Bluetooth et WiFi

De la théorie à la pratique : Calculs et expérimentations simples

Module Réseaux et Mobilité
M1 IUP STRI

Enseignant :Thierry GAYRAUD

A partir du mémoire d'ingénieur CNAM de Michel PLANQUES

Table des matières

1 Etat de l'art des technologies étudiées

1.1 Bluetooth (norme 802.15)

Bluetooth définit, au travers de sa norme 802.15, les réseaux d'un rayon d'action de quelques mètres jusqu'à un maximum d'une centaine de mètres, avec pour objectif de réaliser les connexions entre diverses unités devant communiquer. Cela peut concerner les connexions d'un PC et de ses périphériques (clavier, souris, imprimante, modem …), d'un PC avec un PDA, d'un téléphone avec un kit mains libres ou toute autre application nécessitant un échange par un lien de communication à faible distance.

1.1.1 Technologie Bluetooth

Pour communiquer, Bluetooth emploie des sous canaux de 1 MHz sur les fréquences de 2400 MHz-2483.5MHz en utilisant la technique FHSS sur 79 canaux, c'est à dire qu'une communication ne se déroule pas sur un canal unique mais sur toute la bande de fréquence. L'algorithme de calcul de sauts de fréquence est défini à partir de l'adresse du maître du réseau, ce qui permet de synchroniser maître et esclaves d'un même sous réseau sur une séquence identique de sauts et en conséquence de pouvoir dialoguer immédiatement. Les sauts de fréquence sont effectués au rythme de 1600 par seconde.

1.1.2 Architecture des Réseaux Bluetooth

Un réseau Bluetooth est organisé sur un schéma de type maître/esclave, avec au maximum
7 esclaves dans ce qui est appelé « piconet ». Le terminal élu maître du réseau gère toutes les communications et les droits de parole ; par exemple un esclave qui aura des données à envoyer devra attendre que le maître l'invite à parler. Comme dans tout réseau maître/esclave, les communications ne peuvent intervenir qu'entre un maître et un esclave : Une communication d'esclave à esclave est impossible au niveau du protocole Bluetooth.

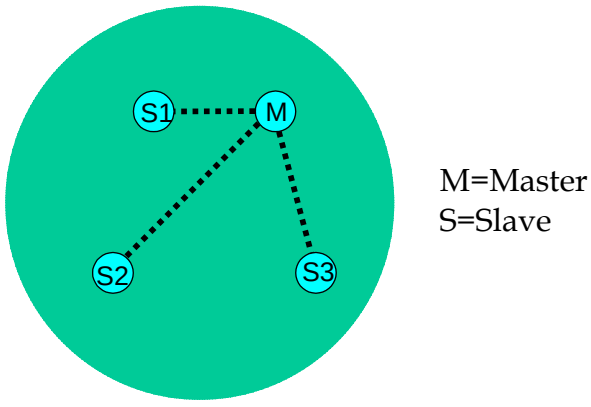
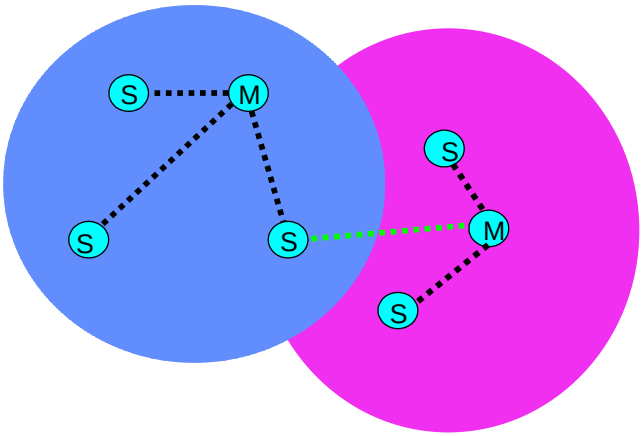


Figure 1 : Piconet Bluetooth

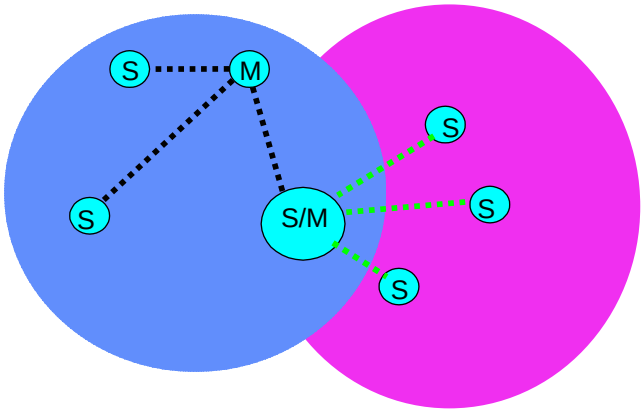
Il est possible d'étendre un réseau Bluetooth par l'interconnexion de plusieurs piconets afin de former ce que l'on appelle un scatternet. Dans ce cas, l'unité partagée entre deux piconets, peut être soit esclave des deux réseaux, soit esclave d'un réseau et maître d'un autre ; il est par contre totalement impossible d'être le maître de plusieurs piconets.

- Partage d'un esclave entre deux piconets



Dans cette topologie, nous avons un esclave qui est associé à deux piconets

- Le terminal esclave dans un piconet et maître dans l'autre



Ici, le réseau est chainé au travers d'un terminal esclave dans un piconet et maitre dans l'autre.

Figure 2 : Scattenets Bluetooth

Dans tous les cas une unité commune à plusieurs piconets doit partager son temps en consacrant une partie de ses intervalles à chaque sous-réseau.

Même si les sauts de fréquence de chacun des sous-réseaux sont différents (liés à l'adresse du maître de chaque piconet), il y a dans ce type d'architecture des collisions qui entraînent soit des retransmissions, soit des pertes de données suivant le type de paquets transmis (voix ou données).

1.1.3 Communications Bluetooth

Le canal de communication Bluetooth a une bande passante théorique maximale de 1 Mb/s, mais une liaison Bluetooth ne pourra jamais dépasser 433.9 kbits/s pour une liaison symétrique bidirectionnelle et 723.2/57.6 kbits/s pour une liaison asymétrique.
Bluetooth distingue 2 types de communications :

- asynchrones pour lesquelles une liaison de type ACL indépendante de la connexion permet un dialogue avec un débit maximal de 723.2 kbit/s ;
- synchrones pour lesquelles une liaison de type SCO orientée connexion est établie avec un débit maximal de 64 kbit/s.

Il existe au plus une seule liaison ACL entre deux périphériques ou 3 liaisons SCO. On peut également avoir une liaison ACL et une liaison SCO simultanément.

Comme nous l'avons vu précédemment, les communications Bluetooth sont acheminées sur le support physique au travers de slots temporels de 625 µsec (1600 sauts par seconde). La transmission sur la bande de base est de type TDD (Time Division Duplex), ce qui signifie que les slots temporels sont réservés séquentiellement au maître puis aux esclaves. Le maître transmet dans les slots temporels pairs et les esclaves dans les slots impairs.
Dans un échange, c'est le maître qui attribue et décide quel esclave peut utiliser le slot temporel suivant.
Le maître effectue un polling sur ses esclaves à intervalles réguliers pour leur permettre d'envoyer des données. L'intervalle de polling est négocié entre le maître et l'esclave.

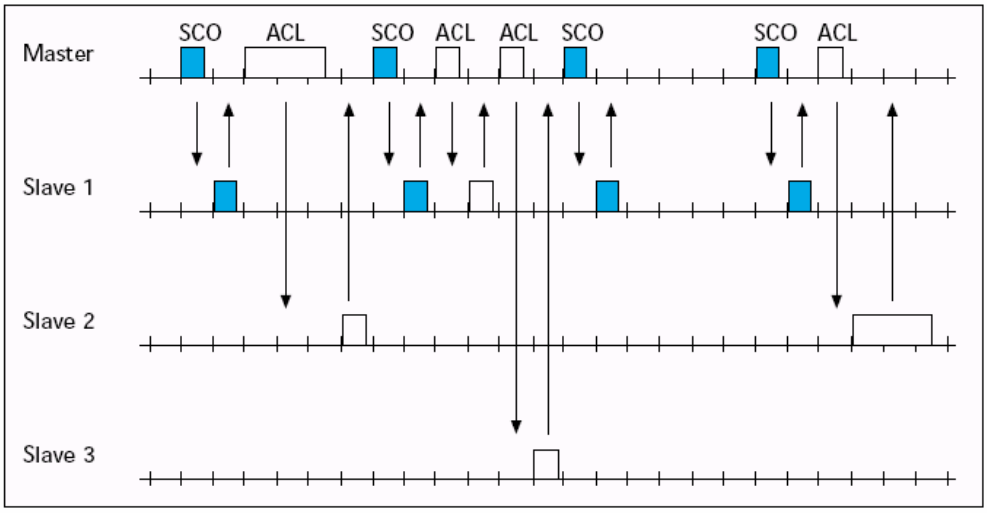


Figure 3 : Distribution des slots temporels

On peut remarquer que les slots temporels sont distribués régulièrement et aux mêmes instants pour les liaisons SCO (récurrence de 6 slots, soit 3.75 msec). Les liaisons ACL occupent les slots laissés libres par les liaisons synchrones. Nous avons également dans cet exemple des communications qui s'étalent sur plusieurs slots temporels sur des liens asymétriques. En effet Bluetooth supporte plusieurs types de paquets, dont certains occupent un nombre de slots temporels supérieur à 1.

1.1.4 Types de paquets

Bluetooth définit trois types de paquets principaux : les paquets de contrôle, les paquets de données synchrones utilisant une liaison SCO et les paquets de données asynchrones utilisant une liaison ACL.

Les liaisons de données synchrones ou asynchrones permettent de transporter plusieurs types de paquets :

- Les paquets DH1, DH3 et DH5 qui utilisent les liaisons ACL occupent respectivement 1, 3 ou 5 slots temporels sans correction d'erreur.
- Les paquets DM1, DM3 et DM5 qui utilisent les liaisons ACL occupent respectivement 1, 3 ou 5 slots temporels avec correction d'erreur FEC (Forward Error Correction).
- Les paquets HV1, HV2 et HV3 qui utilisent les liaisons SCO avec une correction d'erreur FEC respectivement de 1/3, 2/3 ou sans correction d'erreur (cas du HV3).
- Les paquets DV qui utilisent les liaisons SCO comportent un champ de données et un champ destiné à la voix.

Les paquets multi slots permettent d'occuper la bande passante de manière plus efficace par une diminution de la charge protocolaire. Les paquets avec correction d'erreur fiabilisent la transmission des données.

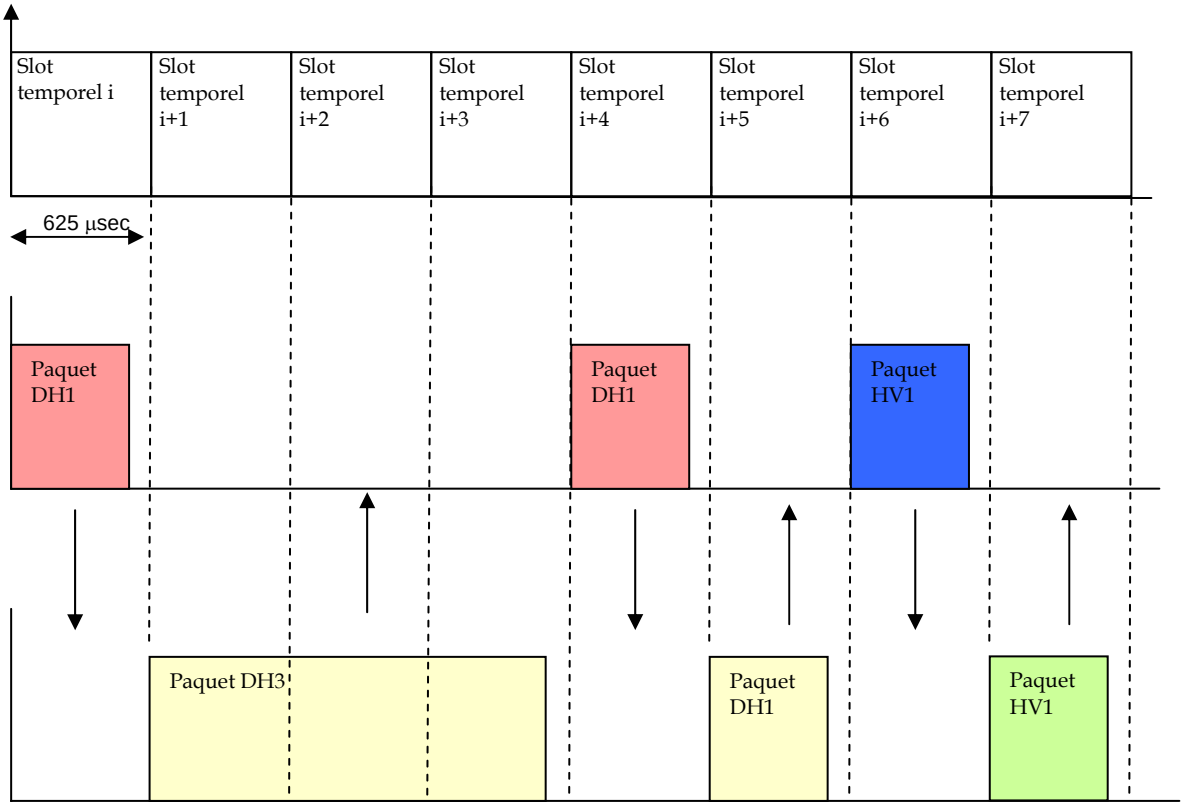


Figure 4 : Paquet multi slots

1.1.5 Etats des terminaux Bluetooth

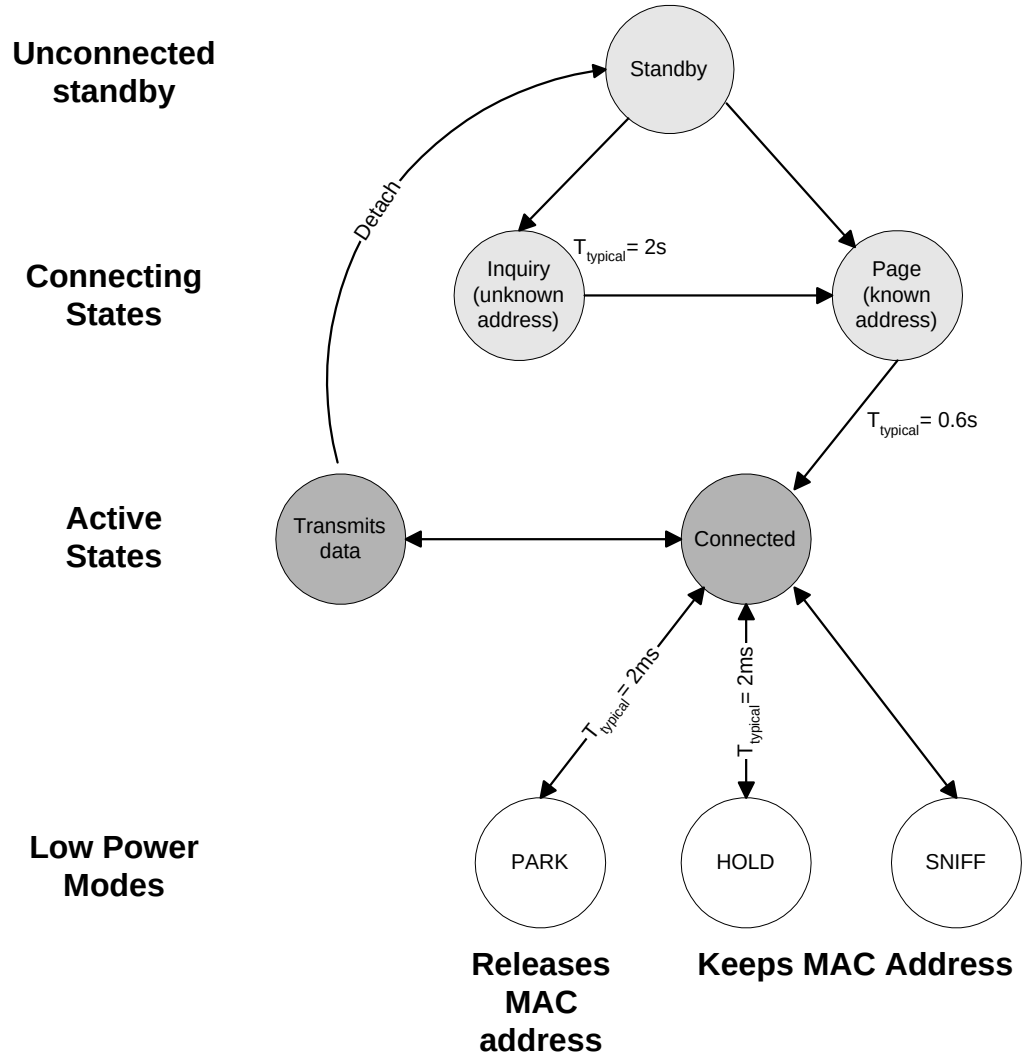


Figure 5 : Etats des terminaux Bluetooth

Mode standby : le terminal est inactif,
Mode Inquiry : le terminal cherche d'autres terminaux,
Mode Page : le terminal cherche à se connecter avec un autre terminal,
Mode Connecté : dans le mode, le terminal peut transmettre ou se positionner dans des modes d'économie d'énergie (Hold, Snif ou Park).

Les deux principaux états des terminaux bluetooth sont Standby et Connected. Le mode Standby est le mode basse consommation par défaut et pour mettre en œuvre des communications avec Bluetooth il est nécessaire de passer en mode Connected.

Le principe du saut de fréquence ne facilite pas la mise en liaison de deux entités car un esclave et un maître qui veulent établir une liaison doivent le faire alors qu'a priori leurs horloges sont asynchrones et qu'ils n'ont normalement aucune

information sur la fréquence d'émission utilisée par leur partenaire de communication à venir.

Le mécanisme prévu par Bluetooth qui permet de passer de l'état de *Standby* à *Connected* utilise les procédures *Inquiry* et *Page*.

La procédure *Inquiry* consiste à découvrir les autres entités Bluetooth qui sont présentes dans un environnement, cette procédure est optionnelle, tandis que la procédure de *Page* établi la connexion.
Sachant que la séquence de saut est liée à l'adresse du maître, il est nécessaire de passer par une procédure *d'Inquiry* lorsqu'on ne connaît pas a priori le partenaire de communication (son adresse MAC Bluetooth).

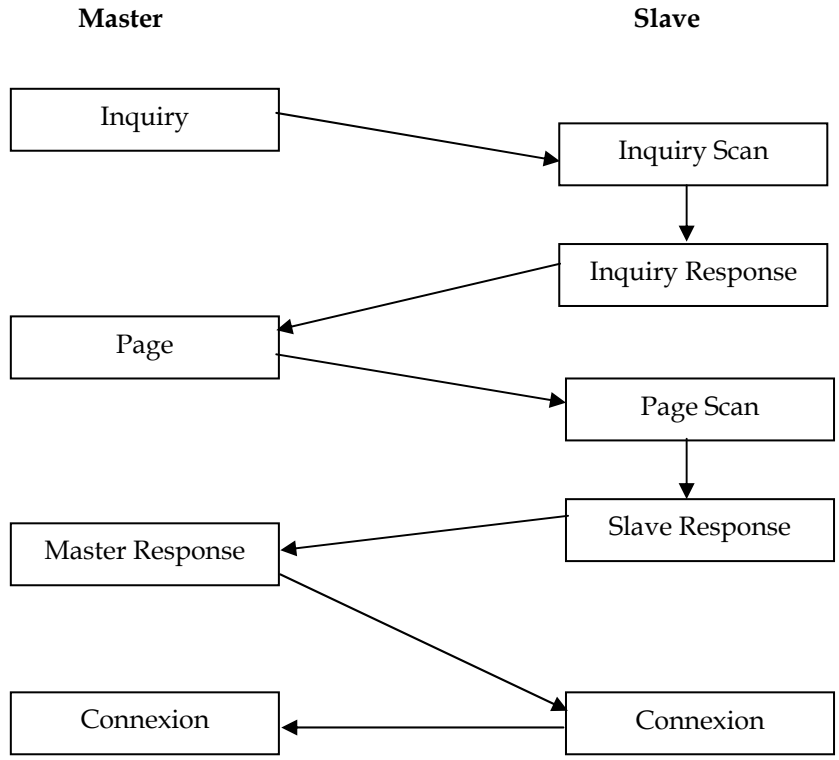


Figure 6 : Procédure de connexion Bluetooth entre un Maître et un esclave

1.1.5.1 Procédure d'Inquiry

La procédure *d'Inquiry* est utilisée quand l'adresse de destination est inconnue ou quand un nœud veut découvrir des partenaires de communication éventuels dans son environnement.

Sous état d'Inquiry
Une entité qui cherche à collecter les adresses et les horloges d'autres terminaux Bluetooth entre dans le sous état *d'Inquiry*. Cela signifie qu'il émet périodiquement

un message IAC (Inquiry Acces Code) en effectuant des sauts de fréquences. Ne répondront à cette requête, que les terminaux qui autorisent leur découverte

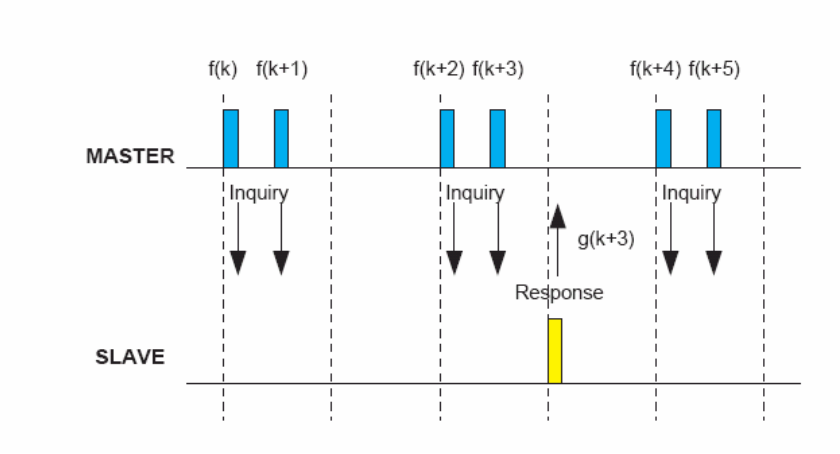


Figure 7 : Echange des paquets en cas d'états Inquiry/Inquiry scan

Comme le message *d'Inquiry* est très court (68 bits), les sauts de fréquence peuvent être effectués deux fois plus vite (3200 sauts de fréquence par seconde au lieu de 1600). En conséquence, le message peut être envoyé sur deux fréquences différentes dans la durée d'un slot. Sur le slot suivant, il écoute les réponses éventuelles sur deux fréquences (toujours 2 sauts sur un slot) en utilisant la séquence de sauts pour la réponse à *l'Inquiry*.
L'unité continue à transmettre des messages *d'Inquiry* dans les slots pairs, et écoute les réponses entre deux transmissions jusqu'à ce qu'il décide qu'il a eu assez de réponses ou atteint son timeout.
Les séquences de saut *d'Inquiry* et de réponse *d'Inquiry* sont calculées à partir de l'IAC (Inquiry Acces Code) et l'horloge de l'unité effectuant la découverte.

Sous état *d'Inquiry Scan*
Une unité qui permet sa découverte doit régulièrement entrer en sous état *d'Inquiry scan* : pendant 10 ms toutes les 1.28 s. Dans cet état il écoute le support sur une seule fréquence.
Si durant cette période, il reçoit un message *d'Inquiry* alors il rentre dans l'état de réponse *d'Inquiry*.

