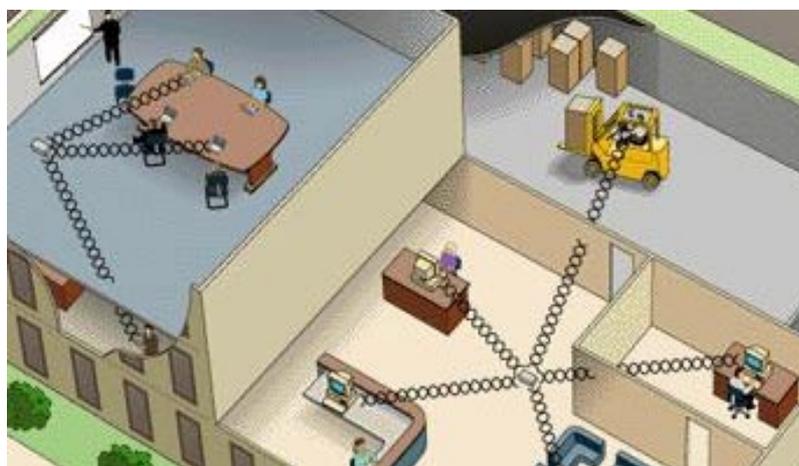




Wireless LAN :

techniques RF, Wifi, Bluetooth



jean-philippe muller

Version mai 2002

Sommaire

1. Les réseaux et la mobilité
2. Les aires d'usages des réseaux locaux
3. La place des normes IEEE802.11
4. Topologies des réseaux : le mode « infrastructure »
5. Topologies des réseaux : le mode « ad-hoc »
6. La constitution de l'interface radio
7. Les fréquences de travail
8. Les perturbations des fours à micro ondes
9. La protection contre les brouillages
10. L'étalement de spectre par saut de fréquence FHSS
11. L'étalement de spectre par code DSSS
12. Les circuits de l'émission DSSS
13. La modulation DSSS en présence de brouillage
14. La portée d'une liaison à 2,4 GHz
15. La techniques des antennes multiples
16. Le réseau sans fil : du rêve à la réalité
17. Les activités de gestion du réseau
18. Le protocole d'échanges de données
19. Les espaces entre trames
20. La protection contre les brouillages
21. Le format des trames
22. La sécurité des échanges

23. Annexe : l'émission FHSS dans le standard Bluetooth
24. Annexe : la cohabitation entre les standards
25. Annexe : le point d'accès Wifi Ericsson
26. Annexe : le chipset Prism d'Intersil

27. Quelques sites utiles

1- Les réseaux et la mobilité

L'informatique mobile permet aux utilisateurs de se déplacer tout en restant connectés au réseau, il leur devient donc possible d'accéder à leur environnement de travail et de continuer à communiquer (par exemple par messagerie électronique).

Pour cela, les machines doivent disposer d'interfaces de communication sans fil utilisant des ondes radio fréquences ou lumineuses comme mode de transmission pour l'établissement de réseaux de données entre ordinateurs.

Le câblage n'est plus nécessaire, ce qui représente un avantage certain dans de nombreux cas :

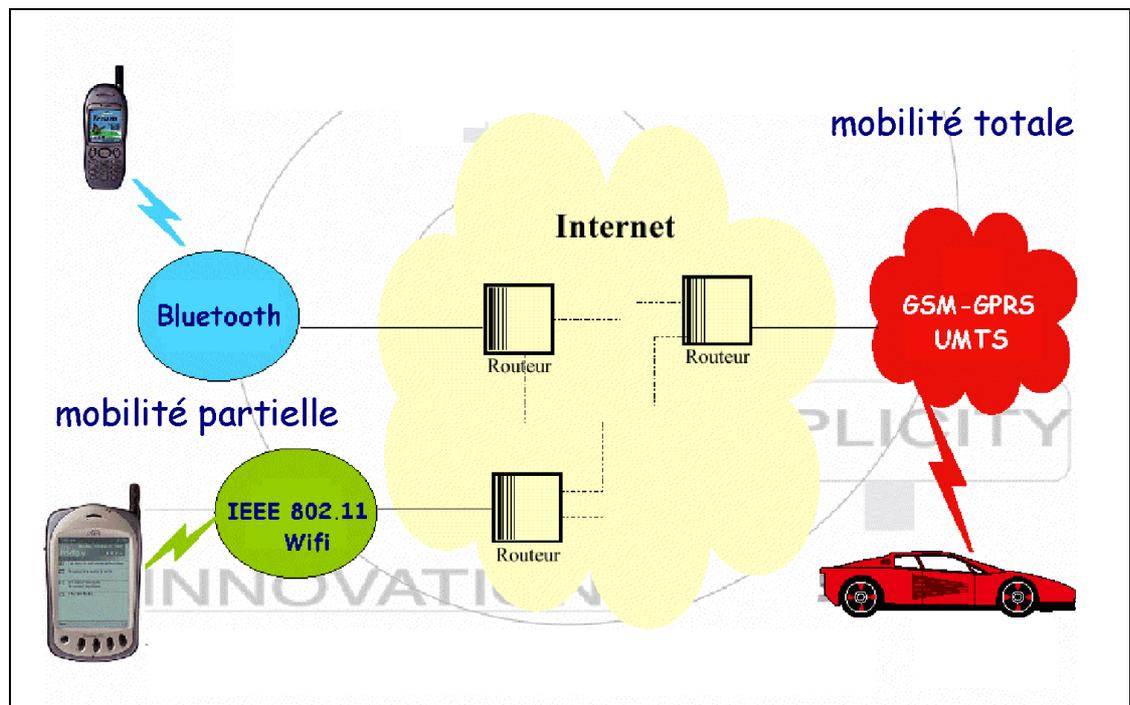
- mise en place d'un réseau dans un bâtiment classé « monument historique »
- mise en place d'un réseau de courte durée (chantiers, expositions, locaux loués, formations)
- accès aux informations enregistrées sur chaque patient pendant les visites dans les hôpitaux
- accès à une connexion Internet pour les usagers des aéroports, gares ...
- lecture de codes barres dans les supermarchés
- liaison par voie hertzienne entre deux bâtiments ayant chacun leur réseau câblé

Les opérateurs de la téléphonie mobile ont mis en œuvre un certain nombre de techniques pour permettre l'utilisation du téléphone mobile pour la transmission de données :

- abonnement « data » pour l'échange des données par GSM à 9600 bits/s (trop lent)
- augmentation du débit avec le GPRS par l'utilisation de plusieurs time-slots par trame (trop cher)
- augmentation de débit et changement de technologie avec l'UMTS (n'existe pas encore)

Mais tout le monde a fini par comprendre qu'une mobilité complète est rarement indispensable, ce qui a permis l'essor des réseaux locaux radio qui permettent une mobilité de l'utilisateur à l'intérieur d'une certaine zone de couverture.

Figure 1.
Les réseaux
locaux et
téléphoniques.



Par leur coût d'installation réduit et leur débit offert élevé, les réseaux locaux comme Bluetooth ou Wifi se positionnent, pour beaucoup d'applications, comme de redoutables concurrents pour les opérateurs de téléphonie mobile et pourront même selon certains gêner le développement rapide de l'UMTS.

2- Les aires d'usages des réseaux locaux

⇒ WPAN (Wireless Personal Area Network)

Le téléphone mobile, le baladeur MP3, la montre, l'écharpe communicante, le PDA et bien sûr le micro-ordinateur échangent des informations entre eux, tous situés "autour" de la personne ou d'un point fixe.

Figure 2.
Le réseau
Bluetooth.



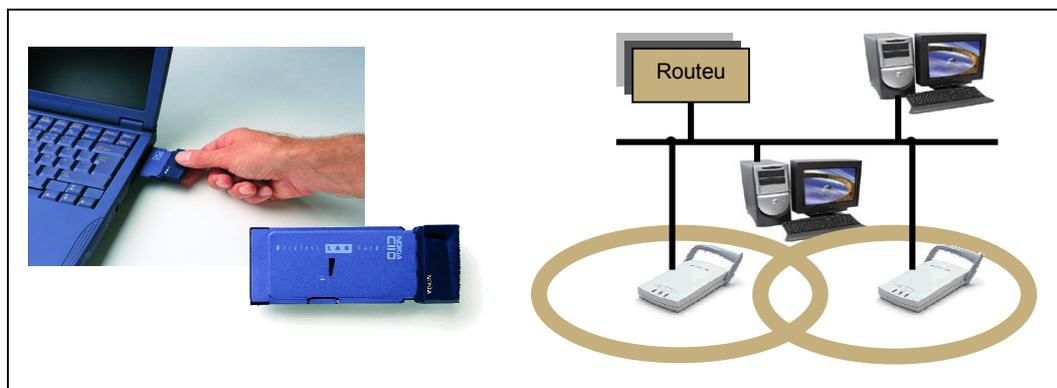
La norme **Bluetooth** lancée par Ericsson et Nokia (ainsi nommée en l'honneur du roi danois **Harald Blaatand** qui se traduit par Harald à la dent bleue) semble la mieux adaptée pour ce type de liaison et prend le pas sur la norme **HomeRF**, les premiers objets Bluetooth (téléphones, PDA...) étant d'ores et déjà disponibles.

⇒ WLAN (Wireless Local Area Networks)

Un réseau sans fil est installé dans la maison, dans l'entreprise, dans un espace public tel qu'un campus universitaire, un café, un centre de conférence, un hôtel, un aéroport... Tous les appareils situés dans la zone de couverture et dotés d'une interface réseau sans fil peuvent s'y raccorder sous réserve de disposer des autorisations nécessaires.

Les normes les plus utilisées pour ces type de réseaux sont l'**IEEE802.11b** ou **Wifi** et l'**Hiperlan**.

Figure 3.
Exemple de
réseau WLAN à
2 cellules.



Le WLAN autorise une totale mobilité sur la zone couverte, mais il ne permet pas de passer d'une cellule à une autre (couverte pas une autre borne) sans couper la liaison.

Les appareils s'échangent des informations de leur propre initiative ou sur commande de l'utilisateur. Il est possible de partager un accès Internet (ADSL, câble...) sur plusieurs machines reliées au réseau sans fil.

⇒ WMAN (Wireless Metropolitan Area Network)

Un réseau sans fil peut se tisser sur une ville, permettant à tous les habitants d'être connecté entre eux. Relié à l'Internet ou non, il permet des échanges à haut débit, entre voisins, entre entreprises, etc. Des WMAN libres et pirates se mettent en place un peu partout à Seattle, San Francisco, Portland... en Europe également, et même en France bien que la loi interdise pour le moment les réseaux de ce type.

3- La place des normes IEEE802.11

La famille des normes IEEE802.11 concerne la transmission de données par liaison radio ou infrarouge dont les caractéristiques générales ont été définies par plusieurs versions :

IEEE802.11 :

- adopté en 1997, le système est économique à installer
- avec une puissance limitée à 100 mW, son rayon d'action est de 50 à 100 m, et peut être étendu si on installe des relais (ou *nodes*)
- il offre des débits limités (1 et 2 Mbits/s), insuffisants pour la vidéo et le multimédia
- il fonctionne à 2,4 GHz avec une technique d'étalement de spectre ou par faisceau infrarouge
- utilisation d'une puissance de transmission de 100 mW ou moins, suffisante pour couvrir jusqu'à 100 mètres en intérieur, suivant les débits et la géométrie des bâtiments

IEEE802.11b ou Wifi :

- adoptée en 1999, cette nouvelle version de la norme permet de créer de véritables réseaux locaux capables d'accueillir de nombreux utilisateurs
- elle offre des débits de 1, 2, 5,5 et 11 Mbits/s pour une cellule (en fait 3 à 4 Mbits/s à se partager entre tous les utilisateurs de la cellule)

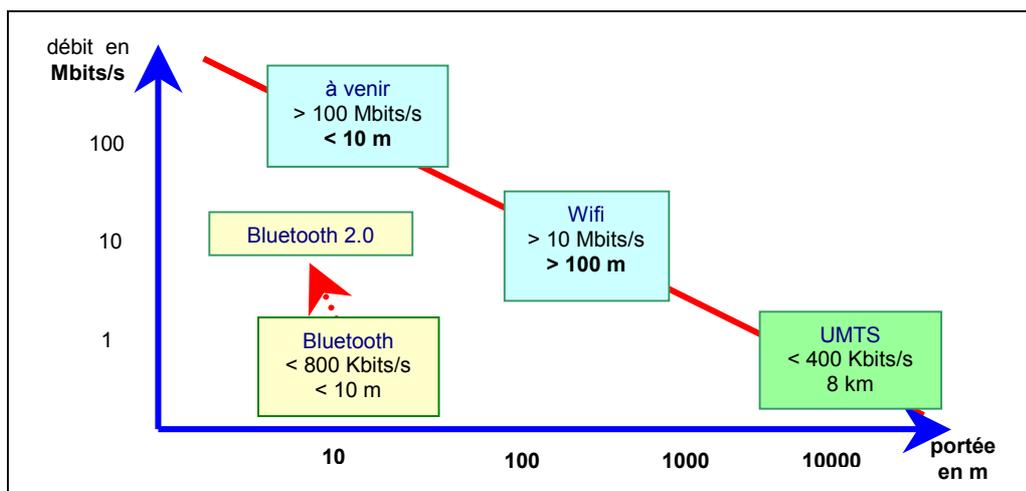
Figure 4.
Les différentes applications des réseaux radio.

	Voix	Internet	Données	Images
WPAN	DECT		Bluetooth - 1 Mbits/s	
WLAN	DECT GSM		802.11 - 1 et 2 Mbits/s 802.11b Wifi - 11 Mbits/s 802.11a - 22 Mbits/s Hiperlan - 23,5 ou 54 Mbits/s	Hiperlan
WAN	GSM UMTS	GSM - 9600 bits/s GPRS - 56 kbits/s max UMTS - 2Mbits/s max	GPRS UMTS	UMTS

IEEE802.11a et g :

- le standard 802.11g, doit permettre d'élever le débit à 54 Mbits/s, tout en restant à 2,4 GHz par l'utilisation d'un nouveau type de modulation à porteuses multiples : l'OFDM
- le 802.11a permet également des débits de 54 Mbits/s., mais devrait se situer sur la gamme de fréquence des 5 GHz, beaucoup moins encombrée que celle des 2,4 GHz

Figure 5.
La concurrence entre Wifi et Bluetooth .



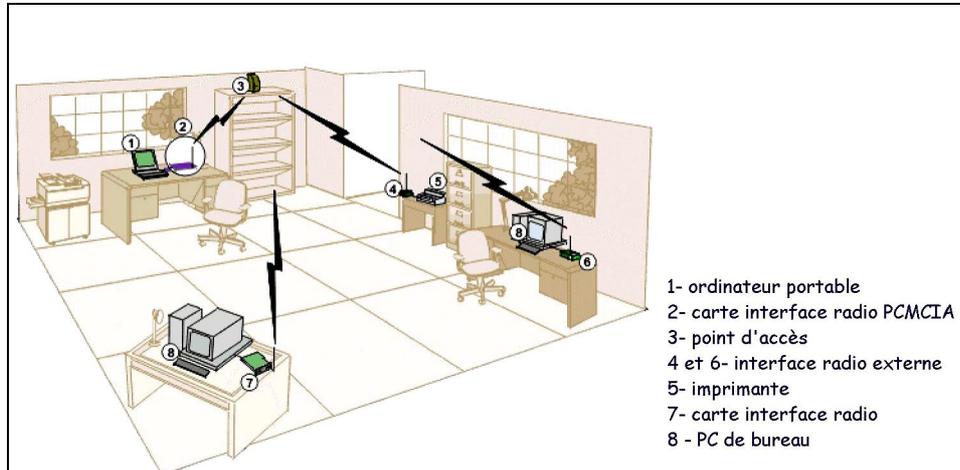
4- Topologie de réseau : le mode « infrastructure »

Les WLAN peuvent fonctionner de deux façons différentes : en mode infrastructure ou en mode ad-hoc.

Le mode infrastructure fait appel à des bornes de concentration appelées **points d'accès** qui gèrent l'ensemble des communications dans une même zone ou cellule, comme dans les réseaux GSM.

Les réseaux IEEE802.11b ou Wifi et Hiperlan fonctionnent en général selon ce mode.

Figure 6.
Les différents
éléments d'une
cellule Wifi.

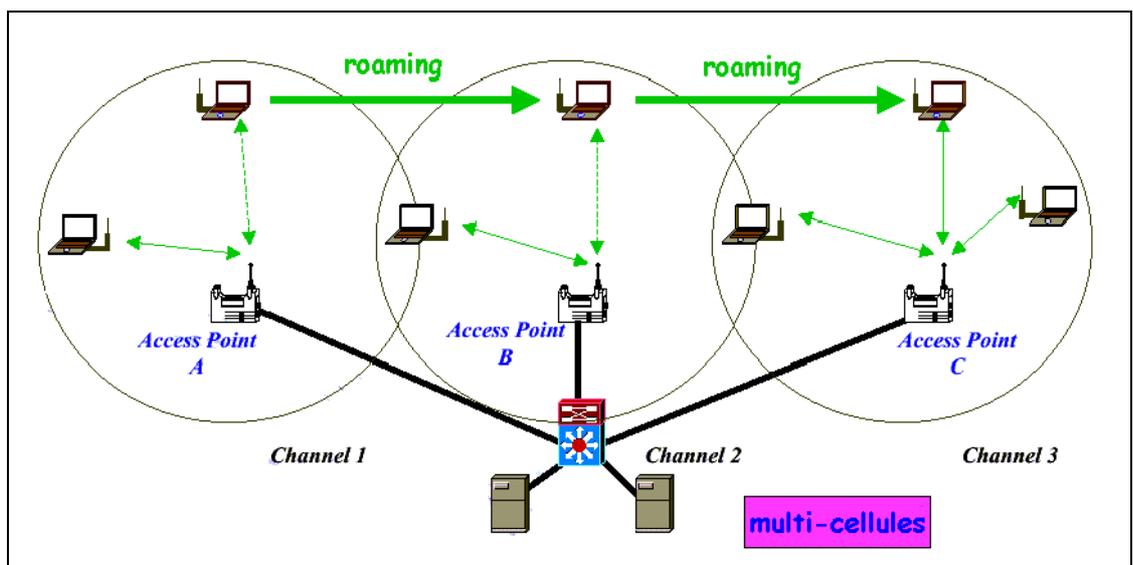


Les équipements mobiles communiquent entre eux en passant par un point d'accès, bien que dans certains cas particuliers un échange direct entre deux interfaces soit possible :

- le réseau Wifi est formé de cellules appelées BSS (Basic Service Set)
- la station de base d'une cellule est le point d'accès AP (Access Point)
- l'ensemble des cellules et de leur point d'accès est l'ESS (Extended Service Set)
- l'ESS est relié au réseau Ethernet câblé par un portail, souvent intégré dans l'AP

Dans un réseau à infrastructure et à plusieurs cellules, les bornes sont connectées entre elles par une liaison ou un réseau filaire ou hertzien. Les terminaux peuvent alors se déplacer au sein de la cellule et garder une liaison directe avec le point d'accès, ou changer de cellule, ce qui s'appelle le **roaming**.

Figure 7.
Structure d'un
réseau à
infrastructure
à 3 cellules.



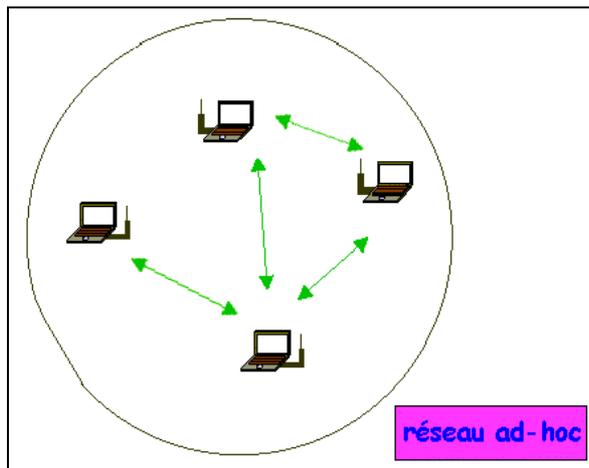
Remarque : dans certains cas, les différentes cellules se superposent complètement, ce qui permet d'offrir plusieurs fréquences aux utilisateurs de la cellule, et donc un débit plus satisfaisant.

5- Topologie de réseau : le mode « ad-hoc »

Un réseau ad-hoc est un réseau où il n'y a pas d'infrastructures fixes et le signal est transmis par l'intermédiaire des mobiles présents et routé dynamiquement :

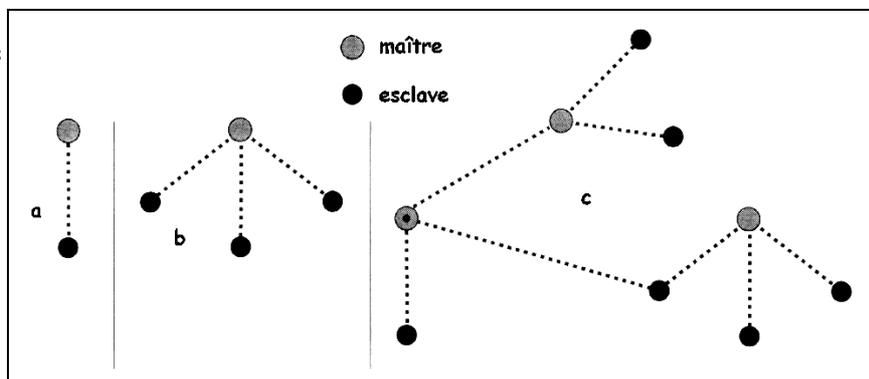
- le réseau ad hoc est auto-configurable : lorsque deux machines mobiles se retrouvent dans le même secteur géographique, elles peuvent se reconnaître puis échanger des données.
- chaque machine peut échanger des informations avec n'importe quelle autre machine
- dans le mode de fonctionnement le plus simple, (le seul implémenté dans les protocoles actuels) les nœuds peuvent échanger des données uniquement lorsqu'ils sont à portée de réception l'un par rapport à l'autre
- dans un mode de fonctionnement idéal (à venir), chaque nœud du réseau peut servir de routeur lorsque deux machines ne peuvent se joindre directement

Figure 8.
Structure d'un
réseau ad-hoc.



Bluetooth est un exemple typique de réseau ne fonctionnant qu'en mode ad-hoc. Les équipements mobiles communiquent directement entre eux par l'intermédiaire de leur interface radio avec les autres systèmes compatibles situés dans un rayon d'une dizaine de mètres :

Figure 9.
Les différentes
configurations
d'un réseau
Bluetooth.



L'ensemble des appareils reliés définit un espace de communication appelé **piconet**. Dans un piconet, l'appareil qui initie l'échange joue le rôle de **maître**, tandis que le ou les autres sont dits **esclaves** :

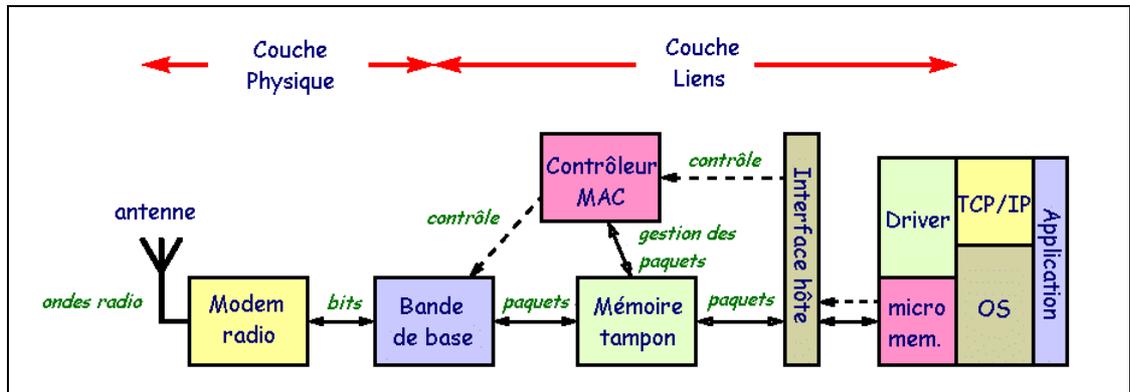
- Bluetooth permet bien-sûr une **liaison point à point** (a) avec un maître et un esclave
- plusieurs mobiles (8 au maximum) communicants constituent un réseau « **piconet** » (b), dans lequel l'un (le maître) dialogue avec un autre (l'esclave)
- si plusieurs piconets se trouvent dans la même zone, ils peuvent être interconnectés (c) pour former un **réseau de diffusion** ou **scatternet** (10 piconets au maximum)

Deux équipements équipés d'interfaces IEEE802.11b peuvent communiquer directement entre eux dans le mode ad-hoc sans nécessiter de point d'accès à proximité.

