

Valentin Rudy  
2<sup>ème</sup> informatique  
Helho

Périphérique :



Année 2007-2008:



## Table des matières

I) Introduction.....	P 5-9
- 1 Qu'est ce que le bluetooth ?.....	P 5
- 2 Pourquoi utiliser le bluetooth ?.....	P 5-6
- 3 Historique.....	P 6
- 4 Origine du nom.....	P 6-7
- 5 Les normes.....	P 7-8
- 6 Les évolutions bluetooth.....	P 8-9
II) Le bluetooth SIG.....	P 9
III) Les schémas de connexions.....	P 10-11
- 1 Le réseau le plus simple.....	P 10
- 2 Le piconet.....	P 10-11
- 3 Le scatternet.....	P 11
IV) La pile bluetooth.....	P 12-16
- 1 La couche radio.....	P 12
- 2 La couche bande de base.....	P 12-13
- a Le mode synchrone.....	P 13
- b Le mode asynchrone.....	P 13-14
- 3 La couche contrôleur de liaison.....	P 14
- 4 La couche gestion de liaison.....	P 14
- 5 L'interface.....	P 14
- 6 Le L2CAP.....	P 14
- 7 Protocol RFCOMM.....	P 15
- 8 Protocol SDP.....	P 15
- 9 Protocol TCS.....	P 15
- 10 Protocol OBEX.....	P 15
- 11 Les profils.....	P 15-16
V) Trame bluetooth.....	P16-20
- 1 Les champs principaux.....	P 16
- 2 Définition des champs d'Access code.....	P 16-17
- a Les types de code d'accès.....	P 16-17
- b Le champ preamble.....	P 17
- c Le champ sync word.....	P 17
- d Le champ trailer.....	P 17
- 3 Définition des champs de HEADER.....	P 18-19
- a Le champ AM_ADDR.....	P 18
- b Le champ TYPE.....	P 18
- c Le champ FLOW.....	P 18
- d Le champ ARQN.....	P 18
- e Le champ SEQN.....	P 18
- f Le champ HEC.....	P 18
- g Le FCE.....	P 18-19
- 4 Définition des champs de PAYLOAD.....	P 19-20
VI) Création d'une connexion entre bluetooth .....	P 20-21

VII) La sécurité .....	P 21-24
- 1 Le couplage.....	P 22
- 2 Comment se passe l'authentification ?.....	P 22-23
- 3 Les différentes attaques.....	P 23-24
- a Bluejacking.....	P 23
- b Bluesnarfing.....	P 23
- c Bluebug.....	P 24
- d Bluesmack.....	P 24
VIII) Cas d'utilisation et composant bluetooth.....	P 24-28
- 1 Les composants bluetooth.....	P 24-25
- 2 Utile.....	P 25-26-27
- 3 Inutile.....	P 27-28
IX) Le future.....	P 28
X) Conclusion.....	P 28
XI) Bibliographie.....	P 28-29

## I) Introduction :

Dans ce rapport, nous allons aborder le thème du bluetooth.

Il s'agit d'un mode de communication assez récent qui offre des avantages incomparable par rapport aux autres modes de communication sans fil.

On débutera sur la façon de communiquer du bluetooth , le type de réseau possible et comment créer une connexion entre tout ces périphériques bluetooth.

Ensuite, une partie sera consacrée aux problèmes de sécurité rencontrés, plusieurs types d'attaques recensées seront expliqués.

On finira en abordant les cas d'utilisation présent et future. Ainsi que l'avenir du bluetooth.

### - 1 Qu'est ce que le bluetooth ?:

Bluetooth est une nouvelle technologie de transmission sans fil. Son but est de permettre la communication à courte distance entre plusieurs appareils en utilisant les ondes radio.

Le bluetooth est destiné à un usage personnel et se classe dans la catégorie PAN (Personal Area Network). On peut même le placer dans la catégorie des WPAN, Wireless Personal Area Network (= réseau personnel sans fil). Puisque sa principale caractéristique est de relier de manière simple divers appareils électroniques (imprimantes, téléphones portables, oreillettes sans fil, souris, claviers, etc.) sans que cela nécessite l'utilisation d'un fil.

Il s'agit en quelque sorte de l'équivalent du port USB mais sans fil.

### - 2 Pourquoi utiliser le bluetooth ? :

Aujourd'hui, l'installation de composants (tels que des imprimantes) et leur mise en réseau n'est pas une chose simple : cela nécessite une configuration parfois compliquée et un câblage souvent difficile à mettre en œuvre. Bluetooth permet une simplification de ces problèmes : cette technologie permet de mettre en liaison un ensemble de périphériques simplement en les rapprochant et de s'en servir immédiatement.

Les avantages du bluetooth par rapport aux autres normes de réseau sans fil (tels que le WiFi ou l'infrarouge) sont :

- Un faible prix.
- Faible consommation électrique : Très utile pour les appareils fonctionnant sur batterie.
- Taille réduite : Il s'agit d'une puce de 9 mm de côté. (Pour la plus petite du marché).
- Il ne se fonde pas sur l'utilisateur : le bluetooth peut détecter automatiquement et communiquer avec les autres périphériques bluetooth sans aucune demande de l'utilisateur.
- Pas besoin d'une « vue directe » comme pour l'infrarouge, le bluetooth peut même traverser les murs.



(Taille d'une puce bluetooth)



(La puce prend place dans une clé de 5 cm)

### - 3 Historique :

- 1994 : création du bluetooth par le fabricant suédois Ericsson.
- Septembre 1998 : Création du bluetooth SIG (le bluetooth Special Interest Group), les principaux constructeurs présents dans ce groupe sont : Ericsson, IBM, Intel, Nokia, Toshiba
- Juillet 1999 : Le groupe bluetooth SIG publie la spécification 1.0A
- Décembre 1999 : Sortie de la version 1.0B. Le groupe bluetooth SIG compte maintenant 9 sociétés après que 3COM, Lucent, Microsoft, Motorola les aient rejoints.
- Novembre 2003, la version 1.2 de la spécification bluetooth a été adoptée
- 2004 : Le groupe bluetooth SIG compte maintenant plus de 2000 sociétés. La version 2.0 est adoptée
- Mars 2007 : Sortie de la version 2.1

### - 4 Origine du nom :

Le mot bluetooth fait référence à un roi Viking du 10<sup>ème</sup> siècle Harald Blatand.

Son nom, Blatand est devenu bluetooth dans un anglais récent.

La traduction littérale de ce mot donne Harald à la dent bleue, se surnom lui viendrait du fait qu'il appréciait énormément les bleuets (plus connu sous le nom de myrtille) et qu'elles lui coloraient les dents en bleu.



(Harald Blatand)

Il unifia la Norvège et le Danemark en préférant la consultation et la coopération plutôt que d'utiliser la puissance des armes.

L'instigateur de la norme bluetooth, Ericsson, a trouvé que ce nom serait parfait pour une technologie qui à pour but d'unifier les connections entre les ordinateurs et les appareils de télécommunication.

Ericsson était un géant des télécoms norvégiens c'est pourquoi leur choix c'est porté sur un roi Viking plutôt qu'un autre.

