

Valentin Rudy
Informatique

Périphérique:



Année 2007-2008

Table des matières

- I) Introduction
- II) Le Bluetooth SIG
- III) Les schémas de connexions
- IV) La pile bluetooth
- V) Trame bluetooth
- VI) Création d'une connexion entre bluetooth
- VII) La sécurité
- VIII) Cas d'utilisation et composant bluetooth
- IX) Le future
- X) Conclusion

I) Introduction

- - 1 Qu'est ce que le bluetooth
- - 2 Pourquoi utiliser le bluetooth
- - 3 Historique
- - 4 Origine du nom
- - 5 Les normes
- - 6 Les évolutions 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).

- 2 Pourquoi utiliser le bluetooth ? :

- L'installation de composants (tels que des imprimantes) et leur mise en réseau n'est pas toujours facile à cause d'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



Puce bluetooth agrandie



La puce peut prendre place dans une clé USB-Bluetooth

- 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 références a un roi Viking du 10^{ème} 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.
- Il unifia la Norvège, le Danemark et la Suède 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 suédois c'est pourquoi leur choix c'est porté sur un roi Viking plutôt qu'un autre.



Photo de Harald Blatand

- 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 version 1.x:
 - 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.
 - L'évolution logique de la norme 802.15.1.
 - Capacités accrues en termes de bande passante, de portée, de sécurité et de débit.
 - La version 2.x du bluetooth repose sur cette norme.

- 802.15.4 : Il s'agit d'un standard visant à proposer du bas débit : LR-WPAN pour Low Rate WPAN.
 - Réseau de communication simple et peu coûteux.
 - Besoin énergétique très limité afin d'assurer une longue durée de vie
 - Principalement utilisés pour les réseaux domestiques.

- 6 Les évolutions bluetooth :

- Bluetooth 1.0 et 1.0 B :

- Ces versions ont rencontré beaucoup de problèmes:

- L'interopérabilité des composants.

- 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 ratifié en 2002.
 - Correction de la plupart des erreurs du bluetooth 1.0 et 1.0 B.
 - 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, Les principales améliorations sont :
 - La découverte et la connexion à d'autres composants est plus rapide.
 - Plus résistant aux interférences.
 - Vitesse de transmission accrues.

■ Bluetooth 2.0 :

- Adopté par le SIG en novembre 2004.
- Cette version est elle aussi retro-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: Fournit 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.
- 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, ils ont le rôle clé dans le développement de la technologie sans fil Bluetooth. Ils intègrent celle-ci à leurs différents produits et ils la commercialise.
- Le SIG comporte des équipes spécialisées restreintes à Hong Kong, en Suède et aux États-Unis.

- Le siège social du bluetooth SIG à Washington, aux États-Unis.
- Composition:
 - Directeur exécutif: Michael Foley
 - Directeur marketing: Anders Edlund
 - Une petite équipe de professionnels du marketing, de l'ingénierie et de l'exploitation.
 - Des bénévoles, apportent leurs compétences 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.
- Le bluetooth SIG comprend des milliers de sociétés affiliées et adeptes

III) Les schémas de connexions

- - 1 Le réseau le plus simple
- - 2 Le piconet
- - 3 Le scatternet

- Pour qu'il y est une communication, il faut:

- au moins un maitre.

Un maitre peut administrer jusqu'à 7 esclaves actifs en même temps et 255 esclaves parked.

- Parked définit un état passif d'un esclave.

L'esclave n'envoi pas et ne reçoit pas de donné. Il ne fait que se réveiller de temps en temps pour se synchroniser avec le maître grâce à des "balises" que le maitre envoi à des intervalles régulier.

Cet état permet de ne pas prendre une des 7 places réservé aux esclaves actifs.

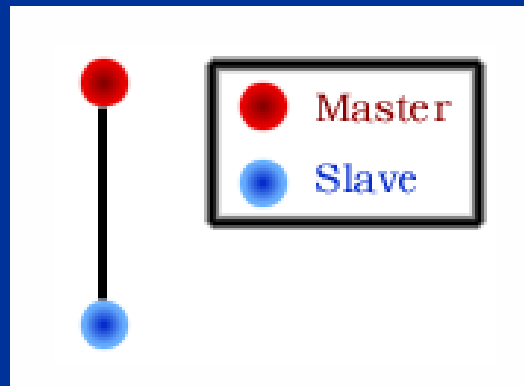
- Il peut donc y avoir jusqu'à 8 appareils chainés et actifs pour former un réseau bluetooth que l'on appelle picoréseau ou piconet.

- Il est possible d'interconnecter des piconets pour former des réseaux plus grands appelé scatternets.

Dans ce cas, certains appareils bluetooth serviront de passerelle. Ils auront un double rôle celui de maitre et celui d'esclave. On peut connecter 10 piconets ensemble aux maximum, ce qui nous donne 72 systèmes actifs.

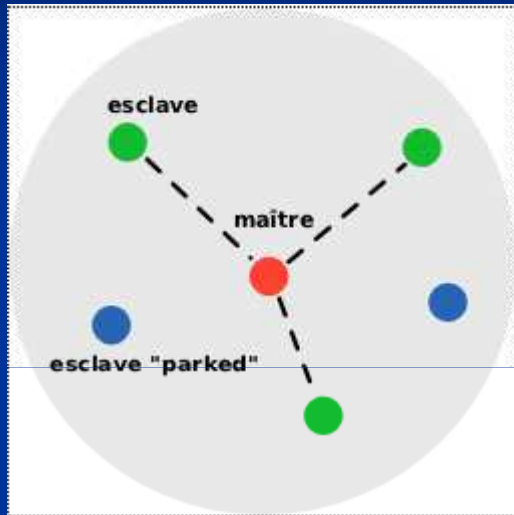
- 1 Le réseau le plus simple :

- 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.

