N° d'ordre : 17/L3/TCO Année Universitaire : 2009/2010

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

En vue de l'obtention

Du DIPLOME de LICENCE ES SCIENCES TECHNIQUES

en TELECOMMUNICATION

par : **RASOLOSON Faly Mathieu**

Application du Bluetooth : télécommande d'un ordinateur à partir d'un téléphone portable

Soutenu le Vendredi 04 Mars 2011 devant la Commission d'Examen composée de :

Président :

M. RATSIHOARANA Constant

Examinateurs :

M. RADONAMANDIMBY Edmond Jean Pierre

M. RAKOTOMALALA Mamy Alain

M. RANDRIAMITANTSOA Andry Auguste

Directeur de mémoire :

M. ANDRIAMIASY Zidora

REMERCIEMENTS

Le présent mémoire fait suite à un cursus universitaire de trois ans à l'Ecole Supérieure Polytechnique d'Antananarivo.

Je tiens à présenter mes vifs remerciements entre autre :

- Monsieur ANDRIANARY Philippe, Directeur de l'Ecole Supérieure Polytechnique D'Antananarivo.
- Monsieur RAZAKARIVONY Jules, Chef de département Télécommunication à l'Ecole Supérieure Polytechnique d'Antananarivo.
- Monsieur RATSIHOARANA Constant qui m'a fait l'honneur de présider le jury de ce mémoire.

Je tiens également à remercier les membres de jury :

- M. RADONAMANDIMBY Edmond Jean Pierre
- M. RAKOTOMALALA Mamy Alain
- M. RANDRIAMITANTSOA Andry Auguste

Je voudrais aussi exprimer ma profonde gratitude à tous les professeurs.

Je remercie ma famille qui m'a beaucoup apporté un soutient moral et financier.

Enfin, je présente particulièrement mes remerciements très sincères à Monsieur ANDRIAMIASY Zidora qui m'a témoigné son entière confiance et qui a accepté de m'encadrer tout au long de notre travail.

TABLE DES MATIERES

NOTATIONS ET ABREVIATIONS

ACL : Asynchronous Connection-Less

AM_ADDR : adresse de membre actif

AR_ADDR : adresse de requête d'accès

ARQN : bit d'indication d'une transmission

ATM : Asynchronous Transfert Mode

BIOS : Basic Input and Output System

BNEP : Bluetooth Network Encapsulation Protocol

BPP : Basic Printing Profile

BT_ADDR : Bluetooth Address

CAIJ : Code d'accès enquête Limited

CDMA : Code Division Multiple Access

CTP : Cordless Telephony Profil

DIAC : Dedicated Inquiry Access Code

DUN : Dial Up Networking Profile

EDGE : Enhanced Data Rates for GPRS Evolution

ETSI : European Telecommunications Standards Institute

FEC : Forward Error Connection

FHSS : Frequency Hopping Spread Spectrum

FLOW : bit de contrôle de flux

FTP : File Transfer Protocol

$g(D)$: polynôme générateur du code de hamming

GAP : Generic Access Profile

GFSK : Gaussian Frequency Shift Keying

GIAC : General Inquiry Access Code

GPRS : General Packet for Radio Service

GSM : Global System for Mobile Communication

HCI : Host Control Interface

HCRP : Hardcopy Cable Replacement

HEC **:** bit de contrôle de paquet

HID : Human Interface Device

IEEE : Institute of Electrical and Electronic Engineer

IP : Internet Protocol

IrDA : Infrared Data Association
ISM : Industrial Scientific Medical
ISO : International Standardization Organization
LLCAP : Logical Link Control and Adaptation Protocol
MAC : Media Access Control
MTU : Maximum Transmission Unit
OBEX : Object Exchange
OPP : Object Push Profile
OSI : Organization for Standardization International
PAN : Personal Area Network
POI : Point Of Interest
PBAP : Phone Book Access Profile
PDA : Personal Digital Assistant
PIN : Personal Identification Number
PM_ADDR : adresse de membre parqué
PPP : Point to Point Protocol
RFCOMM : Radio freq Communication
SCO : Synchronous Connection-Orientated
SDP : Service Discovery Protocol
SDAP : Service Discovery Application Profile
SEQN : bit de mise en ordre des paquets reçus
TAR : Tape ARchiver
TDMA : Time Division Multiple Access
Tcycle : durée d'un cycle d un saut de fréquence
UMTS : Universal Mobile Telecommunications System
UART : Universal Asynchronous Protocol
USB : Universal Serial Bus
WAP : Wireless Application Protocol
WIFI : Wireless Fidelity
WLAN : Wireless Local Area Network
WMAN : Wireless Metropolitan Area Network
WPAN : Wireless Personal Area Network
WWAN : Wireless Wide Area Network
XML : Extensible Markup Language

INTRODUCTION

La technologie Bluetooth est une technologie de transmission sans fil permettant la communication à courte distance entre plusieurs appareils via les ondes radio. Il est ainsi possible grâce à cette dernière de mettre en liaison un ensemble de périphériques (dans un rayon de 10 mètres) sans aucune configuration préalable.

Outre la communication entre appareils informatiques, elle permet de relier n'importe quel appareil électronique et ce grâce à une puce de 9 mm de côté. Il est alors possible de relier son ordinateur à des équipements variés tel qu'un téléphone portable, un agenda électronique ou encore une voiture ou d'utiliser ce réseau comme télécommande sur un ordinateur.

Cette technologie a été à l'initiative de plusieurs constructeurs. En effet, Ericsson, initiateur du projet, fut rapidement rejoint par Nokia, Toshiba et IBM. Ils développèrent ensemble cette nouvelle technologie de communication sans fil.

Cette technologie est aujourd'hui en plein essor. Grace à son architecture réseau, Bluetooth peut être exploité dans plusieurs domaines comme dans la télécommande mentionnée ci-dessus. La télécommande est l'une des choses qui facilitent la vie de l'homme. Actuellement, on peut télécommander n'importe quel appareil informatique.

Ce que nous allons voir c'est comment on utilise le réseau Bluetooth pour commander un ordinateur à distance. D'ou le titre de ce présent mémoire « application du Bluetooth : télécommande d'un ordinateur à partir d'un téléphone portable ».

Dans le chapitre I, on parlera des réseaux sans fil. Le chapitre II décrit les caractéristiques de la technologie Bluetooth tandis qu'on trouvera dans le chapitre III l'application du Bluetooth dans la télécommande.

CHAPITRE 1

PRESENTATION DES RESEAUX SANS FIL

1.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central, puis des stations de travail et des serveurs entre eux, afin de partager les ressources de manière optimale et de faciliter la gestion. Les équipements du réseau sont interconnectés par le biais de supports de transmission.

L'évolution des technologies de l'information et de la communication et le besoin croissant de mobilité ont donné naissance aux réseaux sans fil qui utilisent comme support de transmission les ondes hertziennes suivant la technologie cellulaire. Les réseaux informatiques sans fil sont en plein développement du fait de leur interface radio qui offre la mobilité aux utilisateurs et sont souvent utilisés comme extension d'un réseau filaire déjà existant.

Ce sont des réseaux faciles et rapides à déployer et qui permettent, en plus de la transmission de données, d'autres applications telles que la voix, la vidéo et l'Internet. Ces réseaux comportent cependant des failles, ils sont moins sécurisés que les réseaux filaires et la qualité de service laisse parfois à désirer.

Les réseaux sans fil sont classés en quatre catégories selon leur étendue géographique et normalisés par un certain nombre d'organismes parmi lesquels nous citerons l'ISO (International StandardizationOrganization), l'IEEE (Institute of Electrical and ElectronicsEngineers) et l' ETSI (EuropeanTelecommunications Standards Institute).

1.2 Classification des réseaux sans fil

De manière générale, les réseaux sans fils sont classés, selon leur étendue géographique, en quatre catégories. :

-les réseaux wpan (Wireless Personal Area Network)

-les réseaux wlan (Wireless Local Area Network)

-les réseaux wman (Wireless Metropolitan Area Network)

-les réseaux wwan (Wireless Wide Area Network)

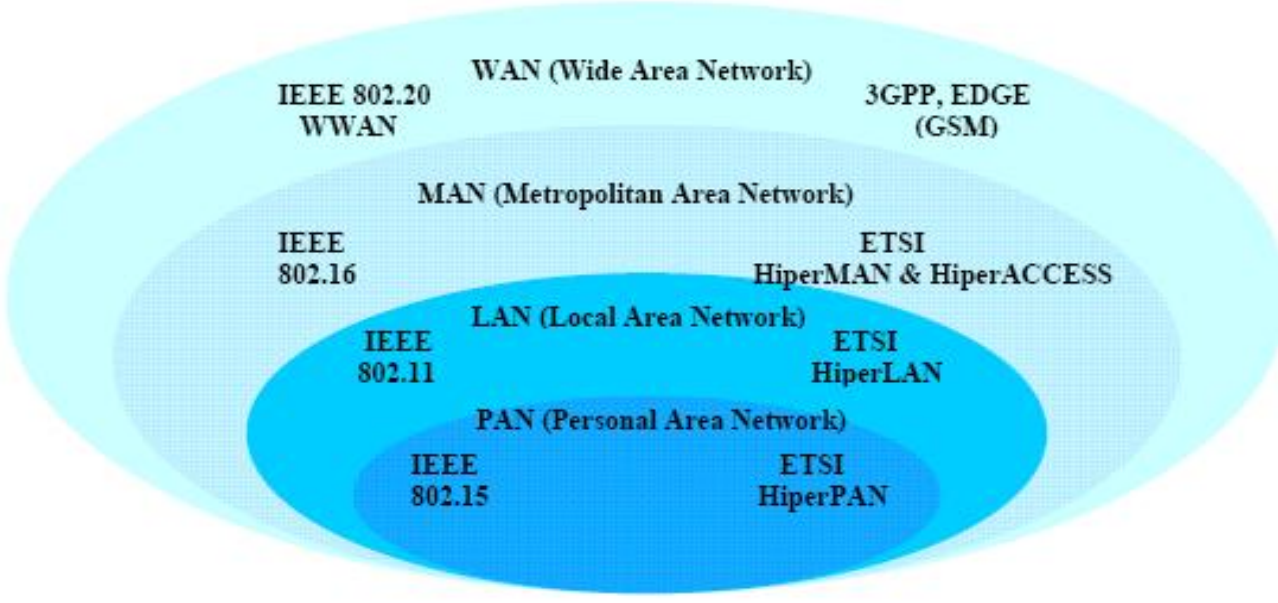

Figure 1.01 *: Classification des réseaux sans fil selon l'étendue géographique*

1.2.1 Les réseaux WPAN

Ces réseaux personnels sans fils regroupent les technologies suivantes :

Technologie	Norme	Débit théorique	Portée (m)	Bande de fréquence (GHz)	Observation
Bluetooth	IEEE 802.15.1	1 Mbits/s	30ène	2,4-2,4835	- Bas prix - L'émission de puissance dépend de la réglementation
HomeRF	Consortium (Intel, HP, Siemens ,Motorola et Compaq)	10 Mbits/s	50	2,4-2,4835	Permet de relier des PC portables, fixes et d'autres terminaux.
ZigBee	IEEE 802.15.4	20 – 250 kbits/	100	2,4-2,4835	- Très bas prix - Très faible consommation d'énergie.

Tableau 1.01 *: Réseau WPAN*

1.2.2 Les réseaux WLAN

Ce sont des réseaux permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Ils permettent de relier entre eux des terminaux présents dans la zone de couverture. Afin de permettre l'interopérabilité, les réseaux locaux (filaire et sans fil) sont normalisés par des organismes de normalisation dont les principaux sont l'IEEE et l'ETSI.

Technologie	**Norme**	**Débit théorique**	**Portée (m)**	**Bande de fréquence (GHz)**	**Observation**
wifi	IEEE 802.11	2-54Mb/s	30 -50	2,4-2,4835	Elle comporte plusieurs déclinaisons
Hyperlan1	ETSI	19-20	50	5	- La vitesse de déplacement de l'utilisateur ne peut excéder 10 m/s - Permet d'accéder aux réseaux ATM
Hyperlan2		25	200		
Hyperlink		155	150-200	17,2-17,3	Permet des liaisons fixes entre 2 points
DECT		2	300	1800-1900(mhz)	Technique d'accès TDMA

Tableau 1.02 *: Réseau WLAN*

1.2.3 Les réseaux WMAN

Ce sont des réseaux qui couvrent partiellement ou totalement la superficie d'une ville.

Technologie	**Norme**	**Débit (Mbits/s)**	**Portée (km)**	**Bande de fréquence (GHz)**	**Observation**
WiMax	IEEE 802.16	70	50	1 – 66	- Permet le raccordement des hots spots WiFi pour l'accès à Internet - Techniques d'accès TDMA - Comporte plusieurs déclinaisons
HiperAcces	ETSI	25	5	5	- Permet d'accéder aux réseaux ATM

Tableau 1.03 *: Réseau WMAN*

1.2.4 Les réseaux WWAN

Ils sont plus connus sous le nom de réseaux cellulaires mobiles.

Technologie	Norme	Débit théorique	Portée (Km)	Bande de fréquence	Observation
GSM	Européenne	9,6 kb/s	0.3-30	[890-915] MHz [935-960] MHz [1710-1785]MHz [1805-1880] MHz	- Utilise une commutation de circuits - Système très sécurisé
GPRS	Européenne	≤120Kbits/s	0.3-30	[890-915] MHz [935-960] MHz [1710-1785]MHz [1805-1880]MHz	- Utilise une commutation de paquets - Prise en charge des applications de données à moyens débits - Utilise le protocole IP pour le formatage des données
UMTS	Européenne 'ETSI'	≤ 2 Mbits/s	0.3-30	2GHZ	- Offre un accès à Internet et à ses serveurs web - Supporte des applications audio et vidéo basse définition - Fonctionne en mode paquet et mode circuit
CDMA2000	Américaine (TIA)	≤ 2 Mbits/s	0.3-30	2GHZ	- Utilise la technique d'étalement de bande
EDGE	Européenne	59,2 Kbits/s		2GHZ	-Utilise la commutation de circuit

Tableau 1.04 *: Réseau WWAN*

Notre étude portera essentiellement sur les réseaux locaux sans fil de type IEEE 802.15.1.

1.3 Présentation de la technologie

La technologie Bluetooth est normalisée par le Bluetooth *Special Interest Group* (SIG). Il s'agit d'une association créée en 1998, elle compte aujourd'hui plus de 8000 membres et a pour mission de promouvoir le développement de cette technologie sans pour autant être partie prenante dans sa conception. [Voir annexe 1].

La technologie sans fil Bluetooth fonctionne sur la bande de fréquence de 2,4GHz identique à celle utilisée par certaines normes IEEE 802.11. La fonction «saut de fréquence» définie dans la spécification Bluetooth permet de limiter les interférences et d'améliorer la qualité de service.

1.3.1 Réseau personnel sans fil de courte portée

Les appareils équipés de la technologie Bluetooth communiquent entre eux en formant des réseaux ad-hoc (maître-esclave) de faible portée nommés picoréseaux. Un périphérique esclave peut avoir plusieurs maîtres, mais ne sera pas en mesure de communiquer directement avec un autre esclave.

Ces picoréseaux permettent à 8 périphériques (1 maître et 7 esclaves) de communiquer de façon simultanée. La limitation des picoréseaux à 8 périphériques actifs est due à l'utilisation de trois bits. Cependant ces picoréseaux peuvent contenir jusqu'à 255 équipements Bluetooth en mode parked.

Un équipement Bluetooth appartenant à un picoréseau qui ne nécessite plus de communiquer peut rester synchronisé à celui-ci pour, à terme, communiquer à nouveau. Un équipement Bluetooth en mode parked est identifiable par son adresse Parked Member.Si cette adresse est nulle, l'équipement en mode parked reste identifiable via son adresse MAC.

Toutefois, un périphérique peut appartenir à plusieurs picoréseaux ce qui constitue alors un scatternet (réseau chaîné). Les scatternet et picoréseaux se font et se défont de façon dynamique au fil des connexions et des déconnexions des périphériques Bluetooth.

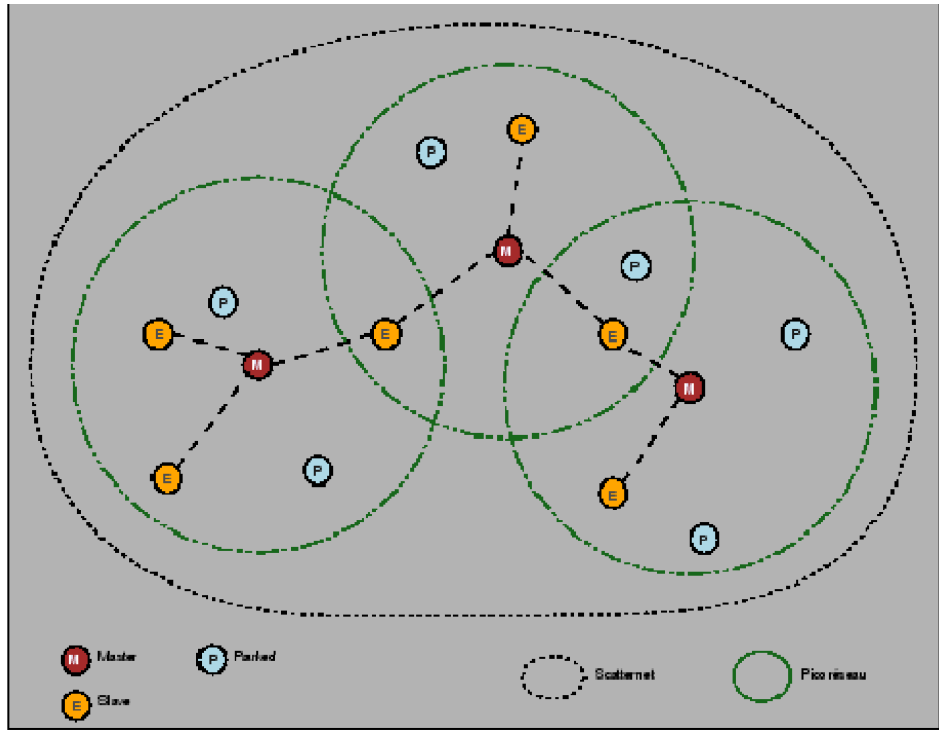

Figure 1.02 *: Scatternet et Picoréseau*

1.3.2 Bluetooth 1.2 et Bluetooth 2.0

Les équipements Bluetooth connectés à un picoréseau peuvent se transmettre simultanément des informations de type voix et données (comme défini dans la spécification du protocole Bluetooth).