Sous état Réponse *d'Inquiry*
Lorsqu'un message *d'Inquiry* est reçu, un paquet FHS (Frequency Hopping Synchronization) de réponse est transmis en retour. Ce paquet contient les informations adresse et horloge de l'unité afin de permettre la synchronisation des fréquences. A partir de cet instant l'unité bascule dans l'état de *Page Scan*.

Plusieurs noeuds pouvant répondre au même instant, un protocole de résolution de contention est mis en oeuvre.

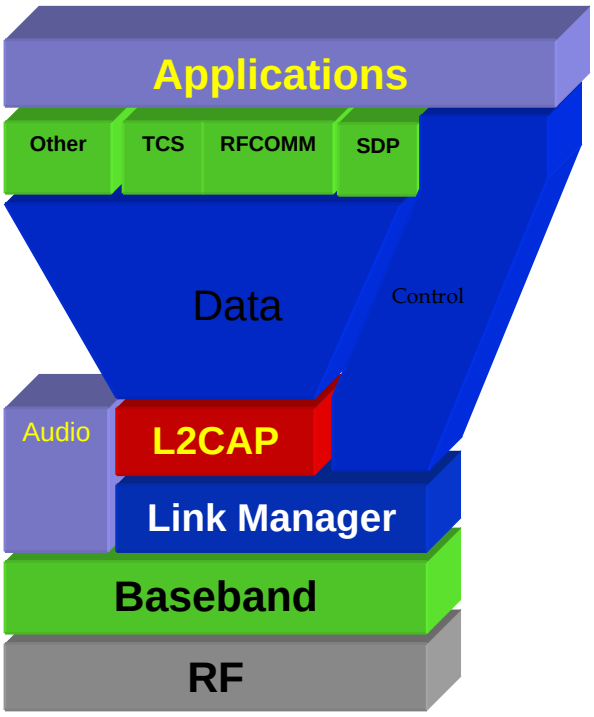
1.1.5.2 Procédure de Pagination

Dans la procédure de pagination, une connexion peut être établie si l'adresse destination est connue. L'état de pagination est utilisé par le maître pour activer un esclave, ce dernier devant périodiquement se réveiller pour passer en état de *Page Scan*. Dans cet état, l'esclave écoute le support sur une seule fréquence dans le but de recevoir son DAC (Device Acces Code). Si l'unité reçoit un message contenant son DAC, alors elle entre en état de *Slave Response* et répond dès le slot temporel suivant. Lorsque le maître reçoit la réponse, il entre en état de *Master Response* et envoie à l'esclave un paquet comprenant la BD_ADDR (Bluetooth Device Address) du maître et son horloge : ces informations étant nécessaire à l'esclave pour se synchroniser sur la séquence de saut du maître et donc établir la connexion.

1.1.6 La pile de protocoles et l'encapsulation des données

La pile de protocoles Bluetooth se décompose en 3 parties :

- les protocoles de transport Bluetooth,
- la couche d'adaptation (Middleware),
- les applications.



1.1.6.1 *Les protocoles de transport*

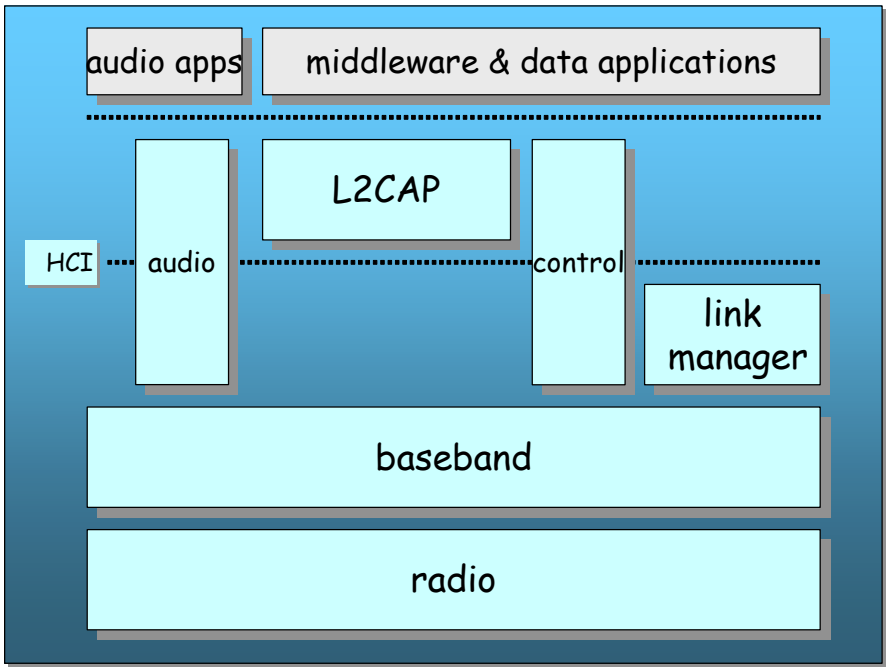
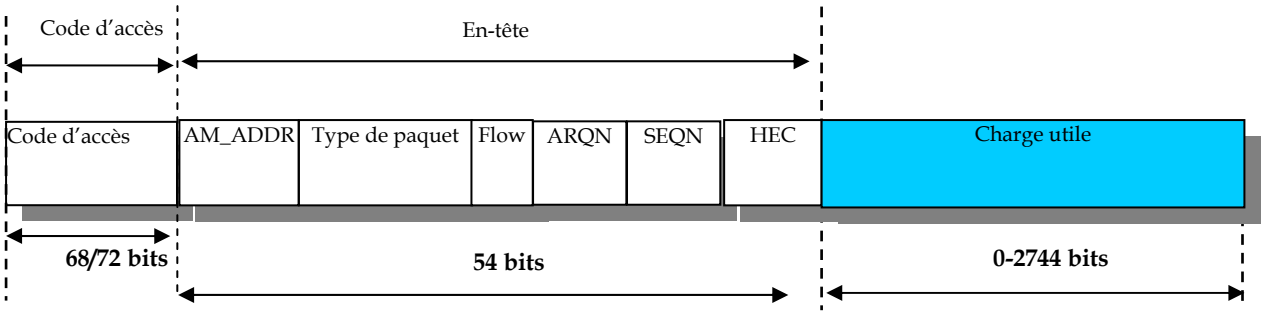


Figure 8 : Pile de protocole de transport Bluetooth

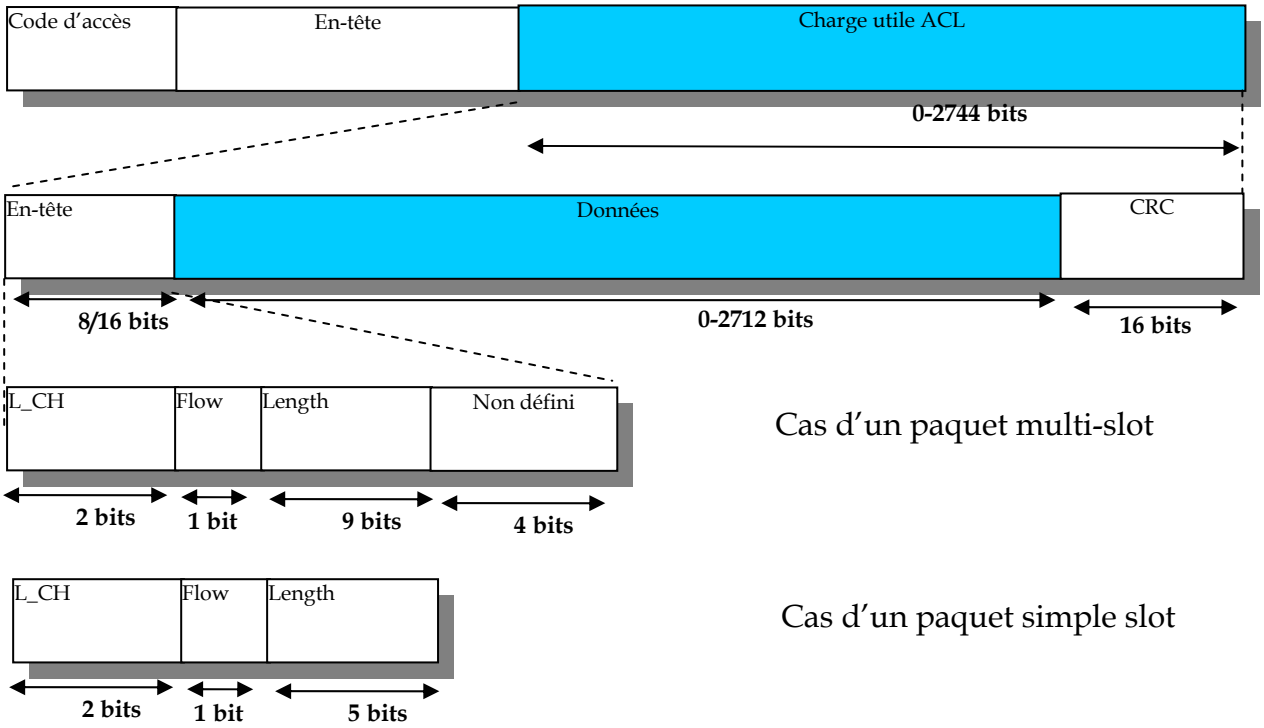
Paquet de bande de base :



Le code d'accès sert à identifier le piconet auquel appartient le message.
L'en-tête sert au contrôle de liaison et par mesure de robustesse, le protocole utilise un encodage FEC 1/3, qui consiste à dupliquer trois fois les mêmes données (18 bits utiles). L'en-tête indique l'adresse de périphérique esclave participant à la communication, le type de paquet transporté (données ACL/SCO ou contrôle), l'état du tampon du périphérique (contrôle de flots de données) et acquitte les trames par les indicateurs ARQN/SEQN.

Charge utile ACL :

Une charge utile ACL transporte des paquets de données provenant de la liaison L2CAP ou des messages de contrôle de la liaison LMP (Link Manager Protocol) entre les deux entités.



L_CH : indique le type du paquet. Cela peut être un nouveau message L2CAP, une suite d'un message L2CAP ou message LMP.
Flow : permet de contrôler le flot de données au niveau L2CAP,
Length : indique la taille en octets du champ de données,

Charge utile SCO :

Les données SCO ne font pas l'objet de contrôle de flux, ni de contrôle d'erreur (pas de champs CRC) ; les paquets peuvent donc êtres altérés ou perdus.

Le protocole L2CAP :
Le protocole L2CAP (Logical Link Control and Adaptation Protocol), permet d'offrir de multiples connexions au dessus des liens ACL. Il s'occupe également de la segmentation des paquets avant de les délivrer à la base de bande (baseband).

Le multiplexage de protocoles est supporté par la mise en place de canaux virtuels. Chaque canal est lié à un protocole de niveau supérieur. On peut lier plusieurs canaux à un seul protocole, mais il est impossible de lier plusieurs protocoles à un seul canal. Chaque paquet L2CAP reçu sur un canal est transmis au protocole lui correspondant.
L2CAP supporte des tailles de paquets jusqu'à 64 Ko et se charge de la segmentation et du ré-assemblage pour les couches de protocoles inférieures.
Les connexions L2CAP utilisent un CID (Connexion ID) pour s'identifier. Le CID 0x0001 est réservé pour les signaux de signalisation ; 0x0002 est réservé pour les données de diffusion.
Les piles de protocole au dessus de L2CAP sont identifiées par une valeur PSM (Protocol Service Multiplexor). Les entités qui demandent une connexion pour un PSM particulier, reçoivent en retour un CID de la part de L2CAP.

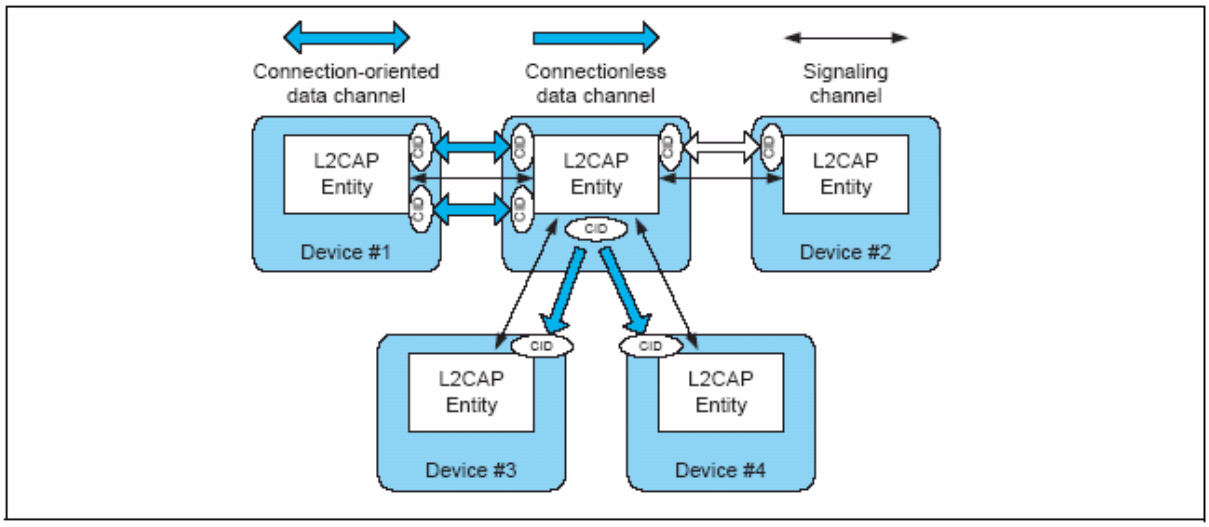


Figure 9 : Canaux L2CAP entre unités Bluetooth

Les paquets de données L2CAP ont 3 champs :

- Longueur : indique la taille du champ charge utile ; sert à la vérification d'intégrité lors du processus de réassemblage,
- Channel ID : définit l'unité et le protocole destinataire,
- Charge utile : données en provenance/à destination du protocole de niveau supérieur.

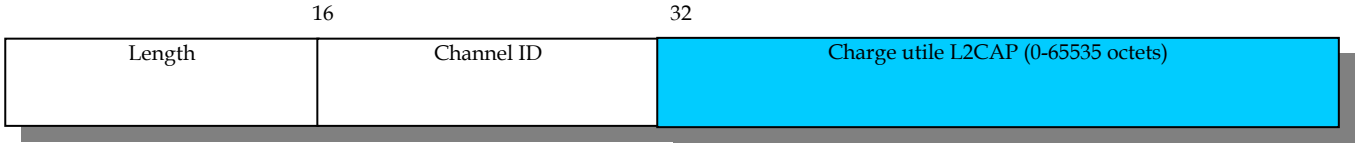
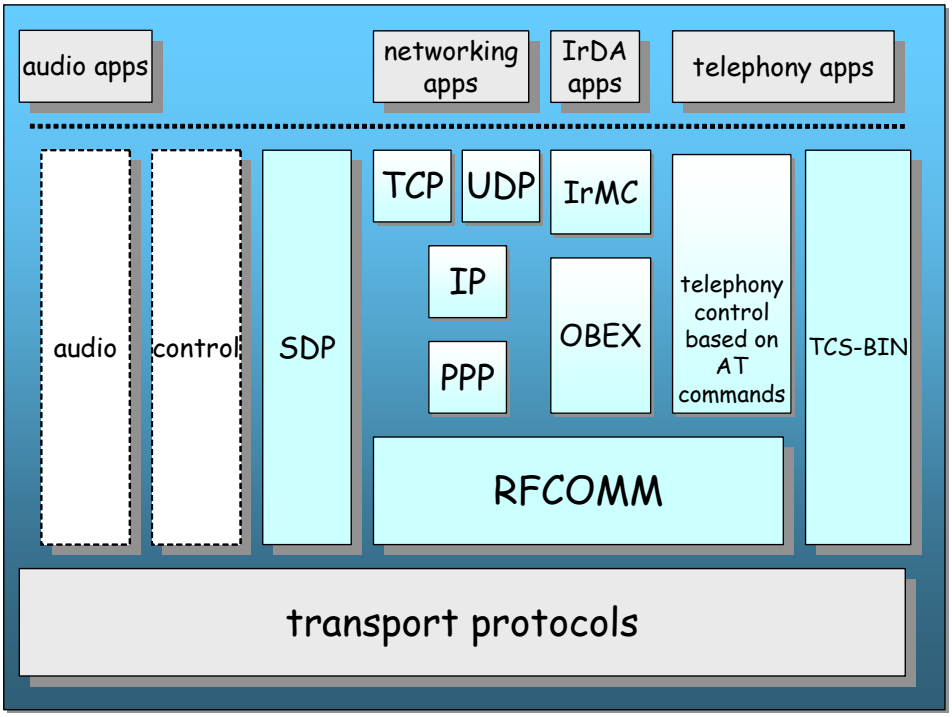


Figure 10 : Paquet L2CAP

La couche L2CAP permet aux protocoles de niveau supérieur de faire abstraction de la taille restreinte des paquets de la bande de base.

1.1.6.2 Les protocoles Middleware

Cette famille de protocoles s'intercale entre les protocoles de transport Bluetooth et les applications afin de faciliter l'interopérabilité des applications quelle que soit l'architecture de transport sous-jacente.



SDP (Service Discovery Protocol) est une composante essentielle du Middleware Bluetooth, car il offre un service d'enregistrement et de découverte de protocole, qui facilite la mise en oeuvre d'équipements Bluetooth.
Le schéma ci-dessus n'est pas exhaustif et il existe actuellement d'autres protocoles.

1.1.7 Les profils bluetooth

Les profils Bluetooth définissent comment sont effectués les assemblages de protocoles afin de répondre à une application donnée. Cette définition de profils permet de décrire sans ambiguïté les protocoles à mettre en œuvre pour répondre à une application précise et facilite ainsi l'interopérabilité des équipements Bluetooth.

1.1.8 La puissance, la portée et les débits

La puissance d'émission permise pour un équipement Bluetooth est réglementée, la portée du rayonnement radio et donc d'une liaison de communication est par conséquent limitée. Trois classes de puissance sont définies par la norme (voir tableau), mais seulement deux sont couramment utilisées (classes 1 et 3).
Le choix d'une classe est effectué vis-à-vis de zone de portée nécessaire à l'application visée, sachant que le coût et la consommation électrique augmentent avec la portée radio.

Classe de puissance	***Puissance de sortie maximum***	***Portée***
1	100mW (20dBm)	100 m*
2	2.5mW (4dBm)	30 m *
3	1 mW (0dBm)	10 m *

* il faut savoir que ces distances sont des distances mesurées en champ libre c'est à dire sans obstacle entre l'émetteur et le récepteur. En espace clos (par des murs par exemple), les portées sont plus faibles (100m devient environ 30 à 40 mètres et 10 m peut devenir 4 m).

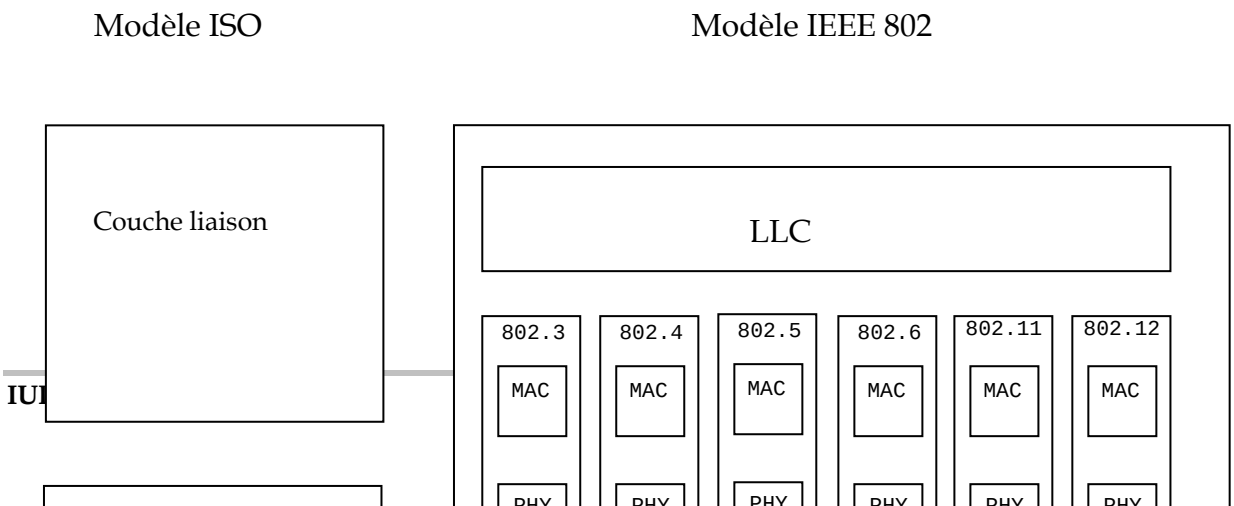
Plus l'éloignement entre l'émetteur et la source sera important, plus les débits seront faibles, de part le simple mécanisme de retransmissions.

1.2 Wifi (norme 802.11)

1.2.1 Introduction Wi-Fi

Le Wi-Fi (*Wirelesss Fidelity*) est le nom commercial donné à la norme IEEE 802.11b par la Wi-Fi alliance. Cette organisation est une association à but non lucratif qui certifie l'interopérabilité des matériels WLAN basés sur la norme IEEE 802.11b.

Les réseaux conformes à la norme 802.11 appartiennent à la famille du standard IEEE 802. Le principal intérêt de ce standard est de normaliser les couches physique et liaison afin de rendre facilement interopérables les différents standards de réseaux locaux.



La couche LLC identique entre 802.3 et 802.11 permet l'interopérabilité entre Ethernet (802.3) et Wi-Fi (802.11) au niveau de la couche 2.

1.2.2 Technologie Wi-Fi

Wi-fi est une technologie de communication dont le but principal est de permettre la connexion à un réseau local non plus par l'intermédiaire d'un câble mais au moyen d'un support sans fil. La principale force de Wi-Fi est de garder les fonctionnalités des réseaux locaux et d'inter opérer avec des machines connectées au réseau Ethernet filaire « classique ».

Comme nous venons de le voir, un réseau local Wi-Fi se comporte comme un réseau Ethernet à la différence prés que les données ne transitent plus sur support de transmission filaire mais par ondes hertziennes. Les communications Wi-Fi utilisent la bande de fréquences 2400 MHz-2483.5 MHz.

Les éléments nécessaires pour constituer un réseau sans fil sont les points d'accès d'une part ,et les clients d'autre part. Pour accéder au réseau sans fil, les cartes clientes doivent s'associer avec un point d'accès.

