INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

BLUETOOTH LOW ENERGY (BLE)

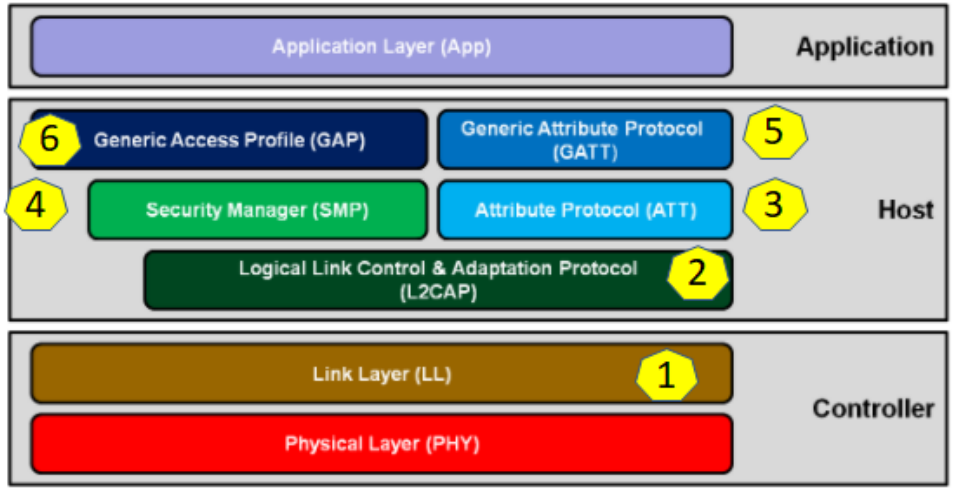
INNOVATIVE SMART SYSTEMS

SKIKER HICHAM

Planning

1. Physical Layer
2. MAC Layer
3. Power consumption
4. Security

Link Layer



FUNCTIONS

6 Definition of interaction between devices

5 Exchange of data between applications

4 Generation & exchange of security keys

3 Client/server protocol based on shared attributes

2 Transport of data

1 Addressing + communication

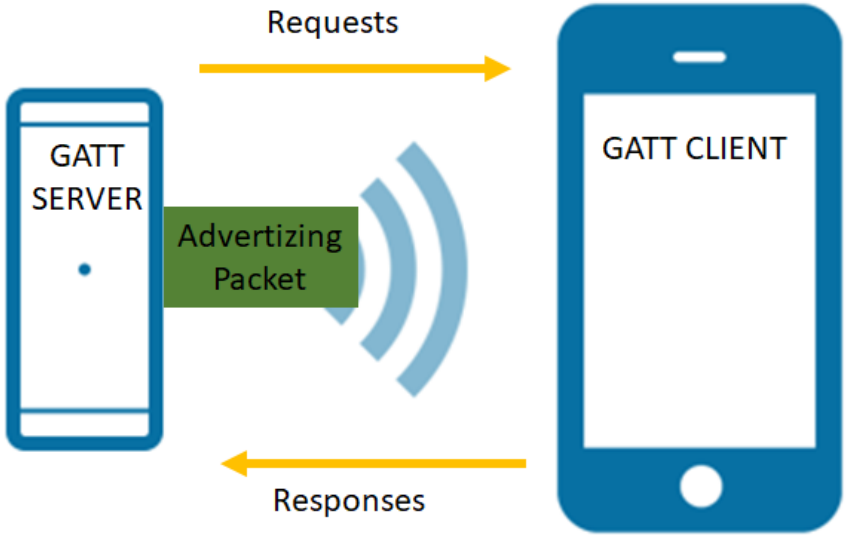
Connection

GAP role

L2CAP

Link Layer

Connectable?
Scannable?
Directed?



Active scan?
Passive scan?