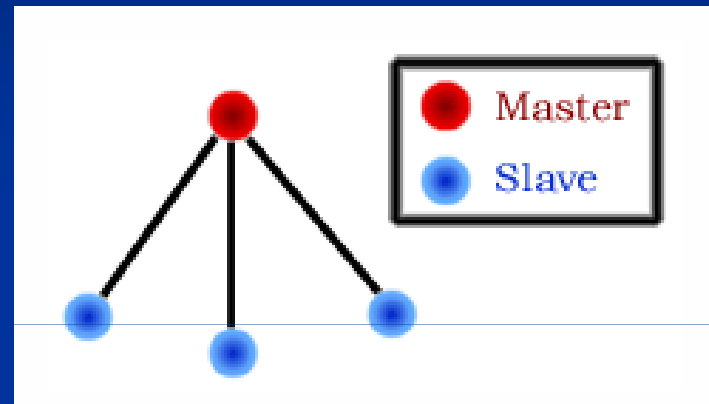


- 2 Le piconet :

- Il faut au moins trois périphériques.
 - Un des périphériques devient le maître.
 - Les autres, les esclaves.
 - Le maître est chargé de gérer les communications entre les différents esclaves.
 - Si 2 esclaves souhaitent échanger des informations, cette discussion est orchestrée par le maître. Les esclaves ne peuvent pas communiquer directement entre eux.



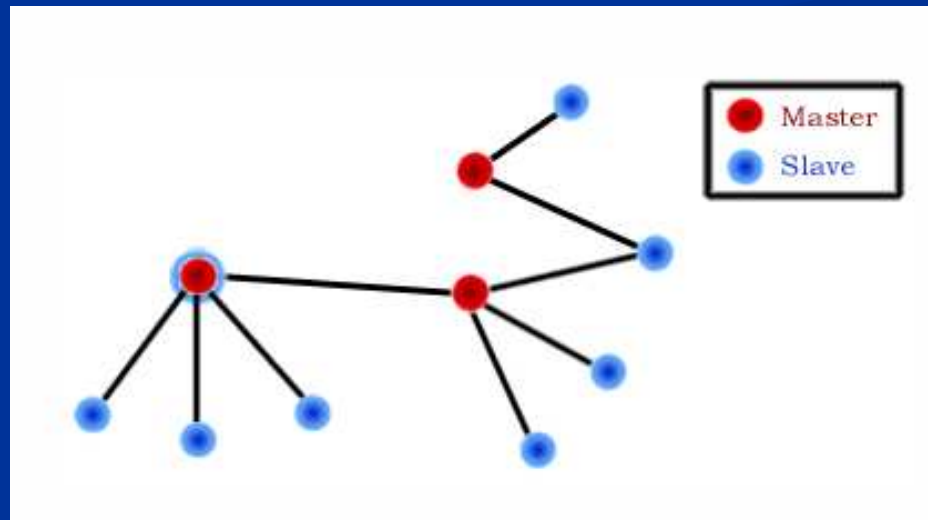
Un piconet avec ses
esclaves « parked »



Un Piconet

- 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.
 - Un maître d'un piconet peut être un esclave dans un autre piconet.