1.2.3 Architecture des Réseaux Wi-Fi

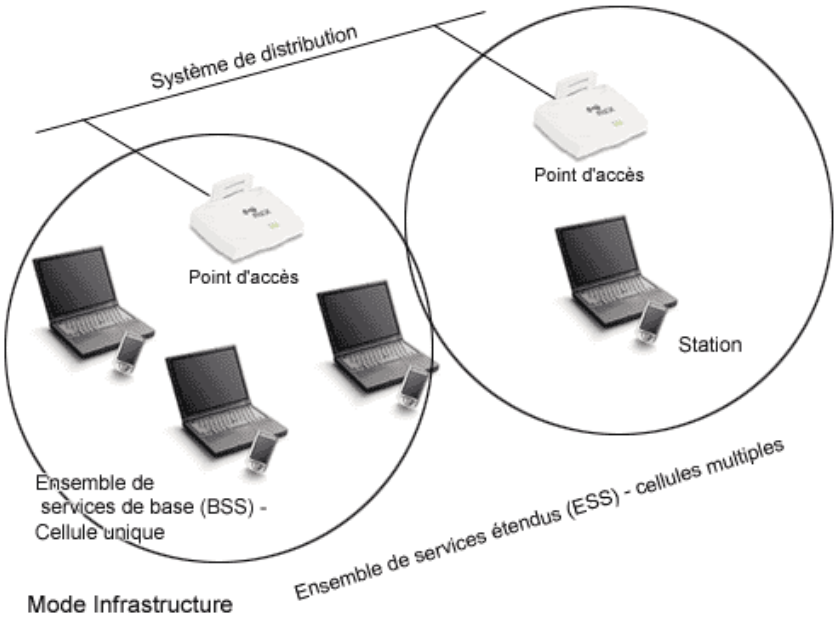
Un réseau Wi-Fi peut fonctionner avec deux types d'architecture :

- en mode Infrastructure,
- en mode ad-hoc.

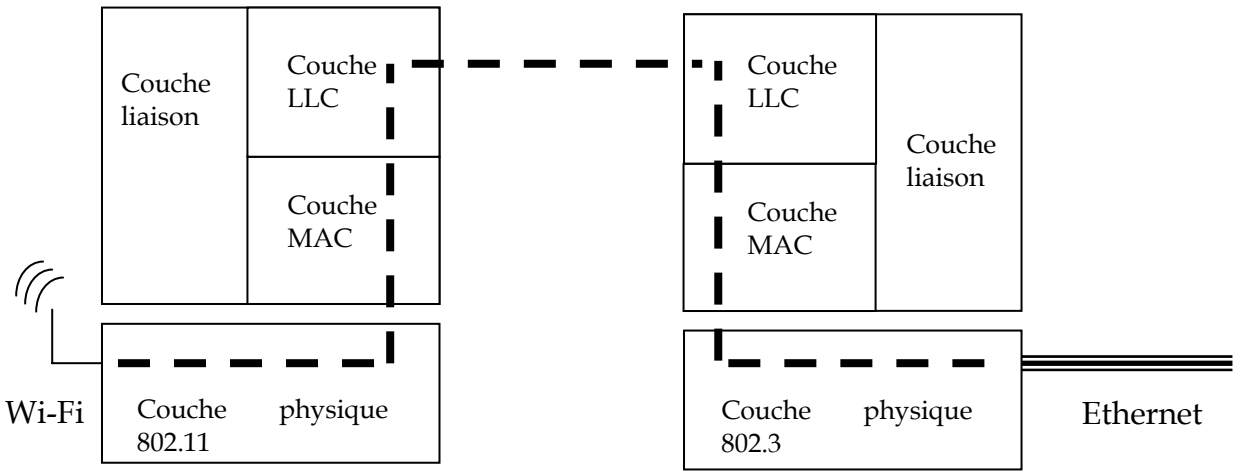
Le mode infrastructure est un mode dans lequel toute machine qui veut accéder au réseau, doit au préalable s'associer avec une station particulière appelée « point d'accès ».
En mode ad-hoc, une machine peut s'associer avec n'importe quelle autre qui est dans sa zone de portée radio, les dialogues s'effectuent en mode point à point.

1.2.3.1 Mode Infrastructure

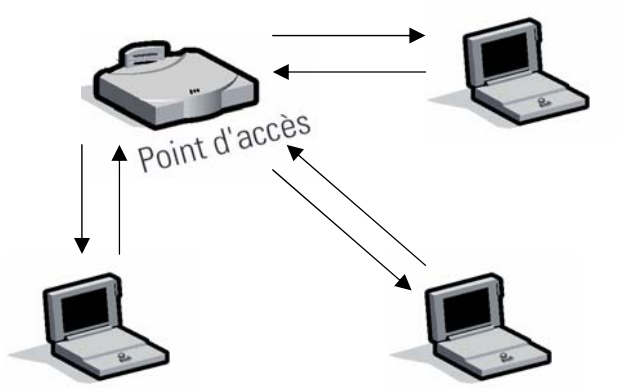
Le mode infrastructure ou BSS (Basic Service Set) fonctionne sur une architecture de type cellulaire. Chaque BSS est géré par un point d'accès (AP) qui administre l'accès au réseau des stations Wi-Fi.



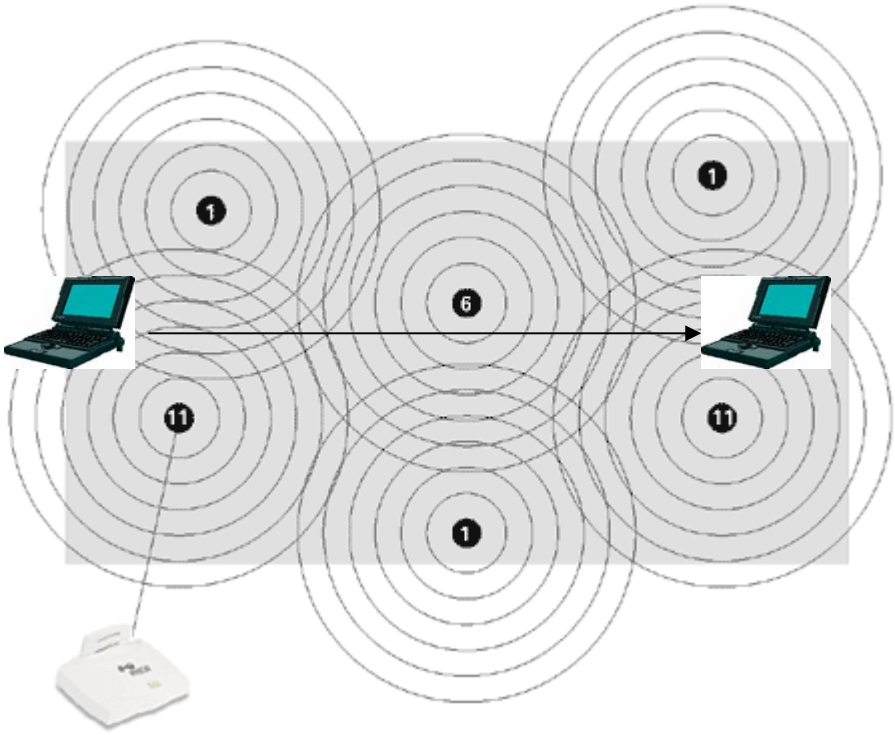
Un point d'accès ne permet de couvrir qu'une zone géographique limitée à une cellule qui est en fait la zone autour de laquelle le signal radio est suffisamment puissant pour cet AP. La norme Wi-Fi définit l'ESS, qui étend le réseau local par l'utilisation de plusieurs points d'accès eux-mêmes interconnectés par l'intermédiaire d'un système de distribution (DS). Le DS couramment utilisé est Ethernet mais l'utilisation de Wi-Fi est tout à fait possible.
L'ESS peut fournir aux différentes stations associées au réseau un accès à d'autres réseaux par le biais d'une passerelle. Comme nous l'avons vu précédemment, une passerelle avec Ethernet fonctionne à la manière d'un pont.



Une station qui entre dans le réseau pour la première fois et souhaite joindre le BSS devra rechercher un point d'accès et s'associer avec lui avant toute autre opération.
Toutes les communications d'une station seront relayées sur le réseau par le point d'accès auquel elle est associée.

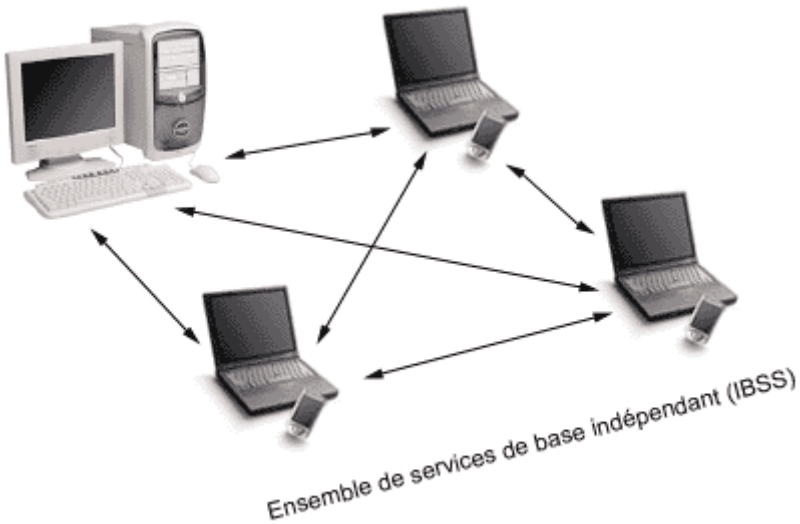


La structure d'un réseau sans fil en mode infrastructure doit être conçue de manière à offrir une continuité de service sur toute la zone à couvrir. Pour ce faire, les différents points d'accès de l'ESS devront être mis en place à la manière d'un réseau cellulaire téléphonique.
Pour assurer une réelle continuité de service, il faudra que les cellules se recouvrent.



1.2.3.2 Mode ad-hoc

Le mode ad-hoc ou IBSS (Indépendant BSS) permet à des stations sans fil 802.11 de communiquer directement entre elles sans point d'accès. La condition expresse pour que deux stations d'un même IBSS en mode ad-hoc puissent communiquer est qu'elles doivent être à portée de vue (dans le sens ondes radio) l'une de l'autre.



Mode Ad Hoc

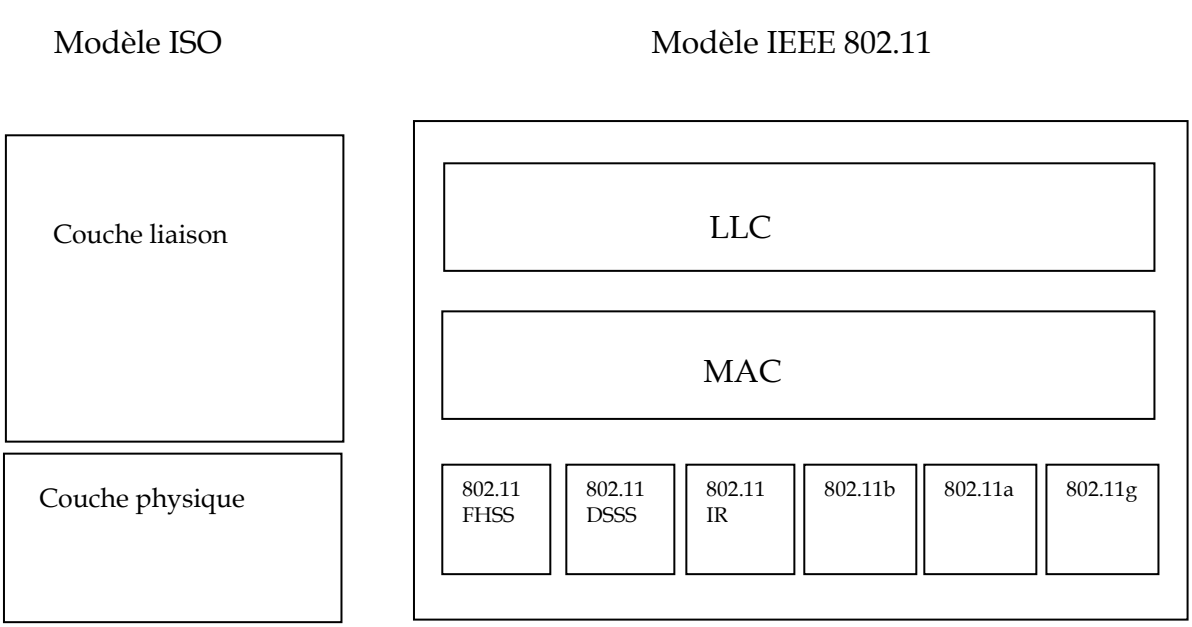
Si plusieurs stations sont dans un même IBSS, il ne sera pas possible de faire communiquer deux stations qui ne sont pas à portée de vue ; en effet la norme ne propose pas de protocole de routage qui permettrait aux machines de relayer les

informations. C'est pour cette raison qu'on utilise le terme de mode ad hoc en non pas réseau ad hoc.

Nous verrons par la suite qu'il existe des possibilités de routage ad hoc qui ne sont pas couverts par la norme 802.11.

1.2.4 La couche physique

La norme 802.11 couvre les deux premières couches du modèle OSI. Il existe plusieurs couches physiques normalisées, et le standard définit une couche MAC identique, ce qui permet de rajouter de nouvelles couches physiques tout en restant compatibles avec les couches supérieures.



Les différentes couches physiques disponibles sont :

- 802.11 FHSS : utilisation de la bande des 2.4 GHz avec une technique d'étalement de bande fondée sur le saut de fréquence (technique identique à Bluetooth) pour des communications à 2 Mbits/s,
- 802.11 DSSS : utilisation de la bande des 2.4 GHz avec une technique de séquence directe sur 14 canaux pour des communications à 1 ou 2 Mbits/s,
- 802.11 IR : utilisation des ondes infrarouges pour des communications à 1 ou 2 Mbits/s,
- 802.11b : est une extension du 802.11 DSSS qui grâce à de nouvelles techniques de codage et de modulation introduit les vitesses de communication de 5.5 et 11 Mbits/s,
- 802.11a : utilise la bande des 5 GHz pour des communications de 6 jusqu'à 54 Mbits/s,
- 802.11g : est une extension du 802.11b qui grâce à la modulation OFDM permet d'atteindre des vitesses de communication jusqu'à 54 Mbits/s.

A présent nous nous intéresserons uniquement à la couche physique 802.11b, actuellement la plus couramment utilisée.

La couche physique a pour rôle principal d'établir et de maintenir une transmission sans fil entre les stations composant le réseau. Elle propose certaines primitives à la couche supérieure. En particulier, elle offre à la couche MAC des primitives lui permettant de tester l'état – occupé ou disponible – du canal ou bien encore de savoir si une transmission ou une réception vient de commencer ou de se terminer.

Le mode de transmission utilisé par Wi-Fi est la technique de DSSS (Direct Sequence Spead Spectrum).

La technique de la séquence directe divise la bande des 2.4GHz en 14 canaux de 22MHz chacun. Les données sont envoyées uniquement sur l'un des 14 canaux. Les canaux adjacents se recouvrent partiellement, n'offrant au maximum localement que 3 canaux ne se chevauchant pas. Trois réseaux DSSS peuvent donc cohabiter dans un même espace sans interférer entre eux. Une même cellule ne peut donc abriter que trois bornes d'accès transmettant sur des bandes de fréquences totalement disjointes. Avec 50 personnes par bornes d'accès, cela correspond à 150 utilisateurs au maximum dans une cellule.

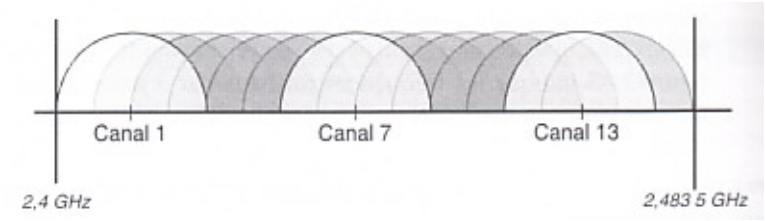


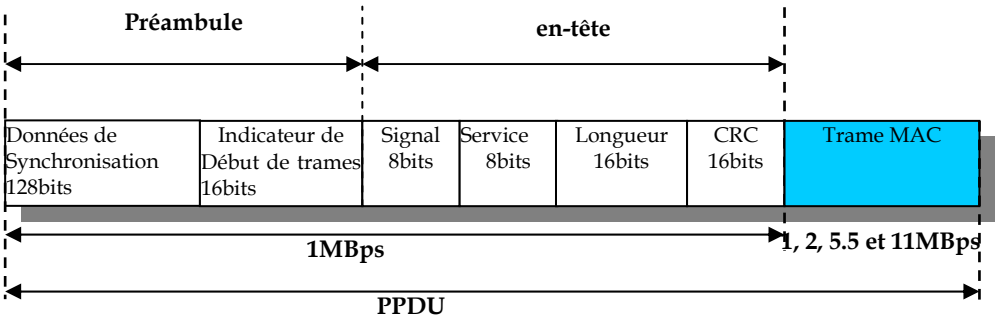
Figure 11 : Canaux de transmission 802.11b

La norme 802.11b supporte 4 vitesses de transmission : 1 Mbps, 2 Mbps, 5.5 Mbps et 11 Mbps. Les vitesses étant obtenues par l'utilisation de différentes techniques de modulation et de codage.

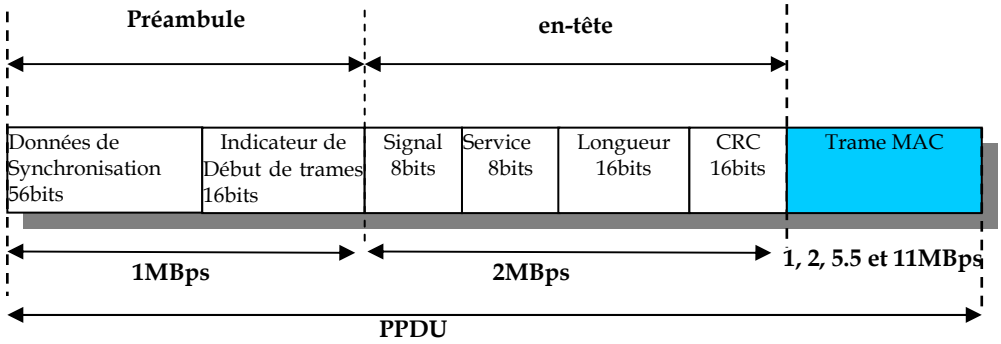
Débits	Codage	Modulation	Vitesse de symbole	Nombre de bits/symbole
1 Mbps	11 (*Barker Sequence*)	BPSK	1 MSps	1
2 Mbps	11 (*Barker Sequence*)	QPSK	1 MSps	2
5.5 Mbps	8 (*CCK*)	BPSK	1,375 MSps	4
11 Mbps	8 (*CCK*)	QPSK	1,375 MSps	8

Il existe 2 types de trame physique 802.11b qui ont les structures suivantes :

- trames avec en-tête long



- trames avec en-tête court



Les en-tête longs doivent être utilisés pour conserver la compatibilité avec le matériel de première génération de norme 802.11. Les en-tête courts permettent une meilleure efficacité de transmission.
Les données d'en-tête permettent de synchroniser récepteur et émetteur au niveau physique, pour la trame MAC encapsulée. Les différents champs sont les suivants :

- SYNC : synchronisation des horloges (champs composé de 1),
- SFD : pattern de signalisation de début de trame (0000010111001111),
- Signal : indique la vitesse de transmission du paquet MAC (permet la sélection du mode de modulation et de codage),
- Service : ce champ est réservé pour des extensions de la norme 802.11,
- Longueur : indique la durée (en microsecondes) nécessaire à la transmission de la trame MAC à suivre,
- CRC : code permettant au récepteur de savoir si l'en-tête a été ou non corrompu lors de la transmission sur le canal radio.

1.2.5 Format des trames MAC

Toutes les trames Mac ont la même forme de base (cf. Figure 12) :

- Une en-tête MAC
- Un corps
- Un FCS (Frame Check Sequence)

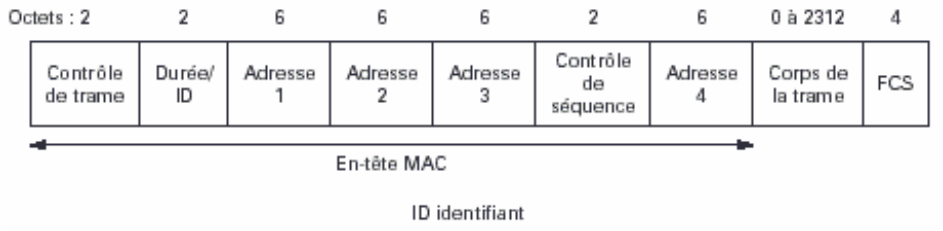


Figure 12 : Format général des trames MAC

Le FCS permet de détecter les erreurs de transmission. Le corps de la trame contient les données utilisateur.

Le champ « contrôle de trame » contient la version du protocole utilisé, le type de trame envoyé (contrôle, administration ou donnée), l'information d'une fragmentation ou non de la trame, d'un processus de chiffrement (WEP) ou non.
Le champ « Durée/Id» contient une durée calculée pour la transmission de la trame fonction du débit de la couche physique.

Les champs « adresse » contiennent l'adresse de l'émetteur, du récepteur, et l'adresse de la station à laquelle la trame est envoyée (utile en cas de stations relais), l'adresse de la station transmettant la trame.

Le champ « contrôle de séquence » stocke le numéro de séquence ou le numéro de fragment.

Les types de paquet MAC sont au nombre de trois : les paquets de données, de contrôle (RTS, CTS et ACK…) et d'administration (balise Beacon,…).

Les trames d'acquittement et CTS sont longues de 14 octets et le RTS 20 octets.

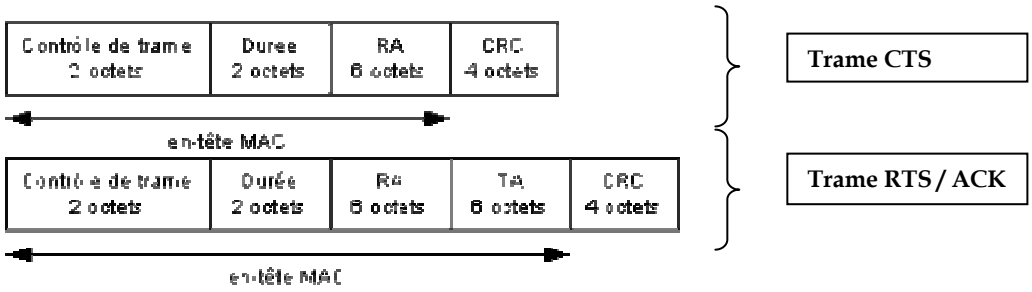


Figure 13 : Format des trames RTS, CTS et ACK

1.2.6 Deux modes de partages du médium

La couche MAC dispose de deux méthodes d'accès fondamentalement différentes : DCF (Distributed Coordination Function) et PCF (Point Coordination Function). La norme prévoit également un mode combinant les deux au sein d'une BSS.

PCF
La fonction de coordination par point (PCF) est prévue pour la transmission de données sensibles, comme la voix ou la vidéo. Lorsque ce mode est activé, le Point d'Accès élit chaque station pour un temps déterminé et passe à la station suivante. Ainsi, chaque station n'est autorisée à transmettre ou à recevoir les données que si elle a été élue. Ce fonctionnement permet de garantir une certaine qualité de service.
Mais, sur un réseau comprenant beaucoup d'utilisateur, le fait d'avoir un seul point d'accès au support et d'élire tour à tour chaque station peut vite être un inconvénient. Par ailleurs, le caractère centralisé de la fonction de coordination par point (PCF) explique qu'elle ne soit pas implémentée dans le mode ad-hoc.

Finalement, la norme 802.11 n'en parle qu'en terme optionnel ce qui a conduit à la voir fort peu implémentée par les différents constructeurs.

DCF

Cette méthode d'accès avec contention se base sur la méthode d'accès multiple à détection de porteuse et évitement de collision (CSMA/CA détaillé au paragraphe 2.5.3) et elle reste la méthode d'accès fondamentale de la norme 802.11.