Le symbole du bluetooth lui-même fait référence au roi Harald Blatand.  
Il s'agit des initiales du roi en alphabet runique (l'alphabet utilisé par les anciens peuples de langues germaniques)

Alphabet runique :

Ʒ Ɔ Ɔ Ɔ Ɔ Ɔ   \* † † † † †   † † † † † † †  
Ʒ Ɔ Ɔ Ɔ Ɔ Ɔ   † † † † † † †   † † † † † † †  
f u þ a r k   h n i a s   t b m l r

Le plus récent futhark(ou alphabet runique) nordique à 16 runes :

- 1<sup>re</sup> ligne, la variante danoise aux brindilles normales (Celle utilisé pour le symbole).
- 2<sup>e</sup> ligne, la variante suédoise-norvégienne aux brindilles courtes

(Les variantes ont permis de faciliter le travail des écrivains de cette époque)

H: \*      B: †

Le logo final donne :



### - 5 Les normes :

Le bluetooth a été déposé comme standard à l'IEEE par le bluetooth SIG.  
Il s'agit de la norme 802.15, cette norme est elle-même découpée en 4 sous standard

- 802.15.1 : Le bluetooth lui-même version 1.x: il s'agit de la technologie la plus utilisée dans le monde des réseaux sans fil de faible portée. il offre des débits moyens (1Mbits/s en théorie).

- 802.15.2 : Cette norme propose des recommandations pour l'utilisation de la bande de fréquence également utilisée par le Wifi, le 2.4 GHz (Giga Hertz). Ces recommandations ont pour but de permettre la coexistence entre des périphériques WLAN et WPAN tout en évitant les conflits.
- 802.15.3 : Le wireless haut débit jusqu'à 20 Mbps. Il s'agit de l'évolution logique de la norme 802.15.1. Elle a des capacités accrues en termes de bande passante, de portée, de sécurité et de débit. De plus, jusqu'à 245 connexions simultanées peuvent être établies. Il s'agit du bluetooth 2.x
- 802.15.4 : Il s'agit d'un standard visant à proposer du bas débit : LR-WPAN pour Low Rate WPAN. Il s'agit d'un réseau de communication simple et peu coûteux permettant des communications avec un besoin énergétique très limité afin d'assurer une longue durée de vie, principalement utilisés pour les réseaux domestiques. Cette technologie en directe concurrence avec l'USB2 pourrait, à terme la remplacer.

## - 6 Les évolutions bluetooth :

### Bluetooth 1.0 et 1.0 B :

Ces versions ont rencontré beaucoup de problèmes, la plus grande difficulté rencontrée par les fabricants était l'interopérabilité de leurs composants.

De plus, l'anonymat au niveau protocolaire était impossible car lors de la connexion la transmission de la BD\_ADDR (l'équivalent bluetooth de l'adresse MAC des cartes réseau) était obligatoire.

### Bluetooth 1.1 :

La norme 802.15.1 pour le bluetooth 1.1 est ratifiée en 2002, cette norme corrige la plupart des erreurs du bluetooth 1.0 et 1.0 B.

Il faut indiquer aussi l'ajout du RSSI (Received Signal Strength Indicator) qui sert à mesurer la force du signal radio reçu.

### Bluetooth 1.2 :

Version rétro-compatible avec le bluetooth 1.1.

Il ratifie la norme 802.15.1 en 2005.

Les principales améliorations sont :

- La découverte et la connexion à d'autres composants plutôt est plus rapide.
- Plus résistant aux interférences.
- Vitesse de transmission accrue.

### Bluetooth 2.0 :

Il a été adopté par le SIG en novembre 2004.

Cette version est elle aussi rétro-compatible avec la version 1.1. La principale évolution est l'introduction de l'EDR (Enhanced Data Rate) qui permet :

- Des transferts jusqu'à 3 Mbit/s théorique.
- Une baisse de l'énergie consommée.
- La création des réseaux multi-connexions est simplifiée.

### Bluetooth 2.1 :

Adopté par le SIG le 26 juillet 2007, il est, comme les versions précédentes, entièrement rétro-compatible avec la version 1.1.

Cette spécification inclut les fonctionnalités suivantes:

- Extended inquiry response: Permet de fournir davantage de renseignements au cours de la procédure d'enquête afin de permettre un meilleur filtrage avant la connexion.
- Sniff subrating: réduit la consommation d'énergie.
- Encryption Pause Resume: Il s'agit d'une clé de chiffrement qui peut être rafraîchi, c'est une sécurité beaucoup plus solide.  
Un cryptage utilisé pour les connexions qui reste en place très longtemps.
- NFC coopération: Permet la création automatique et sécurisé d'une communication avec un autre composant bluetooth équipé de cette technologie. Exemple, la création d'une connexion entre une oreillette bluetooth et un GSM.

## II) Le bluetooth SIG :

Le bluetooth Special Interest Group (ou SIG) est une association privée, à but non lucratif. Le Special Interest Group a été fondé au mois de septembre 1998. Ce groupe n'est pas impliqué dans la conception, la fabrication ou la vente de produits bluetooth. Le bluetooth SIG compte plus de 9 000 membres leaders dans le domaine des télécommunications, de l'informatique, de l'industrie automobile, de la musique, de l'habillement, de l'automatisation industrielle et de la réseautique. Les membres du SIG jouent un rôle clé dans le développement de la technologie sans fil Bluetooth en intégrant celle-ci à leurs différents produits et en la commercialisant. Le SIG comporte par ailleurs des équipes spécialisées restreintes à Hong Kong, en Suède et aux États-Unis.

Le siège social du bluetooth SIG se trouve à Bellevue, Washington, aux États-Unis. Le groupe dispose également de succursales à Hong Kong et à Malmö, en Suède.

Son personnel est composé de Michael Foley, directeur exécutif et titulaire d'un doctorat, d'Anders Edlund, directeur marketing, et d'une petite équipe de professionnels du marketing, de l'ingénierie et de l'exploitation.

En plus de cet effectif limité, des bénévoles, issus de différentes sociétés membres, apportent également leurs compétences clés au SIG. Chacune des sociétés membres a la charge d'un certain nombre de groupes de travail ayant des tâches spécifiques : ingénierie, marketing, homologations, etc.

Outre ses membres fondateurs Ericsson, Intel, Lenovo, Microsoft, Motorola, Nokia et Toshiba, le bluetooth SIG comprend des milliers de sociétés affiliées et adeptes

## III) Les schémas de connexions :

Dans ce paragraphe, on va voir comment un réseau bluetooth s'articule.

Une communication ne peut se faire que s'il y a au moins un maître mais un maître peut administrer jusqu'à 7 esclaves actifs en même temps et 255 esclaves parkés.

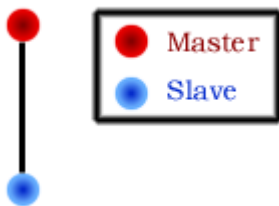
Parked définit un état passif d'un esclave. L'esclave n'envoie pas et ne reçoit pas de données. Sa seule activité est de se réveiller de temps en temps pour se synchroniser avec le maître grâce à des "balises" que le maître envoie à des intervalles réguliers. Cet état permet de ne pas prendre une des 7 places réservées aux esclaves actifs.

Il peut donc y avoir jusqu'à 8 appareils connectés et actifs pour former un réseau bluetooth que l'on appelle piconet ou piconet.

Il est cependant possible d'interconnecter des piconets pour former des réseaux plus grands appelés scatternets. Dans ce cas, certains appareils bluetooth serviront de passerelle. Ils auront un double rôle celui de maître et celui d'esclave. On peut connecter 10 piconets ensemble au maximum, ce qui nous donne 72 systèmes actifs.

