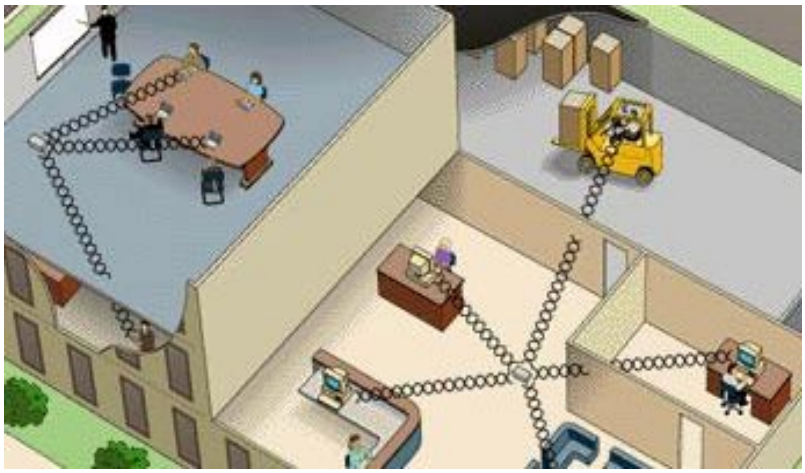
Wireless LAN :

techniques RF, Wifi, Bluetooth



jean-philippe muller

Version mai 2002

Sommaire

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 :

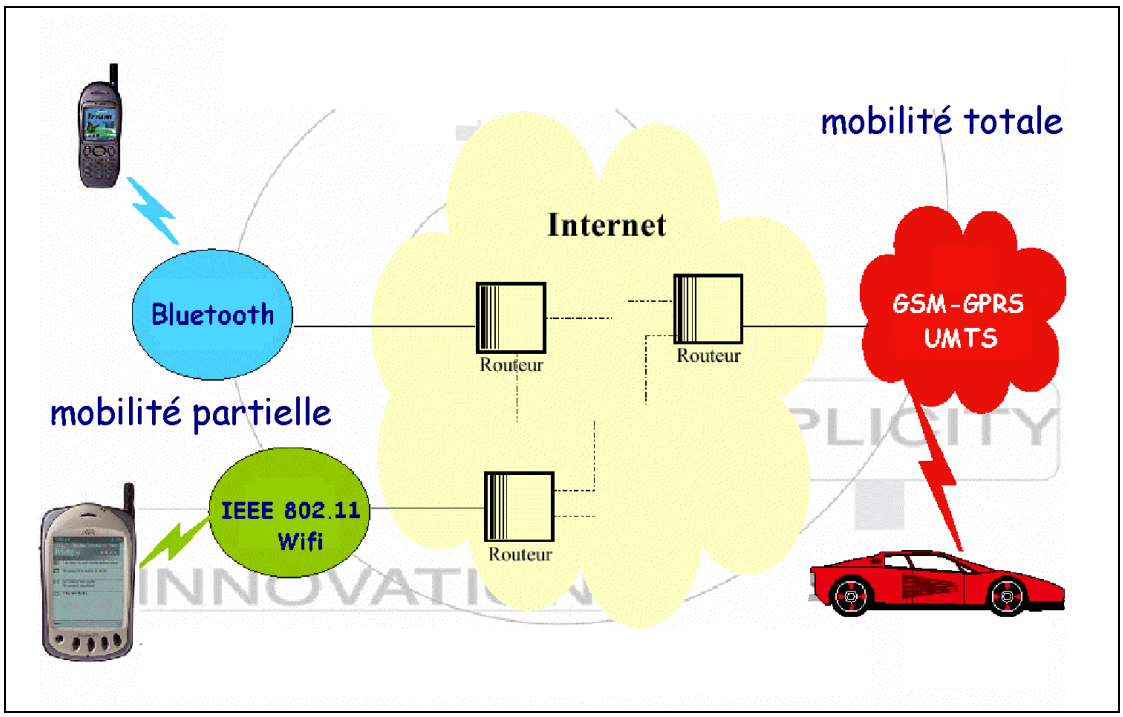
- mise en place d'un réseau dans un bâtiment classé « monument historique »
- mise en place d'un réseau de courte durée (chantiers, expositions, locaux loués, formations)
- accès aux informations enregistrées sur chaque patient pendant les visites dans les hôpitaux
- accès à une connexion Internet pour 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 opérateur 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.

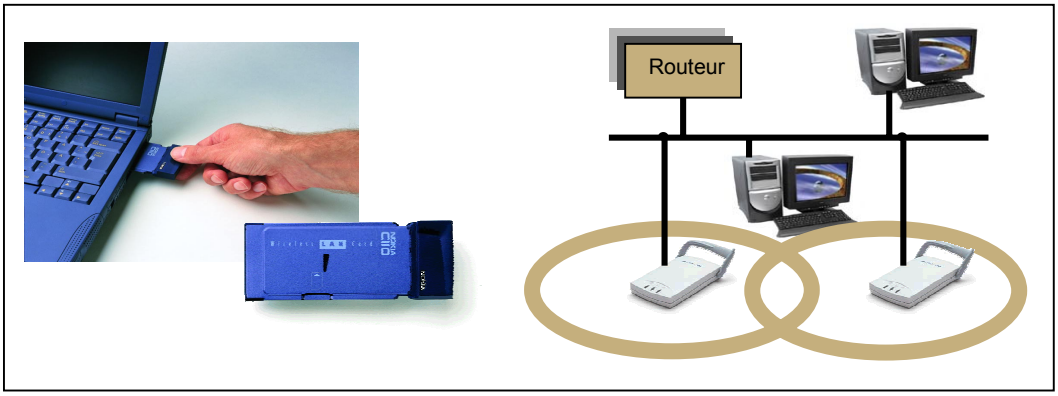
La norme **Bluetooth** lancée par Ericsson et Nokia (ainsi nommée en l'honneur du roi danois Harald Blaatand qui se traduit par Harald à la dent bleue**)** semble la mieux adaptée pour ce type de liaison et prend le pas sur la norme **HomeRF**, les premiers objets Bluetooth (téléphones, PDA...) étant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

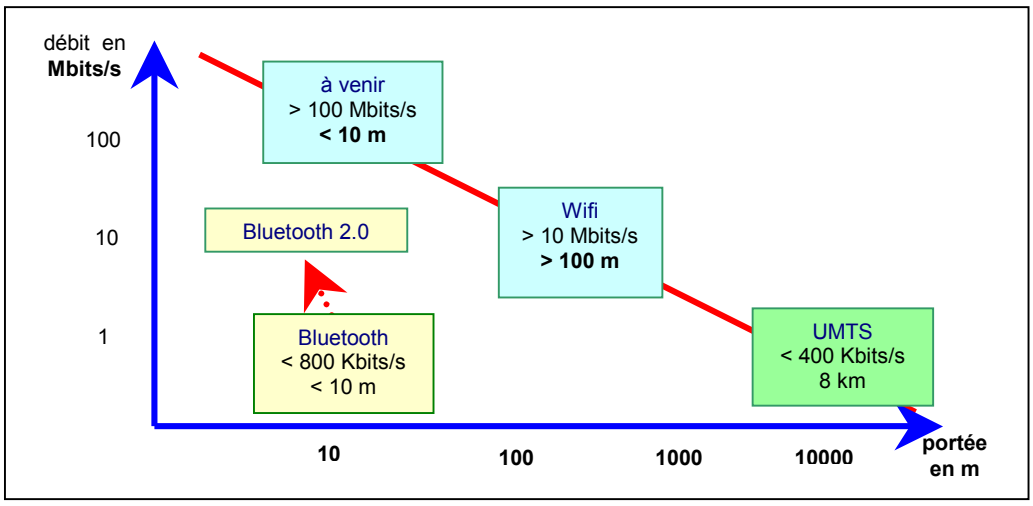
Figure 4.
Les différentes applications des réseaux radio.

	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 .



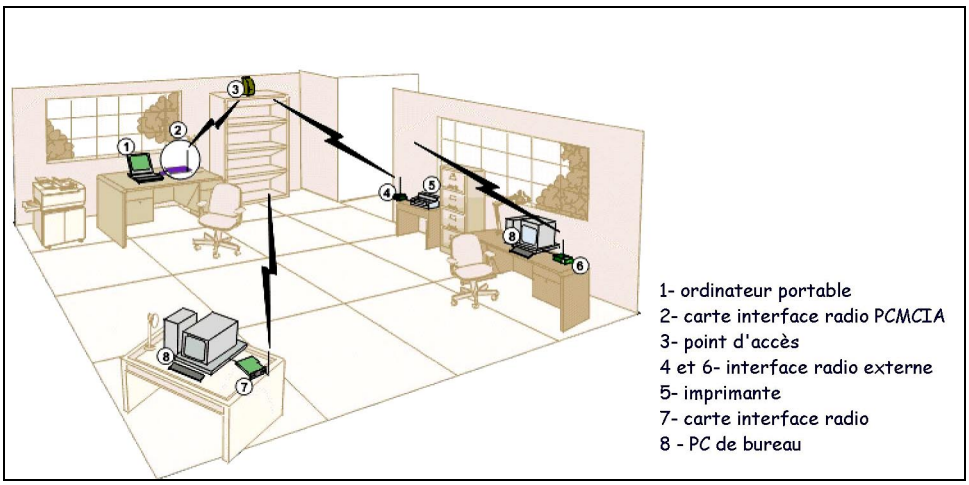
4- Topologie de réseau : le mode « infrastructure »

Les WLAN peuvent fonctionner de deux façon 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 communication 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.