6- La constitution de l'interface radio

L'interface radio permettant de réaliser un réseau est constituée le plus souvent d'une carte ISA ou PCMCIA à installer dans un PC ou une station de travail.

Figure 10.
Structure d'une interface radio.



Elle comprend les fonctionnalités suivantes :

- le **modem radio**, qui émet et reçoit, en modulant et démodulant la porteuse avec les données binaires à transmettre. Il est surtout constitué de fonctions analogiques (une ou plusieurs antennes, amplificateurs, synthétiseur de fréquence, filtres etc ...) et est souvent masqué par un blindage qui évite les rayonnements parasites.

Il est essentiellement caractérisé par sa fréquence de travail, son débit, sa puissance d'émission et le type de modulation utilisé.

- le **contrôleur MAC** (Medium Access Controller) mettent en œuvre le protocole d'accès au support physique radio. Il est souvent piloté par un microcontrôleur, bien qu'une partie de ses fonctionnalités puisse être déportée vers le PC hôte. Il est étroitement associée à sa mémoire tampon qui permet de stocker temporairement les données entrantes et sortantes.

Les principales caractéristiques sont le format des paquets (taille, en-têtes), les mécanismes d'accès au canal et la gestion des échanges.

- l'**interface hôte**, qui utilise un des bus du PC (ISA, PCI, PCMCIA) ou un des ports de communication (série, parallèle, USB, Ethernet ...). Elle permet au logiciel (**driver**) de communiquer avec le contrôleur MAC, la plupart du temps en écrivant à des emplacements mémoire dédiés.

Figure 11.
Exemple
d'interface
radio PCMCIA.



7- Les fréquences de travail

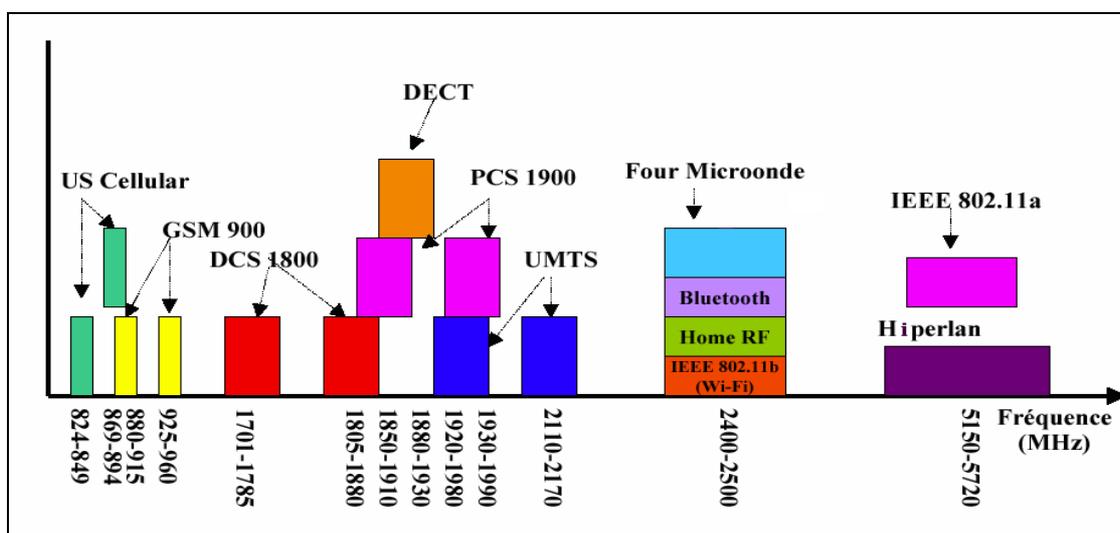
Les bandes de fréquences affectées aux réseaux locaux radio sont les **bandes ISM** (Industrial, Scientific and Medical), destinées à l'origine aux équipements de chauffage micro-ondes, aux réseaux hertziens point à point et à divers dispositifs industriels et médicaux. Deux bandes sont utilisées :

- la **bande des 2,4 GHz**, qui a l'avantage d'être commune à la plupart des pays, pour les standards IEEE802.11b (Wifi), Bluetooth et HomeRF
- la **bande des 5,5 GHz** moins encombrée et perturbée que la précédente, pour les standards IEEE802.11a et Hiperlan

En 1985 les autorités de régulation ont autorisé l'utilisation de la bande des 2,4 GHz inutilisable pour des applications « nobles » car très perturbée pour les réseaux locaux, avec un accès libre sans licence, à condition que les dispositifs mis en œuvre respectent les exigences suivantes :

- puissance d'émission limitée, la limite étant plus basse en extérieur
- insensibilité aux perturbations par l'utilisation d'une technique d'étalement de spectre

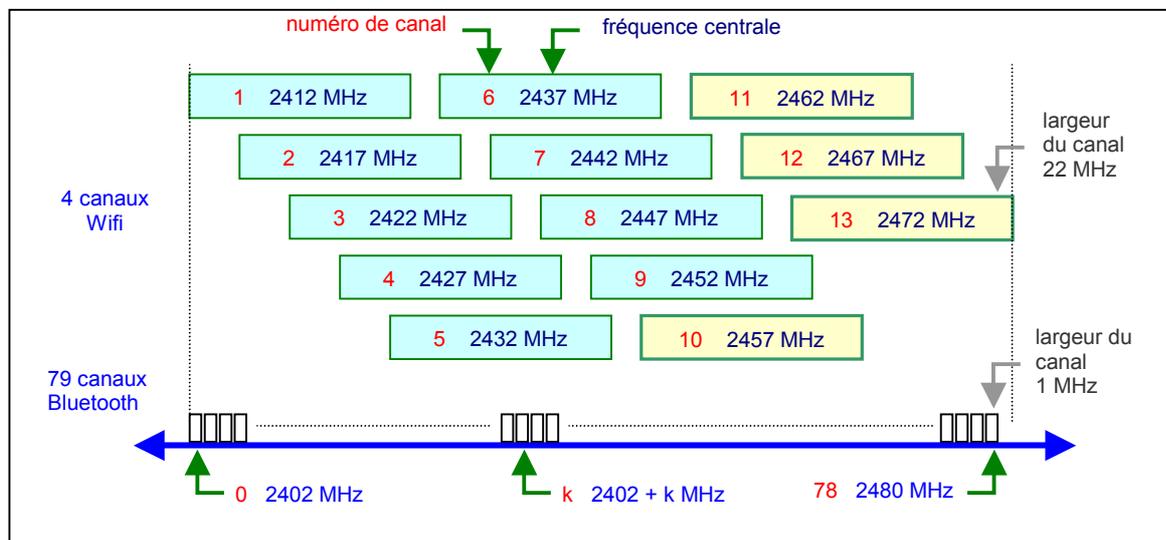
Figure 12. Bandes de fréquences utilisées dans les réseaux RF.



En France, une partie de la bande ISM est utilisée par le Ministère de la défense ce qui ne permet pas d'ouvrir la totalité de la bande ISM aux réseaux sans fil, comme c'est le cas dans les autres pays :

- pour la norme **Wifi** : seuls 4 canaux sur 13 sont disponibles, pas d'autorisation nécessaire pour une utilisation à l'intérieur des bâtiments si la puissance reste inférieure à 100 mW
- pour la norme **Bluetooth** : 79 canaux, pas d'autorisation nécessaire pour une utilisation à l'intérieur des bâtiments si $P < 10$ mW, et à l'extérieur avec $P < 4$ mW (JO du 16/06/2001)

Figure 13. Canaux Wifi et Bluetooth utilisables en France.

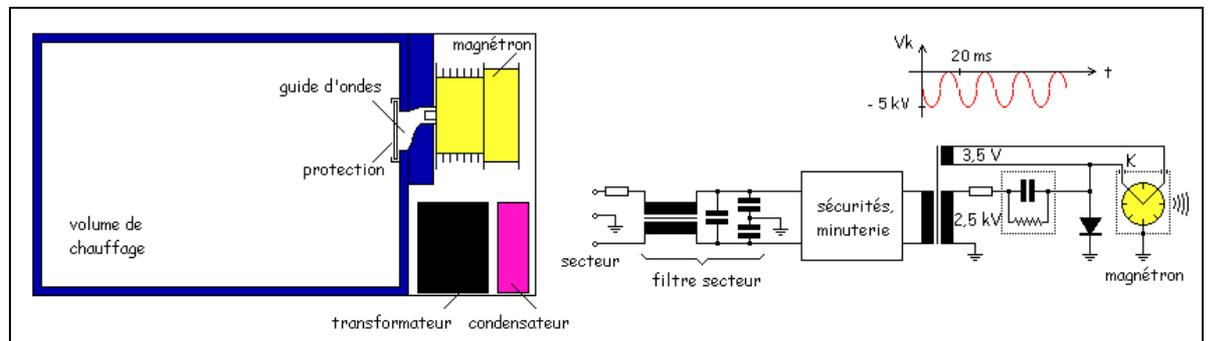


8- Les perturbations des fours à micro ondes

Le four à micro ondes est construit autour d'un générateur appelé magnétron qui comporte :

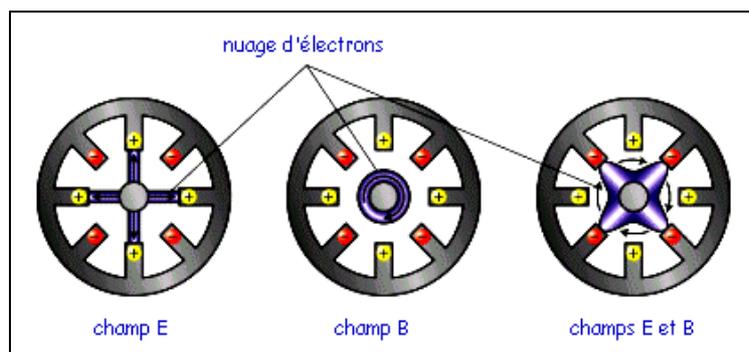
- une cathode chauffée qui émet des électrons dans une cavité métallique
- une alimentation fournissant la tension de chauffage (3,5V) et la haute tension pulsée polarisant la cathode (-5kV, 400 mA)
- un tronçon de guide d'onde conduisant les ondes du magnétron dans le four

Figure 14.
La constitution
d'un four à
micro ondes.



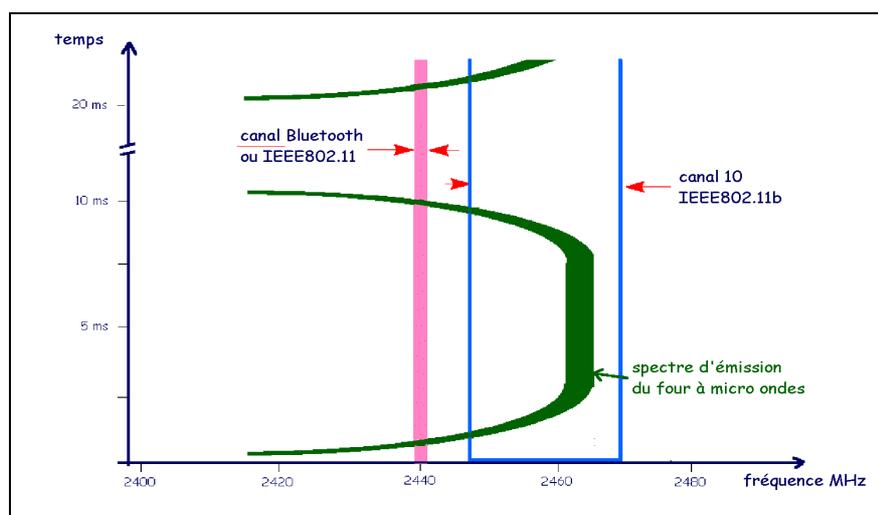
A l'intérieur du magnétron, les électrons s'éloignent de la cathode avec un mouvement de rotation à cause de l'effet conjugué des champs électrique et magnétique régnant dans la cavité.

Figure 15.
La trajectoire
des électrons.



Le mouvement de ce nuage d'électrons, semblable à celui du rotor d'un moteur, induit des courants dans la structure métallique de la cavité, et produit donc une onde électromagnétique dont la fréquence dépend essentiellement des dimensions et du nombre d'ailettes de la cavité.

Figure 16.
Spectre
dynamique
d'émission d'un
four.



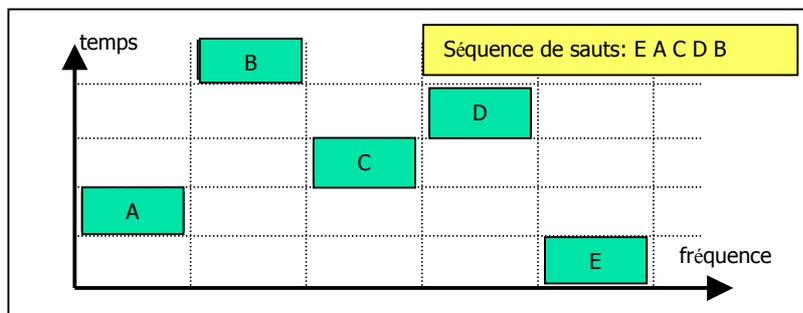
Parce que la tension d'alimentation n'est pas constante, l'onde produite est discontinue dans le temps et sa fréquence n'est pas constante : les fuites d'un four à micro ondes polluent donc « allègrement » la quasi totalité de la bande ISM.

9- La protection contre les brouillages

A cause des perturbations causées essentiellement par les fours à micro ondes, il a fallu protéger la transmission radio contre les brouillages. On utilise pour cela les techniques d'**étalement de spectre** qui consistent à utiliser une bande de fréquence beaucoup plus large que celle qui est nécessaire.

⇒ **l'étalement par saut de fréquence** (Frequency Hopping Spread Spectrum ou FHSS) consiste à sauter périodiquement d'un canal à l'autre et conduit donc à une utilisation de la totalité des canaux au bout d'un certain temps.

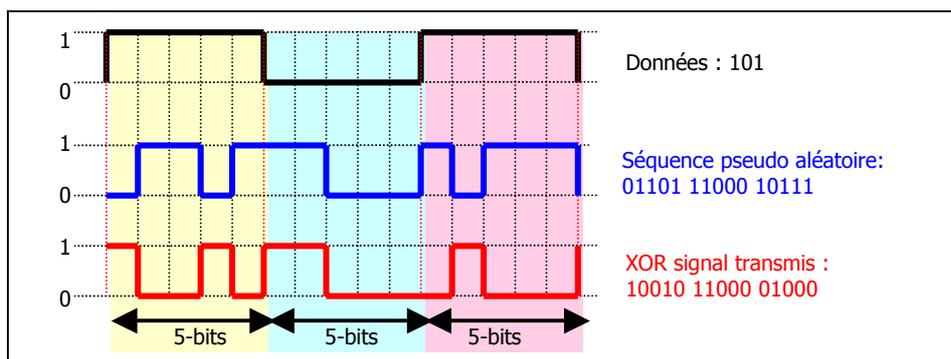
Figure 17.
Principe du saut de fréquence.



Cette technique, utilisée dans le standard Bluetooth avec **1600 sauts/seconde**, nécessite la gestion des collisions qui peuvent se produire avec d'autres émissions Bluetooth ou des signaux de brouillages. La durée du brouillage est limitée à la durée du time-slot qui est de $1/1600 = 625 \mu\text{s}$.

⇒ **l'étalement par code binaire** (Direct Sequence Spread Spectrum ou DSSS) qui consiste à mélanger le signal binaire à une séquence numérique pseudo aléatoire de débit plus élevé.

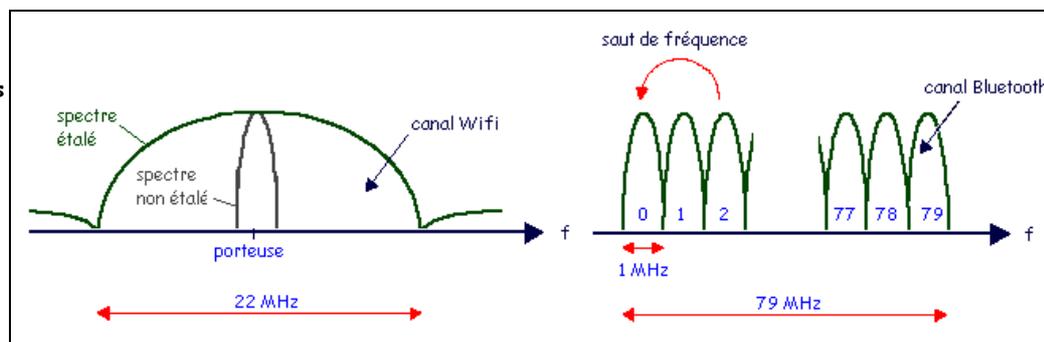
Figure 18.
Le signal modulant dans un étalement par code 1bit/5 bits.



Dans cet exemple, le signal modulant a un débit 5 fois plus élevé, et l'encombrement spectral de la porteuse modulée 5 fois plus important. Cette technique d'étalement par code est utilisée dans le standard IEEE802.11b et pour l'UMTS.

Dans les 2 cas, la bande occupée est bien plus large que celle qui est strictement nécessaire à la transmission des informations. Mais l'avantage de ces techniques est une relative insensibilité à la présence de signaux de brouillages.

Figure 19.
Allure des spectres après étalement.

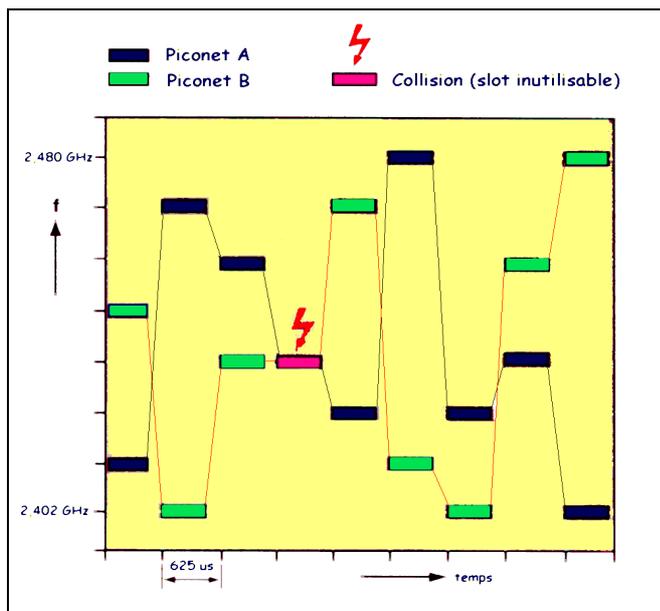


10- L'étalement de spectre par saut de fréquence FHSS

⇒ l'étalement par saut pour Bluetooth

- l'information est transmise sur une fréquence pendant **un time-slot de 625 μ s**
- les sauts en fréquence ($1/625\mu\text{s} = 1600$ sauts par seconde) ont une **amplitude de 6 MHz** au minimum et sont déterminés par calcul à partir de l'adresse du maître et de l'horloge
- ils sont donc aussi connus par le récepteur qui change de fréquence de manière synchrone avec l'émetteur pour récupérer le signal transmis
- chaque réseau ou piconet utilise une succession de fréquences différentes, et la probabilité de brouillage ou de collision reste faible
- en cas de brouillage les données perdues seront retransmises dans le time-slot suivant

Figure 20.
Les sauts de fréquence dans la norme Bluetooth.



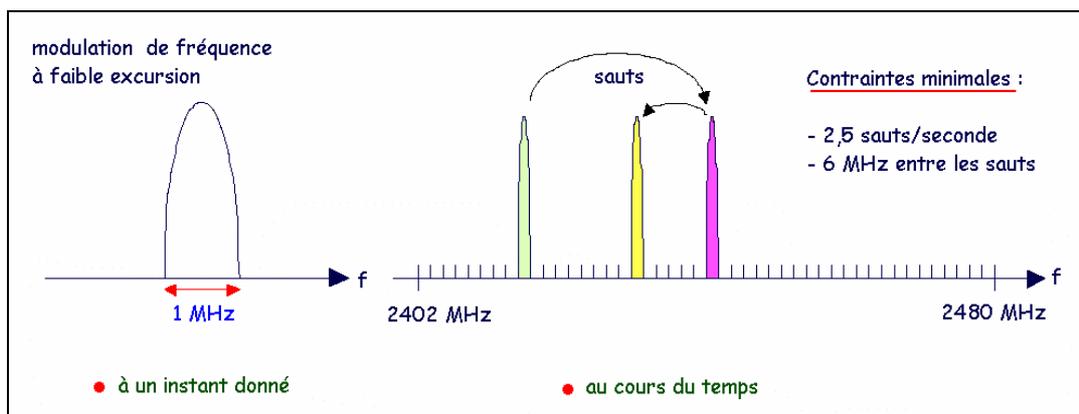
Chaque liaison utilisant la technique FHSS occupe donc, à cause des sauts de fréquence, la totalité de la bande de fréquence ISM.

Les **signaux perturbateurs** ne perturbent la liaison que de temps en temps et pour une durée limitée à un time-slot.

⇒ l'étalement par saut pour IEEE802.11

Les premières spécifications de la norme IEEE802.11 utilisaient aussi cette technique d'étalement de spectre, avec la même largeur de canal et le même débit que Bluetooth, soit 1 Mbits/s.

Figure 21.
Les sauts de fréquence dans la norme IEEE802.11.



La norme définit 3 set de 26 séquences soit 78 séquences de sauts (ou patterns) différentes, ce qui permet un fonctionnement correct avec un maximum de 13 points d'accès différents dans la même zone géographique.