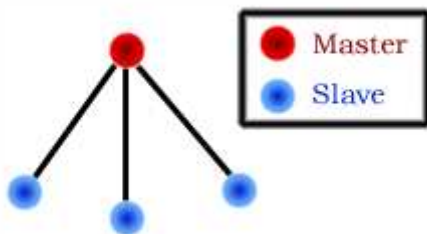
### - 1 Le réseau le plus simple :

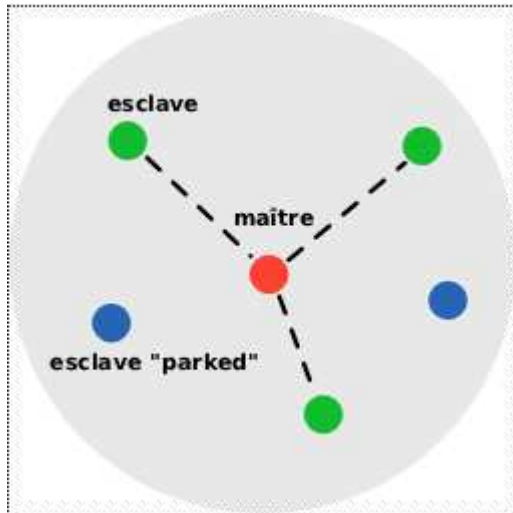
Il n'y a que 2 périphériques bluetooth, un maître et un esclave. Le maître est chargé de gérer la communication entre les deux périphériques : c'est lui qui initialise la connexion.



### - 2 Le piconet :

S'il y a au moins trois périphériques qui veulent communiquer ensemble. Un des périphériques devient le maître et les autres, les esclaves. Le maître est alors chargé de gérer les communications entre les différents esclaves : lorsque 2 esclaves souhaitent échanger des informations, cette discussion est orchestrée par le maître. Les esclaves ne peuvent pas communiquer directement entre eux.

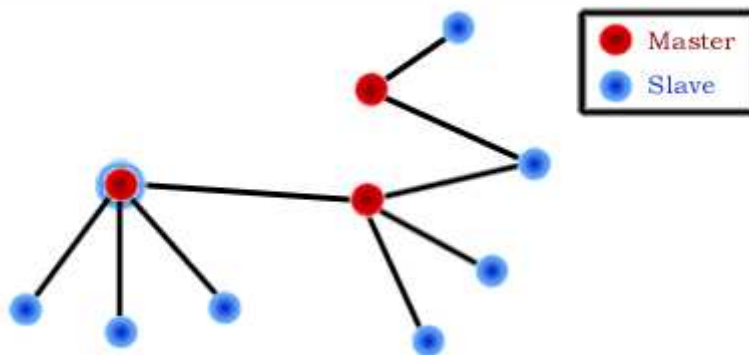




(On peut voir ci-dessus les esclaves « parked », ils ne sont pas entrain d'échanger des données avec le maître)

### - 3 Le scatternet :

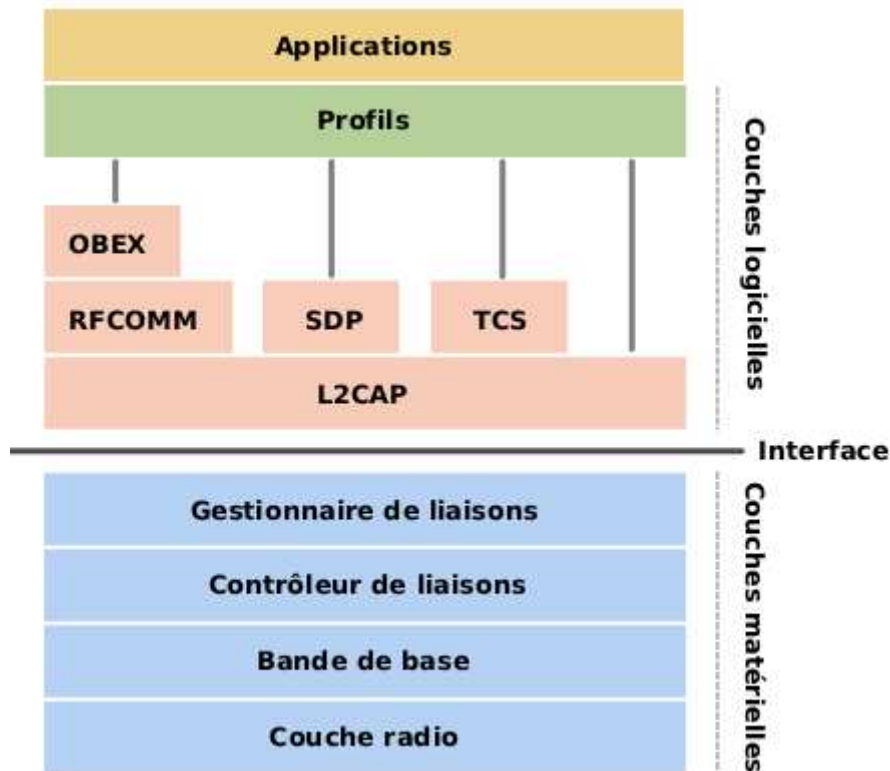
Il s'agit donc d'une connexion entre piconets. Un périphérique peut également devenir l'esclave de plusieurs maîtres de différents piconets.



(Le point rouge entouré de bleu représente le maître d'un piconet qui est en même temps l'esclave d'un autre piconet)

### IV) La pile bluetooth :

Le transport de données en Bluetooth utilise une architecture en couches. Les deux premières couches correspondent au niveau le plus bas de la transmission. La couche physique s'occupe du transfert des bits par modulation de fréquence, des sauts de fréquence, de la détection, etc. La couche logique, séparée en deux couches lien et transport, distingue quant à elle un lien logique utilisé pour des transports indépendants entre deux ou plusieurs périphériques.



(Couches de la spécification bluetooth)

### - 1 La couche radio :

La couche la plus basse, il s'agit d'une couche matérielle. C'est à son niveau que les flux de données sont transformés afin d'être émis sur le support de transmission et les fréquences reçues transformées en bits.

C'est sur cette couche que l'on retrouve l'émetteur. Il faut savoir que la technologie bluetooth est définie en trois classes d'émetteurs et qu'une classe correspond à une puissance d'émetteur et donc à une portée d'émission du signal différent.

Classe	Puissance	Portée
Classe I	100 mW	100 m
Classe II	2.5 mW	15 à 20 m
Classe III	1 mW	10 m

(Tableau des classes d'émetteurs)

### - 2 La couche Bande de base :

Il s'agit d'une couche matérielle aussi.

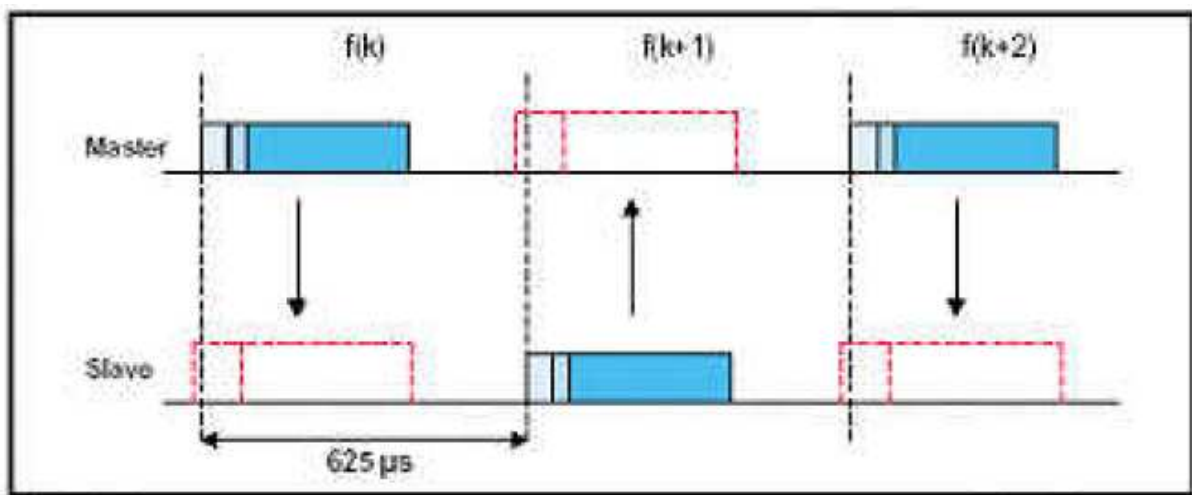
La bande de base (= baseband) définit les adresses matérielles des périphériques bluetooth (correspond à l'adresse MAC d'une carte réseau). Cette adresse est nommée BD\_ADDR (Bluetooth Device Address) et est codée sur 48 bits. Ces adresses sont gérées par l'IEEE Registration Authority.

