إنترنت الأشياء - كهت ٤٠١٥

Internet of Things (IoT) - ELC4015

IoT Communication Technologies: Bluetooth Classic - Part 1

Dr. Mahmoud El-Hadidi

(mahmoud.hadidi@cu.edu.eg)

2024-10-09

Outline:

- Motivation for a New Wireless Technology
- Realization of the New Wireless Technology
- Bluetooth and Bluetooth Special Interest Group (SIG)
- Historical Evolution of Bluetooth
- Network Components & Topology
- Bluetooth Architecture & Protocol Stack
- Bluetooth Lower Layers: Bluetooth Radio
- Bluetooth Lower Layers: Baseband Controller

Professor Mahmoud El-Hadidi

Motivation for a New Wireless Technology [Wikipedia]

During the 1990's, efforts intensified to find a new wireless technology with the following requirements:

- Replacing serial cables by wireless links capable of connecting headsets to mobile phones, keyboard and mouse to PC's, printers to laptops, … , etc)
- Avoiding predefined infrastructure (such as routers in the case of wired LANs, or access points in the case of wireless LANs)
  ==> need Ad Hoc connectivity
- Covering distances < 100 m (typically < 10 m), which is adequate for expected applications
- Using license free spectrum to avoid high operational costs
  ==> use of Industrial Scientific Medical (ISM) spectrum

Professor Mahmoud El-Hadidi

Realization of the New Wireless Technology [Wikipedia]

To meet the stated requirements, following technical concepts were deployed:

- Using Frequency Hopping Spread Spectrum (FHSS)

  to combat interference from other systems operating in ISM (such as WiFi, ZigBee, Microwave Ovens, … , etc)

- Using Gaussian Frequency Shift Keying (GFSK) for baseband modulation:

  to increase spectral efficiency (compared with ASK, PSK)
  to overcome nonlinearity effects associated with amplifiers used in linear modulation schemes
  to reduce inter-symbol interference occurring with other pulse shaping techniques (such as Raised Cosine shaping)

Realization of the New Wireless Technology (Cont'd-1)

- Performing node discovery + service profile discovery + unattended connection establishment

  to achieve Ad Hoc connectivity between two neighboring nodes

- Deploying effective access control scheme

  to support multiple node operation

- Restricting network topology to be:
  - Star (for few # of nodes)
  - Tree (for larger # of nodes)

  to avoid the need for sophisticated routing algorithms (required in case of mesh topologies)

Bluetooth and Bluetooth Special Interest Group (SIG) [Wikipedia]