1.2.7 CSMA/CA

Très proche du CSMA/CD IEEE 802.3, le protocole CSMA/CA est forcé de pratiquer l'évitement de collision car les systèmes radio simples sont incapables de transmettre et d'écouter simultanément (nécessité d'une liaison radio full-duplex). Partant de ce constat, l'équivalent de la détection de collision sera assuré par un accusé de réception systématique de chaque paquet non corrompu reçu. Cette surcharge protocolaire inconnue dans Ethernet explique que les performances d'un LAN 802.11 sont toujours inférieures à celle d'un LAN 802.3 équivalent.

L'accès aux ondes est donc partagé et chaque émission est précédée par une écoute du support. Plus précisément, le protocole fonctionne de la manière suivante : avant d'émettre, la station vérifie l'état du médium et, si le support est libre, elle attend un temps aléatoire avant d'émettre, à condition que le support soit toujours libre. Si le paquet ne subit aucune altération, la station réceptrice renvoie un acquittement qui clôt le processus. En cas d'échec, la station émettrice retransmet. La Figure 14 résume ce processus :

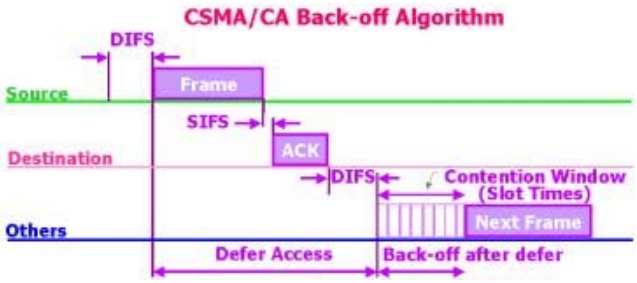


Figure 14 : Schéma classique de transmission en CSMA/CA

Détection de porteuse (physique et virtuelle)

La couche physique met à disposition de la couche MAC une primitive de vérification de la disponibilité du canal (CCA ou Clear Channel Assessment). Avant d'émettre, la station vérifie que le médium est libre, en analysant toutes les trames détectées ainsi qu'en évaluant une quelconque activité à partir de la force relative du

signal provenant des autres machines. En cas d'occupation du canal, l'émetteur probable diffère sa transmission jusqu'à ce que le médium redevienne libre.

Parallèlement, la station émettrice effectue également une détection virtuelle de porteuse. Basée sur les informations contenues dans l'en-tête des trames RTS (Request To Send), CTS (Clear To Send) et des trames de données, le champs « Durée/Id » indique le temps en microsecondes qu'il faudra pour que la prochaine trame de contrôle ou de donnée soit transmise avec succès. Ce procédé permet de réserver auprès des autres stations le médium pendant la durée de la transmission. Chaque station détient un vecteur d'allocation réseau (NAV) qu'il met à jour à chaque fois que la transmission d'une trame est détectée. Avant sa propre émission, il vérifie préalablement par l'intermédiaire du NAV si le médium est libre puis ensuite il vérifie physiquement s'il l'est vraiment.

Temporisateurs et Algorithme de back-off

Quatre temporisateurs apparaissent dans la norme. Le SIFS (Short Inter Frame Space) est le plus court utilisé pour les trames d'acquittement et la transmission en rafale de fragments. Le second est le PIFS (PCF IFS) plus court que le DIFS ce qui permet aux transmissions PCF de prendre le pas sur les données DCF. Le DIFS (DCF IFS) correspond au temps minimal avant transmission en mode DCF. Et finalement l'EIFS (Extended IFS) est relativement long par rapport aux autres et sert à éviter les collisions en série. Il reste le *slot time* qui représente l'unité du canal, soit l'intervalle minimal entre deux détections physiques de porteuse.

Afin de pouvoir accéder au médium à nouveau, il faut que la précédente transmission réussie ou non soit suivie respectivement d'une période égale à un DIFS ou un EIFS durant lequel le médium reste libre. A ce moment-là, l'accès concurrent au médium entre les différents émetteurs peut se faire ce qui constitue l'instant le plus propice aux collisions. Afin de réduire cette probabilité de collision, un mécanisme de tirage aléatoire, « l'algorithme de back-off », a été introduit (cf. Figure 15). Lors de la première tentative de transmission, tous les concurrents tirent un temporisateur dans un intervalle basé sur la taille de la Contention Window qu'ils décrémentent jusqu'à ce que le médium soit occupé ou que le décompte atteigne zéro :

- s'il atteint zéro, la station correspondante transmet,
- si deux ou plusieurs stations atteignent zéro simultanément, un nouveau tirage pour chaque participant est effectué dans un intervalle plus important (cf. Figure 16),
- si le médium devient occupé avant la fin du décompte, la station bloque le temporisateur.

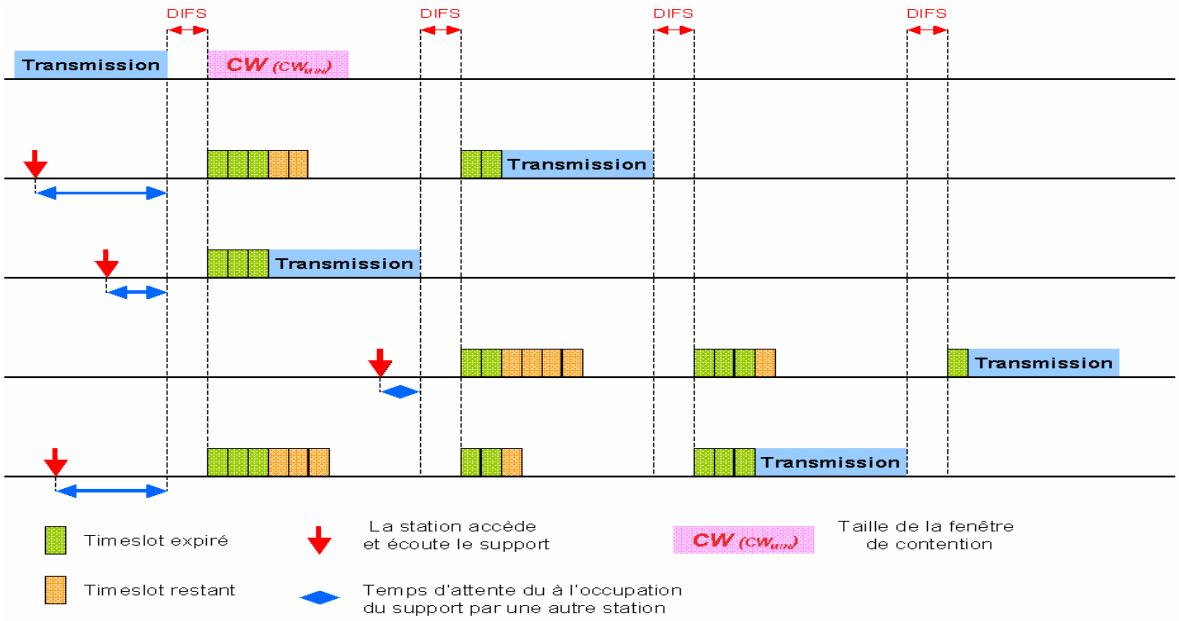


Figure 15 : Accès concurrent au médium

La taille de la *fenêtre de contention*, qui détermine la taille de l'intervalle où est tiré le temporisateur, est contenu entre une valeur minimale et maximale caractéristique de la couche physique concernée (Cwmin et Cwmax).

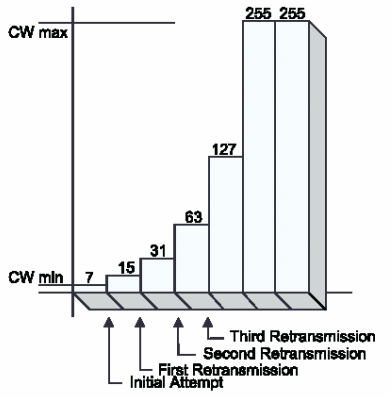


Figure 16 : Exemple d'une croissance exponentielle d'une fenêtre de contention

Ce mécanisme est l'un des obstacles que présente DCF quant à la garantie d'un délai minimal, essentiel pour les applications temps réelles mais il assure bien sa fonction première qui est un accès au médium équitable.

1.2.8 L'accès au réseau

Si une liaison sans fil présente un certain nombre d'avantages, il comporte également quelques inconvénients. Dans le cas de la technologie Ethernet, la simple action de branchement d'une prise RJ45 nous donne accès au média ; ceci est moins simple

pour Wi-Fi car il n'y a pas de connexion physique. Un client Wi-fi voulant accéder au réseau, doit donc suivre une suite d'opérations séquentielles :

- recherche du réseau : scanning,
- joindre le réseau : *joining*,
- authentification,
- association.

1.2.8.1 Scanning

Comme nous venons de le voir, avant d'accéder au réseau, il faut d'abord vérifier la présence d'un réseau compatible avant de le joindre.
La norme prévoit deux méthodes :

- scanning passif,
- scanning actif

Le scanning passif consiste à rechercher sur tous les canaux de transmission la présence de trames balises (*Beacon frames*). Ces trames balises sont stockées par le client afin d'en retirer toutes les informations sur le BSS émises.
En scanning actif, la station émet des trames *Probe Request* sur tous les canaux afin de solliciter un réseau dont elle connaît le nom. Si une station à laquelle on peut s'associer reçoit cette trame alors elle renvoie une trame *Probe Response.*

1.2.8.2 Joining

Une fois les informations collectées, la station choisit son point de raccordement au réseau en fonction du réseau choisi (nom de BSS) et de la puissance du signal reçu. Elle règle également ses paramètres en fonction de ceux du réseau choisi : canal de transmission, vitesse de communication.

1.2.8.3 Authentification

La norme prévoit deux types d'authentification :

- Authentification système ouvert,
- Authentification par clé partagée.

En système ouvert, le client envoie une trame d'authentification vers la station choisie. La station réceptrice, récupère l'adresse MAC de la station émettrice et effectue un test d'authentification. Si le test est bon il renvoie une trame d'acceptation.
Remarque : Le test d'authentification peut être un filtrage sur adresse MAC ; cela peut également être aucun test.

L'échange de clé partagée, permet un meilleur niveau de sécurité, mais des études ont prouvé que l'on pouvait trouver la clé en espionnant le trafic et il existe des logiciels du domaine public permettant de réaliser cette opération sans connaissances particulières sur sécurité (Airsnort).

La sécurité est le gros point faible des réseaux sans fil de la famille 802.11.

1.2.8.4 association

La procédure d'association est la dernière étape pour l'accès au réseau. Elle s'effectue en 3 phases :

- demande d'association de la part du client,
- réponse d'association avec un code de succès,
- début de gestion du trafic par le point d'accès ayant accepté ce client.

1.2.9 La puissance, la portée et les débits

Nous envisageons d'utiliser Wi-Fi pour des communications inter véhicules, avec la réglementation pour contrainte au niveau de la puissance d'émission radio. Les normes d'émission sont liées a des contraintes de deux types :

- d'une part, la bande de fréquence utilisée était par le passé utilisée par l'armée et n'est que progressivement libérée,
- d'autre part les émissions d'ondes électromagnétiques sont contrôlées afin que notre environnement ne se transforme pas en gigantesque four micro-ondes pour les humains.

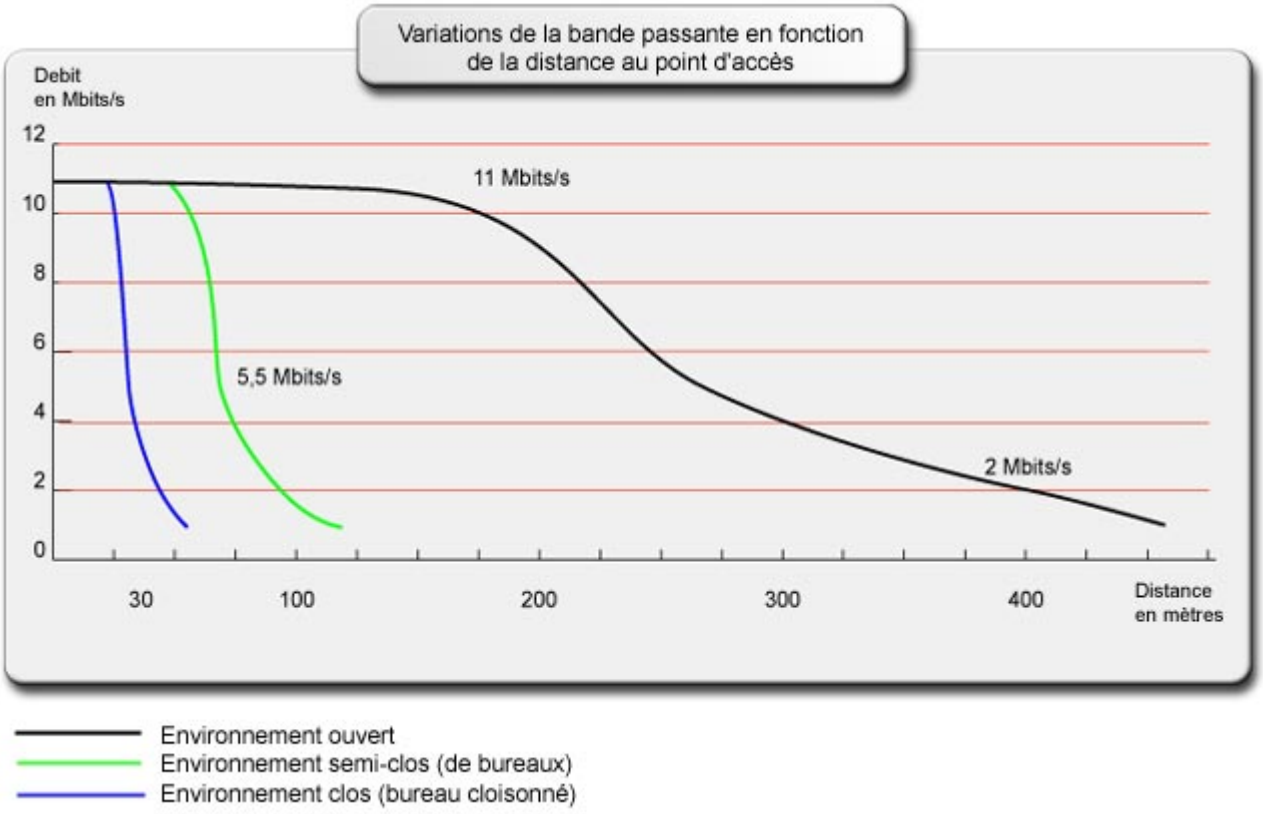
La réglementation fixe actuellement les règles suivantes :

	Intérieur	Extérieur	Canaux Wi-Fi
2400 MHz 2454 MHz	100 mW	100 mW	1 à 9
2483,5 MHz		10 mW	10 à 13

L'IEEE 802.11b définit un débit de transmission allant jusqu'à 11Mbit/s. Les communications utilisent la propagation par ondes radio, les puissances sont réglementées et sont donc soumises aux aléas de ce support physique, ceci a nécessairement une influence sur le débit réel. Le débit du WLAN dépend de plusieurs facteurs, dont :

- la puissance d'émission,
- les interférences,
- la propagation des ondes radio,
- le partage du lien Wi-Fi entre plusieurs clients.

Tout cela réduit en pratique la bande passante disponible et les conditions. Bien entendu, tout ce qui affecte le trafic des données sur les portions filaires du réseau (par exemple : la latence, les goulets d'étranglement) affectera aussi la portion sans fil. Cela correspond globalement aux débits d'un réseau Ethernet 10 Mbps, car le débit maximal d'un réseau câblé ne peut qu'être atteint approximativement. Cependant, dans un Wireless LAN, plus la portée est grande, plus le débit diminue. Dès les 30-150 m de distance le débit est de 5.5 Mbps puis chute à 2 Mbps et à 1 Mbps. La plus longue distance est atteinte à 1 Mbps (jusqu'à 400 m).



On peut ajouter au résultat présenté dans ce graphique, que le paramètre de mobilité va sans aucun doute encore diminuer la portée obtenue si on utilise Wi-Fi dans des véhicules. L'effet doppler du au mouvement des véhicules les un par rapport aux autres, va modifier les signaux physiques, ce qui aura pour effet d'augmenter le BER (Bit Error Rate)

1.3 Le routage Ad hoc

Wi-Fi permet une communication entre deux clients par l'intermédiaire du mode Ad hoc, ce qui permet de communiquer entre deux machines à portée radio l'une de l'autre, mais ceci ne permet pas de router des paquets de saut en saut au travers de noeuds intermédiaires pour des noeuds qui ne seraient pas à portée radio les uns des autres. Une solution consiste à mettre en œuvre des techniques de routage Ad hoc. Le routage Ad hoc est la possibilité donnée à un réseau de constituer ses nœuds et

ses routes non plus de façon statique, mais dynamiquement en fonction des apparitions/disparitions/déplacement de nœuds dans le réseau.

Deux approches de routage sont possibles : le routage réactif et le routage proactif. Dans un protocole de routage réactif, les mobiles ne conservent pratiquement aucune information sur la topologie globale du réseau. Seules sont stockées les informations sur les routes actives. Les routes sont construites à la demande et sont détruites lorsqu'elles ne sont plus utilisées.
Dans un protocole de routage proactif, la topologie du réseau est connue de tous les mobiles. Les routes sont disponibles immédiatement mais, en contrepartie, il faut diffuser régulièrement des informations sur les changements de topologie du réseau.
Les protocoles réactifs génèrent a priori un volume plus faible de signalisation mais en contrepartie engendrent un délai lors de la construction des routes et produisent plus difficilement des routes optimales. Les protocoles proactifs disposent en permanence d'une route pour chaque destination dans le réseau mais génèrent un volume de signalisation important.

Il existe également des protocoles géographiques qui utilisent des informations de localisation fournies par un système GPS pour affiner le routage. Il faut noter qu'il n'y a pas relation totale entre distance physique et connectivité radio, même si certaines limitations liées aux propriétés du signal associées aux informations de positionnement permettent d'optimiser les routes.

Dans notre cas, les protocoles de routage réactifs sont les plus adaptés de par la mobilité constante des véhicules.

En terme de normalisation, le groupe Manet de l'IETF travaille actuellement sur la standardisation de plusieurs protocoles de routage pour les réseaux ad-hoc. Le protocole de routage réactif AODV fait partie des favoris, il est actuellement implémenté dans de nombreux réseaux communautaires Wi-Fi.

1.4 Quelle place pour ces technologies dans l'automobile ?

Dans ce chapitre, nous avons observé les caractéristiques des technologies Wi-Fi et Bluetooth, et on peut déjà limiter le domaine d'intervention de Bluetooth à l'intérieur du véhicule ou sa proximité. En ce qui concerne Wi-Fi, nous pouvons imaginer qu'il sera difficile de l'utiliser en mode infrastructure de part le nombre de cellules nécessaire pour couvrir tout un réseau routier. Nous avons vu que le routage Ad hoc pourrait constituer une alternative par l'utilisation d'un protocole de routage réactif.

Nous allons à présent nous intéresser aux performances réelles de ces technologies et pour cela les mettre en œuvre au sein d'une plateforme expérimentale de test.

2 Plate-forme expérimentale et investigations

2.1 La plate-forme

2.1.1 Environnement logiciel

La plate-forme expérimentale est construite sur la base du système Linux Redhat 8.0. Ce système supporte le matériel Bluetooth et Wifi au travers de pilotes de matériel (modules linux) et de logiciels open source.

Le matériel Wifi (cartes d'interface clientes au format PCMCIA) est supporté au travers de drivers se chargeant en tant que modules au niveau du système d'exploitation. La prise en charge de Wi-Fi est effectuée de la même manière une interface réseau Ethernet et Linux intègre tous les outils nécessaires à la configuration réseau. Des outils complémentaires spécifiques à la configuration des paramètres Wi-Fi et au monitoring existent mais font encore l'objet de mises à jour régulières.

Le matériel Bluetooth est supporté depuis peu sous linux. Plusieurs piles de protocoles sont disponibles, mais une seule a été récemment intégrée au noyau linux; la pile bluez développée en open sources par Qualcomm. La récente intégration dans le noyau (depuis le kernel 2.4.18) nécessite une mise à jour régulière du noyau par application de divers patchs pour corriger certains dysfonctionnements.

2.1.2 Environnement matériel

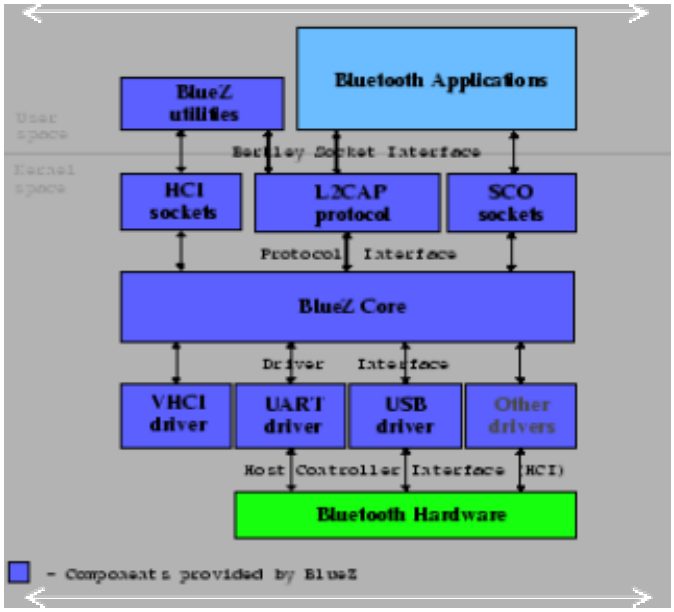
Pour la réalisation de la plateforme j'ai utilisé plusieurs configurations dont les sous-ensembles sont :

- 2 Pc Portables Dell,
- 2 cartes Wi-Fi Pcmcia Dell Truemobile 1150,
- 2 cartes Wi-Fi Pcmcia Cisco PCM352,
- 3 dongles usb Bluetooth classe 1 (portée théorique 100m),
- Pc desktop Dell

2.1.3 L'intégration de Bluetooth au sein de la plateforme

2.1.3.1 l'implémentation de Bluetooth dans linux

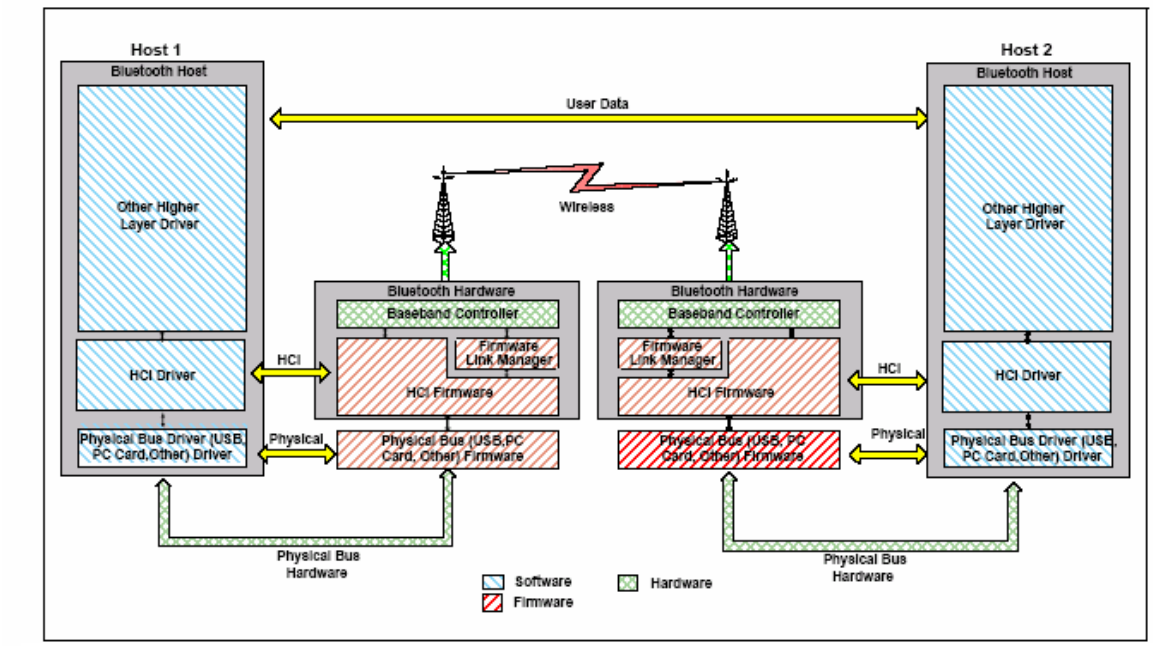
L'intégration de Bluetooth dans la plate-forme requiert l'installation de la pile de protocole Bluetooth Bluez.



