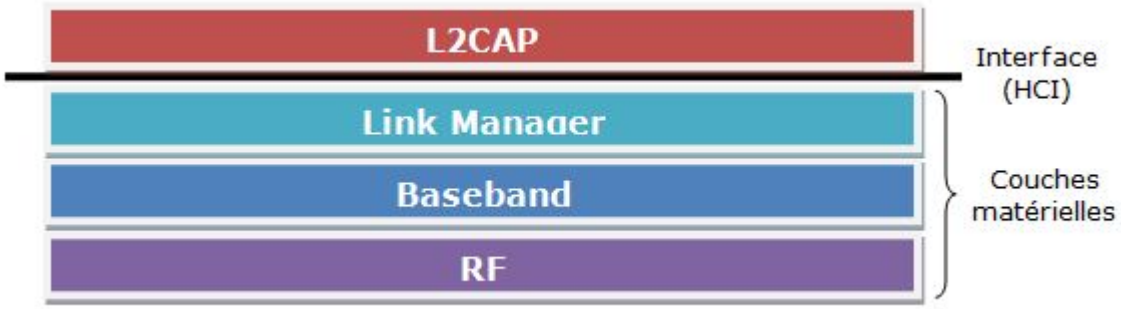
Bluetooth - La couche physique



La couche radio fréquence
La couche radio (la couche la plus basse) s'occupe de l'émission et de la réception des ondes radio. Elle définit les caractéristiques telles que la bande de fréquence et l'arrangement des canaux, les caractéristiques du transmetteur, de la modulation, du receveur, etc.
La technologie Bluetooth utilise l'une des bandes de fréquences ISM (Industrial, Scientific & Medical) réservée pour l'industrie, la science et la médecine. La bande de fréquences utilisée est disponible au niveau mondial et s'étend sur 83,5 MHz (de 2,4 à 2,4835 GHz).
Cette bande est divisée en canaux de 1 Mhz soit 79 canaux au total. Pour transmettre des datas, la technologie Bluetooth utilise le FHSS (Frequency Hopping Spread Spectrum).
Le principe du FHSS est la commutation rapide entre plusieurs canaux de fréquence, utilisant un ordre pseudo aléatoire connu tant à l'émetteur qu'au récepteur pour la synchronisation. Ainsi, les équipements radio participant à une transmission utilisant FHSS doivent utiliser la même séquence de saut de fréquence pour pouvoir communiquer.
Il existe trois classes de modules radio Bluetooth sur le marché ayant des puissances différentes et donc des portées différentes :

Classe	**Puissance (Attenuation)**	**Portée**
1	100 mW (20 dBi)	100 mètres
2	2,5 mW (4 dBi)	10-20 mètres
3	1 mW (0 dBi)	1-10 mètres

Les produits de la Classe 2 sont les plus courants. La puissance habituelle est d'environ 2,5 milliwatts. La portée est nettement plus courte, environ une dizaine de mètres.
La couche bande de base
La bande de base (ou baseband en anglais) est également gérée au niveau matériel. C'est au niveau de la bande de base que sont définies les adresses matérielles des périphériques Bluetooth (équivalent à l'adresse MAC d'une carte réseau). Cette adresse est nommée BD_ADDR (Bluetooth Device Address) et est codée sur 48 bits. Ces adresses sont gérées par la IEEE Registration Authority.
C'est également la bande de base qui gère les différents types de communication entre les appareils. Les connexions établies entre deux appareils Bluetooth peuvent être synchrones ou asynchrones. La bande de base peut donc gérer deux liens de connexions:
Les liaisons SCO (Synchronous Connection-Oriented)
Les liaisons ACL (Asynchronous Conection-Less)
Les liaisons de base
La couche Link Manager
Cette couche est gère la supervision des différentes connexions, de l'authentification des appareils, et du chiffrement. Il gère également les mises en veille des différents appareils. Ce gestionnaire de liaisons qui implémente les mécanismes de sécurité comme:
l'authentification
le pairage
la création et la modification des clés
le cryptage
L'interface HCI
Cette couche fournit une méthode uniforme pour accéder aux couches matérielles. Son rôle de séparation permet un développement indépendant du matériel et du logiciel.
Une fois que l'on peut communiquer avec le matériel, la méthode de communication est uniformisée quelque soit le type de matériel auquel on a affaire via la couche HCI (Host

Controller Interface). Cette interface est exhaustivement définie dans la norme Bluetooth. Elle est composée de commandes et d'évènements. Le périphérique envoie des commandes à la puce Bluetooth et reçoit des évènements en retour.
La couche L2CAP
Le L2CAP est le protocole minimal d'échange de données de la spécification Bluetooth. On peut écrire des applications Bluetooth utilisant le L2CAP pour communiquer entre elles, via des dispositifs Bluetooth.
C'est également en utilisant le L2CAP que sont implémentées les plus hautes couches du protocole Bluetooth tels que le SDP (pour les protocoles de recherche de services) ou RFCOMM (qui a pour but l'émulation d'une liaison série entre deux dispositifs Bluetooth).
Le L2CAP est un protocole relativement simple à mettre en œuvre. Bien qu'il existe un mode non connecté au L2CAP pouvant être utilisé pour l'envoi de paquets en diffusion (broadcast) sur le réseau Bluetooth, on l'utilise majoritairement en mode connecté.