En novembre 2003, la version 1.2 de la spécification Bluetooth a été adoptée. Cette version permet des taux de transfert de l'ordre de 1Mbits/s, en pratique cela se traduit par un débit de 720kbits/s. Un an plus tard, c'est la version 2.0 qui est adoptée à son tour. Cette nouvelle version permet des transferts plus rapides, le taux de transfert peut aller jusqu'à 3Mbit s/s théorique.

1.3.3 Distance et puissance

La technologie sans fil Bluetooth est destinée à des réseaux personnels de courte portée. La distance maximum spécifiée entre les équipements peut varier de quelques mètres à une centaine de mètres pour les appareils les plus puissants. La distance est directement liée à la puissance d'émission et à la sensibilité de réception des dispositifs Bluetooth.

La technologie Bluetooth, à l'inverse de la technologie infrarouge, ne requiert pas des appareils communicants qu'ils soient sur ligne directe et dégagée, en effet, cette technologie est omnidirectionnelle et les ondes radio sont capables de traverser des objets massifs tels que des murs.

Les appareils Bluetooth sont divisés en trois catégories définies par leur puissance d'émission et donc par leur portée. Les équipements dont la puissance est la plus faible sont appelés Classe 3 tandis que ceux dont la puissance est la plus importante sont appelés Classe 1.

Classe	Puissance (Atténuation en dBm)	Portée
Classe 3	1 mW (0dBm)	<10 mètres
Classe 2	2,5 mW (4dBm)	10 à 20 mètres
Classe 1	100 mW (20dBm)	100 mètres

Tableau 1.05 : *Bluetooth : classe, puissance et portée*.

Ces données sont théoriques et le matériel peut être modifié de manière à étendre la portée en réception.

1.3.4 Profils Bluetooth

Les services ou applications d'un équipement Bluetooth sont déterminés par les profils Bluetooth de façon à permettre l'interopérabilité entre les appareils Bluetooth disposant des mêmes profils.

Dans la spécification Bluetooth, au moment de la rédaction de ce document, il existe 33 profils Bluetooth qui offrent des fonctionnalités variées. Parmi ces profils Bluetooth, on retrouve des services permettant :

- de transporter des données audio de qualité stéréo (casque audio , haut-parleurs, baladeur audio, ...) ;
- de contrôler un système d'imagerie afin d'envoyer ou de récupérer des images ou même d'utiliser la fonction de capture et d'affichage à distance (appareil photo, caméscope, ...) ;
- de transmettre des données vidéos en continu ;
- d'imprimer à distance ;
- d'accéder aux données, signalisation et services fournies par le réseau RNIS ;
- d'accéder à l'Internet au moyen d'un modem ;
- d'accéder ou d'offrir un service FTP (File Transfer Protocol) ;
- ...

Dans cette liste de profils Bluetooth, on peut expliquer l'engouement des industriels pour cette technologie aux multiples possibilités. Pour les utilisateurs, cette technologie permet d'échanger, de partager, d'accéder à un grand nombre d'informations et de don nées à tout moment avec une facilité poussée. Cependant, ces informations qui transitent dans l'atmosphère doivent être protégées afin d'assurer un niveau minimum de sécurité (confidentialité et intégrité).

1.4 Problèmes spécifiques aux réseaux sans fil de type IEEE 802.15.1

1.4.1 Support de transmission [8]

Malgré leurs nombreux avantages, les réseaux sans fil posent d'énormes problèmes liés au support de transmission. Les ondes radio se propagent dans l'air, en ligne droite, à la vitesse de la lumière et peuvent être déviées par réflexion, réfraction ou diffraction à cause des obstacles rencontrés sur leur trajectoire. Les ondes radio peuvent même être totalement absorbées.

L'existence d'interférences, principalement dues aux réflexions multiples, a des conséquences néfastes sur les paramètres de la liaison c'est-à-dire sur le taux d'erreur, la portée ainsi que le débit, qui sont des grandeurs étroitement liées.

Parallèlement aux problèmes dus au support de propagation, la sécurité, la mobilité ainsi que la qualité de service (fonction de l'application utilisée) restent les maillons faibles des réseaux sans fil.

1.4.2 Sécurité

1.4.2.1 Présentation

Bien que les réseaux sans fil offrent la mobilité ainsi que la rapidité et la facilité de déploiement, la sécurité demeure un réel problème. La propagation dans l'espace fait que n'importe quel individu ayant des équipements d'écoute appropriés (adaptateur radio, antenne directive, scanner) peut écouter le trafic sur le réseau.

L'utilisation de cette technologie, avec tous les services qu'elle propose, est assortie à des risques bien réels de voir des informations dérobées par des individus qu'il sera très difficile d'identifier, car les équipements en question sont conçus pour être petits, légers et mobiles.

1.4.2.2 Attaques et vulnérabilité

La spécification Bluetooth propose 3 modes de sécurité. Il est à noter que ces modes de sécurité sont déployés ou non dans les équipements Bluetooth selon la décision prise par les fabricants. Les modes de sécurité sont les suivants :

- mode de sécurité 1 : non sécurisé ;
- mode de sécurité 2 : sécurisé au niveau applicatif ;
- mode de sécurité 3 : sécurisé au niveau de la liaison.

Le mode de sécurité 3 intervient sur la couche de liaison du modèle OSI, il permet d'établir une connexion avec authentification et chiffrement au moyen d'une clé.

Le mode de sécurité 2 permet de sécuriser de façon logicielle le dispositif Bluetooth en paramétrant les profils Bluetooth.

Le mode de sécurité 1 permet à un appareil Bluetooth d'offrir ses services à tous dispositifs Bluetooth à portée.

De nombreuses vulnérabilités liées aux dispositifs Bluetooth ont été découvertes depuis la création et l'utilisation des équipements Bluetooth. Ces vulnérabilités ont d'ailleurs été suivies par l'apparition d'attaques à l'intitulé accrocheur. Les principales attaques sont détaillées ci -dessous :

a) *Bluejacking* **:**

Cette première attaque consiste à détourner l'utilisation principale liée au profil OBEX Object Push Service qui sera vu plus tard .Le protocole OBEX est un protocole de transfert qui définit des objets de données ainsi qu'un protocole de communication qui permet à deux périphériques de les échanger

Ce profil Bluetooth permet d'envoyer des éléments (contacts, carte de visite, rendez -vous ...) entre périphériques compatibles.

Un utilisateur malintentionné peut remplir arbitrairement les cham ps de sa carte de visite et faire afficher ce texte sur un appareil Bluetooth choisi.

b) *Bluesmack* **:**

Cette attaque consiste en l'exploitation d'une vulnérabilité présente dans des piles réseau Bluetooth**.** Un utilisateur malintentionné peut fabriquer des paq uets spécialement conçus pour réaliser un déni de service de la pile réseau Bluetooth ou sur l'équipement vulnérable.

c) *Bluebug* **:**

Cette attaque affecte principalement les téléphones portables équipés d'une interface Bluetooth**.** Un utilisateur ayant accès au profil Bluetooth vulnérable d'un téléphone portable peut exécuter arbitrairement toutes sortes de commandes lui donnant ainsi un contrôle total sur l'équipement ciblé. Les actions auxquelles l'individu pourrait avoir accès sont :

- l'accès en lecture et en écriture au répertoire téléphonique ;
- appel vers n'importe quel numéro (surtaxé ou malveillant) ;
- modification de la configuration de l'appareil (volume sonore, renvoi d'appel,...) ;
- lecture et envoi de message;
- etc.

d) *Bluesnarfing* ***:***

Cette attaque permet à un utilisateur malintentionné de télécharger arbitrairement depuis l'équipement Bluetooth vulnérable un ou plusieurs fichiers.

1.4.2.3 Mode découverte et sécurité

Un dispositif Bluetooth peut activer ou non le mode découverte. Ce mode de fonctionnement permet à un appareil Bluetooth de manifester sa présence en répondant aux requêtes destinées à découvrir les équipements Bluetooth à portée.

La désactivation de ce mode peut s'avérer très utile lorsque l'on souhaite établir une communication entre deux appareils Bluetooth sans pour autant révéler leur présence aux autres équipements Bluetooth à portée. Le mode découverte est de plus en plus souvent désactivé par défaut sur les équipements Bluetooth tels que les oreillettes Bluetooth.

Un équipement Bluetooth ayant désactivé le mode «découverte» reste tout de même détectable par un utilisateur malintentionné. Pour un utilisateur non averti, le fait de désactiver le mode découverte donne une fausse impression de sécurité car un périphérique Bluetooth sous tension reste joignable.

Une attaque consiste à envoyer une requête spécifique qui ne peut être ignorée par les périphériques Bluetooth à portée, même avec le mode découverte désactivé. Ainsi, une personne malveillante va tenter de balayer une ou plusieurs plages d'adresses physiques prédéfinies associées aux dispositifs Bluetooth afin de détecter leur présence. Cette attaque de type force brute est coûteuse en temps pour l'attaquant mais reste efficace.

Ces attaques ont beaucoup perdu en furtivité depuis que les fabricants d'équipements Bluetooth implémentent par défaut le mode sécurité 2. Pour arriver à ses fins un utilisateur malintentionné devra associer à ces attaques de l'ingénierie sociale.

Conclusion

Dans ce chapitre, nous avons vu que Bluetooth est un réseau sans fil de type 802.15.1 de faible portée et présente quelque problème au niveau de la sécurité. Comme tous réseaux de communication, ce dernier a aussi sa propre caractéristique. Le chapitre suivant nous décrit les caractéristiques du Bluetooth.

CHAPITRE 2

CARACTERISTIQUES DU BLUETOOTH

2.1 Architecture

2.1.1 Protocoles Bluetooth [6]

Comme tous réseaux, la technologie Bluetooth peut être décrite avec une notion de couche mais son modèle est différent du modèle OSI. On parle de piles de protocoles.

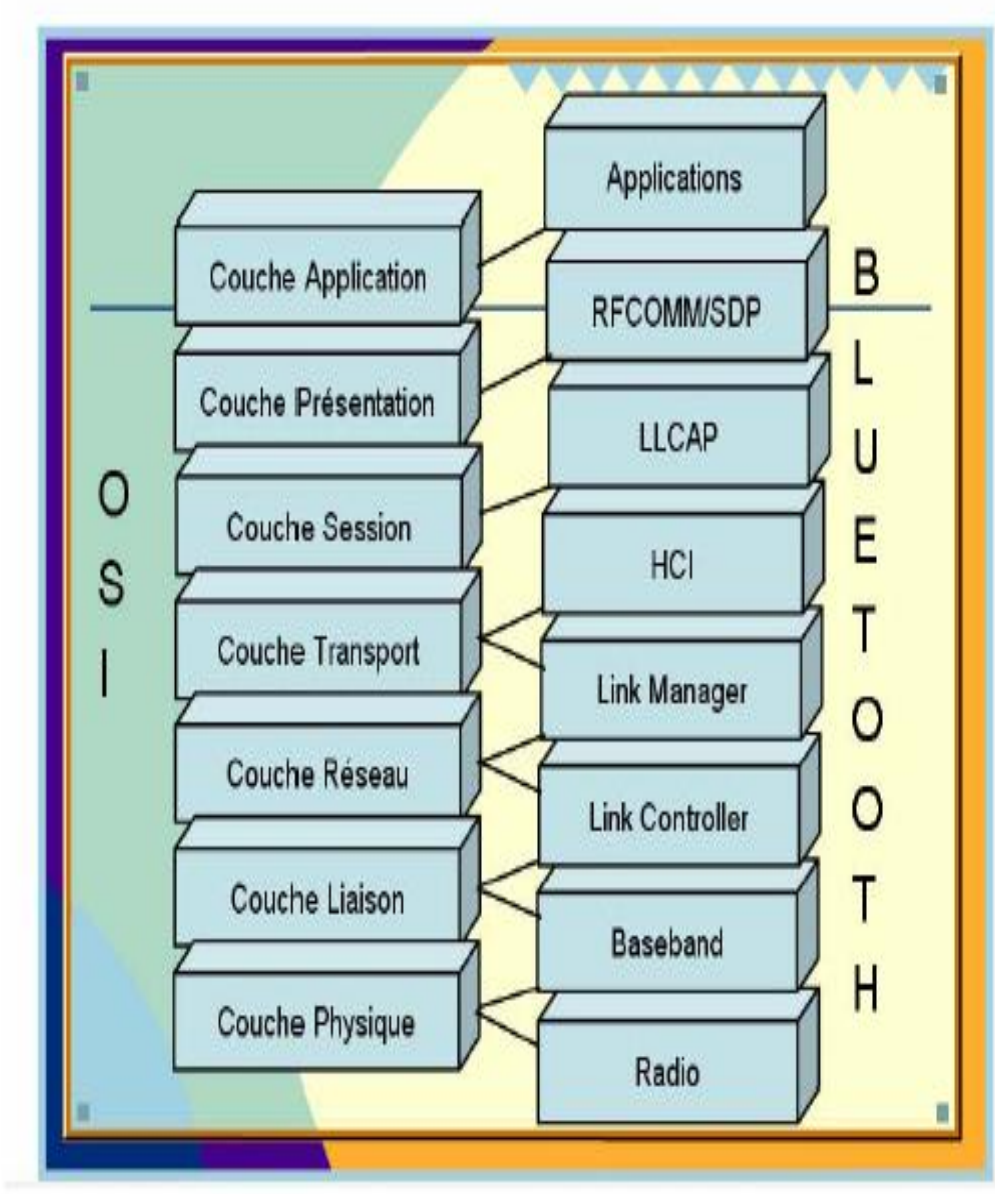

Figure 2.01 *: Couche OSI et Bluetooth*

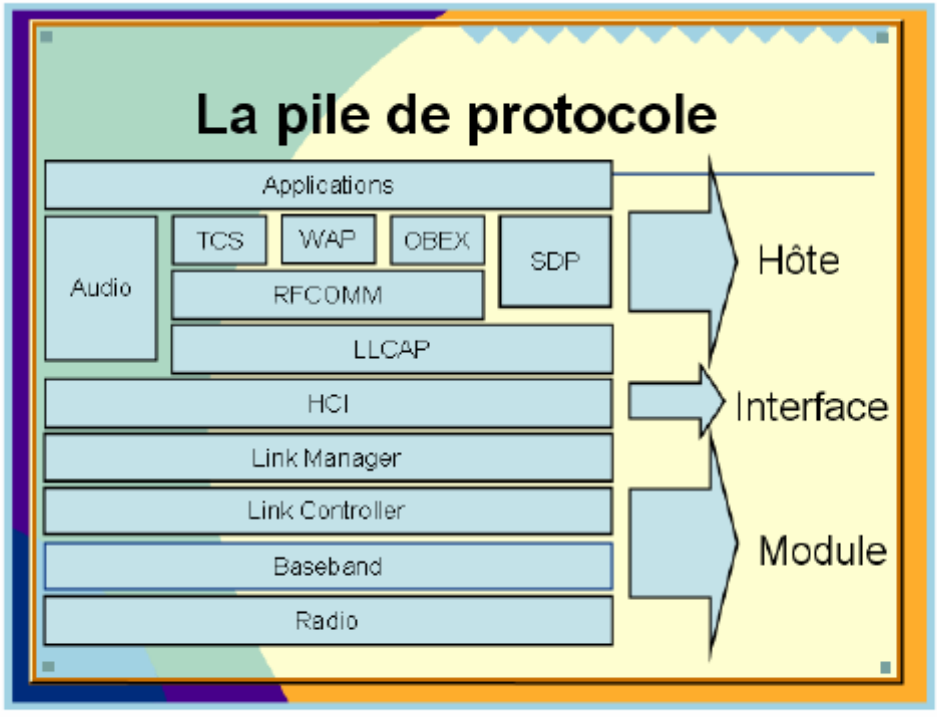

Figure 2.02 *: Pile de protocole*

Pour nos explications, nous allons séparer la pile de protocoles en deux, une couche physique (appelée aussi hôte) et la couche applicative (appelée aussi module). C'est le HCI (Host Interface Controler) qui fera le lien entre le matériel et le logiciel.

2.1.2 Spécifications techniques

2.1.2.1 Présentation de la couche physique

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

a) La couche radio fréquence (RF)

La couche radio (la couche la plus basse) est gérée au niveau matériel. C'est elle qui 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 79 canaux (23 en France) séparés de 1 MHz. Le codage de l'information se fait par sauts de fréquence. La période est de 625µs ce qui permet 1600 sauts par seconde.
Il existe 3 classes de modules radio Bluetooth sur le marché ayant des puissances différentes et donc des portées différentes :

Classe	Puissance	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	10 à 20 mètres
3	1 mW (0 dBm)	Quelques mètres

Tableau 2.01 : *Bluetooth : classe, puissance et portée*

La plupart des fabricants du SIG d'appareils électroniques utilisent des modules de classe 3.
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.