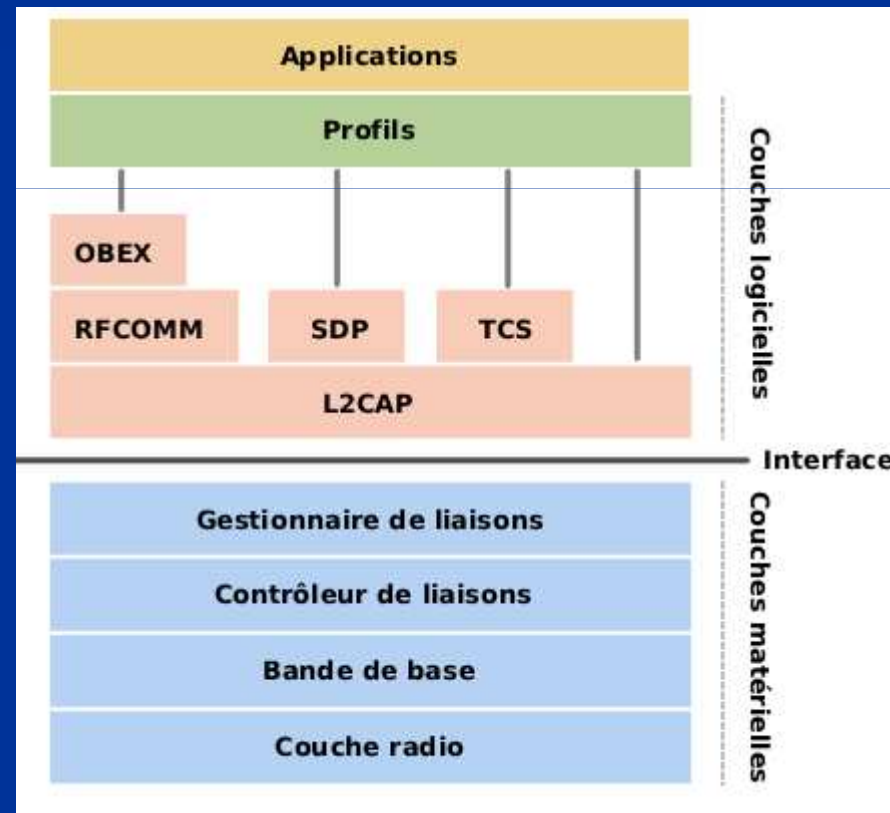


IV) La pile bluetooth

- - 1 La couche radio
- - 2 La couche bande de base
 - a Le mode
 - b Le mode asynchrone
- - 3 La couche contrôleur de liaison
- - 4 La couche gestion de liaison
- - 5 L'interface
- - 6 Le L2CAP
- - 7 Protocol RFCOMM
- - 8 Protocol SDP
- - 9 Protocol TCS
- - 10 Protocol OBEX
- - 11 Les profils

■ Structure en couche

- Couches matérielles.
- Couches logicielles
- L'interface qui sert de lien entre les couches matérielles et logicielles.



- 1 La couche radio :

- La couche matérielle, la plus basse. 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.
- On y trouve l'émetteur.
 - La technologie bluetooth est définie en trois classes d'émetteurs.
 - Une classe correspond à une puissance d'émetteur et donc à une portée d'émission du signal différent.

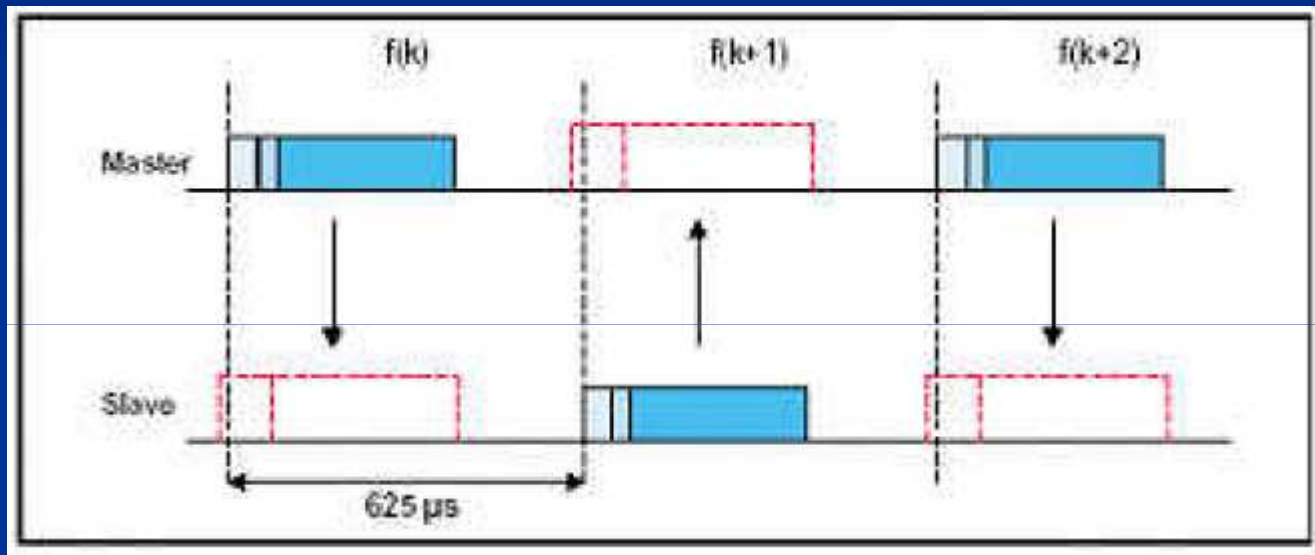
Classe	Puissance	Portée
Classe I	100 mW	100 m
Classe II	2.5 mW	15 à 20 m
Classe III	1 mW	10 m

- 2 La couche Bande de base :

- Il s'agit d'une couche matérielle aussi.
- Définie les adresses matérielles des périphériques bluetooth (correspond à l'adresse MAC d'une carte réseau).
 - Adresse BD_ADDR (Bluetooth Device Address)
 - codée sur 48 bits.
 - Adresses gérées par l'IEEE Registration Authority.
- Elle gère également 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):