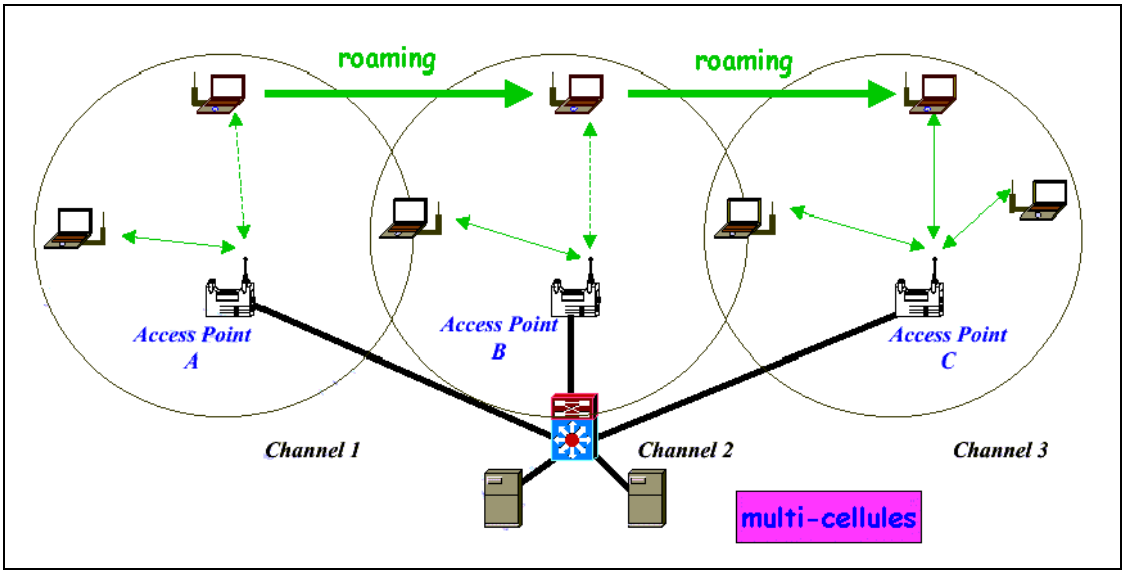


Les équipements mobiles communiquent entre eux en passant par un point d'accès, bien que dans certains cas particuliers un échange direct entre deux interfaces soit possible :

- 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.



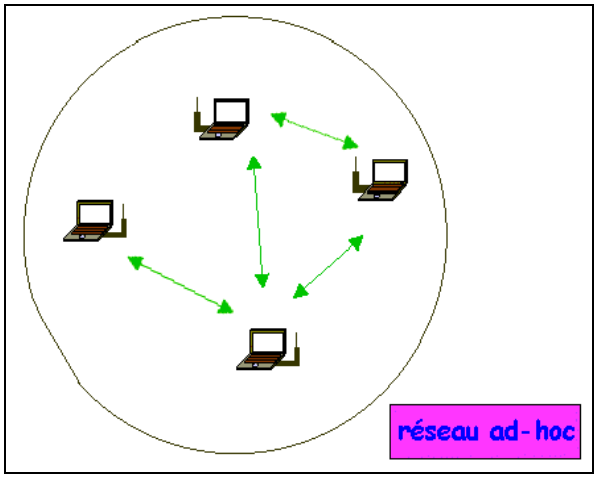
Remarque : dans certains cas, les différentes cellules se superposent complètement, ce qui permet d'offrir plusieurs fréquences aux utilisateurs de la cellule, et donc un débit plus satisfaisant.

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 :

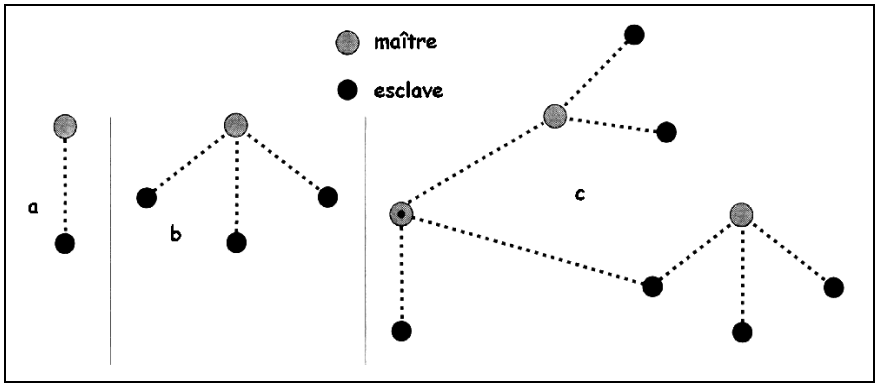
- le réseau ad hoc est auto-configurable : lorsque deux machines mobiles se retrouvent dans le même secteur géographique, elles peuvent se reconnaître puis échanger des données.
- chaque machine peut échanger des informations avec n'importe quelle autre machine
- dans le mode de fonctionnement le plus 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.

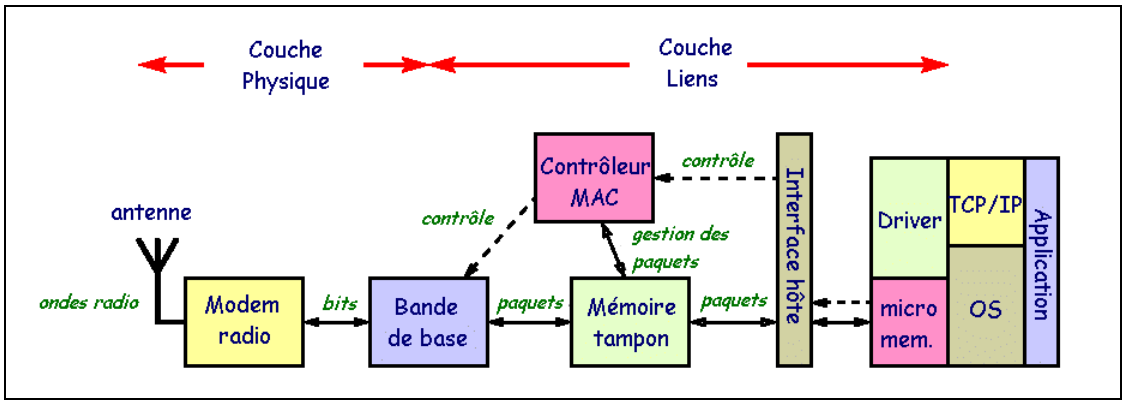


Figure 10. Structure d'une interface radio.

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.

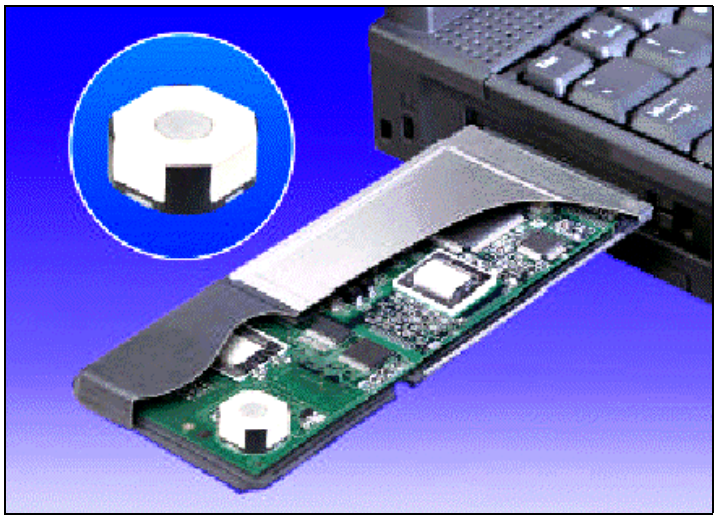


Figure 11. Exemple d'interface radio PCMCIA.

7- Les fréquences de travail

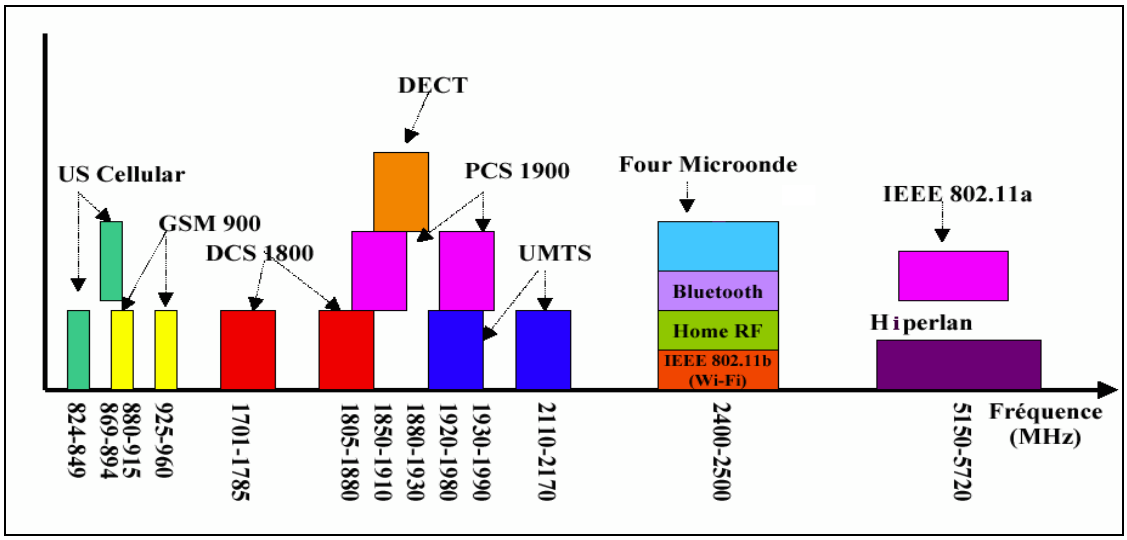
Les bandes de fréquences affectées aux réseaux locaux radio sont les **bandes ISM** (Industrial, Scientific and Medical), destinées à l'origine aux équipements de chauffage micro-ondes, aux réseaux hertziens point à point et à divers dispositifs industriels et médicaux. Deux bandes sont utilisées :

- la **bande des 2,4 GHz**, qui a l'avantage d'être commune à la plupart des pays, pour les standards IEE802.11b (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

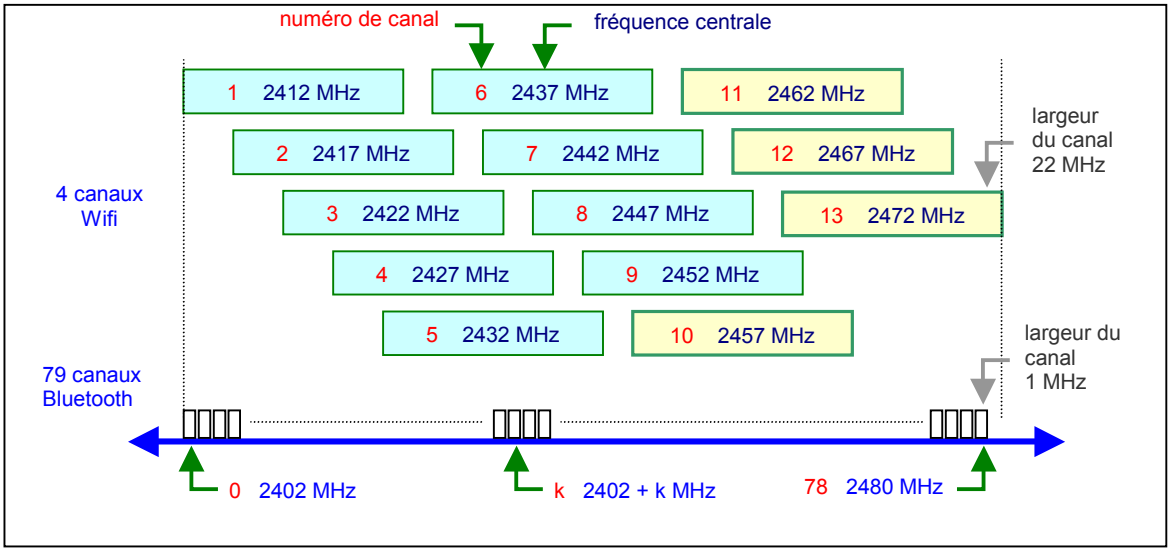
Figure 12. Bandes de fréquences utilisées dans les réseaux RF.



