Bluetooth : technologie et potentiel industriel

M. Van DROOGENBROECK et J.-M. WAGNER

Mai 2002

Table des matières

Chapitre 1

Le contexte normatif

1.1 Origine de la technologie Bluetooth

`Bluetooth` est une norme de transmission sans fil dite *ouverte*, c'est-à-dire que tout constructeur peut concevoir un appareil utilisant cette norme pour autant que celui-ci réussisse tous les tests de certification spécifié par la norme. Cette liberté a été introduite dans le but de faciliter l'adoption de Bluetooth.

Un objectif important du design de la norme Bluetooth visait à permettre son utilisation partout dans le monde. Pour ce faire, elle utilise une bande de fréquence qui ne nécessite pas l'octroi d'une licence et qui est libre d'utilisation partout dans le monde.

Un autre point crucial du développement de la norme Bluetooth fut de privilégier l'interopérabilité afin que des périphériques d'origine différente puissent fonctionner par paire et sans procédure d'établissement complexe.

1.1.1 Origine du nom Bluetooth

En général, la plupart des nouvelles technologies se voient attribuer un nom relatif à la technologie associée ou à leur application. Le choix de la dénomination de Bluetooth fait exception à cette règle. Le nom "Bluetooth" est la traduction littérale du nom d'un personnage historique, le roi Harald BLATAND, qui fut Roi du Danemark de 940 à 985 Av. J-C et qui unifia le Danemark et la Norvège.

1.1.2 Le SIG (Bluetooth Special Interest Group)

La technologie de communication sans fil Bluetooth a été conçue par des ingénieurs de la société Ericsson qui ont voulu promouvoir une technologie globale de communication sans fil pour

courtes distances. En 1994, ERICSSON a lancé un projet pour étudier la faisabilité d'une technologie de communication à faible coût et à faible consommation avec pour objectif de supprimer les câbles entre les téléphones mobiles et leurs accessoires.

Pour en favoriser l'adoption, les ingénieurs d'Ericsson décidèrent de former un groupement d'industriels et d'ouvrir l'accès aux spécifications. Ainsi, en 1998, plusieurs compagnies informatiques et d'équipements de télécommunications formèrent le *Bluetooth Special Interest Group* (`SIG`) avec pour unique but de développer une telle norme. Les cinq compagnies à l'origine du SIG furent ERICSSON, INTEL, IBM, NOKIA et TOSHIBA.

Au cours du développement de la norme, de nombreuses autres sociétés joignirent le SIG en tant qu'*adopteurs*, ceci dans le but d'avoir accès aux spécifications et de pouvoir développer des produits portant officiellement le nom Bluetooth. Aujourd'hui, le SIG compte plus de 1800 membres adopteurs, parmi lesquels des universités, des sociétés actives dans les domaines de l'électronique, des télécommunications ou de l'informatique.

Le SIG est organisé en plusieurs groupes de travail ayant chacun pour fonction le développement spécifique d'une partie de la norme ou le suivi d'un service :

- Le groupe *"Interface Air"* s'occupe essentiellement de l'interface radio
- Le groupe *"Software"* s'occupe du développement des protocoles de la norme
- Le groupe *"Interopérabilité"* s'occupe des profils de la norme
- Le groupe *"Certification"* s'occupe de la définition des tests et processus de certification
- Le groupe *"Juridique"* s'occupe des affaires légales comme par exemple les droits de la propriété intellectuelle
- Le groupe *"Marketing"* est chargé de promouvoir la norme Bluetooth

Les groupes de grande taille, comme le groupe *"Software"*, sont divisés en sous-groupes de travail. La coordination des groupes ainsi que la direction du SIG est réalisée par un comité de représentants de chacune des compagnies promotrices de Bluetooth.

Le but original du SIG fut de développer, aussi rapidement que possible, une norme ouverte suffisamment complète pour permettre une implémentation aisée et rapide. Si bien que les volumes 1 et 2 constituant la norme Bluetooth V1.0, publiées en 1999, contenaient à eux deux plus de 1500 pages. Mais le SIG ne s'est pas contenté de fournir des notes techniques relative à la norme ; il a également fourni toute une gamme de directives permettant l'implémentation de cette nouvelle technologie. Ces directives sont connues sous le nom de *profils d'utilisation* de la norme Bluetooth. En plus du corps de la norme et des profils d'utilisation, le `SIG` à établi une série de tests de compatibilité et de certifications permettant d'assurer la conformité d'une implémentation particulière. Ces mesures ont pour but d'assurer l'interopérabilité entre différents équipements ; elles répondent au problème de compatibilité qui s'est produit lors de la conception des premiers produits et prototypes.

Un descriptif complet du SIG est disponible sur le site officiel :

`http://www.bluetooth.com/`

1.2 L'IEEE et les autres groupes de normalisation

L'IEEE[1] a produit plusieurs normes pour les réseaux LANs. Ces normes, bien connues sous l'appellation IEEE 802, incluent les spécifications des protocoles CSMA/CD (détection de collisions), *Token bus* (bus à jeton) et *Token Ring* (anneau à jeton). Les réseaux locaux se distinguent par trois caractéristiques : leur taille, leur technologie et leur topologie.

Un groupe de travail de l'IEEE travaille sur la normalisation de la spécification Bluetooth. Ce groupe est l'IEEE 802.15 TG1 qui a pour but de développer un standard de `WPAN` basé sur la norme Bluetooth V1.1. L'état actuel de ces travaux est accessible à la page web `http://www.ieee802.org/15/pub/TG1.html`.

1.3 Évolution future

La première version de la norme Bluetooth, la version V1.0, est apparue en 1999. La version 1.1 de la norme a été fournie en 2001 et comprend à certain nombre de corrections apportées à la version 1.0 ainsi qu'un certain nombre d'éclaircissements. Les différences essentielles entre les versions 1.0 et 1.1 sont une plus grande fiabilité et interopérabilité.

Aujourd'hui, les groupes de travail du SIG continuent le développement de la norme Bluetooth dans trois directions particulières :

- la correction et la clarification de la version V1.1
- le développement de nouveaux profils d'utilisation
- l'évolution du cœur de la norme afin d'obtenir de meilleures performances. Cette évolution devrait essentiellement concerner la couche physique (constituée des couches *radio* et *baseband*, cf. supra)

Dans les années qui viennent, le développement de nouveaux profils par des sociétés "adopteurs" devrait favoriser l'apparition d'implémentations de Bluetooth optimisées pour des applications spécifiques. La version future (version 2.0) de la norme est susceptible de fournir des taux de transmission beaucoup plus élevé (allant de 2 à 10 Mb/s) et des options axées sur des applicatifs multimédia.

[1] http://www.ieee.org

Chapitre 2

Description de la norme Bluetooth

2.1 Contexte : équipements concernés et exemple simple d'utilisation

La technologie Bluetooth a été conçue pour des communications de type radio-fréquence (RF), pour courte distance (typiquement 10m), de faible coût et à faible consommation.

Un exemple d'utilisation typique consiste à remplacer tous les câbles reliant un ordinateur à ses périphériques (imprimantes, souris, clavier, scanner, ...) par des liaisons radio, ce qui réduit l'encombrement autour de la machine et permet une meilleure disposition des différents périphériques. Certains périphériques comme l'imprimante ou le scanner peuvent même être utilisés par plusieurs ordinateurs sans nécessiter une connectique élaborée. Le type de données transmises peut donc aussi bien être de la voix que des données numériques.

Dans l'optique d'un remplacement des câbles, il a fallu faire en sorte que le coût de cette nouvelle technologie n'excède pas celui des câbles. De plus, comme les appareils visés sont généralement portables (GSM, PC portable, écouteurs, microphone, ...), le module Bluetooth doit être de petite taille et donc de consommation réduite.

2.2 Aspect logique des transmissions : modèles de référence

La communication passe obligatoirement par la mise en réseau des terminaux. Cette dernière nécessite alors l'établissement de conventions claires et non ambiguës, d'autant plus qu'on assiste à un accroissement de l'interopérabilité des réseaux informatiques et des réseaux de télécommunications.

En transmission de données, il existe plusieurs architectures dont les principales sont l'architecture provenant de la normalisation de l'ISO que l'on appelle *Open System Interconnection* (OSI) et l'architecture utilisée sur Internet baptisée *TCP/IP*, du nom des deux principaux protocoles qui la constituent.

2.2.1 Modèle de référence OSI

Le principe adopté dans la conception des réseaux est d'être le plus indépendant possible des supports physiques et de regrouper les fonctions de communication en catégories. Le modèle de référence développé par l'ISO[1] comporte 7 couches ; la figure 2.1 montre la communication entre deux ordinateurs à travers un réseau suivant le modèle `OSI`.

Les trois couches inférieures sont liées au réseau ; elles concernent les mécanismes de communications entre ordinateurs. Les trois couches supérieures gèrent les aspects propres aux applications. Au centre, la couche transport sert de tampon entre les deux autres séries de couches.

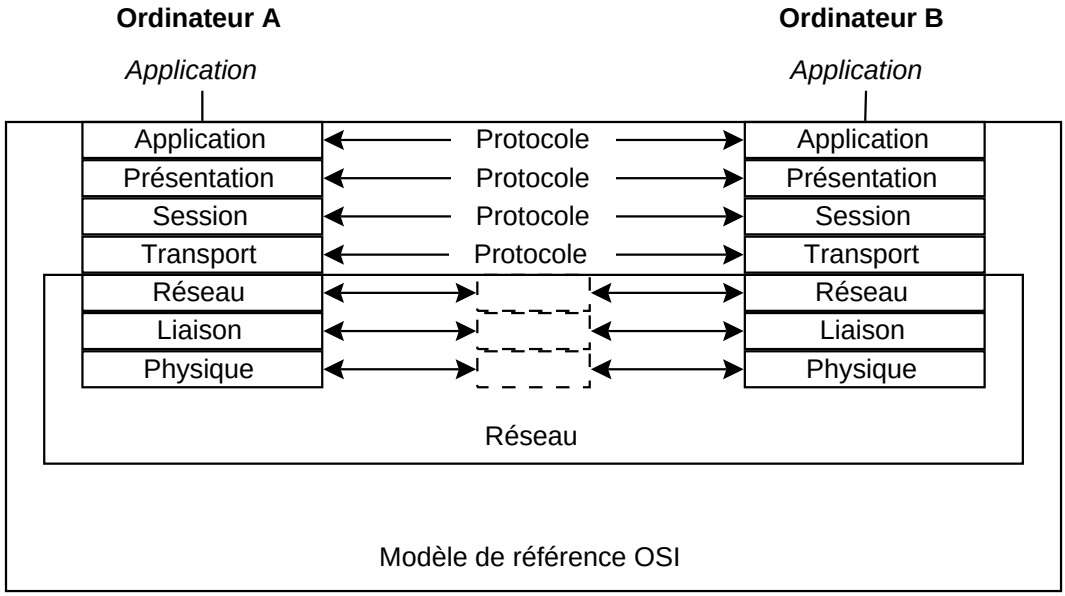

FIG. 2.1 – Structure générale du modèle OSI.

Les concepts architecturaux utilisés pour décrire le modèle de référence sont décrits dans la norme 7498–1. Le concept d'architecture en couches demande la définition de trois objets pour chaque niveau N :

– le *service*. Il correspond aux événements et aux primitives associées, à mettre en place pour rendre un service au niveau supérieur, c'est-à-dire au niveau $N + 1$;
– le `protocole`. Le protocole de niveau N définit un ensemble de règles nécessaires pour que le service de niveau N soit réalisé. Ces règles définissent les mécanismes qui vont permettre de transporter les informations d'un niveau N au niveau N d'une autre machine. En particulier, le protocole N va proposer les règles pour contrôler l'envoi des données ;
– les points d'accès au service N (*Service Access Point* ou *SAP* en anglais). Les points d'accès au service N sont situés à la frontière entre les couches $N + 1$ et N. Les services N sont fournis par une entité N à une entité $N + 1$ à ces points d'accès aux services N.