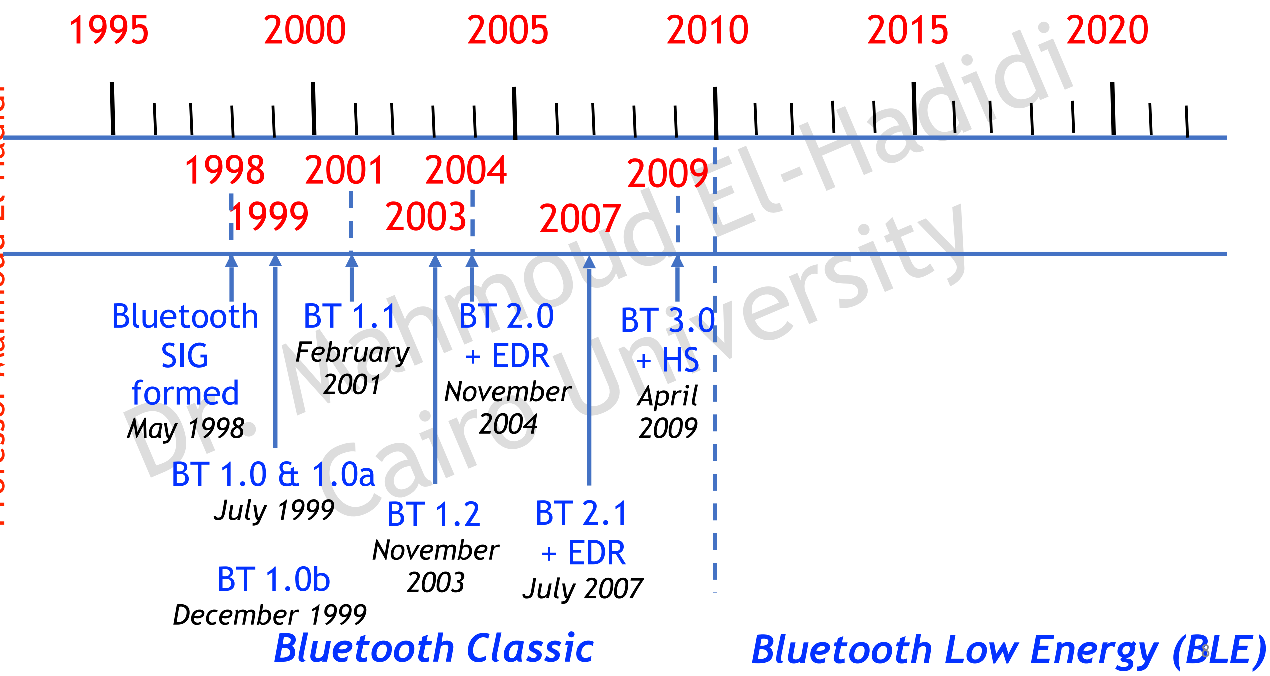
- LM Ericsson pioneered efforts for the new wireless technology since 1994 (being interested to connect its mobile phones with wireless headsets). It called the technology "Bluetooth" after the name of the Viking King (Harald "Blåtand" Gormsson) who united large parts of Denmark and Norway in the 10th century.
- Ericsson then invited IBM to join its efforts which was interested in connecting its "ThinkPad" laptop with peripherals (such as printers).
- Both were later joined by Intel, Nokia and Toshiba.Together, the FIVE companies formed the Bluetooth Special Interest Group (SIG) in 1998.

Bluetooth and Bluetooth Special Interest Group (SIG) [Gupta,2016](Cont'd-1)

- Goals of Bluetooth SIG are:
  - Publish Bluetooth ***specifications***
  - Administer the ***qualification program***
  - ***Evangelize*** Bluetooth wireless ***technology***
- Membership categories of Bluetooth SIG:
  - ***Adopter membership*** (Free): Provides access to Bluetooth resources and specifications to build Bluetooth products and license to use the Bluetooth word mark and logos
  - ***Associate membership*** (Annual fee): Provides early access to Bluetooth specifications which are still under development along with the opportunity to contribute to the specifications by joining working groups and committees. This membership also provides discounts on qualification fees, tools, trainings and more.

Naresh Gupta, Inside Bluetooth Low Energy, Artech House, 2016

Historical Evolution of Bluetooth [WikiPedia]



Historical Evolution of Bluetooth *(Cont'd-1)* [Gupta,2016]

Bluetooth Basic Rate (BR)

Specification Version	Release Date	Key features of the version
1.0 & 1.0a	Jul 1999	Very first versions of the Bluetooth specification. Primary objective was to replace the serial cables with a wireless link.
1.0b	Dec 1999	Added minor updates to fix some issues.
1.1	Feb 2001	Bluetooth was ratified as IEEE 802.15.1-2002 standard.
1.2	Nov 2003	Added new facilities including the following: • Adaptive Frequency Hopping (AFH) to provide better resistance to interference in noisy environments • Extended Synchronous Connection Oriented (eSCO) links to provide better voice quality. This was also ratified as IEEE 802.15.1-2005. *(This was the last version issued by IEEE and after that Bluetooth technology evolved independently.)*

Historical Evolution of Bluetooth *(Cont'd-1)* [Gupta,2016]

Bluetooth Enhanced Data Rate (EDR)

Bluetooth High Speed (HS)

Specification Version	Release Date	Key features of the version
2.0 + EDR	Nov 2004	Introduced enhancements to the throughput using Enhanced Data Rates (EDR). The previous versions of the standard supported a throughput up to 721 kbps. This version increased it to 2.1 Mbps.
2.1 + EDR	Jul 2007	Several enhancements & adding SSP (Secure Simple Pairing) to both simplify the pairing mechanism and to improve security.
3.0 + HS	Apr 2009	Significant increase in throughput by introducing the support for multiple radios. This was referred to as Alternate MAC/PHY (AMP). Supported maximum throughput went up to 24 Mbps. The rationale, very briefly, was that several devices like Laptops, Mobile phones and Tablets have both Bluetooth and 802.11 chips on them. This version of the specification allowed connection using Bluetooth and then moving on to the 802.11 chip to achieve high speed data transfers.

