.6. Tendance impulsée par le marché des réseaux de capteurs.

Depuis 2009, l'idée de réutiliser la technologie WiFi dans un mode dégradé en débit pour les réseaux de capteurs fait son chemin et des composants dédiés à ce type d'applications sont annoncés. Des efforts pour économiser l'énergie sont faits à partir de la version 802.11b, la solution repose sur un état de sommeil particulièrement sobre, une activité d'émission très peu fréquente et des débits instantanés offerts limités à 1 ou 2 Mbits/s. L'ambition en termes d'autonomie est généralement annoncée par une durée de vie de 5 ans.

De telles solutions ont été proposées par G2 Microsystems pour des stations dont la production de données est plutôt de type périodique. Des durées de vie de plusieurs années à partir d'une pile AA sont envisagées si les données sont produites toutes les 40 secondes par exemple. Cette espérance est entretenue à partir d'un niveau très faible de consommation dans l'état « sleep » (10 µA).

Il en est de même pour RF Monolithics, Inc qui a annoncé le WSN802G : un composant WiFi travaillant à 1 ou 2 Mbits/s (compatible avec les versions b et g de WiFi) et intégrant un état actif et un état sommeil optimisés en énergie. L'ambition étant une autonomie maximale estimée à 5 ans.

9.1.12. WiDom

Dans les réseaux filaires, les messages peuvent êtres organisés efficacement en utilisant le bus CAN. Le CAN possède une couche MAC qui permet des transmissions sans collisions et permet d'implémenter une priorité pour l'émission des messages. Ainsi, il est possible, connaissant les caractéristiques du message (période, temps de transmission, gigue…etc.), de calculer le délai maximum d'un message, en l'absence de perte.

Ce protocole de niveau MAC appartient à une famille de protocole appelé protocole à bit dominant. L'émission d'une trame commence par l'émission de son identifiant d'objet. Les collisions sont résolues par un principe de « bit dominant » : si une station émet un '1' pendant qu'une autre émet un '0', c'est le '0' qui est transmis sur le support. La station qui a émis le 1 voit qu'elle n'est pas seule, qu'elle n'est pas la plus prioritaire et cesse d'émettre.

9.1.12.1. Principe:

La principale idée de WiDom est qu'un message se voit assigner une priorité statique. Pour tout message souhaitant accéder au canal, un tournoi est effectué en fonction de la priorité du message, le message de plus haute priorité est transmis en premier.

Dans l'état initial, le protocole attend l'arrivée d'un message dans la file d'attente. Ensuite, le protocole attend durant un long temps d'inactivité avant de transmettre une impulsion servant de point de référence temporelle pour tous les nœuds.

Un nœud dépile le message de plus haute priorité se trouvant dans sa pile et effectue le tournoi. Si le nœud perd, il continue d'écouter le canal afin de savoir qui a gagné le droit de transmettre et pour recevoir le message qui lui est éventuellement destiné.

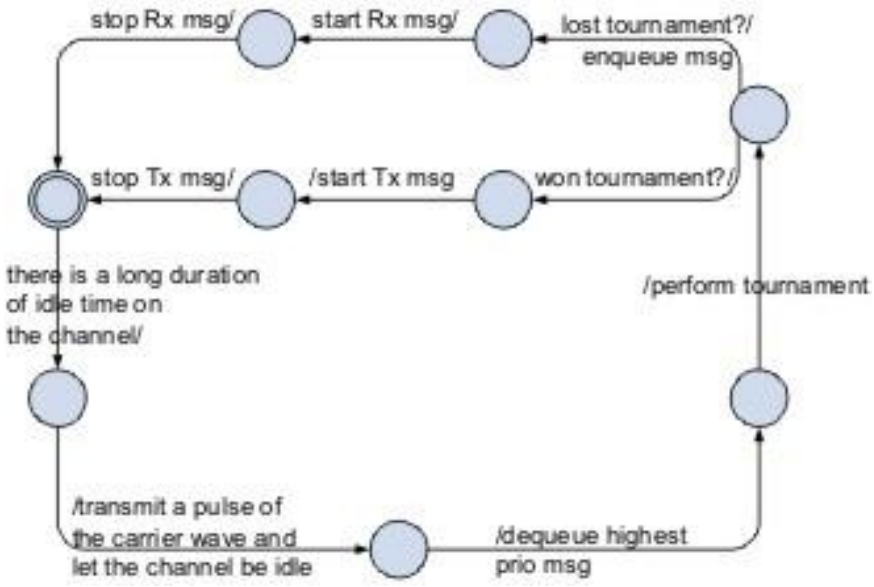

Figure 16 : Principe du protocole