Dans un environnement Redhat 8.0, le kernel 2.4.18 requiert l'installation du patch « patch-2.4.18-mh9 » et donc une compilation du noyau linux pour faire fonctionner notre matériel et toute la pile de protocole sur notre plate-forme.

2.1.3.2 *L'interface de contrôleur hôte*

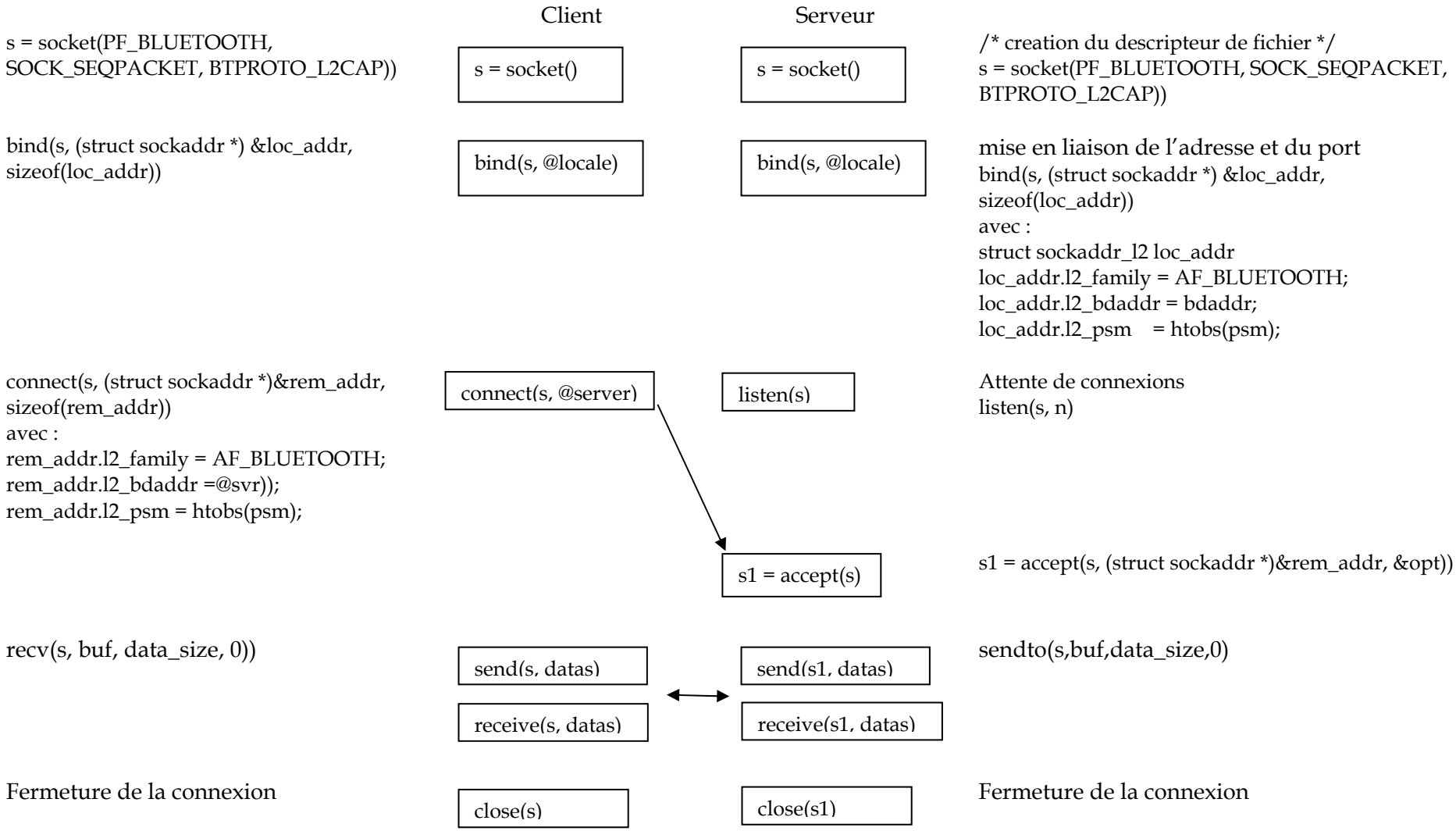
L'utilisation de dongles Bluetooth USB requiert l'usage d'une couche de transport supplémentaire qui est la Host contrôleur interface. le protocole HCI réalise l'interface entre les couches hautes de la pile Bluetooth incluse dans le PC et les couches basses de la pile incluses dans le dongle.



2.1.3.3 L'interface de programmation : les sockets Bluetooth

Bluez est un projet open source, et sa documentation n'est pas très fournie. De plus il n'y a pas d'API de programmation. Le seul moyen disponible pour le programmeur est de regarder les programmes d'exemples disponibles, de s'abonner à la liste de diffusion et de fureter sur le net pour glaner quelques informations. Les sources des exemples sont également peu commentés et un travail d'analyse a été nécessaire pour commencer le travail de programmation proprement dit. Cette remarque à pour objet de rappeler que même si la mise à disposition des sources est certainement un avantage pour bien analyser les mécanisme d'un programme et l'améliorer, une API bien documentée peut également faire gagner du temps.
Fort heureusement, Bluez implémente l'interface de programmation au travers de sockets suivant le standard Unix.

Pour envoyer des données entre un client et un serveur sur un lien L2CAP, le schéma suivant doit être suivi :


Client
Serveur
s = socket(PF_BLUETOOTH, SOCK_SEQPACKET, BTPROTO_L2CAP))
s = socket()
s = socket()
/* creation du descripteur de fichier */
s = socket(PF_BLUETOOTH, SOCK_SEQPACKET, BTPROTO_L2CAP))
bind(s, (struct sockaddr *) &loc_addr, sizeof(loc_addr))
bind(s, @locale)
bind(s, @locale)
mise en liaison de l'adresse et du port
bind(s, (struct sockaddr *) &loc_addr, sizeof(loc_addr))
avec :
struct sockaddr_l2 loc_addr
loc_addr.l2_family = AF_BLUETOOTH;
loc_addr.l2_bdaddr = bdaddr;
loc_addr.l2_psm = htobs(psm);
connect(s, (struct sockaddr *)&rem_addr, sizeof(rem_addr))
avec :
rem_addr.l2_family = AF_BLUETOOTH;
rem_addr.l2_bdaddr =@svr));
rem_addr.l2_psm = htobs(psm);
connect(s, @server)
listen(s)
Attente de connexions
listen(s, n)
s1 = accept(s)
s1 = accept(s, (struct sockaddr *)&rem_addr, &opt))
recv(s, buf, data_size, 0))
send(s, datas)
receive(s, datas)
send(s1, datas)
receive(s1, datas)
sendto(s,buf,data_size,0)
Fermeture de la connexion
close(s)
close(s1)
Fermeture de la connexion

2.1.4 L'intégration de Wi-Fi sur la plateforme

La première étape pour faire fonctionner le matériel est d'installer les drivers. En effet sur la version de Linux installée, nos cartes n'étaient pas reconnues à priori.

On identifie d'abord la carte connectée sur le port Pcmcia.
Pour la carte Cisco350

```
#cardctl ident
product info: "Cisco Systems", "350 Series Wireless LAN
Adapter"
  manfid: 0x015f, 0x000a
  function: 6 (network)
```

Pour la carte Dell Truemobile 1150

```
#cardctl ident
product info: "Dell", "TrueMobile 1150 Series PC Card",
"Version 01.01", ""
  manfid: 0x0156, 0x0002
  function: 6 (network)
```

Le chipset de la carte Cisco est Aironet et le module à charger est le airo_cs.o.
Le chipset de la carte Dell est Hermes et le module à charger est le orinoco_cs.o.

Nous devons ensuite créer une référence correspondant à notre matériel dans le fichier /etc/pcmcia/config et la lier au driver (module Linux).
Les lignes suivantes seront ajoutées pour lier le matériel aux modules :

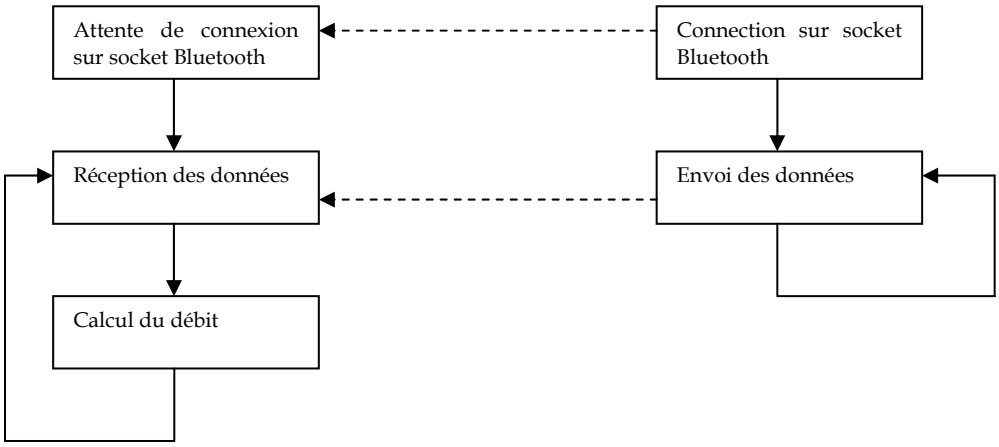
```
card "350 Series Wireless LAN Adapter"
  manfid 0x015f, 0x000a
  bind "airo_cs"

card "Intersil PRISM2 11 Mbps Wireless Adapter"
  manfid 0x0156, 0x0002
  bind "orinoco_cs"
```

Avec cette configuration, les cartes Wi-Fi sont automatiquement reconnues lors de leur insertion dans le port Pcmcia.

2.2 Les performances de Bluetooth

2.2.1 Générateur de traffic Bluetooth

Le programme de test est une application fonctionne suivant le principe client/serveur sur une liaison ACL Bluetooth au moyen du protocole L2CAP.



La transmission des données s'effectue toujours à la capacité maximale du lien.

2.2.2 Génération de trafic entre deux entités Bluetooth

Nous savons que la bande passante théorique maximale est de 1Mbps, mais qu'une liaison asymétrique de type ACL atteint 723.2/57.6 kbit/s. Suivant le type de paquet transportant les données, nous obtenons des performances différentes.
Le trafic est généré en mode client/serveur Bluetooth sur une liaison ACL.

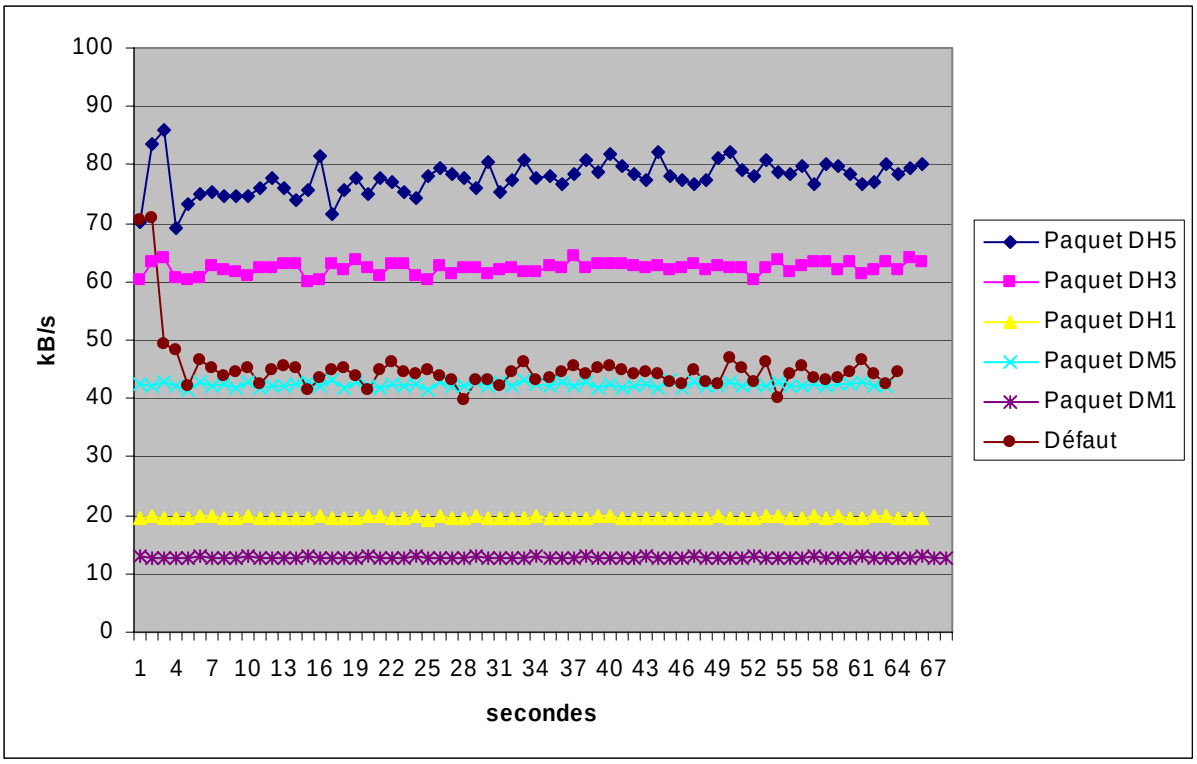
coté serveur :

Montage de l'interface matérielle
#hciconfig hci0 up
Configuration du type de paquet
#hciconfig hci0 ptype <type>
#hciconfig hci0 lm ACCEPT
Lancement de l'application en réception
#l2test –r

coté client :

Montage de l'interface matérielle
#hciconfig hci0 up
Configuration du type de paquet
#hciconfig hci0 ptype <type>
#hciconfig hci0 lm MASTER
Lancement de l'application en émission
#l2test –s 00 :30 :c2 :08 :2f :ff

C'est une liaison ACL qui est utilisée, le type de paquet sera choisi parmi DM1, DM5, DH1, DH3 ou DH5.



On constate que le meilleur débit est obtenu avec un type de paquet dh5 (5 slots sans correction d'erreur).

Les débits théoriques que l'on peut obtenir suivant les types de paquet sont les suivants :

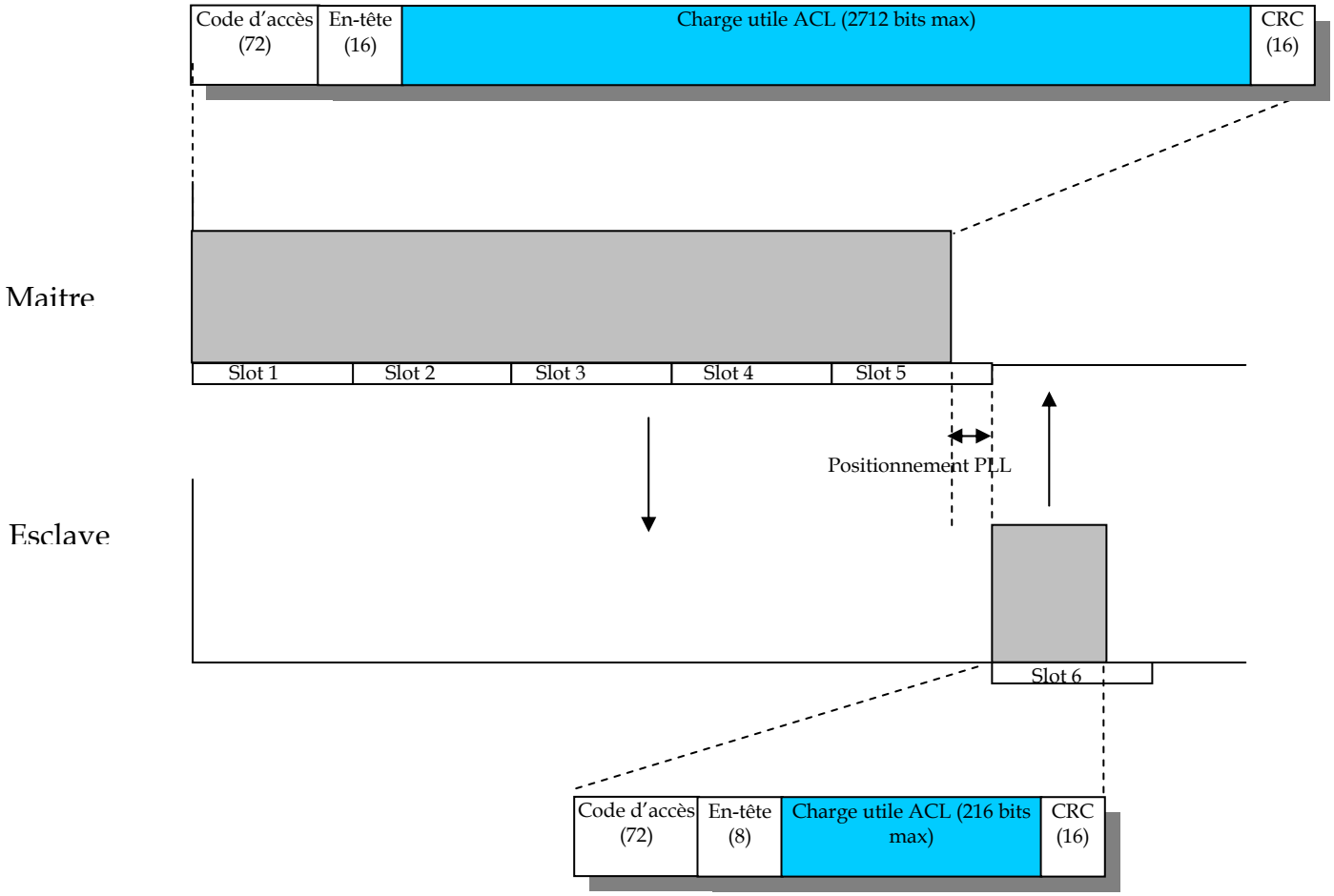
Type de paquet	Bande passante symétrique (kbit/s)	Bande passante asymétrique (kbit/s)	Charge utile (bits)
DH5	433.9	723.2 / 57.6	2712 / 216
DM5	286.7	477.8 / 36.3	1792 / 136
DH3	390.4	585.6 / 86.4	1464 / 216
DM3	258.1	387.2 / 54.4	968 / 136
DH1	172.8	172.8 /172.8	216 /216
DM1	108.8	108.8 / 108.8	136 / 136

Les débits réels sont inférieurs aux théoriques, ce qui se justifie par les pertes sur le lien sans fil : toutes les trames n'arrivent pas a destination correctement ce qui occasionne des retransmissions.

Lorsque aucun type de paquet n'est sélectionné par défaut, on constate qu'au démarrage le débit est proche du maximum, puis chute aux alentours des 40 kbit/s, ce qui correspond au type de paquet DM5. La spécification de Bluetooth 1.1 ne couvre pas cette partie et chaque constructeur est libre d'implémenter un algorithme spécifique de sélection de type de paquet dans son gestionnaire de liaison. Si aucune des deux entités n'a de paquet par défaut, la négociation de type de paquet est effectuée entre les deux entités au travers du Link Manager Protocol (LMP).
Le comportement obtenu, pour le paquet par défaut, est donc spécifique au matériel utilisé et sera probablement différent avec un autre matériel.

La dernière spécification Bluetooth 1.2 est plus claire sur ce point, car elle impose l'utilisation de paquet DM1 à défaut de sélection du type de paquet.

La bande passante théorique :

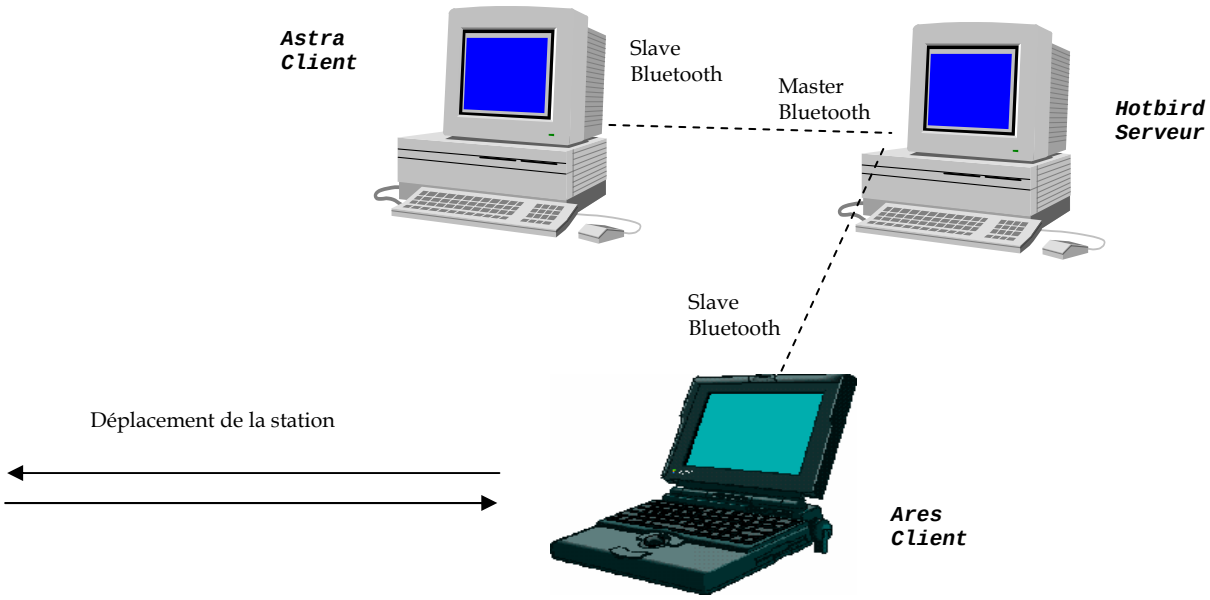


Chaque slot a une durée de 625 µsec (1600sauts par seconde), et à 1 Mbps, on peut donc en théorie avoir 625 bits par slot.
Pour une liaison asymétrique ACL supportant un paquet dh5, on a au maximum 6*625 =3750 bits sur la liaison.
Un paquet dh5 transportant une charge utile de 2712 au maximum, cela nous donne donc 2712/3750 x 1 Mbps = 723.2 kbits/seconde.
Dans le sens de retour, on obtient 216/3750 x 1 Mbps = 57.6kbits/seconde.
216 = charge utile d'un paquet dh1.

