Bluetooth

IUT Béziers, dépt. R&T © 2009 - 2017
http://www.borelly.net/
cb@iutbeziers.fr

Généralités

- Protocole sans fil développé en 1994 chez Ericsson.
- Formalisé en 1998 par le Bluetooth SIG (Special Interest Group) : IEEE 802.15.1
- Transmission sur courtes distances (10-100m)
- Conçu initialement comme une alternative aux câbles RS232
- Possibilité de connexions multiples
- Faible coût, faible consommation électrique

Versions 1

- Bluetooth 1.1 : 802.15.1-2002
  - Gaussian Frequency Shift Keying (GFSK)
  - Received Signal Strength Indicator (RSSI)
- Bluetooth 1.2 : 802.15.1-2005
  - Adaptive frequency-hopping (AFH)
  - Débit jusqu'à 721 Kbps
  - Extended Synchronous Connections (eSCO)
  - Host Controller Interface (HCI) pour 3 UART (Universal Asynchronous Receiver/Transmitter)

Versions 2 et 3

- Bluetooth 2.0 : Nov. 2004
  - Enhanced Data Rate (EDR) : jusqu'à 3 Mbps
  - π/4-DQPSK (2 Mbps) et 8DPSK (3 Mbps)
- Bluetooth 2.1 : Juil. 2007
  - Secure Simple Pairing (SSP)
  - Near Field Communication (NFC)
- Bluetooth 3.0 : Nov. 2009
  - High Speed (HS) : jusqu'à 24 Mbps
  - AMP (Alternative MAC/PHY) – 802.11

Versions suivantes

- Bluetooth 4.0 : 2010 (Low Energy)
  - Incompatible avec les versions précédentes !
  - Chiffrement AES
  - GATT (Generic Attribute Profile)
- Bluetooth 4.1 : 2013
- Bluetooth 4.2 : 2014
- Bluetooth 5.0 : 2016 : jusqu'à 50 Mbps

Appairage

- Legacy pairing (avant 2.1)
  - Utilisation d'un code **PIN** (jusqu'à 16 caractères)
- Secure Simple Pairing (SSP)
  - Just works : pas d'interactions !
  - Numeric comparison : comparaison d'un nombre de 6 chiffres sur les 2 équipements.
  - Passkey Entry : Un code est affiché sur un dispositif est doit être entré sur l'autre.
  - Out of band (OOB) : Echange d'informations par un autre média (ex. NFC) pendant l'appairage.

Particularités radio

- Utilisation de la bande ISM à 2.4 GHz (Industrial, Scientific, and Medical)
- Technologie **FHSS** (frequency-hopping spread spectrum)
- Transmissions synchrones (**SCO** - Synchronous Connection-Oriented)
- Transmissions asynchrones (**ACL** - Asynchronous Connection-Less)