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.

**- a Le mode synchrone (SCO):**

Synchronous Connection-Oriented dans ce mode on a une liaison symétrique point à point entre un maître et un seul esclave. Pour ce type de mode, des slots à intervalles réguliers sont réservés pour la transmission. Il n'y a pas de retransmission possible dans ce mode.

Ce mode est utilisé pour la transmission de données de type vocale.

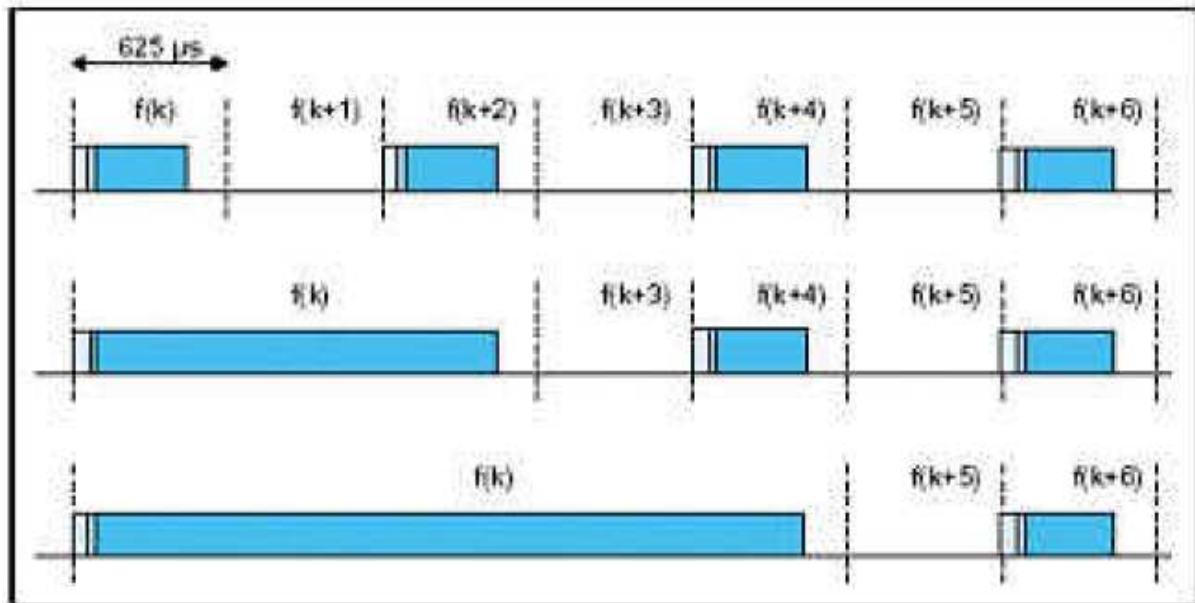


(Chronogramme d'une communication de type synchrone)

**- b Le mode asynchrone (ASC) :**

Asynchronous Connection-Less dans ce mode on a une liaison point à multipoint entre un maître et plusieurs esclaves. Il n'y a pas de slots réservés, une demande ou une réponse peut donc prendre plusieurs slots. La réponse à une demande doit se faire obligatoirement dans le slot suivant. On l'utilise principalement pour la transmission de données.

La retransmission est possible.



(Chronogramme d'une communication de type asynchrone)

### - 3 La couche Contrôleur de liaison :

Cette couche gère la configuration et le contrôle de la liaison physique entre deux appareils.

### - 4 La couche Gestionnaire de liaison :

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

### - 5 L'interface :

Plus précisément L'interface de contrôle de l'hôte (HCI).

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

### - 6 Le L2CAP :

Le protocole d'adaptation et de contrôle de lien logique (L2CAP).

L2CAP est l'équivalent d'un protocole d'accès au média, propre au Bluetooth, permettant de multiplexer des protocoles de couches supérieures (RFCOMM par exemple). Il peut gérer la fragmentation des paquets et le ré-assemblage.

Ce protocole offre la possibilité aux couches supérieures d'envoyer ou de recevoir des paquets allant jusqu'à 64 Ko.

Il fonctionne via des canaux appelés PSM (Protocol/Service Multiplexer) qui se chargent de rediriger les requêtes vers les protocoles des couches supérieures.

Exemple le protocole RFCOMM utilise le PSM 3 tandis que SDP utilise le PSM 1.

Chaque PSM est attaché à un protocole suivant le schéma plusieurs-vers-un. Donc plusieurs canaux peuvent être attachés au même protocole, mais un canal ne peut pas être attaché à plusieurs protocoles.

### - 7 Protocol RFCOMM :

RFCOMM est un protocole de transport simple, il permet des communications de type RS232 (série). RFCOMM peut supporter jusqu'à 60 connexion simultanée.

### - 8 Protocol SDP :

Service discovery protocol (= protocole de découverte de service).

Le SDP permet de découvrir d'autre composant équipé bluetooth et de lister tout les services qu'offre cet équipement.

### - 9 Protocol TCS:

Telephony Control Protocol Specification.

Il s'agit du protocole utilisé pour la circulation des communications audio entre deux appareils bluetooth.

### - 10 Protocol OBEX :

Object Exchange, il permet d'échanger des objets entre deux composants bluetooth.

Les types d'objets échangés sont assez variés, il peut s'agir de carnet d'adresse, de photo, de vidéo etc.

### - 11 Les profils:

Les profils ont été inventés pour faciliter les connexions et pour assurer l'interopérabilité entre les composants bluetooth. Il définit les couches qui devront être utilisé.

Tout les composants bluetooth sont obligatoirement placé dans un profil.