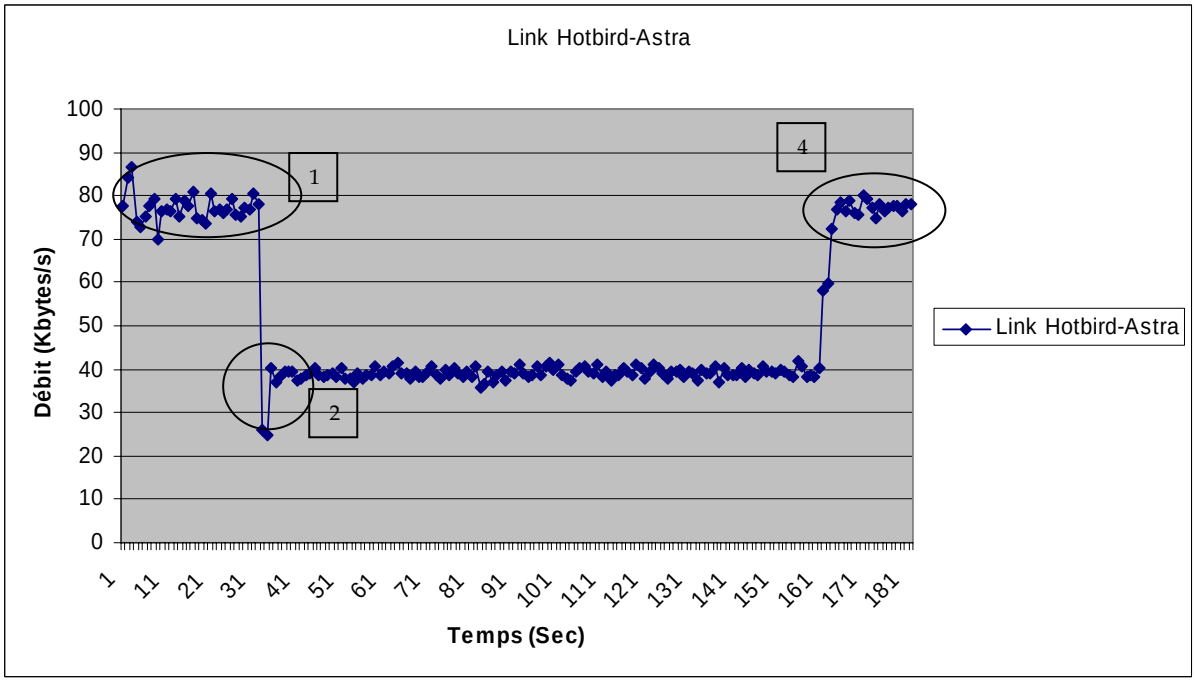
Le temps inutilisé entre la fin du paquet dh5 et la fin du slot temporel 5, sert au niveau radio pour la stabilisation de l'oscillateur lors du saut de fréquence.

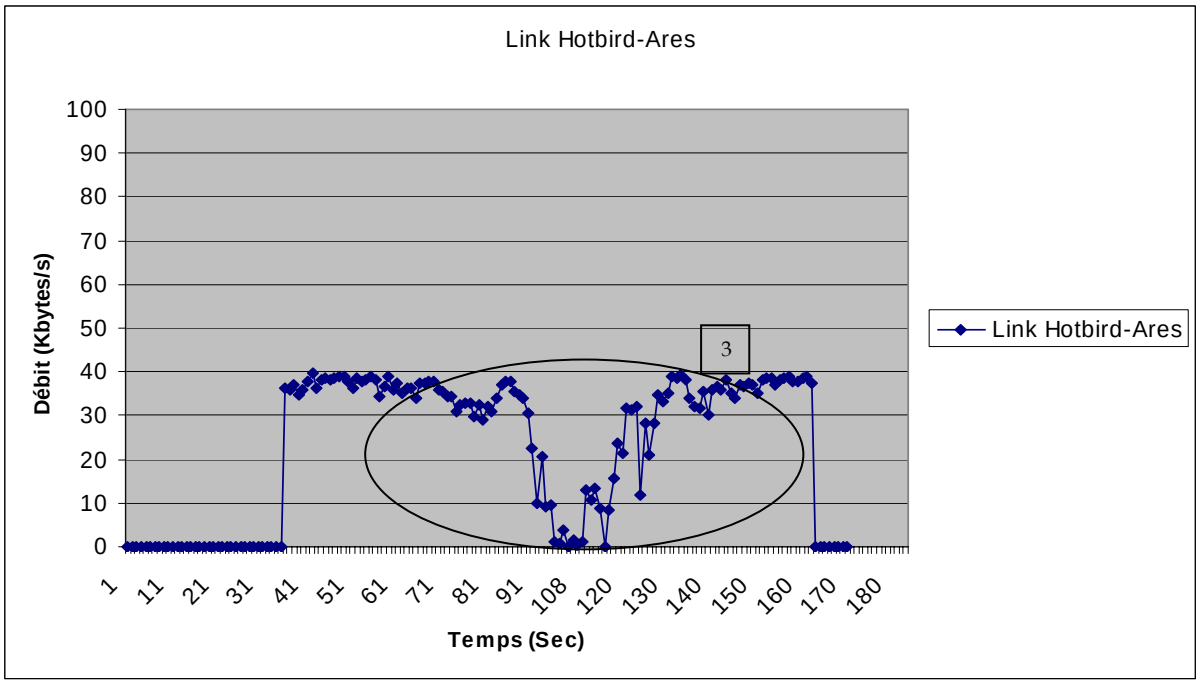
2.2.3 Le partage de la bande passante entre plusieurs entités Bluetooth

Dans la série de mesures suivante, nous nous intéressons à la façon dont le lien est partagé entre diverses stations associées au même maître.
Le type de paquet utilisé est dh5.



Le trafic est dans un premier temps généré entre Hotbird et Astra (section 1 du graphique), dans une seconde phase une autre session client serveur est lancée entre hotbird et Ares (section 2) , ensuite Ares se déplace d'une vingtaine de mètres (à l'intérieur de bureaux cloisonnés) jusqu'à la limite de réception (section 3), puis retourne à son point initial, pour finir la session entre hotbird et Ares est clôturée (section 4).





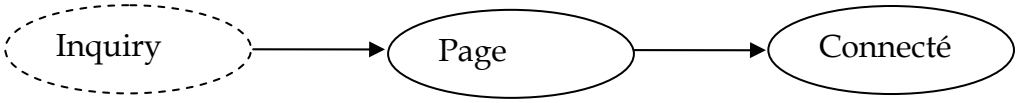
Phase 1 :
Au début de l'échange, un seul lien est actif et nous obtenons un débit conforme à nos précédentes expérimentations pour les paquets dh5.
Phase 2 :
On observe que le trafic est perturbé lors du lancement de la communication entre Hotbird et Astra : ceci est lié à l'établissement de la liaison L2CAP entre les deux entités Bluetooth.
Phase 3 :
La bande passante est équitablement répartie entre les deux esclaves et lorsque le signal se dégrade entre Hotbird et Ares, cela n'influence pas l'autre liaison : c'est le gestionnaire de liaison qui répartit équitablement les slots temporels entre les deux

liens. Lorsqu'un paquet n'est pas arrivé à destination sur un lien, il ne sera pas réémis immédiatement, mais seulement après que le gestionnaire de liaison du maître ait délivré les slots nécessaires à l'autre lien. L'accès au média est administré par le maître du réseau, cela permet d'avoir un comportement plus déterministe sur chaque liaison.

Phase 4 :
Lorsqu'on met fin au lien entre Hotbird et Ares, la bande passante est à nouveau libérée pour l'unique liaison restante entre Hotbird et Astra.

2.2.4 Le temps d'établissement de connexion

Deux entités voulant communiquer doivent au préalable établir une connexion, et suivent donc le processus d'établissement de connexion.



On a dans un premier temps réalisé des connexions successives afin d'obtenir le temps moyen d'établissement de la liaison. Il est à noter que pour passer de l'état de *Page* à *Connected*, il faut au préalable que l'adresse Bluetooth du partenaire destination soit connue.

Le temps d'établissement de la connexion, lorsque l'adresse destination est connue, varie entre 1 seconde et .43 s, la moyenne s'établit à 0.51 secondes.

Dans le cas ou l'adresse du destinataire n'est pas connue, selon la norme la procédure de connexion peut durer jusqu'à 12.5s. J'ai mesuré des temps proche de cette valeur.

Les temps d'établissement de connexion interdisent l'utilisation de Bluetooth pour certaines applications : une clé de voiture Bluetooth n'est pas concevable pour des raisons d'ergonomie.

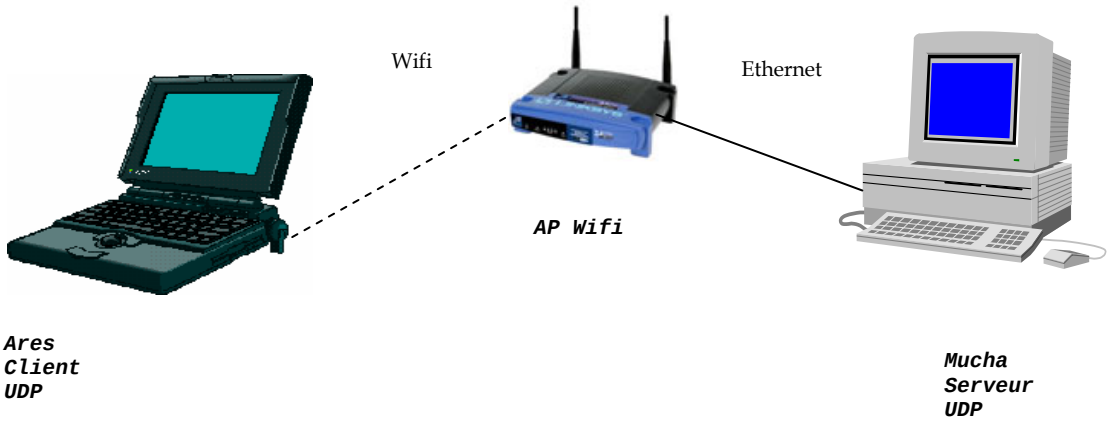
2.3 Les performances de Wi-Fi

2.3.1 Générateur de traffic pour Wi-Fi

L'analyse de performances de Wi-Fi a été effectuée à l'aide de Iperf qui un outil de génération de trafic. Le critère principal qui a guidé le choix de cet outil est sa disponibilité sous Linux et Windows, ce qui a permis de contourner certaines difficultés liées à la prise en charge du matériel sous Linux à certains moments.

2.3.2 Génération de trafic entre un client Wi-Fi et un AP Wi-Fi

Le but de cette mesure est de vérifier la bande passante sur un réseau Wi-Fi en fonction des conditions de réception.

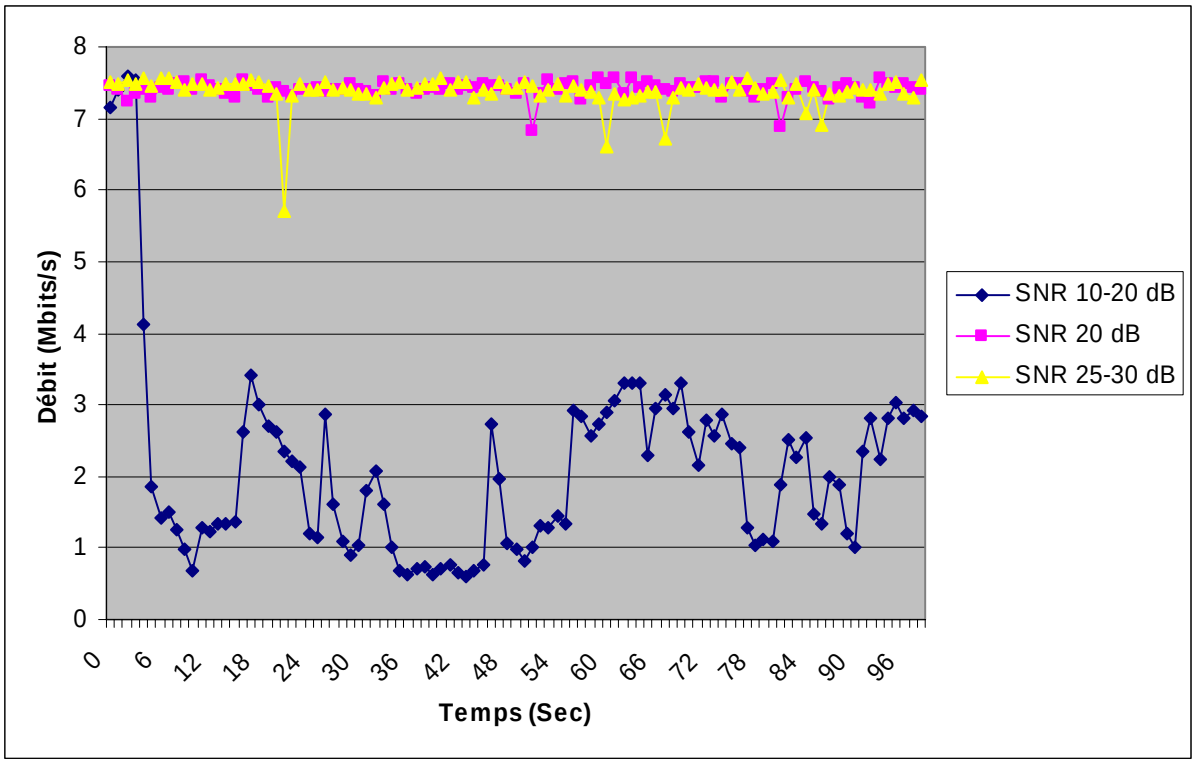


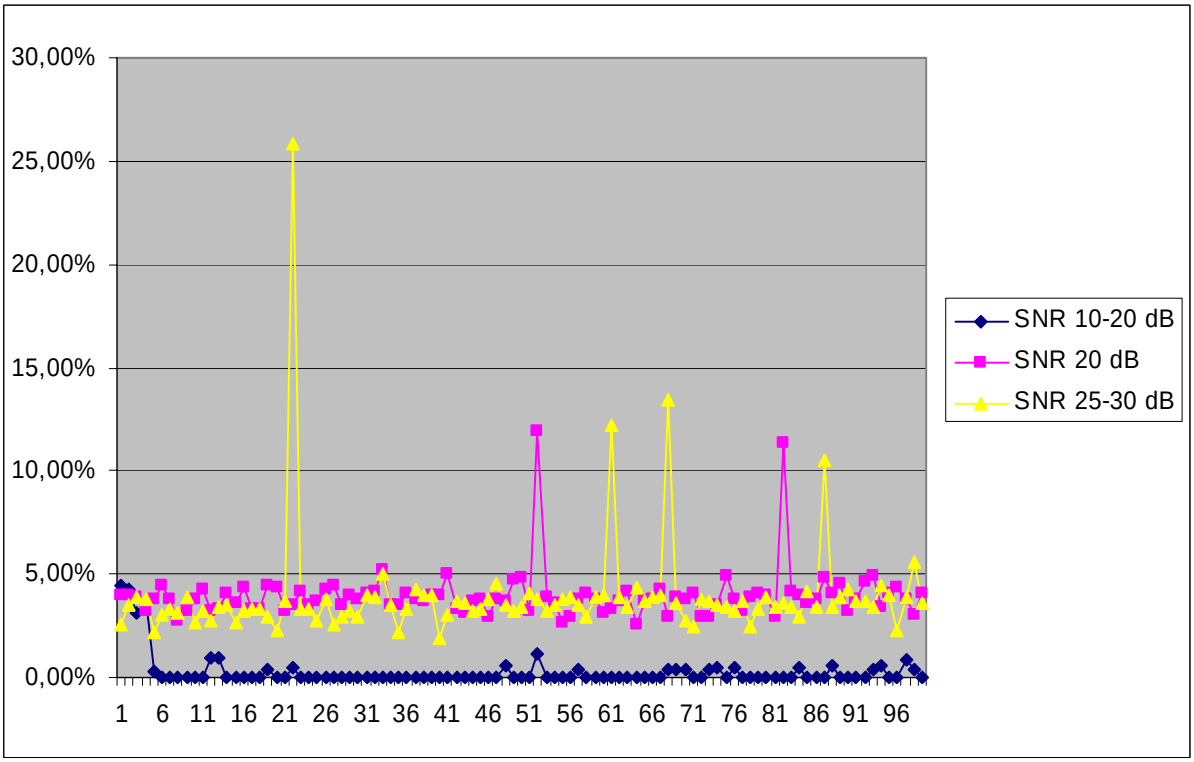
Le trafic est généré en mode client/serveur entre un client Wi-Fi (Ares) et une station (Mucha) reliée sur le réseau Ethernet. Le client est associé au réseau Wi-Fi en mode infrastructure, au travers un réseau local Ethernet.

Les mesures ont été effectuées en mode sans connexion (trafic UDP).

Il y a trois séries de mesures :

- une série pour laquelle les conditions de réception sont mauvaises : 10 à 20 dB de SNR,
- - une série pour laquelle nous obtenons le meilleur signal entre le client Wifi et le point d'accès : 25 à 30 dB de SNR,
- une série pour un signal intermédiaire : 20 dB de SNR.

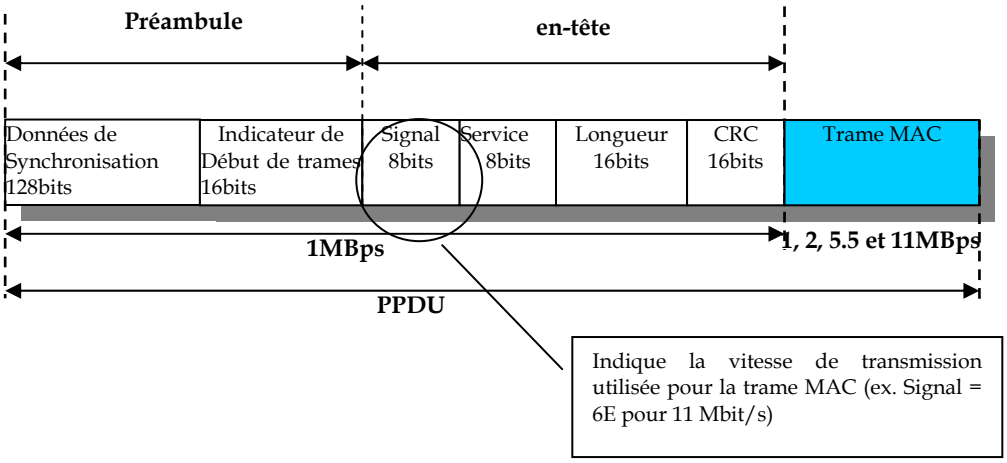




On constate que le taux d'erreur augmente avec la qualité du rapport signal sur bruit (SNR) et que dans le même temps le débit progresse. En réalité, le débit est contrôlé par le point d'accès en fonction de la qualité du signal : c'est le mécanisme de DRS (Dynamic Rate shifting) qui est mis en œuvre.
Au démarrage d'une communication, le débit est réglé au maximum (11 Mbits/s), et par la suite en fonction de la qualité du signal, la vitesse de communication est

automatiquement ajustée au niveau physique. De par cette fonction, une station arrive à conserver sa liaison sur une plus grande distance : les modulations utilisées pour les faibles vitesse favorisent la zone de portée radio.

Ce mécanisme n'est pas normalisé et fait appel à des techniques propriétaires que chaque constructeur peut implémenter au niveau de la couche physique. L'indication du débit de la trame à venir étant indiqué dans l'entête de chaque trame physique (cet entête étant lui-même émis à la vitesse de 1 Mbits/s).



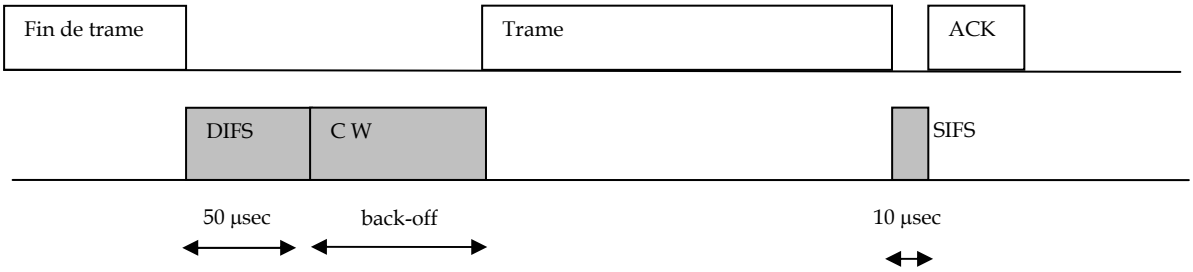
2.3.3 la bande passante réelle

Lors des expérimentations on atteint dans le meilleur des cas un débit de 7 Mbits/s, alors que les performances théoriques annoncées sont de 11 Mbits/s pour le 802.11b. En réalité les 11 Mbits/s annoncés à titre commercial correspondent à la bande passante maximale disponible au niveau physique. Comme nous allons le voir ci-dessous, la charge protocolaire des différentes couches consomme une partie de la bande passante mise à disposition en bande de base.

Nous devons considérer la technique d'accès au média CSMA/CA qui pour minimiser les collisions, utilise plusieurs mécanismes, tels que :

- l'écoute du support pendant une durée minimale pour vérifier que celui-ci est disponible,
- l'algorithme de back-off pour gérer au mieux l'accès concurrentiel au média,
- l'acquittement systématique des trames qui permet de s'assurer que la trame est bien arrivé à destination.

Si on décompose une séquence de transmission complète comprenant la trame utile et l'overhead protocolaire, nous pouvons démontrer le résultat obtenu en pratique.

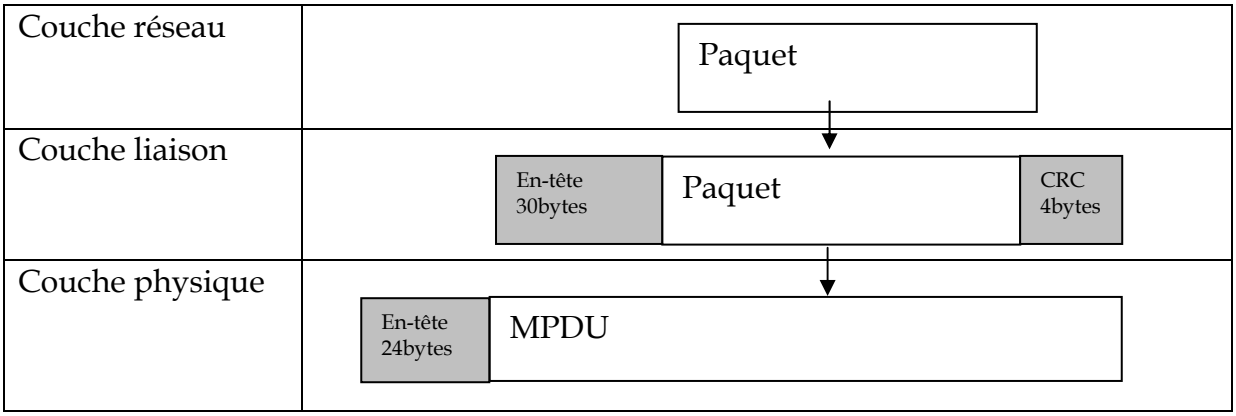


Timers inter trames :
Les valeurs des compteurs inter trames correspondantes à notre configuration (Accès au média en DCF et couche physique DSSS) sont les suivants :

	Durée (µsec)
timeslot	20
SIFS	10
DIFS	50

Fenêtre de contention :
La durée de la fenêtre de contention est calculée suivant le temporisateur
T = Random (0,CW) x timeslot
Lors du premier tirage la fenêtre de contention est comprise entre 0 et 31. La valeur moyenne sera donc de 31/2 x 20 µsec = 310 µsec

Durée de la trame utile :



Au niveau de la couche physique, il existe 2 types d'en-tête, un entête court et un entête normal. L'entête normal est compatible avec les anciennes versions, tandis que l'entête court est plus efficace.