L'utilisation de FHSS dans Bluetooth permet :
- Une synchronisation parfaite entre l'émetteur et le récepteur car ils sont obligés d'utiliser la même séquence de sauts pour communiquer.
- D'émettre à plusieurs simultanément en utilisant des combinaisons de saut de fréquences différentes. Les fréquences sont ainsi partageables.
- De limiter les interférences (collisions) car les fréquences ne sont plus polluées.

b) La bande de base (baseband)
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 (équivalent à l'adresse MAC d'une carte réseau). Cette adresse est nommée BD_ADDR (Bluetooth

DeviceAddress) 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 types de paquets :

- Les paquets SCO (SynchronousConnection-Orientated) utilisés principalement pour la voix.
- Les paquets ACL (AsynchronousConnection-Less) utilisés principalement pour les autres types de données.

c) Le contrôleur de liaisons (Link Controller)

Cette couche gère la configuration et le contrôle de la liaison physique entre deux appareils. Le travail du contrôleur de lien est de commander la construction de paquets à la couche inférieur (baseband), un à un, afin d'établir et de maintenir une ligne de transmission fiable.

d) Le gestionnaire de liaisons (Link Manager)

Cette couche gère les liens entre les périphériques maîtres et esclaves (dans les réseaux Bluetooth). Il gère aussi les types de liaisons (synchrones ou asynchrones).C'est le gestionnaire de liaison s qui implémente les mécanismes de sécurité comme :

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

e) L'interface de contrôle de l'hôte (HCI)

Cette couche fournit une méthode uniforme pour accéder aux couc hes 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

2.1.2.2 Les différentes topologies de réseaux Bluetooth

a) Réseau piconet

Un piconet est un réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon. Ce réseau suit une topologie en étoile : 1 maître / plusieurs esclaves. Un périphérique maître peut administrer jusqu'à 7 esclaves actifs ou 255 esclaves en mode parked (=inactif).

La communication est directe entre le maître et un esclave. Les esclaves ne peuvent pas communiquer entre eux.

Tous les esclaves du piconet sont synchronisés sur l'horloge du maître. C'est le maître qui détermine la fréquence de saut de fréquence pour tout le piconet.

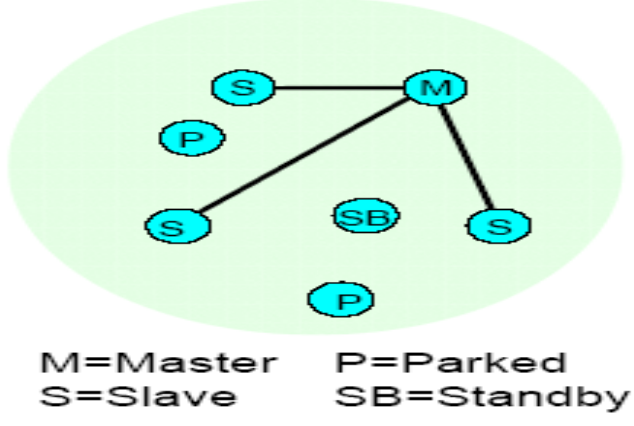

Figure 2.03 *: Réseau piconet*

b) Réseau scatternet

Les Scatternets sont en fait des interconnexions de Piconets (Scatter = dispersion).Ces interconnexions sont possibles car les périphériques esclaves peuvent avoir plusieurs maîtres, les différents piconets peuvent donc être reliés entre eux.

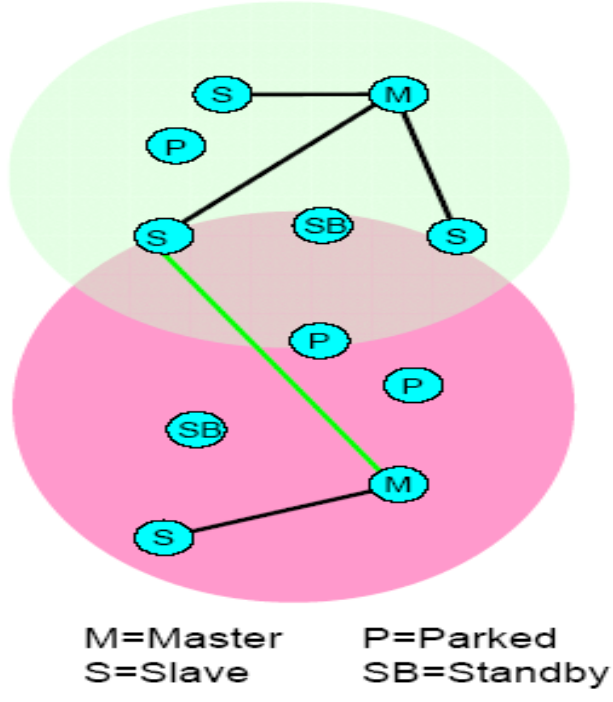

Figure 2.04 : *Réseau scatternet*

2.1.2.3 Présentation de la couche applicative

a) La couche L2CAP

L2CAP signifie Logical Link Control & Adaptation Protocol. Cette couche permet d'utiliser simultanément différents protocoles de niveaux supérieurs. Un mécanisme permet d'identifier le protocole de chaque paquet envoyé pour permettre à l'appareil distant de passer le paquet au bon protocole, une fois celui-ci récupéré (Multiplexage).

La couche L2CAP gère également la segmentation (et le réassemblage) des paquets de protocoles de niveaux supérieurs en paquets de liaison de 64 Ko.

b) Les services

RFCOMM est un service basé sur les spécifications RS-232, qui émule des liaisons séries. Il peut notamment servir à faire passer une connexion IP par Bluetooth. SDP signifie Service Discovery Protocol. Ce protocole permet à un appareil Bluetooth de rechercher d'autres appareils et d'identifier les services disponibles. Il s'agit d'un élément particulièrement complexe de Bluetooth. OBEX signifie Object Exchange. Ce service permet de transférer des données grâce à OBEX, protocole d'échange de fichiers IrDA.

c) La couche application

Le concept de profils est utilisé afin d'assurer le maximum de compatibilité entre les produits des différents constructeurs de produits Bluetooth. Ainsi, tous auront les mêmes modèles utilisateurs dans leur couche logicielle : on aura pour tous les appareils Bluetooth les mêmes appellations pour chaque fonctionnalité supportée.

Les profiles Bluetooth ont donc été développés afin de décrire comment implémenter les modèles utilisateur. Ils définissent :

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

d) Hiérarchie des profils [7]

Il existe une hiérarchie entre profil, et donc des dépendances entre eux. Pour illustrer ce phénomène, observons le schéma suivant

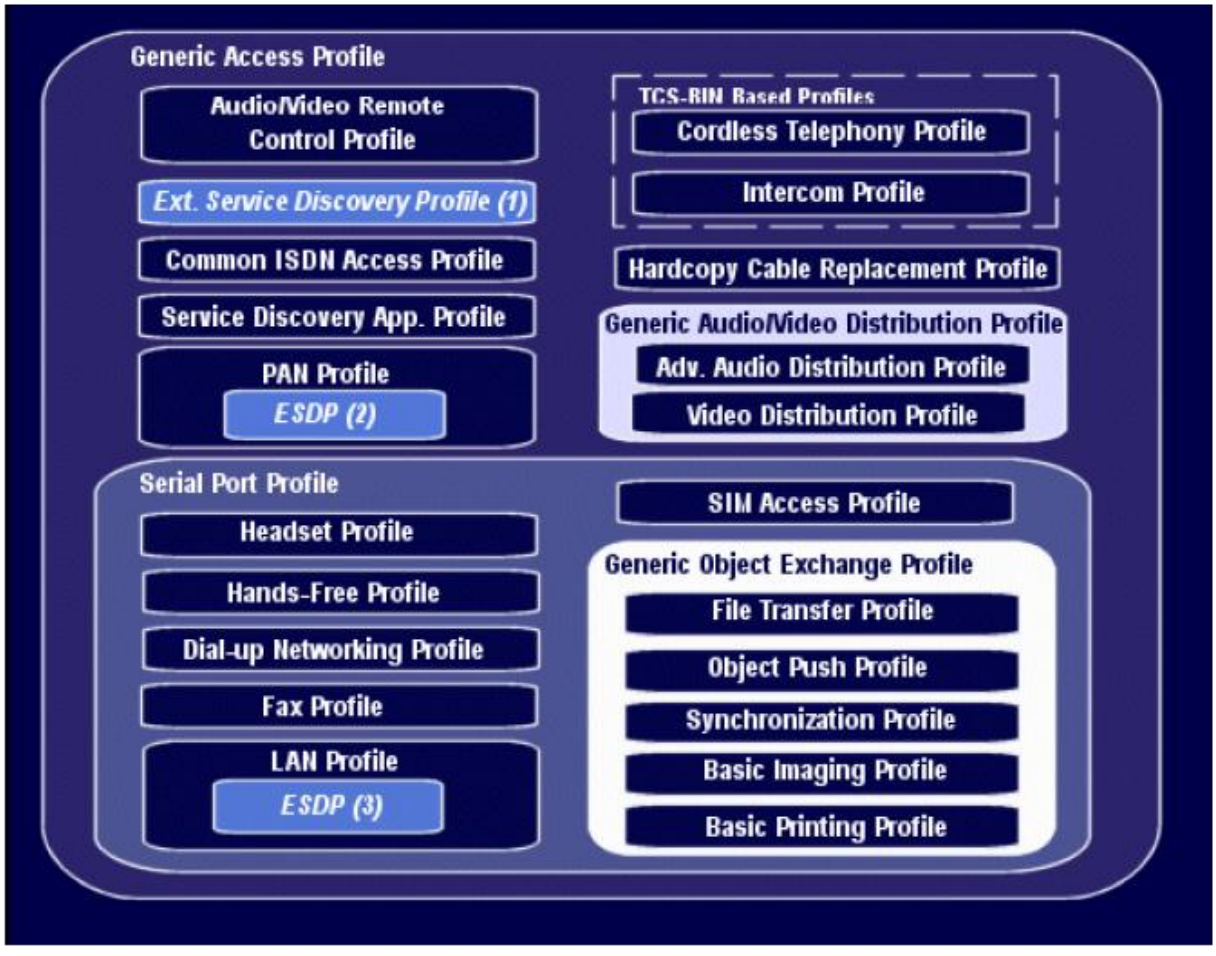

Figure 2.05 *: Profils*

Ainsi, le File Transfert Profil est dépendant du Generic Object Exchange Profile, du Serial Port Profile, et du Generic Access Profile.

e) Generic Acces Profile

Ce profil est le profil de base qui doit être implémenté par tous les appareils Bluetooth.

En effet, c'est celui qui définit les procédures génériques de découverte d'équipement, ainsi que de gestion de connexion aux autres appareils Bluetooth.

Pour chaque profil, il existe plusieurs points qui sont redéfinis ou non : rôle, scénario, principes de base…

On utilise les termes d'initiateur et d'Accepteur. Pour les 2 rôles que les protagonistes d'une communication Bluetooth peuvent prendre. L'initiateur est celui qui pour une procédure donnée, est à l'origine de l'établissement d'un lien ou d' une transaction sur un lien existant. Un utilisateur Bluetooth doit en principe pouvoir se connecter à n'importe quel autre appareil Bluetooth, même si ils n'ont aucune application en commun. Cela doit être possible en utilisant les fonctions basiques de Bluetooth. En effet, il n'y a aucune application commune entre une oreillette Bluetooth Logitech et un téléphone mobile Nokia par exemple.

Ce profil expose l'ensemble des caractéristiques de tous les équipements Bluetooth. Il expose les spécifications sur la représentation des propriétés Bluetooth : l' adresse Bluetooth, le nom d'un équipement, son type, le PIN number utilisé pour authentifier 2 périphériques.

Il définit les « modes » génériques à tous les profiles : discoverability mode (on peut le détecter), connectability mode (on peut s'y connecter), pairing mode (on peut créer un lien avec).

Il définit les procédures générales qui peuvent être utilisées pour « découvrir » les propriétés basiques des équipements Bluetooth (nom, type…) qui sont «découvrables».

Il décrit les procédures générales de connexions à d'autres dispositifs Bluetooth et donc la procédure générale de création de liens entre des dispositifs Bluetooth.

Ce profil est celui dont tous les autres dépendent, et tous les profils héritent de ses caractéristiques.

f) Autres profils importants

• Service Discovery Application Profile

Ce profil décrit les fonctionnalités et procédures d'une application ou périphérique Bluetooth afin qu'il puisse découvrir les services associés à d'autres périphériques Bluetooth et récupérer toute information relative à ces services.

Il définit également les protocoles et procédures à utiliser par une application de détection de services sur un périphérique pour localiser des services disponibles sur d'autres périphériques Bluetooth activés.

• Serial Port Profile

Ce profil est un autre profil principal : en effet, c'est celui qui définit les protocoles et procédures qui doivent être utilisées par les périphériques utilisant Bluetooth pour émuler le protocole RS232 (connexion par câble série, ce que Bluetooth est appelé à remplacer).

De ce profil dépendent les suivants :

- Headset profile : utilisation des casques sans fil ;
- Dial up networking profile : permet d'utiliser un périphérique Bluetooth en tant que pont Internet (possibilité de se connecter à Internet à partir d'un Pocket PC via un téléphone GSM Bluetooth) ;
- Fax profile : envoi/réception de fax via un téléphone GSM Bluetooth - Etc.…

• Generic Object Exchange Profile

Ce profil définit les spécificités des modèles utilisateur d'échanges d'objets entre périphériques Bluetooth : carte de visite, synchronisation, transfert de fichier…

- File Transfert Profile : utilisé par les applications de transfert de fichier (comme son nom l'indique).
- Synchronisation Profile : Ce profil va permettre à un PDA de synchroniser ses données avec une station de base (ordinateur par exemple via Bluetooth (comme il pourrait le faire via port série, USB ou IrDA).

Il existe d'autres profils Bluetooth permettant de définir d'autres modèles utilisateurs (utilisation d'un récepteur GPS par exemple), et d'assurer la compatibilité de tous les équipements implémentant ces profils entre eux.

Nous avons vu que Bluetooth utilise une architecture basée sur des profils qui offrent des fonctions précises. Techniquement, le fonctionnement est assez simple : quand deux appareils disposent du même profil, ils fonctionnent ensemble. Voici quelques profils courants :

g) profils courants

.BIP - Basic Imaging Profile

Un profil dédié à la gestion des images. Il propose plusieurs fonctions intéressantes (pas nécessairement implémentées) : envoyer et recevoir des images (avec création de vignette automatique), imprimer une image, commander un appareil photo à distance ou utiliser l'écran d'un appareil photo à distance.

.BPP - Basic Printing Profile

Un profil pour l'impression. Il a été créé pour être utilisé d'une façon bien précise : imprimer vers une imprimante compatible Bluetooth nativement à partir d'un terminal de type GSM ou PDA. Pour les impressions depuis un PC, le profil HRCP est nettement plus adapté.

.CTP - Cordless Telephony Profil

C'est un profil permettant d'utiliser un terminal (GSM, PDA, PC) pour téléphoner en utilisant une passerelle reliée au réseau commuté. En utilisant une base intégrant ce profil, vous pourrez ainsi utiliser un GSM via le réseau téléphonique classique.

.DUN - Dial Up Networking Profile

Le DUN permet d'utiliser un modem via le Bluetooth. Le modem peut être un modem RTC, mais est plus généralement un modem GPRS ou UMTS intégré dans un téléphone mobile.

.FTP - File Transfer Profile

Ce profil permet de visualiser la liste des fichiers et des répertoires d'un client, et d'envoyer ou recevoir des fichiers à celui-ci.

.HCRP – Hardcopy Cable Replacement

Ce profil permet d'émuler une connexion parallèle (IEEE1284) via Bluetooth. Un adaptateur Bluetooth est placé sur le port parallèle de la machine cible (imprimante ou scanner) et le système pourra utiliser le Bluetooth pour communiquer avec ce périphérique. Surtout utilisé pour les imprimantes qui n'ont pas de Bluetooth en natif.

.HID – Human Device Interface

Ce profil permet d'utiliser des périphériques compatibles avec la norme USB HID via Bluetooth par exemple un clavier, une souris, une manette de jeux, etc.

.PAN - Personal Area Network

Un profil permettant de créer un réseau ad hoc entre deux périphériques. Il émule une connexion de type Ethernet, pratique pour utiliser une connexion Internet fournie par un routeur par exemple. Le PAN est normalisé sous le nom IEEE 802.15.1 . Il remplace le LAP, qui est obsolète et retiré de la norme Bluetooth 1.2.

.PBAP - Phone Book Access Profile

Un profil qui permet d'accéder au répertoire d'un GSM via un autre périphérique, par exemple une oreillette.

.SAP - SIM Access Profile

Un profil créé essentiellement pour les téléphones de voiture. Il permet à un système embarqué d'utiliser la carte SIM d'un autre téléphone connecté en Bluetooth. Cela évite de devoir changer la carte de téléphone ou de devoir utiliser deux cartes différentes.

2.2 Avantages et inconvénients [8]

2.2.1 Principal avantage :

2.2.1.1 La liberté du sans fil :

Le principal objectif du Bluetooth est bien évidemment une utilisation sans fil, augmentant de manière générale l'ergonomie et l'utilisation des appareils connectés.

2.2.1.2 Autre avantage :

a) Pas de contact visuel obligatoire entre les appareils :

Grand avantage d'utiliser les ondes radio, les appareils ne sont pas obligatoirement en contact visuel, contrairement à la technologie infrarouge .

b) Dérivé de l'USB :

Comme cette technologie est une amélioration de l'USB, elle possède aussi les avantages de cette dernière. Les branchements peuvent se faire l'ordinateur allumé et l'installation se fait automatiquement quand le pilote est générique et connu par le système d'exploitation.

c) Le coût :

Bluetooth utilise une norme radio qui deviendra un standard international. Son marché potentiel est donc énorme ce qui devrait contribuer à faire chuter les coûts de fabrication des composants. L'utilisateur final ne paiera pas de surcoût sur les appareils équipés de Bluetooth. Et aussi : faible consommation d'énergie et possibilité d'implantation dans des équipements de petite taille.