Bluetooth Network Components & Topology [Gupta, 2016]

Case of two nodes:

Step 1: Device B allows itself to be"seen" or discovered by other devices (is said to be ***discoverable***).

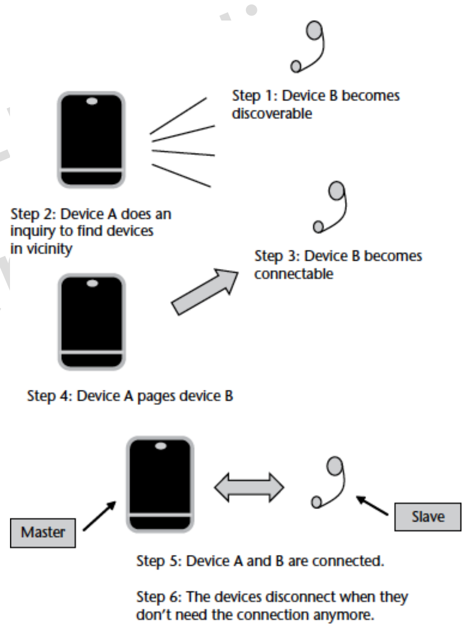
Step 2: Device A searches for devices in the vicinity (called ***"inquiry process"***), and it will locate device B (if it is in its coverage range).

Step 3: Device B allows other devices to connect to it (is said to be ***connectable***).

Step 4: Device A creates a connection to device B (called ***"paging process"***).

Step 5: With connection created, device A is said to become the Master and device B is said to become the Slave (***devices are said to be connected***).

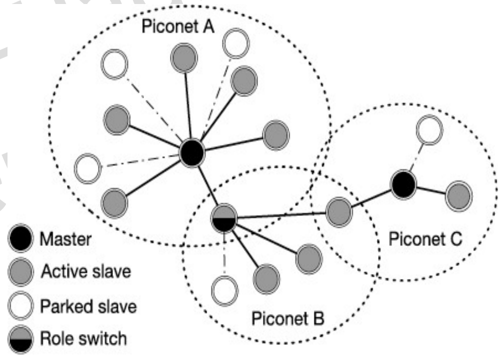
Step 6: When two devices don't need the connection any more, they ***disconnect*** (either the Master or the Slave can initiate the disconnection).



Network Components & Topology (Cont'd-1) [Nikoukar, 2018]

Case of multiple nodes:

- Nodes are grouped into "piconets" - which is a star topology - where communication is allowed with only one node (called "Master") and all other nodes are called "Slaves"
- Master node has built-in clock that synchronizes master-slaves communication
- Master node sends an *"inquiry"* message to a slave in order to identify "address" and "phase" information. *This enables the salve to compute the channel hopping sequence (when and on what channel to listen).*
- A slave can only "initiate communication" with master after receiving "permission" from it.
- Two types of slave nodes: "active" and "parked" slaves. One piconet accommodates 1 master node + up to 7 "active" slaves + up to 255 "parked" slaves.
  ==> in a piconet need 3 bits to address "active" slaves + 8 bits to address "parked" slaves).

