Bluetooth Low energy

Le protocole a ete designé par Nokia et d'autres entreprises pour repondre au besoin d'un protocole sans fil peu gourmand en energie pour les peripheriques personnels (telephone portable, montre, casque). Nommé Wibree, il a ete integre au standard Bluetooth sous le nom *Low Energy*.
Le Bluetooth ne comprend pas seulement un protocole mais une multitude d'entre eux (BR, EDR, HS) qui ont en commun de permettre la communication (et l'echange de donnees) sans fil avec des peripheriques personnels. Ils font partit des protocoles WPAN (reseau personnel sans fil) et leur distance d'emission est de quelques metres jusqu'a 30 metres.
La specification Bluetooth 4.0, sortie en 2011, integre le protocole LE (Low Energy) et permet au Bluetooth de touché le marché des systemes embarques, fonctionnants sur batterie.

Différences

Les autres protocoles du Bluetooth sont principalement connus et utilises pour le transfert de contenu multimédia, que ce soit des fichiers entre ordinateurs comme de la musique avec un casque ou encore une voiture. Ils fonctionnement avec une connexion continue et un transfert en flux.

Le BLE, visant a reduire la consommation d'energie, n'etablie pas de connexion continue. L'appareil reste la plupart du temps en mode veille, pouvant emettre des annonces, dans l'attente d'une connexion qui aura pour effet d'arreter la transmission d'annonce. Pour chaque requete recu, une reponse pourra etre renvoyee directement ou une notification mise en place periodiquement.

Les appareils BLE et Bluetooth BR/EDR ne sont pas compatibles, n'utilisant pas les memes technologies, protocoles et repondant a des besoin differents (voir tbl. 1).

Table 1: Cas d'utilisation et protocole Bluetooth adapté

Besoin	Flux données	Transmisson données	Localisation	Reseau capteurs
Appareils	ordinateur, smartphone, casque, enceinte, voiture	accessoires bureautique ou fitness, equipement medical	beacon, IPS, inventaire	automatisation, surveillance, domotique
Topologie	point à point	point à point	diffusion (1 à N)	mesh (N à N)
Technologie	Bluetooth BR/EDR	Bluetooth LE	Bluetooth LE	Bluetooth LE

Protocole

Pour permettre une interoperabilité maximale entre les appareils BLE, le standard defini 4 profiles en fonction du role de l'appareil: Peripheral, Central, Broadcaster, Observer. Ces roles constituent le *GAP* (*Generic Access Profile*).
Chaque appareil se conformant au standard ne doit implementer qu'un seul de ces roles a la fois.

Le *Broadcaster* ne communique qu'avec des annonces, on ne peut pas s'y connecter. Ce mode est tres populaire pour les beacons. L'*Observer* est sont opposé, il ne fait qu'ecouter les annonces, n'etabliera jamais de connexion.

Le *Peripheral* et le *Central* forment la seconde pair et permettent la mise en place d'une architecture

client-serveur. Le *Peripheral* joue le role du serveur et est dit *esclave* du *Central* qui endosse le rôle du client et *maître*.
L'esclave transmet des annonces jusqu'a recevoir une connexion d'un maitre, apres quoi il arrete de s'annoncer car il ne peut etre connecté qu'a un maitre a la fois. Le maitre ecoute les annonces d'esclave (annonces connectables) pour se connecter, puis interroge ses services via le *GATT* (*Generic Attribute*).

Couche physique

Le BLE opère dans la bande ISM 2.4GHz tout comme le Wi-Fi. Contrairement aux canaux Wi-Fi de 20MHz, le BLE découpe le spectre en 40 canaux de de 2MHz (plage de 2400 à 2480MHz).
Le protocole met en place le *saut de fréquence*, consistant à changer de canal d'émission tout les laps de temps donné, pour réduire le risque de bruit sur les fréquences utilisées (la bande ISM 2.4Ghz étant libre d'utilisation).
Sur les 40 canaux que compose le spectre, 3 sont utilisés pour la transmission d'annonce. Ils sont choisit pour ne pas interferer avec les canaux Wi-Fi car les deux protocoles sont amenés à coexister (voir fig. 1).
Les 37 autres canaux permettent le saut de fréquence lors de la transmission de données.