[1] http://www.iso.ch

Ainsi, chaque couche fournit une série de *services* à la couche supérieure et utilise les services fournis par la couche qui lui est inférieure. Par exemple, la couche transport permet la transmission de messages indépendants du réseau au niveau de la couche session et s'appuie sur la couche réseau pour transmettre ses messages à la couche transport d'un autre ordinateur. Concrètement donc, la couche masque l'implémentation des couches inférieures de sorte que l'application soit indépendante du réseau. La figure 2.2 reprend respectivement les fonctionnalités principales et services de l'ensemble des couches.

Les couches liées au réseau sont importantes et méritent quelques explications supplémentaires ; par ailleurs, leur mode de fonctionnement dépend du réseau physique auquel est raccordé l'ordinateur. D'une manière générale, la couche réseau est responsable de l'établissement et de la libération d'une connexion. Elle comprend des fonctionnalités comme le `routage`, aussi appelé *adressage*, et parfois le contrôle du débit. Comme le dit sa dénomination, la couche liaison veille sur l'état de la connexion. Elle se charge de la détection d'erreur et de la retransmission de messages si nécessaire. Elle offre deux types de service :

1. Sans connexion permanente, *connectionless* en anglais. Ce type de connexion traite chaque trame d'information comme une unité autonome transmise sans garantie d'arriver à destination. De plus, une trame incorrecte à l'arrivée est simplement ignorée. Le réseau Internet fonctionne suivant ce mode au niveau de la couche 3 (couche réseau). On peut y remédier par les couches des niveaux supérieurs ; ainsi, le protocole `TCP` implémente un mécanisme de transmission avec accusé de réception.
2. Avec connexion permanente, *connection oriented* en anglais. Il s'agit d'un mode de connexion, aussi appelé *mode* `circuit`, qui garantit une permanence dans le trajet utilisé pour la transmission de l'information.

Quant à la couche physique, elle concerne les interfaces entre l'équipement et le réseau. La norme `Ethernet` qui décrit principalement l'interface avec un réseau local correspond à la couche physique.

Le modèle OSI a été développé pour servir de cadre aux activités de normalisation relatives à la communication entre ordinateurs. Il n'a jamais eu pour but d'associer un standard unique à chacune des couches du modèle. D'ailleurs, la pratique a conduit à des familles de standards par niveau.

2.3 Modèle Bluetooth

Tout comme la plupart des techniques de communications actuelles, la norme de communication Bluetooth repose sur un découpage du processus de communication en différentes couches ayant chacune sa fonctionnalité propre.

La figure 2.3 représente un schéma bloc de la pile de protocoles correspondant à la norme Bluetooth. Les couches basses de la pile correspondent essentiellement à tout ce qui concerne l'aspect

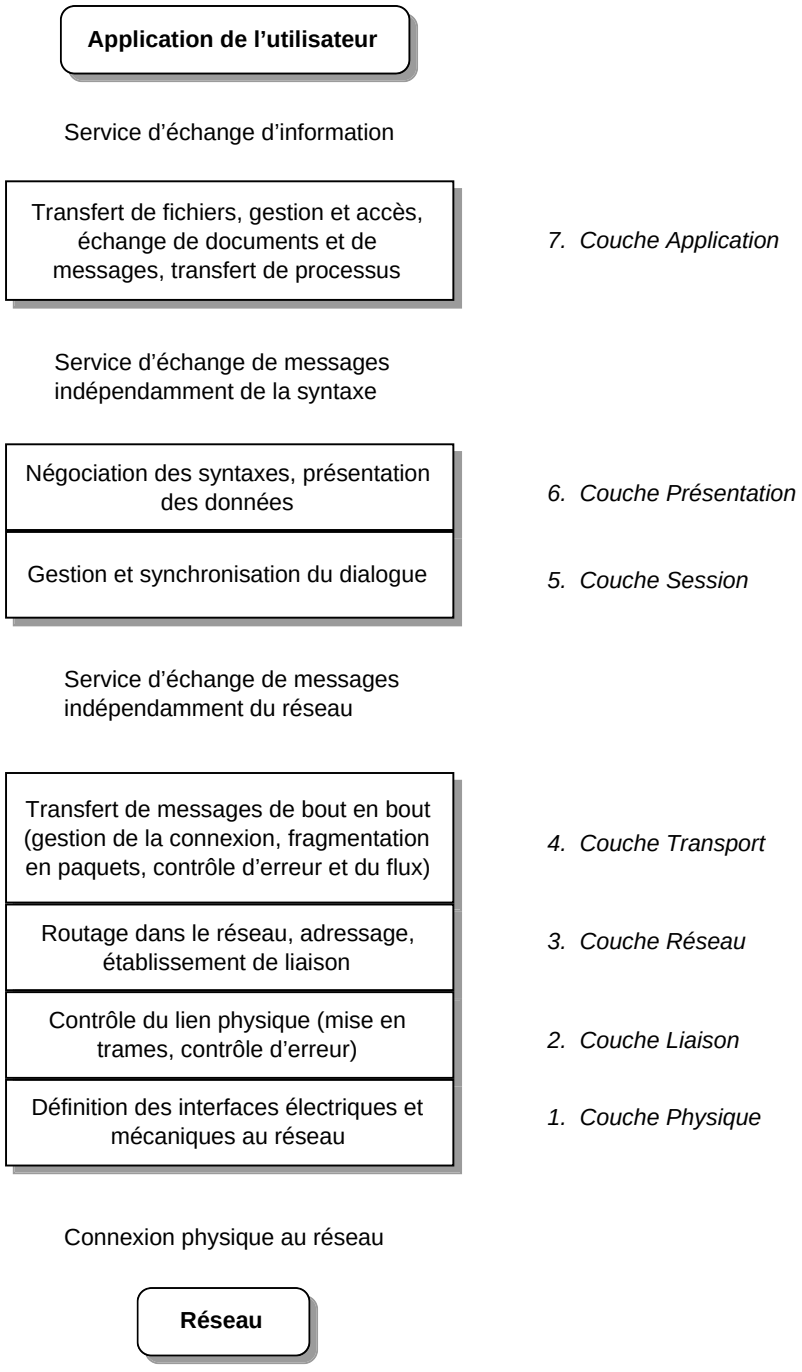

FIG. 2.2 – Résumé des principales fonctions du modèle OSI.

physique de la communication comme par exemple le support de transmission ou la modulation utilisée. Les couches supérieures concernent l'aspect logiciel de la communication comme par exemple le type d'application pour laquelle la communication est envisagée (transfert de données, téléphonie, ...).

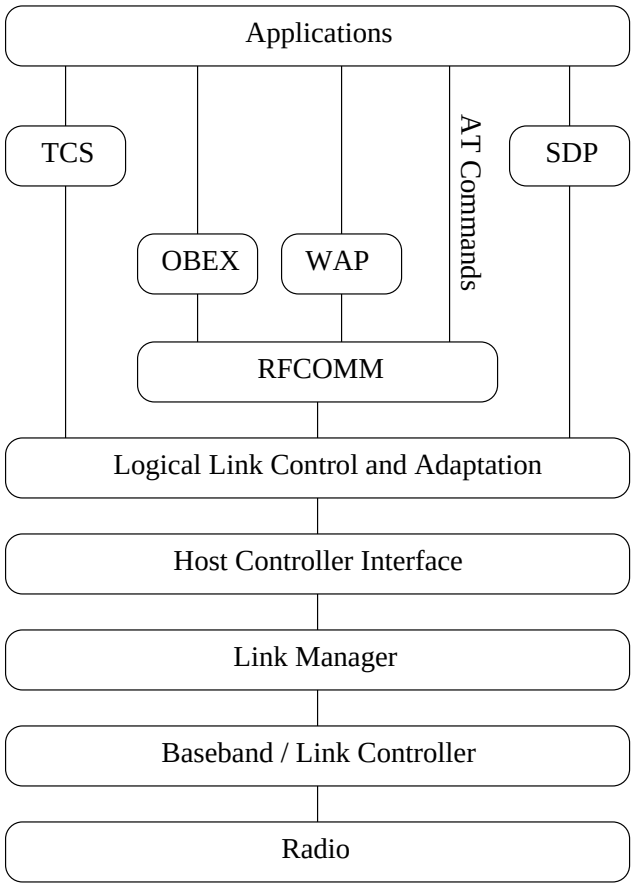

FIG. 2.3 – La pile de protocoles Bluetooth (d'après [1, page 6]).

Les fonctions de chacune de ces couches sont détaillées, brièvement, ci-après.

- La couche *"radio"* est responsable de la modulation et de la démodulation des données en vue de la transmission sur le canal.
- La couche *"*`Baseband`*/Link Controller"* contrôle la couche physique *"radio"*, assemble les paquets de données sous forme de trames et contrôle la technique du saut de fréquences (*"Frequency Hopping"*).
- La couche *"Link manager"* (`LM`) contrôle et configure les liens avec d'autres périphériques Bluetooth.
- La couche *"Host Controller Interface"* (`HCI`) s'occupe des communications entre un hôte et un périphérique Bluetooth.
- La couche *"Logical Link Control and Adaptation"* (`L2CAP`) multiplexe les données provenant des couches supérieures et réalise des conversions entre paquets de tailles différentes.

– La couche RFCOMM fournit une interface série du type RS232 afin d'en assurer la compatibilité.
– Les WAP et OBEX constituent une interface vers les protocoles des couches supérieures.
– le *"Service Discovery Protocol"* (SDP) permet à un périphérique Bluetooth de découvrir les services fournis par un autre périphérique Bluetooth.
– Le *"Telephony Control Protocol Specification"* (TCS) fournit un service de téléphonie.

La figure 2.4 fournit une comparaison entre les couches de la pile de protocoles de Bluetooth et les couches du modèle OSI de référence. Cette comparaison permet de mettre en évidence la division des tâches et des responsabilités entre les différentes couches de la pile Bluetooth.

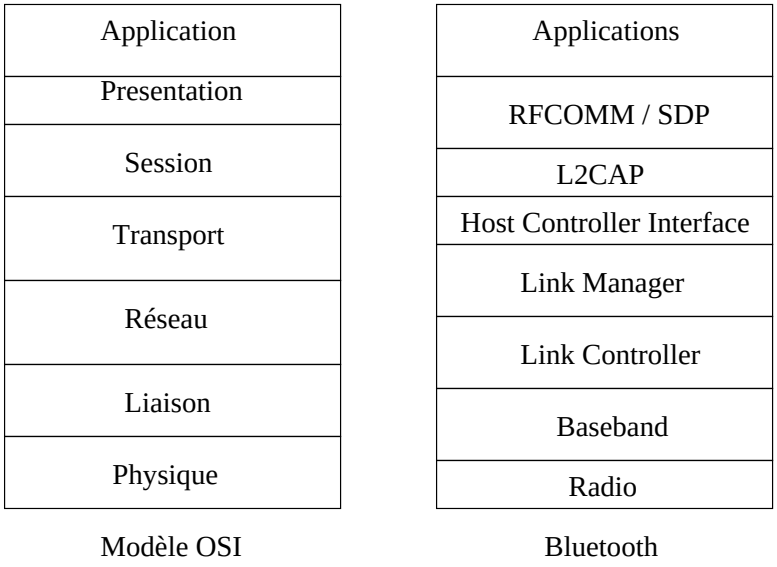

FIG. 2.4 – Le modèle OSI de référence et Bluetooth.