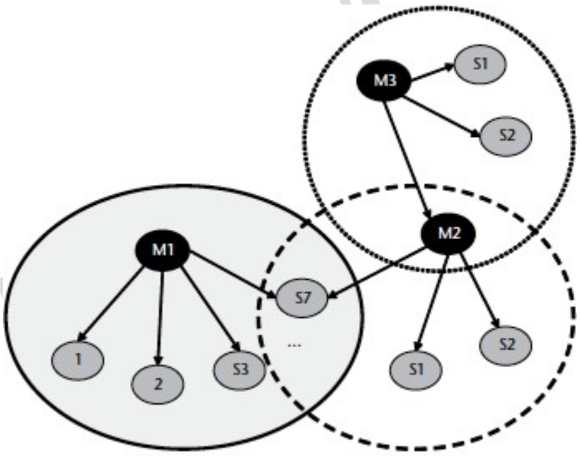


Ali Nikoukar, Salem Raza, Angelina Poole, Mesut Gunes, Benham Dezfouli, Low-Power Wireless for the Internet of Things- Standards and Applications, IEEE Access 6, 2018

Network Components & Topology (Cont'd-2) [Gupta, 2016]

Case of multiple nodes (Cont'd-1):

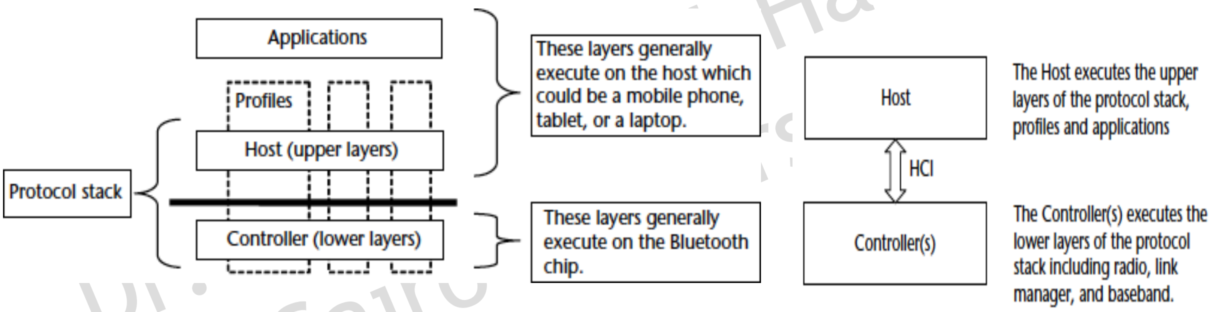
- Master node continuously *"polls"* active slaves to see if they have data to transmit. If an active slave does not respond to the polling for a long time, it loses its 3-bit address and becomes a parked slave (by obtaining an 8-bit address).
- Master node periodically checks status of parked slaves to see if they have data to transmit. If so, master node may assign "3-bit" address to them.
- Each piconet uses its own frequency hopping pattern generated by the master node. This allows several piconets to coexist. Several piconets can form a larger network - called "scatternet - by "node sharing". A shared node " can be a slave in one piconet and a master in another piconet (e.g. M2), or it can be a slave in both piconets (e.g. S7).



Scatternet operation with 3 piconets
M2 is Master in 1 piconet and slave in another
S7 is slave in 2 piconets

Bluetooth Architecture & Protocol Stack [Gupta, 2016]

General Architecture

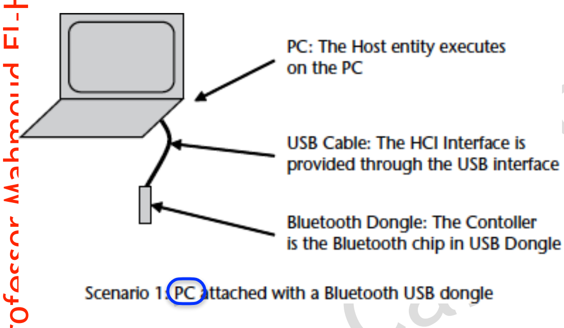


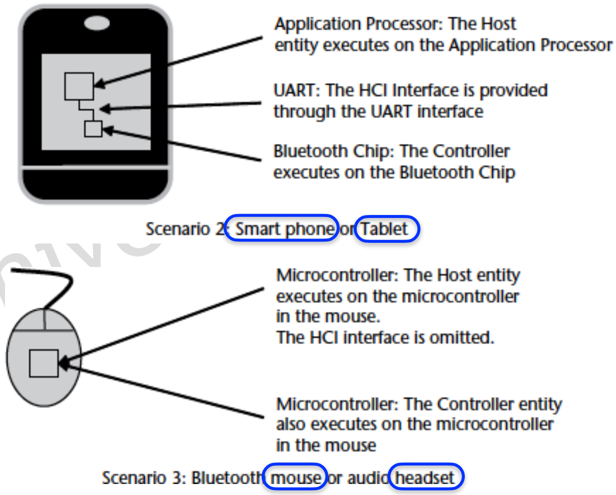
Realization of Bluetooth (BT) as a functional system necessitates implementation of:

- Low level (lower layer) functions, collectively called "Controller"
- High level (upper layer) functions, collectively called "Host"
- "An optional" interface between the controller & the Host, called Host Controller Interface (HCI)

Bluetooth Architecture & Protocol Stack (Cont'd-1) [Gupta, 2016]

Real Life Examples





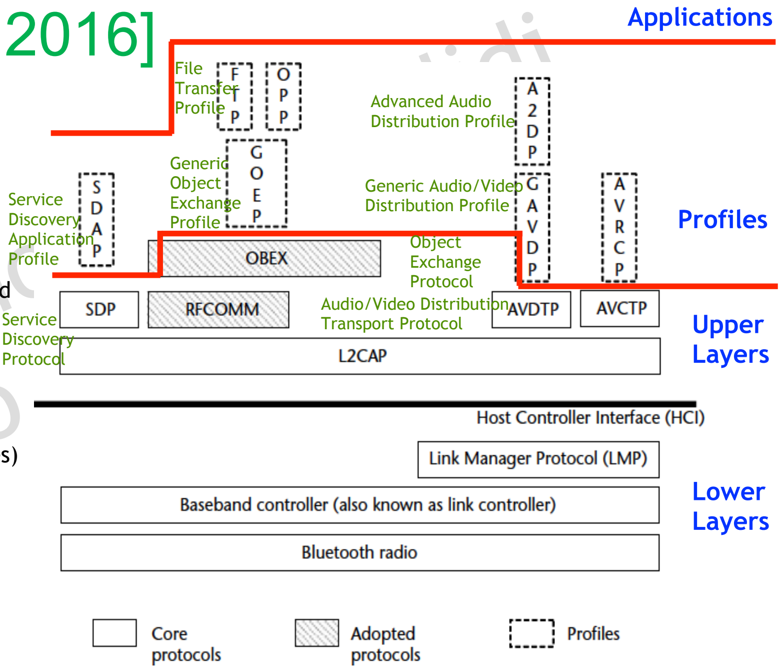
Remarks:

- Typically, Host software executes on an application processor or micro-controller.
- Typically, the Controller functionality is embedded in a Bluetooth chip that is attached to the Host.
- Physically, Host Controller Interface (HCI) may run on top of an interface like UART, RS-232, USB or SD.

Bluetooth Architecture & Protocol Stack (Cont'd-2) [Gupta, 2016]

Detailed Architecture

- Functions deployed in BT are classified into:
  - Functions developed specifically for BT (Called "Core Functions". Are developed from scratch).
  - Functions adopted from existing realizations of wireless technologies (Called "Adopted Functions". Are adapted from specifications issued by other standardization bodies).
- Other components of the BT architecture include:
  - Profiles (customized for specific Use Cases)
  - Application modules that support:
    - * common activities such as node pairing, Man/Machine Interfacing, … ,etc
    - * Specific Use Cases such as audio streaming



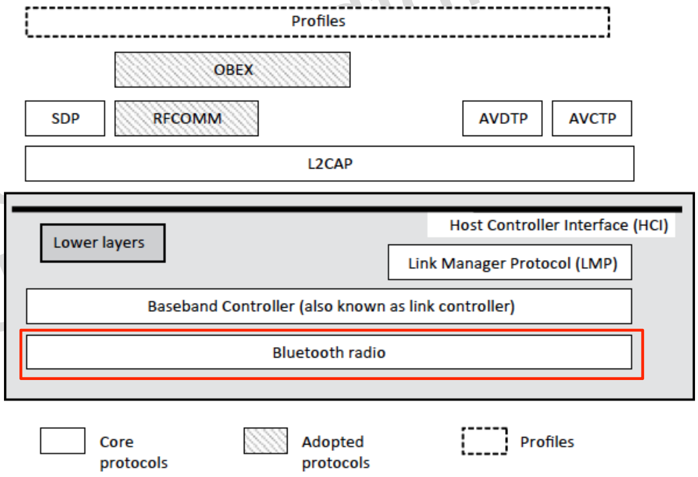
Bluetooth Lower Layers: Bluetooth Radio [Gupta, 2016]