Il existe 24 profils différent :

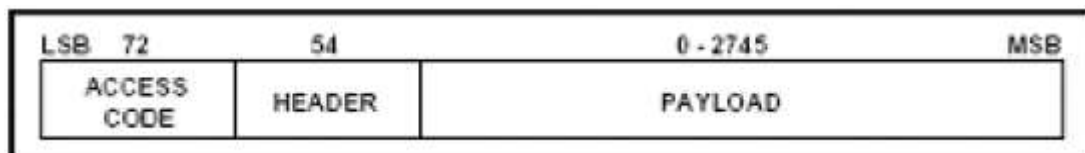
1. GAP: Generic Access Profile
2. SDAP: Service Discovery Application Profile
3. SPP: Serial Port Profile
4. HS Profile: Headset Profile
5. DUN Profile: Dial-up Networking Profile
6. LAN Access Profile (Ce profil est maintenant obsolète. Il est remplacé par le profil PAN)
7. Fax Profile
8. GOEP: Generic Object Exchange Profile
9. SP: Synchronization Profile
10. OPP: Object Push Profile
11. FTP: File Transfer Profile
12. CTP: Cordless Telephony Profile
13. IP: Intercom Profile
14. A2DP : Advanced Audio Distribution Profile (profil de distribution audio avancée)
15. AVRCP : Audio Video Remote Control Profile (Commande à distance)
16. HFP : HandsFree Profile

- 17. PAN: Personal Area Network Profile
- 18. VDP: Video Distribution Profile
- 19. BIP: Basic Imaging Profile
- 20. BPP: Basic Printing Profile
- 21. SYNC: Synchronisation Profile
- 22. SAP: SIM Access Profile
- 23. PBAP : PhoneBook Access Profile
- 24. HIDP : Human Interface Device Profile

## V) Trame bluetooth :

### - 1 Les champs principaux :

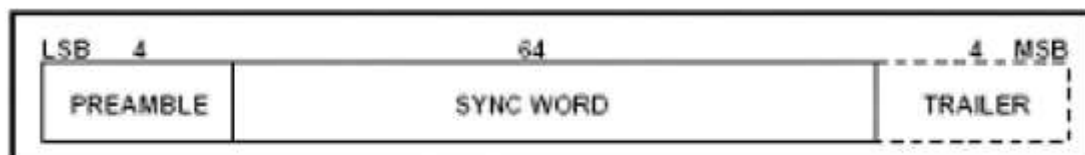
Voici à quoi ressemble une trame de message bluetooth, elle possède trois champs principaux :



- Le champ code d'accès (Access code) est codé sur 68 ou 72 bits, son rôle est de synchroniser, compenser et identifier.
- Le champ En-tête (Header) à une longueur de 54 bits, il code les informations de contrôle (Ex : l'adresse du destinataire, le type de message...).
- Le Corps du message (Payload) peut contenir de 0 à 2745 bits, il s'agit des données à transmettre.

### - 2 Définition des champs d'Access code :

Il se décompose de la manière suivante :



#### **- a Les types de code d'accès :**

Il en existe trois,

- Le CAC : code d'accès du canal.

Il définit le type de réseau bluetooth (le piconet).

C'est le seul type de code d'accès qui possède les trois champs (preamble, sync word et trailer).

- Le DAC : code d'accès du dispositif.

Ce code est utilisé dans certaine procédure de réveil (certain composant bluetooth sont mis en veille pour diminuer leur consommation d'énergie, ex : le mode « parked »). Il ne possède que deux champs, le champ preamble et le champ sync word.

- L'IAC : code d'accès d'inquiry.

Ce type de code est utilisé par un composant bluetooth pour rechercher un autre composant bluetooth qui est à portée. Tout comme le DAC il ne possède que deux champ, le preamble et le sync word.

**- b Le champ preamble :**

Ce champ ne peut prendre que deux valeur 1010 ou 0101 en fonction de la valeur du bit de poids faible du champ sync word. Il est utilisé pour contre balancer la composante continu (éviter une suite de 0 ou une suite de 1). Il est codé sur 4 bits.



**- c Le champ sync word( = mot de synchronisation) :**

Le sync word est composé de 64 bits qui dérivent des 24 bits de poids faible de l'adresse du composant bluetooth. Il s'agit de la LAP (low address part).

L'adresse choisie (celle du maître, de l'esclave ou autre voir en dessous) dépend du type de code d'accès.

Voici un tableau qui définit qu'elle LAP utilisée en fonction du type de code d'accès.

Type de code d'accès	LAP
IAC	réservées
DAC	esclave
CAC	maître

Pour l'IAC des adresses dédiées sont utilisées.

**- d Le champ Trailer :**

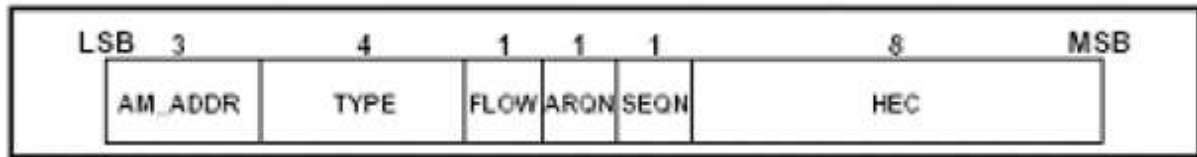
Tout comme pour le preable, le Trailer à pour but de contre balancer la constante continu mais cette fois si du bit de poids fort du sync word.

Il est composé de 4 bits et ne peut prendre que deux valeur (1010 ou 0101).



### - 3 Définition des champs de HEADER :

Il est composé de 6 champs et ressemble à ceci:



Description des champs :

**- a Le champ AM\_ADDR (3 bits):**

Il indique l'adresse du destinataire du message.

**- b Le champ TYPE (4 bits) :**

Il indique le type de paquet de données et le type de liaison si c'est une liaison synchrone (SCO) ou asynchrone(ACL).

**- c Le champ FLOW (1 bit) :**

Il permet de contrôler le flux, uniquement pour les liaisons asynchrones.

Si flow=0, on interrompt la transmission.

Si flow=1, on transmet.

**- d Le champ ARQN (1 bit) :**

Il s'agit d'un bit d'acquiescement. Ce bit est transmis avec le message de retour.

Si sa valeur vaut 1 : le message à bien été reçu.

Si sa valeur vaut 0 : Le message n'a pas été reçu ou il n'y a pas de message de retour.

Par défaut ARQN vaut 0.

**- e Le champ SEQN (1 bit) :**

Il s'agit du numéro de séquence, il permet de filtrer les retransmissions.

Ce bit est inversé à chaque nouvelle transmission de paquet de données.

Le destinataire peut grâce à ce bit ignorer la retransmission d'un paquet de données qu'il à déjà reçu mais qui n'a pas été acquitté.

**- f Le champ HEC (8 bits) :**

Header error check.

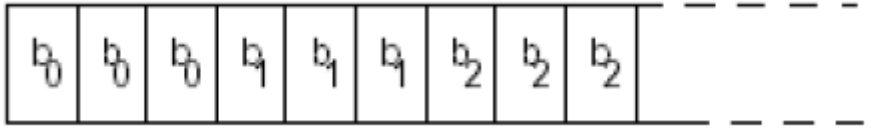
Il contrôle les erreurs de l'entête.

Le champ header comprend donc 18 bits mais se champs est protéger par un codage FCE (1/3 FCE pour être plus précis). Le champ header à donc une taille de 54 bits.

### - g Le FCE :

FCE signifie forward correcting error, le but de ce type de protection est d'écrire des informations, de manière redondante, dans le corps des paquets.

Le 1/3 FCE contient trois la même information.



(Exemple du 1/3 FCE)

### - 4 Définition des champs de PAYLOAD :

Le champ PAYLOAD dépend de 4 paramètres.

Ces paramètres sont :

1. Type de liaison : il y aura des modifications en fonction du fait qu'i s'agit d'une liaison synchrone ou une liaison asynchrone.
2. Type de message : Il s'agit des informations donné dans le HEADER.
3. Application d'un codage correcteur d'erreur (EX : le 1/3 FCE).
4. Présence d'un CRC : cyclic redundancy check. Le CRC permet de détecter les erreurs et de demander une retransmission.

Mais en général, on retrouve deux types de champ :

-Le champ Data Field (données) qui possède sa propre entête (PAYLOAD HEADER).

-Le champ Voice Field (voix).

Attention un message en mode synchrone ne possède que le champ voix tandis qu'un message en mode asynchrone ne possède que le champ données.