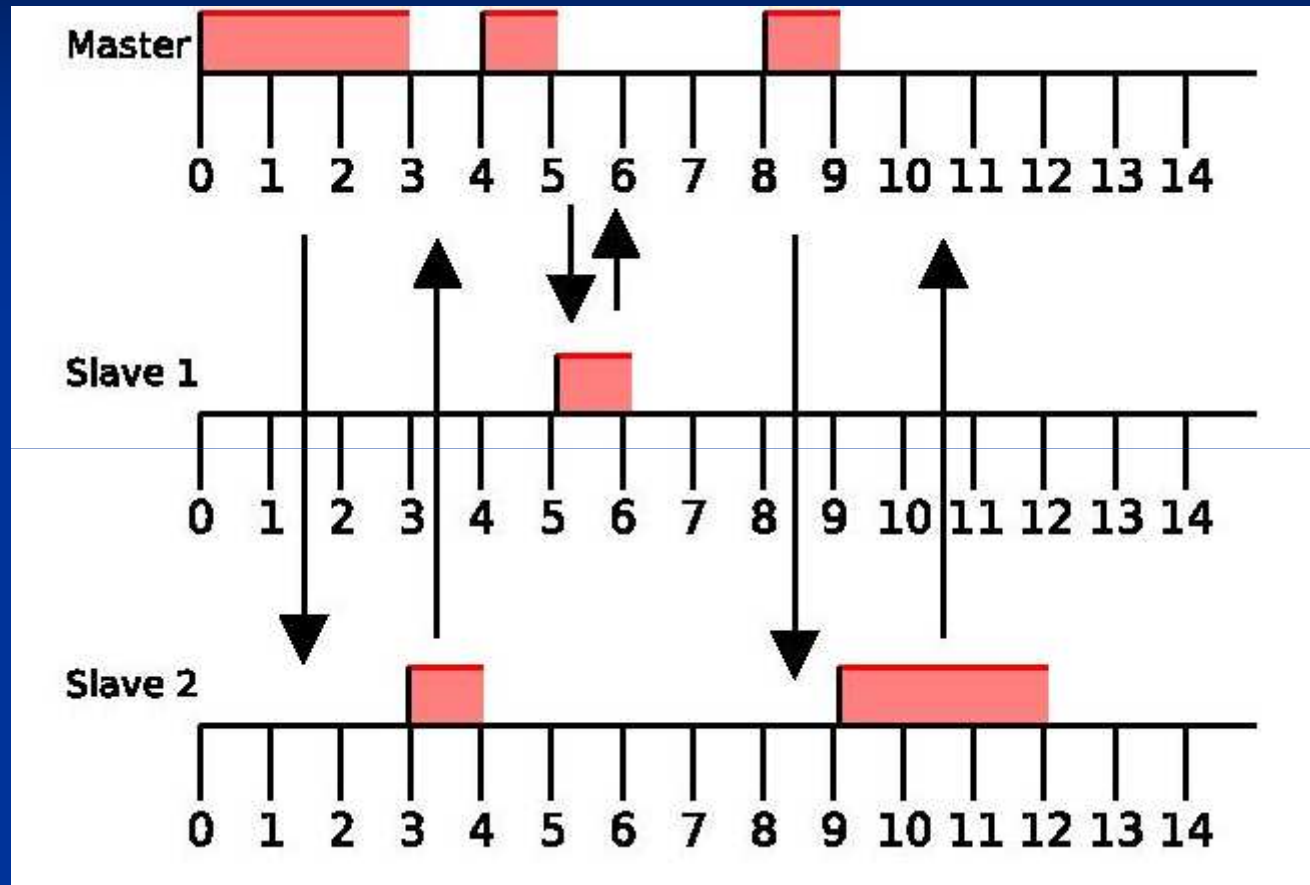
- Synchronous Connection-Oriented.
 - On à une liaison symétrique point à point entre un maitre et un seul esclave.
 - Des slots à intervalles réguliers sont réservés pour la transmission.
 - Pas de retransmission possible.
- Ce mode est utilisé pour la transmission de donnée de type vocale.



Chronogramme d'une communication de type synchrone

- b Le mode asynchrone (ASC) :

- Asynchronous Connection-Less
 - On a une liaison point à multipoint entre un maître et plusieurs esclaves.
 - Pas de slots réservés, une demande ou une réponse peut donc prendre plusieurs slots.
 - La réponse doit se faire obligatoirement dans le slot suivant.
 - La retransmission est possible.
- Ce mode est utilisé principalement pour la transmission de données.



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. Commande la construction de paquet à la couche inférieure.

- 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).
- C' est l'équivalent d'un protocole d'accès au média(mais pour le Bluetooth).
 - Il permet de multiplexer des protocoles de couches supérieures.
- Il peut gérer la fragmentation des paquets et le ré-assemblément.

- Il 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).
 - Ils redirigent les requêtes vers les protocoles des couches supérieures.
- Chaque PSM est attaché à un protocole suivant le schéma plusieurs-vers-un.
 - 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:

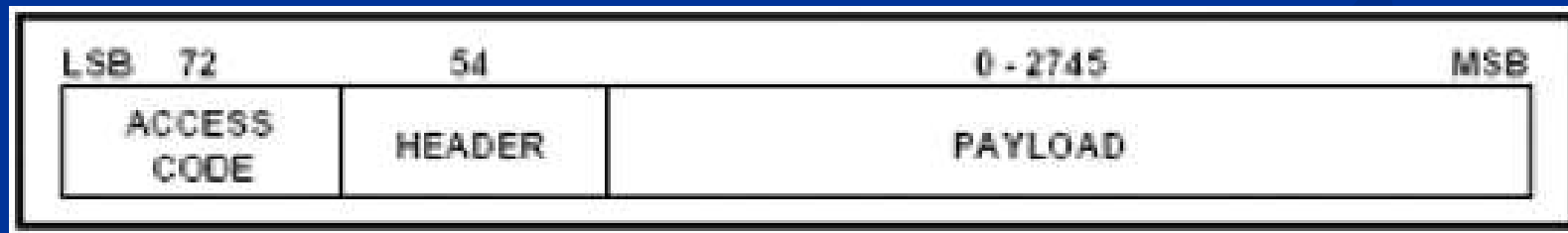
- Les profils facilite les connexions et assure l'interopérabilité entre les composants bluetooth.
- Tout les composants bluetooth sont obligatoirement placé dans un profile.
- Il définit les couches qui devront être utilisé.
- Il existe 24 profiles différent :
 - GAP, SDAP, SPP, HS Profile, DUN Profile, LAN Access Profile, Fax Profile, GOEP, SP, OPP, FTP, CTP, IP, A2DP, AVRCP, HFP ,PAN, VDP, BIP, BPP, SYNC, SAP,PBAP, HIDP

