Université de Marne la Vallée
Ingénieurs 2000
Informatique et Réseaux 3

Exposé NT réseaux

Olivier Boitel
Denis Guillon
Cédric Fodouop Kamologne

Enseignant : Étienne Duris

Table des matières

I. Introduction

Bluetooth est une nouvelle technologie de transmission sans fil. Son but est de permettre la communication à courte distance entre plusieurs appareils, et sans le moindre câble, en utilisant les ondes radio. C'est une norme utilisée pour faire fonctionner des applications pour la maison, le travail et les loisirs.

Ce dossier exposera les grands principes techniques cette norme, dressera un état des applications existantes et à venir, et en exposera les avantages et inconvénients.

II. Présentation générale

1. Les réseaux sans fils

a) Qu'est-ce qu'un réseau sans fils ?

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

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

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

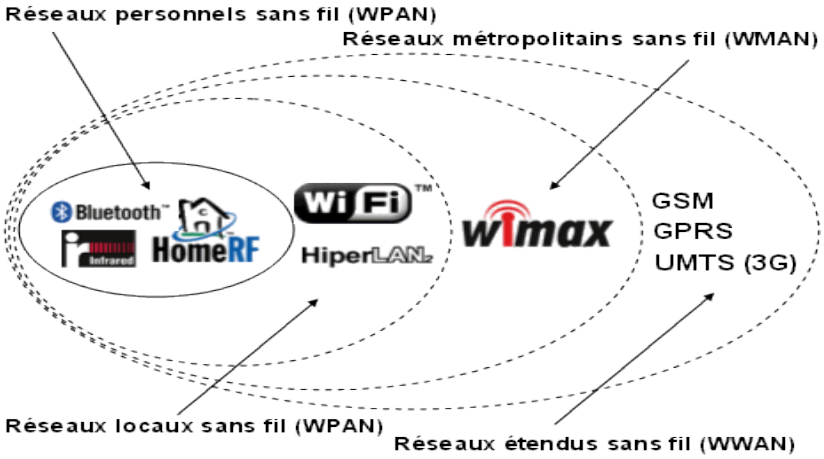
Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées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

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

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

b) Catégories des réseaux sans fils

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



Réseaux personnels sans fil (WPAN)

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

HomeRF

HomeRF (pour Home Radio Frequency), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été abandonnée en Janvier 2003, notamment car les fondeurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

ZigBee

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

Liaisons Infra rouge

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

La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon uni-directionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé PPM (pulse position modulation).

Réseaux locaux sans fil (WLAN)

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

Le WIFI

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

HyperLAN2

hiperLAN2 (HIgh Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 Mhz.

Réseaux métropolitains sans fil (WMAN)

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

Réseaux étendus sans fil (WWAN)

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

- GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile),
- GPRS (General Packet Radio Service),
- UMTS (Universal Mobile Telecommunication System).

2. Le bluetooth

a) Présentation de la technologie Bluetooth

Description

Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques (ordinateurs, imprimantes, scanners, téléphones portables, PDAs...) en en supprimant les liaisons matérielles. Un des principaux objectifs de Bluetooth est donc de remplacer les ports séries, les ports parallèles et l'USB.

Bluetooth (déposé à l'IEEE, sous le nom de 802.15) constitue donc une technologie de réseau personnel ou PAN (Personal Area Network).

C'est une technologie non protégée gérant les connexions sans fil de type onde radio utilisant la bande des 2,45 GHz, d'un débit de 1 Mbps, d'une portée de 10 m et offrant un balayage de 360°, tout en s'affranchissant des obstacles les plus courants. Cette technologie concurrence fortement IrDA.

Ce système radio à courte distance permet à la fois les échanges voix et données. En effet, un appareil Bluetooth peut fonctionner en mode commutation de paquets IP (sous forme de données avec un débit montant de 57,6 kbit/s et en descendant de 721kbit/s : connexion asynchrone) ou commutation de circuit (sous forme de voix avec un débit de 64 kbit/s : connexion synchrone) et même les deux simultanément.

De plus,la zone de réception du signal, extêmement limité, constitue une sécurité plus importante que celle du Wireless Fidelity qui nécessite la mise en place de moyens plus importants de contrôle d'accès à l'information.

Détails techniques

La bande de fréquence utilisée par Bluetooth est identique à celle du WI-FI (ou 802.11b) soit 2,4Ghz et utilise 79 fréquences différentes.

Bluetooth permet d'atteindre 1600 échanges par seconde soit un débit d'environ 1 Mbit par seconde mais avec une portée faible de plusieurs mètres seulement. Cependant, les dernières versions peuvent aller jusqu'à 100 m.

b) Usage

La consommation électrique du Bluetooth est faible, il est donc adapté aux périphériques. Plus ceux-ci sont petits et plus leur puissance d'émission est faible, plus leur usage sera de proximité (10 mètres maximum pour clavier, souris, PDA ou téléphone). Les plus puissants d'entre eux (micros, imprimantes, ... qui émettent sur 30 m pour une puissance d'émission de 100 mW) atteignent sans peine les limites de réception.

Le Bluetooth doit donc être considéré comme le remplaçant du port USB pour un espace de mobilité restreint limité à une pièce voire à deux lieux très proches, séparés par une cloison sèche.

Par contre le champ d'application du Bluetooth est considérable on peut aujourd'hui y connecter : PALM, micro casques téléphoniques, appareils photo, clavier, souris, imprimantes, GPS même. C'est un produit et une technologie fiables qui sont embarqués par de plus en plus nombreux équipements.

Bluetooth permet la reconnaissance, l'inscription et la création automatique de liaisons entre des outils utilisant la technologie Bluetooth, le tout sans réglage (ou presque) de la part de l'utilisateur. On peut donc synchroniser automatiquement son PC et son PDA, son téléphone portable, son lecteur MP3, etc.

De plus, il est également possible de relier un ordinateur portable ou un PDA à un téléphone mobile qui assurera la fonction modem, ce qui permet d'être relié au Web depuis n'importe quel endroit.

Au niveau des téléphones portables d'ailleurs, on a vu apparaître de multiples accessoires comme l'oreille Bluetooth qui sert de kit main libre sans fil.

Certaines marques ont élaboré des enceintes audio et également des écouteurs se reliant au pc par Bluetooth.

En résumé, Bluetooth permet :

- le téléphone et les conférences universels,
- le bureau sans fil,
- les réseaux domestiques,
- la synchronisation automatique

Grâce au Bluetooth on peut avoir :

- Accès à Internet
  - Terminal de données : PC/portable/PDA,
  - Modem : Téléphone mobile ou modem sans fil,
  - Point d'accès,
- Transfert de fichiers et échange d'objets
  - Transfert d'objets d'un appareil à l'autre,
  - Objets génériques, e.g., xls, ppt, wav, jpg, doc, dossiers, …
  - Possibilité de parcourir les dossiers sur l'appareil distant,
  - Opérations "push" simples : carte de visite.
- Synchronisation
  - Synchro de données personnelles - typiquement : répertoire, agenda, e-mails, notes.

c) Bluetooth SIG

La technologie Bluetooth a été originairement mise au point par Ericsson en 1994. En février 1998, un consortium d'industriels baptisé « Bluetooth Special Interest Group » (Bluetooth SIG), réunissant plus de 2000 entreprises dont Agere, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia et Toshiba, a été formé afin de produire les spécifications Bluetooth 1.0, qui furent publiées en juillet 1999.

Le nom « Bluetooth » (littéralement « dent bleue ») est directement inspiré du roi danois Harald II (910-986) surnommé Harald II Blåtand (« à la dent bleue »). On lui attribue l'unification de la Suède et de la Norvège ainsi que l'introduction du christianisme dans les pays scandinaves. Cette unification fait écho à la volonté du SIG de définir un satandard commun de communication.

Le logo de Bluetooth, est inspiré des initiales en alphabet runique de Harald Bluetooth :

d) Spécifications

Sous-standards

Norme	Informations/Etat
802.15.1	débit de 1Mbit/sec Wireless PAN, Bluetooth v1.x, v2.x standard déposé et publié
802.15.2	recommandations liées à l'utilisation de la bande de fréquence 2,4 Ghz, standard en cours de validation
802.15.3	Haut débit allant à plus de 20 Mb/s pour une utilisation multimédia
802.15.4	Bas débit.

La pile de protocoles

Afin d'assurer une compatibilité entre tous les périphériques Bluetooth, la majeure partie de la pile de protocoles est définie dans la spécification.

Les éléments fondamentaux d'un produit Bluetooth sont définis dans les deux premières couches protocolaires, la couche radio et la couche bande de base. Ces couches prennent en charge les tâches matérielles comme le contrôle du saut de fréquence et la synchronisation des horloges.