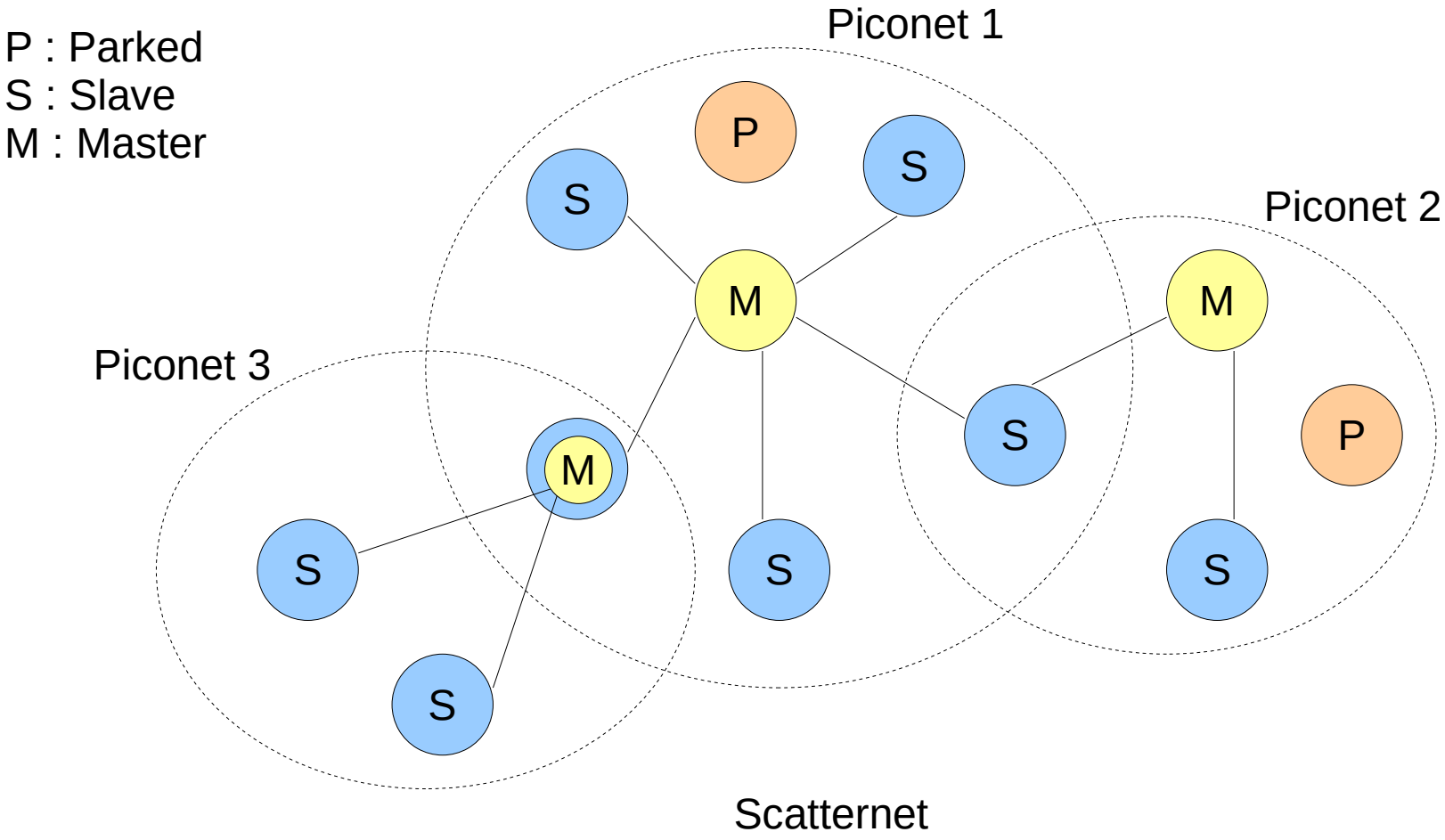
Particularités radio

- Classic : BR/EDR
  - 79 canaux (1 MHz), 1600 sauts/s
  - 2402+k MHz avec k=0, ..., 78
- BLE (Low Energy) : v4.0
  - 40 canaux (2 MHz), 1600 sauts/s
  - 2402+2.k MHz avec k=0, ..., 39

Topologies réseau

- Un piconet est un réseau dynamique (ad-hoc) de 2 à 8 équipements actifs (jusqu'à 255 équipements inactifs ou « parkés »).
  - Le « Maitre » détermine la séquence des sauts de fréquence.
  - Il y a 7 « Esclaves » actifs au maximum.
- Un scatternet est l'association de plusieurs piconets.
  - Un équipement ne peut-être « Maitre » que dans un seul piconet.
  - Les autres combinaisons sont possibles.