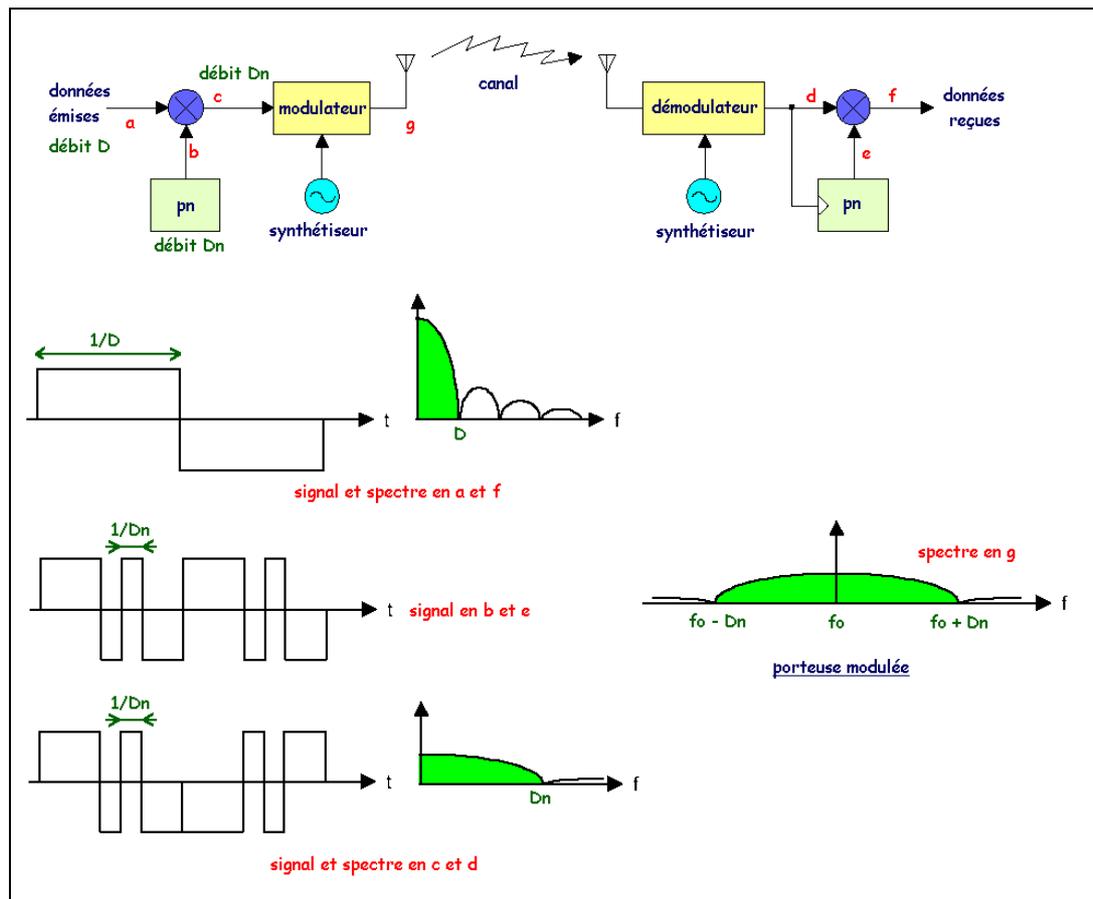
La norme Wifi ou IEEE802.11b a abandonné l'étalement par saut et offre un débit plus élevé en utilisant l'étalement par code, les équipements Wifi ne sont donc pas compatibles avec les équipements IEEE802.11 fonctionnant en FHSS.

11- L'étalement de spectre par code DSSS

L'étalement de spectre par code (ou par séquence directe) utilisé dans le standard Wifi met en œuvre les traitements suivants :

- le signal binaire des données ayant un débit de base $D = 1$ MHz est multiplié par une séquence pseudo-aléatoire pn de débit plus élevé $D_n = 11$ MHz
- le signal résultant, de débit D_n , module la porteuse de l'émetteur en modulation de phase à 2 états ou BPSK, la porteuse modulée occupe alors une bande égale à $2.D_n = 22$ MHz
- à la réception, la porteuse est démodulée et le résultat mélangé à la même séquence pseudo aléatoire pour récupérer les données binaires

Figure 22.
L'étalement de spectre par séquence (à 1 Mb/s).



Dans la pratique, les techniques utilisées sont un peu différentes :

- au lieu d'utiliser un générateur de séquence pseudo aléatoire, on associe simplement deux séquences « Barker » différentes de 11 bits aux données « 0 » ou « 1 ».
- en utilisant une modulation de phase à 4 états le débit a pu être doublé à 2 Mbits/s
- la modulation CCK utilise un alphabet de 64 mots de 8 bits et code des groupes de 4 (ou 8) bits par un mot, ce qui donne des débits de 5,5 (ou 11) Mbits/s dans un canal de 22 MHz

Débit binaire	Séquence	Modulation	Rapidité de modulation
1 Mbits/s	11 (Barker Sequence)	BPSK	1 Mbauds - 1 bit/symbole
2 Mbits/s	11 (Barker Sequence)	QPSK	1 Mbauds - 2 bits/symbole
5.5 Mbits/s	8 (Complementary Code Keying)	QPSK	1,375 Mbauds - 4 bits/symbole
11 Mbits/s	8 (CCK)	QPSK	1,375 Mbauds - 8 bits/symbole

Pour réduire le taux d'erreurs lorsque l'environnement est très bruyants, les WLANs 802.11b utilisent, comme les modems, le repliement vers un débit plus faible appelé [dynamic rate shifting](#) pour une transmission plus sûre. Ce mécanisme est totalement transparent pour l'utilisateur.

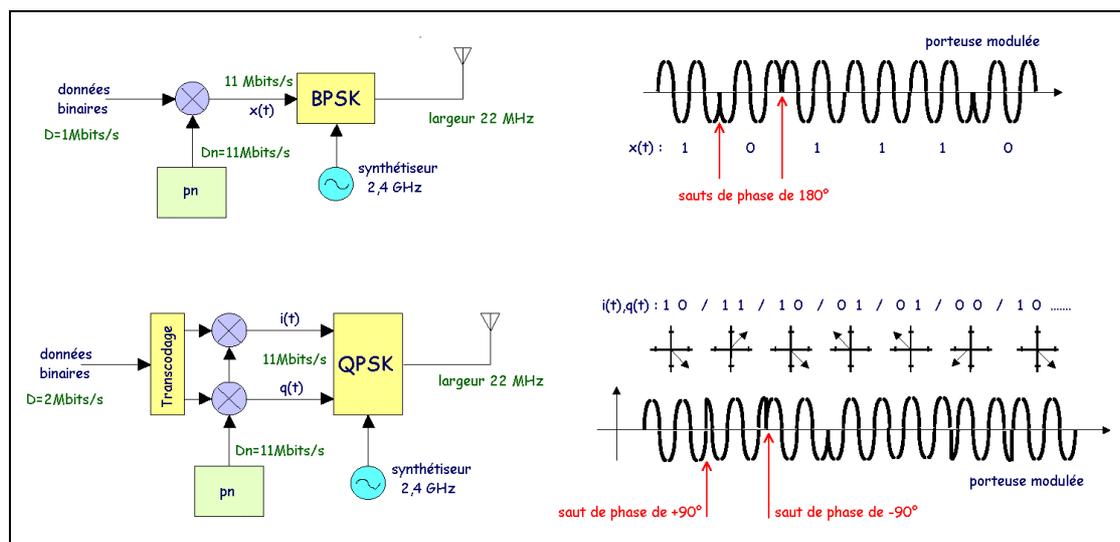
12- Les circuits de l'émission DSSS

Les modulations utilisées sont les mêmes que celles utilisées dans les autres applications de communication numérique (modems, TV satellite ...) .

La modulation de phase en quadrature ou QPSK est utilisée dès que le débit dépasse 1 Mbits/s :

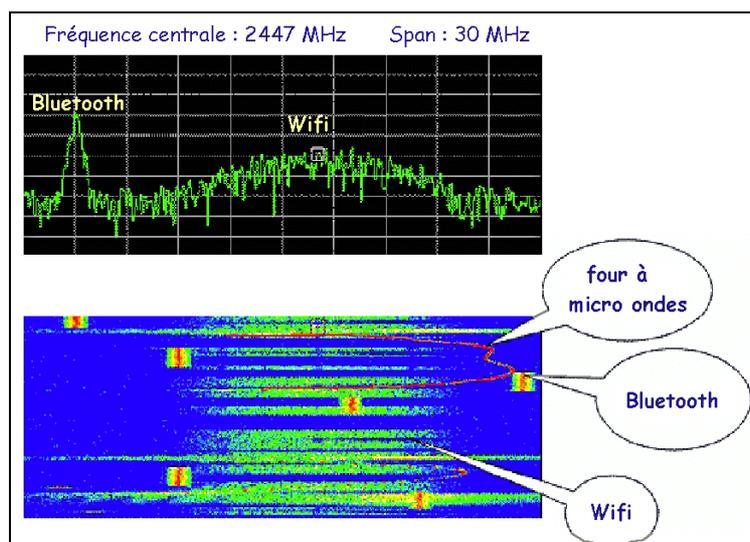
- les données sont séparées en dibits par le circuit de transcodage
- les deux signaux obtenus sont mélangés à la séquence pseudo aléatoire pour obtenir les 2 signaux modulateurs en phase $i(t)$ et en quadrature $q(t)$
- $i(t)$ et $q(t)$ modulent la porteuse en lui imposant des sauts de phase de 0° , $+90^\circ$, $+180^\circ$ ou $+270^\circ$ selon la valeur du dibit
- en réalité $i(t)$ et $q(t)$ sont traités par un passe-bas, ce qui rend les sauts de phase progressifs et atténue l'importance des lobes secondaires du spectre RF (moins de perturbations pour les canaux adjacents)

Figure 23. Les modulations BPSK et QPSK.



Quelque soit le débit binaire au niveau des données (1,2,5,5 ou 11 Mbits/s) et quelque soit le type de modulation utilisé (BPSK ou QPSK), l'essentiel de la puissance émise se trouve dans une bande de largeur 22 MHz centrée sur la fréquence de la porteuse .

Figure 24. Le spectre d'une émission Wifi.



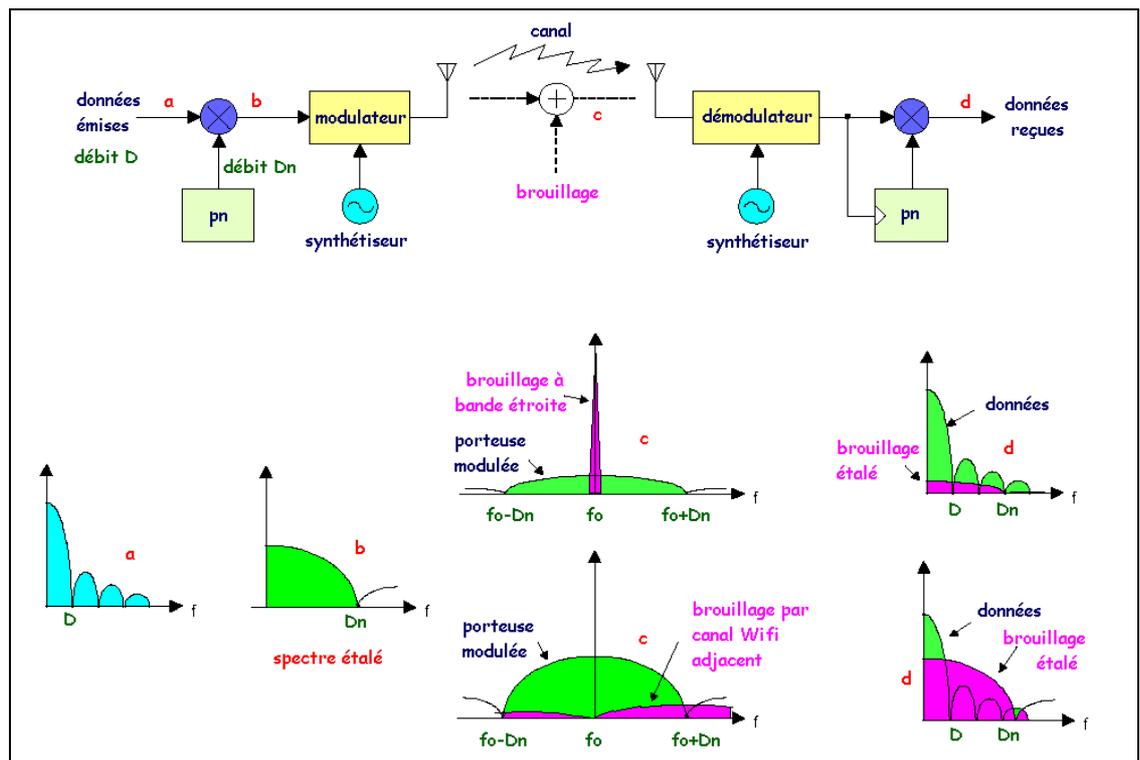
La transmission radio avec la technique d'étalement de spectre par code se fait à fréquence de porteuse fixe. Ce spectre est discontinu (phases d'émission et de réception), mais contrairement à Bluetooth reste fixe en fréquence.

13- La modulation DSSS en présence de brouillage

L'efficacité de l'étalement de spectre par séquence pseudo aléatoire réside dans sa robustesse par rapport aux signaux de brouillage qui se superposent au signal lors de la propagation :

- le spectre du signal modulant (données) est étalé par la séquence pn à l'émission, et contracté par mélange avec la même séquence pn à la réception
- un brouillage à bande étroite (émission Bluetooth, four à micro ondes ...) se superposant au signal durant la transmission voit son spectre étalé par la séquence pn à la réception
- le signal correspondant est assimilable à un bruit qui ne gêne pas la réception des données tant que son niveau n'est pas excessif
- un brouillage à bande large (canal Wifi adjacent, parasites industriels ...) voit aussi son spectre étalé par la séquence et la situation est similaire

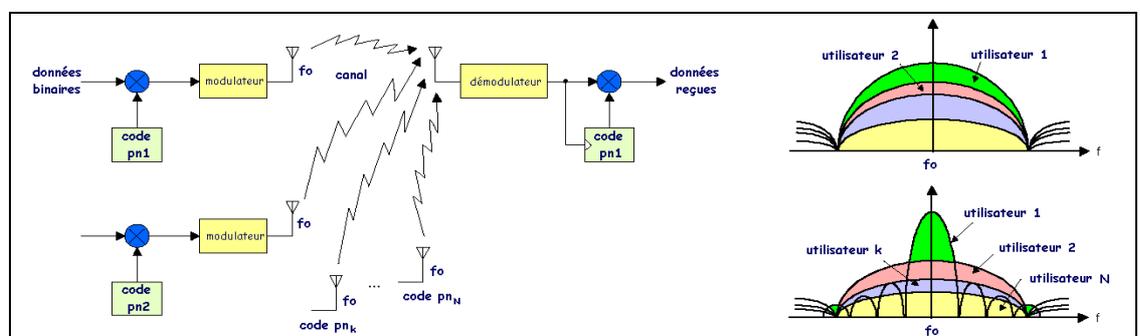
Figure 25.
L'étalement de spectre en présence de bruit.



Dans le standard Wifi, l'algorithme générant la séquence pseudo aléatoire est figé, et tous les étalements se font donc avec le même code pn.

Remarque : c'est exactement cette technique CDMA (Code Divison Multiple Access) qui est utilisée dans l'UMTS où dans une cellule un grand nombre d'utilisateurs travaille sur la même fréquence et ont chacun un code différent.

Figure 26.
Le CDMA utilisé pour l'UMTS.



Dans un réseau Wifi où tous les utilisateurs utilisent le même code pour des raisons de simplicité et de coût, le CDMA n'est donc pas possible et le petit nombre de porteuses disponibles en France limite fortement la multiplication des réseaux dans une même zone géographique.

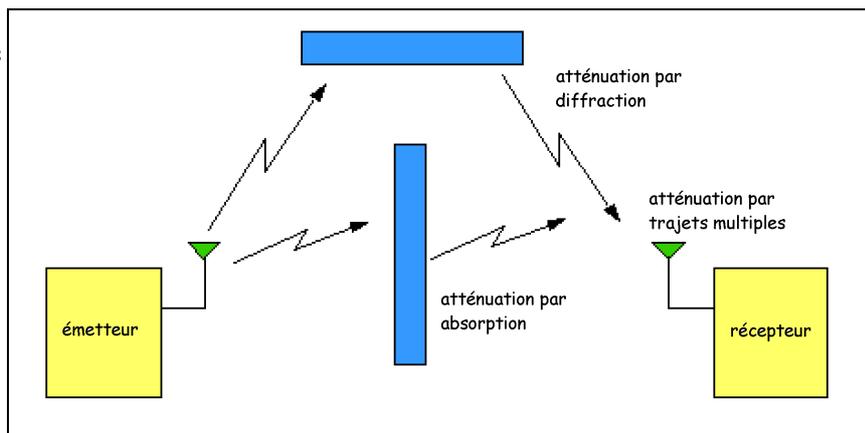
14- La portée d'une liaison à 2,4 GHz

Bien qu'il soit difficile de prévoir la portée exacte d'une liaison RF à l'intérieur d'un local, on peut quand même simplement estimer la portée d'une liaison RF à 2,45 GHz qui dépend :

⇒ **de la puissance émise et du gain de l'antenne** : la puissance est un paramètre essentiel, et un dispositif d'adaptation de la puissance émise permet d'optimiser la liaison et de maintenir le taux d'erreur à un niveau suffisamment bas. Une antenne de bonne qualité permet d'augmenter la portée, mais est difficile à installer à l'intérieur d'un portable.

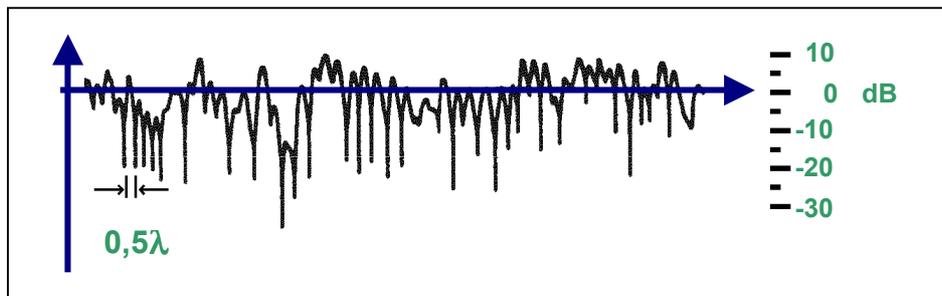
⇒ **de l'environnement** : l'onde électromagnétique doit traverser plusieurs obstacles (corps humain, cloisons ...) avant d'arriver sur le récepteur. Ces obstacles absorberont une partie de l'énergie émise et la transformeront en chaleur, ce qui diminuera d'autant la portée du système.

Figure 27.
Les différentes causes d'atténuation du signal.



⇒ **du fading** : en intérieur, l'onde est souvent diffractée par un obstacle conducteur et renvoyée dans toutes les directions. L'arrivée sur l'antenne du récepteur d'ondes ayant suivi des trajets différents conduit à des variations de niveau du signal reçu (interférences constructives ou destructives appelées fading).

Figure 28.
Exemple de fading lié aux trajets multiples.



La sensibilité des récepteurs Wifi est moins bonne pour les débits élevés, et passe -90 dBm pour un débit de 1 Mbits/s à -83 dBm pour le débit maximal de 11 Mbits/s.

De ce fait, la portée dépend non seulement de la puissance d'émission, mais aussi du taux de transfert :

Débit	11 Mbits/s	5,5 Mbits/s	2 Mbits/s	1 Mbits/s
Portée en extérieur @ 100mW	65 m	90 m	125 m	180 m
Portée en intérieur @ 100mW	30 m	35 m	45 m	55 m

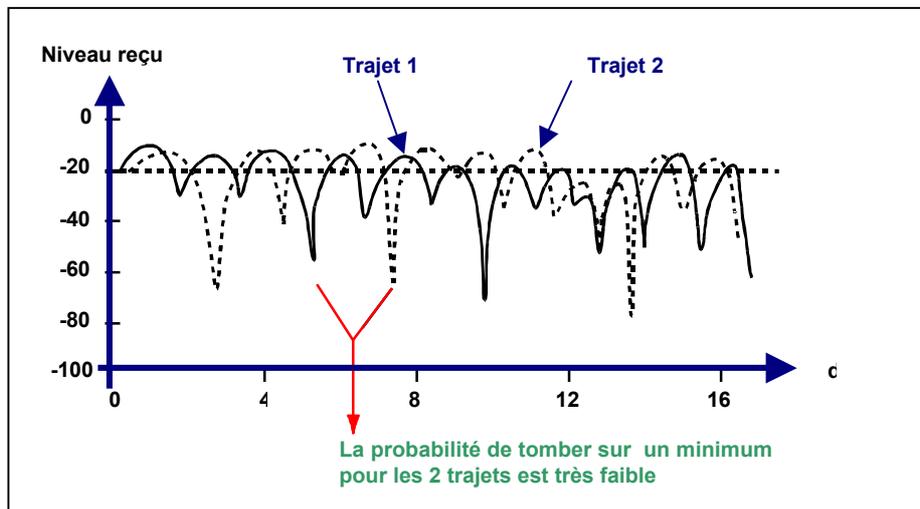
Lorsque la station s'éloigne du point d'accès, le débit s'ajuste pour maintenir un taux d'erreurs suffisamment bas.

15- La technique des antennes multiples

La réponse au problème des trajets multiples et du fading associé est l'utilisation de plusieurs antennes au niveau du point d'accès.

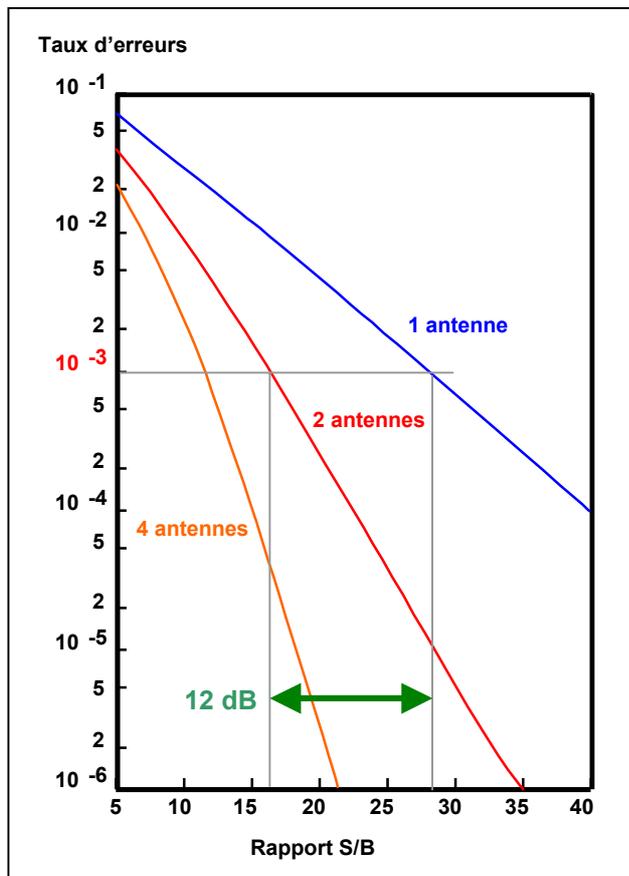
La probabilité de tomber exactement sur un minimum pour deux trajets différents est très faible, même si la différence de trajet parcouru est faible ($\lambda = 12,5 \text{ cm}$ à $2,4 \text{ GHz}$).

Figure 29. Influence du trajet sur le fading.



Si on utilise plusieurs antennes pour la réception au niveau de la station de base, on peut optimiser la réception en commutant l'antenne qui procure le signal le plus élevé.

Figure 30. Bases à antennes multiples.