V) Trame bluetooth

- - 1 Les champs principaux
- - 2 Définition des champs d'Access code
 - a Les types de code d'accès
 - b Le champ preamble
 - c Le champ sync word
 - d Le champ trailer
- - 3 Définition des champs de HEADER
 - a Le champ AM_ADDR
 - b Le champ TYPE
 - c Le champ FLOW
 - d Le champ ARQN
 - e Le champ SEQN
 - f Le champ HEC
 - g Le FCE
- - 4 Définition des champs de PAYLOAD

- 1 Les champs principaux

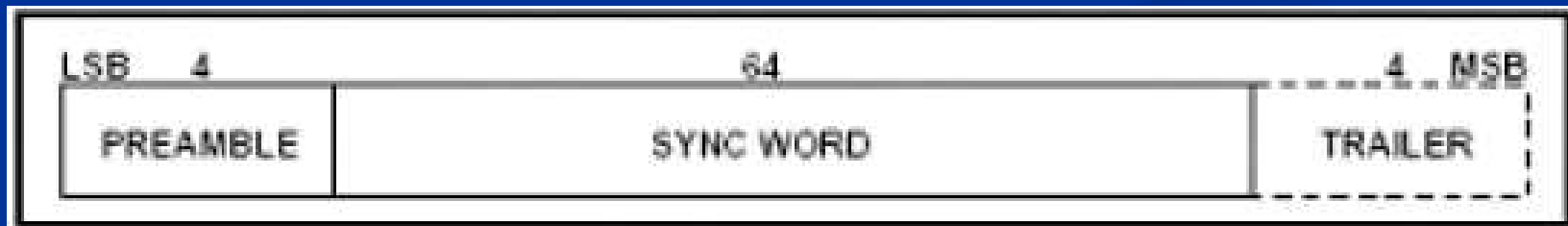
- Une trame de message bluetooth à 3 champs principaux
 - Le champ code d'accès (Access code), 68 ou 72 bits.
Son rôle est de synchroniser, compenser et identifier.
 - Le champ En-tête (Header), 54 bits,
Il code les informations de contrôle (Ex : l'adresse du destinataire, le type de message...).
 - Le Corps du message (Payload), de 0 à 2745 bits, il s'agit des données à transmettre.



- 2 Définition des champs d'Access code :

- Access code est composé de trois champs.

Les trois champs ne sont pas forcément présent, tout dépend du type de code d'accès



- a Les types de code d'accès :

- Il en existe trois:

- Le CAC : code d'accès du canal.

- Définit le type de réseau bluetooth (le piconet).

- Il possède les trois champs (preamble, sync word et trailer).

- Le DAC : code d'accès du dispositif.

- Utilisé dans certaine procédure de réveil (ex : le mode « parked »).

- Il possède deux champs(pas de champ trailer)

- L'IAC : code d'accès d'inquiry.

Utilisé par un composant bluetooth pour rechercher un autre composant bluetooth à portée.

Il possède deux champ(pas de champs trailer).

- b Le champ preamble :

- Ce champ ne peut prendre que deux valeurs 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)
- 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) dépend du type de code d'accès.

- Voici un tableau qui définit qu'elle LAP utilisée en fonction du type de code d'accès.
- Pour l'IAC des adresses dédiées sont utilisées.

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

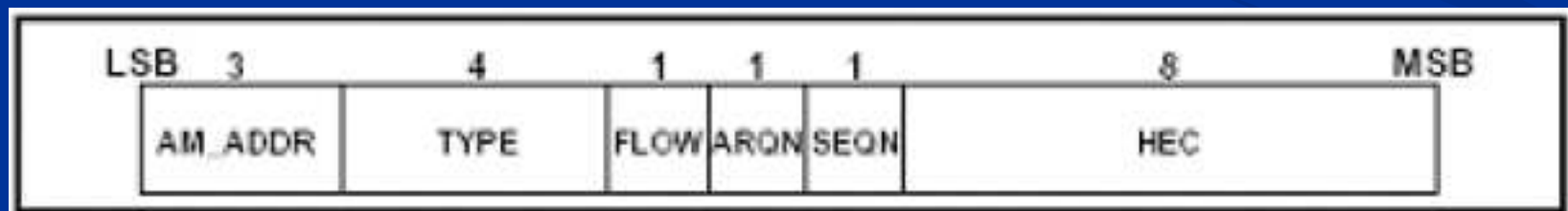
- d Le champ Trailer :

- Idem 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:
 - Am_addr
 - Type
 - Flow
 - Arqn
 - Seqn
 - Hec



- 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 (synchrone ou asynchrone).

- c Le champ FLOW (1 bit) :

- Il contrôle 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) :

- Bit d'acquittement 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 a déjà reçu mais qui n'a pas été acquitté.