Tous les équipements ne doivent pas implémenter la totalité des couches. Pour permettre de sélectionner des jeux de protocoles cohérents en vue de certaines applications, le SIG a défini des *profils d'utilisation* (profile en anglais dans la terminologie *ad hoc*). Les profils d'utilisation Bluetooth fournissent les règles d'utilisation de la pile de protocoles par une application particulière. Nous reviendrons plus en détail sur les notions de profils à la section 2.6.

2.4 Aspects matériels

2.4.1 Interface radio

L'interface radio constitue une partie cruciale dans l'implémentation de la technologie Bluetooth. Bluetooth fonctionne à la fréquence de $2,4\,[GHz]$, ce qui correspond à une longueur d'onde de $12,5\,[cm]$. Pour cette fréquence, un simple dipôle, constitué d'un bout de fil conducteur, suffit

comme antenne. Cependant, afin d'obtenir des performances optimales, le développement d'antennes sophistiquées est nécessaire. Selon les périphériques utilisés, différentes antennes doivent être envisagées. Un périphérique destiné à bouger régulièrement dans la pièce devra être muni d'une antenne à rayonnement isotrope dans le plan de la pièce afin de rester accessible par tous les autres périphériques quelle que soit sa position. Par contre, deux périphériques fixes pourront utiliser des antennes directionnelles. En pratique, on utilise le plus souvent des antennes omnidirectionnelles.

Les antennes les plus utilisées sont le dipôle, l'antenne planaire et l'antenne micro-ruban. Ces deux dernières peuvent être montées directement sur un circuit imprimé, voir même sur un processeur. L'avantage est de pouvoir diminuer l'encombrement et le coût du module.

Un mot à propos de la bande de fréquences couverte

Bluetooth fonctionne à la fréquence de $2,4\,[GHz]$, plus précisément de $2,4\,[GHz]$ à $2,4835\,[GHz]$, soit dans la bande `ISM` destinées à des utilisations Industrielles, Scientifiques et Médicales, et ne nécessitant aucune licence d'utilisation. L'utilisation de cette bande de fréquence (ISM) est néanmoins soumise à un certain nombre de contraintes comme :

– la limitation de la puissance émise,
– un gabarit sur le spectre du signal émis, et
– des spécifications précises quant au niveau des interférences produites.

Ces spécifications sont définies par les normes `ETSI` ETS 300-328 en Europe et `FCC` CFR47, partie 15 aux États-Unis. La bande de fréquence ISM va exactement de $2,4\,[GHz]$ à $2,4835\,[GHz]$ aux États-Unis, au Japon et en Europe sauf actuellement en France où elle diffère encore quelque peu. Suite aux démarches du SIG, la France devrait s'aligner sur les autres pays vers la fin 2003.

La bande de fréquence ISM est occupée par de nombreux utilisateurs dont les applications sont privées (téléphone sans fil, fermeture des portes de voitures à distances, ...) ou encore par des réseaux locaux sans fil (IEEE[2] `802.11`). D'autres générateurs de signaux dans cette bande de fréquence peuvent être les fours micro-ondes, lampes à vapeurs de sodium (éclairage des rues) qui contribuent au bruit ambiant d'une manière significative. La bande ISM n'est donc ni stable, ni fiable. Néanmoins, l'accès mondial à cette bande de fréquence ainsi que l'absence de licence présentent un avantage certain pour l'acceptation et l'expansion de la technologie Bluetooth.

La bande de fréquence ISM englobe la fréquence critique à $2,450\,[GHz]$ qui correspond à la première fréquence d'oscillation des molécules d'H_2O. C'est précisément la fréquence utilisée pour l'échauffement des aliments dans un four micro-onde. En raison du faible niveau d'émission des équipements, les applications utilisant la bande ISM sont considérées comme inoffensives.

[2] http://www.ieee.org

2.4.2 Étalement de spectre par saut de fréquences

L'utilisation de la bande ISM exige des choix technologiques particuliers pour contrer les interférences des signaux parasites. Dans le cas particulier de la norme Bluetooth, les concepteurs ont utilisé des techniques comme l'étalement de spectre par saut de fréquences, le contrôle adaptatif de la puissance et l'envoi de paquets de données relativement courts. Certains prétendent également que le saut de fréquences garantit un niveau élevé de sécurité mais cet argument est contestable.

La bande ISM est large de $83,5\,[MHz]$. Si l'on considère les bandes de garde et dans le cas particulier de Bluetooth, la bande de fréquence est divisée en 79 sous-bandes espacées de $1\,[MHz]$. Chacune de ces bandes offre un débit théorique brut maximum de $1\,[Mb/s]$, ce qui correspond donc à une efficacité spectrale de $1\,[b/s/Hz]$, soit une valeur assez typique pour ce type d'utilisation. Une communication se fait par saut de sous-bande en sous-bande via la technique de l'étalement de spectre par saut de fréquences, techniques appelée *"Frequency Hopping Spread Spectrum"* (FHSS). Concrètement, Bluetooth gère des trames longues $625\,[\mu s]$ et jusqu'à 1600 sauts de fréquence par seconde selon une séquence pseudo-aléatoire, ce qui permet de réduire considérablement l'effet des interférences.

2.4.3 Modulation

La modulation utilisée dans chacune des sous-bandes est le *Gaussian Frequency Shift Keying* (GFSK). Avec cette modulation, on atteint bien $1\,[Mb/s]$ par sous-bande. Le bit 1 correspond à une déviation positive de la fréquence instantanée du signal modulé par rapport à la fréquence porteuse tandis que le bit 0 correspond à une déviation négative de la fréquence instantanée.

La modulation GFSK utilise un filtre gaussien pour adoucir les transitions de fréquence du signal modulé. Ceci rend la phase du signal modulé continue, réduit la largeur du spectre du signal et augmente l'efficacité spectrale. La norme Bluetooth spécifie une déviation de fréquence minimale (en valeur absolue) de $115\,[kHz]$.

2.4.4 Contrôle de la puissance d'émission

Le niveau de puissance transmise dans la bande ISM est majorée par les différents organismes régulateurs nationaux ou supranationaux. Aux États-Unis, les normes FCC permettent, dans la bande ISM, la transmission de signaux de puissance maximum égale à $1\,[mW] = 0\,[dBm]$ sans nécessiter l'utilisation de la technique d'étalement de spectre. Pour une émission de puissance supérieure, l'étalement de spectre est donc obligatoire. Grâce au saut de fréquences, Bluetooth est capable de fonctionner jusqu'à $20\,[dBm]$, ce qui permet une portée de $100\,[m]$.

La spécification Bluetooth définit 3 classes de puissance, comme indiqué à la table 2.1. La classe 3 est la plus répandue au sein des constructeurs car elle présente la plus faible consommation.

Classe	Puissance émise (max)	Portée $[m]$
1	100 mW (20 dBm)	100
2	2,5 mW (4 dBm)	20
3	1 mW (0 dBm)	10

TAB. 2.1 – Classes de puissance transmise.

Un contrôle de la puissance est réalisé par la transmission de signaux de contrôle. Le récepteur reçoit de l'émetteur un signal de référence appelé *Received Signal Strength Indicator* (`RSSI`), qui lui permet de jauger le niveau de puissance reçue. Si le niveau est très faible ou trop élevé, il renvoie un signal permettant à l'émetteur d'adapter son niveau de puissance à la communication en cours. Bien que ce processus de contrôle ne soit qu'optionnel pour les classes 2 et 3 (elle est obligatoire pour la classe 1), il est toujours préférable d'y recourir pour assurer une consommation minimale.

2.5 Schéma de fonctionnement temporel : chronogramme

Le fonctionnement de la communication Bluetooth est basée sur la technique du multiplexage temporel, *"Time Division Multiplexing"* (`TDM`), dont l'unité de base temporelle est une trame de longueur de $625\,[\mu s]$. Chaque périphérique Bluetooth peut être *maître* et *esclave* mais pas simultanément. Par définition :

– le périphérique *maître* est celui qui initialise une communication et,
– le périphérique *esclave* est celui qui répond au maître.

N'importe quel périphérique peut jouer le rôle du maître ou de l'esclave. En particulier, le même périphérique peut jouer le rôle du maître pour une communication et le rôle de l'esclave pour une autre communication.

Lors de l'établissement de la connexion, c'est le maître qui impose la synchronisation et la séquence de saut de fréquences. La figure 2.5 illustre le chronogramme d'une communication. Le maître transmet en premier lieu ; le terminal esclave est ensuite autorisé à transmettre. Le maître et l'esclave sont alors en communication sur le canal $C[n]$ pendant un laps de temps de $625\,[\mu s]$. Une unité de temps plus loin, les deux périphériques utilisent un autre canal, $C[n+1]$, déterminé par la séquence propre au maître. L'esclave transmet un accusé de réception au maître et attend la prochaine autorisation du maître. Celui-ci est alors libre de transmettre à nouveau ou de contacter un autre terminal esclave.

L'utilisation du saut de fréquences fournit les deux avantages suivants :

– *Sécurité* : la séquence des sauts (de canal en canal) est une séquence pseudo-aléatoire connue uniquement du maître et de l'esclave. Il est donc difficile, mais pas impossible, pour un récepteur quelconque d'écouter une communication.
– *Fiabilité* : si un perturbateur occasionne la perte d'un paquet sur le canal $C[n]$, celui-ci peut être retransmis sur un autre canal $C[n+m]$ qui lui ne sera plus perturbé.

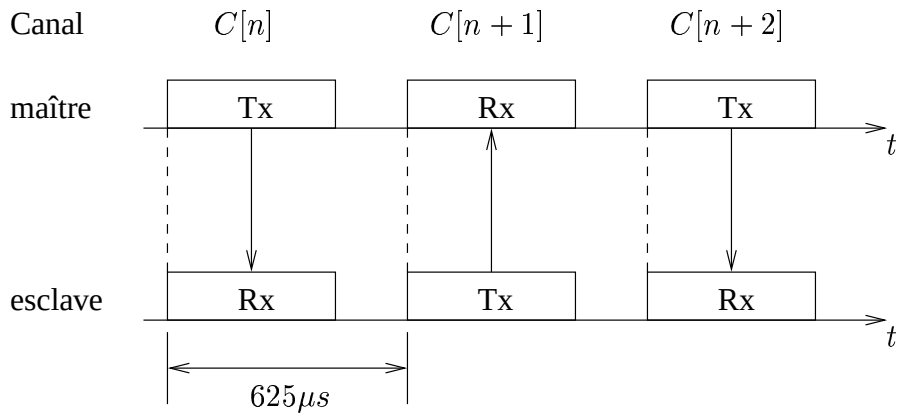

FIG. 2.5 – Chronogramme de la communication.

La norme Bluetooth définit des paquets de données dont la longueur correspond à 1, 3 ou 5 trames. Pour les paquets longs de 3 ($1875\,[\mu s]$) ou 5 ($3125\,[\mu s]$) trames, le canal reste le même pendant la transmission de toutes les trames constitutives du paquet, ce qui permet un plus haut débit de données mais se fait au détriment de la fiabilité.

Un maître peut communiquer avec plusieurs esclaves (jusque 7 esclaves actifs et 255 esclaves passifs[3]). Tous les esclaves communiquant avec le même maître constituent une entité appelée `piconet`. La figure 2.6 illustre la topologie logique d'une liaison point à point et point à multi-point entre maître et esclaves pour un piconet typique. Le diagramme de droite montre un maître avec 3 esclaves et qui est lui-même l'esclave d'un autre maître. L'ensemble forme ce qui est appelé un `scatternet`.