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 < 4mW (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

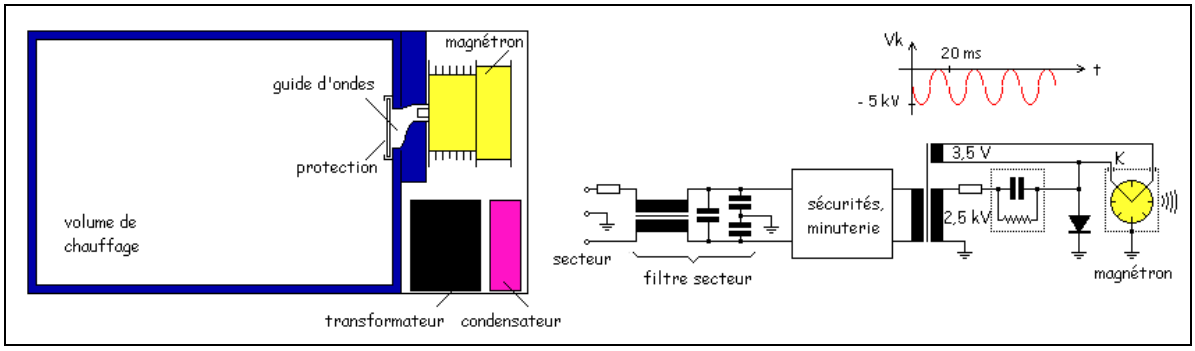


Figure 14. La constitution d'un four à micro ondes.

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.

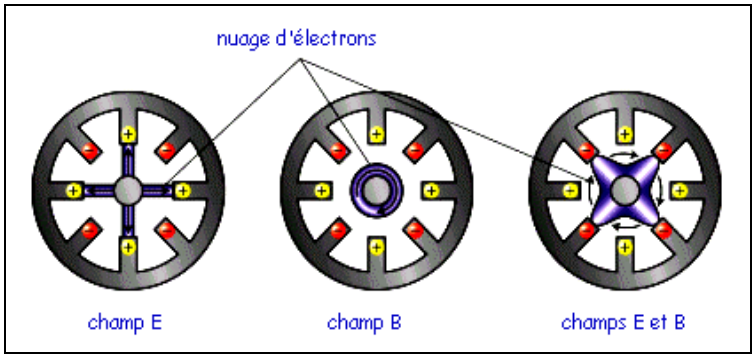


Figure 15. La trajectoire des électrons.

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.

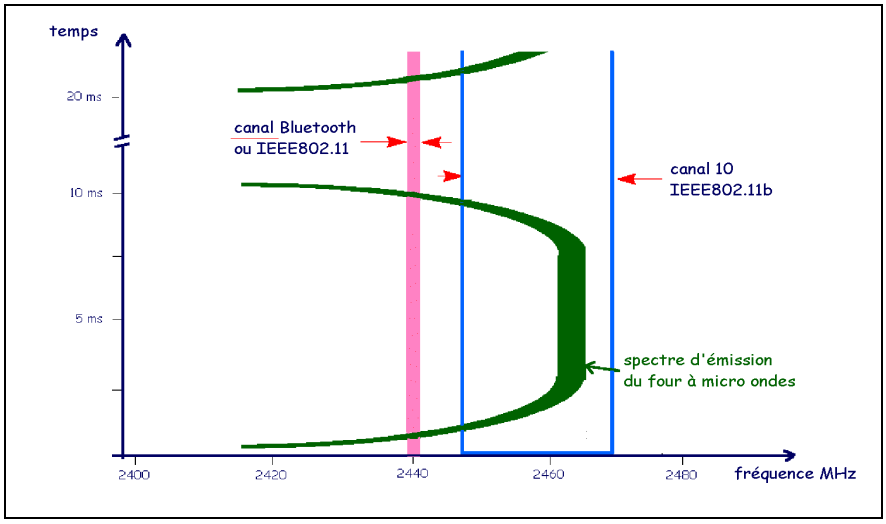


Figure 16. Spectre dynamique d'émission d'un four.

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.

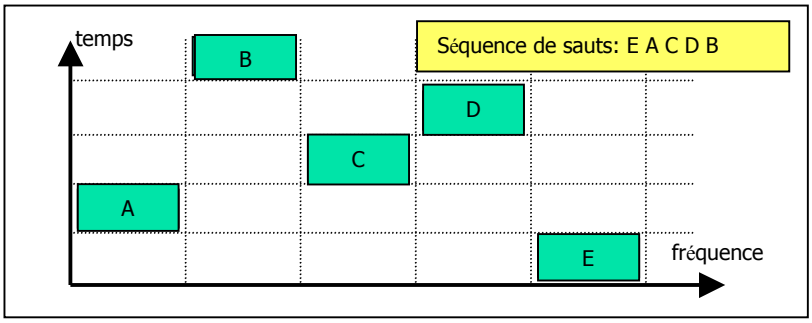


Figure 17. Principe du saut de fréquence.

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 µs.

⇒ 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.

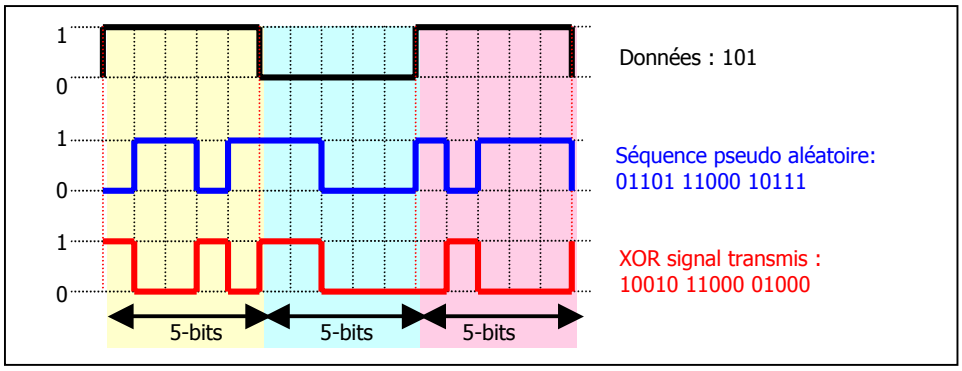


Figure 18. Le signal modulant dans un étalement par code 1bit/5 bits.

Dans cet exemple, le signal modulant a un débit 5 fois plus élevé, et l'encombrement spectrale 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.

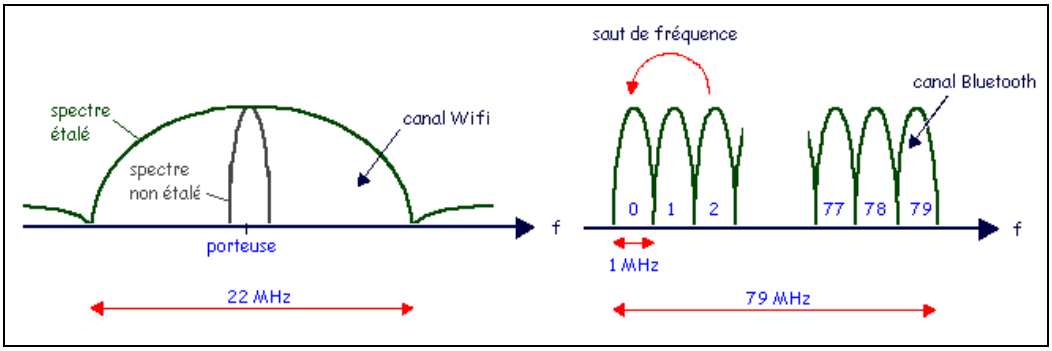


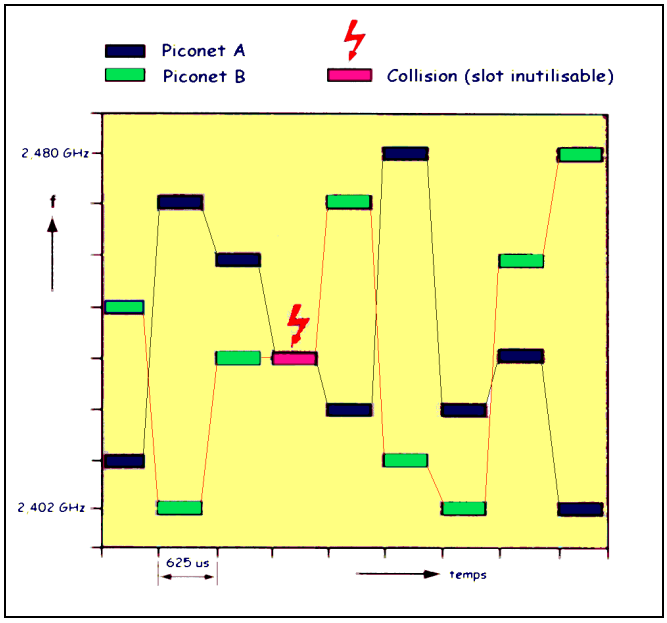
Figure 19. Allure des spectres après étalement.