2.2.2 Principal inconvénient :

2.2.2.1 La sécurité *:*

La première préoccupation des technologies sans fil est la sécurité. En effet, les données circulant par le réseau hertzien, il apparaît théoriquement plus facile de les intercepter que lorsqu'elles circulent dans un câble. Cela pourrait cependant s'avérer être un atout plus tard puisque les trames sont alors plus cryptées avec les protocoles sans fil. Entre le Bluetooth et le WIFI, le premier est cependant plus sécurisé puisque la portée est moindre.

2.2.2.2 Les inconvénients :

a) Les collisions sur le canal hertzien :

La technologie Bluetooth utilise la même fréquence que les ondes radio et que le WIFI (2.4 GHz). Les possibilités de collisions sont donc assez importantes même avec un four à micro-onde par exemple.

b) La portée :

Le Bluetooth est moins puissant que le WIFI et sa portée est donc moindre.

Elle peut aller jusque 100m mais cette distance diminue suivant le nombre d'obstacles rencontrés.

c) *L'utilisation pour les réseaux* :

Malgré l'existence de réseaux Bluetooth (piconet et scatternet), cette technologie n'est pas adaptée à cet usage, contrairement au WIFI du fait de sa faible portée et de son faible débit.

Pour pouvoir étendre notre étude nous allons voir un exemple d'application de ce système qui est le Bluetooth Ip

2.3 Bluetooth Ip [9]

Pour mieux comprendre la suite de notre étude, nous allons revoir les différentes couches du réseau Bluetooth.

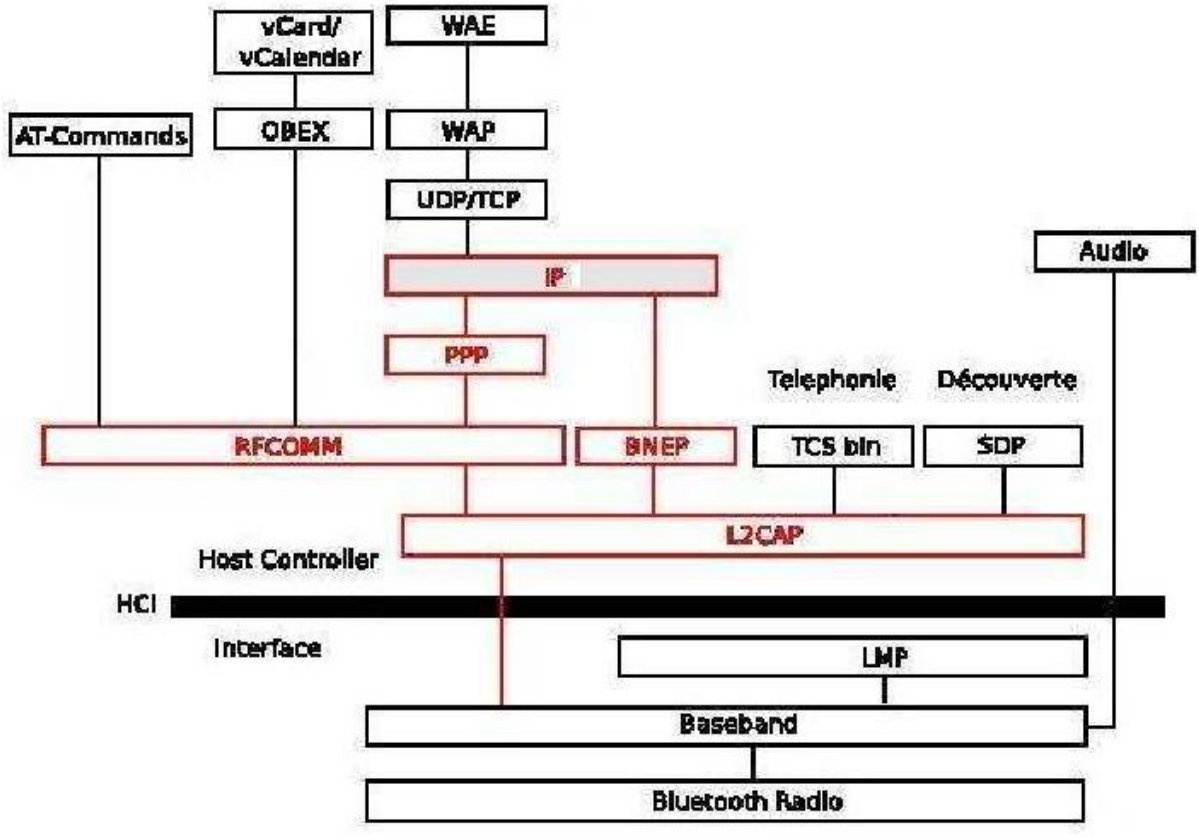

Figure 2.06 *: Couche du réseau Bluetooth*

IP peut fonctionner au dessus de deux couches : soit au dessus de PPP, cela sous-entend que nous utilisons RFCOMM en dessous, soit avec BNEP, dans ce cas là BNEP repose directement sur L2CAP.

2.3.1 RF COMM :

Il s'agit d'une couche de transport. Cette couche réalise le rôle d'émulation et de multiplexage d'un port série (RS232) sur la couche L2CAP. Cette couche émule tous les signaux du port RS232. Cette couche va assigner à chaque application un numéro logique qui correspondra à l'émulation d'un port série. L'utilisation des couches supérieures va dépendre des applications que l'on souhaite faire fonctionner au-dessus de Bluetooth.

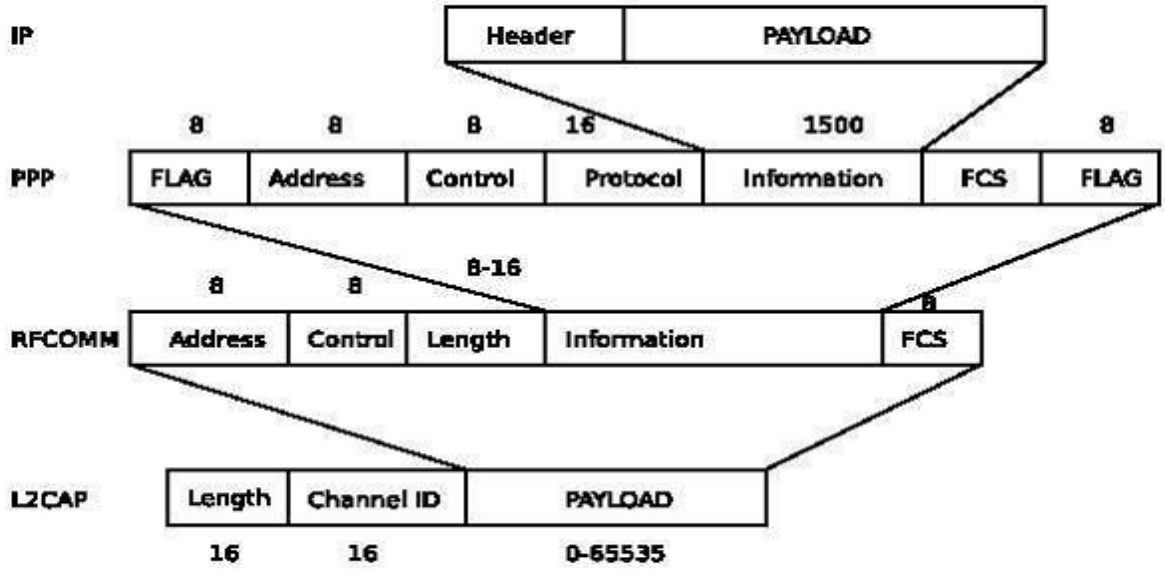

Figure 2.07 *: Paquet RFCOMM*

2.3.2 Utilisation de BNEP :

BNEP simplifie les choses, car il n'y a plus de PPP. BNEP ne fournit pas une émulation RS-232. On arrive donc à un schéma avec BNEP :

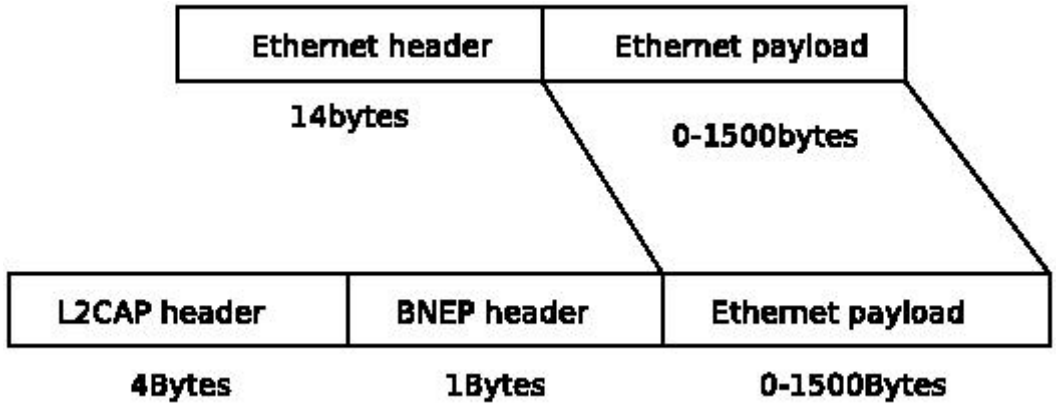

Figure 2.08 *: Paquet BNEP*

2.3.3 Poste mobile esclave

Dans le cas où les mobiles sont esclaves, on est donc limité à 7 mobiles par station de base.

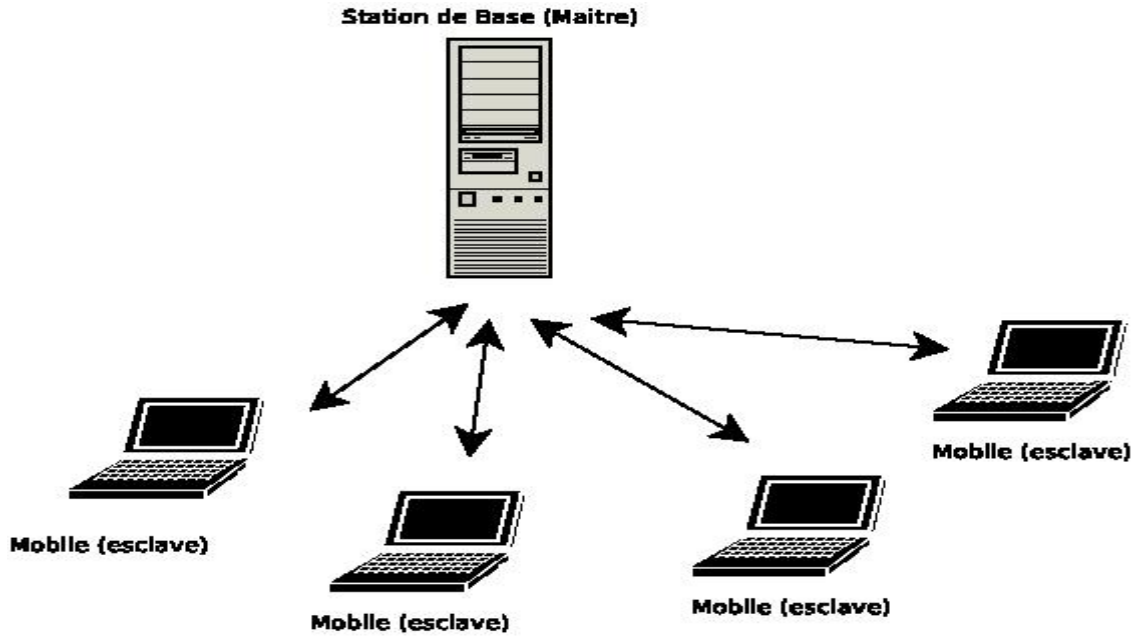

Figure 2.09 *: Station de base maitre*

2.3.4 Poste mobile maitre

Dans ce cas précis, la station de base est esclave d'autant de mobile.

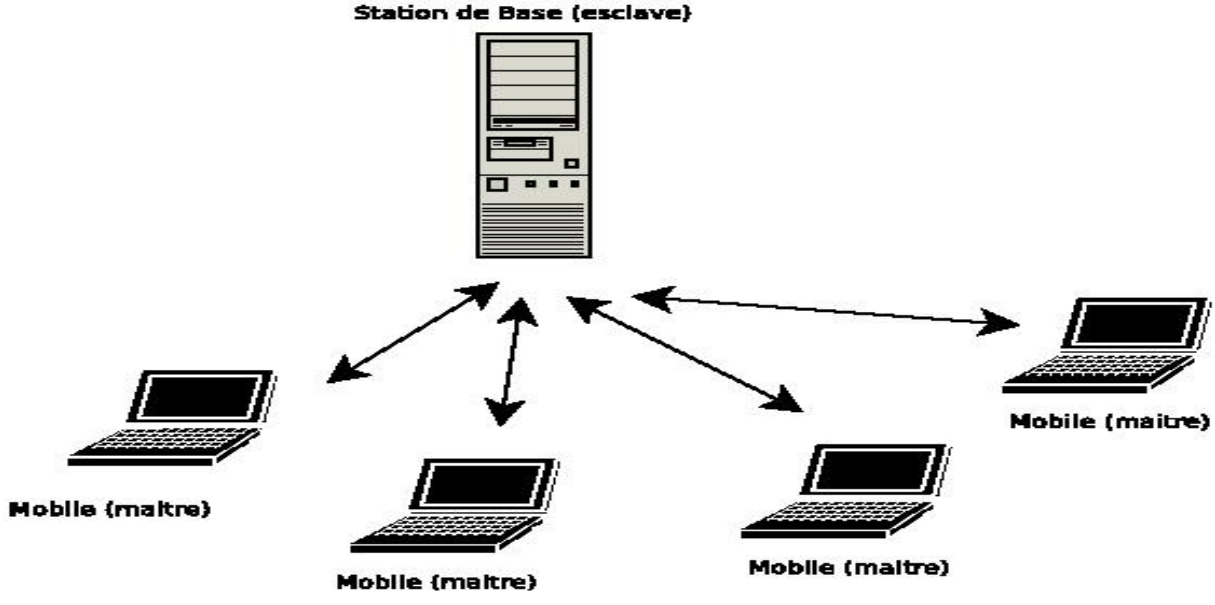

Figure 2.10 *: Station de base esclave*

2.3.5 Adaptation de la couche IP pour périphériques mobiles

La couche IP a trois états possibles :

-Discovery :

Le périphérique est dans cet état au démarrage. C'est dans cette étape qu'il va chercher les stat ions de base les plus proches dont il a généralement aucune information. Il y a une procédure permettant d'obtenir uniquement les stations de base. Cette procédure va être répétée tant qu'une station de base n'a pas été trouvée. Une procédure de connexion est déclenchée pour passer dans l'état Configuration.

-Configuration :

La station de base va donner un état de maître ou esclave au mobile. Le mobile va ensuite établir une connexion bidirectionnelle L2CAP sur la connexion existante. C'est à cette étape que la MTU des datagrammes de la couche L2CAP est négociée. La station d e base va envoyer un datagramme contenant la MTU maximum qu'il peut accepter. Le mobile va ensuite confirmer la valeur en la renvoyant. A ce moment là s'il n'y a pas eu d'erreur, on passe en phase Connected.

-Connected :

Une fois arrivé dans cette étape pour la première fois, il faut affecter une IP au mobile. Pour cela DHCP peut être utilisé, ou alors, si Mobile IP est activé il n'y aura pas de configuration à modifier sur le mobile.

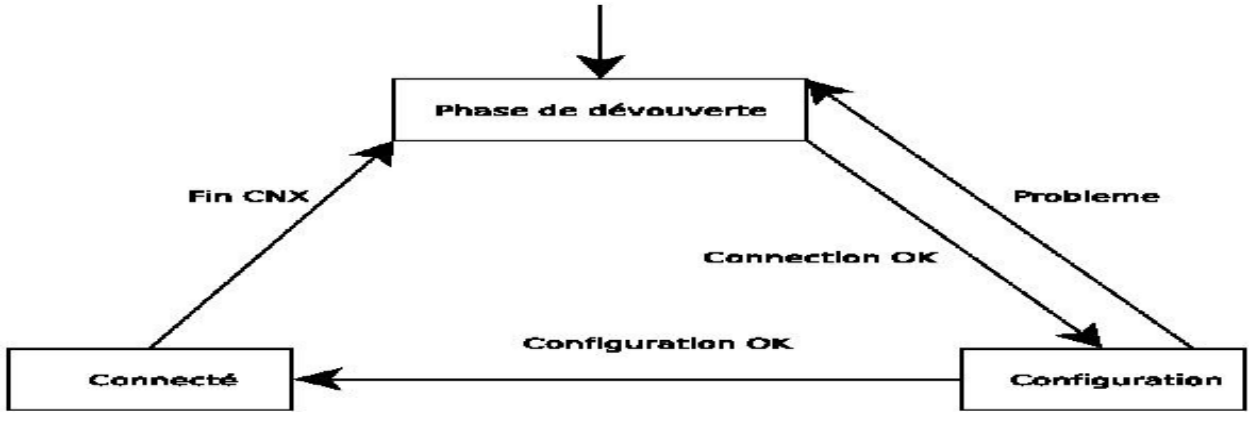

Figure 2.11 *: Etat du Bluetooth IP pour l'élément mobile*

Il faut aussi gérer la perte de lien. Pour détecter cela, la spécif ication Bluetooth propose "Link supervision timer".

Ce compteur est fixé à une certaine valeur et est remis à sa valeur initiale à chaque réception de paquet. Si aucun paquet n'est arrivé avant l'arrivée à 0 de ce timer, une alerte est déclenchée. Cette valeur est fixée par défaut à 20 minutes, il faut cho isir une bonne valeur pour ce timer car une trop faible valeur peut provoquer beaucoup d'erreurs, et donc une perte de temps en reconnexion. Une valeur trop grande va laisser trop de Mobiles connectés alors qu'ils ne sont plus dans la zone, ou autre.