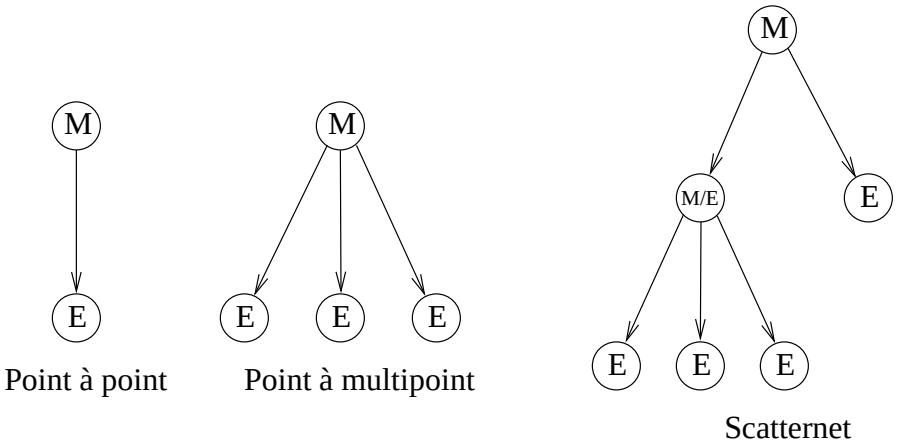

FIG. 2.6 – Piconets et scatternets. (M = Maître, E = Esclave)

Lors de l'accès à un canal, le terminal qui initie la connexion joue le rôle de maître. Ce rôle peut être remis en question en cours de communication. Il est important de remarquer que nombreuses

[3]Les notions d'esclaves *actifs* et *passifs* sont décrites à la section 2.9.

picocellules peuvent coexister. Ainsi, toutes les communications, même proches, peuvent ne pas passer toutes par le même maître. Bien entendu, dans ce cas, il y a le risque que deux picocellules utilisent par hasard la même bande de fréquences et se parasitent mutuellement. Heureusement, comme leurs séquences de saut de fréquences diffèrent, les deux communications utiliseront une autre bande de fréquences à l'instant d'après.

2.6 Notion de profil d'utilisation

Les profils d'utilisation, appelés `profile`, constituent une part importante de la spécification Bluetooth. Tout le volume 2 (en tout 452 pages !) des spécifications de la norme leur est en effet exclusivement consacré. Le but principal de la définition de profils est d'assurer l'interopérabilité entre tous les périphériques respectant la norme Bluetooth. Originellement, la notion de profil a été introduite par l'*International Organisation for Standardisation* (`ISO`/IEC TR1000). Ce concept a ensuite été repris par le `SIG` dans un souci de standardisation.

Les profils d'utilisations constituent, en quelque sorte, un mode d'emploi de la pile de protocoles Bluetooth. Chacun des profils décrit quelles parties de la spécification sont employées ainsi que la manière de les utiliser dans une application particulière. Néanmoins, ils ne constituent pas qu'une simple recommandation d'utilisation. En effet, pour être reconnu Bluetooth, un périphérique doit implémenter au moins un profil d'utilisation conformément à sa description telle que fournie dans le volume 2 de la norme. Ainsi, l'interopérabilité est assurée entre des périphériques Bluetooth provenant de constructeurs différents. En introduisant le concept de profil d'utilisation, les membres du SIG ont voulu favoriser l'intégration de Bluetooth dans toute une série d'appareils leur permettant de communiquer et de fonctionner ensemble. Par exemple, un casque audio respectant le profil d'utilisation *"Headset"* fabriqué par la société A pourra interagir avec un téléphone cellulaire spécifié Bluetooth fabriqué par la société B.

Le volume 2 de la norme Bluetooth est découpé en section, chacune d'elles décrivant un profil d'utilisation. Tous les profils d'utilisation sont décrits selon la même structure, à savoir :

– un paragraphe décrivant ce que le profil réalise
– une liste décrivant le contenu du profil
– une indication des dépendances avec d'autres profils
– les symboles et conventions utilisés
– quelles parties de la pile de protocoles sont utilisées
– le corps du profil décrivant comment il utilise les protocoles des différentes couches de la pile
– des annexes et références.

Le premier profil d'utilisation décrit dans le volume 2 de la norme est le *"Generic Access profile"* (GAP). Il constitue le profil d'utilisation de base. En effet, tout périphérique Bluetooth doit au moins implémenter ce profil. Il permet aux périphériques Bluetooth à proximité suffisante de se détecter et de s'interconnecter au niveau physique (*Radio* et *Baseband*). Il définit également les procédures de base pour une liaison sécurisée. Ce profil est considéré comme le profil de base car tout autre profil est une adaptation du GAP. Tout autre profil hérite en quelque sorte des

fonctionnalités du GAP. On parle également de dépendance entre profils. Un profil dépend d'un autre profil s'il utilise des fonctionnalités de ce dernier.

Un exemple de profil d'utilisation héritant du GAP est le *"Service Discovery Application Profile"* (SDAP) (section 2 du volume 2 de la norme). Il hérite des fonctionnalités du GAP mais permet à un périphérique Bluetooth de découvrir les profils implémentés sur un autre périphérique Bluetooth. La figure 2.7 (en haut à gauche) illustre le SDAP. Sur cette figure, le grand rectangle représente le GAP. Le rectangle contenant le SDAP se trouve dans ce grand rectangle, ce qui signifie que le SDAP hérite des fonctionnalités du GAP.

Un autre exemple de profil d'utilisation héritant des fonctionnalités du GAP est le *"Serial Port Profile"* (SPP). Celui-ci permet d'émuler une liaison série entre périphériques Bluetooth. En fait, tous les profils Bluetooth sont organisés hiérarchiquement en groupe de profils, chacun des profils d'un groupe héritant d'un profil plus simple. La figure 2.7 illustre la situation. Par exemple, le profil *"Fax profile"* hérite des fonctionnalités du profil *"Serial Port Profile"* qui hérite lui-même des fonctionnalités du GAP. Un périphérique Bluetooth peut implémenter plusieurs profils simultanément mais tout périphérique Bluetooth doit impérativement implémenter le GAP.

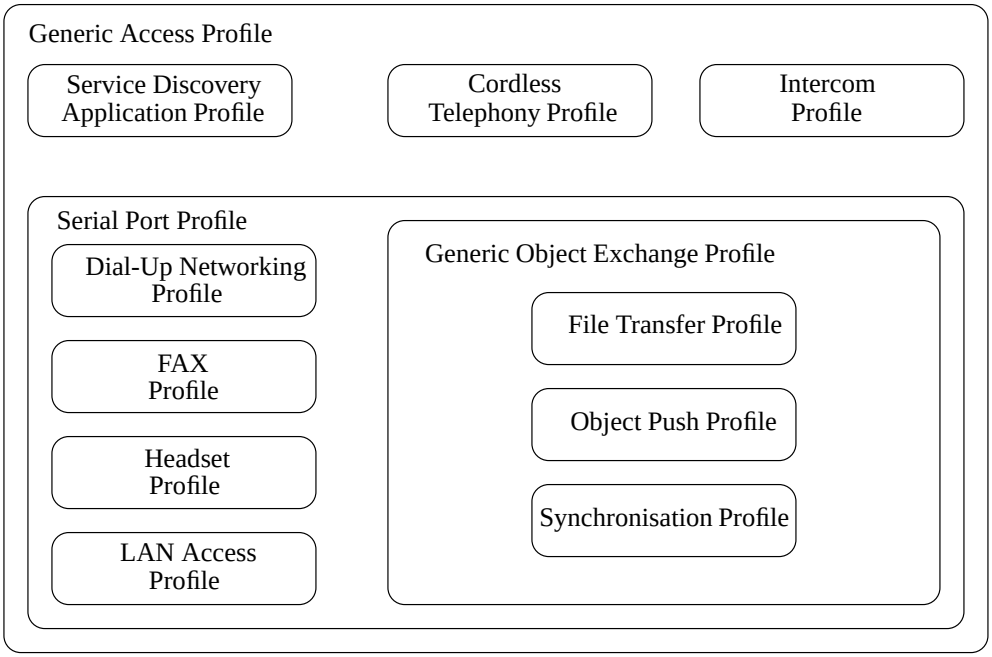

FIG. 2.7 – Les profils d'utilisation Bluetooth (Version 1.0b).

Actuellement, le volume 2 de la norme Bluetooth V1.1 contient 13 profils d'utilisation. Ceux-ci sont tous repris à la figure 2.7. Décrivons brièvement les profils non encore cités :

– Le *"Cordless Telephony Profile"* (CTP) : ce profil implémente le "téléphone 3 en 1". Il fournit en autre un service de téléphonie sans fil (privé ou professionnel) et un service de téléphonie cellulaire permettant de relier un téléphone sans fil au réseau téléphonique classique par l'intermédiaire d'une station de base.

– L' *"Intercom Profile"* : ce profil complète le profil précédent pour le téléphone "téléphone 3 en 1". Il en implémente la partie intercom, ou le service plus populaire "talkie-walkie".
– L' *"Headset Profile"* (HS) : ce profil offre un service de casque audio. Un exemple simple consiste à utiliser un casque audio Bluetooth pour communiquer avec un PC ou un GSM.
– Le *"Dial-Up Networking Profile"* (DUN) : ce profil émule un `modem` permettant, par exemple, à un PC de communiquer sans fil avec un modem relié au réseau téléphonique.
– Le *"Fax Profile"* : ce profile offre un service "Fax". Il permet, par exemple, à un PC de communiquer avec un modem afin d'envoyer un fax.
– Le *"LAN Access Profile"* : ce profil offre un service d'accès à un réseau local.
– Le *"Generic Object Exchange Profile"* : ce profil offre un service d'échange d'objets. Ce profil peut être utilisé, par exemple, entre ordinateurs portables pour échanger des informations.
– L' *"Object Push Profile"* : ce profile permet, par exemple, à un périphérique Bluetooth d'insérer un object dans la boîte aux lettres électronique d'un autre périphérique Bluetooth. L'objet peut alors être une carte de visite ou un rendez-vous.
– Le *"File Transfert Profile"* : ce profil offre un service de transfert de fichier. Il permet, par exemple, à un PC portable Bluetooth de naviguer dans le système de fichiers d'un autre PC portable Bluetooth.
– Le *"Synchronization Profile"* : ce profil offre un service d'échange de données administratives entre périphériques Bluetooth comme par exemple des emplois du temps, des listes de numéros de téléphones, ...

Vu le nombre croissant d'utilisateurs et de développeurs de périphériques Bluetooth, la prochaine version de la norme Bluetooth (V2.0) devrait comporter des nouveaux profils d'utilisation prenant en compte les nouveaux desiderata.

2.7 Protocoles

Les réseaux Bluetooth sont par essence non câblés et auto-configurables ; les appareils en présence peuvent évoluer au cours du temps et entrer ou sortir de la zone d'influence. Dès lors, il se peut que le maître d'un piconet ignore à quel nouveau périphérique il a affaire. Entre autres, il ne connaît pas les fonctionnalités d'un périphérique entrant dans son rayon d'action. Afin de remédier à ce problème, la norme Bluetooth prévoit un mécanisme appelé *"Service Discovery Protocol"* (SDP) qui permet à un périphérique Bluetooth de se connecter et d'utiliser les services d'un autre périphérique Bluetooth.

Recherche d'un périphérique Bluetooth

Considérons deux périphériques Bluetooth comme par exemple un téléphone cellulaire et un PC portable. Le téléphone cellulaire est capable de fonctionner comme un modem en utilisant le profil *"Dial up networking* (DUN) *profile"* et sonde périodiquement la bande de fréquences ISM pour déterminer si un autre périphérique a besoin de lui.