L'obtention d'un taux d'erreurs de 10^{-3} par exemple nécessite un rapport S/B moyen :

- S/B= 28 dB avec 1 antenne
- S/B=16 dB avec 2 antennes

Le gain de 12 dB obtenu par l'utilisation de 2 antennes permettra selon les cas :

- de diminuer le taux d'erreurs
- d'augmenter la portée de la base

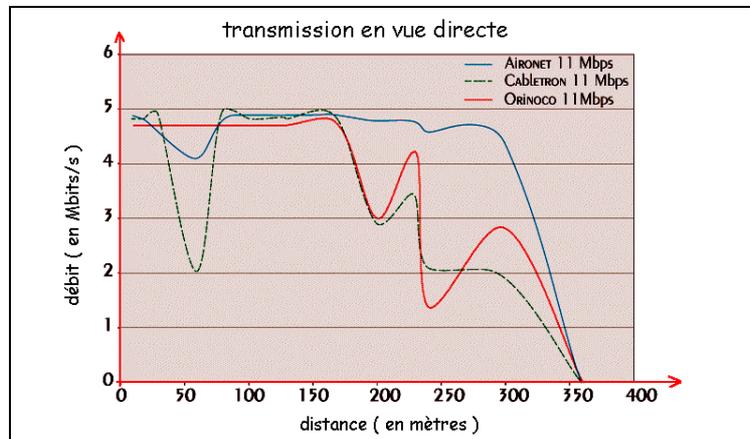


16- Wifi : du rêve à la réalité

Des mesures de débit et de portée sur des systèmes Wifi disponibles dans le commerce montrent que les performances réelles sont en-dessous de celles annoncées :

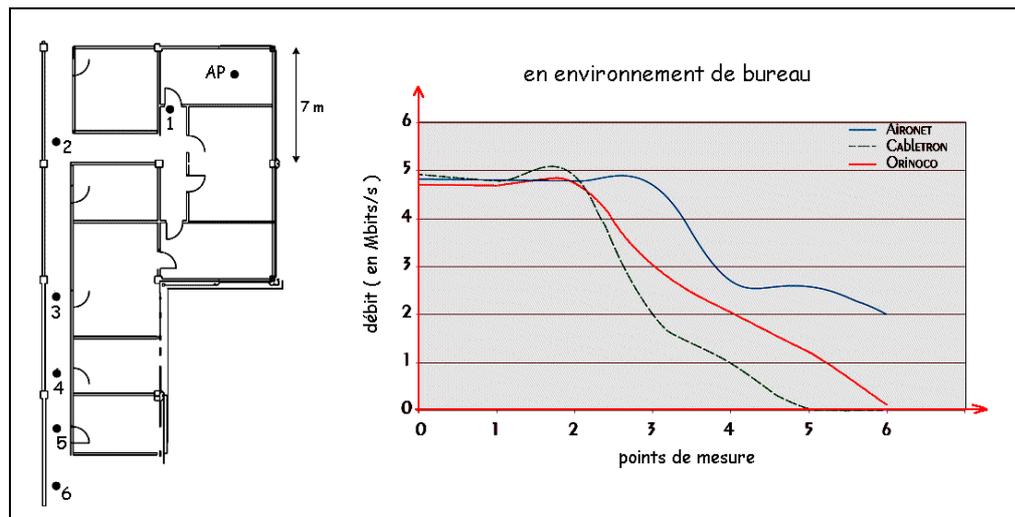
⇒ la vitesse de transmission réelle dans les conditions optimales est toujours inférieure à 5 Mbits/s, loin en-dessous des 11 Mbits/s théoriques

Figure 31.
Portée en
espace libre.



⇒ en environnement de bureau avec des cloisons en briques, la portée est sensiblement plus faible qu'en espace libre.

Figure 32.
Portée en
environnement
de bureau.



⇒ les systèmes radio sont des médias partagés, ce qui veut dire que, par exemple, 30 utilisateurs dans une salle équipée en Wifi vont se partager la bande passante de 5 Mbits/s.

⇒ le fonctionnement en réseau crée des problèmes de confidentialité. La mise en place d'algorithmes de cryptage ralentit le débit, plus ou moins selon le cryptage choisi.

⇒ la norme Wifi prévoit 3 canaux (1, 6 et 11) non chevauchants dans la bande de fréquence des 2.4 GHz. En France, la situation est plus délicate et interdit pratiquement le chevauchement des cellules.

⇒ le nombre d'équipements à l'avenir qui vont utiliser cette bande va augmenter, ce qui va provoquer de sérieux ennuis d'interférences

⇒ la mise en place d'un système sans fils dans un bâtiment d'une certaine importance nécessite une bonne dose de patience et d'expertise dans la mise en place des diverses antennes, afin d'éviter les zones d'ombre et les interférences entre antennes. Certains fabricants recommandent même de faire appel à des consultants en haute fréquence pour l'installation des antennes.

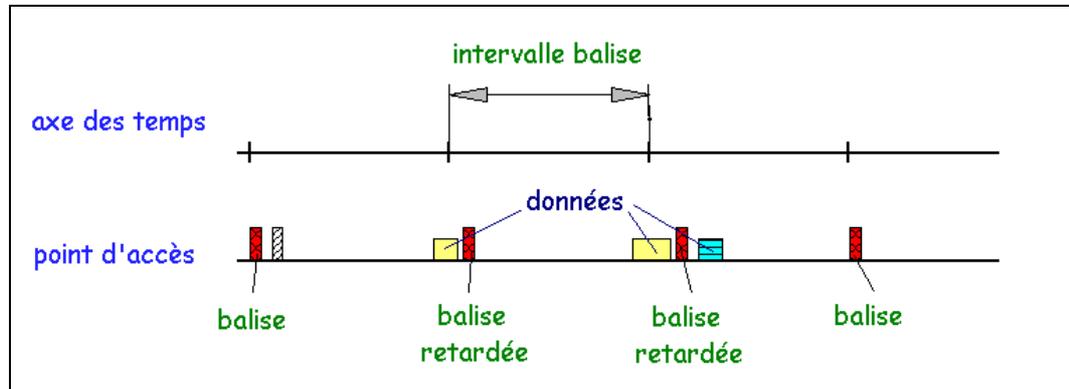
17- Les activités de gestion du réseau

Parmi les nombreux échanges d'informations entre stations et point d'accès concernant la gestion du réseau, les plus importantes sont :

la synchronisation des stations

Le point d'accès transmet régulièrement des trames appelées « trames balise », qui contiennent la valeur de l'horloge du Point d'Accès et permettent aux stations de synchroniser leur horloge.

Figure 33.
L'émission
balise du point
d'accès.



L'instant d'émission des trames balises peut être décalé en fonction de l'état d'occupation du canal.

la gestion de la consommation

Le 802.11 prévoit des fonctionnalités de gestion de la consommation pour augmenter la durée de vie des batteries en faisant passer l'interface radio du mode « actif » au mode « veille » :

- le point d'accès inclut un **buffer** ou tampon permettant de stocker les messages destinés aux différentes stations en veille
- l'AP transmet périodiquement dans les trames balise des informations (Traffic Indication Map) spécifiant quelles stations ont des trames stockées par le Point d'Accès
- ces stations peuvent ainsi se réveiller pour récupérer ces trames balise, et si elles contiennent une indication sur une trame stockée en attente, la station peut rester éveillée pour demander à récupérer ces trames

le raccordement d'un station au réseau

Après démarrage d'une station, son raccordement au réseau passe par un certain nombre d'étapes :

- recherche par **balayage** du canal utilisé par le réseau le plus proche détecté par une mesure de niveau reçu
- **synchronisation** avec l'horloge du point d'accès ou des autres stations dans le cas du mode ad-hoc par **écoute passive (attente d'une voie balise)** ou par **écoute active** (en émettant une Probe Request Frame)
- **authentification** de la station par échange d'informations avec le point d'accès, où chacune des 2 parties prouve son identité par la connaissance d'un mot de passe
- **association** au réseau par échange d'informations sur les différentes stations et les capacités de la cellule et enregistrement de la station par le Point d'Accès

le roaming

Le **roaming** est le processus de mouvement d'une cellule vers une autre sans fermer la connexion. Il est similaire au « hand-over » des téléphones portables, sauf que la transition d'une cellule à une autre doit être faite entre deux transmissions de paquets.

Pour effectuer cette opération, la station doit contrôler en permanence le niveau du signal reçu de la base et effectuer régulièrement un balayage des différents canaux.

18- Le protocole d'échange de données

Le mécanisme d'échange utilisé pour la transmission de données est le **Carrier Multiple Access with Collision Avoidance** (CSMA/CA) qui fonctionne ainsi :

- une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée
- si le support est libre pour un temps spécifique (appelé Distributed Inter Frame Space), alors la station est autorisée à transmettre

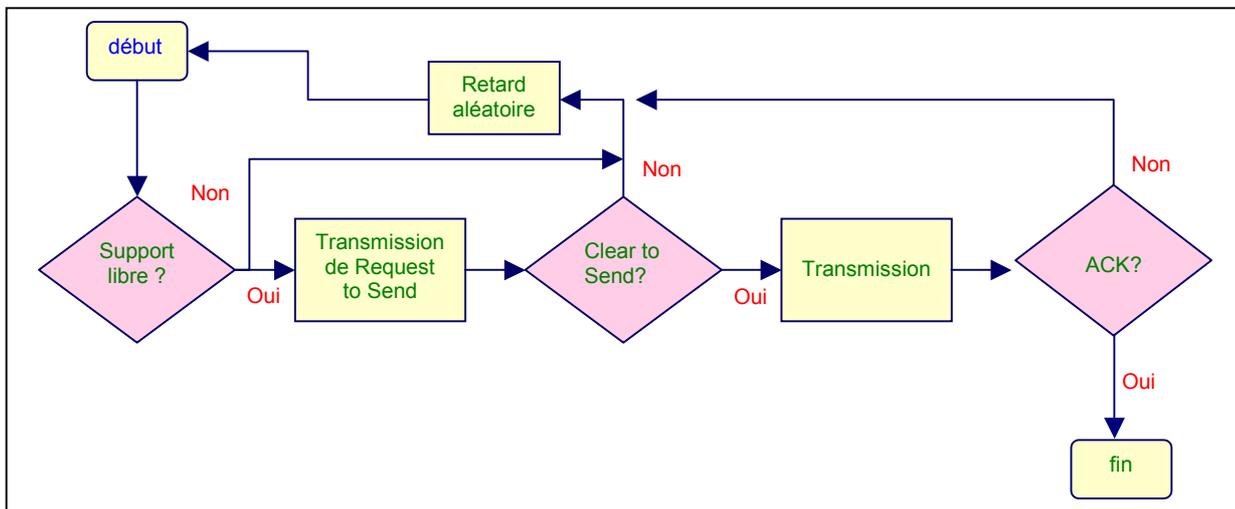
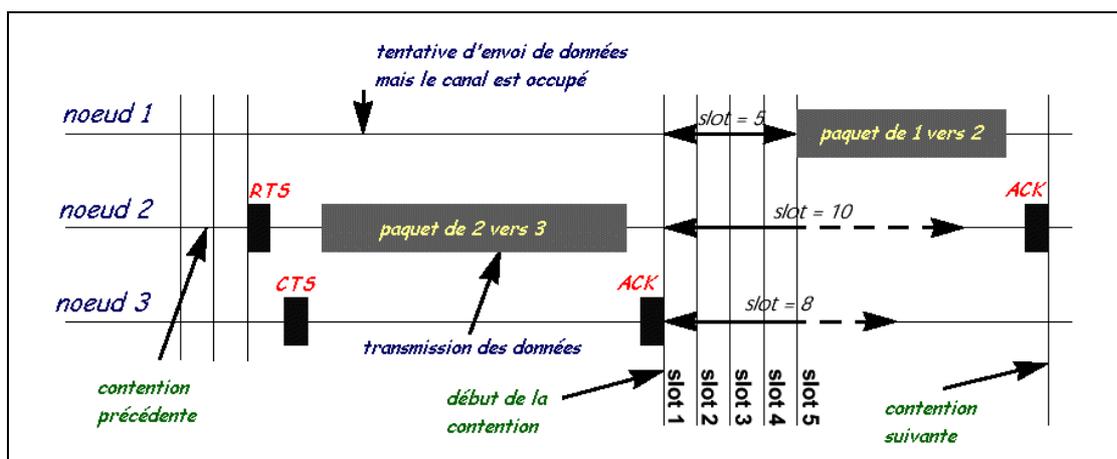


Figure 34. La procédure d'échange.

Pour réduire la probabilité d'avoir deux stations entrant en collision car ne pouvant pas s'entendre l'une l'autre, le standard définit le mécanisme de Virtual Carrier Sense (sensation virtuelle de porteuse) :

- une station voulant émettre transmet d'abord un paquet de contrôle court (risque de collision faible) appelé RTS (Request To Send), qui donnera la source, la destination, et la durée de la transaction
- la station destination répond (si le support est libre) avec un paquet de contrôle de réponse appelé CTS (Clear To Send), qui inclura les mêmes informations sur la durée
- après réception de CTS, la station peut transmettre ses données, dont la bonne réception est confirmée par un paquet ACK (Acknowledge)
- les différents nœuds mettent alors en œuvre un mécanisme de **contention** (retard de durée aléatoire) à l'issue duquel le nœud au retard le plus faible peut envoyer ses données

Figure 35.
Les échanges dans le standard Wifi.



Ce mécanisme de contention permet au point d'accès de distribuer des priorités aux différentes stations du réseau.

19- Les espaces entre trames

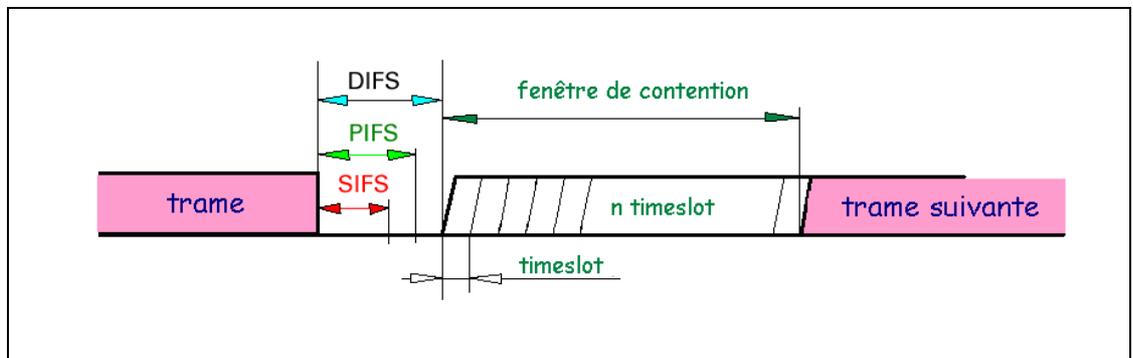
Le standard définit 4 types d'espace en entre deux trames, utilisés pour leurs différentes propriétés :

- le **SIFS** (Short Inter Frame Space) de **28 μ s** est utilisé pour séparer les transmissions appartenant à un même dialogue (par exemple Fragment – ACK). C'est le plus petit écart entre deux trames et il y a au plus une seule station autorisée à transmettre après cet intervalle
- le **PIFS** (Priority Inter Frame Space) de **78 μ s** est utilisé par le Point d'Accès pour obtenir l'accès au support avant n'importe quelle autre station
- le **DIFS** (Distributed IFS) de **128 μ s** est l'intervalle utilisé par une station voulant commencer une nouvelle transmission
- le **EIFS** (Extended IFS) est l'intervalle le plus long utilisé par une station recevant un paquet qu'elle ne comprend pas. Ceci permet d'éviter que la station qui ne comprend pas l'information de durée ne provoque de collision avec un futur paquet

A la fin de la transmission d'un paquet de données, le support redevient libre, et il est possible que deux stations démarrent un échange simultanément.

C'est pour éviter ce genre de situation aboutissant à la collision des RTS que la norme IEEE802.11 a mis en place une temporisation aléatoire appelée **contention** ou back off.

Figure 36.
Le retard aléatoire du back off.

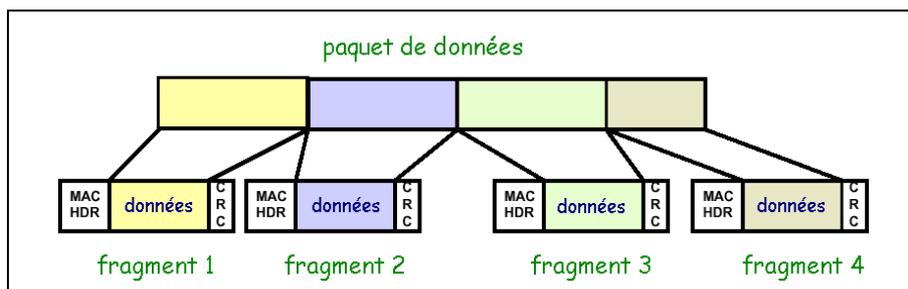


mécanisme de contention chaque station choisit un nombre aléatoire entre 0 et N et attend ce nombre de slots avant d'accéder au support, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle.

- le back off est exponentiel, c'est-à-dire qu'à chaque fois qu'une station choisit un slot et provoque une collision, la valeur maximale N est augmentée exponentiellement
- l'algorithme de back off exponentiel est exécuté quand une station veut émettre et que le support est occupé ou après chaque transmission ou retransmission réussie
- ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS

la fragmentation des paquets pour éviter de ralentir la transmission par la perte de longs paquets, ceux-ci sont divisés en paquets plus courts, qui ont une meilleure probabilité d'être transmis par radio sans pertes.

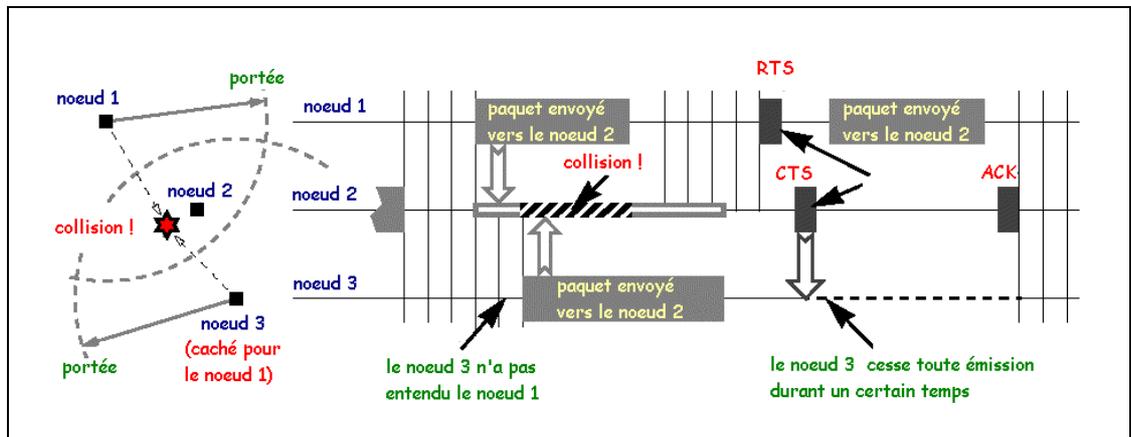
Figure 37.
La fragmentation des paquets longs.



20- La protection contre les brouillages

les stations cachées dans un réseau radio, la portée limitée des interfaces pose le problème des **stations cachées** accessibles par certaines interfaces et inaccessibles à d'autres.

Figure 38.
Existence des
stations
cachées.



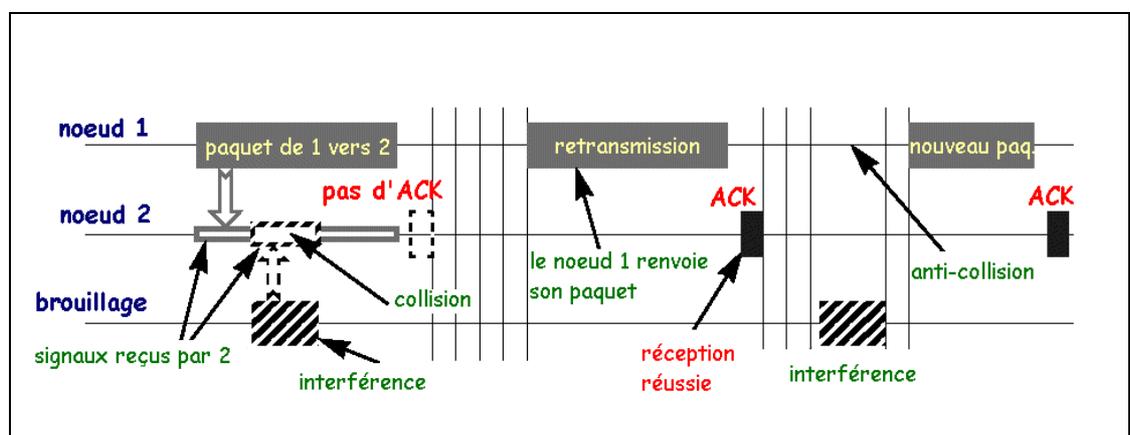
Dans l'exemple ci-dessus, la station n° 3 est une station cachée pour la n° 1. Pour éviter les collisions, la technique utilisée est la suivante :

- la station n°1 voulant émettre transmet le paquet court de contrôle RTS, qui donnera la source, la destination, et la durée de la transaction.
- la station n°2 répond (si le support est libre) avec un paquet de contrôle de réponse CTS qui inclura les mêmes informations sur la durée
- toutes les stations recevant soit le RTS ou le CTS et en particulier la n°3 sauront ainsi que le support radio est occupé et arrêteront d'émettre pendant la durée indiquée dans le paquet RTS
- il est également à noter que grâce au fait que le RTS et le CTS sont des trames courtes (30 octets), le nombre de collisions est réduit, puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis

les parasitages les **brouillages** (four à micro ondes par exemple) empêchant la bonne réception d'un paquet de données sont gérés par le protocole MAC de la façon suivante :

- la station émettrice sait que la transmission ne s'est pas bien effectuée si elle ne reçoit pas de paquet ACK
- elle renvoie alors le même paquet, après un temps de contention aléatoire
- ce mécanisme se reproduit jusqu'à la réception d'un ACK, qui valide la transmission et permet l'envoi du paquet suivant

Figure 39.
La procédure
de
retransmission.



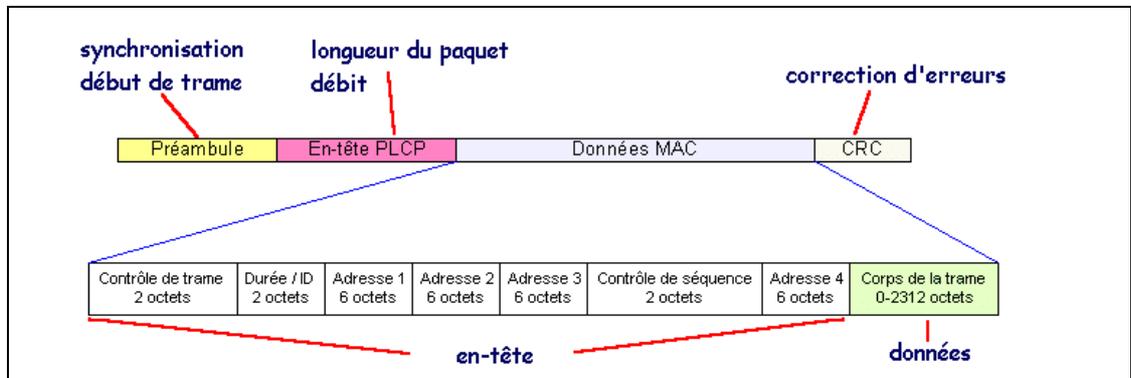
Ce mécanisme ne ralentit pas trop les échanges si la taille des paquets est courte.

21- Le format des trames

Les standard Wifi met en œuvre essentiellement trois types de trames :

- les trames de données, utilisées pour la transmission des données
- les trames de contrôle, utilisées pour contrôler l'accès au support (RTS, CTS, ACK)
- les trames de gestion, transmises de la même façon que les trames de données pour l'échange d'informations de gestion

Figure 40.
Structure générale d'une trame Wifi.

