Université Sidi Mohamed Ben Abdellah
Faculté Des Sciences et Techniques
Fès

Livrable 5

Date début : 19/11/2013 Date Fin : 25/12/2013

Date prévu de soumission : 06/12/2013
Date de soumission : 05/12/2013

Réalisé par :

-ZOUHAIRI Fouad
-EL GHOUBACH Imad
-JIDA Safa
-KHARBANE Yahya
-TABTI Abdelhak

Année universitaire 2013/2014

Résume : L'objectif de ce livrable est de présenter les états des terminaux Bluetooth lors de communication ou échange de données.

Version	Date	Modifié par	Motif de la Modification
V1.0	03/12/2013	ZOUHAIRI Fouad	Rédaction du Livrable 5
V1.1	04/11/2013	EL GHOUBACH Imad	Modification
V1.2	05/11/2013	Tabti Abdelhak	Modification
V1.3	05/11/2013	KHARBANE Yahya	Modification
V1.4	05/12/2013	JIDA Safa	Modification
V1.5	05/12/2013	ZOUHAIRI Fouad	Validation

Table des matières

I. Introduction

Bluetooth est une technologie de réseau personnel sans fils (noté WPAN pour Wireless Personal Area Network), c'est-à-dire une technologie de réseaux sans fils d'une faible portée permettant de relier des appareils entre eux sans liaison filaire. Contrairement à la technologie IrDa (liaison infrarouge), les appareils Bluetooth ne nécessitent pas d'une ligne de vue directe pour communiquer, ce qui rend plus souple son utilisation et permet notamment une communication d'une pièce à une autre, sur de petits espaces.

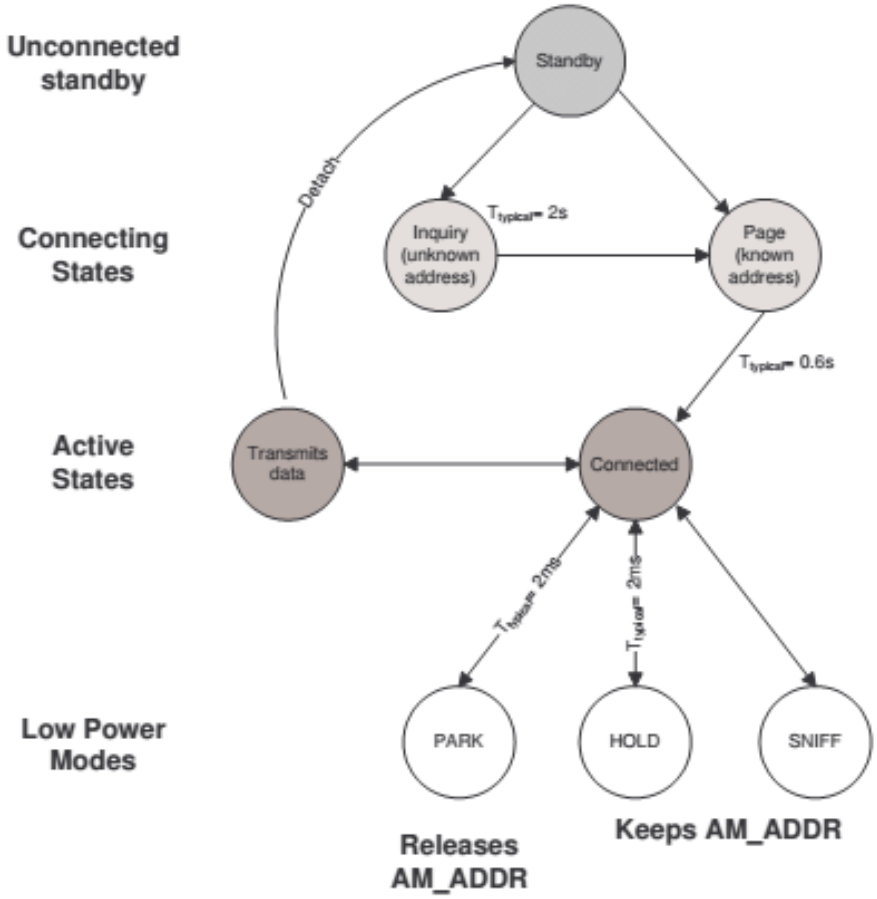
L'objectif de Bluetooth est de permettre de transmettre des données ou de la voix entre des équipements possédant un circuit radio de faible coût, sur un rayon de l'ordre d'une dizaine de mètres à un peu moins d'une centaine de mètres et avec une faible consommation électrique.

