

---

# **ZigBee Documentation**

*Version 0.1*

**Rémy HUBSCHER**

**sept. 27, 2017**



---

## Table des matières

---

<b>1</b>	<b>Sommaire</b>	<b>3</b>
1.1	Concepts de base des réseaux sans fil . . . . .	3
1.1.1	Qu'est-ce qu'un réseau sans fil ? . . . . .	3
1.1.2	Les catégories de réseaux . . . . .	4
1.1.2.1	L'organisme Américain — <b>IEEE</b> . . . . .	4
1.1.2.2	L'organisme Européen — <b>CEPT</b> . . . . .	4
1.1.2.3	Réseaux personnels sans fil (WPAN) . . . . .	5
1.1.2.3.1	Bluetooth . . . . .	5
1.1.2.3.2	HomeRF . . . . .	5
1.1.2.3.3	ZigBee . . . . .	6
1.1.2.3.4	irDA . . . . .	6
1.1.2.4	Réseaux locaux sans fil (WLAN) . . . . .	6
1.1.2.4.1	Wifi . . . . .	6
1.1.2.4.2	HiperLAN2 . . . . .	7
1.1.2.5	Réseaux métropolitains sans fil (WMAN) . . . . .	7
1.1.2.5.1	WiMAX . . . . .	7
1.1.2.6	Réseaux étendus sans fil (WWAN) . . . . .	7
1.2	Bandes de fréquences . . . . .	7
1.2.1	Bande industrielle, scientifique et médicale . . . . .	8
1.2.1.1	Le besoin . . . . .	8
1.2.1.2	Les usages . . . . .	8
<b>2</b>	<b>Bibliographie</b>	<b>9</b>



**Note :** Ce cours est collaboratif, n'hésitez pas à participer à sa rédaction, corriger une faute, ajouter une précision ou une partie oubliée. <https://github.com/Natim/zigbee>

---

ZigBee est un protocole de communication haut niveau permettant la communication sans fil entre deux radios à consommation réduite.

Le protocole est basé sur la norme IEEE 802.15.4 pour les réseaux à dimension personnelle. (WPAN)

La ZigBee Alliance a ratifié les spécifications de ZigBee 1.0 le 14 décembre 2004.

Dans la suite de ce cours, je vous propose d'entrer dans les détails pour comprendre la nécessité de cette norme, ses enjeux et outils à l'heure de l'Internet des Objets.

Nous entrerons également dans le vif du sujet en réalisant des prototypes d'objets connectés communiquants à l'aide du protocole ZigBee.



## Concepts de base des réseaux sans fil

### Qu'est-ce qu'un réseau sans fil ?

Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux (ordinateur portable, PDA, etc.) peuvent communiquer sans liaison filaire.

Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

---

**Note :** *Remarque concernant l'orthographe des réseaux sans fil*

Malgré l'utilisation de "sans fil", communément admise, les orthographes exactes sont « sans fil » et « sans-fil ». On parle ainsi de « réseau sans fil » ou bien « du sans-fil ». Les réseaux sans fil sont basés sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies.

En contrepartie se pose le problème de la réglementation relative aux transmissions radio-électriques. En effet, les transmissions radio-électriques servent pour un grand nombre d'applications (militaires, scientifiques, amateurs, ...), mais sont sensibles aux interférences, c'est la raison pour laquelle une réglementation est nécessaire dans chaque pays afin de définir les plages de fréquence et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation.

De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair (c'est le cas par défaut). Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil.

## Les catégories de réseaux

On distingue plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité. (appelée zone de couverture).

Deux organismes principaux gèrent la normalisation des réseaux et les bandes de fréquences attribuées aux réseaux sans fil.

### L'organisme Américain — IEEE

Le centre **IEEE** (*Institute of Electrical and Electronics Engineers*), associé à la **FCC** ; l'organisme européen est **L'ETSI** (*European Telecommunications Standards Institute*). Une fois les normes établies, des commissions distribuent ces fréquences aux utilisateurs selon la taille du réseau créé.