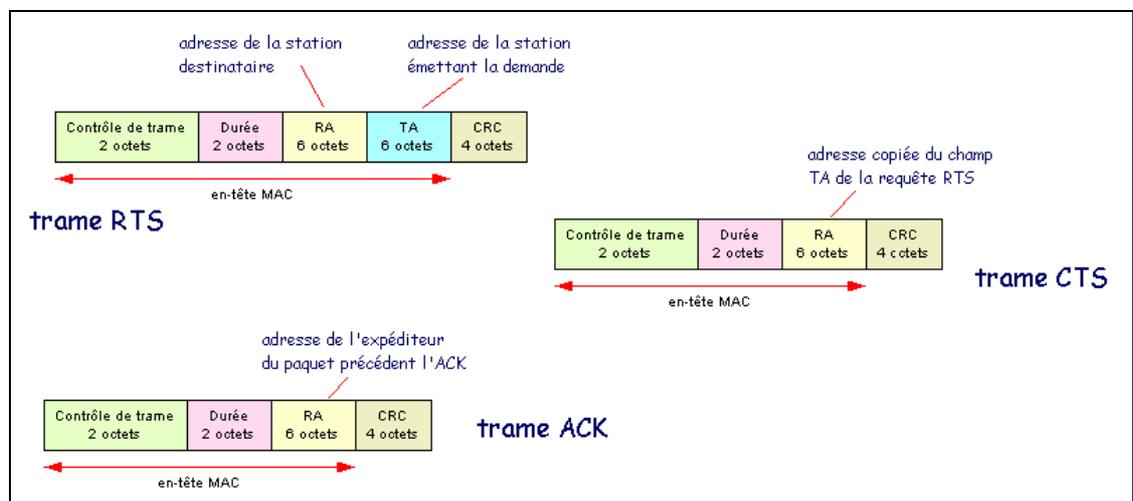


Toutes les trames 802.11 renferment les composants suivants :

- **le préambule** formé de la *Synch*, séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée, et pour corriger l'offset de fréquence et de synchronisation et du *Start Frame Delimiter*, suite de 16 bits 0000 1100 1011 1101 utilisée pour définir le début de la trame.
- **l'en-tête PCLP**, toujours transmis à 1 Mbits/s, contient des informations logiques utilisées par la couche physique pour décoder la trame comme le nombre d'octets que contient le paquet et l'information de taux
- **l'en-tête MAC**, qui précise entre autres s'il s'agit d'une première transmission ou non du paquet, si le paquet est crypté par l'algorithme WEP ou pas, les adresses de l'expéditeur, du destinataire, du point d'accès et le numéro du fragment si le paquet de données a été fragmenté
- **le code de redondance cyclique** permettant de détecter et de corriger un certain nombre d'erreurs sur 4 octets

Les trames de gestion des échanges sont des trames courtes, ce qui limite au minimum les risques de collision.

Figure 41.
Les trames courtes.

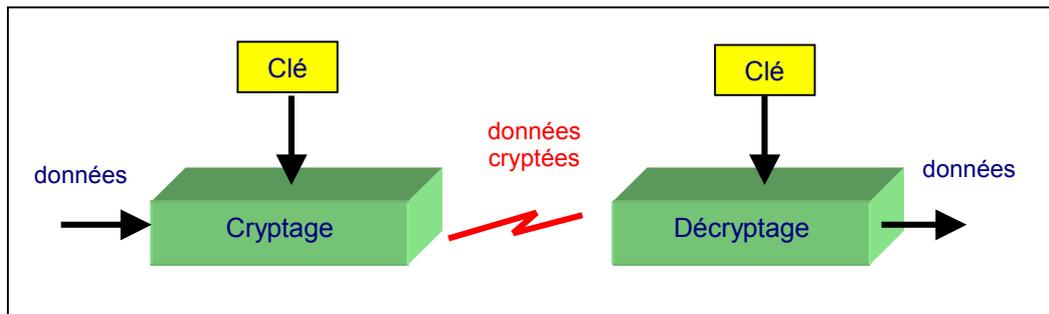


22- La sécurité des échanges

Diverses méthodes de sécurisation permettent d'éviter les interférences et l'espionnage en se basant sur les techniques suivantes :

- l'**identificateur de réseau** SSID (Service Set Identifier) qui permet de donner au réseau un nom unique de manière à ce que seules les personnes autorisées puissent y accéder.
- la **liste de contrôle** d'accès permet de spécifier les adresses MAC des utilisateurs autorisés à utiliser le réseau sans fil
- le **cryptage WEP** (Wireless Equivalent Protocol) optionnel protège les données contre l'écoute clandestine en cryptant les transmissions entre le point d'accès et les périphériques

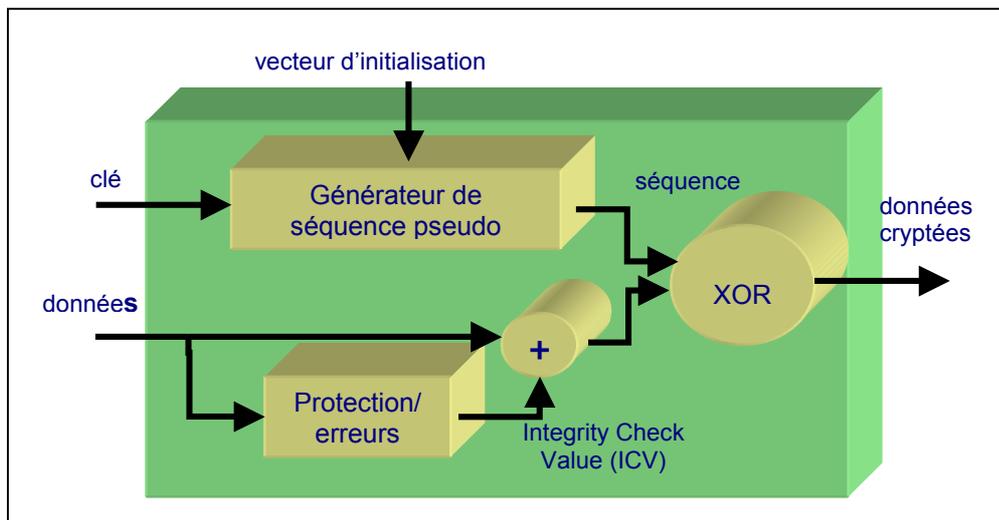
Figure 42.
Le principe du cryptage.



Le cryptage des données WEP est obtenu par l'utilisation de l'algorithme RC4 basé sur un générateur de nombres pseudo aléatoires initialisé par une clé secrète partagée :

- à partir du vecteur d'initialisation de 24 bits et d'une clé choisie par l'utilisateur (40 ou 104 bits), le générateur de nombres pseudo aléatoires produit une séquence de bits de 64 ou 128 bits
- cette séquence pseudo aléatoire est mélangée au données lors de la transmission, les entêtes de paquets n'étant pas cryptés
- l'attaque de cet algorithme est rendue difficile par le fait que chaque paquet de données est envoyé avec un vecteur d'initialisation qui relance le générateur de nombres pseudo aléatoires
- cette resynchronisation pour chaque message est de toutes façons nécessaire compte tenu du fait que des paquets peuvent être perdus lors de la transmission

Figure 43.
Le cryptage WEP des données.



A la suite de nombreuses tentatives de piratage réussies, plusieurs voix se sont élevées pour critiquer l'efficacité de l'algorithme de cryptage WEP qui n'avait pas d'autre objectif au départ que d'assurer une « certaine » confidentialité équivalente à celle offerte par la liaison câblée.

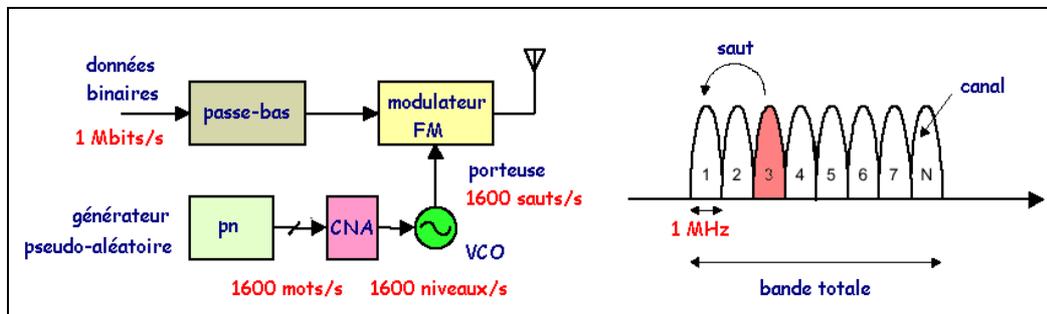
Notons que l'utilisation de l'algorithme WEP pour la liaison radio n'interdit pas l'utilisation en amont d'autres dispositifs de cryptage de donnée plus efficaces.

23- Annexe : l'émission FHSS dans le standard Bluetooth

La porteuse est modulée en fréquence par le signal binaire filtré par un filtre passe-bas gaussien, ce qui donne une **modulation GFSK** (Gaussian Frequency Shift Keying).

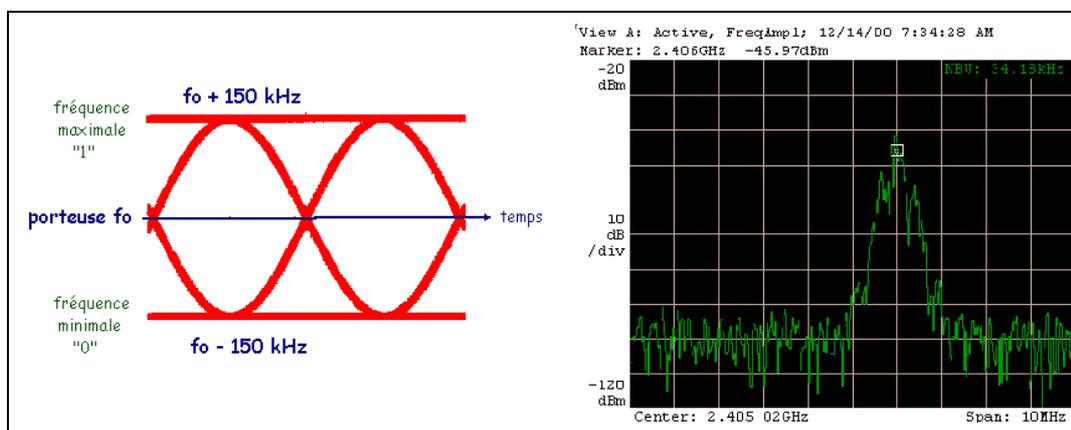
Cette porteuse change régulièrement de valeur, en fonction d'une séquence pseudo aléatoire pn produite par un générateur.

Figure 44.
La modulation FHSS.



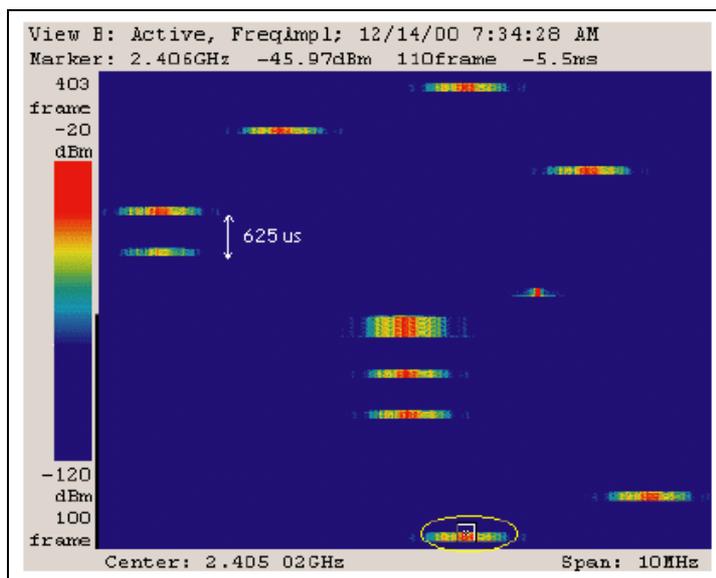
Pour une fréquence de porteuse donnée, l'excursion en fréquence est de ± 150 kHz environ, et le spectre est caractérisé par une largeur environ égale au débit binaire, soit 1 MHz.

Figure 45.
Les variations de fréquence de la porteuse et le spectre résultant.



Le spectre ne tient pas totalement dans le canal de 1 MHz, et on définit un certain gabarit que doit respecter l'émission.

Figure 46.
Spectre d'émission en fonction du temps.



L'enregistrement dynamique du spectre met en évidence les sauts en fréquence et la taille variable des paquets.

Ces émissions doivent être considérées comme un signal perturbant le fonctionnement d'un réseau Wifi.

24- Annexe : la cohabitation entre les standards

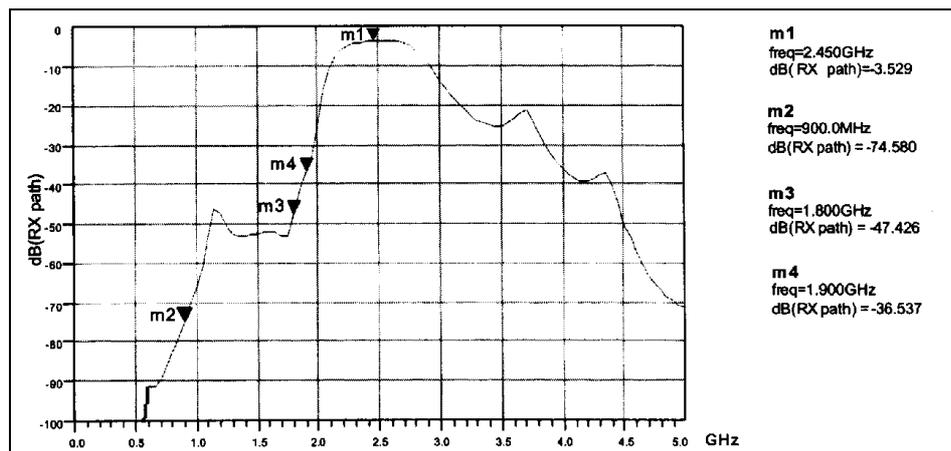
La présence côte à côte d'un téléphone portable GSM/DCS de puissance maximale 2W et d'un module Bluetooth ou Wifi de puissance plus faible peut être à l'origine d'interférences gênantes et nécessite une conception soignée.

Les principaux problèmes qui peuvent survenir sont :

⇒ l'émetteur du téléphone cellulaire GSM bloque le récepteur Bluetooth ou Wifi

La puissance du GSM pouvant monter à 2W et la sensibilité du récepteur Bluetooth étant de 10 pW, l'atténuation apportée par les filtres doit être importante dans les bandes considérées, et il faut absolument éviter des pics parasites à 2,4 GHz dans les filtres GSM.

Figure 47.
Courbe de gain des étages d'entrée d'un module Bluetooth.



Notons que ce problème se posera avec plus d'acuité dans les futures systèmes UMTS qui travailleront dans la bande des 2,1 GHz, très proche de la bande Wifi.

⇒ l'émetteur du Bluetooth ou du Wifi perturbe la réception GSM

Le problème est le même, mais se pose avec moins d'acuité puisque la puissance de l'émetteur Bluetooth ou Wifi est plus faible. Les émissions parasites hors-bande des interfaces radio doivent être filtrées pour rester en-dessous d'un niveau minimal défini par la norme.

Figure 48.
Emissions parasites hors-bande permises pour un module Bluetooth.

Bande de fréquence	Mode actif	Mode veille
30 MHz – 1 GHz	-36 dBm	-57 dBm
1 GHz – 12,75 GHz	-30 dBm	-47 dBm
1,8 GHz – 1,9 GHz	-47 dBm	-47 dBm
5,15 GHz – 5,3 GHz	-47 dBm	-47 dBm

⇒ les interfaces Bluetooth et Wifi se perturbent entre elles

L'existence d'un certain nombre de problèmes a conduit à la mise en place d'un **groupe de travail 802.15** au sein de l'IEEE qui établit des modèles de coexistence et propose des techniques de coexistence entre les deux :

- contrôle de la puissance d'émission
- fragmentation adaptative des paquets pour limiter leur longueur
- saut de fréquence Bluetooth évitant les canaux Wifi

Comme Wifi ne dispose pas de mécanisme de correction d'erreur, le taux d'erreurs peut atteindre 64% lorsqu'il est perturbé par une communication Bluetooth voix (HV1) et 14% dans le cas d'une liaison data (DM5).

25- Annexe : le point d'accès Ericsson

WLAN Access Point A11



Technical Description

Interfaces

Serial
PC AT Serial Port DB-9 female
RS-232 19.2 Kb

LAN Interface
10BaseT RJ45

Compliance
Ethernet / IEEE 802.3 CSMA / CD
standard

Wireless LAN interface

Compliant with
IEEE 802.11b CSMA / CA Wireless
LAN standard

Physical interface – two antennas
Detachable

Radio Specifications

Type
Direct Sequence Spread Spectrum
(DSSS)

Frequency Range
2.4 GHz – 2.4835 GHz (ISM band)
(different ranges available for
countries using other bands)

Transmitted power
Up to 100 mW (20 dBm) EIRP

Sensitivity

- @ 1 Mbps	- 90 dBm
- @ 2 Mbps	- 88 dBm
- @ 5.5 Mbps	- 87 dBm
- @ 11 Mbps	- 84 dBm

Modulation

- @ 1 Mbps	BPSK
- @ 2 Mbps	DQPSK
- @ 5.5 Mbps	CCK
- @ 11 Mbps	CCK

Number of channels
13 Europe
(4 France)
11 US
14 Japan

Antenna Diversity
Yes

Configuration and Management

Configuration and Setup
Local monitor, SNMP,
WLAN DSSS Manager,
Web interface

Modes
AP and WLAP (used for bridge/link)

Front Panel Display LED indicators
Power

Wired LAN Ethernet activity
Wireless LAN radio activity

Software Upgradeable
Through PC application,
Web interface, WLAN DSS Manager
and local monitor

System Considerations

Range (Access Point to Card)
Depends on rate and environment.
(Accurate values must be calculated
for specific installations.)

- **Outdoors** 300 m (1000 ft.)
- **Office Environment** 75 m (250 ft.)

**Max. No of Access Points
per wired LAN**
Unlimited

Max. No of Clients per Access Points
127

Data Rate
1, 2, 5.5 or 11 Mbps

Load sharing support
Yes

Security

WEP
40 bit standard / 128 bit optional

**Dynamic rate selection based on
radio medium quality**
Yes

MTBF

Access Point A11 > 100.000 hours
Power Supply > 50.000 hours

Electrical

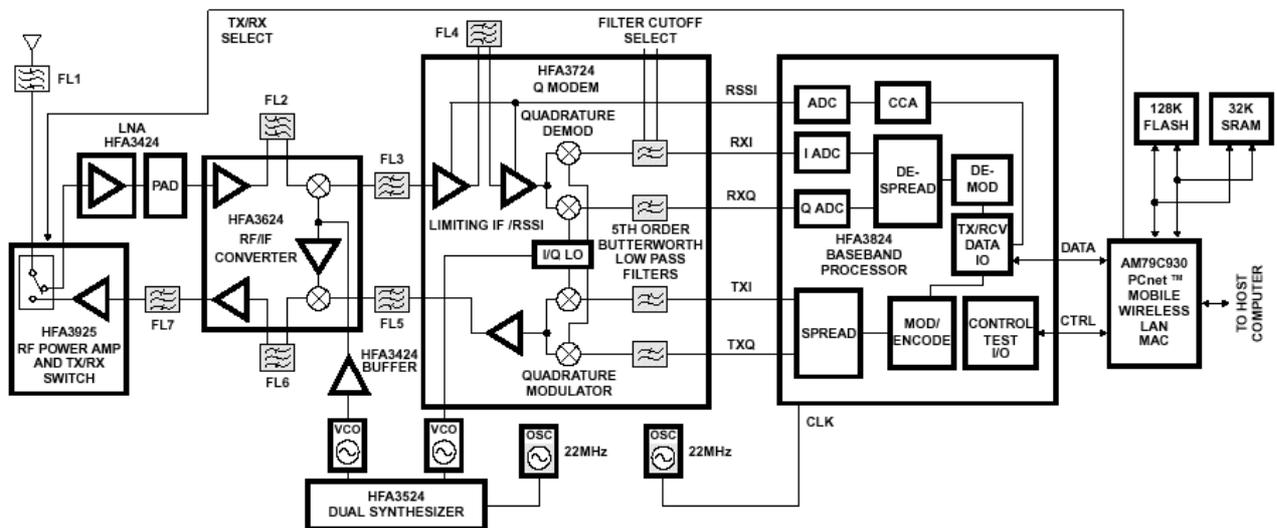
**External Power Supply
(incl. 2 m DC cable)**
100-240 VAC, 50-60 Hz/24 VDC 1.4 A
WLAN A11 average power
consumption 4.1 W @ 20° C

Dimensions (without antennas)
195 x 153 x 35 mm

Weight (without antennas)
0.5 kg

26- Annexe : le chipset Prism d'Intersil

General Specifications	Receive Specifications
<ul style="list-style-type: none"> Targeted Standard IEEE 802.11 (Draft) Data Rate 1Mbps DBPSK 2Mbps DQPSK Range 400ft Indoor (Typ) (Note 1) 3700ft Outdoor (Typ) (Note 1) Frequency Range 2412MHz to 2484MHz Step Size 1MHz IF Frequency 280MHz IF Bandwidth 17MHz RX/TX Switching Speed 2µs (Typ) Operating Voltage 4.5V_{DC} - 5.5V_{DC} Standby Current 190mA at 1µs Recovery (Note 4) 70mA at 25µs Recovery (Note 4) 60mA at 2ms Recovery (Note 4) 30mA at 5ms Recovery (Note 4) Operating Temperature Range 0°C to 70°C (Note 2) Storage Temperature Range -55°C to 125°C Mechanical Type II PC Card, with Antenna Extension Antenna Interface SMA, 50Ω 	<ul style="list-style-type: none"> Sensitivity -93dBm (Typ), 1Mbps, 8E-2 FER (Note 3) -90dBm (Typ), 2Mbps, 8E-2 FER (Note 3) Input Third Order Intercept Point -17dBm (Typ) Image Rejection 65dB (Typ) IF Rejection 80dB (Typ) Adjacent Channel Rejection 63dB (Typ) at 25MHz Offset Supply Current 287mA (Typ) 2Mbps, 100% Duty Cycle
	Transmit Specifications
	<ul style="list-style-type: none"> Output Power +18dBm (Typ) Transmit Spectral Mask -32dBc (Typ) at First Side-Lobe Supply Current 488mA (Typ) 2Mbps, 100% Duty Cycle
	<p>NOTES:</p> <ol style="list-style-type: none"> Using M/A-COM AND-C-107 omnidirectional antenna. AM79C930 limited to 0°C to 70°C. FER = Frame Error Rate or Packet Error Rate. Recovery times do not include MAC recovery.