Supposons que l'utilisateur du PC ouvre une application nécessitant l'utilisation d'un modem. Le PC sait donc qu'il doit établir une connexion Bluetooth avec un périphérique supportant le profil DUN. La première étape pour établir une telle connexion est tout d'abord de trouver les périphériques Bluetooth accessibles dans son rayon d'action. Pour cela, le PC émet une série de paquets du type "`Inquiry`" et le téléphone cellulaire peut répondre avec un paquet du type *"Frequency Hop Synchronisation"* (FHS). Ce paquet contient toute l'information nécessaire au PC pour établir une connection avec le téléphone cellulaire. De la même manière, tous les autres périphériques Bluetooth dans les environs peuvent également répondre par un paquet FHS. Dès lors, le PC portable accumule une liste de périphériques disponibles.

La suite dépend essentiellement de l'application tournant sur le PC. Celle-ci peut afficher une liste des périphériques Bluetooth à l'utilisateur qui peut faire son choix. Ou alors, l'application peut rechercher elle-même parmi les périphériques rencontrés ceux qui supportent le profil DUN.

Connection à une base de données de recherche de services ("Service Discovery Database")

Afin de déterminer les différents services offerts par les périphériques Bluetooth présents, l'application tournant sur le PC doit se connecter aux périphériques et utiliser le protocole *"Service Discovery Protocol"* (SDP). Ce protocole établit une liaison entre les périphériques au niveau des couches *"Baseband"* et *"Logical Link Control and Adaptation Protocol"* (L2CAP). Le PC portable utilise la liaison L2CAP pour se connecter au *"Service Discovery"* du téléphone cellulaire. Ce service recherche dans la base de données du téléphone et transmet au PC portable tous les attributs relatifs à ses fonctionnalités, en particulier le fait qu'il supporte le profil DUN. Une fois l'information parvenue au PC portable, il peut décider de couper la connection afin d'utiliser le protocole SDP sur les autres périphériques.

En résumé, le protocole SDP permet au PC portable d'obtenir toutes les informations disponibles sur les périphériques Bluetooth à portée et, en particulier, tout ce dont il a besoin pour accéder au service DUN du téléphone cellulaire.

Connection à un service Bluetooth

Une fois que le PC portable a décidé quel périphérique il va utiliser, la communication proprement dite, c'est-à-dire le transfert de données, peut commencer. Une liaison est alors établie à tous les niveaux de la pile de protocoles : *"Baseband"*, *"Link Manager"*, *"Host Controller Interface"* et *"RFCOMM"*. Finalement, une connection DUN est établie au sommet de la pile de protocoles et le PC portable peut commencer à utiliser le service DUN du téléphone cellulaire, et donc transmettre des données sur le réseau téléphonique.

Si le téléphone cellulaire sort de la zone du PC portable, celui-ci devra recommencer la procédure et trouver un autre périphérique Bluetooth. Cependant, le téléphone cellulaire continue de sonder la bande de fréquences et peut se connecter à un autre périphérique situé dans une autre pièce.

2.8 Types de connexions

Bluetooth supporte deux types de connexion : les connexions synchrones, dites *"Synchronous connection Oriented"* (SCO) et les connexions asynchrones, *"Asynchronous Connectionless"* (ACL). Les connexions synchrones sont principalement destinées à des communications en temps réel à des débits multiples de $64\,[kb/s]$, comme pour le transfert de la voix. Par contre, le lien ACL a été défini pour le transfert de données. Le débit binaire maximum au sein d'un piconet est limité à $723,3\,[kb/s]$ au niveau de la couche physique.

2.9 Consommation des terminaux

La consommation d'un périphérique Bluetooth dépend de son état de fonctionnement. Deux états principaux sont à considérer :

– L'état *non connecté* dans lequel un périphérique n'est connecté à aucun autre périphérique, c'est-à-dire qu'il n'a initié aucune communication, ni reçu une communication d'un autre périphérique. Un périphérique non connecté est aussi dit en *"standby"*.
– L'état *connecté* dans lequel un périphérique a initié ou reçu une communication.

Un périphérique Bluetooth esclave et connecté peut se trouver dans 4 modes différents, chacun caractérisé par une consommation différente (l'ensemble des modes est représenté à la figure 2.8) :

– Le mode *actif* : l'esclave est toujours prêt à lire un paquet envoyé par le maître et à en renvoyer un autre
– Le mode "Sniff" : l'esclave devient actif périodiquement. Le maître ne transmet des paquets qu'à des instants bien déterminés et connus de l'esclave en mode "Sniff". Si le maître transmet, l'esclave lit jusque la fin du paquet sinon il néglige l'information. Vu que l'esclave n'écoute le maître qu'à des instants bien définis, il peut économiser de l'énergie entre ces instants.
– Le mode "Hold" : dans ce mode, l'esclave peut ne pas écouter le maître pendant un certain temps appelé *"hold time"* et peut faire tout autre chose comme établir une autre communication ou passer en mode dormant. Le mode *"Hold"* est plus économe en termes d'énergie que le mode *"Sniff"*.
– Le mode "Park" : l'esclave ne maintient plus que la synchronisation avec le maître. Contrairement aux deux modes précédents, qui peuvent encore être vus comme des modes actifs, le mode *"Park"* n'est pas actif ; on parle de mode *passif*. Un piconet peut contenir jusque 7 esclaves actifs (c'est-à-dire en mode actif, sniff ou hold) mais peut contenir 255 esclaves passifs. Ce mode permet au maître d'orchestrer un grand nombre de communications au sein du piconet (passage d'un mode actif au mode passif et vice-versa). Ce mode permet de plus la plus grande économie d'énergie.

Il est à noter que plus un mode permet de l'économie d'énergie, moins il est "réactif", c'est-à-dire moins le périphérique sera capable de réagir rapidement à une demande du maître.

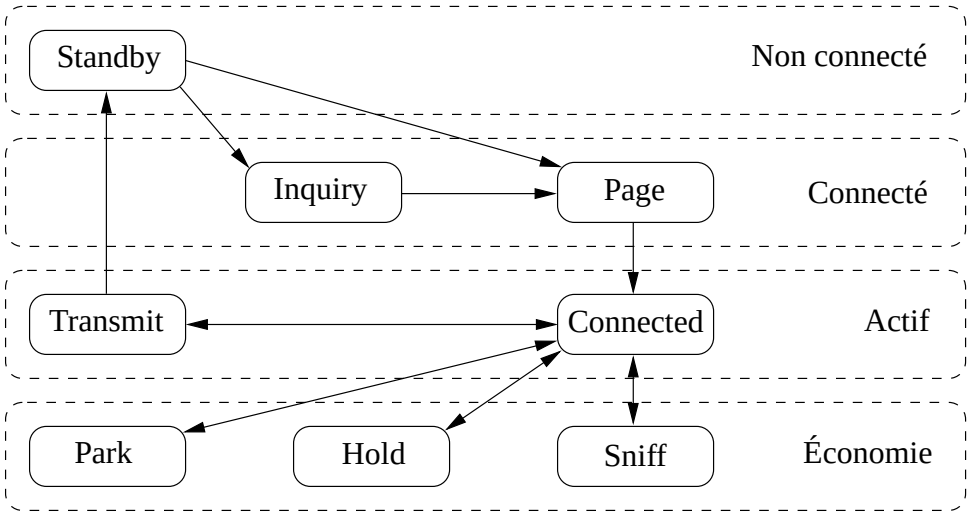

FIG. 2.8 – Diagramme des états possibles d'un terminal Bluetooth.

Un autre moyen d'économie d'énergie envisagé dans la norme Bluetooth est l'"*adaptative transmission power*", système qui permet au maître d'ajuster le niveau de puissance utilisé. Un esclave peut, par l'intermédiaire d'un signal de référence (le RSSI) avertir le maître qu'il utilise trop de puissance (par exemple s'il sont situés trop près l'un de l'autre).

2.10 Comparatif avec d'autres normes de réseaux sans fil

La plupart des normes de réseaux sans fil définies par l'IEEE utilisent la bande de fréquences ISM. Parmi les plus connues, on peut trouver les deux variantes de la norme IEEE `802.11` : la 802.11a et la 802.11b. Ces deux familles de normes partagent une architecture commune telle que décrite à la figure 2.9.

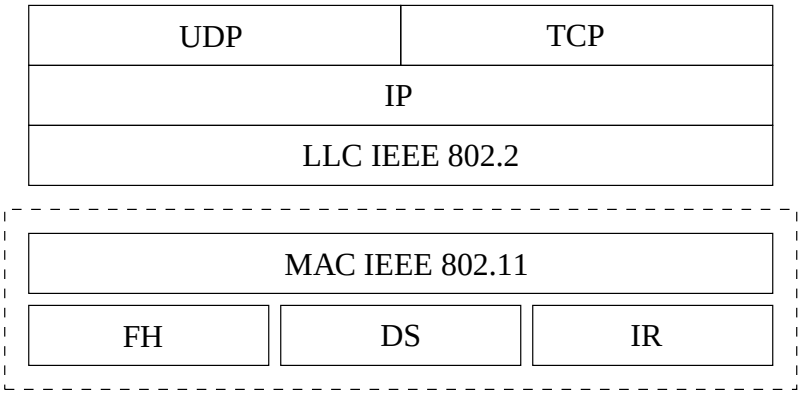

FIG. 2.9 – Couches de protocoles de la famille de normes 802.11.

Sans entrer dans le détail de la comparaison, le tableau 2.2 reprend l'essentiel des caractéristiques des normes les plus courantes de réseaux sans fil.

Débit	Standards	Technologie	Applications typiques	Prix
∼100 kbps	FireFly	DSSS 2.4 GHz	Remote Control, toys	$2
∼1 Mbps	Bluetooth	FH 2.4 GHz	Cable replacement	$5
	HomeRF	DSSS / FH 2.4 GHz	Wireless LAN (WLAN)	$10
	DECT	FH 2.4 GHz	Voice and data	$8
		GFSK 1.9 GHz		$7
∼10 Mbps	IEEE802.11b	2.4 GHz	WLAN	$20
∼50 Mbps	IEEE802.11a	OFDM 5.x GHz	High-Speed WLAN	$30
	BRAN (HyperLAN/2)	OFDM 5.x GHZ	WLAN + isochronous	$30

TAB. 2.2 – Comparatif de normes de réseaux sans fil (d'après [6]).

2.11 Résumé des caractéristiques techniques

En guise de synthèse, le tableau 2.3 reprend les principales caractéristiques de la norme Bluetooth V1.0.

Fréquence radio	2,45 GHz (bande ISM)
Technique d'étalement de spectre	Saut de fréquences
Fréquences utilisées pour les sauts	79 (espacées de 1 MHz)
Taux de sauts	1600 sauts/sec
Puissance transmise	1-100 mW
Distance maximale	10m (0 dBm) / 100m (20 dBm)
Débit maximum	1 Mb/s
Débit max. pratique (ACL-Symétrique)	433,9 kb/s
Débit max. pratique (ACL-Asymétrique)	723,2 kb/s - 57,6 kb/s
Débit SCO	64 kb/s
Unités par piconet	8 (1 maître - 7 esclaves)
Modes d'économie d'énergie	Hold - Sniff - Park

TAB. 2.3 – Résumé des spécifications techniques de la norme Bluetooth V1.0

Chapitre 3

Les aspects de sécurité

3.1 Introduction à la sécurité

La mise en réseau d'information offre moins de garantie de confidentialité, tout simplement parce que plus de personnes y ont accès. La cryptographie, la science qui consiste à assurer la confidentialité des messages, permet néanmoins de conserver un haut degré de sécurité.

En toute généralité, la mise en œuvre d'un système sécurisé comporte trois aspects :

– le *chiffrement*,
– des *fonctions* de sécurité et
– une *implémentation* des fonctions de sécurité dans un réseau.

Pour chacun de ces aspects, il existe plusieurs solutions. Si bien que lors de la comparaison de produits, il importe de bien analyser ces trois aspects en détail. Nous allons à présent traiter ces trois aspects.