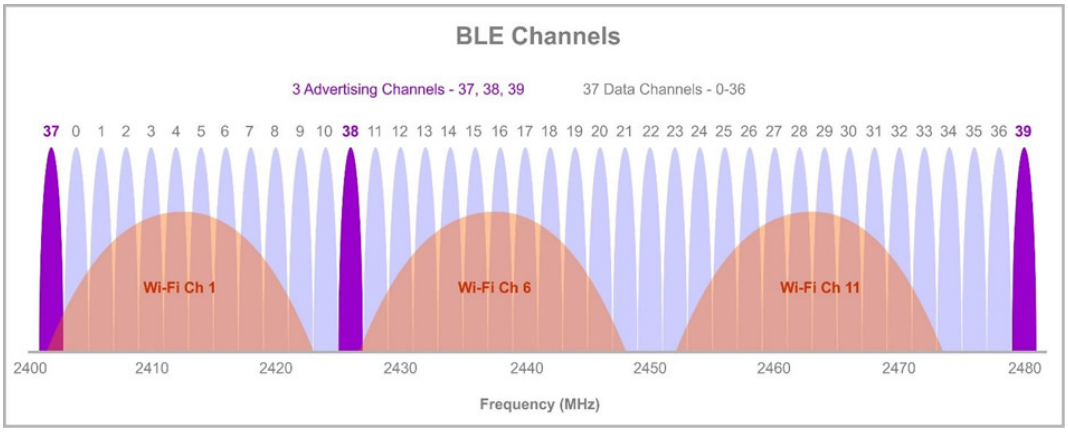

Figure 1: Répartition du spectre BLE en canaux[1]

Couche logique

Scenario client-serveur maitre-esclave central-peripheral avec connexion (pas beacons)

1. Annonces L'esclave indique sa présence avec des annonces émises périodiquement. Ces annonces contiennent sont addresse Bluetooth (permettant une connexion) et des données qui consituent un profile (appelé *GAP*[2]). Ces données permettent aux maîtres de savoir si il est capable de realiser les fonctionnalités recherchées.
La specification Bluetooth definit des profiles type pour des applications communes dans les appareils BLE[3]. Cela inclus par exemple les capteurs corporels pour le sport, les capteurs médicaux de surveillance (pour les diabetiques notamment), la domotique (termometres, lampes), etc.

Dans un environnement BLE, les maîtres ne peuvent pas reconnaitre leurs esclaves a part avec une addresse Bluetooth fixe, mecanisme de moins ne moins utilisé car vulnérable a l'usurpation. Les esclave generent donc des addresses aleatoires et l'identification se fait via les donnees du *GAP* contenues

[1] https://www.accton.com/Technology-Brief/ble-beacons-and-location-based-services/
[2] https://www.bluetooth.com/specifications/assigned-numbers/generic-access-profile/
[3] https://www.bluetooth.com/specifications/gatt/services/

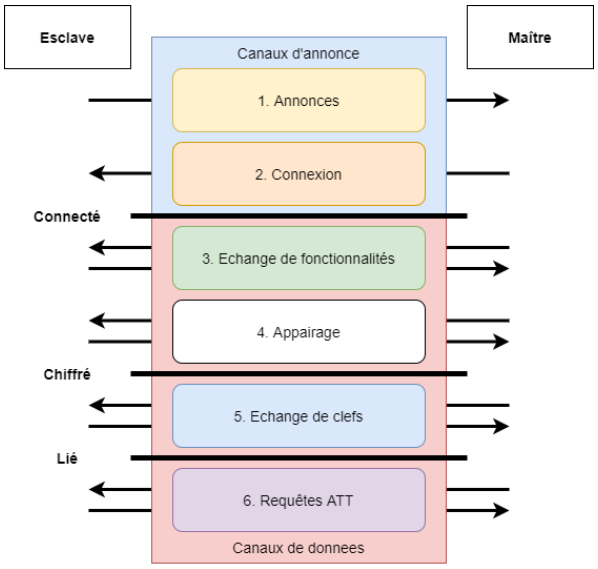

Figure 2: Étapes d'un échange BLE

dans l'annonce. Ce mecanisme permet a n'importe quel maitre de s'appairer a n'importe quel esclave proposant le profil recherché.
Par exemple, une application de smartphone BLE pouvant gerer la temperature pourrait s'appairer et utiliser n'importe quel appareil BLE qui implemente le profil standardisé pour les termometres dans le *GAP*.
Les profils ne sont certes pas exhaustifs mais permettent une integration fonctionnelle avec un maximum d'appreils et prévoient un moyen d'integrer des donnees proprietaires non standardisées[4].