Bluetooth - Synopsis de l'établissement de la connexion

Principe général
L'établissement d'une connexion entre deux périphériques Bluetooth suit une procédure relativement compliquée permettant d'assurer un certain niveau de sécurité, selon le déroulé suivant :
Mode passif
Phase d'inquisition : découverte des points d'accès
Synchronisation avec le point d'accès (paging)
Découverte des services du point d'accès
Création d'un canal avec le point d'accès
Pairage à l'aide d'un code PIN (sécurité)
Utilisation du réseau
En utilisation normale un périphérique fonctionne en «mode passif», c'est-à-dire qu'il est à l'écoute du réseau.
L'établissement de la connexion commence par une phase appelée «phase d'inquisition» (en anglais «inquiry»), pendant laquelle le périphérique maître envoie une requête d'inquisition à tous les périphériques présents dans la zone de portée, appelés points d'accès. Tous les périphériques recevant la requête répondent avec leur adresse.
Le périphérique maître choisit une adresse et se synchronise avec le point d'accès selon une technique, appelée paging, consistant notamment à synchroniser son horloge et sa fréquence avec le point d'accès.
Un lien s'établit ensuite avec le point d'accès, permettant au périphérique maître d'entamer une phase de découverte des services du point d'accès, selon un protocole appelé SDP (Service Discovery Protocol).
A l'issue de cette phase de découverte de services, le périphérique maître est en mesure de créer un canal de communication avec le point d'accès en utilisant le protocole L2CAP.
Selon les besoins du service, un canal supplémentaire, appelé RFCOMM, fonctionnant au-dessus du canal L2CAP pourra être établi afin de fournir un port série virtuel. En effet certaines applications sont prévues pour se connecter à un port standard, indépendant de tout matériel. C'est le cas par exemple de certaines applications de navigation routière prévues pour se connecter à n'importe quel dispositif GPS Bluetooth.
Cas particulier du pairage
Il se peut que le point d'accès intègre un mécanisme de sécurité, appelé pairage (en anglais pairing), permettant de restreindre l'accès aux seuls utilisateurs autorisés afin de garantir un certain niveau d'étanchéité du picoréseau. Le pairage se fait à l'aide d'une clé de chiffrement communément appelée «code PIN[1]» Le point d'accès envoie ainsi une requête de pairage au périphérique maître. Ceci peut la plupart du temps déclencher une intervention de l'utilisateur pour saisir le code PIN du point d'accès. Si le code PIN reçu est correct, l'association a lieu.
En mode sécurisé, le code PIN sera transmis chiffré à l'aide d'une seconde clé, afin d'éviter tout risque de compromission.
Lorsque le pairage est effectif, le périphérique maître est libre d'utiliser le canal de communication ainsi établi.

A noter : comme une adresse Bluetooth est permanente, le pairage est préservé même si le nom Bluetooth est changé.
De façon plus précise, avec les normes antérieures à la 2.1, les appareils utilisent un code PIN pour le pairage entre deux appareils. Bien que le code puisse comprendre entre 1 et 16 octets, habituellement on travaille sur 4 octets.
Le protocole utilise 3 étapes pour initialiser une connexion :
Création d'une clé d'initialisation : le maître envoie un nombre aléatoire (128bits) à l'esclave. L'esclave envoie son adresse BD_ADDR (48bits). À partir de ce nombre aléatoire, de la BD_ADDR et du code PIN (entré sur les deux périphériques) une clef d'initialisation est calculée.
Création d'une clef "de lien" (Link Key) : chacun des 2 périphériques utilise la clef d'initialisation pour coder un nombre aléatoire (128bits). Les 2 nombres aléatoires obtenus sont échangés, et un algorithme permet de créer une clef de liens à partir de ces 2 nombres.
L'authentification elle-même se déroule en utilisant un quatrième nombre aléatoire : une valeur 32bits (SRES) est créée via un algorithme, elle utilise la clef de lien, le nombre aléatoire et l'adresse BD_ADDR. Les périphériques vérifient mutuellement que les valeurs SRES sont identiques.

---

[1] Personal Information Number

Pour aller plus loin…

Bluetooth - Présentation

Présentation

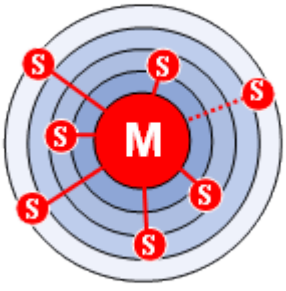
Origines
Bluetooth est une spécification de l'industrie des télécommunications qui utilise une technologie radio courte distance destinée à simplifier
les connexions entre les appareils électroniques.