II. Etats des terminaux Bluetooth

Le contrôleur Bluetooth fonctionne dans 2 états principaux : « stand-by » et « connexion ». Il y a 7 états subsidiaires qui sont utilisés pour ajouter des esclaves ou créer des connexions dans le Piconet. Ces sous états sont : page, page scan, inquiry, inquiry scan, master response, slave response et inquiry response. Un périphérique bluetooth peut prendre les quatre états suivants:

Active, Hold, Sniff and Park.

Voici le schéma des différents états que peut prendre un périphérique Bluetooth :



1. Etats non-connectés

- **Standby**

L'état Standby est l'état par défaut de basse consommation pour un périphérique Bluetooth. Seule l'horloge native est active et il n'y a aucune interaction avec les autres dispositifs. En mode connecté, le maître et l'esclave peuvent s'échanger des paquets en utilisant le code d'accès du canal du maître ainsi que son horloge.
Dans ce mode, une unité non connectée « écoute » les messages périodiquement toutes les 1.28 Secondes. A chaque fois qu'une unité rentre en mode actif, celle-ci écoute un ensemble de 32 sauts de fréquences qui lui sont propre.

- **Inquiry**

Lorsqu'un périphérique désire découvrir les nouveaux dispositifs, il passe en état « inquiry », où il envoie des paquets de broadcast « inquiry », contenant un IAC, à tous les périphériques dans sa zone. Il l'envoie en utilisant le « inquiry hopping sequence » c'est-à-dire qu'il l'envoie aux 32 fréquences d'éveil. Il obtient sa synchronisation et le code d'accès du canal par FHS. Le dispositif peut alors recevoir des réponses à ces « inquiries », mais il ne devra pas acquitter ces paquets de réponse.
Le message INQUIRY est utilisé afin de communiquer avec des équipements dont on ne connaît pas l'adresse (par exemple des imprimantes ou des fax publics).

- **Inquiry Scan**

Lorsqu'un périphérique désire recevoir des paquets « inquiry », il entre en mode « inquiry scan ». Il utilise le « inquiry hopping sequence » c'est-à-dire qu'il écoute successivement sur les 32 fréquences d'éveil.
Il s'agit d'une écoute active de DIAC et GIAC. S'il reçoit un « inquiry », il renverra un FHS.

- **Page**

Une connexion est établie par un message de type PAGE si l'adresse de l'unité à connecter (Unité Esclave) est connue.
Dans l'état initial PAGE, l'unité Maître envoie un train de 16 messages identiques de paging sur 16 différents sauts de fréquences spécifiques à l'unité pagée (Esclave). Ce train de message couvre la moitié de la séquence de sauts de fréquences que l'unité Esclave écoute en modeSTANDBY et il est répété 128 fois, ce qui correspond à 1.28 s. Si aucune réponse n'est reçue après ce délais, le Maître retransmet le même train de message de paging dans les 16 sauts de fréquences restant de la période d'écoute de l'unité Esclave.
Le délai maximum pour que l'unité Maître atteigne une unité Esclave est donc de deux fois 1.28 s c'est à dire 2.56 s.

- **Page scan**

Lorsqu'un périphérique désire recevoir des paquets « page », il entre en mode « page scan ».