Caractéristiques

Le Bluetooth permet d'obtenir des débits de l'ordre de 1 Mbps, correspondant à 1600 échanges par seconde en full-duplex, avec une portée d'une dizaine de mètres environ avec un émetteur de classe II et d'un peu moins d'une centaine de mètres avec un émetteur de classe I.

3. Comparaison avec d'autres technologies sans fils

a) Bluetooth Vs Wifi

Pourquoi Bluetooth plutôt que Wifi ?

La technologie Bluetooth consomme environ 10 fois moins d'électricité que Wifi. Sa consommation est de l'ordre de 20mW pour une distance de 10m et de 100mW pour une distance de 100m. Contrairement à Bluetooth, Wifi ne permet pas encore d'assurer une autonomie suffisamment importante avec des batteries légères (bien que la technologie Centrino d'Intel y vise). Bluetooth est donc la technologie idéale pour intégrer la communication sans fil dans des outils mobiles liés au réseau de l'utilisateur. Wifi et Bluetooth ne sont donc pas concurrents mais plutôt complémentaires puisque WI-FI se situera donc plutot au niveau du réseau local ou LAN (Local Area Network).

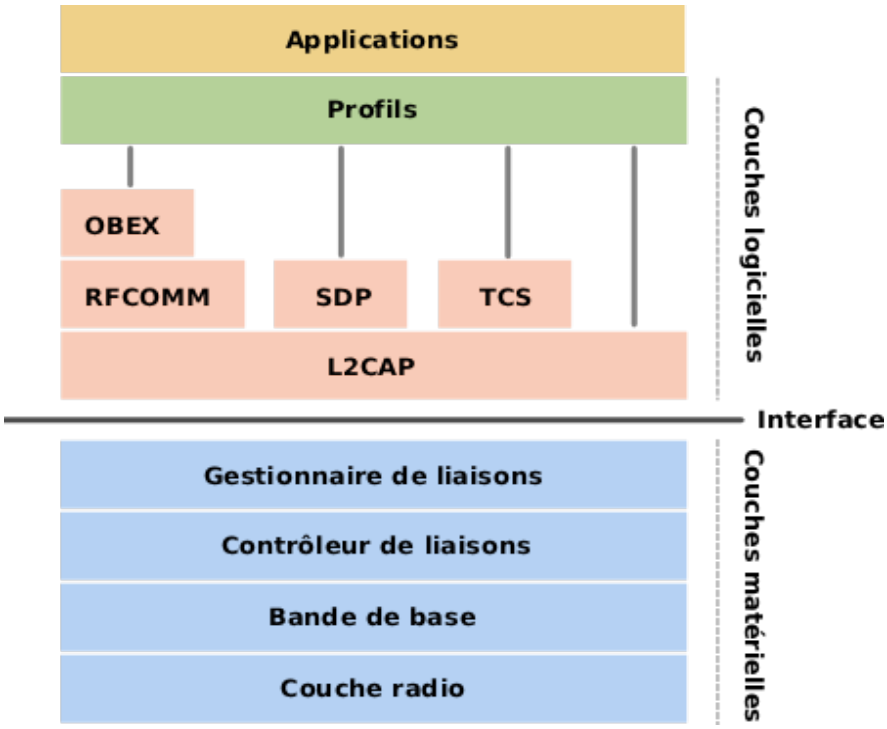
Les technologies Bluetooth et Wi-Fi sont complémentaires. Wi-Fi est un système Ethernet sans fil qui agrandit ou remplace des réseaux câblés reliant des dizaines d'appareils informatisés, tandis que Bluetooth est conçu pour être utilisé en lieu et place de câbles entre plusieurs appareils situés dans un rayon de 10 mètres les uns des autres. Bluetooth assure des connexions pour les données, la voix et le son. Bluetooth est également idéal pour les appareils alimentés par batterie en raison de sa faible consommation d'énergie.

b) Bluetooth Vs Irda

La principale différence est que Bluetooth fonctionne par ondes radio, tandis que l'infrarouge utilise des impulsions lumineuses très rapides. Avec l'infrarouge, les capteurs des deux appareils doivent être l'un face à l'autre, sans obstacle entre les deux, faute de quoi la connexion est interrompue (de même que la connexion entre votre télécommande et votre lecteur DVD est interrompue si une personne se place entre les deux). Bluetooth n'est pas limité par ce type d'inconvénient, et fonctionne même à travers les cloisons. De plus, l'infrarouge ne fonctionne qu'entre deux appareils maximum.

III. Couche physique

Les éléments fondamentaux du Bluetooth sont définis dans les deux premières couches protocolaires, la couche *radio* et la couche *bande de base*. Ces couches prennent en charge les tâches matérielles telle que le contrôle du saut de fréquence et la synchronisation des horloges.



1. La couche radio

La couche radio qui est la couche la plus basse, est gérée au niveau du matériel. D'une manière générale, elle correspond assez bien à la couche physique des modèles OSI et 802. Elle prend en charge la transmission et la modulation du signal radio.

La couche radio transmet des bits du maître vers l'esclave et vice versa : c'est un système radio de faible puissance avec une portée de 10 m qui opère dans la bande des fréquences de 2.4GHz. Celle-ci est divisée en 79 canaux de 1MHz. La technique de modulation utilisée est la modulation de fréquences (FSK) avec 1 bit par Hertz pour un débit brut de 1 Mbit/s. Pour garantir une allocation équitable des canaux, la technique d'étalement de spectre par saut de fréquence (FHSS) est mise en oeuvre, avec 1600 sauts par seconde et un temps de maintien (dwell time) ou période de 625µs. Tous les noeuds d'un piconet changent simultanément de fréquence et c'est le maître qui impose la séquence de sauts.

La technique FHSS (Frequency Hopping Spread Spectrum, en français étalement de spectre par saut de fréquence) consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

Des interférences peuvent exister entre le Bluetooth et le 802.11 car ces deux protocoles utilisent la même bande de fréquence. De plus, le protocole Bluetooth est plus à même de gêner les transmissions 802.11 car il change de fréquence beaucoup plus rapidement que 802.11.

L'étalement de spectre par saut de fréquence a originalement été conçu dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Le FHSS dans Bluetooth permet :

- Une synchronisation parfaite émetteur/récepteur
- Des fréquences partageables, si séquence de saut différente. Cela autorise plusieurs périphériques à émettre simultanément.
- Une limitation des interférences, ceci grâce au saut de fréquence (sur les fréquences polluées)
- De sécuriser grâce aux séquences de saut pseudo-aléatoire.

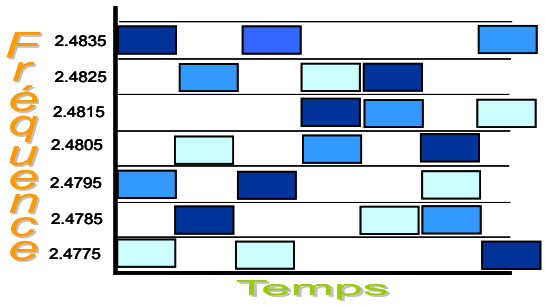


Figure 1 - Exemple d'utilisation de FHSS

2. La couche bande de base

C'est cette couche qui se rapproche le plus de la sous-couche MAC, elle définit donc ainsi les adresses matérielles des périphériques. Cette adresse nommée *BD_ADDR* (Bluetooth Device Adress) est codée sur 48 bits.

C'est également cette couche qui prend en charge la communication entre les appareils. Les différents types de connexions sont au nombre de trois à savoir :

- La liaison synchrone à débit élevé,
- La liaison asynchrone,
- La liaison « canal voix/donné » ou liaison SCO.

a) La liaison synchrone à débit élevé

Ces liaisons sont utilisées lorsque le débit montant (de l'esclave au maître) est du même ordre que le début descendant (du maître à l'esclave). Ces liaisons se partagent donc la bande passante : elle possède un débit bidirectionnel de 432Kb/s. Ces liaisons sont celles qui seront par exemple utiliser pour relier 2 ordinateurs voulant faire de l'échange de fichiers. Un maître peut supporter jusqu'à 3 liaisons de ce type avec ses esclaves.

Dans le cas d'erreur de transmission, un paquet spécial signalant l'erreur sera envoyé à l'émetteur qui réenverra l'information. Ce mode de fonctionnement n'est donc pas adapté à une utilisation temps réelle tel que la diffusion de la voix ...

b) La liaison **ACL** (Asynchronous Connection-Less)

Ce type de liaison est utilisée pour les données acheminées par paquet et disponibles à intervalles réguliers. Ces données proviennent de la couche L2CAP du côté émetteur et sont remises à la couche L2CAP du côté récepteur. Ce type de liaison pratique le « best effort » et aucune garantie n'est fournie en ce qui concerne la livraison des paquets. Les trames perdues ne sont pas forcément retransmises.