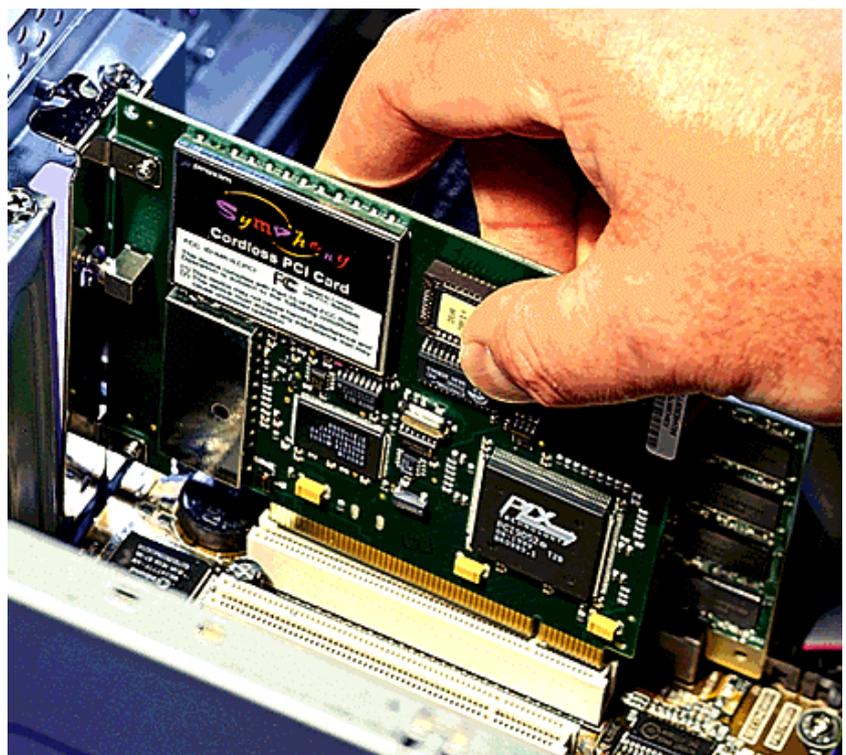


▶ 27- Quelques sites utiles

Wireless Ethernet Compatibility Alliance, WECA : <http://www.wi-fi.org/>

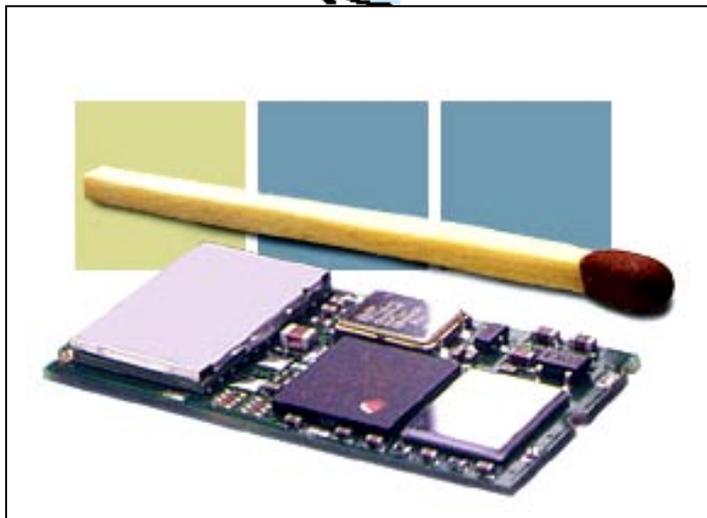
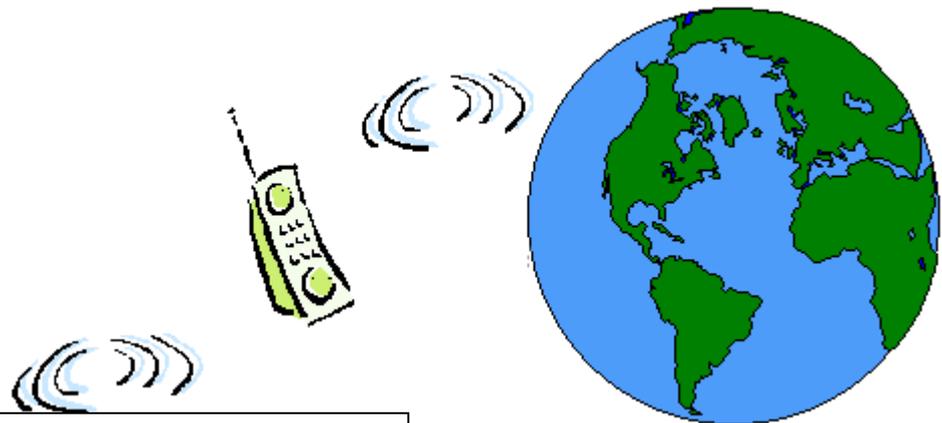
Intersil : <http://www.intersil.com/design/prism/indigo/>

IEEE, normes 802.11 : <http://grouper.ieee.org/groups/802/11/index.html>





Introduction à Bluetooth



Jean-Philippe Muller

Sommaire :

- 1- Présentation de quelques applications
- 2- Les prévisions du marché
- 3- Les caractéristiques du réseau
- 4- Les fréquences de travail
- 5- La technique du saut de fréquence
- 6- Caractéristiques de la liaison radio
- 7- La portée d'une liaison Bluetooth
- 8- Le canal physique de transmission
- 9- La synchronisation temporelle du piconet
- 10- Les 2 types de liens maître-esclave
- 11- Le format du paquet de données
- 12- La mise en place d'une liaison dans un réseau
- 13- Structure et caractéristiques d'un module Bluetooth
- 14- Exemple du module RF Bluetooth Ericsson
- 15- Le module Bluetooth Ericsson complet
- 16- La cohabitation Bluetooth-GSM
- 17- Les tests d'un module Bluetooth

2- Les prévisions du marché

La technologie Bluetooth, développée actuellement pour permettre la liaison entre le téléphone GSM et l'ordinateur (portable ou non) est destinée à équiper progressivement un grand nombre d'appareils.

Les systèmes équipés de la technologie Bluetooth peuvent se classer en 3 grandes catégories :

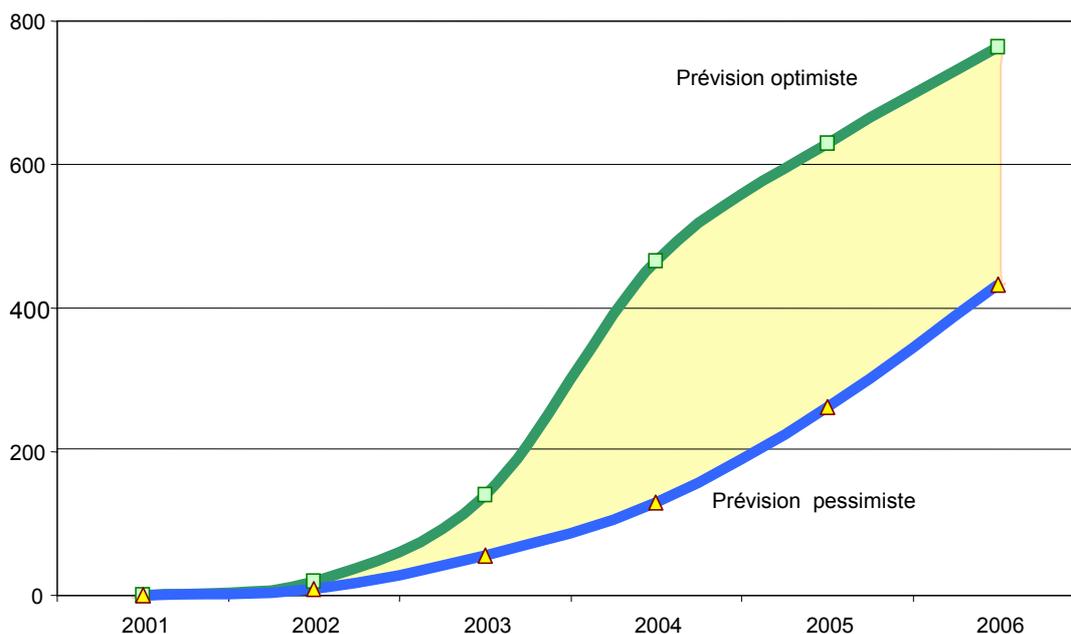
- **systèmes de communication** : téléphones portables (GSM, DCS), casques sans fils, liaisons audio sans fils pour les équipements domestiques
- **ordinateurs** : PC, ordinateurs portables, assistants personnels
- **équipements domestiques** : machine à laver, réfrigérateur/congélateur, téléviseur, décodeur TV numérique, chaîne Hi-fi, console de jeu etc ...

Figure 2.
Répartition de
Bluetooth par
catégorie.

	2002	2006	2010
Systèmes de communication	88%	73%	26%
Ordinateurs	12%	25%	28%
Equipements domestiques	moins de 1%	2%	46%
Total	100%	100%	100%

Le nombre d'appareils différents équipés de cette technologie est amené à se développer de façon très importante dans les années à venir.

Figure 3.
Développement
du nombre
d'applications
de Bluetooth.



Le concept de liaison hertzienne à courte distance Bluetooth a suscité des concurrents :

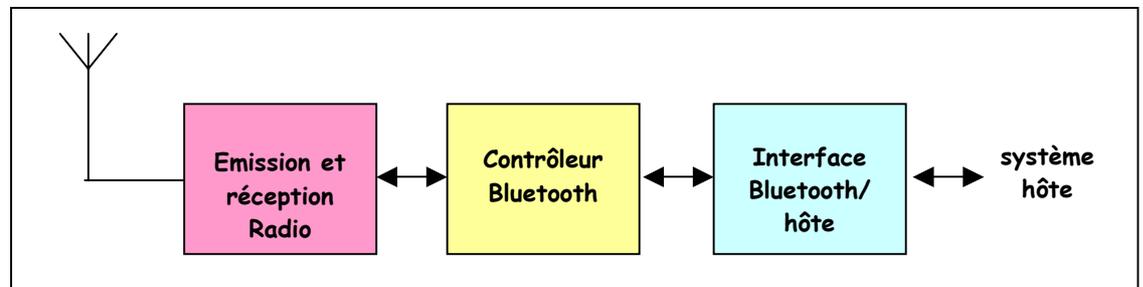
- **les liaisons infra-rouges IrDA** (Infrared Data Association) pour transmettre des données entre un PC et ses périphérique. Mais les infrarouges ne fonctionnent qu'à vue et leur portée n'est au mieux que de quelques mètres alors que Bluetooth traverse les murs
- **la norme radio « HomeRF »** similaire à Bluetooth et née aux USA. Le protocole d'accès sans fil partagé SWAP (Shored Wireless Access Protocol) permet d'utiliser 127 appareils par réseau avec une portée de 50 mètres. Par contre, il faut déboursier 500 \$ de droits d'inscription pour avoir accès au cahier des charges de HomeRF
- **la norme DECT** de téléphonie sans fil fonctionne à 1,8 GHz et sa portée est plus étendue (jusqu'à 500 mètres) grâce à une puissance d'émission plus élevée. DECT et Bluetooth atteignent le même score dans la transmission vocale sans fil et dans la transmission des données à faible débit (64 kilobits/s max.), mais Bluetooth peut atteindre 721 kilobits/s

3-Les caractéristiques du réseau

Bluetooth est le nom de code donné à cette technologie de réseau local qui permet la transmission de la voix et des données simultanément via une liaison radio courte distance.

Une interface Bluetooth est constituée d'une interface radio, d'un contrôleur et d'une interface avec le système hôte.

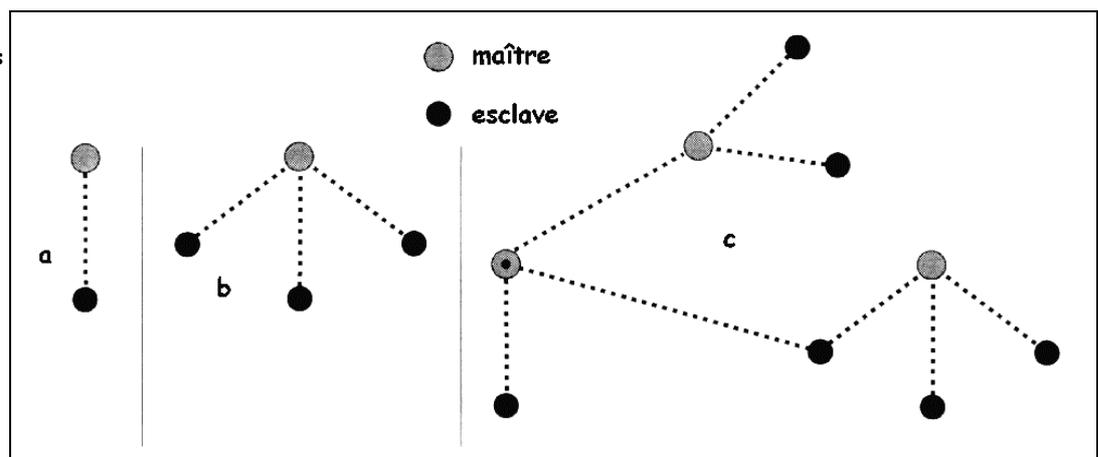
Figure 4.
Structure d'une
interface
Bluetooth.



Chaque système (téléphone, PC ...) compatible « Bluetooth » est équipé d'une telle interface grâce à laquelle il pourra communiquer avec les autres systèmes compatibles situés dans un rayon d'une dizaine de mètres.

L'ensemble des appareils reliés définit un espace de communication appelé **piconet**. Au sein d'un piconet, l'un des appareils joue le rôle de **maître**, tandis que les autres sont dits **esclaves**.

Figure 5.
Les différentes
configurations
d'un réseau
Bluetooth.



Le système Bluetooth permet une **liaison point à point** (situation a) avec un système maître et un système esclave.

Dans un **réseau « piconet »** (situation b), le système maître dialogue avec deux esclaves ou davantage. Le nombre maximal d'esclaves actifs est de 7. Si le piconet est constitué de plus de 8 systèmes, seuls 7 esclaves pourront être gérés, les autres seront « parkés » et restent simplement en réception pour conserver la synchronisation par rapport au maître.

Si plusieurs piconets se trouvent dans la même zone (situation c), les esclaves peuvent, grâce au multiplexage temporel, communiquer avec différents maîtres. De plus, le système maître d'un piconet peut être esclave dans un autre piconet. On parle alors de « **réseau de diffusion** » ou **scatternet**.

4- Les fréquences de travail

Le système Bluetooth travaille dans la bande des 2,4 GHz appelée **bande ISM** (Industrial Scientific Medicine) qui existe dans la plupart des pays du monde. Cette bande de fréquence était à l'origine destinée aux équipements de chauffage micro-ondes, aux réseaux hertziens point à point, et autres dispositifs industriels et médicaux émettant des signaux puissants et perturbateurs.

En 1985 les autorités de régulation ont autorisé l'utilisation de cette bande très perturbée (et donc inutilisable pour des applications « nobles ») pour les réseaux locaux, avec un accès libre sans licence, à condition que les dispositifs mis en œuvre respectent les exigences suivantes :

- puissance d'émission limitée à 1W aux USA et 100mW en Europe
- insensibilité aux perturbations par l'utilisation d'une technique d'étalement de spectre

Dans la plupart des pays du monde, **la bande Bluetooth va de 2400 à 2483,5 MHz** et cette bande de largeur 79 MHz, est divisée en **canaux de largeur 1 MHz**.

Figure 6.
Les fréquences de travail de Bluetooth dans le monde.

Situation géographique	Bande officielle	Fréquences des canaux	Bande de garde inférieure	Bande de garde supérieure
USA, Europe	2400-2483,5 MHz	2402 + k avec k=0 ...78	2 MHz	3,5 MHz
Japon	2471-2497 MHz	2473 + k avec k=0 ...22	2 MHz	4 MHz
Espagne	2445-2475 MHz	2449 + k avec k=0 ...22	4 MHz	26 MHz

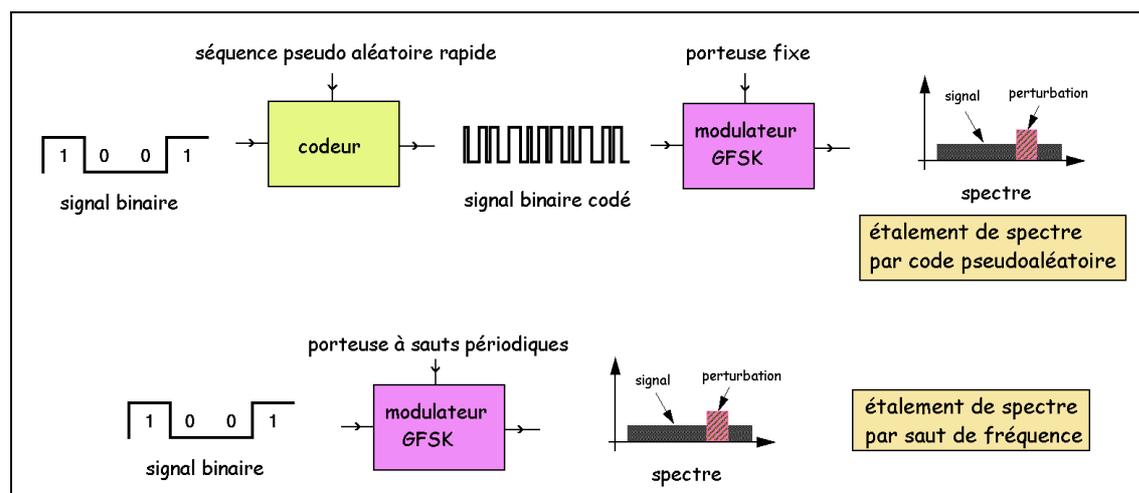
En France, la partie basse de la bande ISM était occupée par les militaires, ce qui posait un problème pour des applications de réseau sans fil comme l'Airport d'Apple et Bluetooth puisque seuls 23 canaux peuvent être utilisés pour une liaison Bluetooth.

Dans un souci de normalisation au niveau mondial, la bande ISM a été libérée par l'armée et ouverte aux équipements Bluetooth à partir du 1^{er} janvier 2001. Une évolution du même type est prévue pour l'Espagne.

L'**étalement de spectre** pour une liaison radio consiste à utiliser une bande de fréquence beaucoup plus large que celle qui est nécessaire, en utilisant l'une des deux techniques suivantes :

- **l'étalement par saut de fréquence**, qui consiste à sauter périodiquement d'un canal à l'autre et qui conduit donc à une utilisation de la totalité des canaux (cas de Bluetooth)
- **l'étalement par code binaire** : on mélange le signal binaire à une séquence numérique pseudo aléatoire de débit nettement plus élevé (cas du téléphone aux USA)

Figure 7.
Les 2 techniques d'étalement de spectre.



Pour fixer les idées, voici quelques exemples chiffrés :

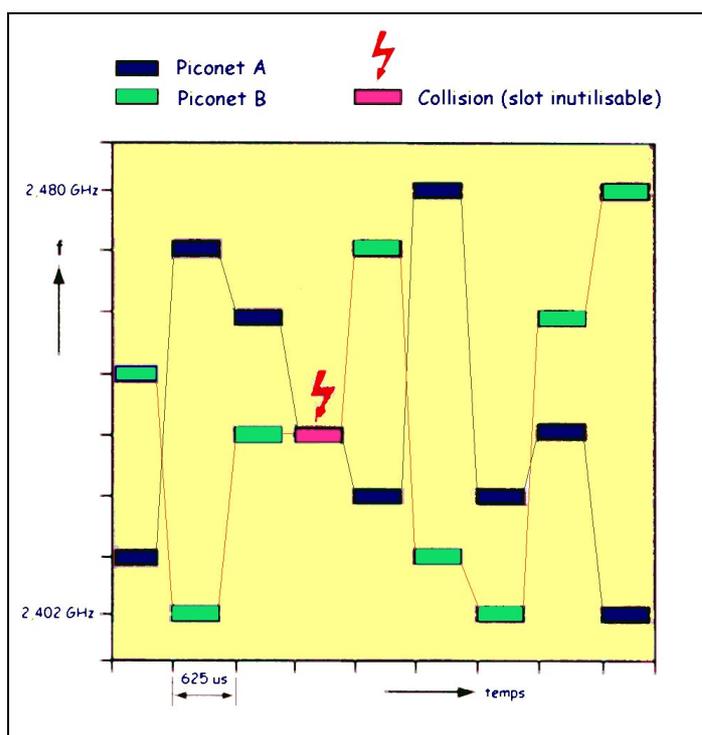
Liaison RF	Débit	Bande nécessaire	Bande utilisée	Etalement
GSM	270 kbits/s	≈ 270 kHz	≈ 270 kHz	non
CDMA/UMTS	9,6 kbits/s	≈ 10 kHz	1,23 MHz	oui, par code
Bluetooth	1 Mbits/s	≈ 1 MHz	≈ 80 MHz	oui, par saut

5- La technique du saut de fréquence

Le saut en fréquence, technique d'étalement de spectre qui permet de rendre une liaison beaucoup moins sensible aux perturbations, fonctionne de la façon suivante pour le Bluetooth :

- l'information est transmise sur une fréquence pendant **un time-slot de 625 μ s**, puis l'émetteur passe sur la fréquence suivante
- les sauts en fréquence ($1/625\mu\text{s} = 1600$ sauts par seconde) ont une **amplitude de 6 MHz** au minimum et sont déterminés par calcul à partir de l'adresse du maître et de l'horloge
- ils sont donc aussi connus par le récepteur qui change de fréquence de manière synchrone avec l'émetteur pour récupérer le signal transmis
- chaque réseau piconet utilise une succession de fréquences différentes, et la probabilité pour que 2 piconets se retrouvent sur la même fréquence reste faible (**collision**)

Figure 8.
Les sauts de fréquence.

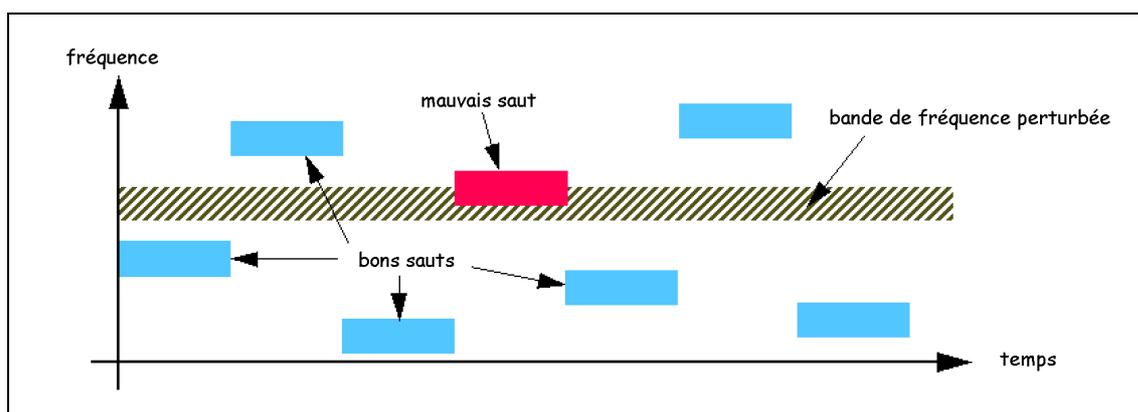


Chaque liaison Bluetooth, à cause des sauts de fréquence, occupe donc la totalité de la bande de fréquence ISM.

Les **signaux perturbateurs** (liaisons point à point, fours à micro-ondes ...) travaillent à fréquence fixe et ne perturberont donc la liaison que de temps en temps et pour une durée très limitée (625 μ s).

Le taux d'erreur global résultant sera bien inférieur au taux d'erreur qu'on aurait eu en travaillant à une fréquence fixe subissant une interférence.

Figure 9.
Perturbation de certains canaux.



6- Les caractéristiques de la liaison radio

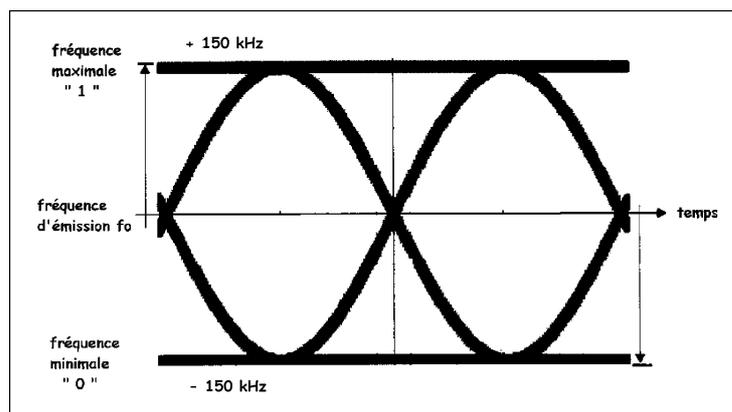
On prévoit, pour les interfaces Bluetooth, 3 catégories de puissance d'émission ou **classes** :

- **classe 1** : puissance maximale émise 100 mW soit 20 dBm, contrôle de la puissance par pas de 2 dB min / 8 dB max dans la gamme 4 dBm - 20 dBm, pouvant être étendu jusqu'à -30 dBm
- **classe 2** : puissance maximale 2,5 mW soit 4 dBm, contrôle de puissance facultatif
- **classe 3** : puissance maximale 1 mW soit 0 dBm, contrôle de puissance facultatif

Les interfaces équipées d'un contrôle de la puissance utilisent la mesure du niveau reçu en sortie de l'étage du récepteur pour augmenter ou diminuer le niveau émis dans le but de réduire le taux d'erreurs à un niveau acceptable, et ce avec une consommation minimale.

La porteuse est modulée en fréquence par le signal binaire filtré par un filtre passe-bas gaussien, ce qui donne une **modulation GFSK** (Gaussian Frequency Shift Keying).