2. Etats connectés

Dans le mode actif, l'unité Bluetooth participe activement sur le canal. Le maître organise les transmissions de base sur la demande de trafic ainsi qu'en fonction des esclaves. En plus, il supporte des transmissions régulières pour que les esclaves restent synchronisés sur le canal. Les esclaves actifs écoutent durant les « slots » maître à esclaves pour les paquets. Si un esclave actif n'est pas adressé, il peut dormir jusqu'à la prochaine transmission du maître.
Représentation du mode actif :

Pour les unités connectées, trois modes d'économie d'énergie peuvent être utilisés si aucune donnée ne doit être transmise :

- **Mode HOLD**

L'unité Maître peut forcer les unités Esclaves à passer en mode HOLD. Dans ce mode, il n'y a plus que l'horloge interne qui fonctionne. Les unités Esclaves peuvent aussi demander à passer en mode HOLD. Le transfert de données ne reprendra que lorsque l'unité aura quitté le mode HOLD. Le mode HOLD est typiquement utilisé dans le cas de connexions avec plusieurs piconets, ou encore lorsque les données ne sont pas envoyées très fréquemment. C'est idéal pour les événements non périodiques et plutôt utiles pour le maître qui aurait besoin d'établir des liens supplémentaires ; Le mode démarre sur une valeur d'horloge prédéfinie.
Représentation mode HOLD :

- **Mode SNIFF**

Dans ce mode, un dispositif esclave écoute le Piconet à un taux réduit, de ce fait réduisant son coefficient d'utilisation. La périodicité est programmable et dépend de l'application ; Il s'agit donc d'une opération répétitive qui est plutôt adapté pour les événements périodique, pour économiser l'énergie des liens ACL (si une certaine latence est toléré), et procure une certaine flexibilité dans les trafics encombré. Représentation mode SNIFF :

- **Mode PARK**

Dans ce mode une unité est toujours synchronisée au piconet mais ne participe pas au trafic. Ces dispositifs ont rendu leur adresse (AM_ADDR) et écoutent occasionnellement le trafic du maître pour se re-synchroniser et vérifier les messages de diffusion généraux (Broadcast). Une adresse membre de parking lui est assigné (PM_ADDR). Une adresse de requête lui est aussi assignée (AR_ADDR) que le maître utilisera pour le faire sortir du mode « park ». L'usage premier du mode park est lorsque plus de 7 esclaves sont attachés au piconet. Il est périodique comme le mode SNiFF mais d'une structure plus rigide car il augmente sa charge, mais permet une meilleur économie d'energie. Il a comme travail supplémentaire de vérifier régulièrement si un esclave est toujours présent. L'esclave doit quitter le mode park

pour pouvoir recevoir ou transmettre des données. Ce mode ne peut pas être utilisé pour les esclaves en lien SCO actif.

III. Comment fonctionne Bluetooth

1. Au départ

Initialement, les périphériques Bluetooth ne se connaissent qu'eux même et ils sont en mode StandBy. StandBy est un mode passif (non-connecté) où les périphériques cherchent la présence de transmission (« Inquiry » ou « Page Scans ») dans sa zone de couverture pendant 10ms toutes les 1.28 secondes pour voir si aucun des périphériques cherchent à communiquer. Ils écoutent successivement 32 « porteuses d'éveil » parmi les 79 fréquences.