Ce mode de communication permet de privilégier un sens de transmission : du maître vers l'esclave. Le maître peut donc envoyer 721Kb/s à l'esclave, et l'esclave peut envoyer 57,6Kb/s au maître. Ce type de liaison est particulièrement adapté dans le cas d'un accès à internet par Bluetooth : en effet, lors d'une consultation internet, le taux de download (téléchargement des pages, des images) est bien plus important que le taux d'upload (envoi des requêtes). C'est également cette solution qui sera utilisée pour le connexion vers une imprimante.

Un esclave peut disposer au maximum d'une liaison ACL avec son maître.

c) La liaison **SCO** (Synchronous Connection Oriented)

Ce type de liaison est utilisée pour la manipulation de données en temps réel, par exemple, pour les connexions téléphoniques. Ce type de canal se voit allouer un slot fixe dans chaque direction. Le délai de transmission étant critique pour ces liaisons, les trames qui y sont transmises ne font jamais l'objet d'une retransmission. À la place, un code de correction d'erreurs peut être utilisé pour assurer une haute fiabilité.

Un esclave peut disposer au maximum de trois liaisons SCO avec son maître, chacune d'elles supportant un canal vocal PCM à 64000 bit/s.

d) Topologie d'un réseau Bluetooth

Réseau piconet

Ce type de réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon (10 m environ). Ce type de réseau suit une topologie en étoile : un maître / plusieurs esclaves.

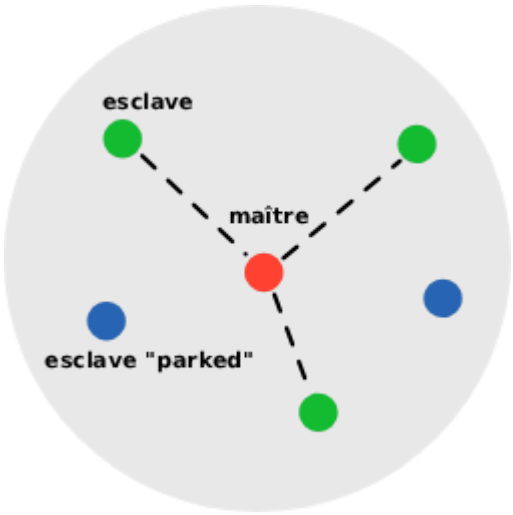


Figure 2 - Exemple de réseau piconet

Dans ce type de réseau, un périphérique maître peut administrer au maximum 7 esclaves actifs et 255 esclaves inactifs (« *parked* »). De plus les communications entre périphériques esclaves n'est pas possible et se fait de façon directe entre un maître et un esclave.

Dans un piconet, les fréquences de saut sont déterminés par le périphérique maître et tous les esclaves sont synchronisés sur l'horloge du maître.

Réseau *scatternet*

Dans un réseau Bluetooth, les périphériques esclaves peuvent avoir plusieurs maîtres, les différents piconets peuvent donc être inter-connectés. Le réseau ainsi formé est appelé un scatternet (littéralement réseau chaîné).

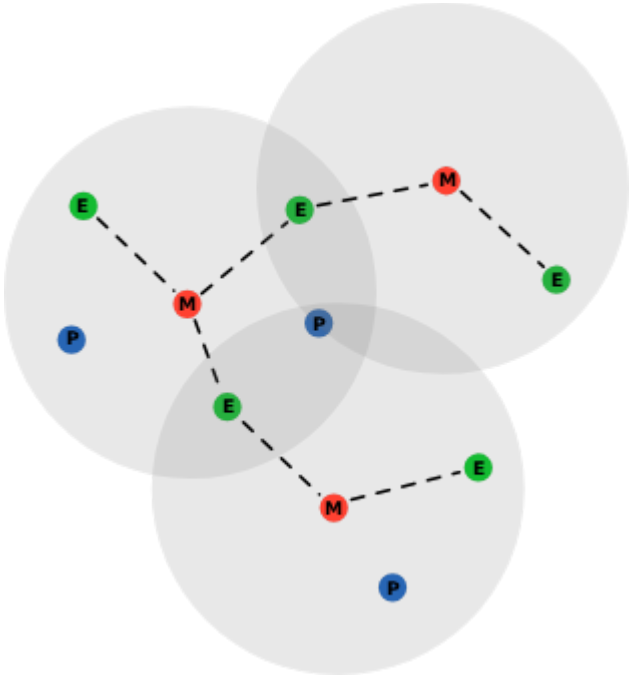


Figure 3 - Exemple de réseau scatternet

Les piconets peuvent s'interconnecter via des esclaves ponts, de plus, les piconets utilisent une séquence de saut de fréquence différente basée sur l'adresse du maître du piconet, ce qui permet la coexistence de plusieurs piconets au même endroit. Une des conséquences de cette coexistence est une augmentation du débit local.

Pour supporter la transmission de données entre piconets, un mécanisme de routage doit être implémenté.

3. La couche Link Manager (LM) ou gestionnaire de liaisons

Cette couche gère les liens entre les périphériques maîtres et esclaves ainsi que les types de liaisons (synchrones ou asynchrones).

C'est le gestionnaire de liaisons qui implémente les mécanismes de sécurité comme :

- L'authentification,
- le pairage,
- la création et la modification des clés,
- le cryptage.

Cette couche prend aussi en charge la découverte de gestionnaires de liaisons distants et communiquent avec eux à travers le LMP (Link Manager Protocol). Pour accomplir son rôle de fournisseur, le gestionnaire de liaisons utilise les services du LC (Link Controller).

Le gestionnaire de liaisons consiste essentiellement en un nombre de PDU (Protocol Data Units) qui sont envoyés d'un périphérique vers un autre déterminé par le AM_ADDR qui est indiqué dans le paquet d'en-tête.

4. L'interface de contrôle de l'hôte (HCI)

Cette couche fournit une méthode uniforme pour accéder aux couches matérielles. Son rôle de séparation permet un développement indépendant du hardware et du software.

Les protocoles de transport suivants sont supportés :

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

5. La couche L2CAP (*Logical Link Control & Adaptation Protocol*)

Cette couche à trois fonctions principales. Premièrement, elle accepte des paquets pouvant atteindre 64Ko en provenance des couches supérieures et les découpe en trames pour la transmission. À l'extrémité réceptrice, les trames sont réassemblées en paquets.

Deuxièmement, elle assure le multiplexage et le démultiplexage pour plusieurs sources de paquets. Une fois qu'un paquet a été réassemblé, elle détermine le protocole de couche supérieure destinataire, par exemple RFCOMM ou le protocole de téléphonie.

Troisièmement, elle satisfait aux exigences de qualité de service, que ce soit au cours de l'établissement des liaisons ou pendant leur exploitation normale. Lors du processus d'établissement, elle négocie également la taille maximale de la charge utile pour empêcher qu'un équipement ne submerge de gros paquets un autre équipement utilisant des paquets plus petits. Cette fonctionnalité est nécessaire car tous les équipements ne sont pas tous capables de gérer une taille de paquet de 64Ko.

IV. Principe de fonctionnement

Les communications sous Bluetooth nécessitent une connaissance préalable des équipements se trouvant dans l'environnement d'émission. Elles se font donc, comme expliqué dans la partie précédente, selon le principe « maitre-esclave ». Un groupe d'équipements forme une cellule appelée Piconet ou Picoréseau comportant un maître et au maximum 7 esclaves. Les piconets peuvent également se chevaucher pour former des scaternet. Les piconets sont indépendants c'est à dire qu'ils n'ont pas la nécessité d'être synchronisés entre eux, et ils ont leur propre canal de fréquence. La communication à dans un piconet peut atteindre 1Mb/s.

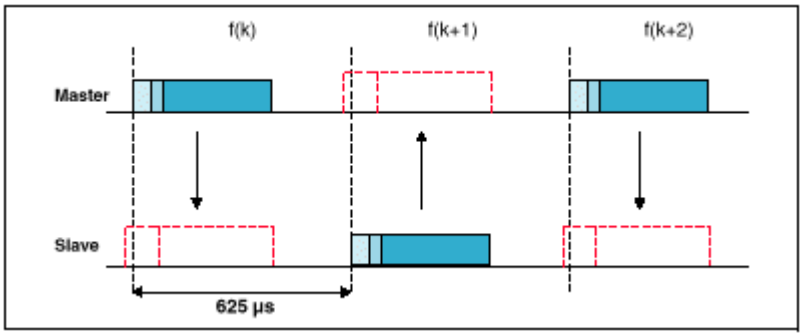
1. Principes de communication : le canal physique

a) Principe de base

Country	Frequency Range	RF Channels	
Europe* & USA	2400 - 2483.5 MHz	f = 2402 + k MHz	k= 0,...,78
Japan	2471 - 2497 MHz	f = 2473 + k MHz	k= 0,...,22
Spain	2445 - 2475 MHz	f = 2449 + k MHz	k= 0,...,22
France	2446.5 - 2483.5 MHz	f = 2454 + k MHz	k= 0,...,22

Le canal est représenté par une séquence de sauts pseudo-aléatoire choisis parmi les 79 ou 23 canaux RF disponibles dans la bande 2,4GHz(tableaux ci dessus). Les appareils Bluetooth qui utilisent la même séquence forment un picoréseau. Cette séquence de saut est unique pour chaque picoréseau. Elle est attribué par le dispositif Bluetooth maître qui fournit l'horloge à tous ses esclaves connecté dans le piconet.