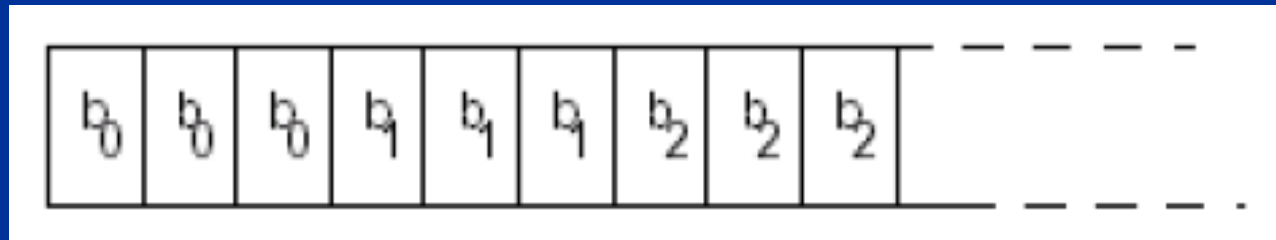
- f Le champ HEC (8 bits) :

- Header error check.
- Il contrôle les erreurs de l'entête.

- Le champ header comprend 18 bits.
 - $3 \text{ Am_Addr} + 4 \text{ type} + 1 \text{ Flow} + 1 \text{ Arqn} + 1 \text{ Seqn} + 8 \text{ Hec} = 18$ bits
- Il est protégé par un codage FCE (1/3 FCE pour être plus précis).
- Le champ header a donc une taille de 54 bits.

- g Le FCE :

- FCE signifie forward correcting error,
 - Protection qui écrit des informations redondante dans le corps des paquets.
- Le 1/3 FCE contient trois la même information.



- Donc les 18 bits du champs header sont écrits 3 fois.
($3 \times 18 = 54$ bits)

- 4 Définition des champs de PAYLOAD :

- Le champ PAYLOAD dépend de 4 paramètres.
 - Type de liaison : liaison synchrone ou asynchrone.
 - Type de message : Il s'agit des informations donné dans le HEADER.
 - Application d'un codage correcteur d'erreur (EX : le 1/3 FCE).
 - Présence d'un CRC : cyclic redundancy check. Le CRC permet de détecter les erreurs et de demander une retransmission.

- En général, on retrouve deux types de champ :
 - Le champ Data Field (données)
 - Le champ Voice Field (voix).
- Un message en mode synchrone ne possède que le champ voix
- un message en mode asynchrone ne possède que le champ données.
- Mais certain type de message possède les deux champs.

VI) Création d'une connexion 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 ".

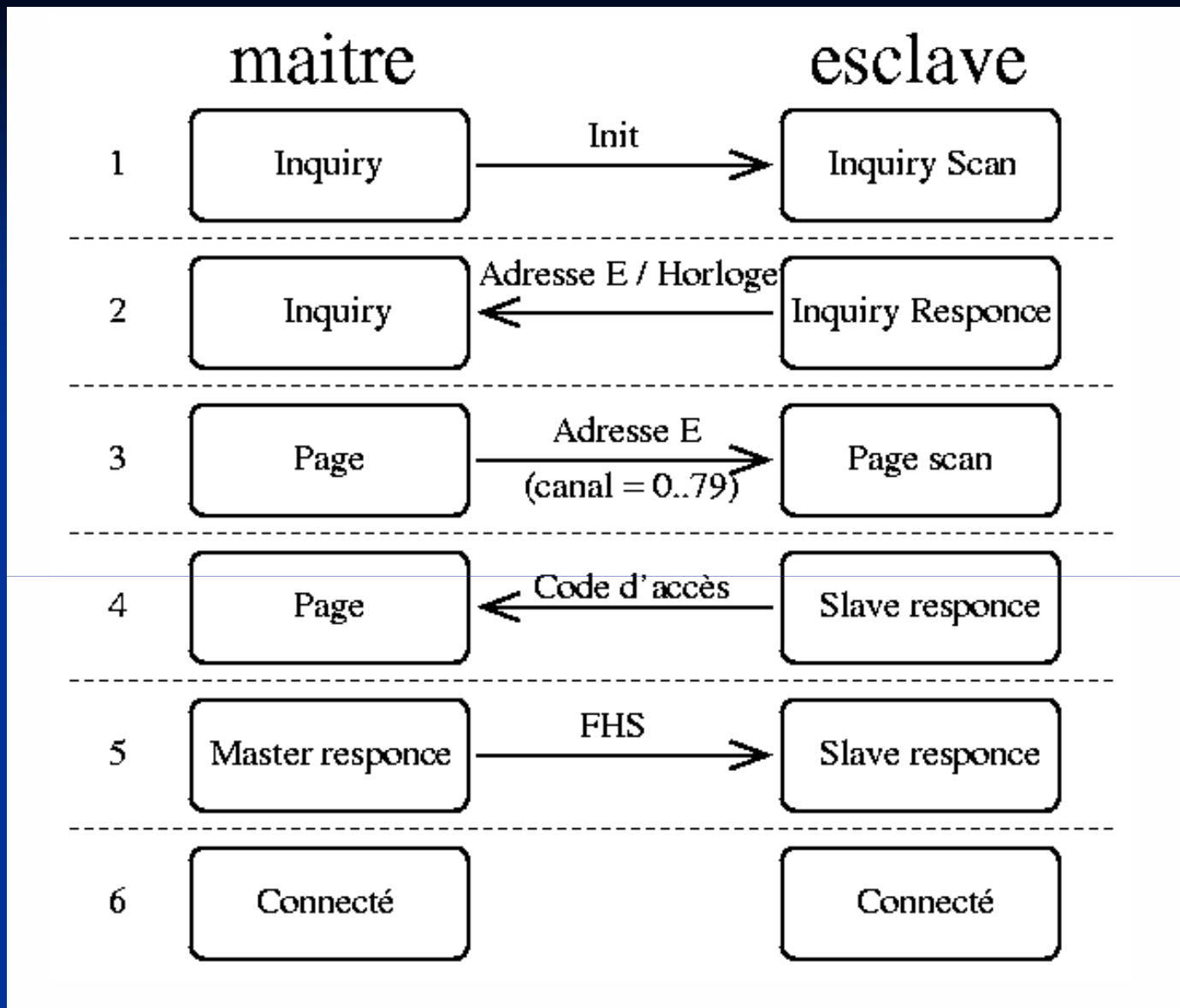


Schéma d'une connexion entre deux périphériques bluetooth

- 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".
- 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.