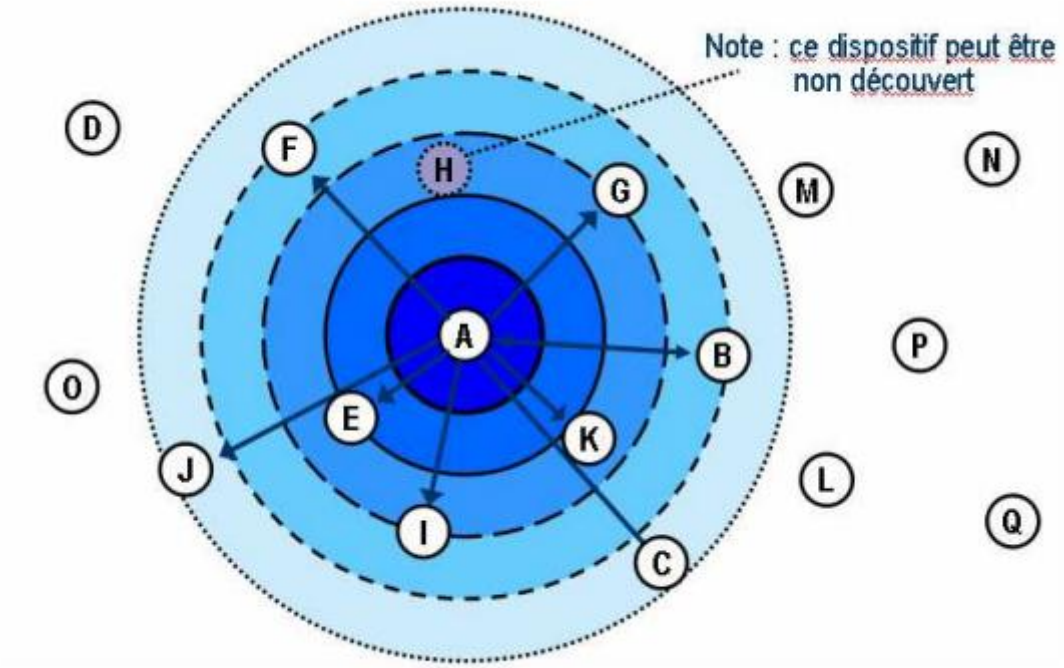
Les états passifs sont occupants plus de la moitié d'états Bluetooth et c'est le mécanisme clef pour réaliser un dispositif de très faible consommation. Parfois, un périphérique Bluetooth en mode Standby peut réduire sa consommation jusqu'à 98%.

Il est important de noter que les périphériques ne sont pas encore synchronisé. Tous les périphériques sont tous en train d'écouter à des temps différents et sur des fréquences différentes.

2. Découvert

Ce processus est différent du processus de pagination car elle possède moins de renseignements. Le master n'utilise pas l'ACCESS CODE, il transmet le GIAC (General Inquiry Access Code) ou le DIAC (Dedicate Inquiry Access code). Le GIAC permet d'extraire l'information sur les capacités des slaves, le DIAC lui informe sur des capacités plus spécifiques.

Tous les éléments utilisent la même fréquence porteuse. Le slave répond à une requête avec ses paquets FHS après que le master lui aie attribué un numéro propre de trame impaire. Les quantités de paquets FHS, reçues, permettent au master de se caler sur le slave et de commencer une communication, en effet les FHS permettent au master d'élaborer la BD_ADDR et donc de construire des paquets valides.



Le mode découverte (Inquiring) est un mode de fonctionnement qui permet de connaître les autres périphériques qui sont dans la zone de portée.

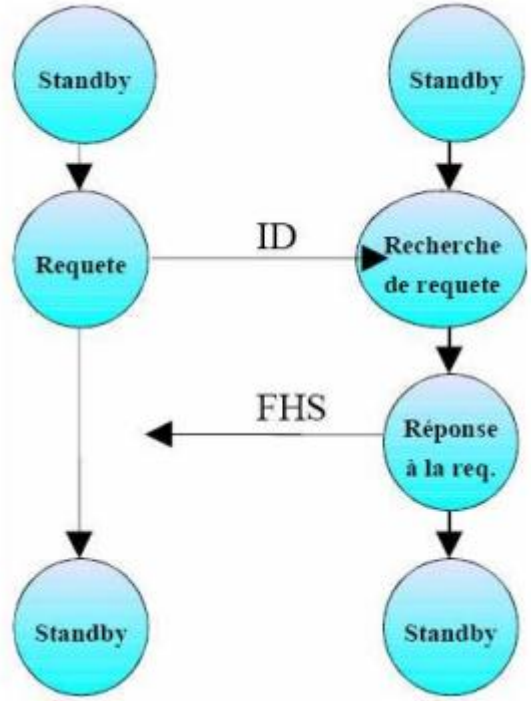
L' « inquiring » est la manière dont un dispositif de Bluetooth se renseigne sur d'autres dispositifs qui sont dans sa zone. Dans l'illustration au-dessus du nœud A exécute une procédure de pagination sur le « BT inquiry ID » (ID de Broadcast) et reçoit des réponses des dispositifs B, C, E, F, G, I, J, et K. Par ces réponses le dispositif A apprend l'identité de ces autres dispositifs.