Figure 10.
Les variations de fréquence de la porteuse.



Le spectre du signal émis a une allure semblable à celle d'un signal GSM, mais nettement plus large (**encombrement spectral de 1 MHz**) puisque le débit numérique est de 1 Mbits/s au lieu des 270 kbits/s du GSM.

Le spectre ne tient pas totalement dans le canal de 1 MHz, et on définit un certain gabarit que doit respecter l'émission.

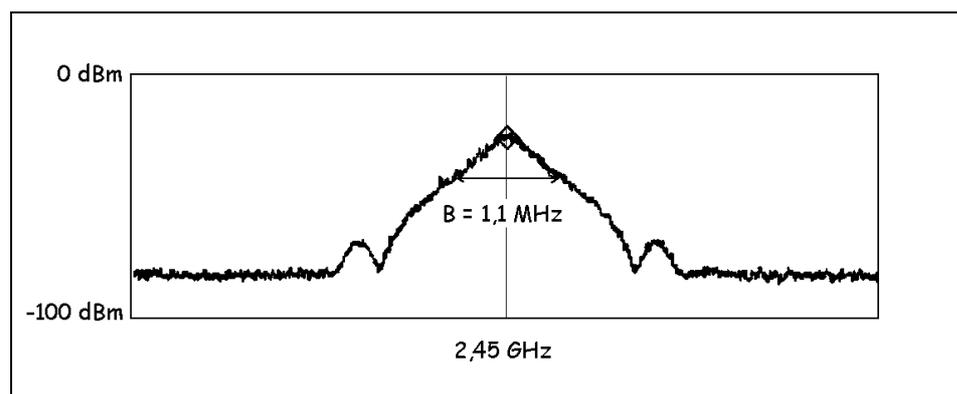
Figure 11.
Gabarit du spectre d'émission.

Offset de fréquence	Niveau émis
0 (canal N)	Po
± 550 kHz	20 dB en-dessous de Po
Canal N ± 2	-20 dBm*
Canal N ± 3,4 ...	-40 dBm*

* : mesurée dans une bande de 100 kHz

Pendant l'émission d'un burst, le spectre a l'allure suivante :

Figure 12.
Allure du spectre d'émission.



7- La portée d'une liaison Bluetooth

Bien qu'il soit très difficile de prévoir la portée exacte d'une liaison RF à l'intérieur d'un local, on peut quand même, à l'aide de quelques règles simples, estimer la portée d'une liaison RF à 2,45 GHz.

Les paramètres qui influent la portée de la liaison sont multiples :

⇒ la puissance émise et le gain de l'antenne

La puissance est un paramètre essentiel, et un dispositif d'adaptation de la puissance émise permet d'optimiser la liaison et de maintenir le taux d'erreur à un niveau suffisamment bas.

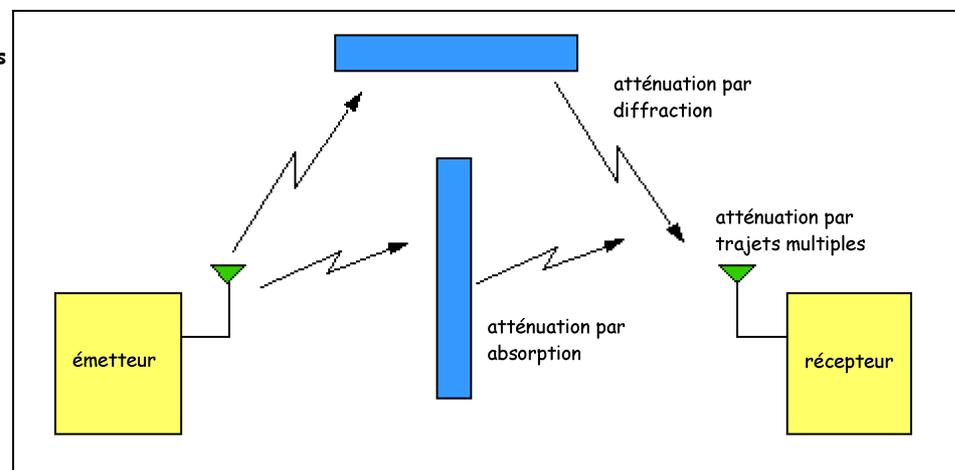
Une antenne de bonne qualité permet d'augmenter la portée, mais est difficile à installer à l'intérieur d'un portable.

⇒ l'environnement

L'onde électromagnétique doit contourner ou traverser plusieurs obstacles (corps humain, cloisons ...) avant d'arriver sur le récepteur. Ces obstacles absorberont une partie de l'énergie émise et la transformeront en chaleur, ce qui diminuera d'autant la portée du système.

L'onde peut aussi être diffractée par un obstacle conducteur et renvoyée dans toutes les directions.

Figure 13.
Les différentes causes d'atténuation du signal.



L'arrivée sur l'antenne du récepteur d'ondes ayant suivi des trajets différents peut aussi conduire à des variations de niveau du signal reçu (interférences constructives ou destructives).

Une règle empirique simple permet de prévoir « en gros » la portée d'une liaison Bluetooth en l'absence d'obstacles :

- atténuation de 50 dB pour les 6 premiers mètres
- atténuation de 10 dB par tranche de 10 mètres supplémentaires

Exemple : une puissance émise de 1 mW est-elle suffisante pour une liaison de 35m ?

Puissance émise : 1 mW = 0 dBm

Atténuation totale : $50 + 3 \cdot 10 = 80$ dB

Niveau reçu : -80 dBm

Sensibilité du récepteur Bluetooth : -70 dBm

la liaison n'est pas possible

L'atténuation totale permise n'est que de 70dB, ce qui correspond à une portée maximale sans obstacle de 26 mètres.

8- Le canal physique de transmission

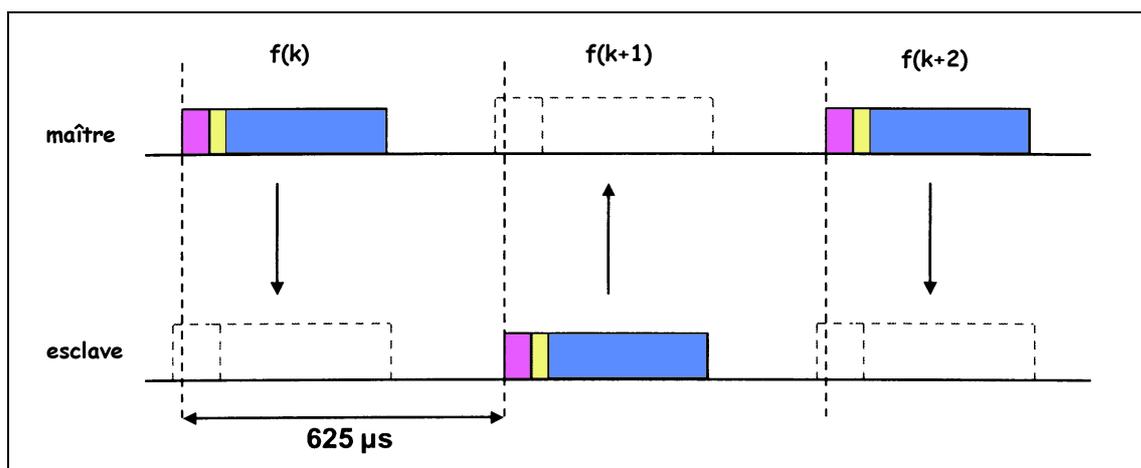
Lorsqu'une interface Bluetooth travaille en émission, elle ne reste sur une fréquence déterminée que durant $625 \mu\text{s}$, durée qui définit un time-slot.

Pour le time-slot suivant, le système émet sur une fréquence différente : c'est la technologie dite « des sauts en fréquence », qui permet une meilleure immunité aux signaux parasites de tous ordre.

Le choix des fréquences successives se fait selon une **séquence pseudo-aléatoire** définie par le système maître et est valable pour tous les systèmes du piconet. Selon les pays, le maître a le choix entre 23 ou 79 fréquences différentes à chaque time-slot.

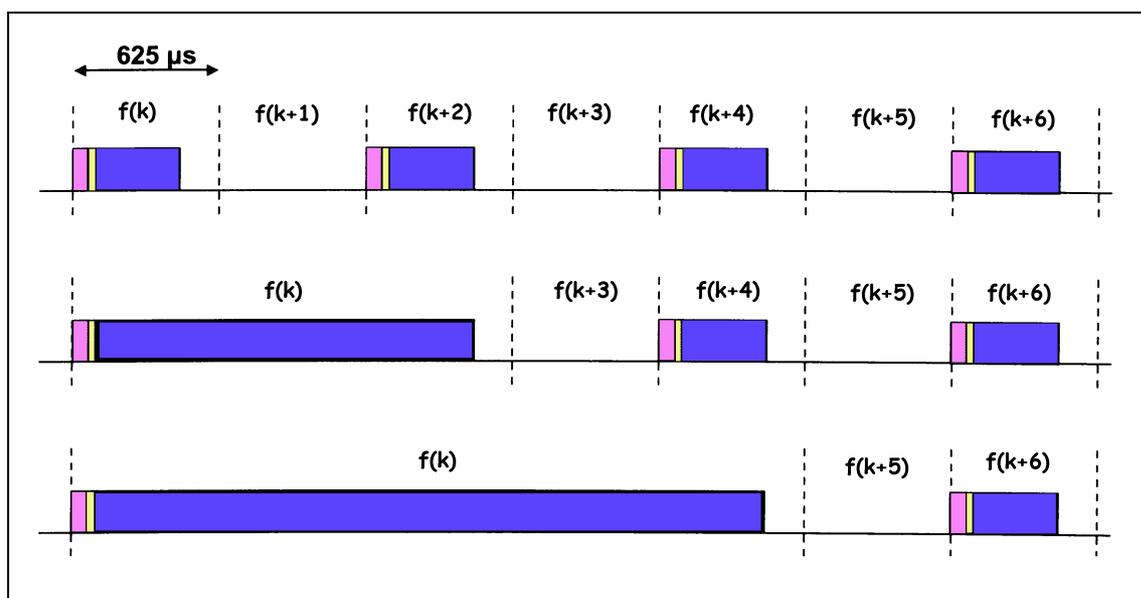
Les **time-slots sont numérotés par le maître**. Dans le cas où maître et esclave émettent alternativement (liaison bidirectionnelle), le maître émet dans les time-slots pairs et l'esclave dans les time-slots impairs.

Figure 14.
Le timing des échanges maître-esclave.



Il peut arriver qu'un paquet de données dépasse la durée d'un time-slot (**possibilité d'utiliser jusqu'à 5 time-slots successifs**). Dans ce cas le saut de fréquence ne se fait pas à la fin du time-slot, mais après transmission du paquet complet.

Figure 15.
Transmission d'un paquet dépassant un time-slot.



Un canal physique de transmission Bluetooth est donc constitué d'un ensemble de time-slots et de leur fréquence associée :

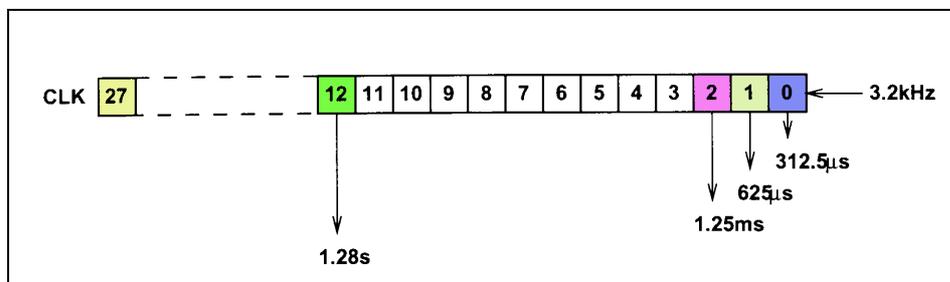
- durée du time-slot $625 \mu\text{s}$
- nombre de sauts de fréquences par seconde : 1600
- nombre de fréquences différentes : 79 (23 dans certains pays)
- numérotation des time-slots de 0 à $2^{27}-1$

9- La synchronisation temporelle du piconet

Chaque module Bluetooth possède une horloge à 13 MHz indépendante qui n'est pas à l'abri de dérives, mais jamais ajustée : c'est **l'horloge locale** (native clock CLKN)

Cette horloge à 13 MHz est traitée par un compteur 28 bits, qui fournit en sortie l'intervalle de temps T le plus faible : $T = 312,5 \mu\text{s}$ soit 3,2 kHz.

Figure 16.
Fabrication de la durée du time-slot.



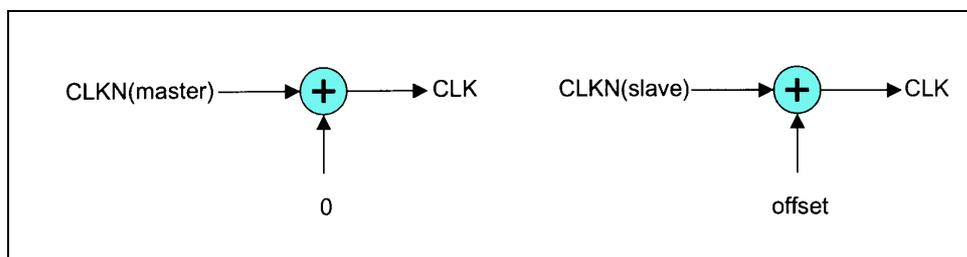
Si cette horloge dérive, la durée du time-slot n'est plus bien définie au niveau du module esclave, et la communication avec le maître devient impossible.

C'est la raison pour laquelle, dans un piconet, tous les esclaves se synchronisent sur l'horloge du maître, même si celle-ci n'est pas exactement à 13 MHz. Cette synchronisation subsiste pendant toute la durée de vie du piconet et fournit à chaque esclave une horloge CLK calée sur celle du maître.

La synchronisation se fait en rajoutant un décalage (offset) positif ou négatif à la période T native, pour la rendre égale à celle du maître.

Ce décalage est par principe nul pour le maître, et différent pour chaque module esclave.

Figure 17.
Elaboration de l'horloge dans le maître et les esclaves.



Du fait de la relative imprécision entre les horloges du maître et de l'esclave, le standard Bluetooth prévoit que les paquets radio transmis soient plus courts que les 625 μs que durent les time-slots.

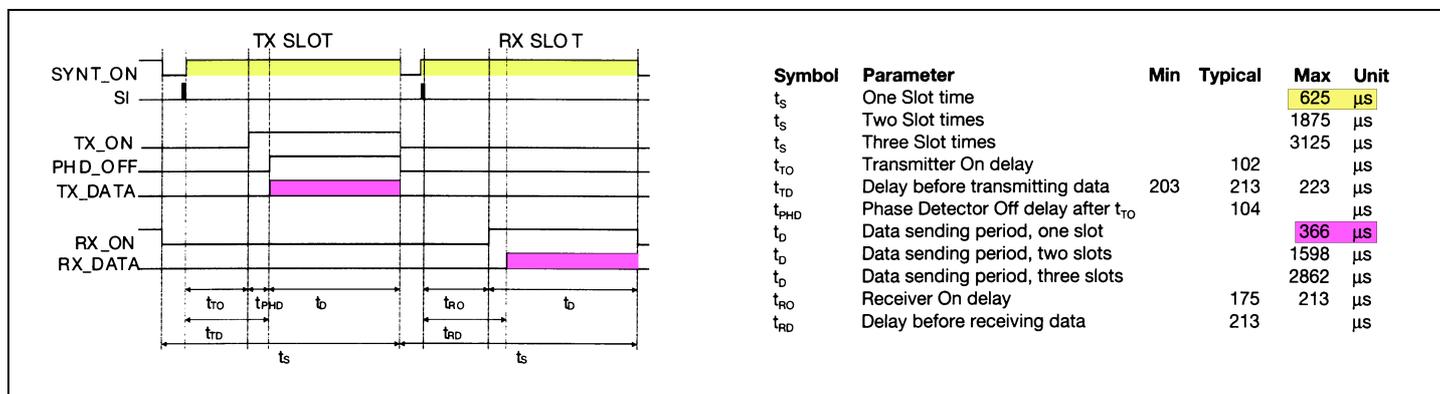


Figure 18. Longueur des paquets par rapports aux time-slots.

Ainsi pour un paquet occupant 1 seul time-slot, la longueur ne dépasse pas 366 μs .

10- Les deux types de liens maître-esclave

Deux types de liens peuvent être mis en place entre le maître et l'esclave :

⇒ **un lien synchrone ou SCO** (Synchronous Connection Oriented)

- lien point à point entre le maître et un unique esclave du piconet
- le maître réserve des slots à intervalle régulier, et dans ce sens le lien SCO s'apparente à une liaison « commutée »
- ce type de lien est utilisé pour transmettre des données dépendant du temps comme la voix
- le maître peut gérer jusqu'à 3 liens SCO, avec le même esclave ou des esclaves différents
- un esclave peut gérer jusqu'à 3 liens SCO avec le même maître, ou 2 liens SCO au maximum avec des maîtres différents
- ce lien est initialisé par un message du maître contenant la valeur de l'intervalle T_{SCO} entre deux time-slots réservés à cette fonction.
- l'esclave est autorisé à répondre dans le time-slot suivant le time-slot de réception, à moins qu'un autre esclave ait été adressé (fin des échanges avec un esclave par exemple)

⇒ **un lien asynchrone ou ACL** (Asynchronous Connection Less)

- en dehors des slots réservés pour les échanges synchrones, le maître peut utiliser les autres time-slots pour échanger des données avec n'importe quel esclave du piconet
- un seul lien ACL peut exister entre un maître et un esclave
- contrairement aux paquets SCO qui ne sont jamais renvoyés, les paquets ACL reçus peuvent être renvoyés vers l'expéditeur pour vérifier l'intégrité des données transmises
- comme dans la liaison SCO, l'esclave est autorisé à répondre dans le time-slot suivant le time-slot de réception, à moins qu'un autre esclave ait été adressé
- les paquets ACL qui ne sont pas destinés à un esclave particulier sont appelés « broadcast » et seront lus par tous les esclaves

Les données dans les paquets peuvent être protégées contre les erreurs de transmission et cette protection est adaptative, ce qui signifie que si la liaison est très bonne, la protection contre les erreurs est sacrifiée en faveur du débit.

La correction d'erreur en aval, dite FEC (Forward Error Correction) à deux étages, n'intervient que lorsque la communication éprouve des difficultés.

Figure 19.
Variation du débit en fonction de la protection et du mode.

FEC	slots	Débit symétrique	Débit asymétrique
sans	1	2x172,8 kbits/s	172,8+172,8 kbits/s
sans	3	2x384,0 kbits/s	576,0+ 86,4 kbits/s
sans	5	2x432,6 kbits/s	721,0 + 57,6 kbits/s
avec	1	2x108,8 kbits/s	108,8 + 108,8 kbits/s
avec	3	2x256,0 kbits/s	384,0 + 54,4 kbits/s
avec	5	2x286,7 kbits/s	477,8 + 36,3 kbits/s

A cette protection par code s'ajoute, sauf pour les canaux vocaux où la perte d'un paquet n'est pratiquement pas sensible, une **demande automatique de retransmission ARQ** (Automatic Retransmission Query).

Ce moyen permet de demander qu'un paquet soit retransmis en totalité (cas de la collision par exemple).

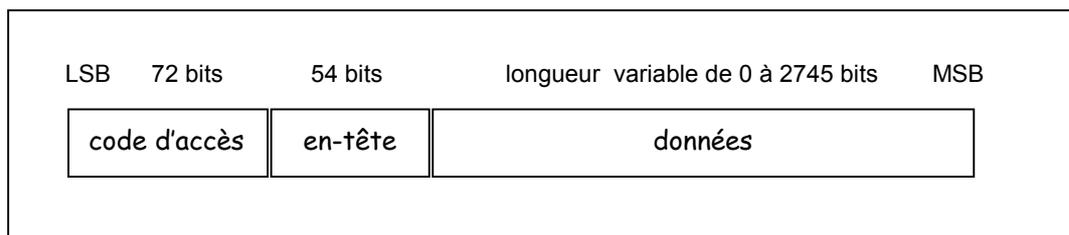
L'en-tête de chaque paquet est toujours protégé par une correction d'erreur en aval (FEC) donc, même si la correction FEC a été désactivée, il est possible de demander la retransmission d'un paquet par ARQ lorsque des perturbations apparaissent.



11- Le format du paquet de données

Un paquet transmis a une structure constituée de 3 champs : le code d'accès, l'en-tête et les données proprement dites.

Figure 20.
Format d'un
paquet.



⇒ **code d'accès** : chaque paquet débute par un code d'accès utilisé pour la synchronisation des esclaves et l'identification du canal.

- le code d'accès de canal ou CAC (Chanel Access Code) est propre à un piconet. Tous les paquets échangés dans un piconet débutent donc par le même code d'accès de canal.
- le code d'accès de composant ou DAC (Device Access Code) est utilisé pour des applications de signalisation comme le paging.
- le code d'accès de recherche ou IAC (Inquiry Access Code) est utilisé lorsque le maître recherche d'autres équipements Bluetooth du piconet.

⇒ **en-tête** : ce champ contient dans l'ordre l'adresse de l'esclave qui échange des données, le type de paquet et des bits de contrôle (erreurs, buffer de réception ...)

- les adresses des esclaves (7 au maximum) sont codées sur 3 bits et sont affectées temporairement aux esclaves actifs, les autres étant en mode « parked ».
- on distingue 16 types de paquets différents (type codé sur 4 bits) selon qu'il s'agit d'une liaison SCO ou ACL et que le paquet occupe 1 ou plusieurs time-slots.

Figure 21.
Les différents
types de
paquets.

Code	slots	SCO	ACL	utilisation
0000	1	NULL	NULL	paquet ne transportant aucune donnée, informe le maître sur le succès de la transmission, l'état du buffer ...
0001	1	POLL	POLL	idem, mais du maître vers l'esclave pour l'obliger à répondre même s'il n'a rien à dire
0010	1	FHS	FHS	paquet de contrôle permettant entre autres de synchroniser les esclaves à la mise en place du piconet
0011	1	DM1	DM1	transporte des données (Data Medium), protégées par code 2/3 FEC et code CRC
0100	1		DH1	idem à DM1, mais sans code de protection CRC
0101	1	HV1		transporte des données vocales (High quality Voice) sur 240 bits, protégées par code 1/3 FEC, 1,25 ms de voix à 64 kbits/s, tous les 2 slots ($T_{SCO}=2$)
0110	1	HV2		transporte des données vocales sur 240 bits, protégées par code 2/3 FEC, 2,5 ms de voix à 64 kbits/s, à transmettre tous les 4 slots ($T_{SCO}=4$)
0111	1	HV3		transporte des données vocales sur 240 bits, non protégées, 3,75 ms de voix à 64 kbits/s, à transmettre tous les 6 slots ($T_{SCO}=6$)
1000	1	DV		transporte à la fois des données et de la voix non protégée
1001	1		AUX1	idem à DM1, mais les données ne sont pas protégées du tout
1010	3		DM3	idem à DM1, mais le paquet est plus long et utilise 3 time-slots
1011	3		DH3	idem à DH1, mais le paquet est plus long et utilise 3 time-slots
1100	3			
1101	3			
1110	5		DM5	idem à DM1, mais le paquet est plus long et utilise 5 time-slots
1111	5		DH5	idem à DH1, mais le paquet est plus long et utilise 5 time-slots

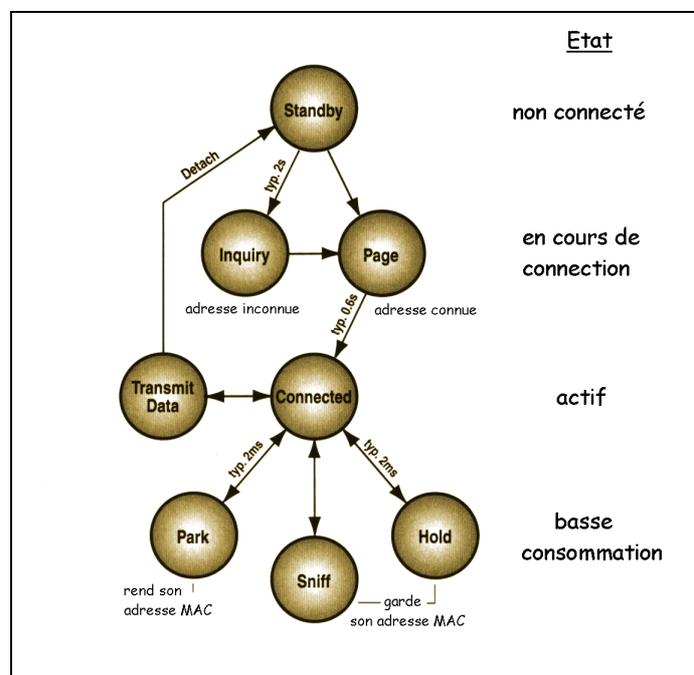
12- La mise en place d'une liaison dans un réseau

Un dispositif Bluetooth peut se connecter à 7 autres appareils, dans un rayon de 10 mètres, constituant ainsi un réseau provisoire appelé piconet.