Le canal est divisé en intervalles de temps appelés slots. Un terminal Bluetooth utilise une fréquence sur un slot, puis, par un saut de fréquence, il change de fréquence sur l'intervalle de temps suivant. Les clients d'un même picoréseau possède la même suite de sauts de fréquence puisqu'il sont déterminés par l'horloge du maître. Lorsqu'un nouveau client Bluetooth souhaite se connecter, il doit donc reconnaître l'ensemble des sauts de fréquence pour s'y adapter. Chaque intervalle de temps ou slot est numéroté et a une durée de 625 µs. On utilise la technique de duplexage par division dans le temps TDD (Time Division Duplex). C'est à dire que les unités maître et esclave transmettent alternativement.



Le canal étant divisé en plages de temps de 625µs, il y aura donc 1600 sauts de fréquences/s/canal. Pour la synchronisation des divers éléments d'un piconnet, les plages de temps seront donc numéroté de 0 à 2^27cycliquement.Un client Bluetooth utilise donc de façon cyclique toutes les bandes de fréquences.

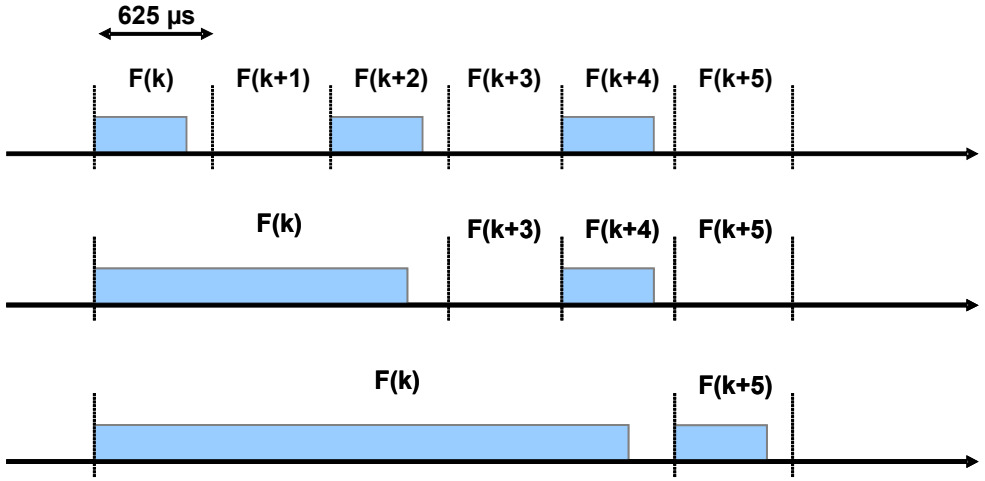
Pour les communication Bluetooth les règles suivantes sont appliqués :

- chaque slot pour une communication maître-esclave est systématiquement suivie par un slot esclave-maître.
- Un esclave ne peut émettre dans un slot que si le maître a préalablement émis dans le slot précédent.
- La communication ente deux esclaves est impossible.
- l'ordonnancement des différents esclaves dans le picoréseau est géré par le maître selon l'algorithme « round robin »(queue circulaire).

Les transmissions effectuées par les unités Bluetooth se font par paquets. Un paquets correspond aux données transmise ou reçus par les différentes entités Bluetooth.

b) Gestion des intervalles de temps

Un paquet peut se juxtapose sur 1 à 5 intervalles de temps consécutifs. Lorsqu'un paquet possède une taille de 1 slot on parle de transmission sur slot unique, et lorsque sa taille est supérieur à 1 time slot on parle de Multi-slot.



Le saut de fréquence appliqué à un paquet est celui du premier slot de ce paquet.

Bluetooth permet donc d'utiliser 3 types de tailles de paquets :

- paquets sur slots unique : 240 bits maxi.
- Paquets sur 3 slots : 1480 bits maxi.
- Paquet sur 5 slots : 2745 bits maxi.

On peut ainsi obtenir différents débits en fonction de la taille des paquets émis et du type de lien. En effet on utilise ce principe pour définir les débits maximum pour un type de lien dans la norme Bluetooth.

c) Les types de liens

Il existe 3 types de liens qui peuvent être établis entre un maître et un esclave : les liens synchrones a débit élevé, les liens asynchrones sans connexion (ACL) et les liaisons canal voix/donnée (SCO).

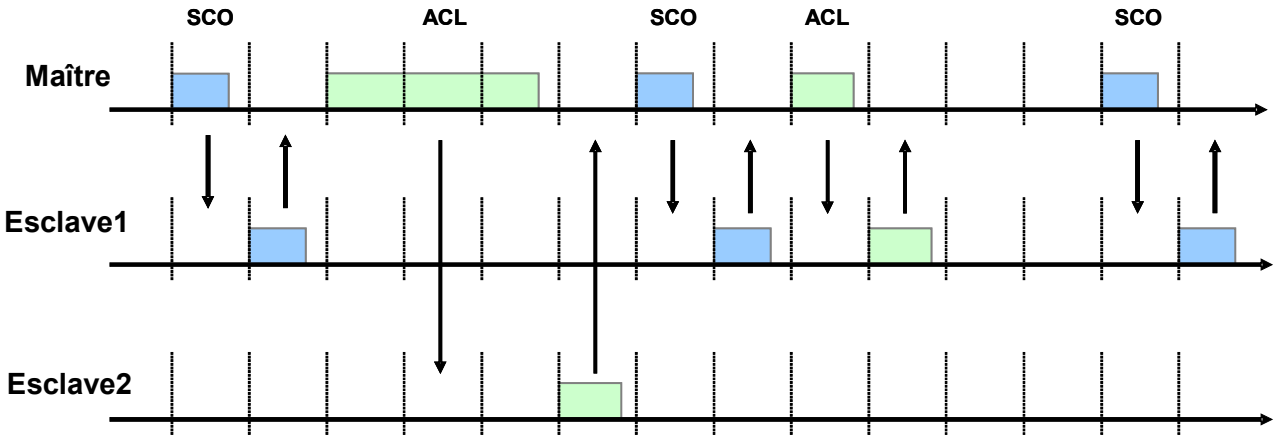
– Les liens synchrone à débit élevé : Ces liaisons sont utilisées lorsque le débit maître-esclave est du même ordre que le débit esclave maître. Il y a donc partage de la bande passante. Le débit dans les deux direction est de 432Kb/s . Ce type de liaison est utilisé par exemple pour relier deux périphériques Bluetooth souhaitant faire de l'échange de fichiers. Un maître peut

posséder trois liaisons de ce types avec ses esclaves. Ce type de liaison n'est pas adapté à la transmission de données en temps réel comme la voix. Lorsqu'une erreur survient, elle est signalé à l'émetteur qui devra retransmettre le paquet.

- Les liens asynchrones (ACL : asynchornous connection-less) : ce type de lien privilégie le sens de transmission maître-esclave. Le maître peut envoyer des informations à un débit de 723,2Kb/s tandis que l'esclave peut transmettre à un débit de 57,6Kb/s vers le maître (un paquet long sur 5 slots en envoi et un paquet court sur slot unique en réponse). Ce type de liaison est particulièrement utilisé dans le cas d'une connexion à internet via Bluetooth. En effet le taux de download est toujours largement supérieur au taux d'upload pour ce type de connexion. On utilisera également ce principe pour la connexion Bluetooth d'une imprimante (la communication de l'imprimante vers le poste de travail nécessitant un faible débit). Un lien ACL peut être simple ou multiple entre le maître et les esclaves du picoréseau (point à point multiple). En cas d'erreur la plupart des paquet ACL sont retransmis.

- Les canaux voix/données (SCO : synchornous connection oriented): Ces liens sont des connexions symétrique point à point entre un maître et un seul esclave du picoréseau. Le maître maintient ce type de liaison en réservant des slots qui reviennent à intervalles réguliers. Un lien SCO fournit une connexion en mode circuit entre un maître et un esclave offrant un débit régulier. C'est cette particularité qui le rend idéal pour le transport de données en temps réels comme la voix par exemple. En cas d'erreur les paquets de type SCO ne sont jamais retransmis. Ce sont des liens full duplex offrant un débit de 64Kb/s.

exemple de communication entre un maître et deux esclaves :



Dans cet exemple le maître possède un lien ACL et un lien SCO avec l'esclave 1 ainsi qu'1 lien ACL avec l'esclave 2.