Pendant la phase de découverte, le noeud A broadcast continuellement la commande de pagination en utilisant le « BT inquiry ID ». Ce qui l'identifie comme une requête « Inquiry ». Ces broadcasts sont diffusés au travers des 32 fréquences porteuses « Standby » où tous les dispositifs en mode Standby sont à l'écoute.

Après quelques secondes, chaque dispositif dans la zone aura reçu l' « inquiry » mais ils ne sont aucunement synchronisés. Par convention ces noeuds répondront avec un paquet standard FHS qui fournit leur identification de BT unique et leur horloge. Avec ces paramètres le noeud d'investigation peut effectuer des connections synchronisées de faible latence.

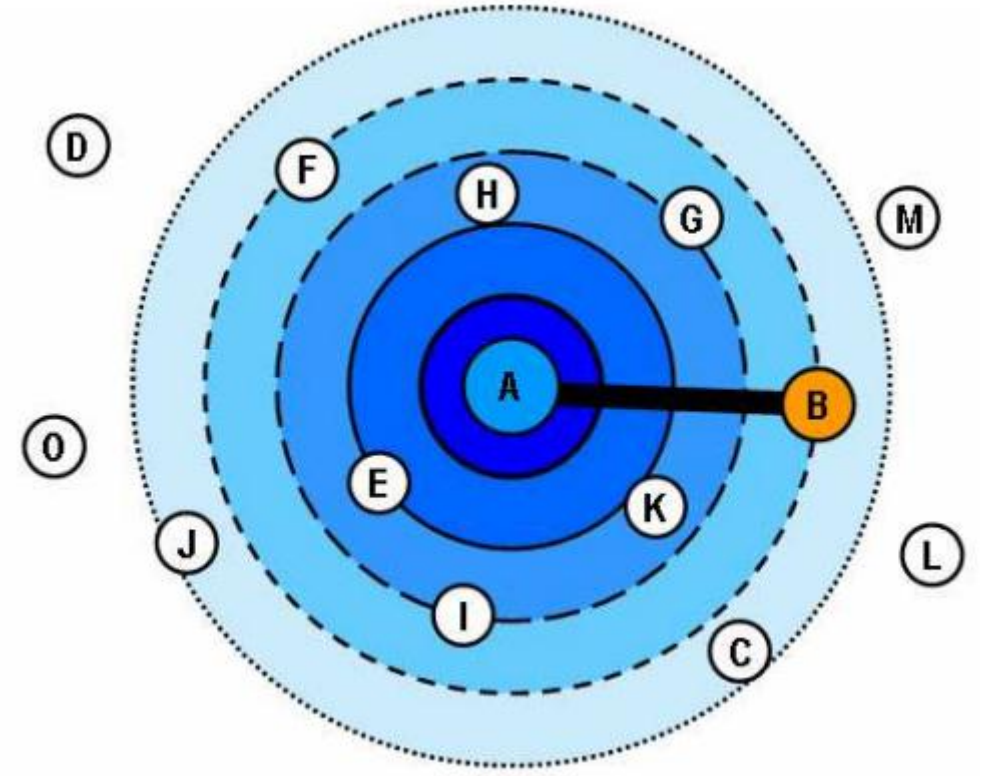
Ici le noeud H illustre un dispositif Bluetooth programmé pour rester anonyme (« Undiscoverable »). C'est une option qui suspend le « Inquiry scan » ainsi aucun dispositif ne peut le découvrir.