Son nom est directement inspiré du roi danois Harald I^{er} surnommé Harald Blåtand («à la dent bleue»), connu pour avoir réussi à unifier les États du Danemark, de Norvège et de Suède. Le logo de Bluetooth, est d'ailleurs inspiré des initiales en alphabet runique de *Harald Blåtand*.
Les dates clef
1994 : création par le fabricant suédois Ericsson
1998 : plusieurs grandes sociétés (Agere, IBM, Intel, Microsoft, Motorola, Nokia et Toshiba) s'associent pour former le Bluetooth Special Interest Group (SIG)
juillet 1999 : sortie de la spécification 1.0
Le 28 mars 2006, le « Bluetooth Special Interest Group » (SIG) annonce la prochaine génération de la technologie sans fil **Bluetooth**, qui sera capable d'assurer des débits cent fois supérieurs à la version actuelle, passant donc de 1 Mb/s à 100 Mb/s (soit 12,5 Mo/s). La nouvelle norme incorporera une technologie radio, connue comme l'ultra wideband ou UWB.
Les différentes versions de Bluetooth
La version 1.0 du Bluetooth a été très peu utilisée. Elle a été très vite remplacée par la version 1.0b, qui a été la première version utilisée commercialement. La seule différence entre les périphériques 1.0 et 1.0b c'est que l'interopérabilité entre marques est meilleure avec la version 1.0b.

La version 1.1 du Bluetooth est une mise à jour mineure, qui apporte peu de choses : quelques corrections de bug par rapport à la version 1.0b, la possibilité d'utiliser des canaux non cryptés et l'ajout d'un signal permettant de connaître la puissance de réception.
La version 1.2 apporte une vitesse pratique un peu supérieure et une meilleure résistance aux interférences (en séparant bien les sauts de fréquences). C'est la version la plus courante dans les dongles PC.
La version 2.0 est rétro-compatible avec les versions 1.x, et réduit la consommation des périphériques tout en améliorant la fiabilité des transferts (en utilisant une meilleure correction des erreurs).
La version 2.0 + EDR permet une plus grande vitesse pratique, jusque 2,1 mégabits (au lieu de 0,7 mégabit avec les versions antérieures). Elle est rarement implémentée pour le moment, que ce soit dans les téléphones ou dans les ordinateurs (l'exception étant Apple, qui équipe tous les Macs en Bluetooth 2.0 EDR de série).
Enfin, la version 2.1 + EDR améliore certains points, dont le jumelage. Avec cette version, l'appairage est plus simple et plus rapide. De plus, quelques améliorations de sécurité sont présentes, ainsi qu'un mode de connexion qui permet des liaisons à très courte portée.
Technique
Fréquence radio
Le standard Bluetooth, à la manière du wifi utilise la FHSS (*Frequency Hopping Spread Spectrum*, en français *étalement de spectre par saut de fréquence* ou *étalement de spectre par évasion de fréquence*), consistant à découper la bande de fréquence (2.402 – 2.480 GHz) en 79 canaux (appelés *hops* ou *sauts*) d'une largeur de 1MHz, puis de transmettre en utilisant une combinaison de canaux connue des stations de la cellule. Ainsi, en changeant de canal jusqu'à 1600 fois par seconde, le standard Bluetooth permet d'éviter les interférences avec les signaux d'autres modules radio.
Exemples de bandes de fréquences radio connues :

Type	**Fréquence**
Radio AM	535 kHz-1.6 MHz
Radio FM	88 MHz-108 MHz
GPS	1.227 GHz-1.575 GHz

Appareils & Fonctionnement maître / esclave
Un matériel qui ne supporte que des connexions point à point ne peut se connecter qu'à un appareil à la fois alors qu'un matériel multipoint peut se connecter à plusieurs appareils.
Le standard Bluetooth est basé sur un mode de fonctionnement maître/esclave. Ainsi, on appelle «**picoréseau**» le réseau formé par un périphérique et tous les périphériques présents dans son rayon de portée. Il peut coexister jusqu'à 10 picoréseaux dans une même zone de couverture. Un maître peut être connecté simultanément à un maximum de 7 périphériques esclaves actifs (255 en mode *parked*). En effet, les périphériques d'un picoréseau possèdent une adresse logique de 3 bits, ce qui permet un maximum de 8 appareils. Les appareils dits en mode *parked* sont synchronisés mais ne possèdent pas d'adresse physique dans le picoréseau.



En réalité, à un instant donné, le périphérique maître ne peut se connecter qu'à un seul esclave à la fois. Il commute donc très rapidement d'un esclave à un autre afin de donner l'illusion d'une connexion simultanée à l'ensemble des périphériques esclaves.
Le standard Bluetooth prévoit la possibilité de relier deux picoréseaux entre eux afin de former un réseau élargi, appelé «**réseau chaîné**», grâce à certains périphériques faisant office de pont entre les deux picoréseaux.

Pour aller plus loin…