2. Adressage des périphériques

Quatres types d'adresse peuvent être assignées aux unité bluetooth : BD_ADDR, AM_ADDR, PM_ADDR, AR_ADDR.

- BD_ADDR (Bluetooth Address Device) : elle correspond à l'adresse du dispositif. En effet, à chaque émetteur récepteur Bluetooth est allouée une adresse de dispositif unique sur 48 bits. Cette adresse est équivalente à une adresse MAC mais ne sert qu'à identifier le dispositif. Elle n'apparaît jamais dans le paquet de données.

- AM_ADDR ou AMA (Active Member Adress) : c'est l'adresse d'un membre actif dans un piconet. Elle correspond à une nombre de trois bits et est seulement valable tant que l'esclave est actif sur le canal maitre-esclave. Cette adresse sur trois bits permet de définir 8 valeur différentes ce qui correspond à la taille maximale d'un picoréseau.

- PM_ADDR ou PMA () : c'est une adresse réservé au membre non actifs. Elle est codée sur huit bits et n'est valable que si l'esclave est inactif.

- AR_ADDR ou ARA () : c'est une adresse de demande d'accès. Elle est utilisé par l'esclave inactif initialement pour determiner le demi slot dans la fenêtre d'accès dans lequel la demande d'accès peut être envoyée. Elle est seulement valable lorsque l'esclave est inactif.

3. Formats des paquets bluetooth

a) Découpage d'un paquet

Le format standard des paquets est le suivant :

72 bits	54 bits	[0 - 2745 bits]
Code d'accès	Entête	Corps du message

Les 72 premiers bits servent à la synchronisation entre les composants Bluetooth. L'entête quant à elle permet :

- De numéroter les paquets (réordonnancement),
- D'indiquer de quel membre d'un pico réseau émane ce message (0 => 7),
- De préciser le type du paquet que l'on est en train de consulter,
- De dire si oui ou non un récépissé est attendu en retour à ce message,
- De contrôler sa propre cohérence (CRC).

Les 54 bits suivants constituent l'en-tête du paquet (3 fois la même séquence de 18 bits) :

3	4	1	1	1	8
Addr	Type	F	A	S	Total de contrôle

Addr: adresse d'un membre actif du piconet (0 pour un broadcast ou de 1 à 6 pour un périphérique spécifique.

Type : type du paquet (SCO, ACL, NULL ou POLL) / type de FEC / durée du payload

F : contrôle de flux pour indiquer si le buffer est plein,

A : demande d'acquittement,

S : Numéro de séquence du paquet

Total de contrôle : contrôle d'erreur sur l'en-tête.

Le corps du message, contenant jusqu'à 2745 bits, sert lui à stocker les données à transporter. Il contient généralement un CRC de 8 ou 16 bits servant à la détection d'erreur. Son utilisation peu varier, comme nous le verrons par la suite. L'envoie d'un paquet nécessite un "slot ".

Lorsqu'un appareil Bluetooth émet un paquet, celui-ci peut appartenir à une des trois grandes familles de paquets existants, son type étant précisé dans le header :

b) Les types de paquets

Les paquets standards : Ils sont utilisés dans les opérations "administratives ". On entend par-lé que le contenu de ces paquets est dédié à la gestion des connections entre les appareils.

Les paquets SCO : Comme son nom l'indique, ce type de paquet est utilisé pour les communications de données de type SCO.

Les paquets ACL : Il existe également des paquets spécifiques au mode de transmission de données ACL.

Pour chacun de ces types, plusieurs sous catégories existent. Les différents types de paquets qui en découlent se sont vus attribuer une nomenclature. On distingue dans cette nomenclature les paquets suivants :

Les paquets DV : Pour " Data Voice packet ". Ce type hétéroclite permet de transporter à la fois des données et de la voie.

Les paquets DM x : Pour "Medium Data rate packet". Ce type de paquet n'est disponible qu'en mode ACL. Cette dénomination est due au fait que le corps de ce type de paquet est toujours encodé afin d'obtenir de la redondance (prévention d'erreur).

Les paquets DH x : Pour " High Data rate packet". Ce type de paquet n'est également disponible qu'en mode ACL. Son nom vient du fait qu'aucun encodage de prévention d'erreur n'est employé, d'où un meilleur taux de transfert.

Les paquets HV y : Pour " High quality Voice packet ". Ce type de paquet n'est disponible qu'en mode SCO. Ces paquets n'utilisent pas de CRC dans leur corps.

Le x dans les notations " DM x " et " DH x " remplace un des chiffres suivants : 1,3 ou 5. Ce chiffre représente le nombre de slots sur lesquels ce paquet s'étend. Par exemple les paquets de type DM3 s'étalent sur 3 slots.

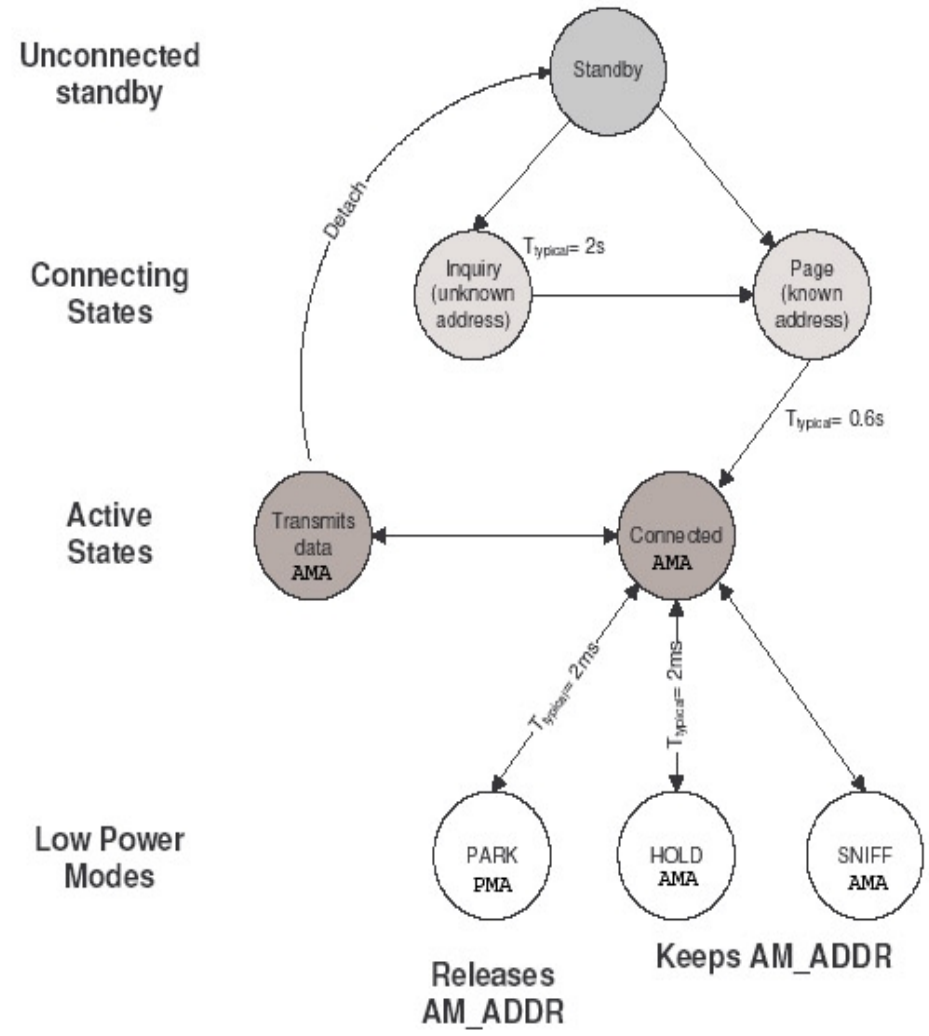
Le y dans la notation " HV y " permet de préciser quel type de prévention d'erreur est utilisée:

- y = 1 <=> 1/3 FCE,
- y = 2 <=> 2/3 FCE,
- y = 3 <=> lorsqu'il n'y a pas de protections mise en place.

4. États des terminaux Bluetooth

Le gestionnaire de liens LM (Link Manager) permet de mettre en place, authentifier et de configurer un lien. Il communique avec d'autres gestionnaire de liens par l'intermédiaire du protocole LMP (Link Manager Protocol). Pour exécuter son rôle de fournisseur de service le protocole de gestion des liens utilise les service du contrôleur de lien (LC : Link Controler). Ce contrôleur gère la configuration et le contrôle de la liaison physique entre deux appareils.