Cependant il faut noter que le nœud H continue à assurer la fonction « page scan ». On peut créer une connexion avec celui-ci en lui envoyant une requête de pagination directement à son Bluetooth Unique ID.



IV. Créer un piconet

La création d'un piconet (Paging) permet de créer un lien Maître/Esclave.



Les connexions Maître/esclave en Bluetooth sont désignées sous le nom de Piconet. Pour créer un piconet, le nœud A diffusé (ou broadcast) une commande de pagination avec un ID Bluetooth explicite (Ici nœud B). Cette ID utilisé a été récupéré plutôt dans la phase de recherche par la procédure « Inquiry » vu plus haut.

Tous les périphériques Bluetooth excepté le B ignorent cette commande de pagination simplement parce qu'elle ne leur est pas adressée. Lorsque le nœud B répond, le nœud A enverra à son tour un paquet FHS et lui assignera un AM_ADDR dans le piconet. Le nœud A devient alors le maître du piconet car c'est lui qui a fait la requête de pagination, et son adresse définit la suite des sauts en fréquence que devront suivre les esclaves.

Le noeud B est maintenant en état actif et se mettra en écoute pour toutes autres commandes provenant du nœud A. Il doit se synchroniser sur les sauts de fréquence du nœud A et calé son horloge.

Le problème est que le maître ne sait pas sur laquelle des 79 fréquences porteuses se fixer. La solution est :

· Balayage des pages sur 32 fréquences porteuses.

· La BD_ADDR contient l'information sur la bonne fréquence à adopter, elle est connue par le master.

· Utilisation de l'horloge Bluetooth des éléments, on connaît ainsi le temps écoulé pendant la dernière connexion de deux unités. Cela a pour effet d'augmenter la vitesse d'élaboration de la page.

En effet le balayage de la page d'état est fait toutes les 2.56 s. Le slave consulte cette page toutes les 11.25 ms à fréquences porteuses variables. Pendant ce temps le master potentiel lance des paquets d'identification pour le slave potentiel sur deux fréquences porteuses différentes en utilisant les trames numérotées paires. Il écoute les réponses sur les trames impaires consécutives. La taille réduite de l'ACCESS CODE permet au dispositif électronique du master de switcher sur deux fréquences différentes en 625 micro s. Ainsi pendant 11,25 ms le master peut envoyer et recevoir les informations de 16 canaux différents. Ne sachant pas quand le slave se reconnecte à la page d'état, il réitère cette opération pendant 2.56s. Si le résultat n'est pas concluant, le master passe en revue 16 autres fréquences jusqu'à réponse ou timeout. L'état de connexion débute avec un paquet POLL (scrutin) envoyé par le maître pour vérifier que l'esclave a commuté et s'est synchronisé sur le maître ainsi que sur la séquence du canal.

Il peut aussi arriver qu'un dispositif (esclave) désire se connecter à un Piconet sans y être invité par le maître. La procédure est presque la même que celle précédemment expliquée, mais voici dans les grandes lignes ce qu'il faut faire :

- Une adresse de connexion est réservée, le dispositif en tire le code d'accès
- Il écoute pendant un long moment la même fréquence
- Par les paquets de Broadcast envoyés par le maître il peut obtenir la séquence de saut du Piconet ainsi que les informations supplémentaires qu'il aurait besoin.

V. Conclusion

Bluetooth est une technologie qui offre plusieurs possibilités à l'usager puisqu'il se caractérise par un faible coût, une faible consommation d'énergie et plein d'autres avantages. Mais malgré toutes ces possibilités il reste limité, et les principaux reproches sont dus aux problèmes de compatibilité entre les puces provenant de divers industriels, ainsi le débit faible et la concurrence de la norme IEEE 802.11.