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 µs**
- les sauts en fréquence (1/625µs = **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.



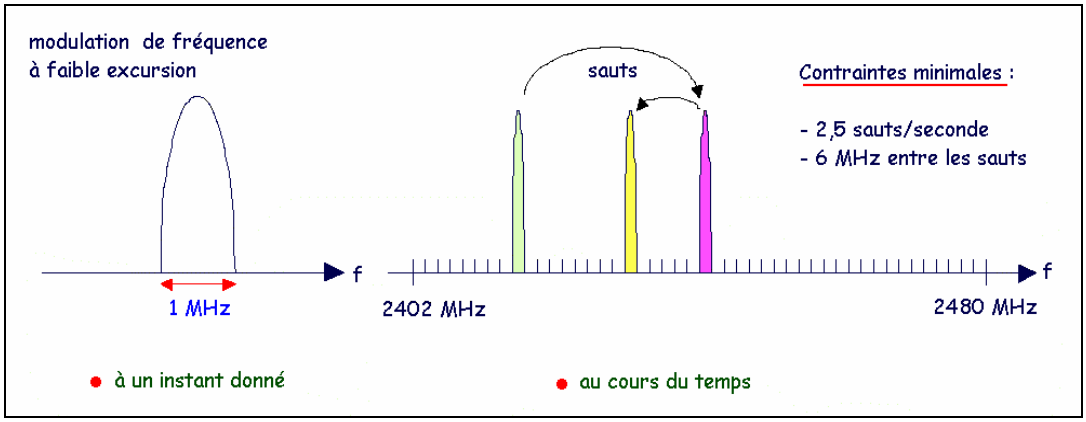
Chaque liaison utilisant la technique FHSS occupe donc, à cause des sauts de fréquence, la totalité de la bande de fréquence ISM.

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.

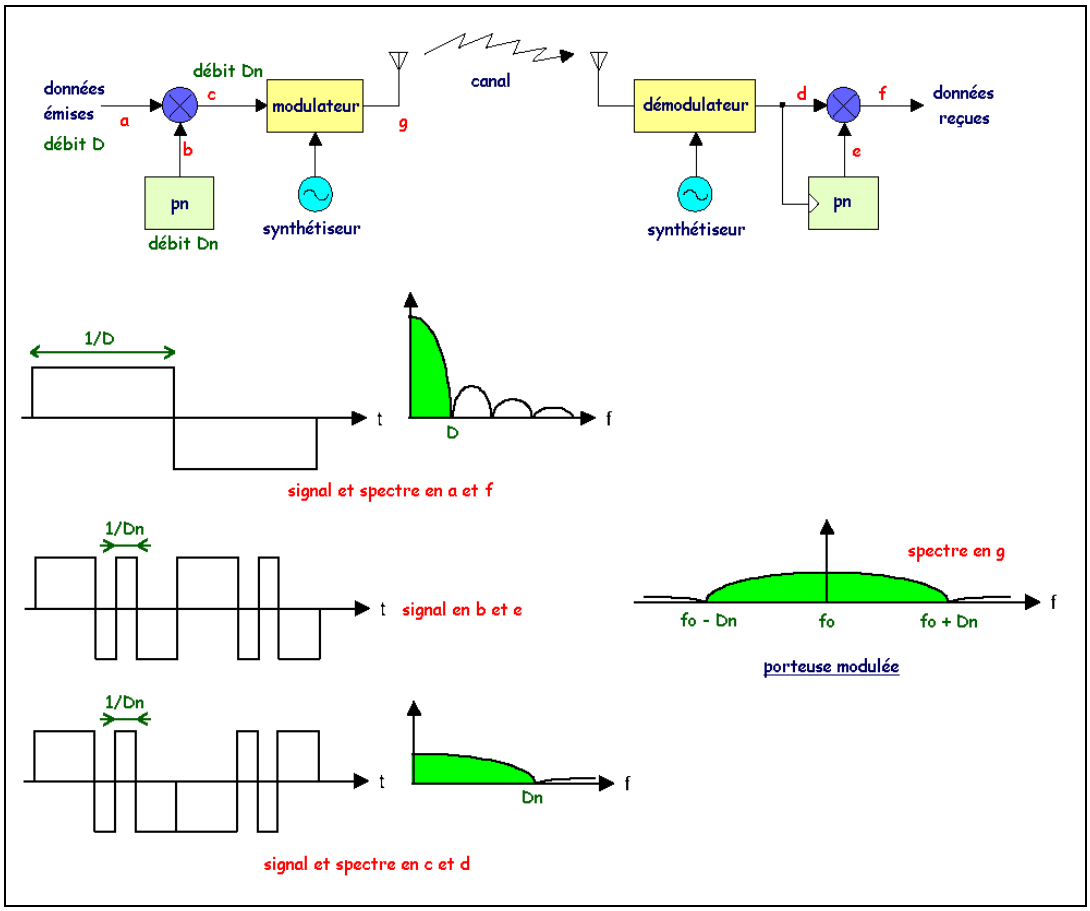
La norme Wifi ou IEEE802.11b a abandonné l'étalement par saut et offre un débit plus élevé en utilisant l'étalement par code, les équipements Wifi ne sont donc pas compatibles avec les équipement IEEE802.11 fonctionnant en FHSS.

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 Dn = 11 MHz
- le signal résultant, de débit Dn, 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.Dn = 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 (ou11) 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.

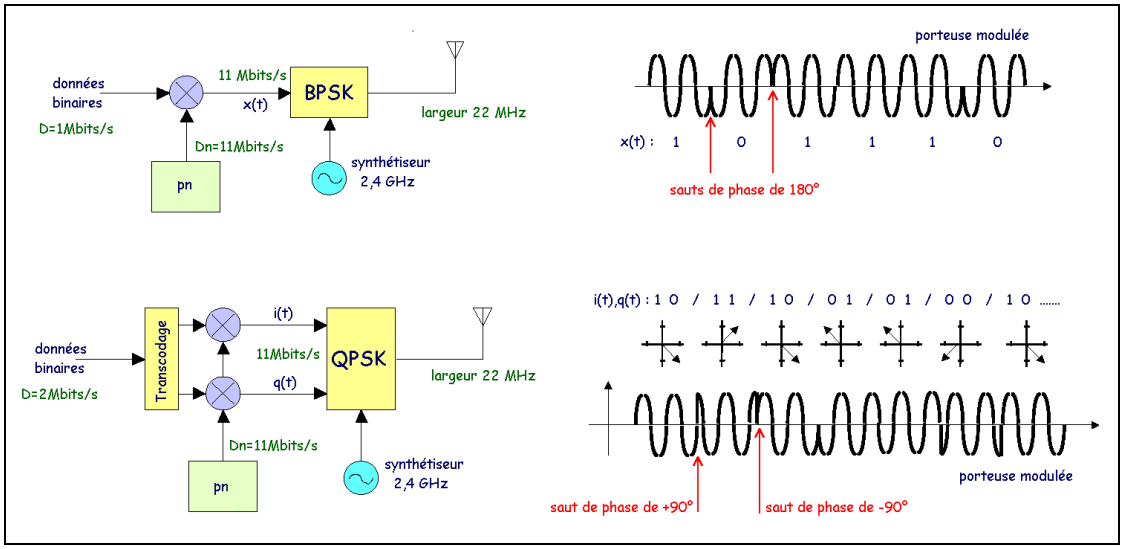
12- Les circuits de l'émission DSSS

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 :

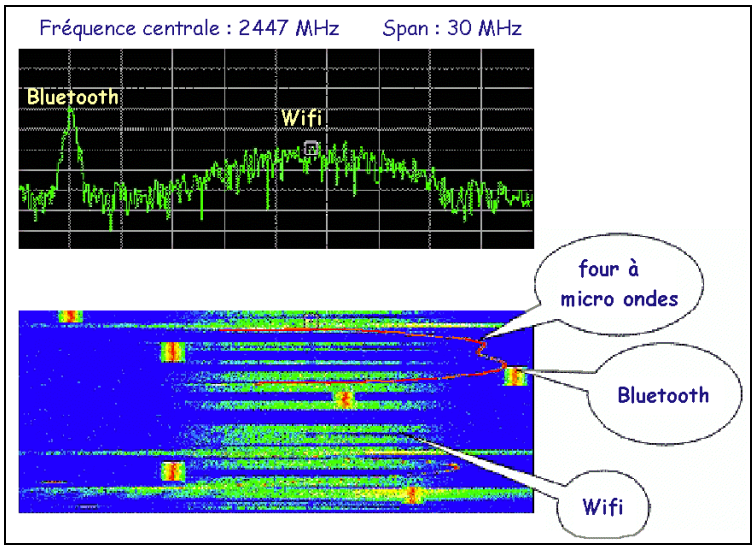
- les données sont séparées en dibits par le circuit de transcodage
- les deux signaux obtenus sont mélangés à la séquence pseudo aléatoire pour obtenir les 2 signaux modulants en phase i(t) et en quadrature q(t)
- i(t) et q(t) modulent la porteuse en lui imposant des sauts de phase de 0°, +90°, +180° ou +270° 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.