2.3.6 Adaptation de la couche IP pour la station de base

La couche pour la station de base est plus simple que pour le Mobile (figure suivante). De ce côté on retrouve uniquement deux états. Son but principal est de maintenir la connexion. Cette couche a aussi pour but de découvrir de nouveaux éléments Bluetooth .

-Configuration :

Cet état a pour but de configurer et d'établir la connexion. Durant cette phase, la station de base est maître et le nouvel élément est esclave. A la fin de cet état, suivant la confi guration décidée, la station de base peut passer esclave. Durant cette phase de configuration, le canal L2CAP est créé et configuré. La configuration du canal est initiée par la station de base. Comme expliqué précédemment, la station de base va donner sa MTU. La station de base passera ensuite dans l'état connecter après confirmation de cette MTU.

-Connected :

On retrouve une base de correspondance entre le numéro de canal au niveau de L2CAP avec l'IP associé.

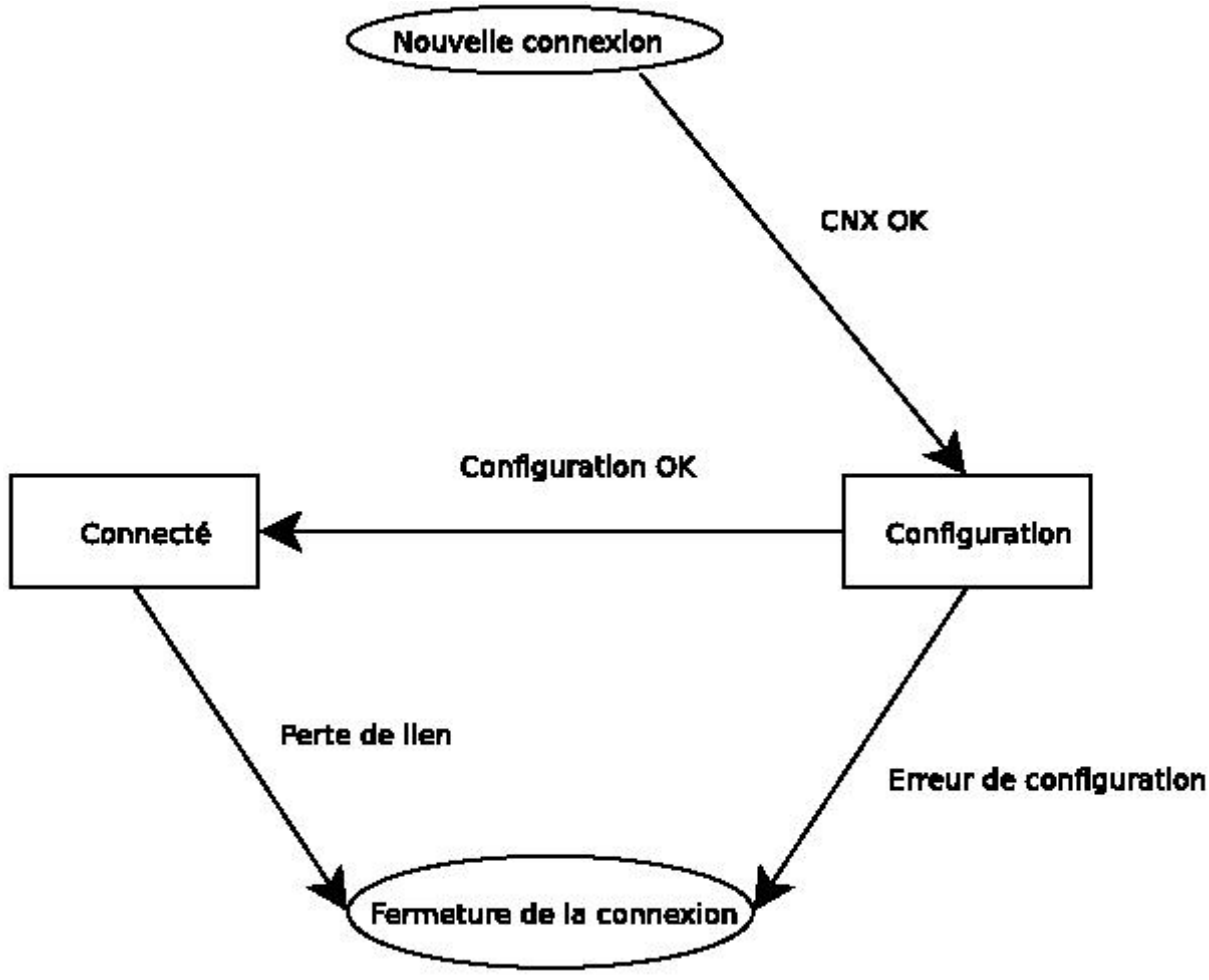

Figure 2.12 *: Etat du Bluetooth IP pour la station de base*

Bluetooth IP n'est pas la seule application de cette technologie. Elle peut être aussi associé à la technologie GPS que nous allons voir.

2.4 Beacon [2]

Beacon est une application réalisée par cinq étudiants de la Kent University. Ce programme, écrit en Java, consiste en une application pour téléphone portable mettant en relation le Bluetooth, le GPS et la gestion de messages (boîte de réception, temps de validité, anciens messages etc.). Il a été développé avec NetBeans et testé via l'émulateur de Sun : Wireless ToolKit.

Les interfaces qui le composent permettent tout d'abord de rechercher un GPS portable, de le coupler au téléphone et de le mémoriser pour une utilisation ultérieure. Puis, une fois le périphérique couplé, il offre la possibilité de mémoriser une ou plusieurs positions géographiques

(appelées « Locations ») et de leur associer des messages. Imaginons que nous voulions enregistrer une liste de courses et l'associer à un magasin donné. Pour ce faire, il faut se rendre dans le menu de création de nouveaux messages, rédiger la liste, lui donner une date limite de validité et l'associer à une position. La position sera donc, dans le cas présent, celle d'un magasin. Au moment où nous entrerons dans le magasin, le message associé sera ajouté à la boîte de réception du téléphone, pour autant que sa date de validité ne soit pas dépassée.

Beacon est donc un bon exemple de ce que peut être le trio Java, Bluetooth, GPS pour la mise à disposition d'un service de mémo géographique mobile. Voyons maintenant deux applications offrant un service de guidage par GPS.

2.5 Nav4All [3]

Nav4All consiste en une application de guidage sur téléphone portable. Via une interface complète, il permet de se guider dans le monde entier comme nous pourrions le faire avec une voiture équipée d'un GPS.

Son installation se fait directement depuis le site web de la société (compatible Wap) et s'adapte donc à quasiment n'importe quel téléphone. L'installation s'effectue de manière transparente pour l'utilisateur et propose l'emploi d'un GPS Bluetooth ou d'un GPS intégré (suivant votre téléphone) pour le guidage. Choisissez votre destination, et par connexion GPRS, l'itinéraire est calculé par les serveurs internet de Nav4all.

L'application étant fournie gratuitement, seul le coût de la communication est facturé par le fournisseur de téléphonie mobile. Une fois l'itinéraire calculé et rapatrié sur le téléphone, la connexion n'est plus nécessaire.

Le guidage est assuré de manière claire via des signaux graphiques et une synthèse vocale et peut, si vous ne possédez pas de GPS, se faire pas à pas en indiquant au programme à quelle étape précise de l'itinéraire vous en êtes

2.6 Amaze [5]

Amaze assure les mêmes fonctions que Nav4All, . Il y ajoute cependant la possibilité de visualiser, via des prises de vues aériennes, les détails d'une position géographique. Notez également la présence de POI Point Of Interest consistant à informer l'utilisateur des divers lieux ou services

intéressants proches de l'endroit où il se trouve et de celui où il souhaite se rendre. Les POI sont classés par catégories telles que restaurants, hôtels, monuments, services publics etc. Ajoutons enfin qu'un service de prévisions météorologiques est mis à disposition. Ceci comme le calcul de l'itinéraire, ayant bien évidemment le coût d'une connexi on GPRS.

Amaze met à disposition sur son site web la liste des téléphones supportés par la version finale et ceux dont l'application n'est qu'en version Beta, ainsi que plusieurs vidéos de démonstration visant à prendre en main rapidement les capacités du logiciel.

2.7 MGMaps [4]

Au contraire des deux autres appli cations ci-dessus, Mobile GMaps permet uniquement la visualisation de cartes et d'images aériennes sur téléphone mobile soit manuellement en sélectionnant une adresse, soit automatiquement en affichant votre déplacement grâce à un récepteur GPS. MGMaps est gratuit et utilise les banques de photos de Yahoo, Maps™, Windows Live Local™, Ask.com™ et Open Street Map™. Précisons également que le programme permet de suivre ses déplacements sur une carte via l'inscription gratuite à GMap -Track.

Conclusion

Grace à son architecture réseau, Bluetooth travaille dans plusieurs domaines et offre plusieurs applications comme citée ci-dessus .Notons que ces applications se basent sur la technologie GPS .Nous allons voir une des applications de la technologie Bluetooth que nous allons étudier qui est la télécommande via Bluetooth.

CHAPITRE 3

APPLICATION DU BLUETOOTH DANS LA TELECOMMANDE

La télécommande est l'une des choses qui facilitent la vie de l'homme . Actuellement, on peut télécommander la télé ou le radio par infrarouge, télécommander à distance un portail etc…..

Ce que nous allons voir c'est comment on utilise Bluetooth pour commander un ordinateur à distance et quels sont les profils et les protocoles qu'ils utilisent. Et à la fin nous allons donc réaliser une interface de commande. Dans notre réalisation, nous allons voir un exemple de commande qui est réalisé à l'aide d' un logiciel qui est le Bluetooth Remote Control .Dans cette réalisation nous avons besoin d'un téléphone mobile, d'un pc ayant un réseau Bluetooth. Mais pour bien comprendre le fonctionnement de cette application nous allons voir le protocole HID.

3.1 Composants du protocole HID

Dans le protocole HID, il y a 2 entités: la "host" et l'"appareil". Le dispositif est l'entité qui interagit directement avec un être humain, tel qu'un clavier ou une souris. L'hôte communique avec le dispositif et reçoit des données d'entrée du dispositif sur les actions effectuées par l'homme. Les données de sortie des flux de l'hôte vont vers le périphérique, puis à l'humain. L'exemple le plus commun d'un hôte est un ordinateur mais certains téléphones cellulaires et PDA peuvent également être des hôtes.

Le protocole HID permet la mise en œuvre des dispositifs très simples. Les dispositifs définissent leurs paquets de données et présentent ensuite un «descripteur HID » à l'hôte. Le descripteur HID est un tableau d'octets codés en dur qui décrivent les paquets de données de l'appareil . Cela comprend: le nombre de paquets chargé par le périphérique, de quelle taille sont les paquets, et le but de chaque octet et des bits dans le paquet. Par exemple, un clavier avec un bouton de programme calculatrice peut dire à l'hôte que le bouton pressé état libéré est stocké comme le bit deuxième dans l'octet de sixième en nombre de paquets de données 4 (ces emplacements n'ont qu'une valeur indicative et sont spécifiques du dispositif.). L'appareil stocke habituellement le descripteur HID dans la ROM et n'a pas besoin de comprendre ou d'analyser intrinsèquement le descripteur HID. Certaines souris et clavier matériel sur le marché d'aujourd'hui sont implémentés en utilisant seulement 8-bit du processeur.

L'hôte doit être une entité plus complexe que le dispositif. L'hôte a besoin de récupérer le descripteur HID de l'appareil et de l'analyser avant de pouvoir communiquer pleinement avec l'appareil. L'analyse du descripteur HID peut être compliquée.

Les systèmes d'exploitation multiples sont connus pour avoir livré des bugs dans le pilote de périphérique responsable de l'analyse des descripteurs HID. Après les pilotes de périphériques ont initialement été diffusés au public. Cependant, cette complexité est la raison pour laquelle l'innovation rapide avec des périphériques HID est possible.

Le mécanisme décrit ci-dessus ce qui est connu comme protocole rapport HID. Comme il était entendu que tous les hôtes ne seraient capables d'analyser les descripteurs HID, HID définit également le protocole d'amorçage. Dans le protocole de démarrage, seuls des appareils spécifiques sont pris en charge avec seulement les caractéristiques car les formats de données par paquets fixes sont utilisés. Le descripteur HID n'est pas utilisé dans ce mode si l'innovation est limitée. Cependant, l'avantage est que la fonctionnalité minimale est toujours possible sur des hôtes qui, autrement, seraient incapables de soutenir HID. Les dispositifs de prise en charge uniquement dans le protocole d'amorçage sont le clavier et la souris. Nous allons maintenant voir le profil HID.

3.2 Le profil Human Interface Device HID

Le profil HID définit les protocoles, les procédures et les caractéristiques pour être utilisé par Bluetooth HID comme les claviers, les dispositifs de pointage, dispositifs de jeux et dispositifs de contrôle à distance. Le HID définit deux rôles, celui d'un Human Interface Device (HID) et un hôte.

Le profil HID utilise le bus série universel (USB), la définition d'un dispositif HID afin de tirer parti des pilotes de classe existantes pour les appareils USB HID. Le profil HID décrit com ment utiliser le protocole USB HID et comment un appareil compatible Bluetooth peut prendre en charge les services HID en utilisant la couche L2CAP. Le profil HID est conçu pour permettre l'initialisation et le contrôle de soi-décrivant les périphériques ainsi que de fournir un lien faible latence avec une faible consommation électrique.

Les HID profil Bluetooth reposent sur les génériques Access Profile (GAP). Afin d'assurer la mise en œuvre plus simple possible, le protocole HID fonctionne nativement sur L2CAP et n'utilise que le Service Discovery Protocol.

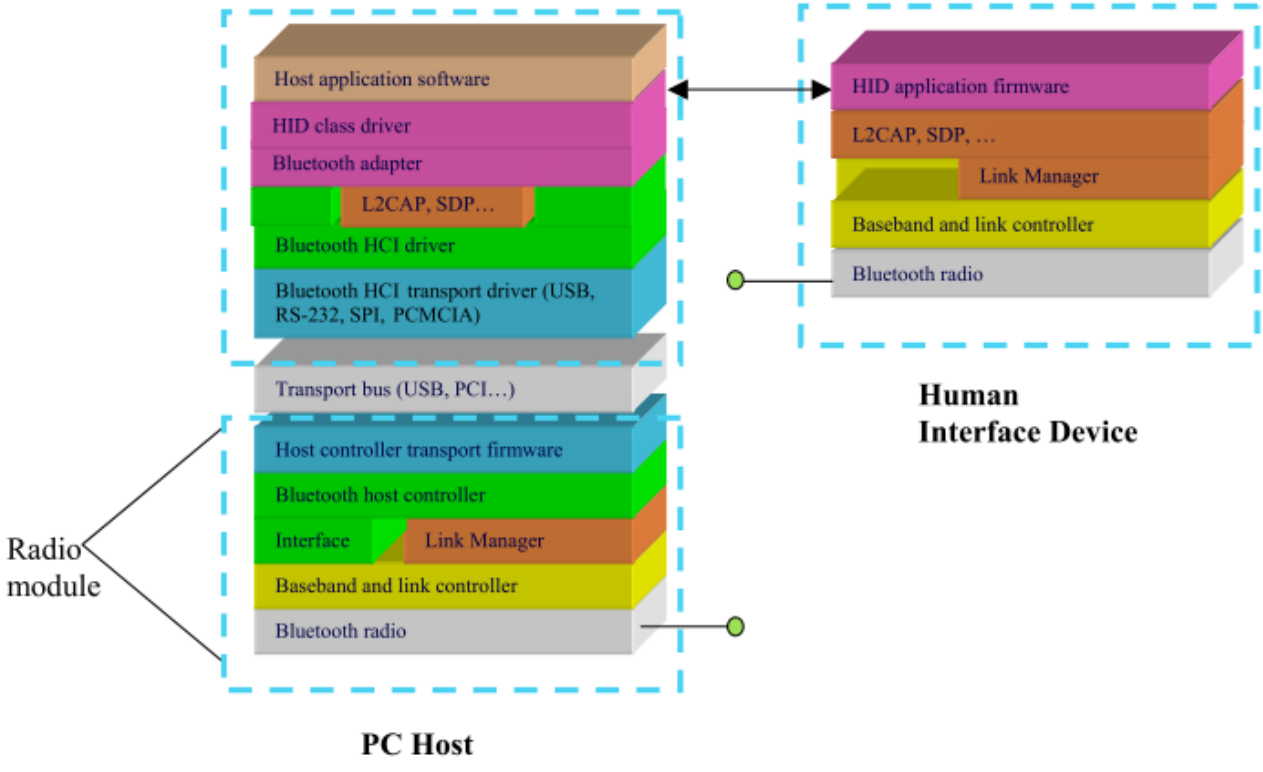

Figure 3.01 *: Profil HID*

3.3 Bluetooth HID Exigences d'accueil

3.3.1 Application et exigences d'accueil [13] [14]

3.3.1.1 Conformité générique HID

Les applications PC hôte doivent être conçues pour fonctionner avec un dispositif HID indépendamment du bus de communication qui les relie. Les PC applications HID doivent se conformer à la règle standard d'un client HID pour la plate-forme et système d'exploitation en question.

3.3.1.2 Format fixe Reporting

Les ressources limitées applications hôte non-PC qui mettent en œuvre HID peuvent éventuellement choisir de mettre en œuvre que le protocole d'amorçage, qui est le niveau minimum requis de la fonctionnalité d'accueil. Cette méthode de déclaration à format fixe élimine le besoin de l'analyseur HID.

Il existe des protocoles de démarrage pour les dispositifs de pointage et des claviers. Le support des fonctionnalités protocole de démarrage et de commande est facultatif pour les hôtes.