Pour effectuer ces liaisons, un dispositif Blutooth possède un certain nombre d'états. Les deux états principaux d'un dispositifs sont « standby ou veille » et « connecté ». Cependant il existe 7 états intermédiaires pour passer de l'un à l'autre. Ces états sont : Inquiry, Inquiry scan, Inquiry response, Page, Page scan, Master response et Slave response. Enfin, une fois dans l'état connecté un dispositif Bluetooth peut encore prendre trois états différents : Actif, suspendu (Hold), parqué (Park) ou reniflement (Sniff).



a) L'état Standby

Lorsqu'aucune connexion n'est établie dans le réseau, tous les périphériques Bluetooth sont en mode « StandBy ». c'est un état de basse consommation pour un dispositif qui n'interagit avec aucune autre unité Bluetooth. Dans ce mode , une unité non connectée écoute les messages périodiquement toutes les 1,28 secondes. La procédure de connexion peut être initiée par n'importe quelle unité du réseau qui deviendra le maître.

b) Les états d'initialisation d'une connexion

- **Inquiry** : un dispositif se trouve dans cet état lorsqu'il désire découvrir les nouveaux dispositifs du réseau. Il envoie alors un paquet « inquiry »en broadcast à toutes les unités Bluetooth se trouvant dans sa zone. On utilise le message Inquiry pour communiquer avec des unités dont on ne connaît pas l'adresse. Ce message est envoyé sur les 32 séquences d'éveil (inquiry Hoping séquence).

- **Inquiry scan** : cet état désigne un dispositif à l'écoute des messages « inquiry » circulant sur le réseau. Il utilise le inquiry hoping sequence en écoutant successivement sur les 32 fréquences d'éveil.

- **Page** : l'envoi d'un message Page permet d'établir une connexion avec un dispositif Bluetooth si son adresse est connue. Un dispositif dans l'état Page signifie qu'il stocke les informations reçues sur une autre unités du réseau.

- **Page scan** : cet état désigne un dispositif à l'écoute des messages de type Page.

c) Les états d'un dispositif connecté

- **Actif** : En mode actif, le maître comme l'esclave participent activement a la communication sur la canal (écoute, envoi de paquets, réception de paquets).

- **Suspendu** (hold) : le lien ACL d'une connexion entre deux unités bluetooth peut être placé en mode suspendu pour un temps spécifique. Pendant ce temps aucun paquet ACL ne sera transmis par le maître à l'esclave se trouvant dans ce mode. Le mode suspendu est typiquement utilisé lorsqu'on a pas besoin d'envoyer des données à un esclave pendant un certain temps. Dans ce mode l'esclave ne peut plus recevoir que des message de type SCO. Les de ce type arrivant à intervalles réguliers, l'esclave peut s'endormir lorsqu'il n'est pas susceptible d'en recevoir. Ce mode permet également au dispositif Bluetooth d'économiser de l'énergie. Le mode hold peut également être utilisé quand un dispositif veux être découvert par d'autres unités Bluetooth ou veux joindre un autre piconet.

- **Parqué** (Park) : Un esclave se trouvant dans cet état est très peu actif et économise son énergie. Il ne reçois plus du tout de message ni n'en envoie. Son unique activité est de se reveiller de temps en temps pour rester synchronisé avec le maître et sa séquence de sauts. Le maître envoie régulièrement des balises pour permettre à ses esclaves de rester synchronisés. Le fait de passer un esclave dans cet état Park permet de libérer une place dans le piconet (seul 7 unités peuvent être active en même temps sur un piconet). Ainsi plus de 7 unités Bluetooth peuvent cohabiter dans le même picoréseau.

- **Sniff** : dans cet état le dispositif Bluetooth est en mode d'écoute. Il alterne N slots d'états endormis (économie d'énergie), et K slots d'états actifs.

5. Détails de fonctionnement

A l'initialisation d'un réseau Bluetooth, tous les périphériques sont en mode standby. C'est à dire qu'ils ne connaissent pas les autres dispositifs Bluetooth qu'il peut y avoir dans leur zone de couverture. Dans cet état les périphériques écoute et cherche la présence de transmission toutes les 1,28 secondes (inquiry scan) afin de savoir si quelqu'un désire communiquer. Aucun dispositif n'est synchronisé (les périphériques écoutent différentes fréquences d'éveil selon le séquencement de leur choix). Le standby est un état passif qui permet à un dispositif Bluetooth d'économiser de l'énergie. Un dispositif Bluetooth passe la moitié de son temps dans ce type d'état lui permettant ainsi d'avoir uneplus grande autonomie.

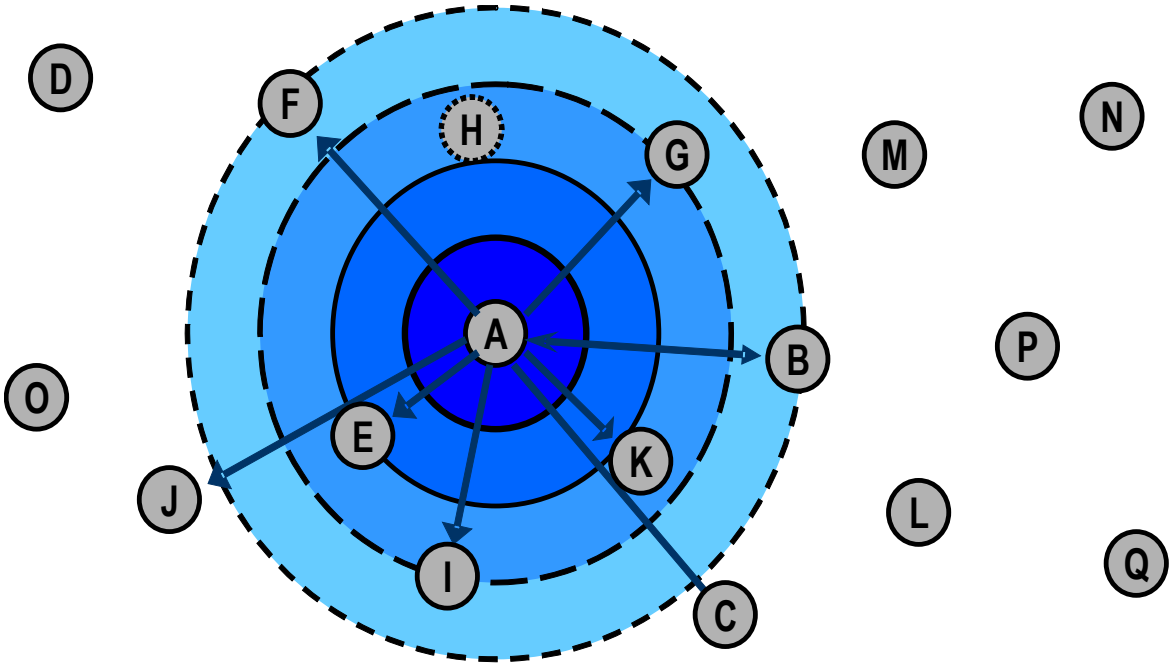
a) Principe général

N'importe quel dispositif Bluetooth peut être à l'initiative de la création d'un réseau de communication. Il deviendra alors le maître du picoréseau qui se créera par la suite.

La processus de connexion du maître avec les différents dispositifs du réseau suit certaines étapes importantes :

- Mode passif,
- Phase d'inquisition : découverte des points d'accès,
- Synchronisation avec le dispositif (paging),
- Découverte des services,
- Création d'un canal avec l'esclave,
- Pairage éventuel à l'aide d'un code PIN (sécurité),
- Utilisation du réseau.

La phase de découverte est donc à l'initiative de la création d'un picoréseau. En effet cette phase va permettre au dispositif maître de découvrir les périphériques Bluetooth qui se trouve dans sa zone de portée. Cela consiste à envoyer une trame en broadcast sur 32 fréquences d'éveil sur lesquelles les dispositifs Bluetooth en mode passif écoutent. Il pourront ainsi répondre et renseigner le maître sur les différentes informations les concernant.