3.1.1 Chiffrement

Nous comprenons les messages que nous lisons parce qu'ils nous sont présentés sous une forme compréhensible. Dans le cas de transactions financières ou d'échanges d'informations militaires, il importe qu'un message intercepté ne soit pas lisible. Le processus par lequel un message est rendu incompréhensible est appelé `chiffrement`. Le processus de reconstruction du texte original à partir du message chiffré est appelé `déchiffrement`. On parle aussi respectivement de *cryptage* et de `décryptage`. Les étapes d'un processus de chiffrement sont illustrées par la figure 3.1.

Ce schéma met en lumière une déconcertante analogie avec la compression. De fait, le chiffrement, tout comme la compression, tente de supprimer la redondance présente dans le message. Il est probable qu'à l'avenir apparaissent des techniques qui mêlent compression et chiffrement. Les algorithmes d'aujourd'hui n'incluent pas encore la notion de compression car un texte chiffré est bien de longueur égale à celle du message original.

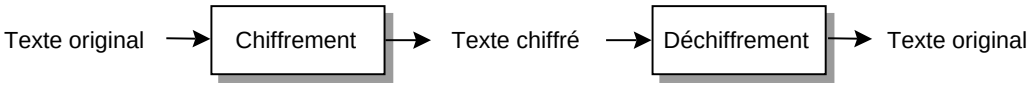

FIG. 3.1 – Chiffrement et déchiffrement.

Algorithmes à clef secrète ou publique

Le texte de départ, noté M ci-après, peut être une suite de bits, un fichier texte, un signal audio, une image, etc ; la fonction de chiffrement $\mathcal{E}$ transforme ce message en un message chiffré C :

$$C = \mathcal{E}_{k_1}(M) \tag{3.1}$$

Si la sécurité du processus de chiffrement repose sur la confidentialité de l'algorithme, on considère que le certain est peu sûr car, tôt ou tard, un utilisateur découvrira le secret et le système de chiffrement s'effondrera. Pour une vraie sécurité, tous les algorithmes modernes de chiffrement utilisent une *clef*, notée k_1 ; c'est la raison de la présence de l'indice k_1 dans l'équation 3.1. Cette clef peut prendre une des valeurs parmi un grand nombre de valeurs possibles. Pour le déchiffrement $\mathcal{D}$ on procède de même, et si la clef de déchiffrement est identique à celle de chiffrement, on a :

$$M = \mathcal{D}_{k_1}(C) \tag{3.2}$$

et donc, par substitution de C de l'égalité 3.1,

$$M = \mathcal{D}_{k_1}(\mathcal{E}_{k_1}(M)) \tag{3.3}$$

Il existe des cas où la clef de déchiffrement, notée k_2, est différente de la clef de chiffrement (cf. figure 3.2). Dans ce cas, les relations deviennent :

$$C = \mathcal{E}_{k_1}(M) \tag{3.4}$$
$$M = \mathcal{D}_{k_2}(C) \tag{3.5}$$
$$M = \mathcal{D}_{k_2}(\mathcal{E}_{k_1}(M)) \tag{3.6}$$

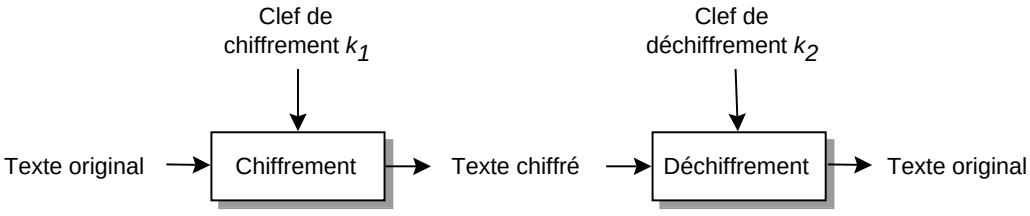

FIG. 3.2 – Chiffrement et déchiffrement avec deux clefs distinctes.

Il y a deux types principaux d'algorithmes à base de clefs : à *clef secrète* ou à *clef publique*. Les *algorithmes à clef secrète* sont des algorithmes où la clef de chiffrement peut être calculée à

partir de la clef de déchiffrement et vice-versa. Les *algorithmes à clef publique* sont différents. Ils sont conçus de sorte que les deux clés soient différentes et qu'il ne soit pas possible de calculer une clef à partir de l'autre dans un temps raisonnable. Le nom d'algorithme *à clef publique* vient de ce que la clef de chiffrement peut être rendue publique. N'importe qui à le droit de l'utiliser pour chiffrer un message mais seul le détenteur de la clef de déchiffrement peut reconstituer le message non chiffré. Dans de tels systèmes, les clefs de chiffrement et déchiffrement sont respectivement appelées clef publique et clef privée.

De l'usage des algorithmes de chiffrement

Les algorithmes de chiffrement tels que décrits ont d'innombrables utilisations autres que le simple fait de vouloir cacher le contenu d'un message ; ils sont alors intégrés dans des protocoles complexes. Par exemple, une personne qui se connecte à un ordinateur doit fournir son identité. Mais comment l'ordinateur peut-il être sûr de l'identité de la personne ? Classiquement, ce problème *d'authentification* se résout par l'octroi d'un mot de passe. Un algorithme de chiffrement transforme alors ce mot de passe et l'ordinateur compare le résultat avec une table de mots de passe chiffrés. Comme cette table ne contient jamais que les mots de passe chiffrés, il n'est pas à craindre qu'un utilisateur indélicat ne prenne connaissance d'un mot de passe en allant parcourir les fichiers de l'ordinateur.

Un autre problème fréquent est celui de la *signature numérique* : comment savoir qu'un texte provient bien d'une personne ? L'algorithme de chiffrement à clef publique fournit entre autres un moyen commode de signature numérique. Il suffit d'imaginer que l'expéditeur utilise sa clef privée pour chiffrer une empreinte propre à son message. Le destinataire, qui possède la clef publique de l'utilisateur, vérifie si l'empreinte déchiffrée correspond au message fourni par l'expéditeur. Vu que l'expéditeur est le seul à connaître la clef privée liée à la clef publique, si l'empreinte correspond, il a toutes les raisons de penser que l'expéditeur a bien signé le message.

Il reste ensuite à savoir si le message n'a pas été modifié en cours de route, c'est le problème de *l'intégrité des messages*. Des solutions existent également pour ce type de problème mais nous n'entrerons pas dans leurs détails. Il nous paraît cependant utile de citer les quatre algorithmes cryptographiques suivants (voir [5] pour plus de détails) :

DES Data Encryption Standard. C'est actuellement l'algorithme de chiffrement le plus populaire. Le DES est un algorithme à clef secrète ; la même clef sert au chiffrement et au déchiffrement.

RSA d'après le nom de ses concepteurs : RIVEST, SHAMIR et ADLEMAN. RSA est l'algorithme à clef publique le plus populaire. Il peut aussi bien être utilisé pour le chiffrement que pour la signature numérique.

IDEA International Data Encryption Algorithm. Il s'agit d'un algorithme de chiffrement à clef secrète utilisé dans le programme de signature numérique PGP (Pretty Good Privacy). IDEA est un algorithme de chiffrement par blocs ; il manipule des blocs de texte en clair de 64 bits. La clef est longue de 128 bits. Le même algorithme est utilisé pour le chiffrement et le déchiffrement.

AES Advanced Encryption Standard. AES utilise l'algorithme RIJNDAEL inventé par deux belges (V. RIJMEN et J. DAEMEN). À l'instar du DES, cet algorithme sert au chiffrement mais il permet de travailler avec des blocs de 128 bits et il supporte des clefs de 128, 192 ou 256 bits, contrairement au DES qui travaille avec des blocs de 64 bits et une clef longue de 56 bits.

3.1.2 Fonctions cryptographiques

Un système sécurisé offre une série de fonctions de sécurité, appelées *fonctions cryptographiques*, parmi lesquelles on distingue :

- *Authentification*. La fonction d'authentification permet d'identifier une personne ; elle est notamment utilisée lors de l'accès à une machine, tel qu'illustré par la figure 3.3.
- *Confidentialité*.
- *Signature numérique*. La signature numérique fournit une information légale fiable au destinataire du document électronique. Elle équivaut à une signature scripturale.
- *Intégrité* des messages. Un message est dit *intègre* s'il y a correspondance exacte, bit à bit, entre le message émis par l'expéditeur et le message reçu par le destinataire.
- *Non-répudiation*. La non-répudiation est en quelque sorte l'équivalent de la possession d'un accusé de réception qui permettrait de garantir qu'un message a bien été reçu ou émis.
- *Anonymat*.

```
[marc@sifnos ~]$ telnet machine.montefiore.ulg.ac.be
Trying 138.164.35.3...
Connected to machine.montefiore.ulg.ac.be (138.164.35.3).
Escape character is '^]'.


UNIX(r) System V Release 4.0 (machine)

login: marc
Password:
Last login: Wed Oct 18 15:36:40 from 195.67.167.98
MODE : STATIC
OPERATING SYSTEM : SOLARIS2 on Sun
machine:~>
```

FIG. 3.3 – Exemple de fonction cryptographique : fonction d'authentification.

Les algorithmes de chiffrement peuvent être utilisés pour assurer des fonctions cryptographiques. Prenons par exemple un algorithme à clef publique. Deux usages sont possibles :

– l'émetteur chiffre un message avec la clef *publique*. Il en résulte que seul le destinataire possédant la clef privée peut déchiffrer le message. On a donc assuré la fonction de *confidentialité*.
– l'émetteur chiffre un message avec la clef *privée*. Dès lors, le destinataire sait que seul l'émetteur possédant la clef privée pouvait chiffrer le message, ce qui équivaut à l'identification de l'expéditeur et donc à la fonction d'*authentification*.

Un *système de sécurité* se décrit toujours par les ***fonctions*** qu'il implémente ! Il convient de remarquer que différentes fonctions d'authentification sont assurées par des implémentations agissant chacune au niveau de couches distinctes du modèle OSI.

Pour terminer cette discussion, précisons qu'en matière de sécurité il n'y a pas de solution *inconditionnellement* sûre ; il faut donc compter d'emblée avec un taux de fraude qui dépendra de la solution choisie.

3.2 La sécurité dans les réseaux : modèle de référence

Le modèle de sécurité dans les réseaux le plus complet consiste à sécuriser l'ensemble des couches. Un sous-ensemble des fonctionnalités à implémenter est repris à la figure 3.4.

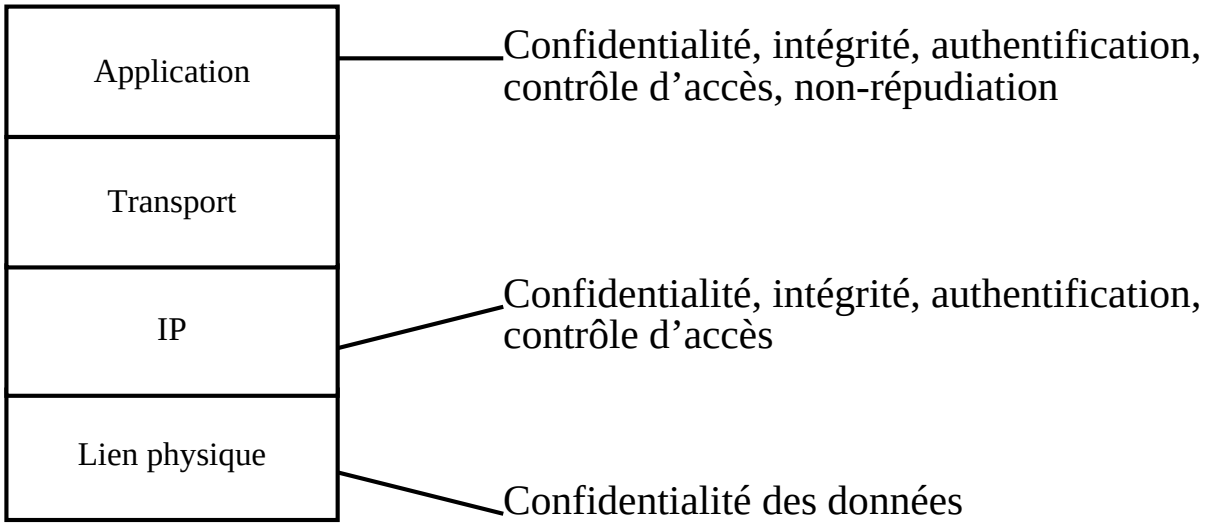

FIG. 3.4 – Modèle de sécurité.