- Une fois que E a envoyé sa réponse, il passe dans l'état " Page Scan ". Ensuite il attend un message avec sa propre adresse. Lorsque M reçoit le message réponse de E, celui-ci passe dans l'état " page ". C'est à dire qu'il stocke les informations reçus (pagination). Ces informations permettent à M d'avoir conscience de la présence de E. Lorsque M veut poursuivre le processus de connexion, celui-ci renvoie un message réponse en y plaçant l'adresse de E.
- 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 avec son code d'accès.

- De son côté, M une fois ce code d'accès récupéré, se place alors dans un état " Master response " et renvoie un paquet FHS à E. Ce paquet de type FHS (Frequency Hopping Synchronisation) permet à E de se synchroniser avec M.
- 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".

- 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

- - 1 Le couplage
- - 2 Comment se passe l'authentification
- - 3 Les différentes attaques
 - a Bluejacking
 - b Bluesnarfing
 - c Bluebug
 - d Bluesmacking

- 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.

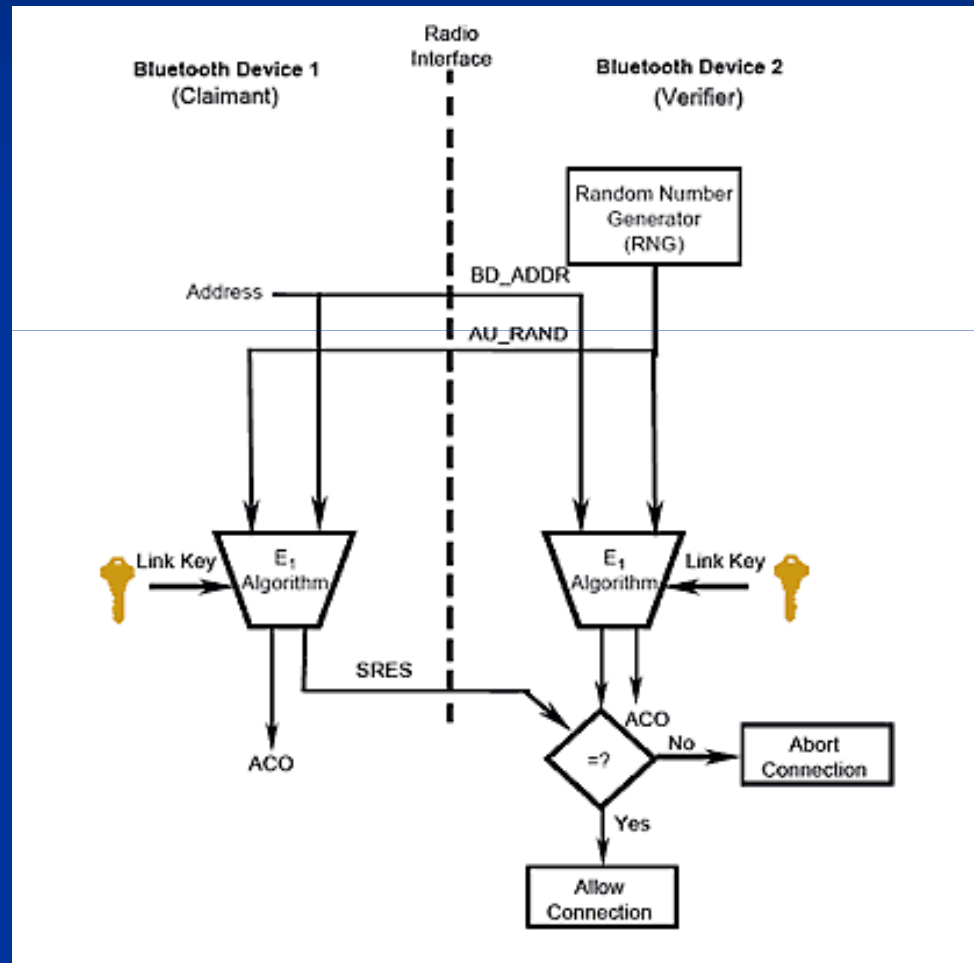
- Le mode de sécurité 3 permet d'établir une connexion avec authentification et chiffrement au moyen d'une clé.
- Le mode de sécurité 2 permet de sécuriser de façon logicielle le dispositif bluetooth. Il nécessite une authentification.
- Le mode de sécurité 1 permet à un appareil bluetooth d'offrir ses services à tous dispositifs bluetooth à portée. Ce mode peut être comparé à un hotspot wifi public.

- 1 Le couplage :

- Par défaut, il n'y a pas d'authentification. N'importe quel périphérique peut parler avec n'importe quel autre périphérique.
- Une authentification peut être demandée pour fournir un service particulier. L'authentification Bluetooth est généralement effectuée avec des codes PIN (une chaîne ASCII)
- Le même code PIN doit être introduit sur les deux périphériques.

- Une fois le code introduit, les deux périphériques génèrent une clé de liaison (link key). 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, l'opération de couplage doit être répétée.