SLAVE

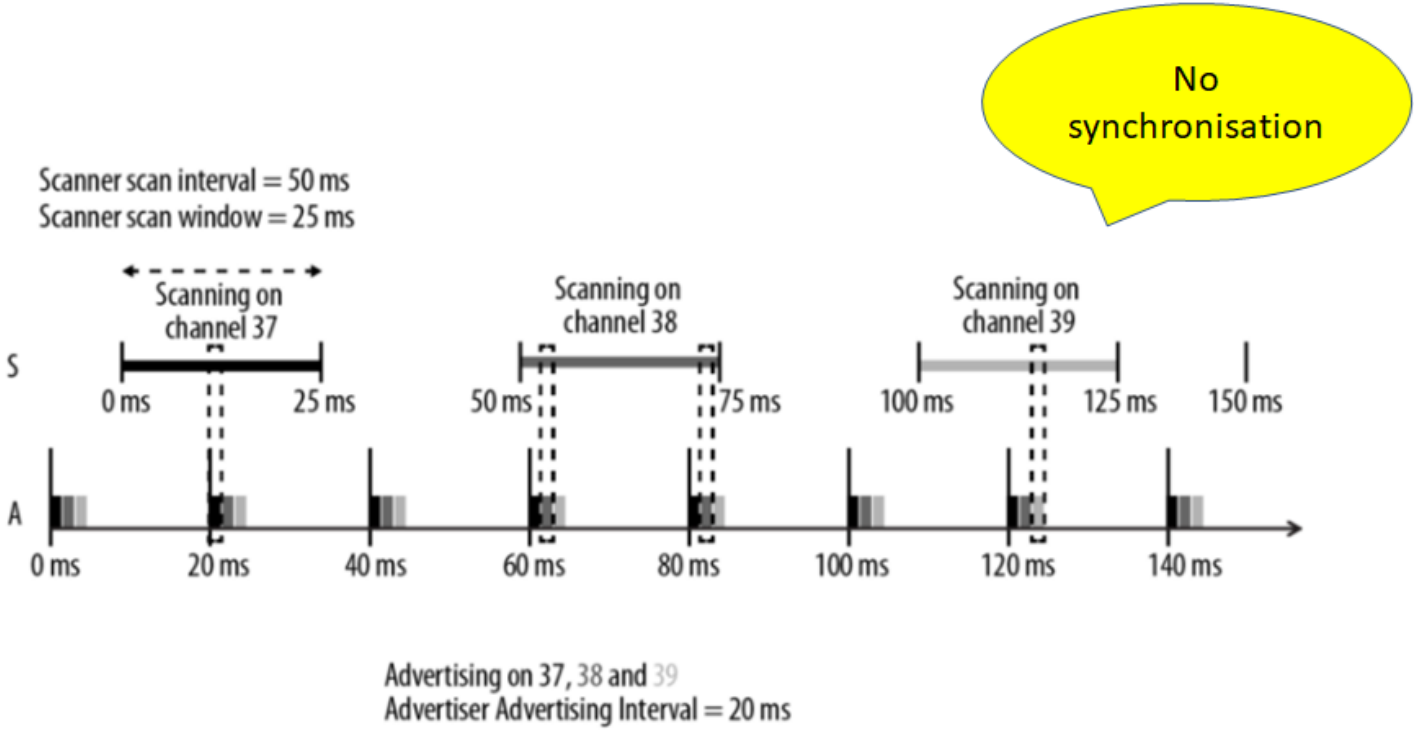
C8:6E:1D:1E:96:2E

MASTER

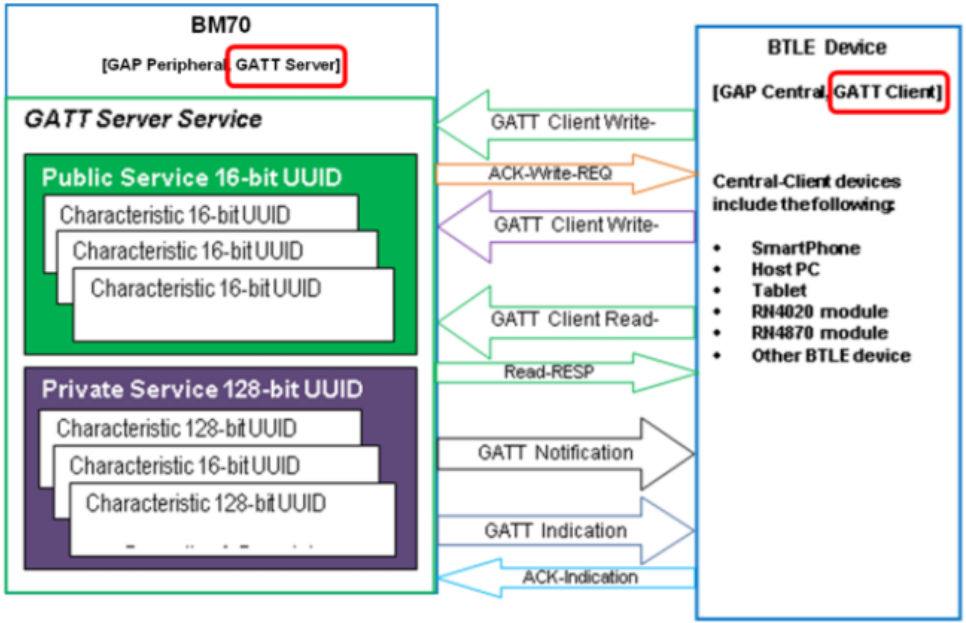
XX:XX:XX:XX:XX

Central/Observer

Synchronisation



Generic Attributes Protocol

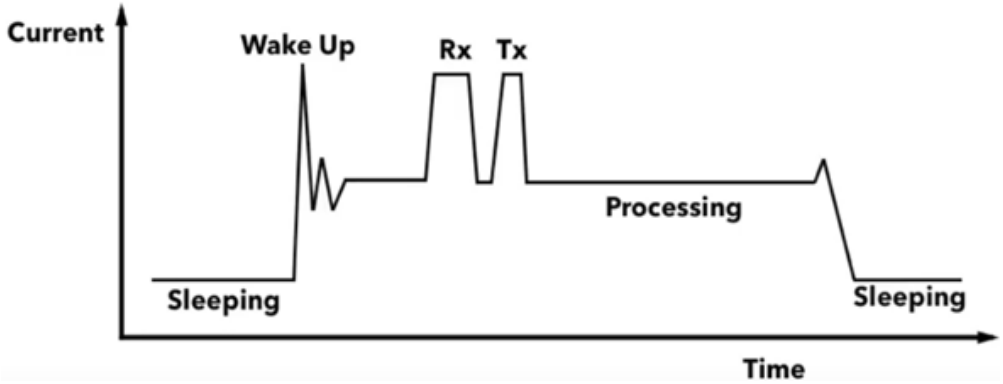


BLE Consumption

It’s not straightforward to predict the exact BLE power consumption due to the several parameter depending on. BLE consumption depend on:

- Chipset/radio
- BLE Stack + version
- BLE parameters
- Firmware efficiency

Current Consumption Draw during a cycle



Awaking Mode Consumption

We can define the overall energy consumption during an awaking mode as a the sum of different energy consumption states: E_awake= E_(wake-up)+ E_rx+ E_tx+ E_Processing+ E_IFS

- Wake-up energy
- RX energy (mainly depends on the data number to receive)
- IFS energy
- TX energy (mainly depends on the data to send and the transmit power used)
- Post-processing energy (mainly depends on the application running)