Il distingue les catégories suivantes :

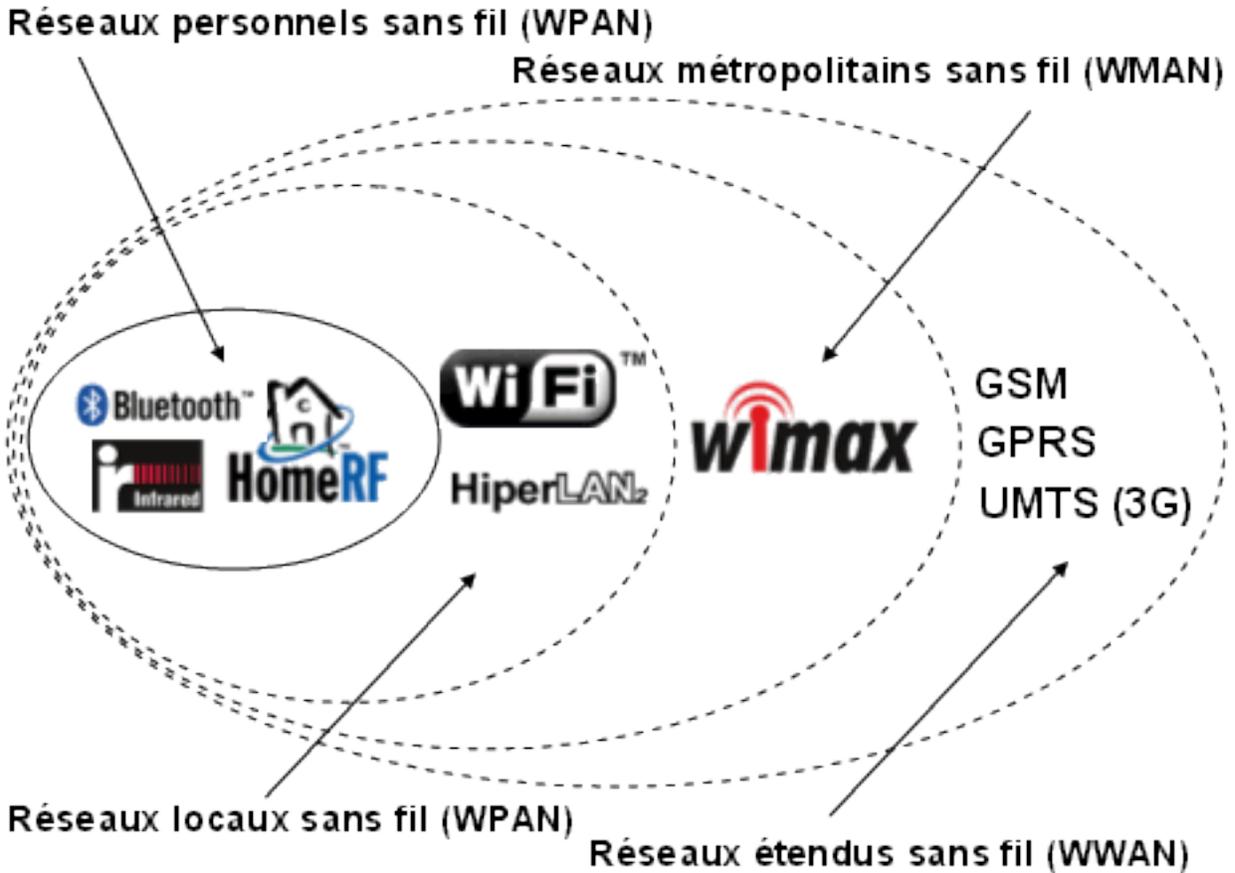
- **PAN** : Personal Area Network
- **LAN** : Local Area Network
- **MAN** : Metropolitan Area Network
- **WAN** : Wide Area Network
- **RAN** : Rural Area Network

### L'organisme Européen — CEPT

Du côté européen, pour les mêmes types de réseaux, la **CEPT** (*Conférence Européenne des Postes et Télécommunications*) organise les fréquences de cette manière :

- **PAN** : Personal Area Network
- **LAN** : Local Area Network
- **MAN** : Metropolitan Area Network
- **WAN** : Wide Area Network

En France c'est l'ARCEP qui gère la distribution et la vente éventuelle des fréquences radio.