2. Connexion

3. Capacités

Table 2: Capacités d'entrée possibles[5]

Capacité	Description
No input	pas la capacité d'indiquer *oui* ou *non*
Yes/No	mécanisme permettant d'indiquer *oui* ou *non*
Keyboard	claver numérique avec mécanisme *oui*/*non*

Table 3: Capacités de sortie possible

Capacité	Description
No output	pas la capacité de communiquer ou afficher un nombre
Numeric Output	peut communiquer ou afficher un nombre

Table 4: Capacité d'entrées/sorties de l'appareil

	No output	Numeric output
No input	NoInputNoOutput	DisplayOnly
Yes/No	NoInputNoOutput	DisplayYesNo
Keyboard	KeyboardOnly	KeyboardDisplay

On ne s'interesse qu'a JustWorks car tres utilisee dans les appareils *smart* car simples.
La comparaison numerique (NumComp) a ete introduit avec les connexions BLE securisees (LE pairing). Passkey et Numcomp permettent d'authentifier l'autre appareil car partageant un secret via un autre canal.
JustWorks ne permet pas d'authentifier les appareils et le chiffrement est moins robuste que les autres methodes mais permet tout de meme d'etablir une communication chiffree.

5. Session

6. Requêtes ATT

Communication

GAP Les beacons utilisent le GAP pour communiquer car ils n'etablissent pas de connexion point a point mais diffusent la meme information.

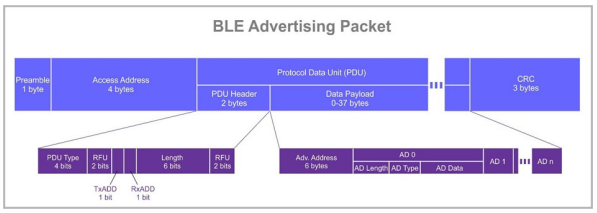

Figure 3: Structure d'une annonce[7]

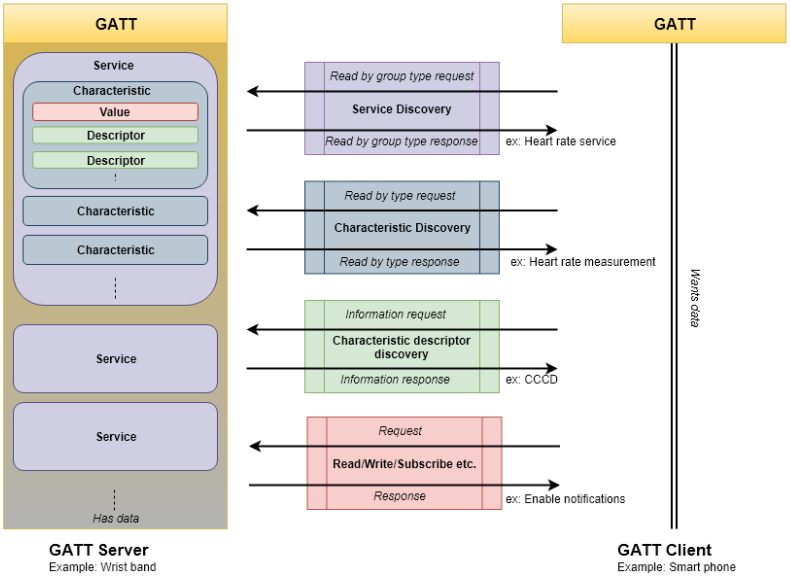

Figure 4: Client et serveur GATT[8]

[6]https://www.bluetooth.com/blog/bluetooth-pairing-part-2-key-generation-methods/
[7]https://www.accton.com/Technology-Brief/ble-beacons-and-location-based-services/

GATT GATT & ATT proto https://fr.mathworks.com/help/comm/examples/modeling-of-ble-devices-with-heart-rate-profile.html

interop via profiles (API commune) -> GATT protocole

All Bluetooth Low Energy devices use the Generic Attribute Profile (GATT). The application programming interface offered by a Bluetooth Low Energy aware operating system will typically be based around GATT concepts.[44] GATT has the following terminology:

Client A device that initiates GATT commands and requests, and accepts responses, for example, a computer or smartphone. Server A device that receives GATT commands and requests, and returns responses, for example, a temperature sensor. Characteristic A data value transferred between client and server, for example, the current battery voltage. Service A collection of related characteristics, which operate together to perform a particular function. For instance, the Health Thermometer service includes characteristics for a temperature measurement value, and a time interval between measurements. Descriptor A descriptor provides additional information about a characteristic. For instance, a temperature value characteristic may have an indication of its units (e.g. Celsius), and the maximum and minimum values which the sensor can measure. Descriptors are optional – each characteristic can have any number of descriptors.

fonctionnement apparaige (phases)

Versions

4.0 arrivee BLE Version visee par le PoC

4.2

5.1

specification du Bt pour les systemes embarques, bcp utilise dans objets connectes

4.0 arrivee

4.2 securite

5.0 mesh networks for home automation or sensor networks use bluetooth mesh profile General Access Profile (GAP)

5.1 localisation

Utilisation “abusive” dans les objets connectes ?

[8] https://fr.mathworks.com/help/comm/examples/modeling-of-ble-devices-with-heart-rate-profile.html