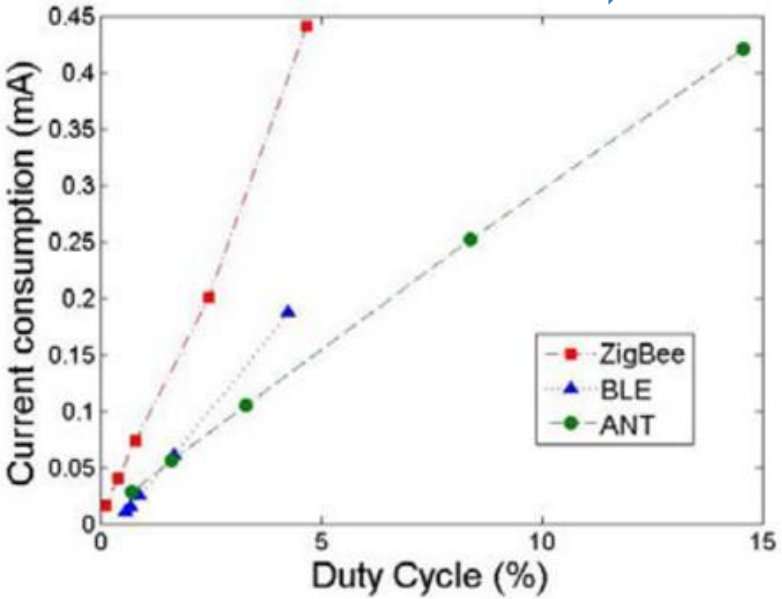
Phase	Power draw ($V_{DD} = 3$V)	Duration
1. wakeup & pre-processing	$P_{wu} = 15$mW	$D_{wu} = 1$ms
2. RX	$P_{rx} = 66$mW	$D_{rx} = 8\mu$s/B
3. IFS	$P_{ifs} = 45$mW	$D_{ifs} = 150\mu$s
4. TX	$P_{tx} = 84$mW	$D_{tx} = 8\mu$s/B
5. post-processing	$P_{mcu} = 24$mW	$D_{mcu} = 1.4$ms

Sleeping Mode Consumption

Sleeping mode is useful for saving energy when the BLE device didn’t send any data. In order to save energy, consumption is very low (2 µW) in this mode. An engineer which is looking for increase a BLE device autonomy, will handle to reduce the duty cycle, in order to maximize the time spent in this mode.

Indeed, overall BLE consumption which is working in cycling mode, is represented as below:

E_ble = E_awake + E_Sleep



Mean current consumption related to the duty cycle

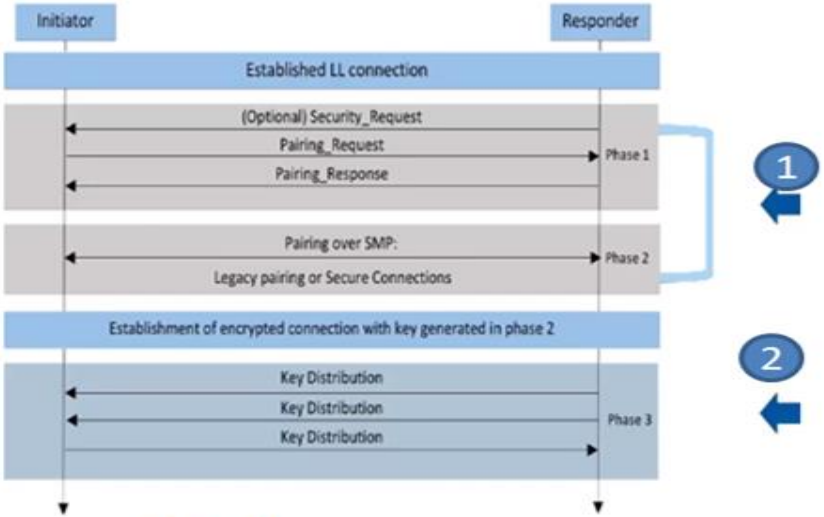
BLE modele de securité

- Pairing: 1

  Processus de création de clés partagées / sécurité temporaire / connexion cryptée .

- Bonding: 2

  Stockage de la clé créée lors du couplage pour une utilisation ultérieure .



1-Concevoir l'authentification:

Vérification des clés stockées .

2-Confidentialité :

Les données ne sont pas lisibles par d'autres utilisateurs .

3-Intégrité : Protection contre l'altération des données .

Sécurité Manager

Sécurité Manager est un module de l'achitecture BLE :

- ❖Protocole et algorithme .
- ❖Génération et échange clés .
- ❖128 Bit de de crypte selon [Standard Avancé de criptage (AES)]

- ❖Maitre initialise la sécurité .
- ❖Esclave peut demander la sécurité

- ❖Garantissez la confiance, l'intégrité, la confidentialité et le cryptage des données.
- ❖Responsable de la sécurité
- ❖Responsable de:

-Pairing
-Distribution des clés .
-Générer des clés à court terme .