3.3.1.3 Règle pour le niveau minimum d'accueil

Afin d'assurer un niveau de base de l'interopérabilité entre les hôtes HID Bluetooth et les dispositifs, Bluetooth HID hôtes qui prennent en charge tout type de dispositif de pointage ou de la fonctionnalité du clavier ont pour objet de soutenir le dispositif correspondant au pointage ou au protocole de démarrage du clavier, ou au protocole normal HID. Le support du protocole HID normal chez l'hôte fournit un clavier du mode de démarrage et de support de la souris, par définition.

3.3.2 Soutien de pilote HID

3.3.2.1 Interface pilote de classe HID à pile Bluetooth

Les hôtes avec l'appui existants pour le protocole HID fonctionnent sur USB doit fournir un pilote de la carte, ce qui génère et décode l'entête du paquet L2CAP nécessaire et demande pour l'exécution du protocole HID sur un canal de données Bluetooth. Le pilote de la carte d'hôte doit fournir les moyens aux applications afin d'établir et de mettre fin aux connexions protocole HID sur un périphérique Bluetooth Human Interface. De même, il doit permettre à Bluetooth Human Interface Devices d'établir et de mettre fin aux connexions protocole HID à l'application hôte après la liaison initiale terminée. Les hôtes lancent toujours le couplage.

3.3.2.2 Support du protocole L2CAP HID

La mise en œuvre de L2CAP sur l'hôte devrait se réunir au minimum par défaut un MTU (unité de transmission maximale) de 48 octets, même si la valeur par défaut de 672 est recommandée. Le pilote de la carte d'accueil BT-HID devrait mettre en œuvre la segmentation et le réassemblage de paquets à la plus grande dimension pratique (64ko maximum) afin de maintenir la compatibilité avec tous les possibles HID Bluetooth, mais ce n'est pas requis pour les hôtes qui ne supportent que le mode de démarrage Protocole.

3.3.2.3 Support SDP dans Host

L'hôte est tenu de mettre en œuvre un client SDP.

3.3.3 Exigences générales L2CAP [13]

3.3.3.1 QoS (Quality of Service) Exigences

Le protocole HID a été mis en œuvre sur l'Universal Serial Bus. USB fournit le matériel qui peut garantir au maximum la latence des données vers et à partir de HID au moyen des conduites d'interruption. Bien que Bluetooth 1.1 contient un support pour les canaux synchrones (liens SCO) avec une latence garantie, sont destinés à la voix, et tout autre trafic est placé sur le ca nal ACL. Le canal ACL et ses abstractions de niveau supérieur ne contiennent pas de mécanismes de matériel pour hiérarchiser les données des canaux L2CAP une sur l'autre, de sorte que toute la qualité des demandes de service à la couche L2CAP connexion doi vent être traitées par un logiciel ou L2CAP couche inférieure.

3.3.3.2 Utilisation des identificateurs de canaux L2CAP (CID)

Dans le cas des multifonctions Human Interface Devices (tels que le clavier avec dispositif de pointage intégré), le protocole HID permet de distinguer l'origine ou la destination des données au moyen d'identifiants rapport. Ainsi, les CID différentes ne sont pas nécessaires pour chaque fonction dans un appareil multifonctions.

3.3.4 Exigences en matière de niveau Link

3.3.4.1 Authentification, couplage, collage

Le support de l'authentification, l'appariement et le collage des routines dans les hôtes et les applications des appareils Bluetooth Human Interface sont facultative s, bien que l'authentification soit fortement encouragée et le cryptage est recommandé pour les programmes de l'application hôte obligeant les utilisateurs à entrer des informations sensibles sur un clavier Bluetooth ou un clavier. Il est normalement sur la responsabilité de l'hôte d'engager des procédures de sécurité, mais HID sont éventuellement autorisés à engager l'authentification (après appariement initial, initié par l'hôte, qui a été terminé) pour éviter l'usurpation d'accueil. Les hôtes doivent être capables d'initier l'authentification et la liais on avant et après la connexion de bande de base établie.

3.3.4.2 Considérations spéciales pour les claviers

Pour le jumelage entre clavier Bluetooth et clavier simple, il faut saisir le mot de passe sur un hôte qui peut ne pas avoir un clavier filaire ou une autre méthode alternative d'entrée pour le mot de passe. Dans ce cas, il est recommandé à l'hôte de générer un code de mot de passe aléatoire qui peut être affiché à l'utilisateur pour l'entrée dans le clavier Bluetooth ou un clavier. Un clavier peut être identifié sans effectuer le Service Discovery à l'aide de la catégorie de bits de périphériques qui est retournée dans le paquet FHS lorsque le clavier répond à une enquête. L'hôte peut trier les réponses du dispositif basé sur ce domaine.

La plupart des claviers n'ont pas connaissance de ce qui est imprimé sur le dessus des touches, au lieu d'envoyer un code d'analyse à l'hôte qui interprète alors le code différemment en fonction du réglage de la langue est en vigueur. Lorsque le mot de passe Bluetooth est inscrit, il n'est pas transmis à l'hôte, de sorte que le clavier doit faire des hypothèses sur ce qui est sur le dessus des touches. Une hypothèse forte pour les fabricants de claviers multi-langue, c'est que les touches numériques sont compatibles entre les langues. Par conséquent, un accueil sans autre moyen de saisie de l'utilisateur ne devrait demander un mot de passe numérique pour les claviers.

3.3.4.3 Hôtes avec une fonction d'entrée Limited

Dans le cas où la liaison avec un nouveau clavier Bluetooth est nécessaire et il n'y a pas d'autres moyens de répondre aux invites pour procéder à la procédure de jumelage, une connexion non sécurisée peut être établie à fins de demander à l'accueil de commencer le processus de jumelage. Dans ce cas, l'application hôte ou d'accueil veillent à ce que le fonctionnement du clavier ne peut pas continuer sans effectuer le processus de jumelage.

3.3.4.4 Utilisation du cryptage

Le cryptage est fortement recommandé pour les applications hôtes qui permettent d'entrer des informations sensibles telles que les noms d'utilisateur et mots de passe via un clavier Bluetooth ou un clavier. Tous les claviers Bluetooth ont pour objet de soutenir n'importe quelle taille de clé de chiffrement, de 8 à 128 bits, demandé par une application. Il est toujours de la responsabilité de l'hôte d'ouvrir la procédure de cryptage et les hôtes sont tenues toujours d'accepter les demandes de cryptage si le cryptage est pris en charge.

3.3.5 Règles Gestionnaire de connexion

3.3.5.1 Mise en place connexion HID Protocole

Les deux canaux HID_Control et HID_Interrupt L2CAP sont établies pour que la connexion protocole HID soit considérée comme établi. La connexion HID_Control doit être lancée le premier. Il est permis à l'hôte (ou le dispositif, en cas de reconnexion dispositif initié) pour configurer les deux canaux simultanément (la séquence de configuration peuvent se chevaucher). Les canaux HID doivent être fermés dans l'ordre inverse, c'est à dire 'interruption puis control.

3.3.5.2 Reconnexion après Reset hôte

Si l'attribut SDP HIDReconnectInitiate est False, l'application hôte ou l'hôte est respon sable de rétablir ou d'ouvrir la connexion au HID après que l'hôte soit remis à zéro. Si HIDReconnectInitiate est vrai et SDP attribut HIDNormallyConnectable est également vrai, l'hôte peut également tenter de se reconnecter après sa remise à zéro.

Notez que de nombreux PC BIOS ne saura pas lire la capacité du drapeau HIDReconnectInitiate si le Service Discovery Protocole n'est pas mis en œuvre. Pour cette raison, il est recommandé que les claviers conçus pour une utilisation avec un PC soient toujours connectables (HIDNormallyConnectable = True) afin qu'ils puissent être découverts au moment du démarrage .

3.3.5.3 Support du mode Page

L'hôte demande une connexion à un périphérique HID exerçant la séquence de pagination pour au moins 2,56 secondes, ou le temps minimum nécessaire pour atteindre un dispositif de balayage page R2 mode sans connexions SCO présente.

3.3.5.4 Page Scan Mode Support

Les appareils qui fonctionnent comme des esclaves des contrôles à distance HID qui initient la connexion en tant que maîtres ont pour objet de soutenir la page appropriée Bluetooth mode de balayage qui correspond à la durée souhaitée de contrôle à distance d'intervention .

3.3.5.5 Résiliation et Re-Création de connexion

La responsabilité de rétablir une connexion suspendue doit être déterminé e par le bit SDP HIDReconnectInitiate.

Dans le cas d'une connexion interrompue en raison d'une rupture de -gamme ou d'une condition d'interférence, le dispositif SDP évalue la valeur booléenne de HIDReconnectInitiate, la valeur True, indique que le HID sera principalement responsable de rétablissement de la connexion. Si cela est faux, ce qui indique l'hôte est principalement responsable de rétablissement de la connexion. Si l'appareil a cette valeur SDP valeur false, le dispositif doit entrer dans la page mo de de balayage en cas de perte de connexion pour permettre à l'hôte de se reconnecter. De même, si le dispositif a cette valeur SDP true, l'hôte devrait entrer dans la page mode de balayage pour permettre au dispositif de se reconnecter. Lorsque reconnexio n automatique est utilisé avec HID, il est recommandé d'utiliser l'attribut SDP HIDSupervisionTimeout pour atteindre la réactivité supplémentaires rétablissement de la connexion. Les dispositifs qui déclare SDP attribut HIDNormallyConnectable = True sont t oujours dans la page mode de balayage (lorsqu'il n'est pas connecté) et peut toujours être paged par l'hôte, indépendamment des autres paramètres SDP.

3.3.5.6 Échec de reconnexion

Si l'hôte ou le dispositif HID tentent de se reconnecter après que la connexion soit perdue pour une raison inconnue, chaque camp doit faire un time-out et cesse la tentative de se reconnexion au bout de 30 secondes. L'intervention de l'utilisateur manuel est acceptable pour ré-initier le processus de reconnexion après que la tentative du délai d'attente soit expirée.

3.3.5.7 Types de paquets hôtes

L'HID soutient DM1, POLL, NULL, et les types de paquets FHS de maintenir un niveau minimal d'interopérabilité avec les appareils conformes au profil Bluetooth HID (voir Annexe 3.5).

3.3.5.8 Support des modes de basses Power Link

Le gestionnaire de Link sur les hôtes HID est toujours esclave de permettre à l'initiative modes SNIFF. Le mode SNIFF est obligatoire pour les hôtes, tandis que les modes Park et HOLD sont facultatifs. Le temps de réponse à UNSNIFF et déparcage ou remise en circulation ne devrait pas être plus d'un intervalle de balise en l'absence de collisions qui se produisent en SCO. Les hôtes qui ont de grandes quantités de données à envoyer à l'HID alors que le lien est dans l'un des modes de faible puissance sont responsables de remise en circulation ou du mode UNSNIFF si cela est nécessaire pour transmettre les données à l'HID avec le débit requis.

Rappelons que le mode SNIFF est à faible consommation, Park à très basse consommation et Hold à liaison SCO seulement.

Le temps de réponse est généralement plus de deux intervalles d'interrogation avant que les données puissent être envoyées, l'une pour la demande unsniff, l'autre pour la réponse de l'hôte, puis la réponse avec des données de sondage suivant l'hôte.

3.3.5.9 Enquêtes ou inquiry

Les hôtes d'interprétation enquête HID ou inquiry pour découvrir qui sont limités doivent se faire en utilisant le code d'accès enquête Limited (CAIJ). Toutefois, HID peut soutenir soit « limitée mode Détection » ou « Découvrable général » tel défini par le Generic Access Profile.

3.3.6 Soutien du périphérique d'amorçage

3.3.6.1 Exigences BIOS pour le soutien de périphériques de démarrage

Afin de fournir un complet clavier Bluetooth et la fonctionnalité périphérique de pointage dans un hôte basé sur PC, le clavier ou la souris de contrôle est souvent nécessaire avant que le système d'exploitation est chargé, pour la configuration système de bas niveau. Pour les claviers et souris Bluetooth puissent fonctionner comme les claviers filaires, le BIOS du PC doit contenir firmware qui comprend la façon de communiquer des claviers et des dispositifs de pointage sur une radio Bluetooth. Si la sécurité est un problème, le jumelage et les procédures d'authentification doit également être effectuée par le BIOS, et la clé résultante partagée avec le système d'exploitation. Bluetooth HID dispositifs de pointage et les claviers sont nécessaires pour soutenir le mode protocole de démarrage.

Depuis que le clavier sans fil et le soutien de la souris nécessitent une mise à jour BIOS pour la plupart des ordinateurs personnels, une autre méthode qui peut être utilisée pour la compatibilité descendante est de développer un USB ou d'une combinaison adaptateur USB/PS2 Bluetooth qui émule le fonctionnement d'un clavier filaire et une souris USB lorsque le protocole HID est en mode de démarrage. Lorsque le protocole est mis en mode normal avec la commande SET_PROTOCOL, l'adaptateur hôte Bluetooth peut énumérer comme un périphérique USB normal Bluetooth.

Le BIOS de votre PC peut utiliser la classe de bits de périphériques dans le paquet F HS qui permet de découvrir une souris et un clavier comme une alternative à la lecture du dossier SDP de l'appareil.

3.3.6.2 Clavier Répétition automatique Fonctionnalité

En mode protocole de démarrage (entrée avec la commande SET_PROTOCOL), Blueto oth HID claviers et claviers fournissent les fonctionnalités clés de répétition automatique interne, comme les claviers USB HID. En mode protocole complet HID, la fonctionnalité autorépétition est prévue dans l'hôte. Toutefois, il convient de noter que la perte de lien après un événement touche enfoncée pourrait générer des frappes involontaires jusqu'à ce que le délai d'attente lien se produit . Après avoir vues quelques explications du protocol e HID, voici un exemple de création d'une télécommande en utilisant Bluetooth Remote Control .

3.4 Bluetooth Remote Control [15]

Bluetooth Remote Control est un logiciel téléchargeable sur Internet .C'est un logiciel de création de menu de télécommande sur les marques de mobile Sony Ericsson qui marche sur Windows .Plus précisément, il crée un fichier « .hid »qui est fonctionnel. Voyons donc le fonctionnement de ce logiciel.

3.4.1 Fichier « hid »

Les fichiers hid sont des archives tar contenant une sorte de XML made in sony ericsson, ainsi qu'une image png. On peut donc les traiter comme des archives tar. Étudions ce pseudo XML (.kcf) de plus près.

3.4.1.1 Le format XML (.kcf)

.Fonctionnement

Son fonctionnement est très simple. Il y a des balises KEY_foo qui représentent chaque touche.<KEY_foo>.

...

</KEY_foo>

À l'intérieur des balises de touche, les balises ACTION permettent de déterminer ce qui est fait lorsqu'on presse la touche.

<ACTION>

...

</ACTION>

Enfin, encore à l'intérieur, vous définissez à quelle combinaison de touches correspond la touche du téléphone. Par exemple,

<KEYBOARD MODIFIERS = "01" USAGEID = "51"/>

<!-- VOL DOWN - (Ctrl + Down) -->

KEYBOARD MODIFIERS (ici 01) est appelé le modificateur. Les modificateurs sont les touches de type Ctrl, Alt, Shift. Sachez que 01 correspond au modificateur Ctrl

USAGEID (ici 51) est la touche concernée. La touche 51 de l'exemple correspond à "flèche bas" sur le clavier.

Autrement dit, Si l'on reprend l'exemple décortiqué :

<KEY_VOL_DOWN>

<ACTION>

<KEYBOARD MODIFIERS = "01" USAGEID = "51"/>

<! -- VOL DOWN - (Ctrl + Down) -->

</ACTION>

</KEY_VOL_DOWN>

On vient d'écrire que lorsqu'on va presser le bouton VOL DOWN du téléphone (sur le côté, la touche pour baisser le son), celui-ci doit envoyer à l'ordinateur l'ordre d'effectuer la combinaison de touche Ctrl+flèche bas.

3.4.1.2 Correspondances des touches

a. Les Modificateurs

Les modificateurs (qui sont donc les touches Ctrl, Alt, Shift) sont un masque de valeurs prises une à une. Autrement dit, il suffit de les additionner pour obtenir le code voulu.

Ex: Ctrl vaut 1, Shift vaut 2, donc Shift+Ctrl = 3… (0 pour n'avoir aucun modificateur) Voici un petit tableau de correspondance :

Rien	00
Ctrl	01
Shift	02
Alt	04

Tableau 3.01 *: Correspondances des touches*

b. Les autres touches [14]

La correspondance entre les quelques touches et leurs codes hexadécimaux dans la colonne USAGEID est donnée par le tableau suivant, elle est basée sur un clavier QWERTY :

ID	USAGE NOM
08	Keyboard e and E
09	Keyboard f and F
0A	Keyboard g and G
0B	Keyboard h and H
0C	Keyboard i and I
0D	Keyboard j and J
0E	Keyboard k and K
0F	Keyboard l and L
10	Keyboard m and M
11	Keyboard n and N
12	Keyboard o and O
13	Keyboard p and P
14	Keyboard q and Q
29	Keyboard ESCAPE
2A	Keyboard DELETE (Backspace)
2B	Keyboard Tab
2C	Keyboard Spacebar
2D	Keyboard - and (underscore)
2E	Keyboard = and +
2F	Keyboard [and {
30	Keyboard] and}

31	Keyboard \ and |
32	Keyboard Non-US # and ~2
33	Keyboard ; and :
34	Keyboard ‘ and “
35	Keyboard Grave Accent and
36	Keyboard, and <
37	Keyboard . and >
38	Keyboard / and ?
39	Keyboard Caps Lock
3A	Keyboard F1
46	Keyboard PrintScreen
47	Keyboard Scroll Lock
48	Keyboard Pause
49	Keyboard Insert
4A	Keyboard Home
4B	Keyboard PageUp
4C	Keyboard Delete Forward
4D	Keyboard End
4E	Keyboard PageDown
4F	Keyboard RightArrow
50	Keyboard LeftArrow
51	Keyboard DownArrow
52	Keyboard UpArrow
69	Keyboard F14
6A	Keyboard F15
6B	Keyboard F16
6C	Keyboard F17
6D	Keyboard F18
6E	Keyboard F19
6F	Keyboard F20
70	Keyboard F21
71	Keyboard F22
72	Keyboard F23
74	Keyboard Execute

Tableau 3.02 *: Correspondances des autres touches*

Voici un exemple de fichier « .hid ».executable.