Exemple


P : Parked
S : Slave
M : Master
Piconet 1
Piconet 2
Piconet 3
P
S
S
M
M
S
P
M
S
S
S
S
Scatternet

Mise en place d'une connexion

- Chaque équipement possède une adresse HCI unique sur 48 bits.
- Un équipement peut (sur demande) donner les informations suivantes :
  - Nom, classe, liste des services, informations techniques...
- Certains équipement ont un fonctionnement exclusif et ne sont pas « visibles » si ils sont déjà utilisés.

Mise en place d'une connexion sécurisée

- La communication radio peut-être chiffrée ou non avec algorithme SAFER+ (Secure And Fast Encryption Routine).
- Après la mise en place de la clé MK (Master Key) grâce à l'algorithme E22, le chiffrement se base sur le système E0 utilisant des clés symétriques.

Piles Bluetooth sur LINUX

- BlueZ (Qualcomm – 2001)
  - http://www.bluez.org/
- Affix (Nokia – 2001)
  - http://affix.sourceforge.net/
- BlueDrekar (IBM – 2000)
  - http://www.alphaworks.ibm.com/tech/bluedrekar
- OpenBT (AXIS – 1999)
  - http://sourceforge.net/projects/openbt/

hciconfig

```
hciconfig
hci0:   Type: USB
        BD Address: 00:00:00:00:00:00 ACL MTU: 0:0 SCO MTU: 0:0
        DOWN
        RX bytes:0 acl:0 sco:0 events:0 errors:0
        TX bytes:0 acl:0 sco:0 commands:0 errors:0
hciconfig hci0 up
hciconfig -a
hci0:   Type: USB
        BD Address: 00:0A:94:F5:2E:36 ACL MTU: 384:8 SCO MTU: 64:8
        UP RUNNING
        RX bytes:85 acl:0 sco:0 events:9 errors:0
        TX bytes:30 acl:0 sco:0 commands:8 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy:
        Link mode: SLAVE ACCEPT
        Name: 'CSR - bc4'
        Class: 0x000000
        Service Classes: Unspecified
        Device Class: Miscellaneous,
        HCI Ver: 2.0 (0x3) HCI Rev: 0x6e6 LMP Ver: 2.0 (0x3) LMP Subver: 0x6e6
        Manufacturer: Cambridge Silicon Radio (10)
```

hcitool

```
hcitool scan
Scanning...
        00:18:C5:5A:33:11       Tim
        00:21:D2:23:12:A2       Max
        00:1A:8A:04:BE:11       SGH-D900
hcitool info 00:18:C5:5A:33:11
Requesting information ...
        BD Address:  00:18:C5:5A:33:11
        Device Name: Tim
        LMP Version: 2.0 (0x3) LMP Subversion: 0x6cc
        Manufacturer: Cambridge Silicon Radio (10)
        Features: 0xbf 0xee 0x0f 0xc6 0x9a 0x39 0x00 0x00
                <3-slot packets> <5-slot packets> <encryption> <slot offset>
                <timing accuracy> <role switch> <sniff mode> <RSSI>
                <channel quality> <SCO link> <HV3 packets> <u-law log>
                <A-law log> <CVSD> <paging scheme> <power control>
                <transparent SCO> <EDR ACL 2 Mbps> <EDR ACL 3 Mbps>
                <inquiry with RSSI> <extended SCO> <EV5 packets>
                <AFH cap. slave> <AFH class. slave> <3-slot EDR ACL>
                <5-slot EDR ACL> <AFH cap. master> <AFH class. master>
                <EDR eSCO 2 Mbps>
```

l2ping

```
l2ping 00:18:C5:5A:33:11
Ping: 00:18:C5:5A:33:11 from 00:0A:94:F5:2E:36 (data size 44) ...
5 bytes from 00:18:C5:5A:33:11 id 0 time 14.89ms
5 bytes from 00:18:C5:5A:33:11 id 1 time 51.01ms
5 bytes from 00:18:C5:5A:33:11 id 2 time 57.94ms
```

Références

- http://en.wikipedia.org/wiki/Bluetooth
- http://www.bluetooth.com/