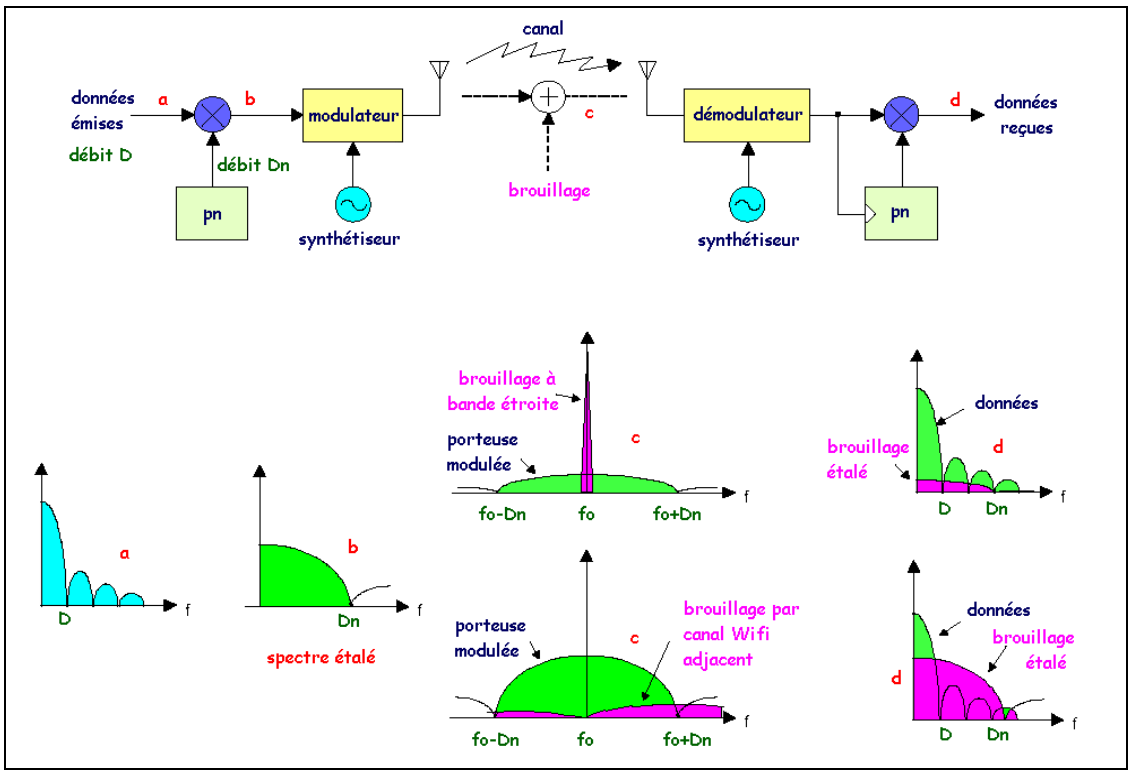
La transmission radio avec la technique d'étalement de spectre par code se fait à fréquence de porteuse fixe. Ce spectre est discontinu (phases d'émission et de réception), mais contrairement à Bluetooth reste fixe en fréquence.

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

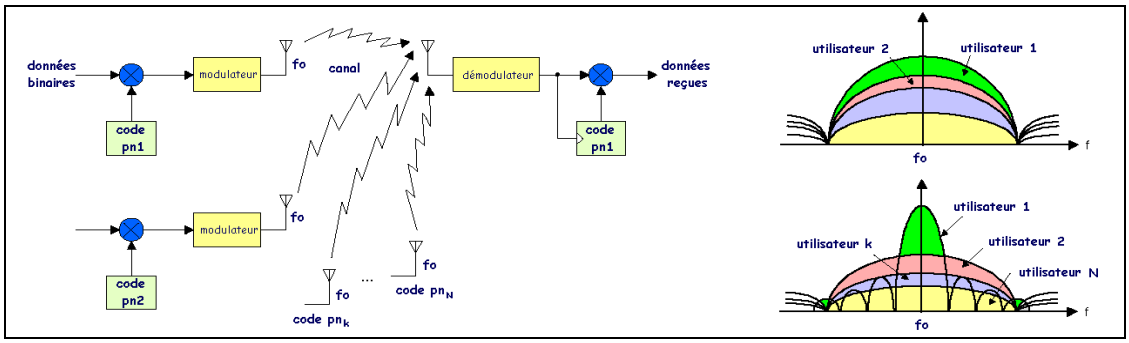
Figure 25. L'étalement de spectre en présence de bruit.



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 Divion 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.

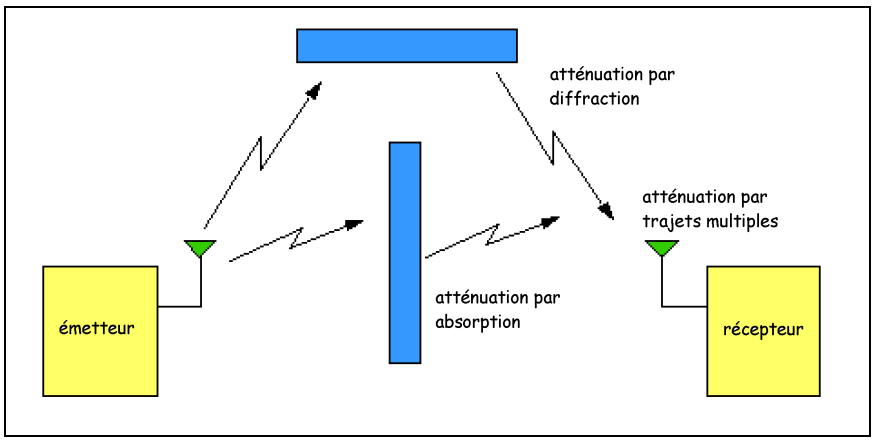
14- La portée d'une liaison à 2,4 GHz

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 : l**a 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.

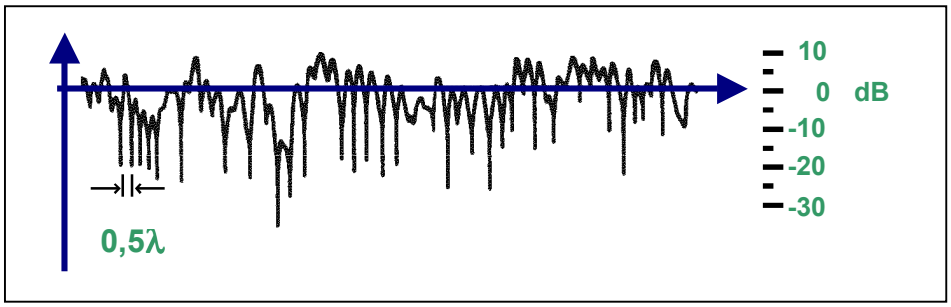
⇒ **de l'environnement : l**'onde électromagnétique doit traverser plusieurs obstacles (corps humain, cloisons …) avant d'arriver sur le récepteur. Ces obstacles absorberont une partie de l'énergie émise et la transformeront en chaleur, ce qui diminuera d'autant la portée du système.

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

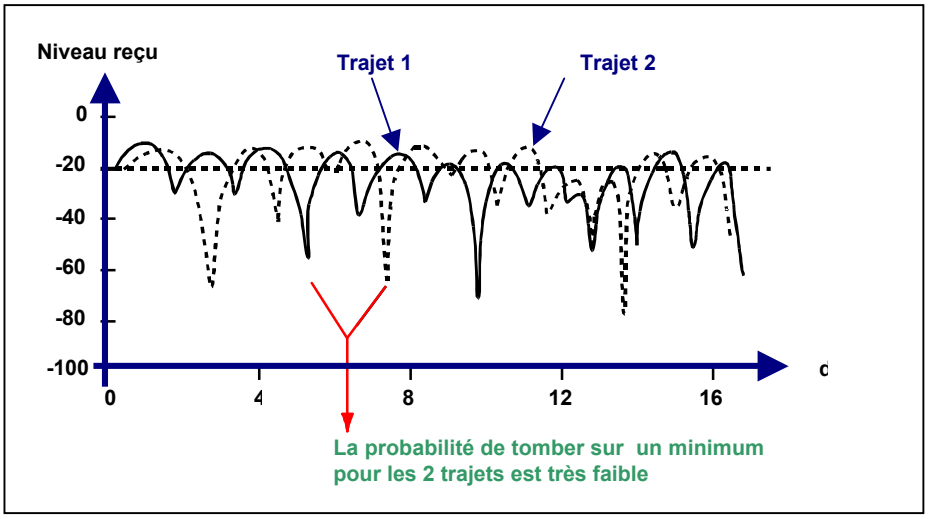
Lorsque la station s'éloigne du point d'accès, le débit s'ajuste pour maintenir un taux d'erreurs suffisamment bas.

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.

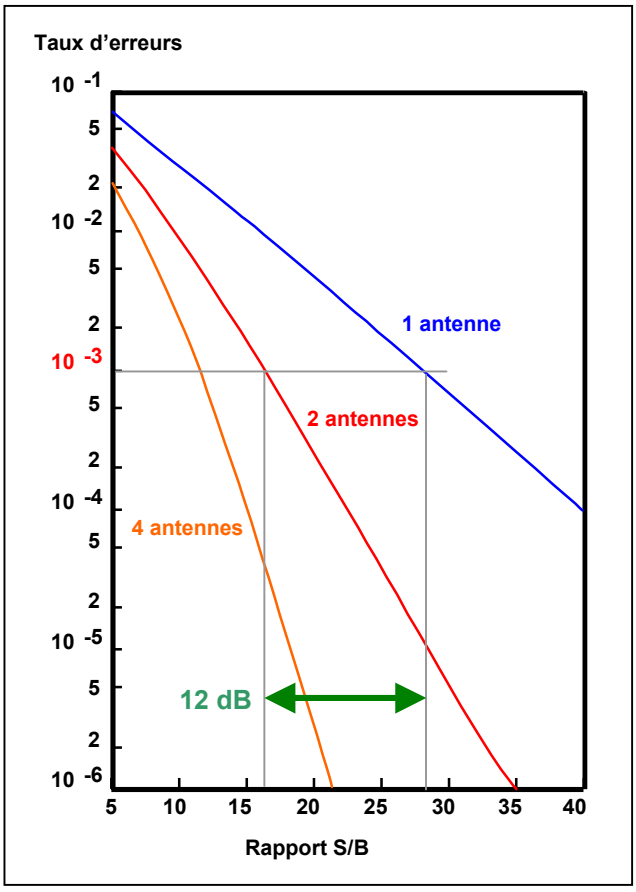
La probabilité de tomber exactement sur un minimum pour deux trajets différents est très faible, même si la différence de trajet parcouru est faible (λ = 12,5 cm à 2,4 GHz).

Figure 29. Influence du trajet sur le fading.