Mais certain type de message possède les deux champs.

Voici un tableau qui reprend les principaux types de message possible :

Packet Type	Type	TYPE Code	Payload Header (Bytes)	User Payload (Bytes)	FEC	CRC	Remarques
Link Control	ID	***	NO	NO	NO	NO	Contient le DAC ou le IAC
	NULL	0000	NO	NO	NO	NO	Contrôle de la transmission précédente (ARQN, FLOW)
	POLL	0001	NO	NO	NO	NO	Permet au Maître de contacter les esclaves qui doivent répondre
	FHS	0010		18	2/3	YES	Transmet l'adresse Bluetooth et le signal d'horloge de l'émetteur
ACL	DM1	0011	1	0-17	2/3	YES	Transfert de data. Longueur de l'émission < 1 timeslot
	DH1	0100	1	0-27	NO	YES	Idem DM1
	DM3	1010	2	0-121	2/3	YES	Transfert de data. Longueur de l'émission < 3 timeslots
	DH3	1011	2	0-183	NO	YES	Idem DM3
	DM5	1110	2	0-224	2/3	YES	Transfert de data. Longueur de l'émission < 5 timeslots
	DH5	1111	2	0-339	NO	YES	Idem DM5
	AUX1	1001	1	0-29	NO	NO	Idem DM1
SCO	HV1	0101	NO	10	1/3	NO	Données synchrones (voix). Pas de retransmission. $T_{SCO} = 2$
	HV2	0110	NO	20	2/3	NO	Données synchrones (voix). Pas de retransmission. $T_{SCO} = 4$
	HV3	0111	NO	30		NO	Données synchrones (voix). Pas de retransmission. $T_{SCO} =$
	DV	1000	1	10 + 0-9	2/3	YES	Données synchrones (10 bytes voix + 0-9 bytes data). FEC, CRC et retransmission pour la partie data seulement

## VI) Création d'une connections entre bluetooth :

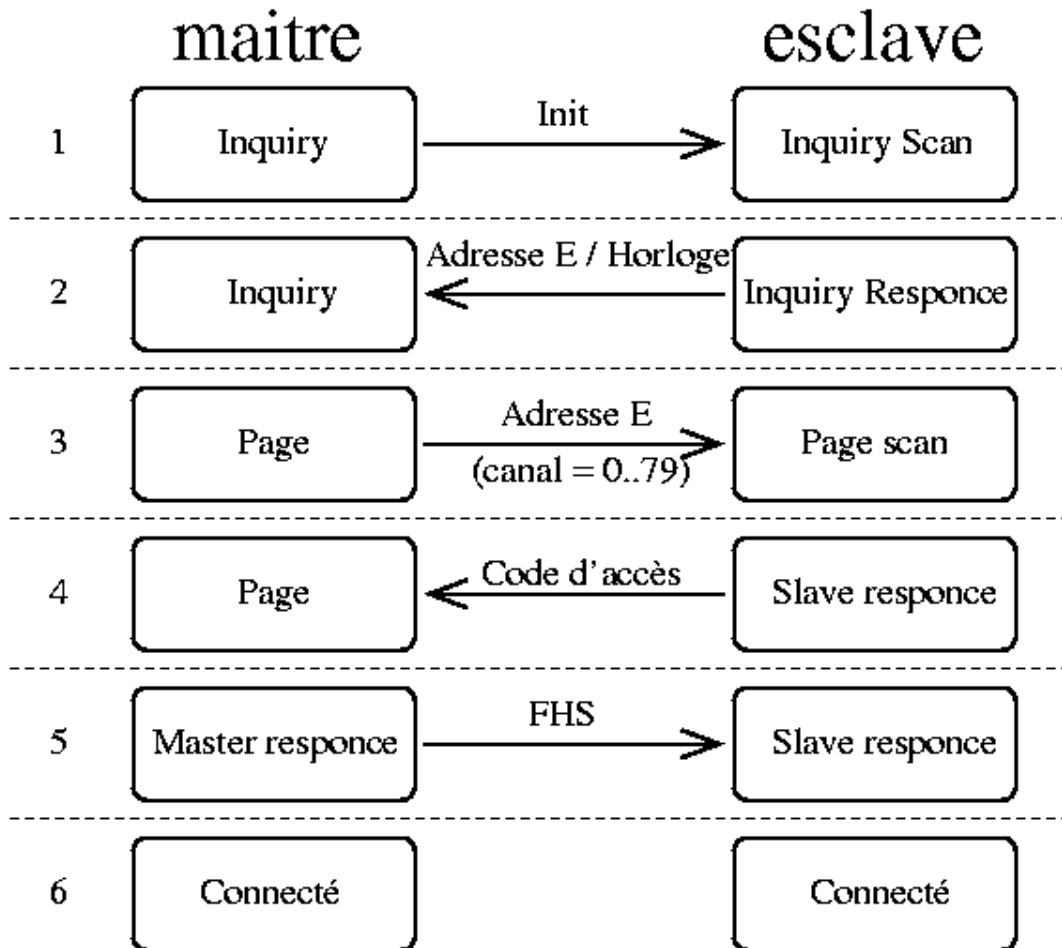
Une connexion bluetooth se fait toujours dans un mode maitre/esclave.

Au début du processus, le maître M doit se trouver dans le sous état " Inquiry " et l'esclave E dans l'état " Inquiry scan " :

1. Etant dans l'état " Inquiry ", M envoie un signal pour prévenir E qu'il souhaite initialiser une connexion. E se trouve alors dans l'état " inquiry scan".
2. Si E se trouve à portée et qu'il est dans l'état " Inquiry scan ", il passe alors dans le sous état " Inquiry response " puis répond effectivement au maître. La réponse de E comporte entre autre son adresse ainsi que des informations sur son horloge.
3. Une fois que E a envoyé sa réponse, il passe dans l'état " Page Scan ". Il se met ensuite en attente d'un message comportant sa propre adresse sur un des 80 canaux existants. Lorsque M reçoit le message réponse de E, celui-ci passe dans l'état " page ". C'est à dire que M stocke les informations reçues (pagination). Ces informations permettent à M d'avoir conscience de la présence de E. Lorsque M souhaite poursuivre le processus de connexion, celui-ci renvoie un message réponse en y plaçant l'adresse de E. Ce message est renvoyé plusieurs fois sur tous les canaux.
4. Lorsque E voit une réponse à son nom arriver, il se place dans le sous état " Slave response " puis renvoie un message - réponse à M en y joignant son code d'accès.
5. De son côté, M une fois ce code d'accès récupéré, se place alors dans un état " Master response " et renvoie un paquet de type FHS à E. Ce paquet de type FHS (Frequency Hopping Synchronisation) permet à E de se synchroniser avec M.

6. Une fois ce dernier message envoyé, M passe dans l'état " connecté". De même, lorsque E reçoit ce message il passe aussi dans l'état "connecté".

Ici l'état "connecté" n'est pas un sous état. Pour vérifier que la connexion s'est bien passée, le maître envoie un paquet et attend en retour n'importe quel type de paquet. Si une connexion s'est effectivement bien passée, l'esclave est synchronisé avec son maître et se trouve sur le bon canal de communication.



## VII) La sécurité :

Vu le nombre croissant d'équipement bluetooth disponible sur le marché, de plus en plus de personnes se sont mises à essayer de pirater cette technologie. Il était donc indispensable d'avoir une sécurité à la hauteur de son succès.