### Réseaux personnels sans fil (WPAN)

Le *réseau personnel sans fil* (appelé également *réseau individuel sans fil* ou *réseau domestique sans fil* et noté **WPAN** pour *Wireless Personal Area Network*) concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :

#### Bluetooth

La principale technologie WPAN est la technologie **Bluetooth**, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres. Bluetooth, connue aussi sous le nom *IEEE 802.15.1*, possède l'avantage d'être très peu gourmande en énergie, ce qui la rend particulièrement adaptée à une utilisation au sein de petits périphériques.

#### HomeRF

**HomeRF** (pour *Home Radio Frequency*), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été

abandonnée en Janvier 2003, notamment car les fondateurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie *Centrino*, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

### ZigBee

La technologie **ZigBee** (aussi connue sous le nom *IEEE 802.15.4*) permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). La technologie ZigBee, opérant sur la bande de fréquences des 2,4 GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.



### irDA

Enfin les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. L'association irDA (infrared data association) formée en 1995 regroupe plus de 150 membres.



### Réseaux locaux sans fil (WLAN)

Le *réseau local sans fil* (noté **WLAN** pour *Wireless Local Area Network*) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

### Wifi

Le Wifi (ou IEEE 802.11) soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

## HiperLAN2

**HiperLAN2** (*High Performance Radio LAN 2.0*), norme européenne élaborée par l'ETSI (*European Telecommunications Standards Institute*). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5150 MHz et 5300 MHz.

## Réseaux métropolitains sans fil (WMAN)

Le *réseau métropolitain sans fil* (**WMAN** pour *Wireless Metropolitan Area Network*) est connu sous le nom de **Boucle Locale Radio** (BLR). Les WMAN sont basés sur la norme *IEEE 802.16*. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

La norme de réseau métropolitain sans fil la plus connue est le WiMAX, permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs dizaines de kilomètres.

## WiMAX

**WiMAX** (*Worldwide Interoperability for Microwave Access*), IEEE 802.16 c'est un label délivré par le *WiMAX forum* aux équipements respectants la norme.

Le WiMAX a été créé par les sociétés Intel et Alvarion en 2002.

## Réseaux étendus sans fil (WWAN)

Le *réseau étendu sans fil* (**WWAN** pour *Wireless Wide Area Network*) est également connu sous le nom de *réseau cellulaire mobile*. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :

- GSM (2G) : 9,05 Kbps
- GPRS (2.5G) : 171,2 Kbps
- EDGE (2.75G) : 383 Kbps
- UMTS (3G) : 1.9 Mbps
- HSDPA (3G+) : 14.4Mbps
- LTE-Advanced (4G) : 1Gbps / 100Mbps

## Bandes de fréquences

Les **bandes ISM** (*industriel, scientifique, et médical*) sont des bandes de fréquences qui peuvent être utilisées, pour des applications industrielles, scientifiques, médicales, domestiques ou similaire, à l'exception des applications de radiocommunication, sans demande d'autorisation auprès des autorités.

Pour l'Union européenne, les bandes de fréquences, et éventuels niveaux limites, sont définis dans la norme **EN 55011**.

Pour les USA, la publication **FCC Part 18** définit ces bandes de fréquences et niveaux limites d'émission.

## Bande industrielle, scientifique et médicale

### Le besoin

- Transmission numérique de données
- Distance de 1 à 3 kms max
- Faible débit
- Souvent une alimentation à piles
- Durée de vie des piles jusqu'à 10 ans
- Faible coût (Bill of Material de quelques euros)
- Le plus souvent des bandes RF libres sans licence

### Les usages

Ils sont multiples :

- **Domotique**
  - Alarme, Éclairage
  - Chauffage et climatisation
  - Fermeture : volets et portes
- **Industrielle**
  - Détecteur (température, lumière) et commandes
  - Programmation de machines-outils
  - Télérelevage
- **Multimédia**
  - Manette de jeux, souris/clavier
  - Déport audio
  - Télécommande
- **Automobile**
  - Tire-pressure monitoring system : Porsche 959, 607, Laguna
  - Remote Keyless Entry (Clé sans fil Renault)

## CHAPITRE 2

---

### Bibliographie

---

— Les réseaux sans fils - <http://www.commentcamarche.net/contents/wireless/> - Creative Commons