La réalité s'écarte fortement de ce modèle. Non seulement, la majorité des messages circulent en clair sur la ligne mais, en plus, il sera toujours difficile de sécuriser une communication dont les paquets peuvent éventuellement emprunter des chemins différents.

3.3 La sécurité de Bluetooth

Un réseau sans fil opère comme un réseau câblé sauf en ce qui concerne le médium de transmission. La sécurisation d'une connexion est généralement plus compliquée pour une communication sans fil en raison de 3 facteurs :

– *écoute passive*. Dans un réseau sans fil, tout terminal se trouvant à proximité de terminaux en discussion est susceptible de suivre passivement la communication. On ne pourra jamais l'empêcher dans la mesure où cela reviendrait tout simplement à interdire la transmission.
– *accès illicite*. De nombreuses affaires relatent l'utilisation d'un réseau sans fil à l'insu du gestionnaire du réseau. Cela est possible dès lors que l'accès n'est pas contrôlé rigoureusement. Certaines attaques procèdent par substitution de la station de base.
– *interférence* et *brouillage* (dit `jamming` en anglais). La bande ISM est libre et connue. Il est dès lors aisé de parasiter, involontairement ou volontairement, la bande. La parade imaginée dans Bluetooth consiste à effectuer des sauts de fréquence pour éviter l'utilisation prolongée d'une bande de fréquences défavorables, étant entendu qu'il n'y a pas de source de brouillage intentionnelle.

Les parades imaginées dans Bluetooth sont de 3 ordres :

– l'étalement par sauts de fréquences,
– le chiffrement et
– l'authentification.

L'architecture, telle que définie par le `SIG`, prévoit des mécanismes d'authentification et de confidentialité par chiffrement ; ces fonctions sont toutes implémentées au niveau du lien. Néanmoins, l'ensemble des couches interagissent avec un module appelé *"Security Manager"* qui doit être greffé dans le système.

Les spécifications détaillent 2 niveaux de confiance (*trusted* ou *untrusted*), qui gère la restriction aux services, et 3 modes de sécurisation, à savoir :

Mode 1 : Non-secure. Aucune fonction de sécurité n'est offerte.

Mode 2 : Service-level enforced security. Des fonctions de sécurité sont imposées après établissement de la communication.

Mode 3 : Link-level enforced security. Des mécanismes de sécurisation sont imposés dès avant l'établissement de la connexion.

La sécurisation de Bluetooth présente de nombreuses failles au niveau de la confidentialité, l'authentification, la disponibilité, la non-répudiation et le caractère privé des communications.

Le problème de la confidentialité provient de la liberté de chiffrer ou non les informations générées au niveau applicatif, avec un renforcement dès lors qu'un terminal hostile a connaissance des clés.

L'authentification est problématique dans la mesure où ce sont les terminaux et non les utilisateurs qui s'authentifient. Il est pourtant difficilement imaginable de mettre en œuvre toute une infrastructure pour répondre à cette carence.

La disponibilité d'un réseau ou d'un terminal Bluetooth n'est nullement garantie. La faible portée des équipements signifie qu'il est peu probable qu'une source d'interférence se trouvant à proximité ne puisse être détectée et supprimée. Néanmoins, certaines expériences ont montré une dégradation des performances entre Bluetooth et certaines technologies de réseaux sans fil (cf. [4] pour plus de détails).

La non-répudiation n'est tout simplement pas présente dans l'architecture ; elle ne pourra jamais être offerte qu'au niveau applicatif. Quant à la protection des données, elle concerne notamment la possibilité d'identifier les mouvements d'un terminal. On peut ainsi reconstituer le trajet d'un terminal et déterminer les services offerts.

Chapitre 4

Quelques produits Bluetooth sélectionnés

Le contenu de ce chapitre ne se veut en aucun cas exhaustif. Il s'agit simplement d'une sélection parmi les très nombreux produits existants. Les documents électroniques sont disponibles dans le répertoire `pdf`.

4.1 Documents informatifs

Voici une liste de documents descriptifs fournis sous électronique :

- Séminaire Bluetooth de Rohde & Schwarz : PDF1
- Séminaire sur les réseaux sans fil réalisé par un chercheur de l'université J. FOURIER : PDF2
- Norme bluetooth : PDF3, PDF4, PDF5
- Whitepaper (comparaison entre Bluetooth et 802.11) : PDF6
- Whitepaper (Starter Kit de IAR Systems) : PDF7
- Whitepaper (Bluetooth Protocol Stack de IAR Systems) : PDF8
- Whitepaper (Atmel) : PDF9
- Whitepaper (Atmel) : PDF10

4.2 Solutions complètes

Les informations reprises dans cette section et dans les suivantes sont issues des informations fournies par les constructeurs sur leur site Web. Dans la majorité des cas, ces informations sont malheureusement incomplètes voire incorrectes.

- **Ericsson** (PRODUITS ERICSSON[1]) :
  - Gamme de téléphones mobiles incluant une solution Bluetooth complète (R520, T39).

[1] http://www.ericsson.com/bluetooth/

  - Module Bluetooth complet à intégrer dans un téléphone mobile : implémente les profils GAP, SDAP, SPP, GOEP, HS, DUN, CTP, PAN.
    Fichier PDF
- **Inventel** (PRODUITS INVENTEL[2])
  - BlueDSL : routeur ADSL / Bluetooth sans fil (jusque 100m, norme 1.1, profils : GAP, SPP, DUN, LAN)
    Fichier PDF
  - EtherBlue : routeur Ethernet sans fil (classe 1, norme 1.1)
    Fichier PDF
  - BlueAirPlug : port série RS-232 sans fil (classe 1, norme 1.1, profils : GAP, SPP)
    Fichier PDF
- **Mitsumi :**
  - Différents modules à intégrer : WML-C06 (norme 1.1, classe 2), WML-C07 (norme 1.1, classe 1), WML-C09 (norme 1.1, classe 2), WML-C11 (norme 1.1, classe 1)
    Fichier PDF Fichier PDF Fichier PDF Fichier PDF
  - Dongle USB : WIF-0402C (norme 1.1, classe 2, antenne, pas besoin d'alimentation supplémentaire, profils : GAP, SDAP, DUN, FAX, Object Push, File Transfert) + kit CD-ROM de démonstration
    Fichier PDF
- **Motorola :**
  - Système Microphone - Haut-Parleur portatif + différents accessoires (classe 2, norme 1.0b, profil : SPP)
    Fichier PDF
  - Carte PC PCMCIA BTPCM101 + drivers Windows (classe 1 ou 2, RF respectant la norme 1.1)
    Fichier PDF
- **Nokia** (PRODUITS NOKIA[3]) :
  - Accesoires mains libres pour GSM Nokia existants : carte à insérer dans le GSM, Headset, kit mains libres voitures

4.2.1 Composants

- **Ericsson** (PRODUITS ERICSSON[4])
  - Emetteurs-Récepteur Radio : PBA 313 01 (classe 2, respecte norme 1.0 et 1.1)
    Fichier PDF Fichier PDF
  - Multi Chip Modules (MCM) : ROK 101 008 : solution dite "complète" à intégrer dans un système (classe 2, norme 1.0b et CE)
    Fichier PDF Fichier PDF

[2]http://www.inventel.com
[3]http://www.nokia.com/bluetooth/
[4]http://www.ericsson.com/bluetooth/

Multi Chip Modules (MCM) : ROK 101 007 (classe 2, norme 1.1)
Fichier PDF Fichier PDF

  - Baseband Controller : PBM 990 90 : chip seul (norme 1.1)
    Fichier PDF Fichier PDF

  - Kits de développements

- **Hitachi** :
  - Emetteur-Récepteur HD57100 (norme 1.1, classe 2 et 3)
  - Processeur Bande de base SH7630 (norme 1.1)

- **IAR Systems** (PRODUITS IAR SYSTEMS[5]) :
  - Kit de développement comprenant deux cartes PC et logiciels de développement fonctionnant sous Windows
    Fichier PDF Fichier PDF

- **Inventel** (PRODUITS INVENTEL[6])
  - BlueBird : module de base Bluetooth longue distance implémentant la couche RF et baseband (classe 1, norme 1.1)
    Fichier PDF
  - Mini-BlueBird : module de base Bluetooth courte distance implémentant la couche RF et baseband sur circuit de très petite taille (classe 2, norme 1.1)
    Fichier PDF

- **Motorola**
  - Plateforme de développement
    Fichier PDF

- **Philips** (PRODUITS PHILIPS[7]) :
  - Modules RF
    Fichier PDF
  - Blueberry Developer's Kit : kit de développement complet comprenant deux cartes mères, 2 cartes RF monté autour du processeur Philips PCF87750 baseband controller, programme de test sous Windows (norme 1.1)
    Fichier PDF

- **Silicon Wave** (PRODUITS SILICONWAVE[8]) :
  - Implémentation de la partie RF sur puce électronique (norme 1.1 ou 1.0b selon le compo-

[5] http://www.iar.com/Products/BT/
[6] http://www.inventel.com
[7] http://www.semiconductors.philips.com/technologies/bluetooth/
[8] http://www.siliconwave.com/bluetooth.html

sant)
Fichier PDF Fichier PDF Fichier PDF (norme 1.1, classe 2 et 3, classe 1 avec circuits extérieurs)
  - Implémentation des couches Baseband et Link Manager sur puce électronique
Fichier PDF (4 modes d'économie d'énergie, CODEC)
Fichier PDF
Fichier PDF (norme 1.1)
Fichier PDF

- **Teleca** (PRODUITS TELECA[9]) :
  - Kits de développement Bluetooth monté avec chip Ericsson (Point to point, point to multipoint)
Fichier PDF (classe 2, norme 1.1)
Fichier PDF (classe 2, norme 1.0b)

4.3 Logiciels

- **IAR Systems** (PRODUITS IAR SYSTEMS[10]) :
  - Implémentation de la pile de protocoles Bluetooth développée dans le but qu'elle soit portable entre différents processeurs et microcontrôleurs. Ils ont également développé un logiciel appelé "IAR MakeApp" qui permet, au développeur, de configurer et d'optimiser la pile facilement pour son application
Fichier PDF
  - Drivers USB permettant de connecter et de configurer un port USB d'un PC à un module Bluetooth
Fichier PDF

- **Microsoft** (PRODUITS MICROSOFT[11]) :
  - Développement en cours, intégration prévue dans la prochaine version de Windows XP

- **Linux**
  - Pile complète de protocoles disponibles sous forme de code source. Cette pile, portant le nom de BLUEZ[12], est officiellement intégrée dans le noyau Linux depuis la version 2.4.6.