3.4.2 Exemples de fichier « .hid »

Voici un fichier .hid capable de fermer toutes les applications et de verrouiller une session sous Windows xp. Il est créé à partir de Bluetooth Remote Control.

```
<SONY_ERICSSON_REMOTE_CONTROL_CONFIGU RATION VERSION="1.0">
<KEYMAP>
<KEY_1>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="29"/>
</ACTION>
</KEY_1>
<KEY_2>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="52"/>
</ACTION>
</KEY_2>
<KEY_3>
<ACTION>
<KEYBOARD MODIFIERS="04" USAGEID="3D"/>
</ACTION>
</KEY_3>
<KEY_4>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="50"/>
</ACTION>
</KEY_4>
<KEY_5>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="28"/>
</ACTION>
</KEY_5>
<KEY_6>
```

<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="4F"/>
</ACTION>
</KEY_6>
<KEY_7>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="43"/>
</ACTION>
</KEY_7>
<KEY_8>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="51"/>
</ACTION>
</KEY_8>
<KEY_9>
<ACTION>
<KEYBOARD MODIFIERS="08" USAGEID="0F"/>
</ACTION>
</KEY_9>
<KEY_LSK>
<ACTION>
<MOUSE BUTTONS="Left"/>
</ACTION>
</KEY_LSK>
<KEY_RSK>
<ACTION>
<MOUSE BUTTONS="Right"/>
</ACTION>
</KEY_RSK>
<KEY_LEFT>
<ACTION>
<MOUSE MOVEMENT="Left"/>

```
</ACTION>
</KEY_LEFT>
<KEY_RIGHT>
<ACTION>
<MOUSE MOVEMENT="Right"/>
</ACTION>
</KEY_RIGHT>
<KEY_UP>
<ACTION>
<MOUSE MOVEMENT="Up"/>
</ACTION>
</KEY_UP>
<KEY_DOWN>
<ACTION>
<MOUSE MOVEMENT="Down"/>
</ACTION>
</KEY_DOWN>
</KEYMAP>
</SONY_ERICSSON_REMOTE_CONTROL_CONFIGURATION>
```

Voici un autre fichier .hid capable d'arrêter, redémarrer, mettre en veille l'ordinateur. Pour cela, on crée des raccourcis claviers et on les combines aux touches du téléphone.

```
<SONY_ERICSSON_REMOTE_CONTROL_CONFIGURATION VERSION="1.0">
<KEYMAP>
<KEY_1>
<ACTION>
<KEYBOARD MODIFIERS="04" USAGEID="3D"/>
</ACTION>
</KEY_1>
<KEY_2>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="29"/>
</ACTION>
```

```
</KEY_2>
<KEY_3>
<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="15"/>
</ACTION>
</KEY_3>
<KEY_4>
<ACTION>
<KEYBOARD MODIFIERS="08" USAGEID="08"/>
</ACTION>
</KEY_4>
<KEY_5>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="3A"/>
</ACTION>
</KEY_5>
<KEY_6>
<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="13"/>
</ACTION>
</KEY_6>
<KEY_7>
<ACTION>
<KEYBOARD MODIFIERS="08" USAGEID="0F"/>
</ACTION>
</KEY_7>
<KEY_8>
<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="4C"/>
</ACTION>
</KEY_8>
<KEY_9>
```

<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="04"/>
</ACTION>
</KEY_9>
<KEY_STAR>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="2B"/>
</ACTION>
</KEY_STAR>
<KEY_0>
<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="14"/>
</ACTION>
</KEY_0>
<KEY_HASH>
<ACTION>
<KEYBOARD MODIFIERS="05" USAGEID="11"/>
</ACTION>
</KEY_HASH>
<KEY_VOL_UP>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="41"/>
</ACTION>
</KEY_VOL_UP>
<KEY_VOL_DOWN>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="42"/>
</ACTION>
</KEY_VOL_DOWN>
<KEY_CAM>
<ACTION>
<KEYBOARD MODIFIERS="00" USAGEID="2C"/>

</ACTION>

</KEY_CAM>

<KEY_LSK>

<ACTION>

<MOUSE BUTTONS="Left"/>

</ACTION>

</KEY_LSK>

<KEY_RSK>

<ACTION>

<MOUSE BUTTONS="Right"/>

</ACTION>

</KEY_RSK>

<KEY_UP>

<ACTION>

<MOUSE MOVEMENT="Up"/>

</ACTION>

</KEY_UP>

<KEY_DOWN>

<ACTION>

<MOUSE MOVEMENT="Down"/>

</ACTION>

</KEY_DOWN>

</KEYMAP>

</SONY_ERICSSON_REMOTE_CONTROL_CONFIGURATION>

Une fois le fichier créé, on l'envoie sur le mobile via Bluetooth par exemple puis on l' exécute. Voici l'interface de commande qu'on a créée

Figure 3.02 *: Interface de commande du téléphone*

En appuyant sur la touche q, on peut arrêter le pc au bout de 30s. En appuyant sur la touche n on peut arrêter cet arrêt automatique. En appuyant sur la touche a, on peut arrêter sur le champ l'ordinateur. Les autres touches servent de raccourcis pour le clavier ou ouvrir des applications.

Figure 3.03 *: Ordinateur commandé*

Conclusion

Pour que la télécommande mobile clavier souris Bluetooth puisse être utilisée, on a besoin du profil HID et cette télécommande peut varier selon le besoin de l'utilisateur. La technologie Bluetooth offre plusieurs points d'application et ouvre dans plusieurs domaines en utilisant ces profils. Cela nous amène à tirer une conclusion générale sur ce livre de mémoire.

Conclusion générale

Bluetooth est une technologie sans fil de type IEEE .802.15.C'est une évolution du port RS232 et de l'USB. Il fonctionne sur la bande de fréquence 2,4 GHz.et utilise 79 fréquences différentes. Il permet d'atteindre en full duplex 1600 échanges par secondes ce qui nous donne au final quand on enlève les informations de contrôle un débit d'environ 1 Mbit par second e mais avec une portée faible de plusieurs mètres seulement. Il est destiné à un usage personnel et se classe dans la catégorie PAN (Personal Area Network), Bluetooth utilise une architecture basée sur des profils, qui offrent des fonctions précises. Grace à ses profils, on peut l'associer à plusieurs applications comme dans la télécommande mobile clavier souris Bluetooth que nous avons vu.

Cette télécommande a pour avantage la liberté de mouvement d'où l'encombrement est moins important, mais aussi la rapidité d'exécution. Mais l'inconvénient est qu'on ne peut utiliser toutes les touches du clavier numérique simple car les touches du téléphone sont insuffisantes. Toutefois, des améliorations devraient être apportées du point de vue matériel et logiciel utilisé. On peut envisager de visualiser dans l'écran du téléphone l'image à l'écran de l'ordinateur ayant ainsi une seule vue pour faciliter les manipulations. On peut aussi envisager de télécommander le téléphone mobile à l'aide du pc par Bluetooth. Ainsi, les constructeurs des marques de mobile ne cessent d'améliorer et d'exploiter ce réseau promettant. Durant la publication du Bluetooth 1.2, un débit 3 fois plus rapide pour une consommation 2 fois moindres a été promouvu. Ce qui sera toujours insuffisant pour faire du réseau mais sera encore plus performant pour les applications actuelles de faible consommation telles que les oreillettes pour téléphones portables et autres souris sans fil.

ANNEXES

ANNEXE 1 : HISTORIQUE DU BLUETOOTH

A1.1 Origine du nom

Le nom Bluetooth est directement inspiré du roi danois Harald Ier surnommé Harald Blåtand (« homme 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.

A1.2 Historique

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 Spécial Interest Group (SIG)

juillet 1999 : sortie de la spécification 1.0

Le 28 mars 2006, le « Bluetooth Special Interest Group » (SIG) annonce la deuxième génération de la technique sans fil Bluetooth, qui est capable d'assurer des débits cent fois supérieurs à l'ancienne version, passant donc de 1 Mb/s à 100 Mb/s (soit 12,5 Mo/s). Cette technique utilisée dans les téléphones mobiles, périphériques informatiques et autres appareils portables comme les assistants personnels (PDA) a vu sa vitesse de transmission augmenter année après année, lui permettant ainsi d'être utilisée pour les vidéos haute définition et l'échange de fichiers avec un baladeur MP3 par exemple. La nouvelle norme incorporera une technique radio, connue comme l'ultra wideband ou UWB.

A1.3 Spécification

Le SIG travaille sur la spécification de la norme, qui a évolué des versions 1.0, 1.1, 1.2, 2.0, 2.0 + EDR (Enhanced Data Rate), 2.1 + EDR et 3.0.

A1.4 Normes Bluetooth

Le standard Bluetooth se décompose en différentes normes :

IEEE 802.15.1 définit le standard Bluetooth 1.x permettant d'obtenir un débit de 1 Mbit/s ;

IEEE 802.15.2 propose des recommandations pour l'utilisation de la bande de fréquence 2,4 GHz (fréquence utilisée également par le Wi-Fi). Ce standard n'est toutefois pas encore validé ;

IEEE 802.15.3 est un standard en cours de développement visant à proposer du haut débit (20 Mbit/s) avec la technique Bluetooth ;

IEEE 802.15.4 est un standard en cours de développement pour des applications sans fils à bas débit et à faibles coûts. Il est actuellement utilisé par Zigbee pour ses couches basses.

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.

A1.5 Accès au canal de transmission

Afin de pouvoir l'utiliser au niveau planétaire, la technologie Bluetooth opère dans la bande ISM. Cette bande de fréquence est libre d'utilisation partout dans le monde (sauf restriction au Japon, France et Espagne).

De nombreux systèmes sont utilisés dans cette bande de fréquence libre. On peut citer WLan, écouteurs sans fil, système de sécurité pour les voitures et les fours à micro ondes. Bluetooth utilise une technique efficace (mais qui ne l'est pas toujours) pour éviter les interférences qui s'appelle les sauts de fréquence (appelé Frequency Hopping ou FH). Le FH a été inventé durant la seconde guerre mondiale par Hedy Lammarr .Le principe est d'effectuer, comme son nom l'indique, des sauts de fréquence après chaque transmission (voir Figure A.01).

L'émetteur et le récepteur doivent connaître la séquence des sauts pour que la communication soit possible. Chaque saut est appelé hop .Dans Bluetooth, le nombre normal de hops par seconde et de 1600.

La modulation utilisée est GFSK (Gaussian Frequency Shift Keying) avec un BT = 0.5.

La représentation binaire du 1 est une déviation positive de fréquence et pour le 0 une déviation négative de fréquence. Le débit brut binaire est de 1 Mbit/s.

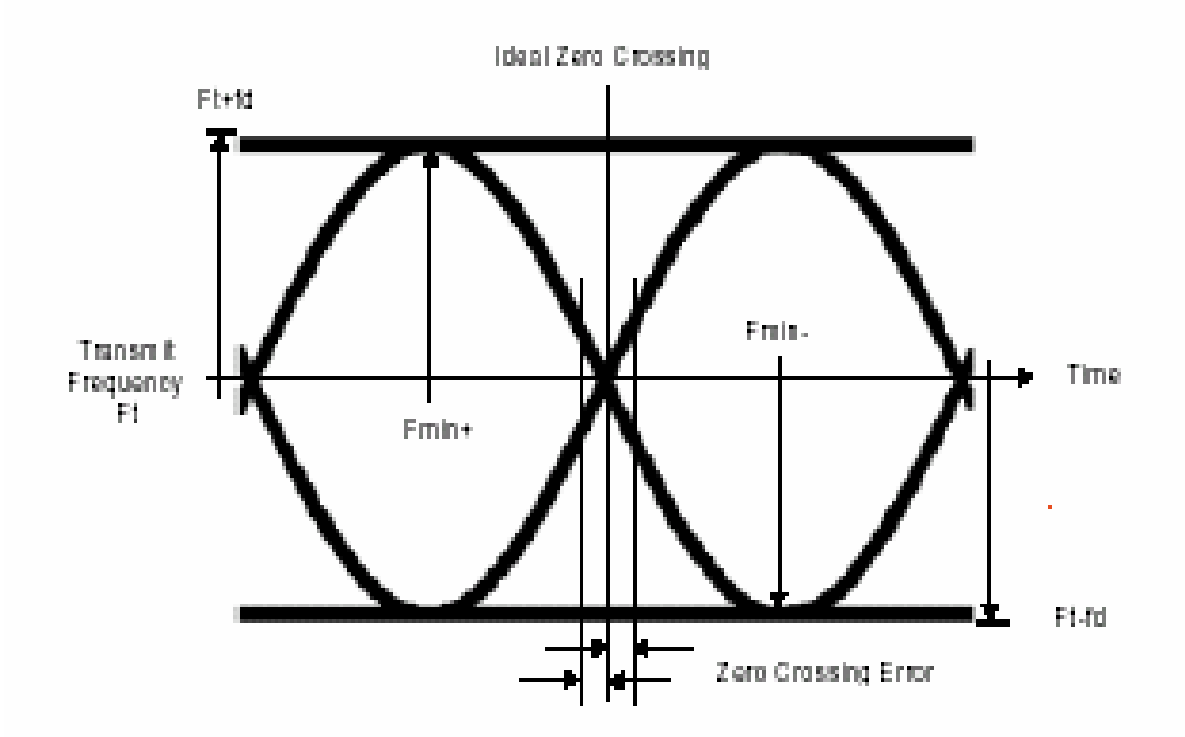

Figure A.01 : *modulation GFK* [13]

Un canal logique Bluetooth est une séquence pseudo-aléatoire qui permet aux différents dispositifs d'utiliser les mêmes sauts de fréquence. Entre chaque hop, un slot de temps de 625 microsecondes est numéroté de manière cyclique de 0 à 2^{27}-1.

Le cycle total dure :

$$T_{cycle}=2^{27}\cdot 625\cdot 10^{-6}=83886[s] \qquad (1.01)$$

Cette équation donne comme résultat 23,3 heures.

Bien évidemment, deux dispositifs utilisant des canaux logiques différents ne peuvent communiquer entre eux.

A1.6 Les adresses Bluetooth

Dans la spécification de Bluetooth, il existe quatre types d'adresse.

-La BD_ADDR (Bluetooth Device Address) est la correspondance de l'adresse MAC IEEE MAC. Elle identifie de manière univoque, comme l'adresse MAC, les dispositifs Bluetooth entre eux.

Elle se décompose en 3 parties bien distinctes :

-NAP (partie non significative de l'adresse) qui regroupe de 16 bits, cette partie est utilisée pour l'encryption

-UAP (partie haute de l'adresse) qui regroupe de 8 bits, cette partie sert à initialiser le HEC et le CRC mais aussi pour les sauts de fréquence.

-LAP (partie basse de l'adresse) regroupe 24 bits. Cette partie sert à créerun mot de synchronisation.

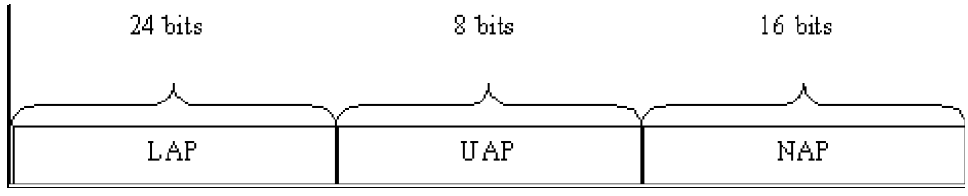

Figure A.02 : *Représentation de l'adresse BD_ADDR*

L'adresse du maître de chaque piconet doit être connue par tous les esclaves pour que tous les dispositifs du piconet utilisent les mêmes sauts de fréquence.

-La AM_ADDR (adresse de membre actif) est une adresse de 3 digits temporaire que chaque membre actif d'un piconet reçoit de la part du maître. Cette adresse sert aux esclaves pour savoir si un paquet leur est destiné et au maître pour différencier les réponses des différents esclaves. L'adresse 000 est utilisée pour le Broadcasting, c'est pour cette raison qu'il y a maximum 7 esclaves actifs par piconet.

-La PM_ADDR (adresse de membre parqué) est une adresse de 8 digits temporaire que chaque esclave parqué d'un piconet reçoit de la part du maître. Un esclave détient uniquement une PM_ADDR quand il est parqué et la perd quand il devient actif.

-La AR_ADDR (adresse de requête d'accès) est une adresse utilisée par les esclaves parqués. Il détermine quels slots peuvent servir pour activer les esclaves en mode parqué. Cette adresse n'est pas unique donc différents esclaves peuvent avoir la même .

ANNEXE 2 : PROTECTION DES DONNEES

Bluetooth utilise différents systèmes pour contrôler et corriger les éventuelles erreurs de transmission.

A2.1 FEC 1/3

Une simple répétition de 3 fois chaque bit. La décision est prise à la majorité de bit. Le FEC 1/3 est utilisé par les entêtes de paquet et aussi par les paquets de type HV1.