Comme nous l'avons vu lors de l'étude de la technologie Wi-Fi, en mode normal, l'entête est transmis à 1 Mbit/s, le reste de la trame est ensuite transmise à 1, 2, 5.5 ou 11 Mbit/s

L'entête physique dure donc 192 µsec (24 octets transmis à 1 Mbit/s).

L'overhead MAC de 34 octets est transmis à la vitesse de transmission sélectionnée.

	1 Mbit/s	2 Mbit/s	5.5 Mbit/s	11 Mbit/s
Entête physique	192 µsec	192 µsec	192 µsec	192 µsec
overhead MAC	272 µsec	136 µsec	49.45 µsec	24.73 µsec
Paquet 1500 octets	12000 µsec	6000 µsec	2182 µsec	1091 µsec
Total	12464 µsec	6328 µsec	2423 µsec	1308 µsec

Durée de la trame ACK :
La trame d'acquittement ACK est une trame de contrôle de niveau MAC de 14 octets et comprends en plus un entête physique de 192 µsec.
En fonction de la vitesse de communication nous aurons :

	1 Mbit/s	2 Mbit/s	5.5 Mbit/s	11 Mbit/s
Entête physique	192 µsec	192 µsec	192 µsec	192 µsec
ACK (14 octets)	112 µsec	56 µsec	20.36 µsec	10.18 µsec
Total	304 µsec	248 µsec	212 µsec	202 µsec

La bande passante réelle :

Nous pouvons à présent calculer le débit maximal atteignable en fonction du débit nominal sélectionné :

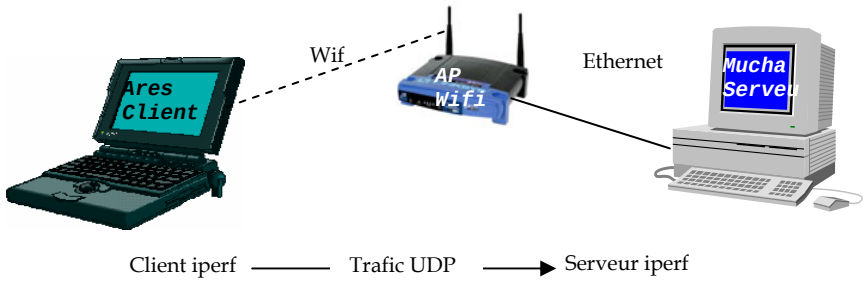
	1 Mbit/s	2 Mbit/s	5.5 Mbit/s	11 Mbit/s
DIFS	50 µsec	50 µsec	50 µsec	50 µsec
Back-off	310 µsec	310 µsec	310 µsec	310 µsec
Trame datas (1500 octets)	12464 µsec	6328 µsec	2423 µsec	1308 µsec
SIFS	10 µsec	10 µsec	10 µsec	10 µsec
Trame ACK	304 µsec	248 µsec	212 µsec	202 µsec
Durée Totale	13138 µsec	6946 µsec	3005 µsec	1880 µsec
Capacité en bits sur la durée	13138 bits	13892 bits	16528	20680
Efficacité	91.34%	86,38%	72,61%	58,03%
Débit maximal	0,91 Mbit/s	1,73 Mbit/s	3,99 Mbit/s	6.38 Mbit/s

De la même manière, nous pouvons démontrer qu'en utilisant l'en-tête court, l'efficacité du canal à 11 Mbits/s passera à 64.63% et le débit maximal réellement atteignable pourra aller jusqu'à 7.11 Mbits/s.

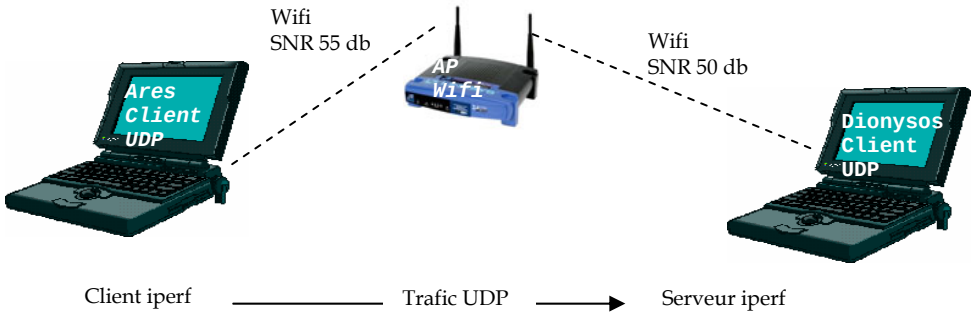
2.3.4 Les problèmes de débits lors du partage du lien radio

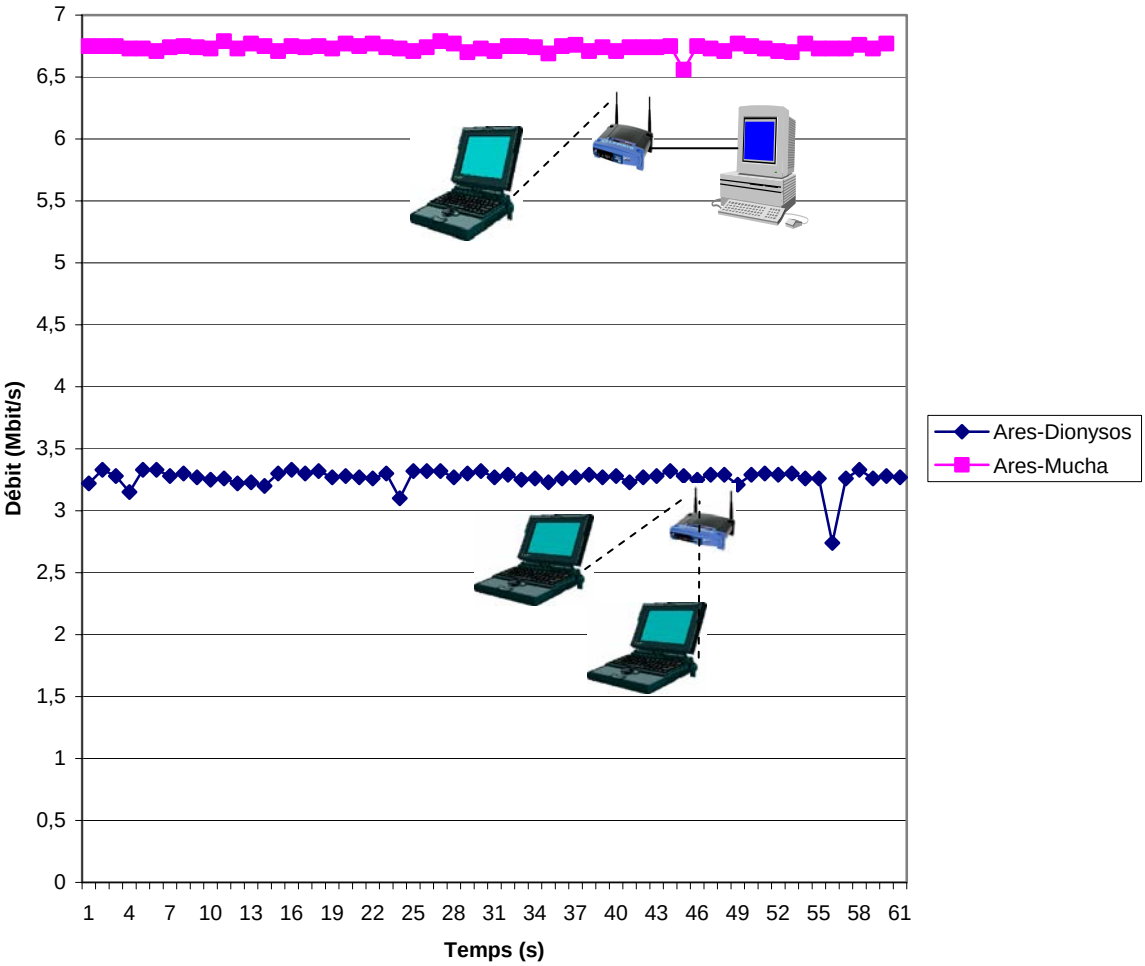
Lors de nos expériences, nous avons mis en évidence le fait que lorsque plusieurs stations joignent un même point d'accès, le partage de la bande passante ne s'effectue pas de la même manière que sur un réseau filaire et dans certaines configurations les mécanismes utilisés par Wi-Fi peuvent révéler des propriétés fort surprenantes à priori.

L'utilisation de la bande passante dans un même sous réseau :
Dans un premier temps nous générons notre trafic avec une seule station cliente et de bonnes conditions sur le lien radio entre l'AP et la station.
Le SNR sur le lien entre Ares et le Point d'accès est de 55 dans ce cas.



Dans un second temps nous générons notre trafic avec deux stations clientes et de bonnes conditions sur le lien radio entre l'AP et les stations.
Le SNR sur le lien entre Ares et le Point d'accès est toujours de 55 et de 50 entre Dionysos et le Point d'accès.



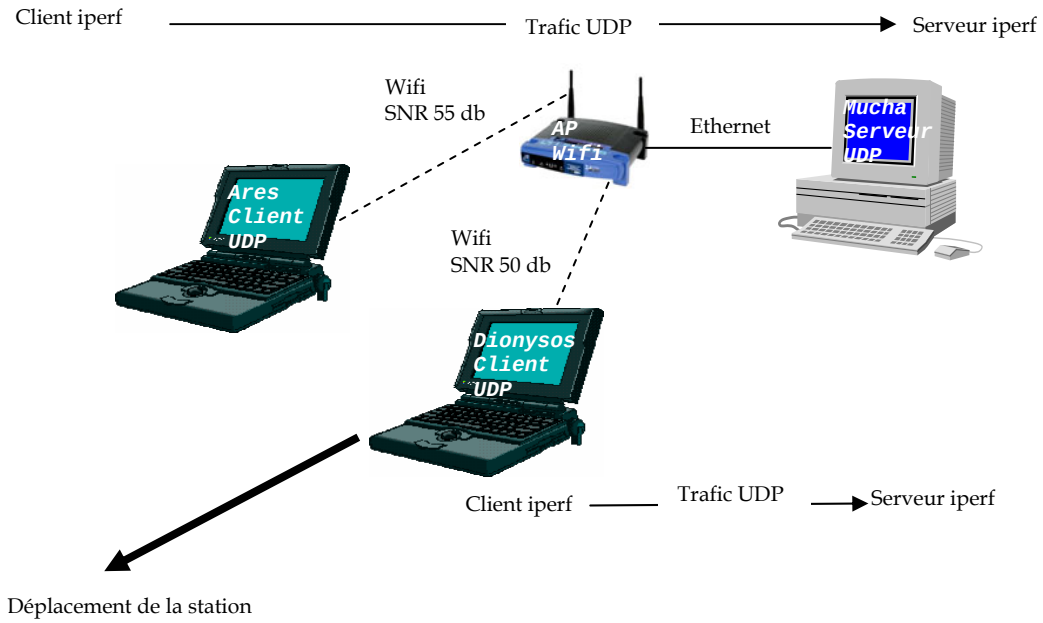


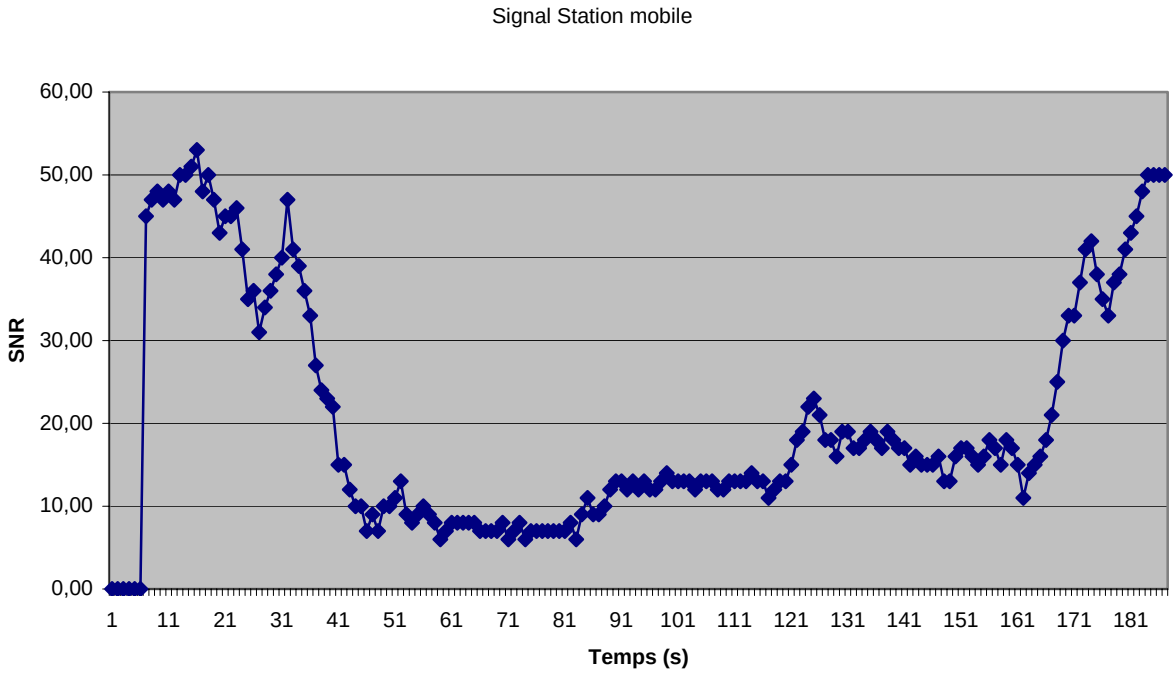
Lorsque une seule station est associée au point d'accès, elle utilise toute la bande passante disponible et s'approche du débit réel possible, c'est-à-dire entre 6 et 7 Mbit/s. Dans le cas ou deux stations associées au même point d'accès communiquent ensemble, nous constatons que le débit est dans ce cas divisé par deux, en effet dans ce cas le support radio est utilisé deux fois pour chaque échange de trame.
Contrairement à un lien filaire ou les trames circulant sur le support sont interceptées par toutes les stations d'un même sous réseau au niveau physique puis filtrées par la couche MAC avant d'êtres délivrées aux couches supérieures, sur un réseau 802.11 en mode infrastructure les trames sont toutes délivrées au point d'accès, qui les relaye ensuite vers la station destination même si ces deux stations sont à portée radio l'une de l'autre.
On peut justifier ce mode de fonctionnement, par le fait que toutes les stations associées à un même point d'accès ne sont pas forcément à portée les unes des autres. La norme n'a pas prévu d'optimisation d'utilisation de la bande passante dans le cas de figure que nous venons de mettre en évidence et il apparaît plus judicieux d'utiliser le mode ad hoc, dans le cas d'un transfert entre deux stations à portée radio l'une de l'autre.

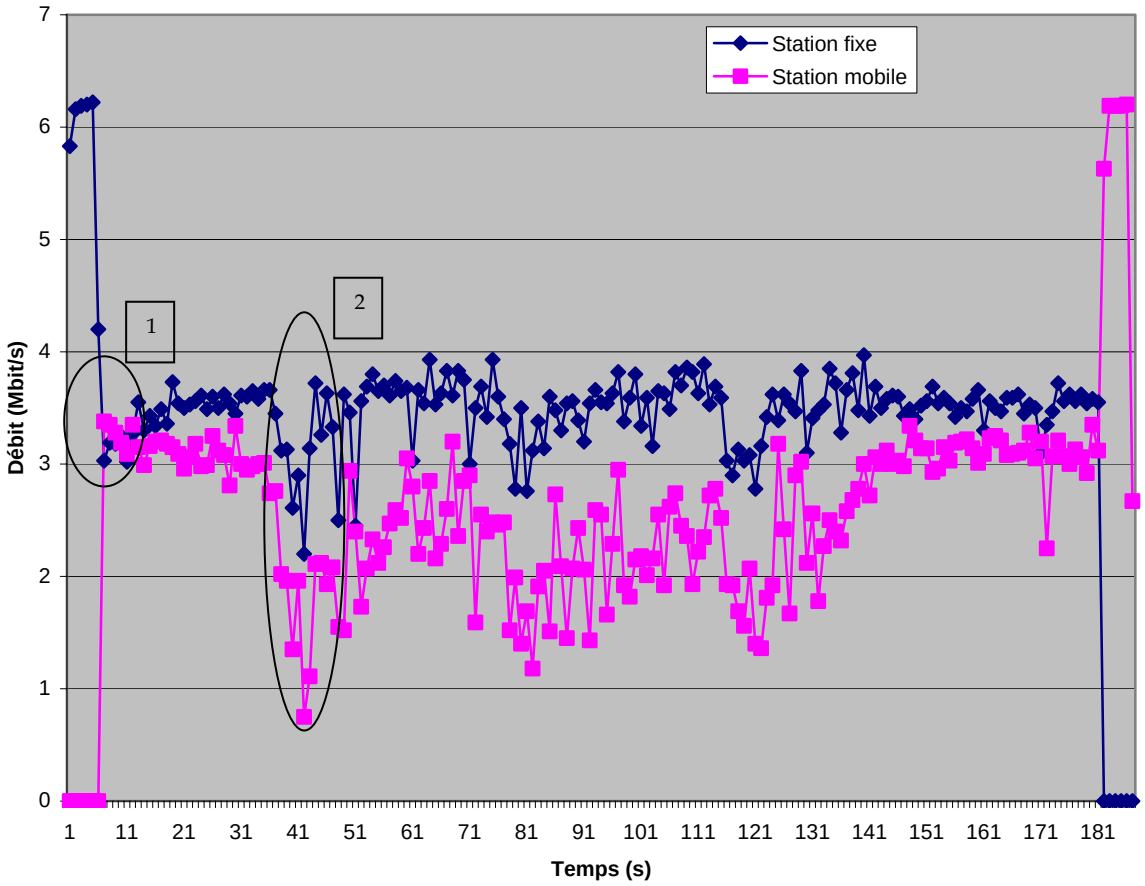
<u>La chute de performances due à une station éloignée :</u>
Nous générons à présent du trafic :

- entre deux stations fixes (Ares → Mucha),
- entre une station fixe (Mucha) et une station mobile que nous allons éloigner du point d'accès (Dionysos).

Le SNR sur le lien entre Ares et le Point d'accès est de 55.
Le SNR sur le lien entre Dionysos et le Point d'accès sera enregistré pendant l'essai.







On observe que dès le début de l'arrivée de la station mobile, la bande passante est équitablement répartie (voir transition en 1) entre les deux liaisons. Lorsqu'on s'est éloigné suffisamment pour atteindre un niveau de signal à la limite de la perte de liaison, la station mobile a descendu son débit à 1 voir 2 Mbit/s (voir transition en 2) ce qui correspond à la mise en œuvre du DRS (Dynamic Rate Shifting) entre cette station et le point d'accès.
Plus surprenant, lorsque le débit de la station mobile chute, le débit de la station fixe est également affecté alors que son rapport signal sur bruit reste inchangé.
Cette situation est liée à la méthode d'accès égalitaire au support conjugué à la possibilité d'avoir plusieurs stations communiquant à des vitesses différentes.
Dans le pire cas avec nos deux stations, nous avons Ares qui communique à 11Mbps et Dionysos à 1Mbps. Supposons qu'ils accèdent à tour de rôle au médium (hypothèse d'accès équitable garanti par DCF) et qu'ils transmettent chacun 1500 octets de données au niveau MAC soit un MPDU de 1534 octets. A partir de ces hypothèses, nous allons estimer la bande passante totale dont les deux utilisateurs peuvent espérer disposer en théorie.

- Calcul du temps nécessaire au premier hôte émettant à un débit de 11MBps pour transmettre une trame de 1500 octets de données MAC et recevoir

l'accusé de réception correspondant (les durées des temporisateurs DIFS et SIFS sont incluses et l'algorithme de back-off est omis),

- Calcul du temps nécessaire au deuxième hôte émettant à un débit de 1MBps pour transmettre une trame de 1500 octets de données MAC et recevoir l'accusé de réception correspondant (les durées des temporisateurs DIFS et SIFS sont incluses et l'algorithme de back-off est omis),
- Calcul de la bande passante utile au niveau MAC disponible par utilisateur.

Le schéma suivant illustre le calcul; l'algorithme de back-off n'apparaît pas dans ce schéma conformément aux restrictions que nous nous sommes fixées précédemment :

- Trame à 1Mbps = Entête Phy + MAC +SIFS+DIFS+ACK = 12.808 ms
- Trame à 11Mbps = Entête Phy + MAC +SIFS+DIFS+ACK = 1651 ms

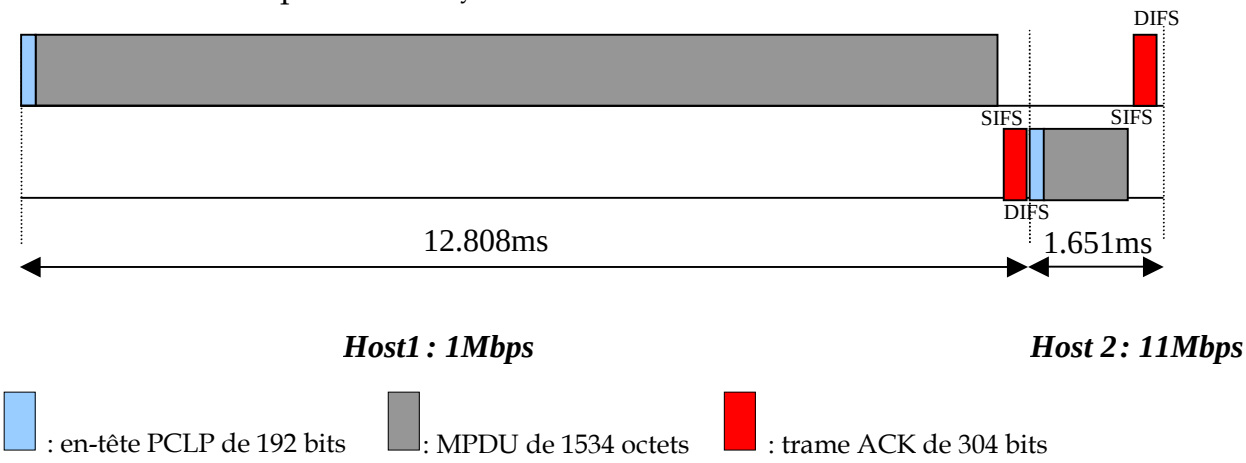


Figure : Bande passante théorique partagée entre deux utilisateurs (1 et 11MBps)

Phy 192 ACK 304
Phy + MAC +SIFS+DIFS+ACK =192+12272+10+50+304 à 1 Mbit/s
Phy + MAC +SIFS+DIFS+ACK =192+1116+10+50+304 à 11 Mbit/s

Le partage entre deux hôtes, l'un transmettant à 1MBps et l'autre à 11MBps, résulte théoriquement en un débit utile disponible au niveau MAC entre chaque utilisateur de :

Débit par utilisateur = TailleMPDU / (H1_Ttransmission + H2_Ttransmission)

Soit un débit de 0.848MBps par utilisateur pour transmettre 1534 octets de données au niveau MAC chacun, d'où une bande passante totale partagée de 1.7MBps.

Les résultats théoriques confirment l'ordre de grandeur obtenu lors de la campagne de mesure effectuée à l'aide du générateur de trafic.