- **TTP Communications** (PRODUITS TTP COMMUNICATIONS[13]) :

[9] http://www.comtec.teleca.se/
[10] http://www.iar.com/Products/BT/
[11] http://www.microsoft.com/hwdev/tech/network/bluetooth/default.asp
[12] http ://bluez.sourceforge.net/
[13] http://www.ttpcom.com/ttpcom/bluetooth.htm

- Vente de code VHDL (IEEE Standard 1076-1993) pour le Baseband Controller, des sources en C pour le Link Controller, Link Manager et Host Controller Interface (norme 1.1), des sources en C pour le L2CAP, RFCOMM, SDP, DUN (norme 1.1)

4.4 Appareils de mesures

- **Ericsson** (PRODUITS ERICSSON[14]) :
  - fournit des services de test et de qualification de téléphones mobiles

- **IAR Systems** (PRODUITS IAR SYSTEMS[15]) :
  - "IAR PreQual for Bluetooth" : Application PC de test complet permettant de vérifier si un produit développé satisfait à la norme Bluetooth
    Fichier PDF
  - Fournit des services de consultance et de test

- **Rohde & Schwarz** (PRODUITS ROHDESCHWARZ[16]) :
  - RF Test System TS8960 : Appareil de mesures RF permettant de vérifier si un appareil vérifie les normes stipulées par le SIG. Le SIG a en effet défini un programme de qualification Bluetooth que doit réussir un appareil pour être homologué
    Fichier PDF
  - Application Software SMIQ-K5 & Vector Signal Generator SMIQ : Ce logiciel ainsi que ce générateur de signaux RF conforme à la norme Bluetooth permettent de réaliser sur un appareil Bluetooth en développement tous les tests nécessaires à son homologation

[14] http://www.ericsson.com/bluetooth/
[15] http://www.iar.com/Products/BT/
[16] http://www.rohde-schwarz.com/bluetooth

Index

Glossaire

`802.11` Groupe de travail qui, au sein de l'IEEE, est responsable de la définition et de la maintenance des standards de réseaux locaux (LAN) sans fil. 12, 21

`ACL` *Asynchronous Connectionless.* Nom désignant une liaison asynchrone dans la terminologie Bluetooth. 20

`AES` *Advanced Encryption Standard.* Standard de chiffrement qui utilise l'algorithme Rijndael inventé par deux belges (V. Rijmen et J. Daemen). À l'instar du DES, cet algorithme sert au chiffrement mais il permet de travailler avec des blocs de 128 bits et il supporte des clés de 128, 192 ou 256 bits, contrairement au DES qui travaille avec des blocs de 64 bits et une clé longue de 56 bits. 26

`Baseband` Bande de base. C'est également le nom d'une couche de la norme Bluetooth contrôlant la couche radio. 10

`Bluetooth` Ensemble de spécifications "ouvertes" de connexion sans fil entre équipements personnels et à courte distance. 3

`chiffrement` Terme qui désigne l'action de chiffrer un texte, des informations ou des données. Le chiffrement consiste à transformer un texte de sorte qu'il faille une clé pour comprendre le message. 23

`circuit` Voie de transmission physique entre deux points ou plus. Un circuit est établi pour la totalité de la durée de transmission. L'établissement et le relâchement du circuit s'effectuent par signalisation. 8

`CTP` *Cordless Telephony Profile.* Profil Bluetooth décrivant l'ensemble du fonctionnement de la pile de protocoles pour des applications de téléphonie sans fil. 17

`déchiffrement` Action consistant à retrouver l'information en clair à partir de données chiffrées. Le déchiffrement est une action légitime du destinataire du message chiffré, contrairement au décryptage. 23

`décryptage` Action consistant à retrouver l'information en clair à partir de données chiffrées sans aucune légitimité, contrairement au déchiffrement. Un bon système doit permettre le déchiffrement mais rendre le décryptage difficile. 23

`DES` *Data Encryption Standard.* Le DES est un système de chiffrement par blocs ; il chiffre les données par blocs de 64 bits. Le chiffrement et le déchiffrement utilisent tous deux le même algorithme avec un clé (secrète) d'une longueur de 56 bits. 25

DUN *Dial-Up Networking.* Terme défini dans la norme Bluetooth. Il s'agit d'un profil définissant comment un terminal Bluetooth peut accéder au réseau via un équipement permettant un accès de type dial-up. 18

Ethernet Protocole de réseau local (LAN) qui utilise une topologie de bus ou d'étoile et permet des transferts de données à 10 [Mb/s]. Il existe des versions plus rapides : Fast Ethernet (100 [Mb/s]) et Gigabit Ethernet (1000 [Mb/s]). 8

ETSI *European Telecommunications Standards Institute.* Groupe de normalisation européen créé à l'initiative du Conseil des ministres. Ce groupe est spécialisé en télécommunications. On lui doit les normes liés au GSM. 12

FCC *Federal Communications Commission.* Commission américaine régulant l'utilisation des bandes de fréquence radio. 12, 13

FHS *Frequency Hop Synchronisation.* Paquet d'information transmis permettant à un périphérique Bluetooth de se synchroniser sur la séquence de saut de fréquences d'un autre périphérique Bluetooth. 19

FHSS *Frequency Hop Spread Spectrum.* Technique de transmission à spectre étalé consistant à modifier la fréquence de la porteuse suivant une séquence pseudo-aléatoire. 13

GAP *Generic Access Profile.* Profil de base de la norme Bluetooth. Ce profil décrit les parties communes à tous les terminaux Bluetooth. 16

GFSK *Gaussian Frequency Shift Keying.* Variante de modulation de fréquence numérique. Technique de modulation pour laquelle l'information numérique est représentée sous la forme de variations douces de la fréquence porteuse. Les variations douces sont obtenues par application d'un filtre gaussien. 13

HCI *Host Controller Interface.* Interface reliant un hôte Bluetooth à un module Bluetooth. Les données et commandes passent au travers de cette interface. 10

Hold État possible pour différents protocoles. Par exmple, mode de fonctionnement d'un périphérique Bluetooth pour lequel la connection est désactivée pendant une courte période. 20

IDEA *International Data Encryption Algorithm.* Algorithme de chiffrement à clef secrète (utilisé dans le programme de signature PGP). IDEA est un algorithme de chiffrement par blocs ; il manipule des blocs de texte en clair de 64 bits. La clef est longue de 128 bits. Le même algorithme est utilisé tant pour le chiffrement que pour le déchiffrement. 25

Inquiry Un périphérique Bluetooth transmet des messages de demande (ou inquiry) afin de déterminer quels autres périphériques Bluetooth sont à sa portée radio. Les périphériques à l'écoute de ce genre de messages répondent en transmettant l'information nécessaire à l'établissement d'une connection. 19

ISM *Industrial, Scientific, and Medical.* Nom d'une bande de fréquence libre mondialement, utilisée par des nombreux systèmes de transmission sans fil dont Bluetooth. Cette bande de fréquences s'étend de $2,4$ GHz à $2,4385$ GHz. 12

ISO *International Organization for Standardization.* Fédération mondiale d'organismes nationaux de normalisation de quelque 130 pays, à raison d'un organisme par pays. Elle a pour mission de favoriser le développement de la normalisation et des activités connexes dans le monde, en vue de faciliter entre les nations les échanges de biens et de services et de développer la coopération dans les domaines intellectuel, scientifique, technique et économique. Les travaux de l'ISO aboutissent à des accords internationaux qui sont publiés sous la forme de normes internationales. 6, 16

jamming Terme désignant le brouillage intentionnel d'une communication par un autre terminal. 28

L2CAP *Logical Link Control and Adaptation.* Nom d'un protocole défini par la norme Bluetooth. Cette couche est responsable du multiplexage des données. 10, 19

LM *Link Manager.* Couche de la pile de protocoles Bluetooth implémentant le protocole LMP. Elle assure la configuration et le contrôle de la couche Baseband de la pile de protocoles. 10

modem *modulateur démodulateur.* Appareil transmettant des signaux numériques sur le réseau téléphonique analogique. Offre les fonctions de numérotation, de connexion, et éventuellement de compression et de correction d'erreur. 18

OBEX *OBject EXchange protocol*. Protocole définit par l'IrDA permettant à des périphériques d'échanger des données arbitraires. 11

OSI *Open System Interconnection.* Standard de référence d'interconnexion de réseaux développé par l'OSI. Ce système est différent du modèle Internet. 6, 7

Park Mode de fonctionnement d'un périohérique Bluetooth esclave dans lequel ce périphérique n'est actif que périodiquement. 20

piconet Groupe de périphériques Bluetooth dépendant d'un même terminal maître. . . 15

profile Ensemble de règles définissant comment la pile de protocoles Bluetooth doit être utilisée dans une application particulière. 11, 16

protocole En télécommunications : ensemble de règles permettant le dialogue entre deux couches équivalentes d'entités différentes. 7

RF *Radio Frequency.* Terme générique désignant les techniques de transmission par ondes électromagnétiques dans l'air. 6

RFCOMM Protocole de la norme Bluetooth assurant l'émulation d'une connexion série RS-232. 11

routage Détermination du chemin emprunté dans un réseau maillé par un message ou un paquet de données. Dans un réseau à routage, les paquets ne suivent pas obligatoirement tous la même route et, de ce fait, peuvent arriver dans le désordre. 8

RSA Algorithme de sécurisation à clef publique, baptisé d'après le nom de ses concepteurs (RIVEST, SHAMIR et ADLEMAN). Il peut être utilisé aussi bien pour le chiffrement que pour la signature numérique. 25

RSSI *Receive Signal Strength Indication.* Dans la technologie Bluetooth, signal de référence destiné à jauger et à décider si la puissance utilisée au cours d'une communication est trop élevée ou trop faible. 14

scatternet Dans la terminologie Bluetooth, groupe de picocellules, appelées piconets, reliées par des périphériques appartenant à plusieurs piconets. 15

SCO *Synchronous Connection Oriented.* Nom désignant une liaison synchrone dans la terminologie Bluetooth. 20

SDAP *Service Discovery Application Profile.* Profil d'utilisation Bluetooth spécifiant comment une application de recherche de périphériques doit être implémentée sous Bluetooth. . . 17

SDP *Service Discovery Protocol.* Protocole Bluetooth permettant à un périphérique Bluetooth de déterminer les fonctionnalités offertes par un autre périphérique Bluetooth. . 11, 18, 19

SIG *Special Interest Group.* Groupe de constructeurs participant au développement et à la promotion de la technologie Bluetooth. 4, 16, 28

Sniff Mode fonctionnement d'un périphérique Bluetooth permettant une économie d'énergie et pour lequel un périphérique Bluetooth est actif seulement en des instants bien déterminés. 20

SPP *Serial Port Profile.* Profil d'utilisation Bluetooth spécifiant comment un port série peut être émulé avec Bluetooth. 17

TCP *Transmission Control Protocol.* Protocole de transport utilisé pour communiquer sur Internet. TCP se charge de numéroter les paquets et gère les acquis (ou accusés de réception). 8

TDM *Time Division Multiplexing.* Mécanisme de répartition de ressources par multiplexage temporel. 14

WAP *Wireless Application Protocol.* Protocoles applicatifs spécialement conçus pour des communications mobiles. 11

WPAN *Wireless Personal Area Network.* Terme décrivant les petits réseaux sans fil à très courte distance, dont celui obtenu avec la technologie Bluetooth. 5

Bibliographie

[1] J. Bray and C. Sturman. *Bluetooth 1.1 : connect without cables*. Prentice Hall, second edition, 2002. 10

[2] J. Haartsen. Bluetooth : towards ubiquitous wireless connectivity. *Revue HF*, 2 :8–16, 2000.

[3] B. Miller and C. Bisdikian. *Bluetooth revealed*. Prentice Hall, 2001.

[4] R. Nichols and P. Lekkas. *Wireless security : models, threats, and solutions*. McGraw-Hill, 2002. 29

[5] B. Schneier. *Cryptographie appliquée : protocoles, algorithmes et codes sources en C*. International Thomson Publishing, Paris, 1995. 25

[6] C. Van Himbeeck. Wireless connectivity. *Revue HF*, 2 :4–7, 2000. 22