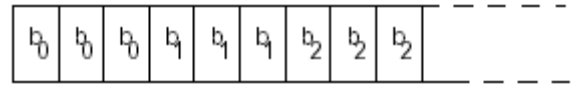

Figure A.03 : *Codage FEC 1/3*

A2.2 FEC 2/3

Cette technique utilise un code Hamming (pour 10 bits, ce code en génère 15) avec comme polynôme générateur :

$$g(D)=(D+1)\cdot(D^4+D+1) \qquad (2.01)$$

La distance de Hamming de ce code est de 4, il corrige 1 erreur et en détecte 2. Ce code est généré par un registre à décalage de 5 bits

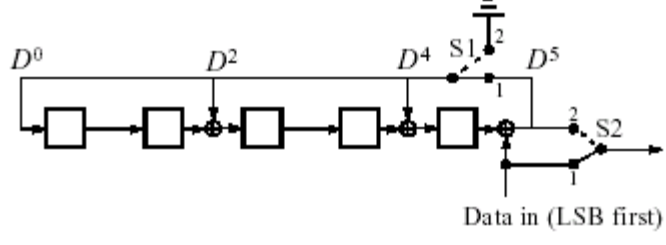

Figure A.04 : *Registre à décalage générateur de code Hamming pour FEC 2/3*

A2.3 ARQ

Pour les paquets protégés par un CRC, il y a répétition du paquet en cas de réception d'un NAK ou si aucun acquittement n'est reçu après un certain temps.

Un bit de séquence évite le problème de doublon si l'acquittement est perdu en route.

A2.4 Taille des paquets [12]

Comme nous l'avons précisé précédemment, le maître utilise les slots paires et les esclaves utilisent les slots impairs. Les transmissions se font par paquets de taille variable qui peuvent prendre 1, 3 ou 5 slots. A la fin de chaque transmission, sur le dern ier slots de transmission, le paquet ne prend pas tout le temps qui lui est imparti. Cette partie du slot est en fait réservée pour la commutation d'une fréquence à la suivante. Sur la figure A.05, une transmission de paquets sur un slot est montrée en exemple.

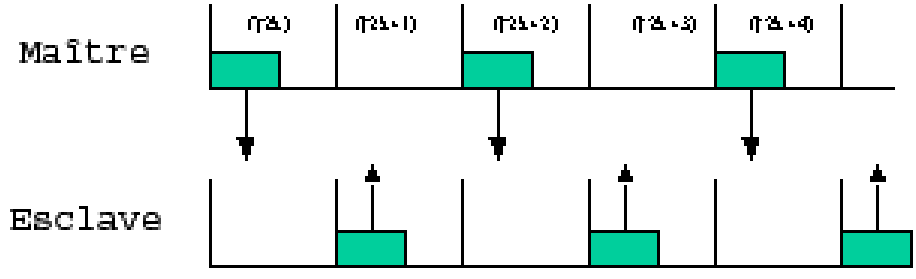

Figure A.05 : *Transmission sur 1 slot*

Un autre exemple pour mieux comprendre en utilisant une transmission ave un paquet de 5 slots.

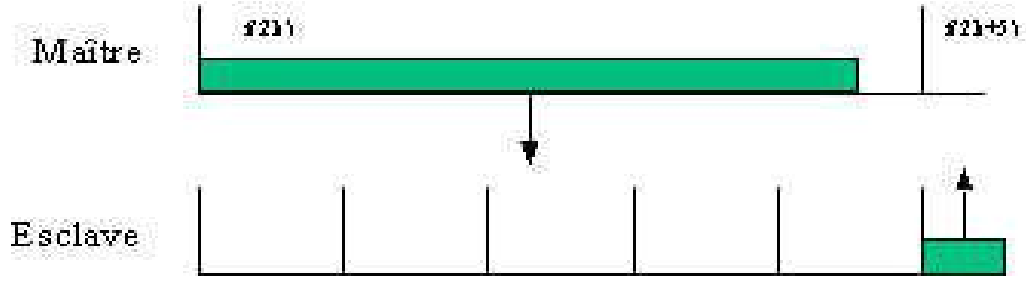

Figure A.06 : *Transmission sur 5 slots*

ANNEXE 3 : STRUCTURE DES PAQUETS BLUETOOTH

La structure d'un paquet Bluetooth se décompose en trois entités qu'il faut bien distinguer :

-Le code d'accès,

-l'entête,

-la cargaison.

La décomposition est faite grâce à leur positionnem ent comme le montre la Figure A.07 .

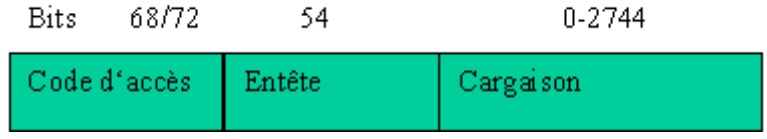

Figure A.07 : *Représentation normal d'un paquet Bluetooth*

A3.1 Access code [11]

Tous les paquets commencent forcément par un access code .Il est utilisé pour la synchronisation, la compensation d'offset et l'identification. A la réception d'un paquet, chaque dispositif peut déterminer s'il a été envoyé par un membre du piconet.

L'accès code est aussi utilisé par les procédures pagging et inquiry.

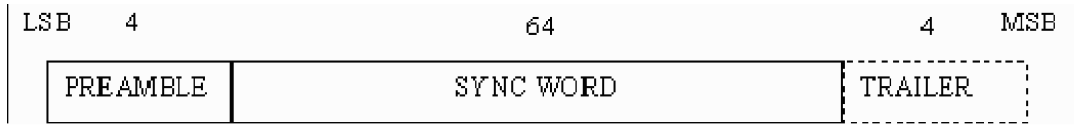

Figure A.08 : *Le format de l'Access code*

Il y a trois différents types de code d'accès :

-Code d'accès du canal (CAC)

-Code d'accès du dispositif (DAC)

-Code d'accès d'inquiry (IAC)

A3.1.1 Preamble

Le préambule est une suite de 1 et de 0 sur 4 bit s. La séquence représente 1010 si le premier bit de syncword vaut 1 ou 0101 si le premier bit de syncword vaut 0.

Figure A.09 : *Séquence du préambule* [11]

A3.1.2 Sync Word

Le sync word (mot de synchronisation) est dérivé des 24 bits de l'adresse LAP mais est long de 64 bits. Pour le CAC, l'adresse du maître est utilisée dans le piconet. Pour le GIAC et le DIAC, des adresses dédiées sont utilisées. Mais par contre pour le DAC, l'adresse de l'esclave est utilisée.

A3.1.3 Trailer

Le trailer suit le syncword. Comme le préambule, il est formé de 4 bits qui peuvent prendre l es valeurs 1010 et 0101.

A3.2 En tête de paquet

L'entête des paquets contient des informations pour la couche link controler. Il est constitué de 6 champs :

AM_ADDR : 3 bits (adresse de membre actif=

Type : 4 bits (type de paquet)

Flow : 1 bit (contrôle de flux)

ARQN : 1 bit (acquittement)

SEQN : 1 bit (numéro de séquence)

HEC : 8 bits (contrôle des erreurs de l'entête)

L'entête au complet comprend 18 bits (voir Figure A.10). Un codage FEC 1/3 est utilisé pour protégé l'entête, ce qui donne un total de 54 bits.

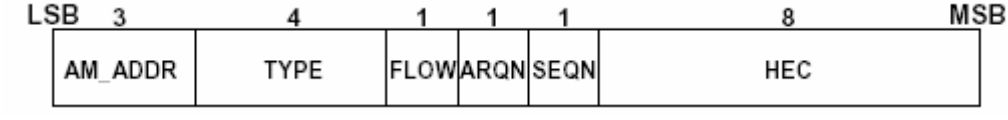

Figure A.10 : *Format de l'entête de paquet*

AM_ADDR :

La AM_ADDR représente l'adresse de membre actif est utilisée pour diff érencier les dispositifs dans un piconet. L'adresse avec que des 0 consiste en une adresse broadcast**.**

Type **:**

Il existe 16 différents types de paquet. Chaque type définit la liaison (ACL et SCO) utilisée par la transmission. Il permet de connaître le nombre de slots occupés (1,3 ou5) .

Flow **:**

Ce bit est utilisé pour le contrôle du flux. Si le bit est à 1, la source peut co ntinuer à émettre. Si le destinataire ne peut plus suivre (buffer plein par exemple), il met le bit à0 dans son message. Il faut noter que ceci ne s'applique qu'aux liaisons ACL.

ARQN :

Ce bit est utilisé pour indiquer qu'une transmission a été effectuée correctement ou non. Le contrôle se fait grâce au CRC.

SEQN :

Ce bit permet d'ordonner les paquets reçus. Ce bit est inversé à l'envoi de chaque nouveau paquet.

HEC **:**

Ces bits servent à contrôler l'entête du paquet. Le HEC est constitué de 8 bits générés par un polynôme 647 (représenté en octal).

A3.3 En tête de cargaison

Uniquement les champs de données ont un entête de cargaison. Cet entête peut faire 1byte (si le paquet prend 1 slot) ou 2 bytes (si le paquet prend 3 ou 5 slots).

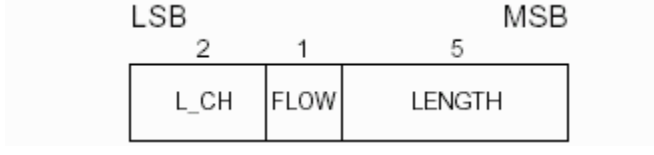

Figure A.11 : *Entête de cargaison sur 1 byte (prend 1 slot)*

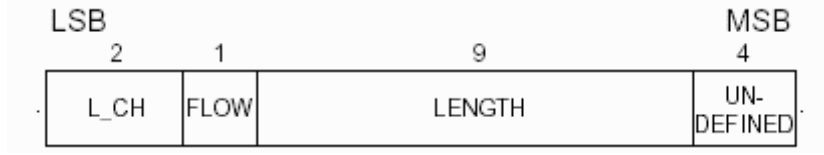

Figure A.12 : *En tête de cargaison sur 2 bytes (prend 3 ou 5 slots)*

L_CH :

Ces 2 bits spécifient le canal logique.

FLOW :

Ce bit contrôle le flux du canal logique. Quand un message est reçu avec FLOW = 1, on peut continuer à transmettre sur le canal logique. Par contre quand le message contient FLOW = 0, la transmission est stoppée.

LENGTH :

Ces bits définissent la longueur de la cargaison en byte.

A3.4. Canaux logiques :

Avec Bluetooth, il existe 5 canaux logiques :

-Canal de contrôle LC

-Canal de contrôle LM

-Canal utilisateur UA

-Canal utilisateur UI

-Canal utilisateur US

Les canaux contrôlent LC et LM sont utilisés respectivement par la couche link control et link manager. Les canaux utilisateur UA UI et US utilisent des transmissions asynchrones, isochrones1 et synchrones de l'information utilisateur.

A3.5 Type de paquet

A3.5.1 Paquet ID

Ce paquet consiste en un accès code du type DAC ou IAC. C'est un paquet très robuste au niveau du corrélateur de l'accès code.

A3.5.2 Paquet NULL

Ce paquet n'a pas de cargaison mais possède un code d'accès et un entête de paquet. Il contient 126 bits au total. Il est utilisé pour envoyer un acquittement ou pour changer
le statue de FLOW. Ce paquet ne doit pas être acquitté.

A3.5.3 Paquet POLL

Ce paquet est très similaire au paquet de type NULL (voir 3.5.2). Il doit cependant être acquitté.

A3.5.4 Paquet FHS

FHS est un paquet de contrôle spécial. Parmi d'autres choses, l' adresse de dispositif Bluetooth et l'horloge de l'expéditeur sont envoyés avec le paquet. La cargaison contient 144 bits d'information et 16 bits de CRC. La cargaison est codés en FEC 2/3 ce qui signifie qu'elle occupe 240 bits réellement. Il n'occupe qu'un slot.

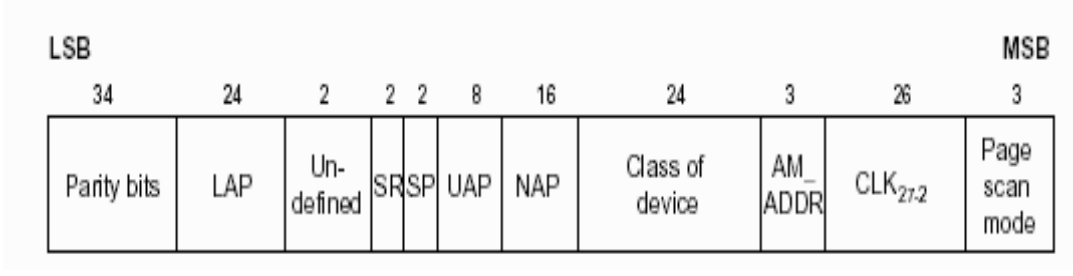

Figure A.13 : *Format de la cargaison d'un paquet FHS* [BT01]

Parity bits : 34 bits de parité
LAP : les 24 bits de la partie inférieure de l'adresse (BD_ADDR) de l'expéditeur du paquet FHS.
Undefined : 2 bits mis à 0 pas encore utilisés.
SR : 2 bits qui indiquent la répétition entre deux scan et l'intervalle entre deux page scan consécutif

SR bit format b1b0	SR mode	Tpage scan	Npage
00	R0	continus	>=1
01	R1	<=1.28s	>=128
10	R2	<=2.56s	>=256
11	Réservé	-	-

Figure A.14 : *Représentation du champ SR*

SP : 2 bits qui indiquent la période pendant laquelle le dispositif se trouve en page scan après la réception de l'Inquiry.

SP bit format b1b0	SP mode	Tmandatorypscan
00	P0	>=20s
01	P1	>=40s
10	P2	>=60s
11	Réservé	-

Figure A.15 : *Représentation du champ SP*

UAP : 8 bits de la partie supérieur de l'adresse (BD_ADDR) de l'expéditeur du paquet FHS.

NAP : 16 bits de la partie non-significative de l'adresse (BD_ADDR). Class of device : 24 bits représentent le type dispositif.

AM_ADDR : 3 bits qui forment l'adresse de membre actif du dispositif qui envoie le paquet FHS.

CLK27-2 : 26 bits qui contiennent la valeur de l'horloge native du dispositif qui envoie le paquet FHS.

Page scan mode : 3 bit qui définit quel scan mode est utilisé par défaut par le dispositif qui a envoyé le paquet.

Bit format b2b1b0	Page scan mode
000	Manadatory scan mode
001	Optional scan mode I
010	Optional scan mode II
011	Optional scan mode III
100	Réservé pour utilisation futur
101	Réservé pour utilisation futur
110	Réservé pour utilisation futur
111	Réservé pour utilisation futur

Figure A.16 : *Représentation du champ Page scan mode*

A3.5.5 Paquet DM1

Ce type de paquet est utilisé pour échanger des messages de contrôle des couches supérieures. Il peut être utilisé par des liaisons SCO pour interrompre le flux d'information et pour envoyer des messages de contrôle. Les paquets DM1 peuvent être considérés comme un paquet ACL.

DM est l'abréviation de Data Medium rate. La cargaison du paquet contient 17 bytes d'informa tion entourées par 1 byte d'en tête et 2 bytes de CRC. Le codage FEC 2/3 est utilisé pour la cargaison. Il n'occupe qu'1 slot.

BIBLIOGRAPHIE

[1] D.Cautillo, « *Guidage par GPS et services associés sur téléphone portable* », heg : Aout 2008.

[2] D.Cautillo, «*Beacon: A context aware Messaging Application* », heg: Aout 2008.

[3] G.Map-, «TrackBETATrackyourpositiononGoogleMaps », heg :Aout 2008.

[4] M.GMaps, "View maps from various sources on your mobile phone", heg : Aout 2008.

[5] B.Bernard, «*Chambre de Commerce et d'Industrie* », CCI :2005.

[6] N Engrand, «*Wifi et Bluetooth* », USTL: 2005.

[7] P.Dandumont, « *Bluetooth et les profiles* », review Bluetooth technology : 2008.

[8] P.Betouin, « *Sécurité du réseau Bluetooth*», CERTA : 2007.

[9] J.Cayssol, « *IP sur Bluetooth* », SNCF: 2004.

[10] G. Pujolle, « Specification of the Bluetooth system version 1.1 », 2001.

[11] S.Mcgowan, «*The Bluetooth Special Interest Group* » SIG: 1998.

[12] M.Rubeistein, "*Bluetooth*", EIVD: 2001.

[13] G.Ranta, "*Bluetooth Human Interface Device Profile*", DG: 2003.

[14] S.Mcgowan, «*Universal Bus Specification, Version* 1.1», DG: octobre 2004.

[15] Sony EricssonMobile Communications AB, «*Bluetooth TM Remote Control* », DG: octobre 2004.

RENSEIGNEMENTS

Nom : RASOLOSON

Prénom : Faly Mathieu

Adresse de l'auteur : Lot A 78 K Ambohitrarahaba

Contact : 033 18 924 99

Titre du mémoire : APPLICATION DU BLUETOOTH : télécommande d'un ordinateur à partir d'un téléphone portable

Nombre de pages : 69

Nombres de figures : 34

Nombre de tableaux : 07

Mots clés : HID, BLUETOOTH, protocole, adresse, Profil

Directeur de mémoire : Monsieur ANDRIAMIASY Zidora

RESUME

La technologie Bluetooth est une technologie en vogue dans le monde .Cette technologie utilise le réseau sans fil offrant ainsi plusieurs applications et peut rentrer dans plusieurs domaines. Dans ce présent mémoire, nous avons étudié cette technologie, ses problèmes et les applications que l'on peut faire. La télécommande souris clavier Bluetooth est l'une de ces applications. Cette télécommande utilise le profil HID dans les profils Bluetooth et peut être amélioré selon le besoin de l'utilisateur.

ABSTRACT

The Bluetooth technology is a technology in vogue in the world. This technology uses the network cordless bidder so several applications and can go back in several domains. In this memory, we see this technology. The remote control mouse Bluetooth keyboard is one of these applications .This remote control uses the HID profile in the Bluetooth profiles and can be improved according to the user's need.