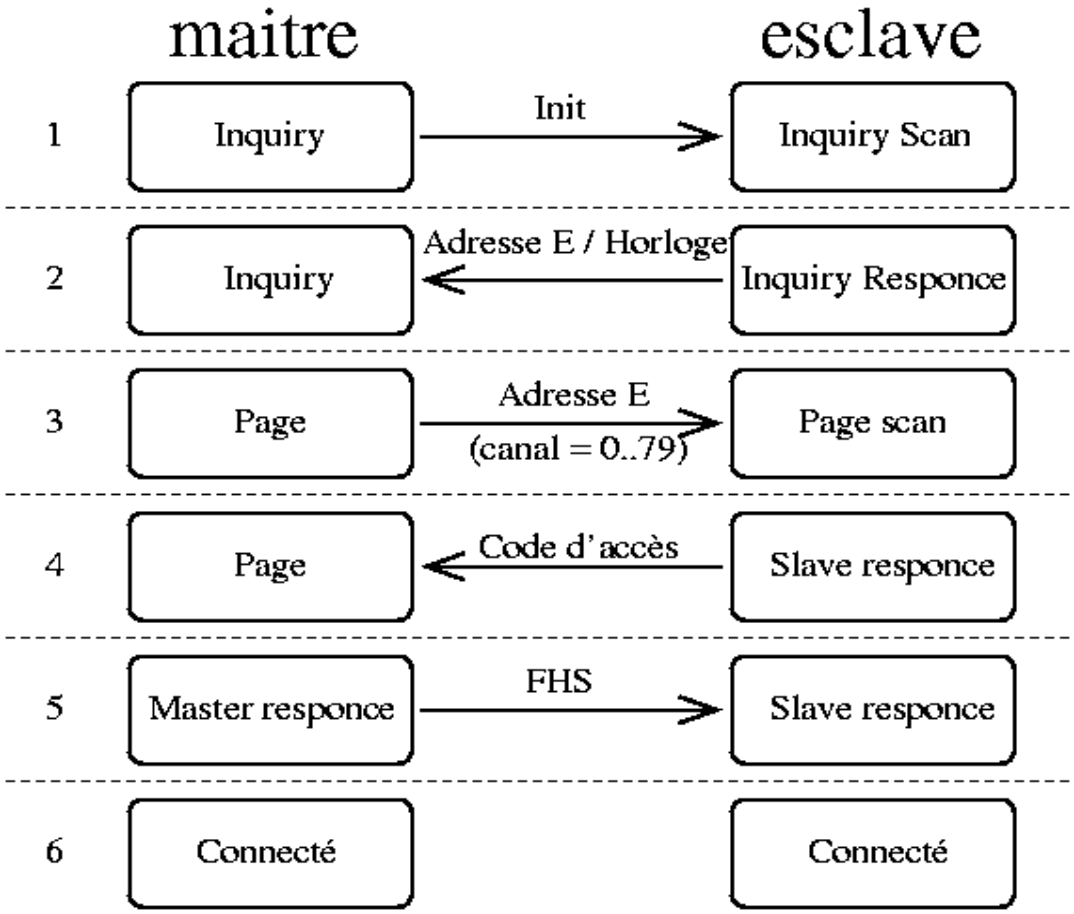
Un dispositif peut être non découvert. C'est les cas de H dans le schéma précédent.

Les codes d'accès utilisés dans cette phase sont spécifiques :

- GIAC (General Inquiry Access Code) : pour extraire les informations générales sur l'esclave.
- DIAC (Dedicate Inquiry Access Code) : pour extraire des capacités plus spécifiques.

Les étapes suivantes se déroule à chaque fois entre deux dispositifs distinct du réseau puisqu'elles consistent à établir un canal de communication spécifique entre le maître et l'esclave.

b) Détails maître-esclave



Comme décrit dans la partie précédente le processus démarre par un « inquiry » du maître vers l'eslave. L'esclave se trouvant à sa portée dans l'état inquiry scan va recevoir ce paquet de demande de découverte sur une des 32 fréquence qu'il écoute. l'esclave passera ensuite dans l'état inquiry response pour répondre au maître. Sa réponse comprendra entre autre son adresse et des informations sur son horloge. Une fois cette réponse envoyée il passe dans l'état page scan c'est à dire que l'esclave reste dans l'attente d'une demande de connexion de la part du maître. Il est alors en écoute sur tous les cannaux disponibles d'un message comportant son adresse propre venant du maître.

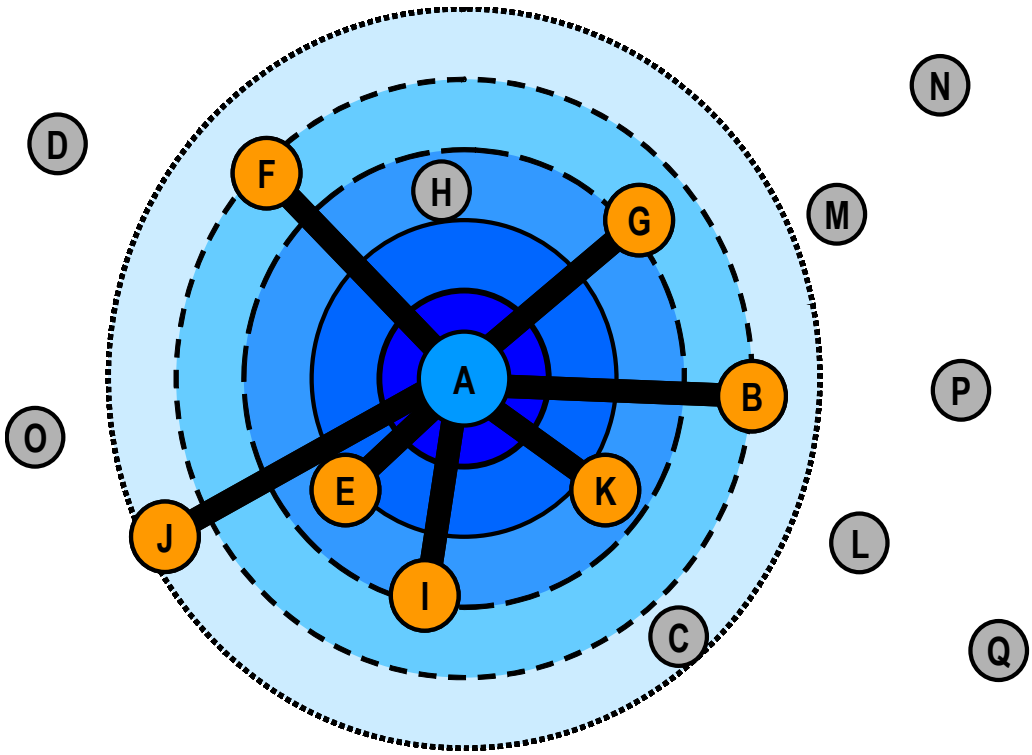
Le maître reçoit la réponse de l'esclave et passe alors dans l'état page. Il va alors stocker les informations concernant cet esclave qui lui permettront d'avoir constamment conscience de la présence de cet esclave sur le piconet. Lorsque le maître souhaitera initialiser la création d'un lien communiquant avec cet esclave il lui enverra un paquet contenant son adresse sur tous les canaux (23 en France) car il ne sont toujours pas synchronisés sur la même fréquence de sauts.

Lorsque l'esclave reçoit ce paquet qui lui est adressé, il passe dans l'état slave response et envoie un paquet au maître contenant son code d'accès. De son côté, le maître une fois ce code d'accès récupéré passe dans l'état master response et renvoie un paquet de type FHS (Frequency Hopping Synchronisation) à l'esclave. Dès lors l'esclave pourra se synchroniser avec le maître sur sa fréquence de sauts.

Les deux dispositifs sont alors dans l'état connecté et peuvent communiquer entre eux.

Le maître envoie cependant un paquet POLL à l'esclave pour vérifier que la synchronisation s'est bien déroulée. L'esclave pourra alors l'acquitter avec n'importe quel type de paquet.

c) Formation du piconet



L'enchaînement de paging successif permettra d'attacher j'usquà 7 esclaves actifs sur le piconet.

V. Profils d'applications

En Bluetooth, un profil correspond à une spécification fonctionnelle d'un usage particulier. Ils peuvent également correspondre à différents types de périphériques.

Les profils ont pour but d'assurer une interopérabilité entre tous les appareils Bluetooth. Ils définissent :

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

Les différents profils sont :

- GAP: Generic Access Profile,
- SDAP: Service Discovery Application Profile,
- SPP: Serial Port Profile,
- HS Profile: Headset Profile,
- DUN Profile: Dial-up Networking Profile,
- LAN Access Profile,
- Fax Profile,
- GOEP: Generic Object Exchange Profile,
- SP: Synchronization Profile,
- OPP: Object Push Profile,
- FTP: File Transfer Profile,
- CTP: Cordless Telephony Profile,
- IP: Intercom Profile.

Le profil d'accès générique est le profil de base dont tous les autres profils héritent. Il définit les procédures génériques de recherche d'appareils, de connexion et de sécurité.

VI. Sécurisation du protocole Bluetooth

Différentes politiques de sécurités sont misent en place dans Bluetooth. Il existe 3 niveaux de sécurité.

- Niveau 1 : pas de gestion de la sécurité.
- Niveau 2 : gestion de la sécurité au niveau service.
- Niveau 3 : gestion de la sécurité au niveau établissement de la liaison.

Le niveau 2 de sécurité fait intervenir un processus d'identification lors de l'accès aux services. Le niveau 3 est plus stricte et fait intervenir le processus d'authentification pendant l'établissement d'une connexion. Ceci complique un peu le schéma de connexion vu précédemment. A la suite d'une authentification réussie, des clefs sont créées de part et d'autre afin de pouvoir établir une communication sécurisée (cryptage / décryptage) entre les protagonistes.