Si on utilise plusieurs antennes pour la réception au niveau de la sation 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 :

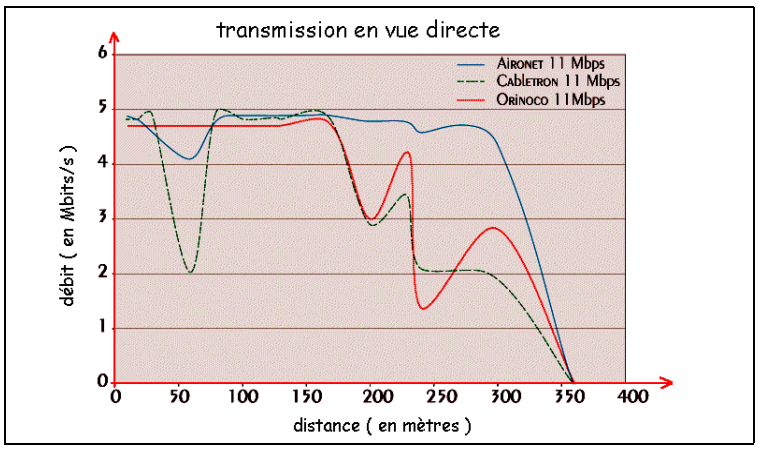
- de diminuer le taux d'erreurs
- d'augmenter la portée de la base

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 :

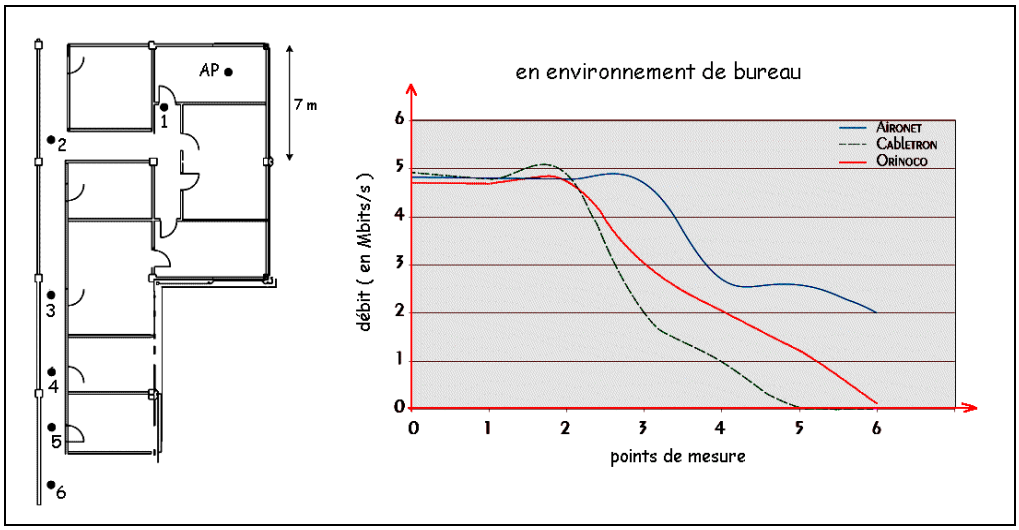
⇒ la vitesse de transmission réelle dans les conditions optimales est toujours inférieure à 5 Mbits/s, loin en-dessous des 11 Mbits/s théoriques

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.

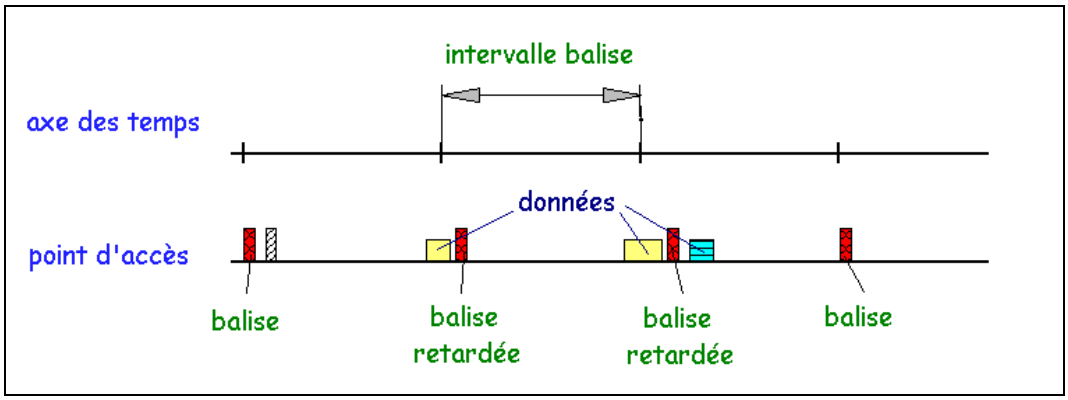


Figure 33. L'émission balise du point d'accès.

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 fonctionnalité 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

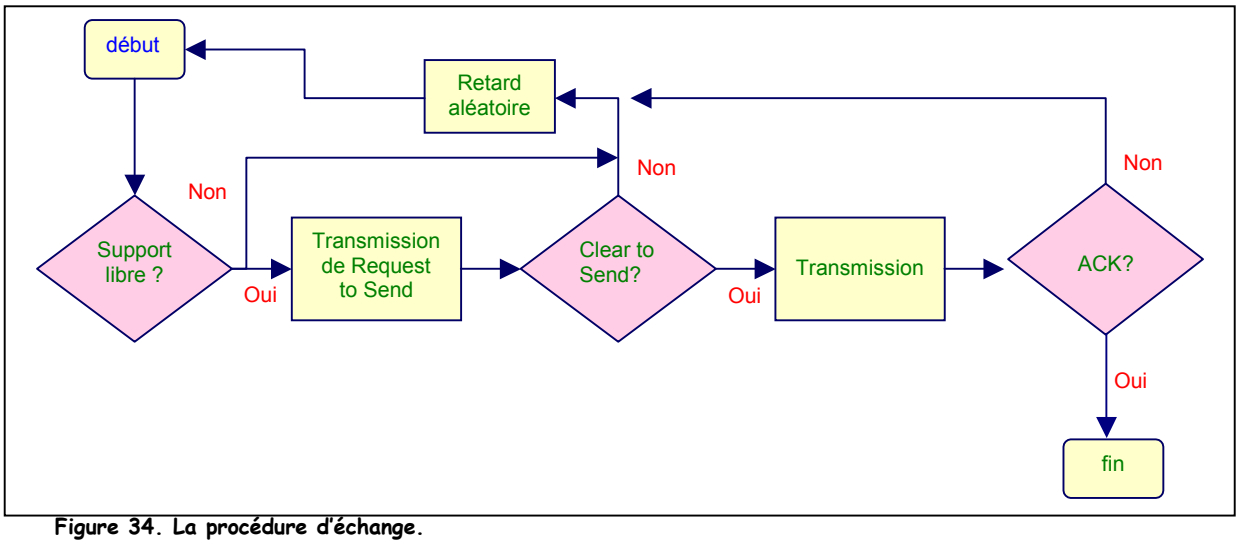
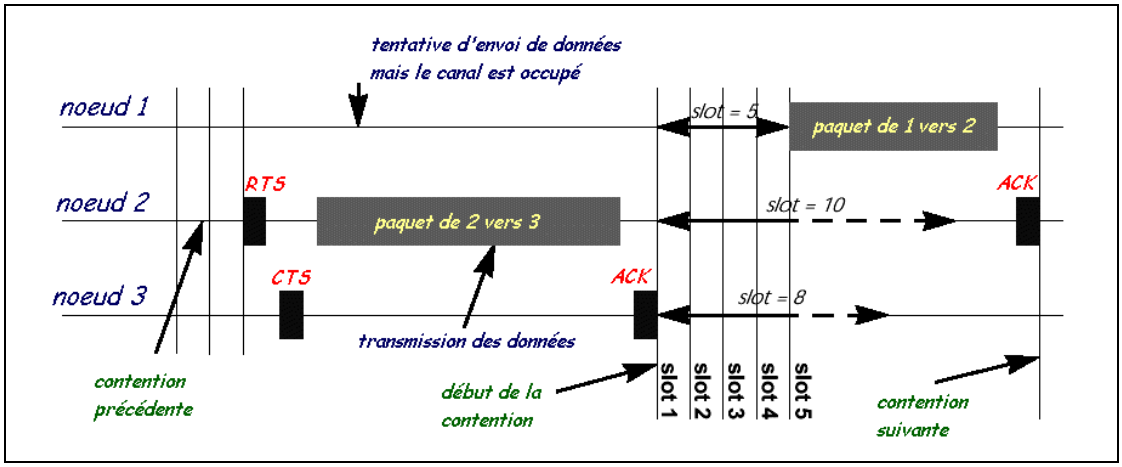


Figure 34. La procédure d'échange.

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 µs 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 (Point Coordination IFS) de 78 µs 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 µs 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.

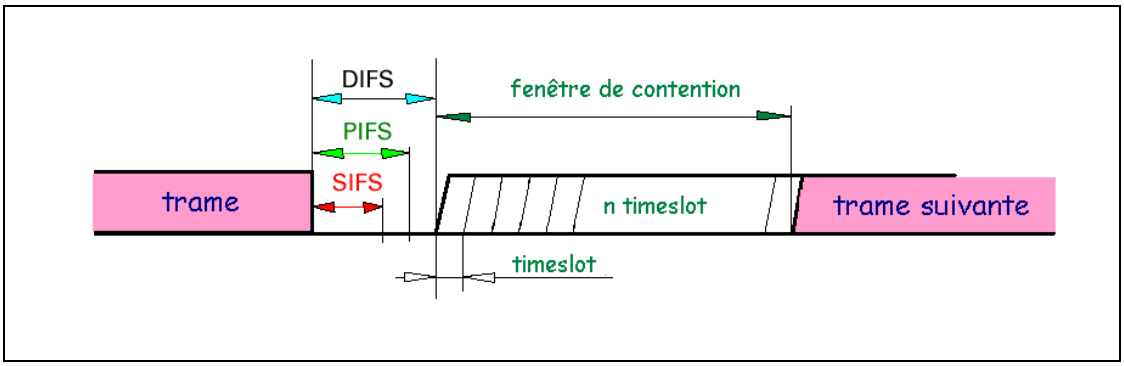


Figure 36. Le retard aléatoire du back off.

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.