- 2 Comment se passe l'authentification ?:



- L'appareil qui initie la connexion envoie son adresse (BD_ADDR).
- La séquence aléatoire de 128 chiffres AU RAND (challenge) est envoyée en réponse.
- Sur la base de BD_ADDR, de la clé de combinaison et d'AU-RAND, les deux appareils génèrent la séquence de cryptage SRES.
- L'appareil qui demande la connexion envoie son SRES.
- L'appareil contacté compare le SRES reçu et le sien et s'ils correspondent, il établit la connexion.

- 3 Les différentes attaques :

- De puis l'apparition du bluetooth plusieurs types d'attaques ont été recensés.

- Les plus courantes sont:
 - Bluejacking
 - Bluesnarfing
 - BlueBug
 - BlueSmack

- a Bluejacking :

- Il s'agit de spamming, On détourne l'utilisation principale du 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 l'équipement bluetooth est équipé du 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 la faille la plus lourde de conséquences pour une victime.
- 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.



- 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
- - 2 Utile
- - 3 Inutile

- 1 Les composants Bluetooth

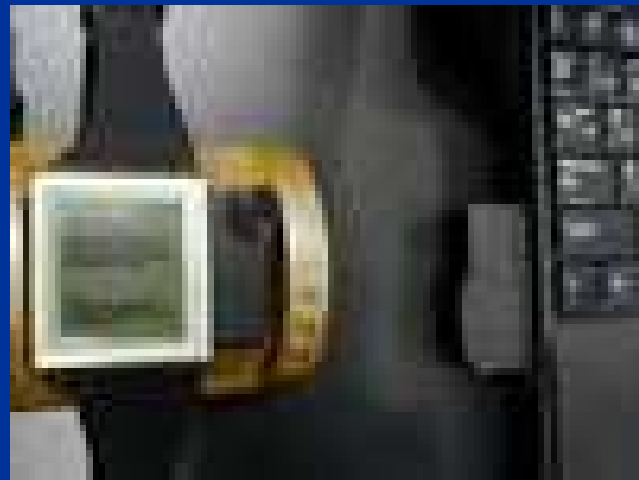
- Cette carte permet de connecter un ordinateur portable à un réseau bluetooth



- L'info stick de Sony:
 - Poids:4g
 - Dimension de 21.5 * 55 * 2.8 mm
 - se connecte sur les PDA et les appareils photo.
- Elle permet de se connecter à Internet sur un PDA
- De rapatrier ses photos numériques sur une unité de stockage plus importante que la mémoire de l'appareil photo.



- 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.



- Modem bluetooth qui permet de connecter un PC à Internet même s'il se trouve éloigné d'une prise téléphonique.

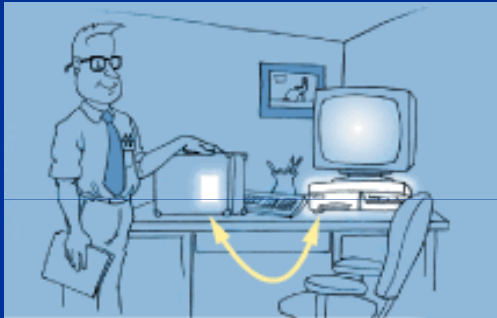


- Des adaptateurs bluetooth pour les imprimantes lasers. L'adaptateur vient se connecter au port parallèle de l'imprimante et communique par ondes radio avec un point d'accès lui-même connecté.



- 2 Utile

- En rentrant chez vous, votre PDA se synchronise avec votre ordinateur, transfère vos fichiers et vos e-mails.



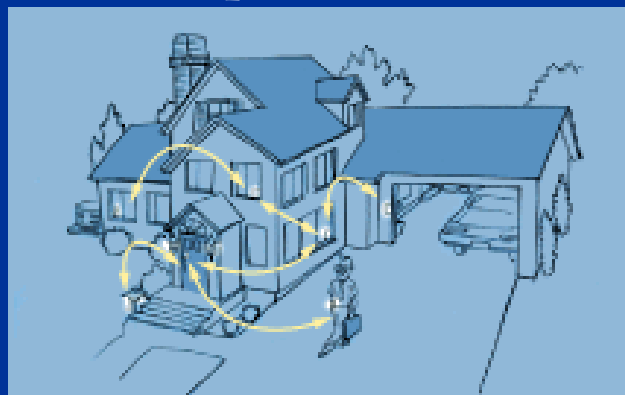
- Envoyez votre présentation (stocké sur votre PDA) sur le projecteur que vous pilotez à distance grâce à votre PDA. A la fin de la réunion, vous transférez cette présentation



- En 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.



- A l'aéroport, plus 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.



- En entrant dans un parc, une carte du parc est envoyée à votre voiture qui l'affiche sur un écran.



- 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.





- 3 Inutile

- Bluespoot :
 - Il 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.
 - C'est de la 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.
 - Prévues pour la fin 2007, sa sortie a 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
 - Son nom sera probablement UWB (Ultra Wideband Bluetooth).
 - Débit équivalant 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.

- Le nouveau protocole n'utilisera plus la bande des fréquences de 2,4 GHz. Il exploitera celle au dessus des 6 GHz.
- Les produits équipés de la norme: caméscopes, téléviseurs et aux appareils photo...
- 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

- 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 secteur que la téléphonie notamment grâce à la sortie de la norme 3.0 qui permettra des transferts de donnée très rapide.

Fin