On ne chiffre que les données et pas les en-têtes ni les codes d'accès.

1. Techniques d'authentification et de codage

Afin de maintenir la sécurité, plusieurs paramètres sont utilisés dans Bluetooth :

- Le N° de série de l'appareil, unique, fournis par l'IEEE, codé sur 48 bits, appelé BD_ADDR.
- La clef privée d'authentification, un nombre aléatoire codée sur 128 bits.
- Une clef privée de codage allant de 8 à 128 bits.
- Un nombre aléatoire de 128 bits qui doit changer fréquemment fournit par le composant Bluetooth lui-même.

Toutes les transactions sécurisées entre un ou plusieurs composant Bluetooth nécessitent une clef de liaison. Cette clef est un nombre de 128 bits aléatoire. La clef de liaison est utilisée dans le mécanisme de d'authentification et comme paramètre pour la production de la clef de cryptage.

Il y a plusieurs moyens d'obtenir cette clef. Elle peut être représentée par une des 4 clefs définies dans la norme Bluetooth :

- La clef unité (unit key). Celle ci est créée dans un seul composant quand il est installé.
- La clef de combinaison. Elle est créée grâce à la mise en commun de données provenant de deux composants Bluetooth.
- La clef maître. Cette clef est temporaire. Elle n'est utilisée que lorsque le maître souhaite transmettre des informations à plus d'un esclave.
- La clef d'initialisation. Elle est utilisée lorsqu'il n'y a pas encore de clef unité ou de clef de combinaison. Celle-ci est créée lors de l'initialisation.

De plus un code PIN (Personal Identification Number) est nécessaire pour sécuriser l'utilisation d'un appareil Bluetooth.

2. L'authentification

L'authentification est réalisée grâce à la clef de liaison. Celle-ci est supposée être en possession des deux parties. Lorsque par exemple A souhaite authentifier B, le mécanisme suivant est utilisé :

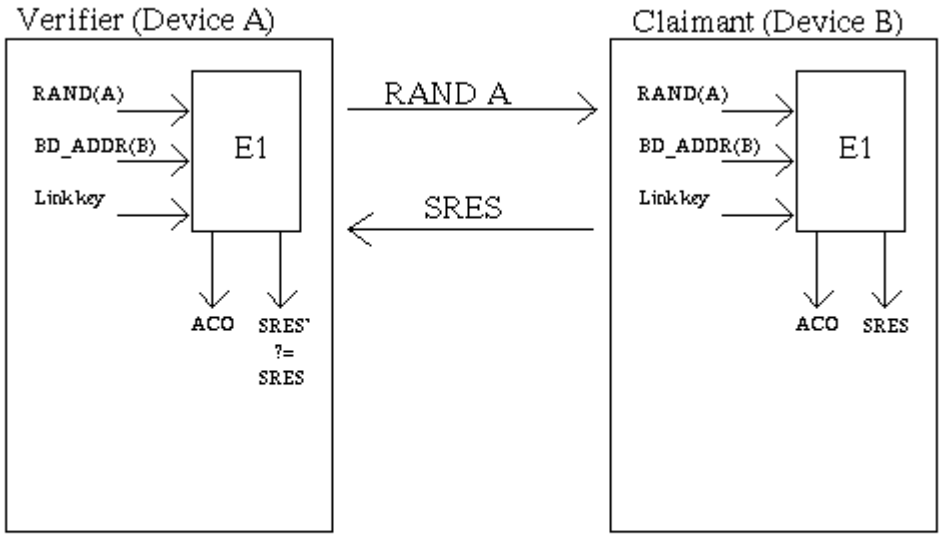


Figure 4 - Description du processus d'authentification

- Tout d'abord A envois à B un nombre aléatoire.
- Ensuite les participants calculent grâce à la fonction d'authentification E1 un résultat (Sres).
- Cette fonction prend en paramètre le nombre aléatoire RAND, la BD-ADDR de B ainsi que la clef de combinaison (link key).
- Une fois le calcule effectué de part et d'autre, B envoie son résultat à A.
- Celui-ci peut alors vérifier que B possède oui ou non la clef de combinaison.

En plus du résultat servant à authentifier B, la fonction E1 produit un nombre (l'ACO). Ce nombre peu par exemple servir de base pour les calcules de cryptage/décryptage qui ont généralement lieux après une authentification.

3. Le cryptage

Le mécanisme de cryptage/décryptage est assez proche de celui présenté précédemment. La différence se situe au niveau des paramètres et de l'algorithme utilisé. Dans le schéma suivant, on voit que l'algorithme permet de produire une clef de cryptage/ décryptage (Kstr) :

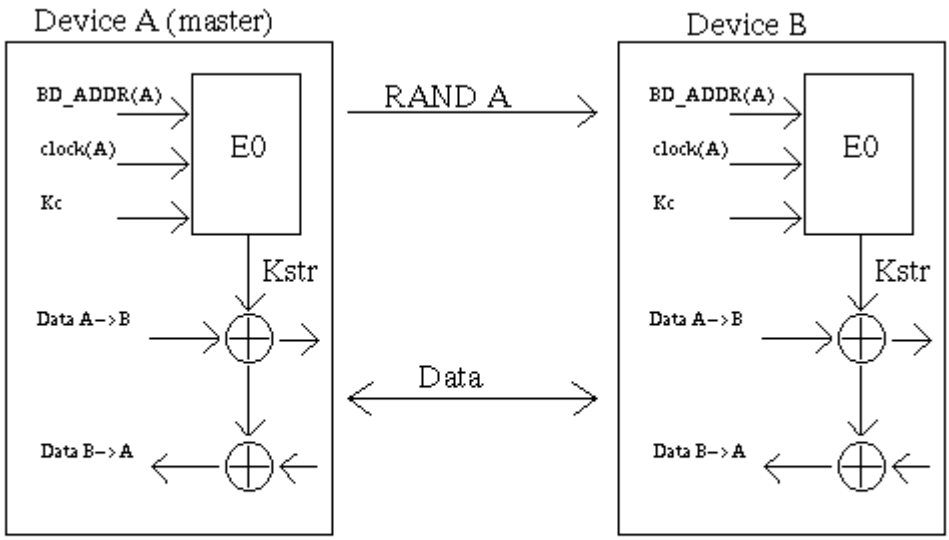


Figure 5 - Mise en oeuvre du cryptage

Le but n'est plus de vérifier que cette clef produite chez A est la même que chez B, mais simplement de s'en servir pour pouvoir déchiffrer les données envoyées. Les paramètres employés ici sont : un nombre aléatoire RAND créé par A, le No de série de A (BD_ADDR), l'horloge de A (clock) ainsi qu'une clef (Kc). La clef Kc elle est créée du coté de A et du coté de B grâce aux valeurs suivantes : le chiffre RAND, le chiffre précédemment calculé lors d'une authentification, l'ACO et la clef de lien.

VII. Conclusion

Bluetooth est une technologie de communication sans fil entre appareils. Peu coûteuse et de faible consommation, elle fonctionne par liaison radio de courte portée. Elle se présente en tan que remplacement de l'infrarouge. Mais, Bluetooth reste un protocole qui n'est pas encore s&curisé. De plus, il présente des risques de parasitage avec la norme 802.11 qui utilise également la fréquence 2,4Ghz.

Pour l'instant, du fait du retard pris sur la mise au point du protocole ainsi que de la complexité de mise en oeuvre importante, Bluetooth n'e s'est pas encore énormément répendu sur le marché. Toutefois, il est indéniable que la baisse des coups des composants utilisés par les appareils d'informatique personnelle tels que les téléphones portables et autres PDA va entraîner l'expansion de cette technologie.

VIII. Bibliographie

http://www.ece.fr:8000/~mercier/cours/bachelor/bluetooth%202005.pdf

http://www.ece.fr:8000/~mercier/these/

http://www.nokia.fr/index.php?content_id=39

http://www.commentcamarche.net/wireless/wlintro.php3

http://www.palowireless.com/infotooth/tutorial.asp

http://www.3ie.org/nouvelles_technologies/fiche/fiche_Bluetooth.htm

http://www.commentcamarche.net/bluetooth/bluetooth-intro.php3

http://fr.wikipedia.org/wiki/Bluetooth

http://www.commentcamarche.net/wifi/wifitech.php3#FHSS

http://www-rp.lip6.fr/~blegrand/cours/DESS/CoursBluetooth.pdf

http://www.aug-strasbourg.org/article.php?sid=67360

http://www-igm.univ-mlv.fr/~duris/NTREZO/20042005/Nguyen-Vongvilay-Wolowiec-Bluetooth.pdf