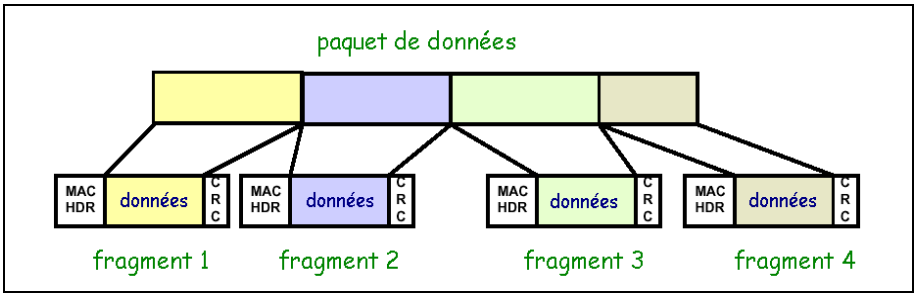
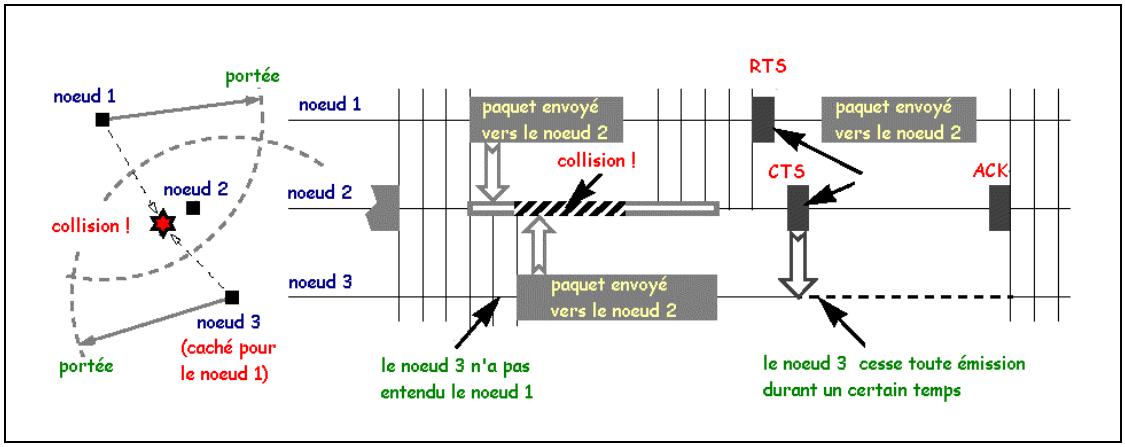


Figure 37. La fragmentation des paquets longs.

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.



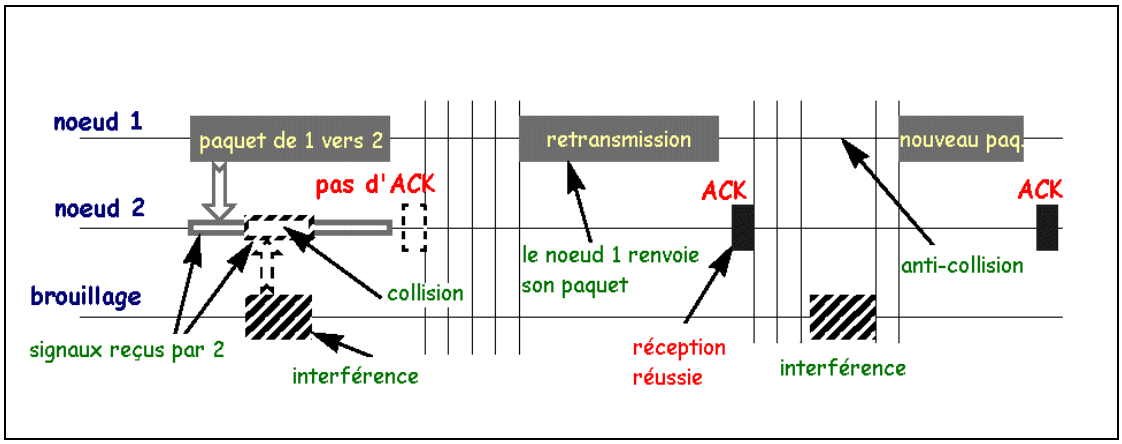
Dans l'exemple ci-dessus, la station n° 3 est une station cachée pour la n° 1. Pour éviter les collisions, la technique utilisée est la suivante :

- 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 suivant :

- 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

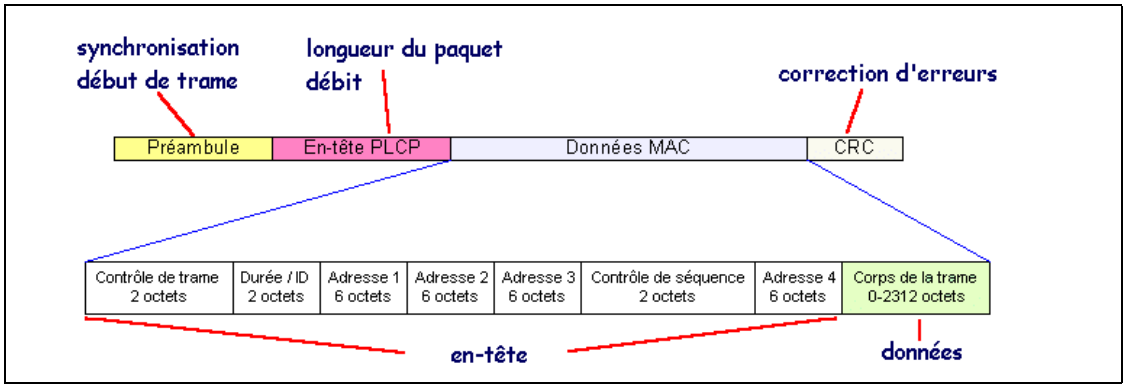


Figure 40. Structure générale d'une trame Wifi.

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.

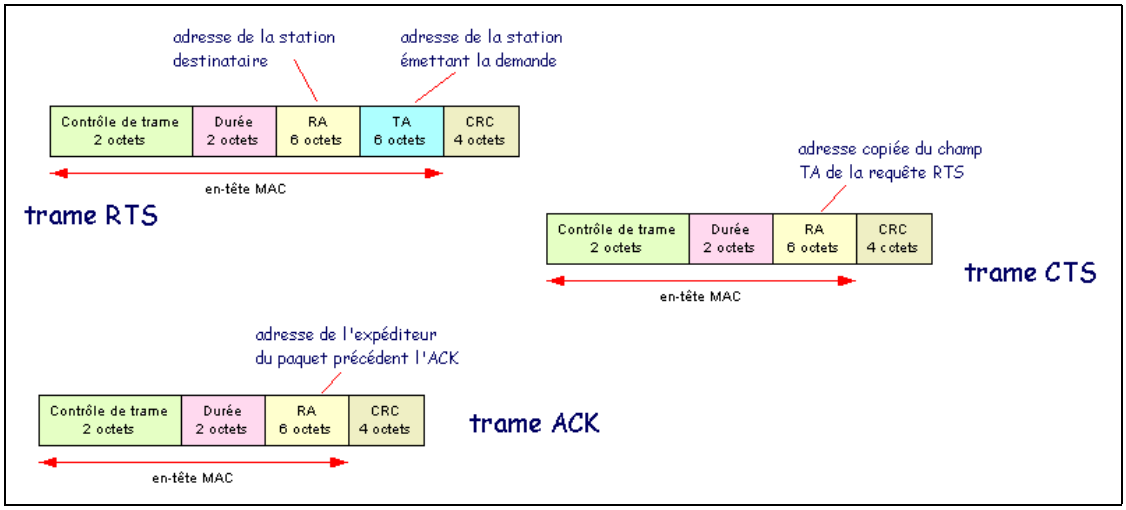


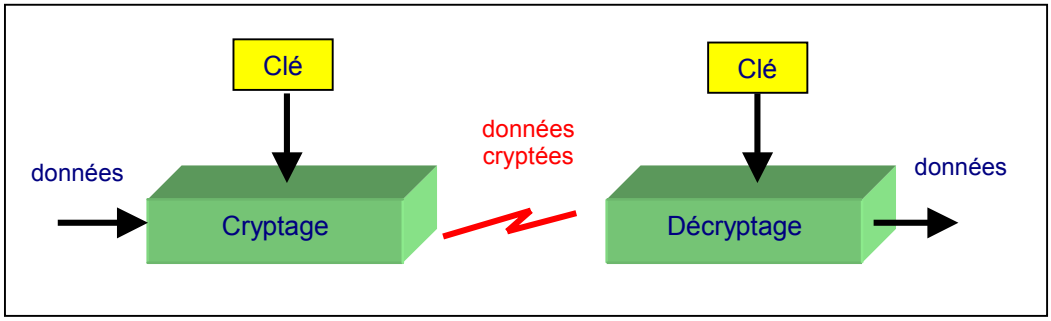
Figure 41. Les trames courtes.

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

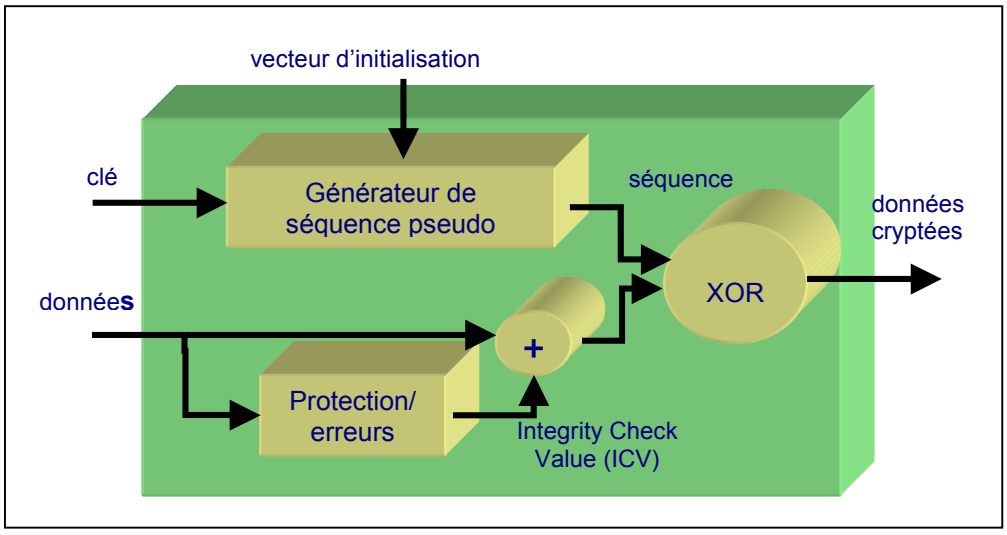
Figure 42. Le principe du cryptage.