Dans ce chapitre, on s'attardera sur les types de sécurités que nous propose le bluetooth. On verra aussi une partie des différentes attaques répertoriées jusqu'à aujourd'hui.

Le bluetooth propose trois modes de sécurité, le choix du mode de sécurité est laissé à l'appréciation du constructeur du composant bluetooth.

Il est implémenté dans le chipset bluetooth.

Ces trois modes sont :

Mode 1 : Pas de mécanisme de sécurité.

Mode 2 : Sécurité assurée au niveau applicatif.

Mode 3 : Sécurité assurée au niveau liaison de données.

Le mode de sécurité 3 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. Il nécessite une authentification.

Le mode de sécurité 1 permet à un appareil bluetooth d'offrir ses services à tous dispositifs bluetooth à portée. Ce mode peut être comparé à un hotspot wifi public.

### - 1 Le couplage :

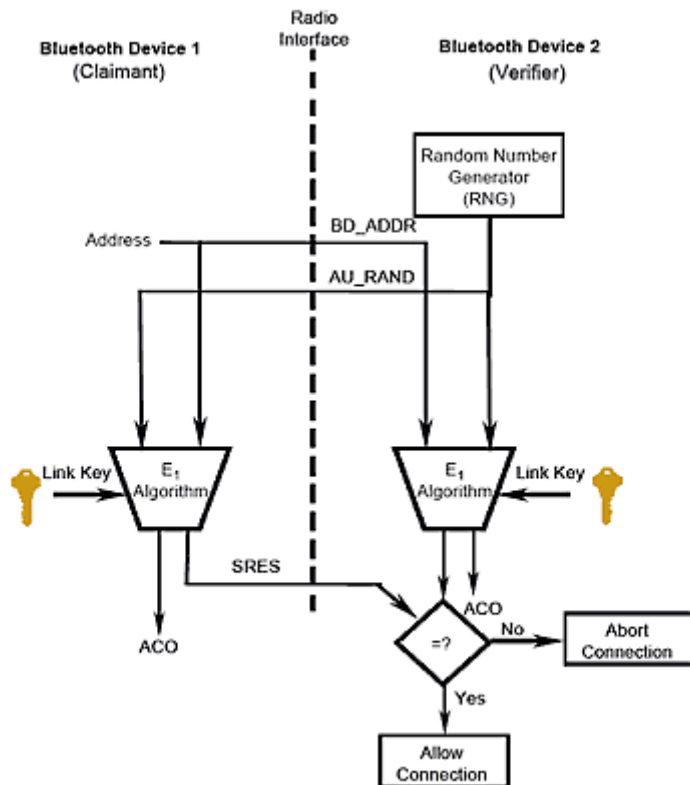
Par défaut, une communication Bluetooth n'est pas authentifiée, et n'importe quel périphérique peut parler avec n'importe quel autre périphérique. Un périphérique Bluetooth peut choisir de demander une authentification pour fournir un service particulier.

L'authentification Bluetooth est généralement effectuée avec des codes PIN. Un code PIN est une chaîne ASCII. L'utilisateur doit entrer le même code PIN sur les deux périphériques. Une fois que l'utilisateur a entré le code PIN, les deux périphériques génèrent une clé de liaison (link key). Ensuite la clé peut être enregistrée soit dans les périphériques eux-mêmes ou sur un moyen de stockage non-volatile. La fois suivante les deux périphériques utiliseront la clé précédemment générée. La procédure décrite est appelée couplage. Si la clé de liaison est perdue par un des périphériques alors l'opération de couplage doit être répétée.

### - 2 Comment se passe l'authentification ?:

Elle s'opère selon le schéma suivant :

1. L'appareil qui initie la connexion envoie son adresse (BD\_ADDR). Cette adresse de 48 octets est unique, tout comme l'adresse MAC de la carte de réseau. L'adresse permet d'identifier le fabricant de l'appareil.
2. La séquence aléatoire de 128 chiffres AU\_RANDOM (challenge) est envoyée en réponse.
3. Sur la base de BD\_ADDR, de la clé de combinaison et d'AU-RAND, les deux appareils génèrent la séquence de cryptage SRES.
4. L'appareil qui demande la connexion envoie son SRES.
5. L'appareil contacté compare le SRES reçu et le sien et s'ils correspondent, il établit la connexion.



### - 3 Les différentes attaques :

#### **- a Bluejacking :**

Cette attaque, que l'on peut comparer à du spam, consiste à détourner l'utilisation principale liée au profil OPP (Object Push Service).

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

Le hacker peut remplir comme il l'entend les champs de sa carte de visite et faire afficher ce texte sur un appareil bluetooth choisi.

#### **- b Bluesnarfing :**

Cette attaque permet à un hacker de télécharger depuis un équipement bluetooth vulnérable un ou plusieurs fichiers. Le bluesnarfing perd beaucoup en furtivité si les fabricants d'équipements bluetooth implémentent le mode sécurité 2.

Par conséquent, le hacker devra avoir un code d'accès et la cible devra autoriser le hacker à se connecter à son réseau bluetooth.

### - c BlueBug :

Le BlueBug est sûrement la faille pouvant se révéler la plus lourde de conséquences pour une victime. Cette attaque touche principalement les GSM. Elle consiste à se connecter sur un port RFCOMM qui ne nécessite aucune authentification permettant ainsi l'accès à un certain nombre de commandes. Ces commandes permettent un contrôle presque complet du GSM. Il suffit de sniffer rapidement les équipements présents dans un lieu public pour se rendre compte du nombre d'utilisateur qui sont des cibles potentielles.

### - d BlueSmack :



BlueSmack est une attaque visant à bloquer les périphériques Bluetooth (crash de la pile ou du système d'exploitation distant) via une requête anormalement longue ou en envoyant beaucoup de requêtes.

La solution à se problèmes est venue des constructeurs qui ont limité la taille des trames L2CAP.

## VIII) Cas d'utilisation et composant bluetooth:

### - 1 Les composants bluetooth.

Voici une liste de quelques produits bluetooth déjà existants ou qui seront bientôt sur le marché.



Cette carte de motorola au format PCMCIA permet par exemple de connecter un ordinateur portable à un réseau bluetooth



L'infostick de Sony. Cette carte pesant 4g et d'une dimension de 21.5 \* 55 \* 2.8 mm se connecte sur les PDA et les appareils photo.

Elle peut donc permettre de se connecter à Internet sur un PDA ou de rapatrier ses photos numériques sur une unité de stockage plus importante que la mémoire de l'appareil photo.



Cet appareil de TDK est un adaptateur USB. Il se branche sur la sortie USB (Universal Serial Bus) de n'importe quel ordinateur et lui apporte la compatibilité Bluetooth.



Certains portables sont directement équipés de la puce bluetooth.



Une montre bluetooth créée par IBM. Elle permet de recevoir en temps réel des données provenant d'un PC et permet de diriger une présentation PowerPoint depuis le poignet.

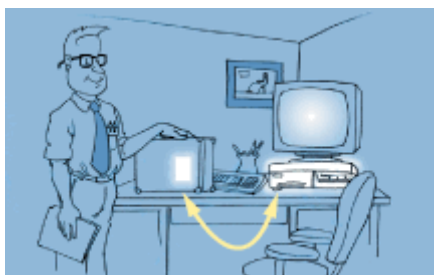


Des adaptateurs bluetooth pour les imprimantes lasers. L'adaptateur vient se connecter au port parallèle de l'imprimante et communique par ondes radio avec un point d'accès lui-même connecté au réseau local et au delà au serveur d'impression.



Ce modem bluetooth d'Elsa permet de connecter un PC à Internet même s'il se trouve éloigné d'une prise téléphonique.