Les modules Bluetooth qui font partie d'un piconet entrent en liaison de la façon suivante :

- ils sont au départ en **mode d'attente** et cherchent la présence de transmissions à proximité toutes les 1,28 secondes. Pour cela, ils écoutent successivement 32 « porteuses d'éveil » parmi les 79 fréquences (16 en France pour le moment)
- le module Bluetooth qui souhaite communiquer envoie des **requêtes en mode Inquiry** si les adresses sont inconnues (imprimantes, fax ...), et en **mode Page** si elles sont connues par les porteuses d'éveil auquel répondent les modules situés à proximité. Ce module devient alors le maître du piconet, et son adresse définit la suite des sauts en fréquence suivie par les esclaves concernés
- les autres modules (esclaves) **se synchronisent** sur l'horloge du maître, et répondent avec leur **numéro d'identification**. Le maître sait maintenant quels sont les modules présents et connaît leur adresse respective. Si plusieurs appareils répondent et que l'utilisateur désire une connexion point à point, il peut sélectionner le dispositif qui l'intéresse.

Figure 22.
Les différents états de la liaison.



- une fois l'adresse de l'autre module obtenue, le maître peut passer en **mode d'appel** (Page Mode) et définit avec le module esclave visé le type et les caractéristiques de la liaison qu'il veut mettre en place
- la liaison sera établie (état : Connected) au bout d'environ 0,6 secondes, tout est prêt alors pour la transmission des données (Transmit Data)

Après l'échange de données, le module Bluetooth peut retourner en mode d'attente ou adopter l'un des trois états à faible consommation :

- le **mode de maintien** (Hold) au cours duquel l'appareil reste actif dans le piconet. Lorsque le temporisateur interne de l'esclave vient à expiration, l'esclave s'annonce brièvement au maître avant de recommencer le compte à rebours. Un esclave en mode de maintien peut passer immédiatement à la transmission des données
- le **mode « renifleur »** (Sniff), l'esclave est programmé pour se mettre périodiquement à l'écoute du piconet afin de déterminer si ce dernier désire lui envoyer des données
- le dernier mode à faible consommation fait appel au **parcage des esclaves** (Park). Dans ce cas, l'esclave se relire du piconet et rend son adresse MAC (Media Access Control, de 0 à 7). Il ne fait alors plus rien d'autre que de se synchroniser à longs intervalles avec le maître de son piconet

13- Structure et caractéristiques d'un module Bluetooth

Pour être intéressante, une interface Bluetooth devra être à terme proposée aux alentours de 5\$ en volume, soit trois à quatre fois moins cher qu'actuellement.

Pour arriver à un prix aussi dérisoire, l'intégration poussée est une alternative viable vu les quantités espérées. De plus le standard, à vocation économique, facilite la tâche des fabricants de silicium en n'ayant pas imposé de contraintes drastiques.

Une interface Bluetooth est donc constituée des éléments suivants :

- un **synthétiseur de fréquence**, qui sert alternativement pour l'émission et la réception
- le VCO du synthétiseur doit être **modulable en fréquence**
- un **amplificateur RF** de faible puissance (donc intégrable)
- d'une **antenne** (la moins encombrante possible)
- un **récepteur** à changement de fréquence à fi moyenne, faible ou même nulle (conversion directe)
- un **processeur bande de base** qui gère la liaison et produit le signal binaire filtré (filtre gaussien)

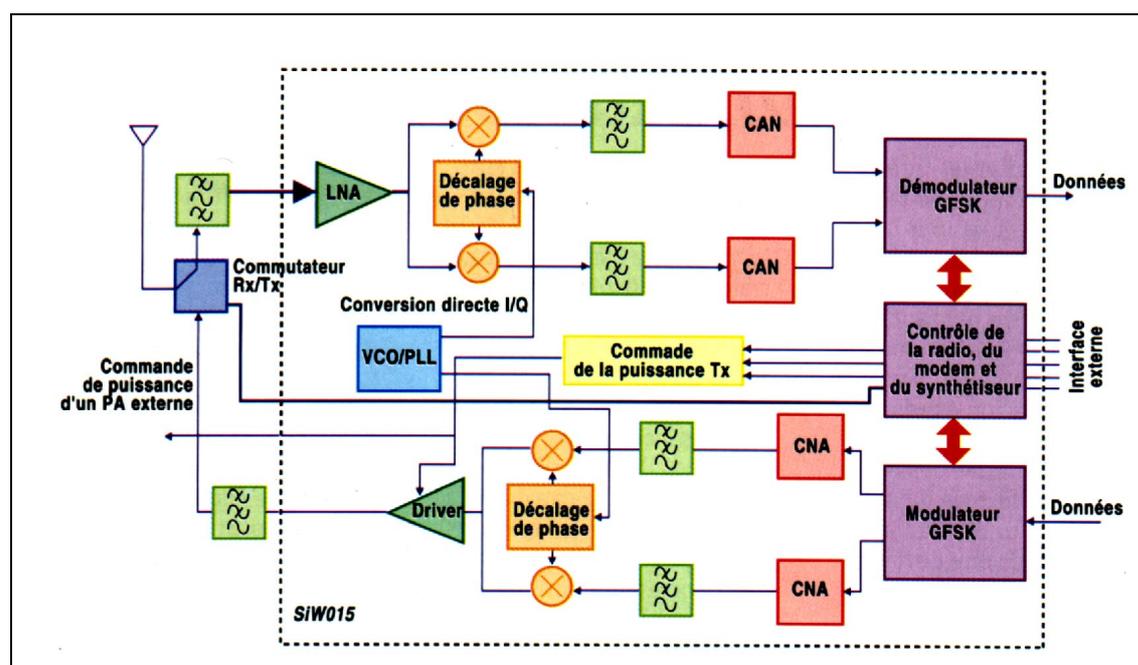
Le souci de miniaturisation et d'abaissement des coûts conduit les concepteurs de modules Bluetooth à travailler en réception avec une « fi » faible ou nulle, ce qui permet de remplacer les filtres fi à onde de surface par un filtrage numérique dans le processeur bande de base.

Figure 23.
Caractéristiques principales d'un module Bluetooth.

Émetteur		Récepteur	
Puissance nominale	0dBm	Sensibilité	-70dBm
Gamme possible	-30 à +20dBm	IP ₃	-16dBm
Indice de modulation	0.28 – 0.35	CP _{1dB}	-6dBm
Déviation de fréquence	<75kHz	Bande passante fi	1.0MHz
Niveau canal adjacent	-20dBm	C/I _{co-canal} (0.1% BER)	11dB
Emissions hors bande	50dB	C/I _{1MHz} (0.1% BER)	-8dB
Contrôle de puissance	-30 - +20dB	C/I _{S 2MHz} (0.1% BER)	-40dB
Générales		C/I _{AWGN} (0.1% BER)	18dB
Précision du timing	20ppm	Réjection f- image	20dB
L _{500kHz}	-89dBc/Hz		
L _{S 2MHz}	-121dBc/Hz		
Temps de com. canal	220 μs		
Temps de com. RX/TX	220 μs		

Voici un **exemple de structure d'un circuit RF** travaillant à une fréquence intermédiaire nulle. Les filtres RF sont deux filtres à onde de surface, le filtrage fi (passe-bas à 1 MHz) étant réalisé par des filtres R,C.

Figure 24.
Schéma fonctionnel du module RF de Silicon Wave.

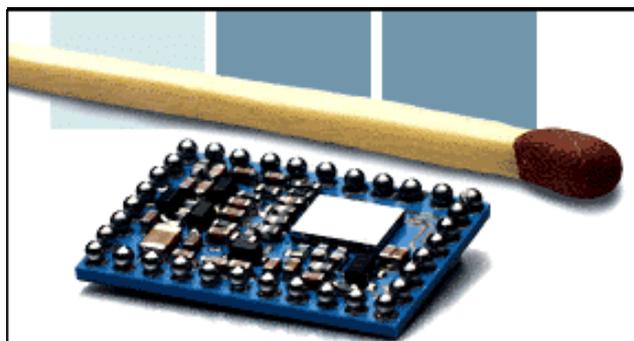


14- Exemple du module radio Bluetooth Ericsson

Le **PBA 313 01/2** du Suédois est historiquement le premier module hybride RF dédié aux applications Bluetooth :

- le circuit RF est un Asic Bi-Cmos, qui réalise les fonctions d'émission classe 2 (+4dBm max) et de réception
- autour de ce circuit gravitent le filtre de boucle, le circuit d'accord du VCO, le commutateur et le filtre d'antenne, les transformateurs baluns des voies Rx et Tx pour un fonctionnement en mode équilibré
- la modulation GFSK est réalisée au niveau du VCO dont les éléments critiques sont ajustés au laser
- le récepteur est à changement de fréquence, avec une fréquence intermédiaire à 3 MHz, et sa sensibilité en réception est conforme aux exigences soit meilleure que - 70 dBm pour un taux d'erreur de 0.1%

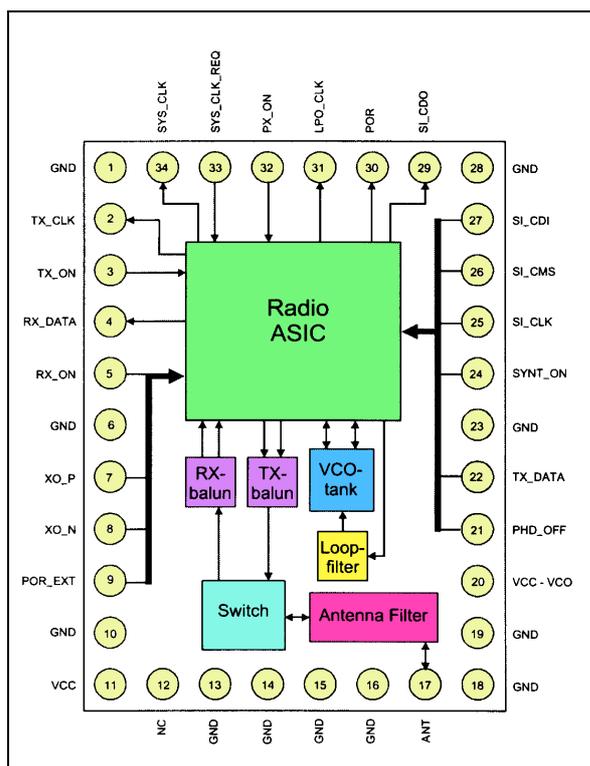
Figure 25.
Le module RF
Ericsson.



Sous une tension d'alimentation de 2.8V, le PBA 313 consomme typiquement 40 mA en mode réception, 35 mA en émission et moins de 100 μ A en veille. Le composant est présenté en boîtier BGA de 14x 10.2x 1,6mm.

Un sous-système radio complet se verra adjoindre une antenne 50 Ω et une référence de fréquence à 13 MHz..

Figure 26.
Structure
interne du
module RF.

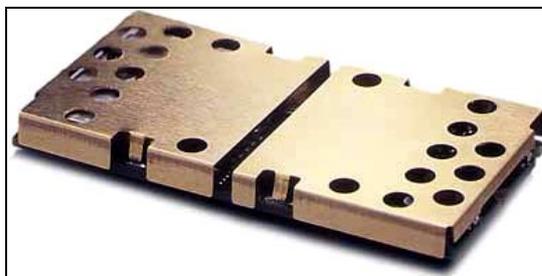


15- Le module Bluetooth Ericsson complet

Sous la forme d'un module blindé de 33 x17x3mm, Ericsson propose par ailleurs une solution Bluetooth complète, supportant les transmissions voix-données, directement insérable dans un PC portable, un périphérique d'ordinateur, un accessoire pour téléphone mobile, etc.

Ce « super-module » **ROK 101 007** réunit le module RF précédent, le quartz à 13 MHz, les régulateurs de tension, la mémoire flash et le contrôleur bande de base.

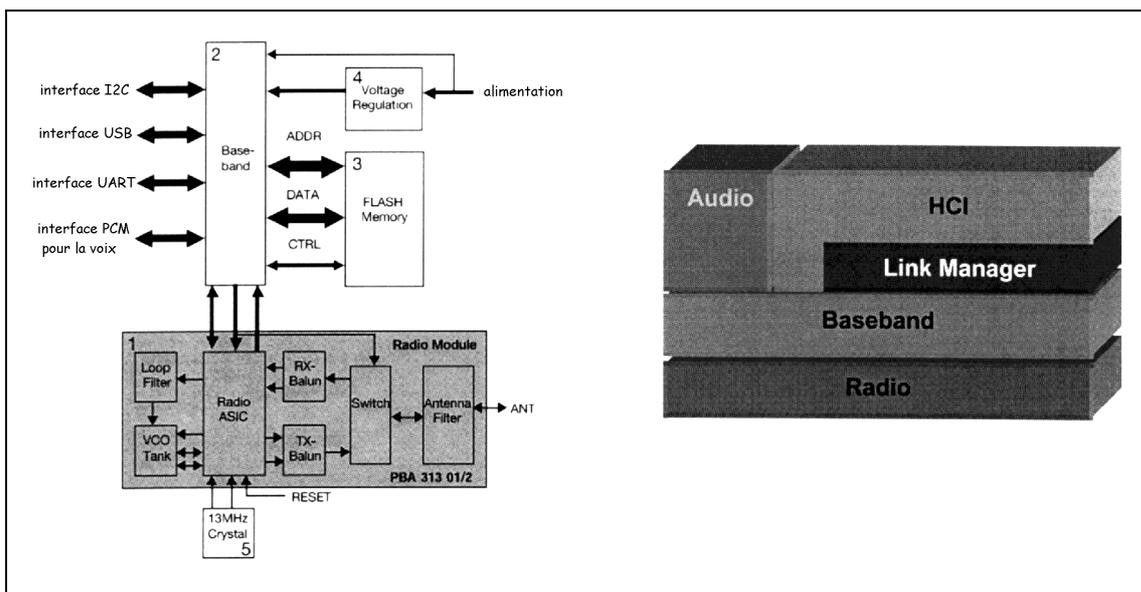
Figure 27. Allure du module Bluetooth complet.



Le module communique avec l'extérieur via des interfaces USB, UART ou PCM pour le codec audio.

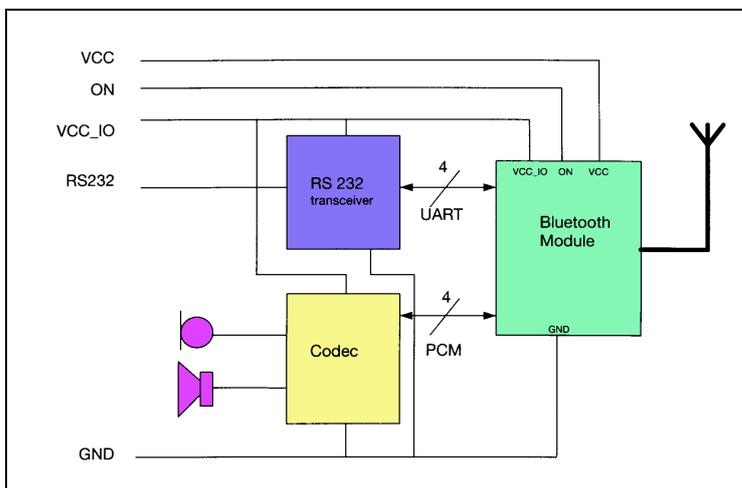
Le logiciel en mémoire flash inclut l'interfaçage avec le contrôleur hôte et les protocoles relatifs à la gestion de la liaison (Link Manager).

Figure 28. Structure interne du module .



Associé à quelques boîtiers, ce module peut-être facilement utilisé pour une liaison voix-données .

Figure 29. Exemple d'utilisation.



16- La cohabitation Bluetooth-GSM

La présence côte à côte dans un téléphone portable d'un bloc RF GSM/DCS de puissance maximale 2W et d'un module Bluetooth de puissance plus faible peut être à l'origine d'interférences gênantes et nécessite une conception soignée.

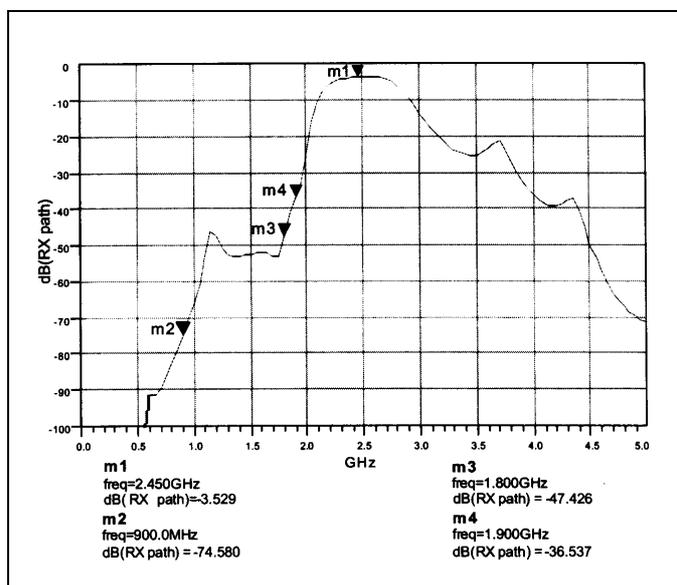
Deux problèmes peuvent survenir :

⇒ **l'émetteur du téléphone cellulaire bloque le récepteur Bluetooth**

L'interférence provient du bruit large bande généré par l'émetteur du téléphone dont une partie tombe dans la bande Bluetooth. Le niveau de ce bruit peut être suffisant pour perturber la réception du signal Bluetooth.

La puissance du GSM pouvant monter à 2W et la sensibilité du récepteur Bluetooth étant de 10 pW, l'atténuation apportée par les filtres doit être importante dans les bandes considérées, et il faut absolument éviter des pics parasites à 2,4 GHz dans les filtres GSM.

Figure 30.
Courbe de gain des étages d'entrée d'un module Bluetooth.



Pour fixer les idées, le bruit généré par le GSM autour de 2,4 GHz et mesuré dans une bande de 1 MHz de large doit avoir un niveau inférieur à -100 dBm. Si ce n'est pas le cas, un réjecteur à 2,4 GHz doit être rajouté en sortie de l'étage RF du GSM.

Notons que ce problème se posera avec plus d'acuité dans les futures systèmes UMTS qui travailleront dans la bande des 2,1 GHz, très proche de la bande Bluetooth.

⇒ **l'émetteur du Bluetooth bloque la réception GSM**

Le problème est le même, mais se pose avec moins d'acuité puisque la puissance de l'émetteur Bluetooth est plus faible.

Les émissions parasites hors-bande du module Bluetooth doivent également rester en-dessous d'un niveau minimal défini par la norme.

Figure 31.
Niveau des émissions parasites hors-bande.

Bande de fréquence	Mode actif	Mode veille
30 MHz – 1 GHz	-36 dBm	-57 dBm
1 GHz – 12,75 GHz	-30 dBm	-47 dBm
1,8 GHz – 1,9 GHz	-47 dBm	-47 dBm
5,15 GHz – 5,3 GHz	-47 dBm	-47 dBm

Des tests de sensibilité à des signaux parasites en bande ISM et hors bande doivent également être prévus pour valider les circuits de réception (émission sur un canal adjacent, émission à la fréquence image ...)

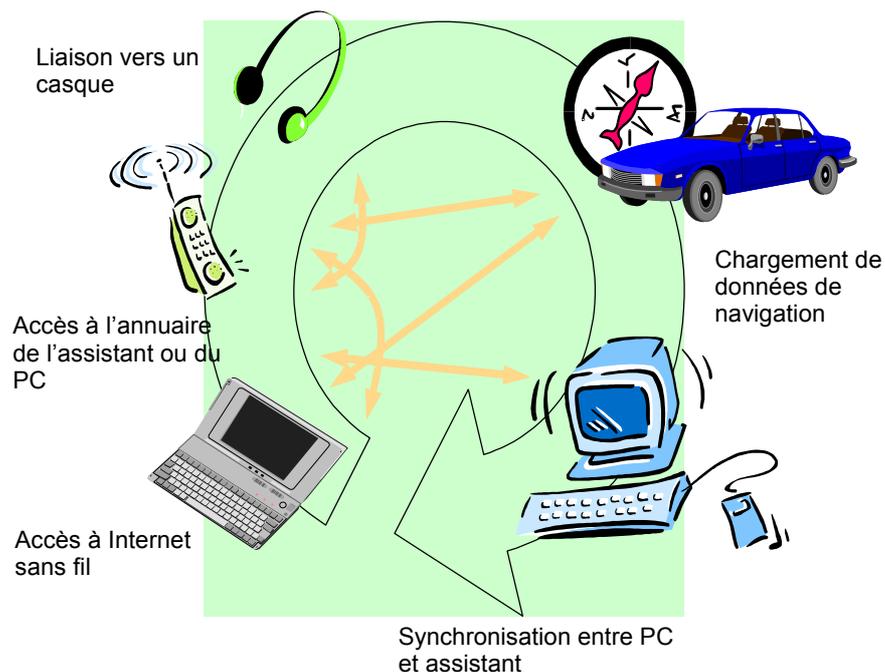
17- Les tests d'un module Bluetooth

L'utilisation d'un module Bluetooth standard ne dispense pas le fabricant de matériel de la vérification des caractéristiques principales de ce standard.

Un certain nombre de paramètres peuvent en effet avoir une influence sur la qualité de fonctionnement de la liaison : puissance émise, interférences et couplages avec la partie GSM, sensibilité du récepteur une fois installé dans le boîtier ...

Les tests sont faits par un équipement spécifique, qui permet de vérifier les spécifications principales comme :

- **la puissance émise**, mesurée durant l'émission d'une salve, le réglage de la puissance
- **la fréquence d'émission**, sa stabilité durant un time-slot, le temps de commutation d'un canal à l'autre
- **la qualité de modulation** pour différentes séquences binaires, l'excursion en fréquence, le filtrage Gaussien
- **le taux d'erreur** (BER : Bit Error Rate) : le testeur transmet une séquence au module Bluetooth qui le renvoie au testeur. Les spécifications Bluetooth imposent une mesure sur 1,6 millions de bits



Quelques liens utiles

<http://www.bluetooth.com/developper/specifications/core.asp>

téléchargement de tous les documents décrivant les différents aspects de la norme Bluetooth

http://bluetooth.ericsson.se/support/bluetooth_external/content/menu.html

site Ericsson sur le Bluetooth

<http://www-us.semiconductors.com/technology/bluetooth>

site Philips sur le Bluetooth

<http://www.palowireless.com/bluetooth/technology.asp>

portail Bluetooth avec de nombreux liens vers les fabricants de composants, accessoires et logiciels