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 en-têtes 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.

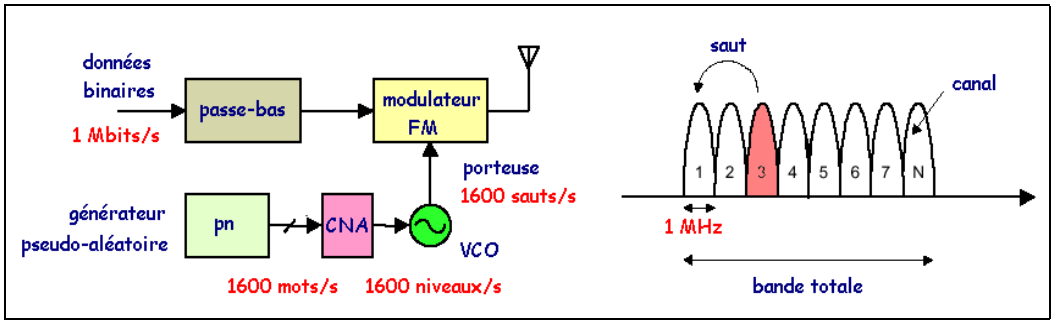
Notons que l'utilisation de l'algorithme WEP pour la liaison radio n'interdit pas l'utilisation en amont d'autres dispositifs de cryptage de donnée plus efficaces.

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).

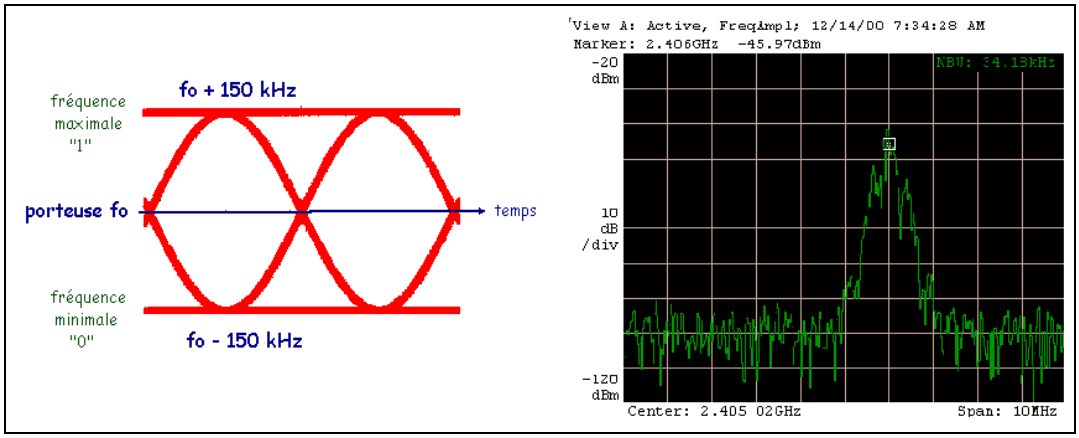
Cette porteuse change régulièrement de valeur, en fonction d'une séquence pseudo aléatoire pn produite par un générateur.

Figure 44. La modulation FHSS.



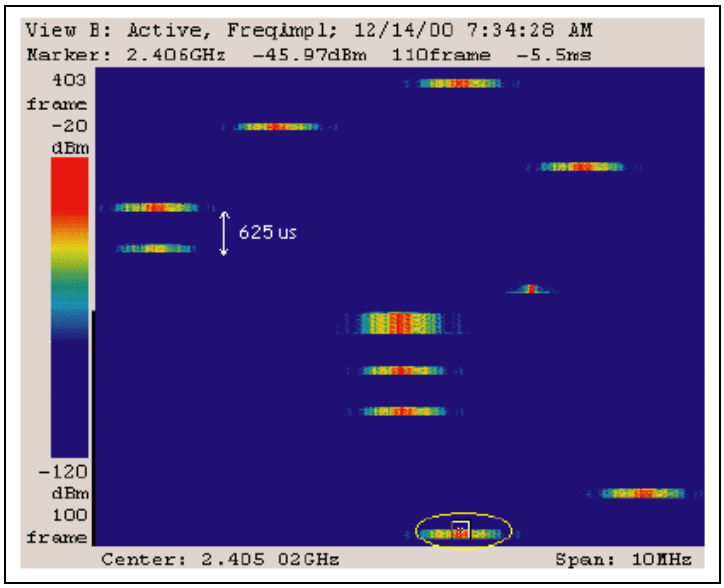
Pour une fréquence de porteuse donnée, l'excursion en fréquence est de ± 150 kHz environ, et le spectre est caractérisé par une largeur environ égale au débit binaire, soit 1 MHz.

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

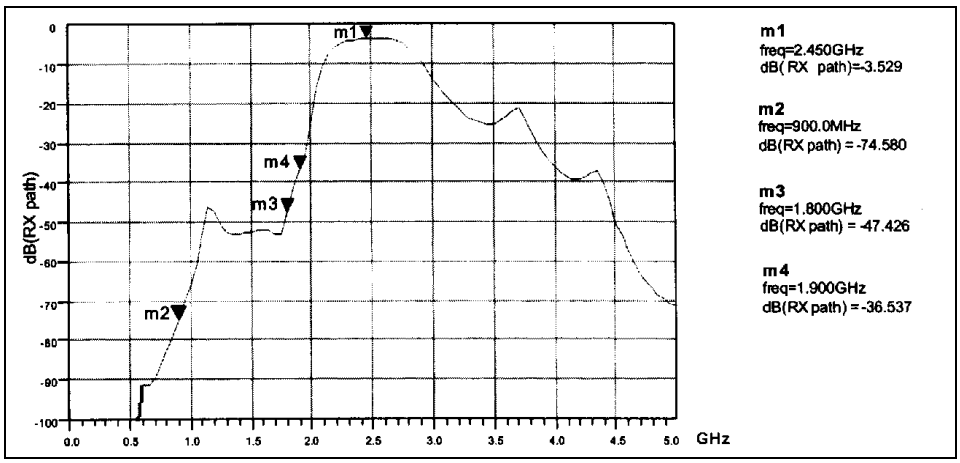
La présence côte à côte d'un téléphone portable GSM/DCS de puissance maximale 2W et d'un module Bluetooth ou Wifi de puissance plus faible peut être à l'origine d'interférences gênantes et nécessite une conception soignée.

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 considérés, 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

- 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 . . . . $0^{o}C$ to $70^{o}C$ (Note 2)
- Storage Temperature Range . . . . . .$-55^{o}C$ to $125^{o}C$
- Mechanical . . . . Type II PC Card, with Antenna Extension
- Antenna Interface . . . . . SMA, 50Ω

Receive Specifications

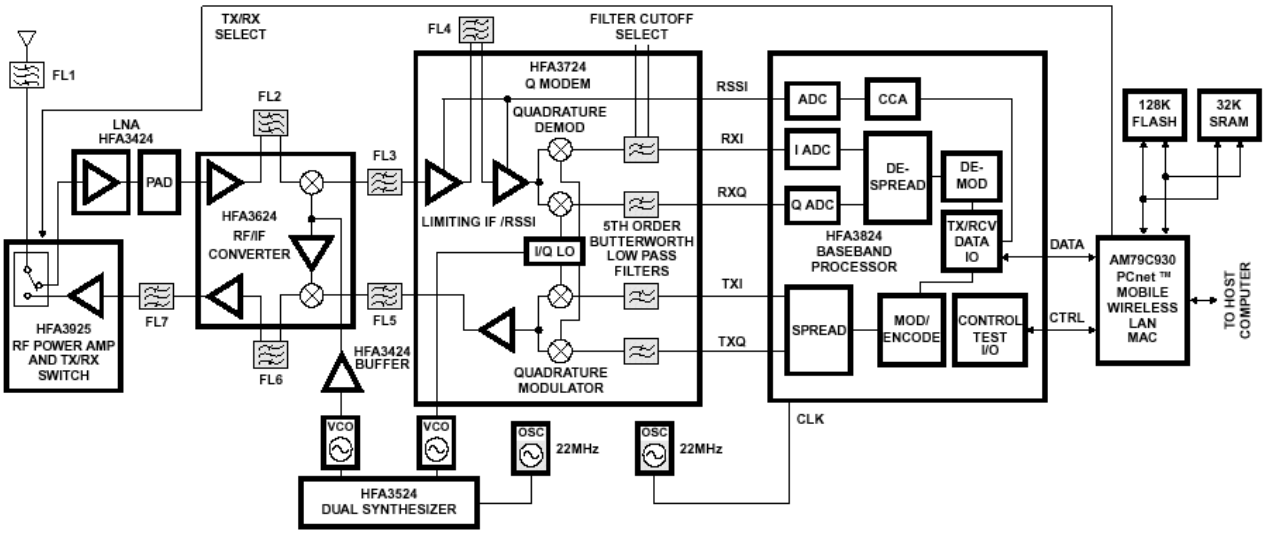
- Sensitivity . . . . .-93dBm (Typ), 1Mbps, 8E-2 FER (Note 3)
  . . . . . .-90dBm (Typ), 2Mbps, 8E-2 FER (Note 3)
- Input Third Order Intercept Point . . . . . .-17dBm (Typ)
- Image Rejection . . . . . 65dB (Typ)
- IF Rejection . . . . . 80dB (Typ)
- Adjacent Channel Rejection . . . . . 63dB (Typ)
  at 25MHz Offset
- Supply Current . . . . . .287mA (Typ)
  2Mbps, 100% Duty Cycle

Transmit Specifications

- Output Power . . . . . +18dBm (Typ)
- Transmit Spectral Mask . . . . . .-32dBc (Typ)
  at First Side-Lobe
- Supply Current . . . . . .488mA (Typ)
  2Mbps, 100% Duty Cycle

NOTES:

1. Using M/A-COM AND-C-107 omnidirectional antenna.
2. AM79C930 limited to $0^{o}C$ to $70^{o}C$.
3. FER = Frame Error Rate or Packet Error Rate.
4. 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