## - 2 Utile :



En rentrant chez vous, votre PDA (Personnal Digital assistant = agendas électroniques) se synchronise avec votre ordinateur, transfère vos fichiers et vos e-mails.



Lors d'une conférence, vous envoyez votre présentation (stocké sur votre PDA) au vidéo projecteur que vous pilotez à distance grâce à votre PDA. A la fin de la réunion, vous transférez cette présentation et d'autres fichiers importants aux participants.



Un rentrant chez vous, votre maison détecte votre arrivée, déverrouille votre porte d'entrée et allume la lumière.



Votre système d'alarme est équipé de composants bluetooth. Vous pouvez améliorer votre système en ajoutant d'autres composants (une sirène, un détecteur). Ils se reconnaissent et se configurent automatiquement en communiquant avec la centrale.



En arrivant à l'aéroport, vous n'avez pas besoin de faire la queue pour prendre un billet : votre PDA bluetooth vous identifie auprès du guichet, confirme votre réservation et sélectionne votre numéro de siège suivant les préférences que vous aviez préalablement réglées.



En entrant dans un parc, une carte du parc est envoyée à votre voiture qui l'affiche sur un écran. On peut sélectionner les lieux que l'on souhaite visiter, et le circuit guidé est alors téléchargé dans votre voiture.



En approchant de votre voiture, elle se déverrouille, le siège se règle à votre hauteur, la radio se met sur votre station préférée.



Vous recevez un appel téléphonique pendant que vous conduisez, celui-ci est automatiquement transmis à votre autoradio qui fait sortir le son par les enceintes de la voiture.

Il y a aussi d'autres cas d'utilisation plus simple et que l'on utilise déjà régulièrement. Comme par exemple transférer des images, des vidéos ou des fichiers audio de son Gsm à son ordinateur et inversement.

### - 3 Inutile :

Malheureusement on en arrive aussi à utiliser le bluetooth à des fins inutile et qui risque de compliquer la vie des gens plus qu'autre chose.

Exemple : le bluespoot.



Le bluespoot permet de diffuser gratuitement un contenu multimédia (son, image, diaporama, vidéo) aux appareils bluetooth environnants.

L'utilisateur à quand même le choix d'accepter ou pas.

Il s'agit tout simplement de publicité par bluetooth.

Pour avoir un aperçu de ses publicités, on peut se rendre sur <http://www.bluespoot.com/> et ensuite choisir l'onglet exemples.

## IX) Le future :

L'avenir du bluetooth c'est la sortie de la version 3.0, elle était déjà prévue pour la fin 2007 mais sa sortie à été repoussée à une date encore inconnue. L'association de la WiMedia Alliance et du Bluetooth Special Interest Group sont à l'origine des spécifications du standard. L'IEEE 802.15.3a sera certainement baptisé UWB (Ultra Wideband Bluetooth). La version 3.0 devrait proposer un débit équivalent à celui d'un câble USB 2.0 dans un rayon d'environ trois mètres. Ainsi, il atteindra les 100 Mbit/s (12,5 Mo/s) contre environ 1 Mbit/s actuellement.

Pour cela, le nouveau protocole n'utilisera plus la bande des fréquences de 2,4 GHz, celle qu'il utilise actuellement, mais il exploitera celle au dessus des 6 GHz. L'alliance compte également élargir la gamme de produits équipés de la norme aux caméscopes, téléviseurs et aux appareils photo.

Même si l'UWB sera principalement utilisé pour les GSM, une telle diversification risque de la mettre en concurrence directe avec le WUSB, l'USB sans fil qui proposera quant à lui des débits supérieurs de l'ordre de 60 Mo/s.

## X) Conclusion :

Suite à ce rapport on peut en conclure que le bluetooth est une norme qui offre de très nombreux avantages et très peu d'inconvénient.

Son faible prix, sa petite taille et sa faible consommation énergétique en font l'allier principale de la communication sans fil pour tout les équipements fonctionnant sur batterie. De plus, les petits soucis de sécurité rencontrés restent assez marginaux et ils devraient être rapidement résolus.

Il devrait continuer à s'imposer même dans d'autres que la téléphonie notamment grâce à la sortie de la norme 3.0 qui permettra des transferts de donnée très rapide.

Il ne faut pas oublier que le bluetooth est une norme encore assez récente, il faut lui laisser le temps de se faire connaître notamment au prêt du grand public.

## XI) Bibliographie :

-<http://blog.bbreton.net/index.php?post/2004/06/28/66-un-peu-dhistoire>

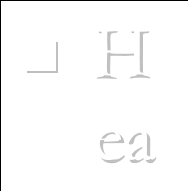
-<http://www.fujitsu.com/ca/fr/news/publications/articles/bluetooth.html>

-<http://fr.wikipedia.org/wiki/Bluetooth>

-[http://fr.wikipedia.org/wiki/Alphabet\\_runique](http://fr.wikipedia.org/wiki/Alphabet_runique)

-<http://www.frameip.com/bluetooth/>

-<http://www.jmburri.ch/details.php?recordID=124>



- <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/>
- <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/>
- [www.bluespoot.com](http://www.bluespoot.com)
- <http://www.dicodunet.com/actualites/e-commerce/14771-bluetooth-3.0-pourrait-accelerer-a-400-mb-s.htm>
- <http://www.presence-pc.com/actualite/bluetooth-2-1-24536/>
- <http://www.generation-nt.com/bluetooth-sig-bluetooth-2-1-edr-approbation-actualite-43750.html>
- <http://www.generation-nt.com/bluetooth-sig-choix-wifi-rejet-uw-b-actualite-47009.html>
- <http://www.bestofmicro.com/guide/savoir-Adaptateur-Bluetooth,5-aWRHdWlkZT03NyZpZENsYXNzZXVyPTZNCZpZfJ1YnJpcXVIPTQ3OCZpZFBhZ2U9MTc3OQ==.html>
- <http://www.laboratoire-microsoft.org/articles/web/bluetooth/>
- <http://www.aug-strasbourg.org/article.php?sid=67360>
- <http://www.frameip.com/bluetooth/>
- <http://direct.motorola.com/hellomoto/bluetoothpromotion/bluetooth.asp>
- <http://french.bluetooth.com/Bluetooth/Technology/>
- <http://www.clubic.com/article-14372-3-les-reseaux-locaux-sans-fil.html>
- <http://www.ituarabic.org/wireless-systems/2nd-day%5CBluetooth%20Specs%20Report.pdf>
- <http://www.secuobs.com/news/05022006-bluetooth1.shtml>
- [http://www.zdnet.fr/produits/materiels/assistants\\_personnels/0,49050652,1001647,00.htm](http://www.zdnet.fr/produits/materiels/assistants_personnels/0,49050652,1001647,00.htm)
- <http://www.secuobs.com/news/05022006-bluetooth3.shtml>
- <http://www.bestofmicro.com/guide/base-Adaptateur-Bluetooth,4-aWRHdWlkZT03NyZpZENsYXNzZXVyPTEzNCZpZfJ1YnJpcXVIPTQ3OSZpZFBhZ2U9MTc4NQ==.html>
- [http://trifinite.org/trifinite\\_stuff\\_bluesmack.html](http://trifinite.org/trifinite_stuff_bluesmack.html)
- <http://www.viruslist.com/fr/analysis?pubid=180598400>
- <http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/>
- <http://www.presence-pc.com/actualite/bluetooth-uw-b-15818/>
- <http://en.wikipedia.org/wiki/Bluetooth>