L'utilisation des réseaux sans fil facilite les déplacements de l'utilisateur mais cela ne va pas sans contrepartie. En effet, si le taux d'erreur sur un réseau filaire est de …. on peut considérer sa répartition aléatoirement distribuée. Dans le cas d'un réseau sans fil, le taux d'erreur est plus important (….valeur …) et les erreurs augmentent plus les stations sont éloignées. Nous avons vu que la vitesse de communication dans un réseau Wi-Fi était asservie au taux d'erreur par le mécanisme DRS.

L'utilisation de plusieurs vitesses de communication sur un même canal radio, semble attrayante à priori, mais révèle des propriétés fort surprenantes car un utilisateur idéalement placé vis-à-vis du point d'accès et profitant d'excellentes qualités de réception, peut soudainement voir sa communication dégradée par la simple présence d'une station en limite de réception sur le même point d'accès.

2.3.5 Le temps d'établissement de connexion

Nous sommes en situation de mobilité et nous savons que les liens de communication vont évoluer au cours du déplacement des véhicules. Wi-Fi supporte une perte de liaison et prévoit une procédure de ré association. Cette procédure fait appel à trois phases Scanning, Authentification, association et le temps requis pour passer ces étapes peut avoir une influence sur la communication, en particulier sur les temps de latence qui sont un paramètre important pour les applications multimédia.

Dans [MSA2003], on peut remarquer que dans le cas d'une procédure de dé-association – ré-association, la durée d'une telle opération varie entre 40 et 500 msec. Il est à noter que ces essais ont été effectués sur un réseau ou la couverture est totale (cellules Wi-Fi jointes) ce qui est non négligeable et ne sera probablement pas le cas d'un réseau inter-véhicules basé sur Wi-Fi.
Il est à noter que le durée de la procédure est presque totalement liée à la durée du *Probe Request* sur tous les canaux.

2.4 Interopérabilité Wi-Fi-Bluetooth

2.4.1 Introduction

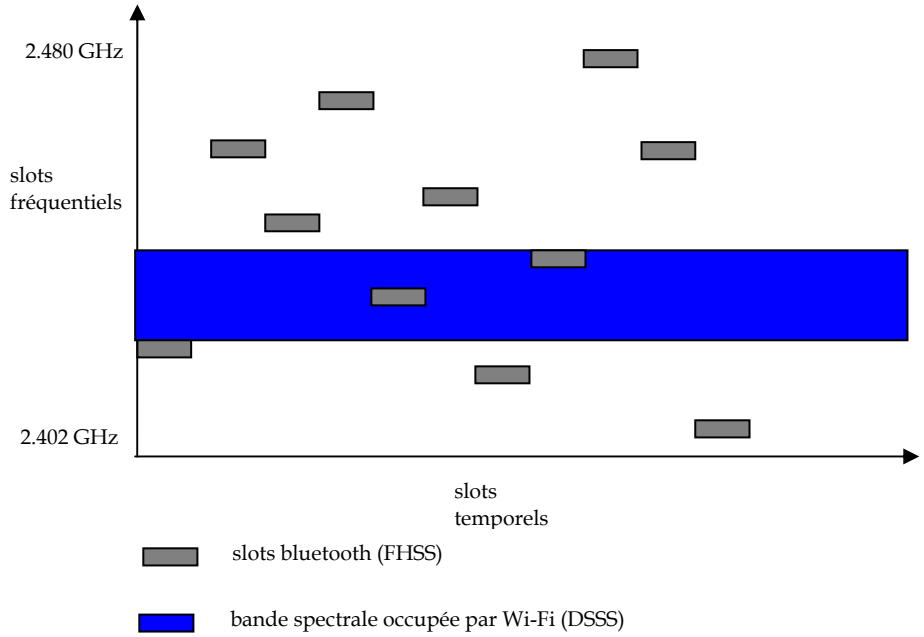
Comme les technologies sans fil Wi-Fi et Bluetooth partagent le même espace spectral et évoluent à proximité l'une de l'autre, les risques de collision sont fort préoccupants. Malgré une résistance naturelle aux autres dispositifs sans fil grâce à leur propriété d'étalement du spectre, Wi-Fi et Bluetooth déçoivent en présence de parasites (préciser). En fait, bien que les protocoles de communication soient très robustes et accompagnés de techniques de vérification et de correction d'erreurs (CRC, FEC), il reste néanmoins que les paquets corrompus doivent être réexpédiés. Par conséquent, les niveaux croissants de parasites provoquent un ralentissement du débit. Ce n'est que dans des conditions extrêmes, comme l'utilisation d'un téléphone cellulaire

Bluetooth à proximité d'un four à micro-ondes en fonction, que les communications risquent d'être entièrement interrompues.

2.4.2 Le partage du canal radio

Comme nous envisageons l'utilisation conjointe des technologies Wi-Fi et Bluetooth, nous devons prendre en compte le fait que celles-ci utilisent la même bande de fréquence et donc qu'elles auront à accéder au média de manière concurrentielle.
Dans un premier temps ces technologies ont été développées de manière indépendante et aucun mécanisme de collaboration n'a été prévu pour partager la bande de fréquence.

Wi-Fi et Bluetooth occupent toutes deux une portion de la bande de fréquence ISM de 2,4 GHz, d'une largeur de 83 MHz. La technologie Bluetooth, utilisant le système à spectre étalé à saut de fréquence (FHSS), est autorisée à alterner entre 79 sous canaux différents de 1 MHz.
La technologie Wi-Fi fait appel au système à spectre étalé avec séquences continues (DSSS) plutôt qu'au système FHSS. La fréquence ne change pas et reste centrée à l'intérieur d'une bande passante d'une largeur de 22 MHz. Bien que l'espace soit suffisant pour recevoir 11 canaux synchronisés dans cette bande de 83 MHz, seuls trois canaux non synchronisés peuvent y évoluer. Par conséquent, pas plus de trois réseaux Wi-Fi différents peuvent être exploités à proximité l'un de l'autre.
Lorsque des fréquences radio Bluetooth et Wi-Fi circulent sur la même bande, le seul canal Wi-Fi de 22 MHz occupe le même intervalle de fréquences que 22 des 79 sous canaux Bluetooth de 1 MHz. Lorsque Bluetooth émet sur un intervalle de fréquences qu'occupe simultanément une transmission Wi-Fi, des parasites peuvent se créer selon la puissance du signal.



Lorsqu'un dispositif Bluetooth se bute à des parasites sur une fréquence donnée, il « saute » à la fréquence suivante et transmet de nouveau. De cette façon, il parvient à éviter les brouillages que cause un réseau Wi-Fi. Dans le cas de transmissions de données ACL (Asynchronous Connection-Less), il se produit une diminution du débit. Toutefois, dans le cas de liaisons SCO (Synchronous Connection Oriented) téléphoniques, les paquets risquent de se perdre car ces liaisons n'utilisent pas le système à demande de répétition automatique (ARQ). La conséquence directe est une diminution de débits et des temps de latence plus élevés pour les liaisons ACL, et une diminution de qualité audio pour les paquets SCO.

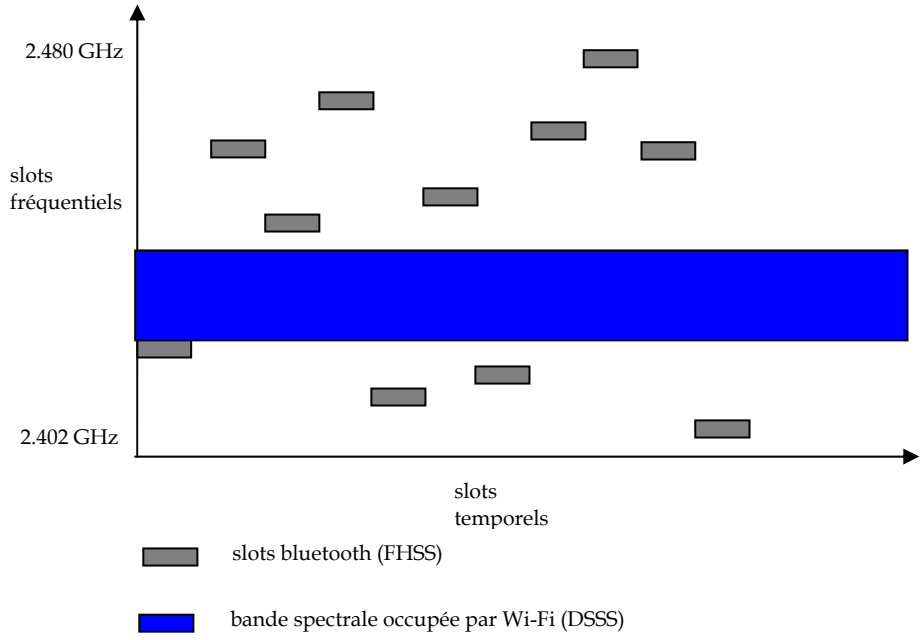
Avec la technologie Wi-Fi, si une transmission échoue (absence d'acquittement de trame), on présume que le problème a été causé par deux stations tentant d'émettre simultanément, et le système ARQ entre en action. De plus, comme nous l'avons vu précédemment, la fonction de modification automatique du débit peut se mettre en action si les collisions sont fréquentes. Cette caractéristique permet au débit de transmission de passer de 11 Mo/s à 5,5, à 2 ou même à 1 Mo/s, dans le but de réduire le taux d'erreur que provoque un piètre rapport SNR (Signal-to-Noise Ratio).

Si un dispositif Wi-Fi se bute aux parasites d'une transmission Bluetooth, il devra dans un premier temps émettre à nouveau les données et ralentira ensuite son débit (mécanisme DRS), ce qui aura pour conséquence de rallonger son temps de transmission et donc d'augmenter l'occurrence des collisions. Le mécanisme DRS qui en théorie améliore les conditions de transmission peut avoir dans ce type de situation l'effet inverse.

Des travaux on été menés par le groupe IEEE 802.15, afin de définir des mécanismes pour faciliter la coexistence avec Wi-Fi.

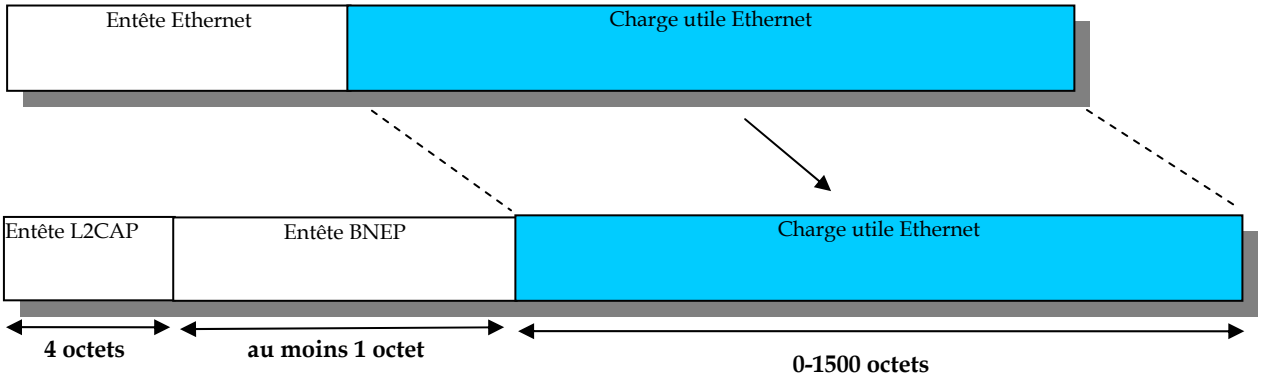
Des techniques de collaboration :
Une coexistence en collaboration s'applique à un environnement où le réseau Bluetooth et le réseau Wi-Fi communiquent et collaborent afin de minimiser les collisions. La technique TDMA (accès multiple par répartition temporelle) a été envisagée pour permettre à Wi-Fi et à Bluetooth d'alterner les transmissions, malheureusement ce type de technique est inapplicable pour les liaison de type SCO d'une part et ne s'appliquent que dans une seule et même machine.

Des techniques de Non-collaboration :
Une coexistence sans collaboration s'applique à un environnement dépourvu de méthode de communication entre les réseaux Bluetooth et Wi-Fi. La sélection et répartition des paquets est une caractéristique MAC (Media Access Control) de Bluetooth destinée à enregistrer des statistiques relatives à l'utilisation des fréquences sur des canaux victimes de parasites. Ces statistiques sont ensuite soumises à des algorithmes de répartition permettant de relancer les transmissions lorsqu'une fréquence adéquate est repérée. Le saut de fréquence classe les canaux et modifie la séquence des sauts de fréquence afin d'éviter les canaux présentant le plus de parasites. Cette technique est nommée AFH (Adaptative Fréquency Hopping) et a été intégrée à la dernière norme bluetooth version 1.2 ratifiée en juin 2003.

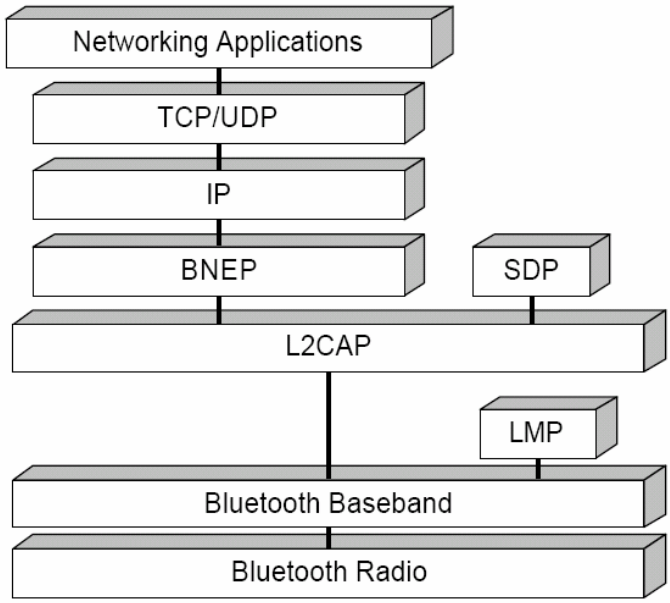


2.4.3 Intégration de bluetooth et Wi-Fi

La cohabitation entre Wifi et Bluetooth au niveau physique est donc possible, il faut maintenant arriver à intégrer ces deux technologies dans un même réseau.
On ne peut pas intégrer un piconet Bluetooth dans un réseau de la famille 802 aussi facilement que nous avons pu le faire dans le cas des réseaux 802.11 et 802.3.
La pile de protocole Bluetooth ne permet pas le transport de paquets IP sans couche d'adaptation (Middleware). Ce type de configuration est décrit par la spécification du profil PAN (*Personal Area Networking*).
Le profil PAN est une couche d'émulation Ethernet pour Bluetooth au travers du protocole BNEP (*Bluetooth Network Encapsulation Protocol*). Les paquets Ethernet sont encapsulés dans le paquet L2CAP en utilisant le protocole BNEP.



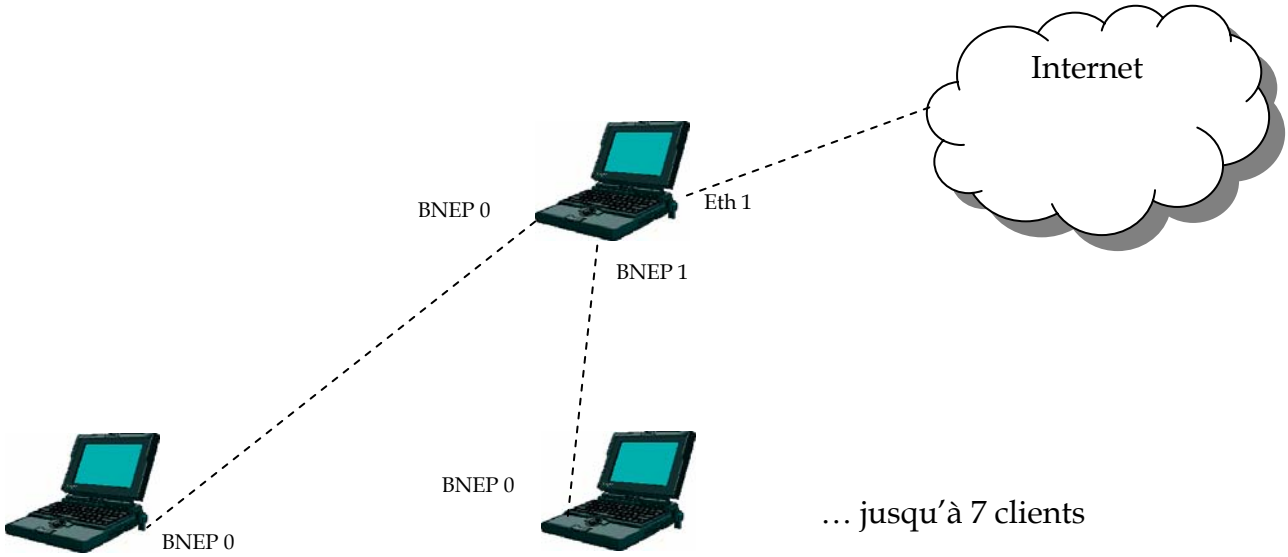
La pile de protocole est constituée de la manière suivante :



Ce profil permet à des terminaux Bluetooth :
- de faire fonctionner des applications TCP/IP,
- de communiquer d'esclave à esclave,
- de fonctionner en pont de niveau 2

Un exemple d'utilisation est la mise en place d'une passerelle Internet au travers d'une machine munie d'une interface Bluetooth d'une part et d'une interface Wi-Fi d'autre part.

Ares (@00 :30 :c2 :08 :33 :37) Machine connectée à Internet par eth1, disposant d'une interface Bluetooth	Hotbird Machine munie d'une interface Bluetooth
Chargement du module bnep.o #modprobe bnep	Chargement du module bnep.o #modprobe bnep
Montage de l'interface matérielle #hciconfig hci0 up	Montage de l'interface matérielle #hciconfig hci0 up
Lancement du serveur en mode NAP (Network Acces Point) #pand - - listen - - role NAP	
	Lancement du client en utilisateur du réseau PAN #pand - - connect - - 00:30:c2:08:33:37
L'interface BNEP0 est crée sur Ares par le système	L'interface BNEP0 est crée sur Hotbird par le système
Attribution d'une adresse IP statique pour l'interface #ifconfig bnep0 10.0.0.1	Attribution d'une adresse IP statique pour l'interface #ifconfig bnep0 10.0.0.1
Configuration de Netfilter pour transférer les paquets provenant de l'interface Bluetooth vers l'interface Wi-Fi #iptables –F FORWARD #iptables –A FORWARD –j ACCEPT #iptables –A POSTROUTING –t nat –o eth1 –j MASQUERADE	
	Ajout de la Route par defaut sur lien Bluetooth #route add default gw 10.0.0.1



Les tests de performances effectués sur Bluetooth à l'aide de iperf en UDP sur cette configuration, donnent des résultats proches de ceux obtenus initialement, ceci est logique car la surcharge protocolaire est peu importante.

2.5 Synthèse

Dans les deux derniers chapitres, nous avons étudié en détail Bluetooth et Wi-Fi, et constaté que bien qu'utilisant la même bande de fréquence, ces deux technologies ont des caractéristiques très différentes et n'ont pas, à l'origine, été conçues pour fonctionner ensembles.

Robustesse :
Bluetooth est plus robuste et les performances restent proches des spécifications, le partage du lien est équitable par le mécanisme de distribution des slots temporels par le maître du réseau. Son rayon d'action est faible et sa pile de protocole n'est pas prévue pour fonctionner sur des réseaux de grande taille ; le principe Maître /Esclave ne permet pas une communication entre deux esclaves. Le temps d'établissement d'un lien peut être très long lors du passage de l'état de *Standby* à *Conneted* en passant par les phases *Inquiry* et *Page*.
Dans des conditions de communications dégradées, une station Wi-Fi a la faculté de conserver le lien par l'utilisation du DRS, mais cela modifie les performances de toutes les stations utilisant le même support de part l'accès équitable au support par l'utilisation de la méthode DCF.

Nous avons également vu que Bluetooth et Wi-Fi peuvent fonctionner dans une zone rapprochée l'un de l'autre, malgré l'utilisation d'une bande de fréquence commune. Le mécanisme AFH permettra de contourner les interférences possibles au niveau du support radio, dès que la norme 1.2 commencera à être intégrée dans des circuits Bluetooth.

Lexique

FHSS = Frequency hopping Spread Spectrum

CDMA = Code Division Multiple Access
Méthode d'accès au réseau sans fil

DCF = Distributed Coordination Function
Méthode d'accès au média égalitaire

DSSS = Direct Sequence Spread Spectrum

SNR = rapport signal sur bruit.

CRC = Code de Redondance Cyclique
Somme polynomiale permettant de vérifier qu'une suite de données binaire n'a pas été corrompue lors d'une transmission.

FEC = Forward Error Correction
Technique pour améliorer la robustesse de la transmission. Des bits supplémentaires sont inclus dans le train de données transmis, ce qui permet d'appliquer des algorithme de correction d'erreur afin de tenter de retrouver les données initiale en cas de corruption lors de la transmission.

Effet Doppler = variation apparente de la fréquence d'une onde émise par une source en mouvement par rapport à un observateur fixe.

Scatternet = réseau chaîné

liaison ACL = Asynchronous Connection-Less
Liaison physique Bluetooth asynchrone

Liaison SCO = Synchronous connection Oriented
Liaison physique Bluetooth synchrone

Bibliographie

Livres :
Les Réseaux / Ed. Eyrolles / Aut. Pujolle / juillet 2002.

Réseaux de mobiles & réseaux sans fil / Ed. Eyrolles / Aut. Al Agha, Pujolle, Vivier / septembre 2001.

B**luetooth 1.1 connexions sans fil** / Ed. Campuspress / Aut. Jennifer Bray, Charles F. Sturman

802.11 et les réseaux sans fil / Ed. Eyrolles / Aut. Muhlethaler / aout 2002.
802.11 wireless Netwoks The definitive Guide/ Ed. O'Reilly / Aut. Matthew S Gast / avril 2002.
Wi-Fi par la pratique / Ed. Eyrolles / Aut. Males, Pujolle / aout 2002.

Réseaux sans fil
Etude de performance de Bluetooth et integration avec 802.11. http://www-rp.lip6.fr/dnac/8.4-sethom-article.pdf

Jim Lansford, Adrian Stephens, Ron Nevo (Mobilian Corporation)
Wifi (802.11b) and Bluetooth enabling coexistence
IEEE Network sept/oct 2001

Wifi :
[MSA2003] Arunesh Mishra, Minho Shin, William Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process"

http://rubb.free.fr/802-11/

http://www.tt-hardware.com/article.php?sid=3683

Logiciel WifiScanner http://www.hsc.fr/ressources/outils/Wi-Fiscanner/

Logiciels diverses Wi-Fi http://www.nantes-wireless.net/index.php?page=logiciels

La bible des drivers linux pour les cartes sans fil :
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/

Liaison wireless sans AP : http://www.sorgonet.com/network/wirelessnoap/

Bluetooth :
BLUETOOTH SPECIFICATION Version 1.0 A / Bluetooth Host Controler Interface

Reseaux ad hoc :

http://www.guill.net/index.php3?cat=3&pro=52

AODV : http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt

The Gray Zone Problem in IEEE 802.11b based Ad hoc Networks :
http://www.it.uu.se/research/group/core/publications/LundMC2R2002.pdf

Coping with Communication Gray Zones in IEEE 802.11b based Ad hoc Networks
http://user.it.uu.se/~henrikl/aodv/grayzones.pdf

Ad hoc networking and IEEE 802.11 :
http://www.sics.se/~lmfeeney/snus_802.11.pdf

Encodage Audio :
http://www.xiph.org/ogg/vorbis/