Functions of Bluetooth Radio

- Transmission and Reception of packets:

  This includes ***modulation and demodulation*** of the packets. Two modulations modes are defined:

  - ***Basic Rate (BR)***: Uses a shaped binary FM modulation (GFSK) mechanism and is designed to minimize complexity of the transceiver. Gross air data rate = 1 Mbps.
  - ***Enhanced Data Rate (EDR)***: Uses Phase Shift Keying (PSK) Modulation (π/4 DQPSK & 8 DPSK) to support higher data rates. Gross air data rate = 2 Mbps or 3 Mbps.



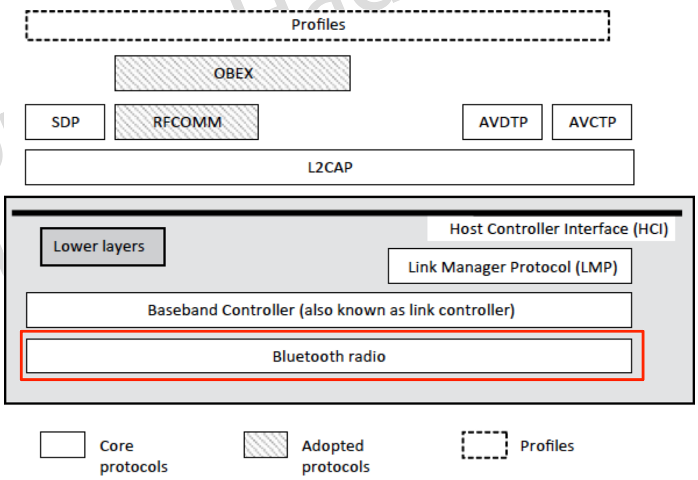
Bluetooth Lower Layers: Bluetooth Radio (Cont'd-1) [Gupta, 2016]

Professor Mahmoud El-Hadidi

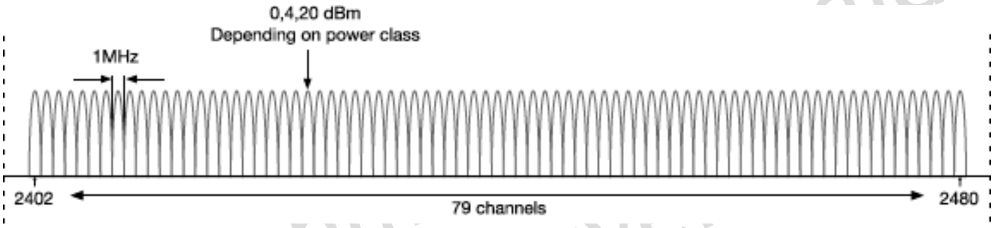
- Supporting appropriate power class:

  Three power classes are defined by the Bluetooth specification based on the maximum output power.

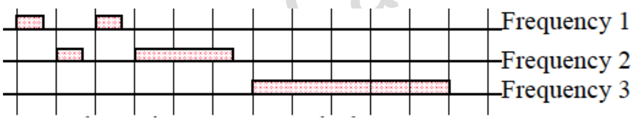
  - Power Class 1: Maximum output power of 100 mW (20 dBm).
  - Power Class 2: Maximum output power of 2.5 mW (4 dBm).
  - Power Class 3: Maximum output power of 1 mW (0 dBm).

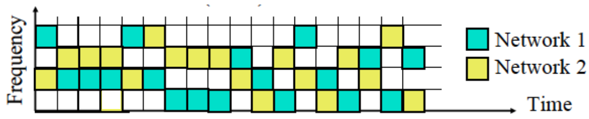


Bluetooth Lower Layers: Bluetooth Radio (Cont'd-2)

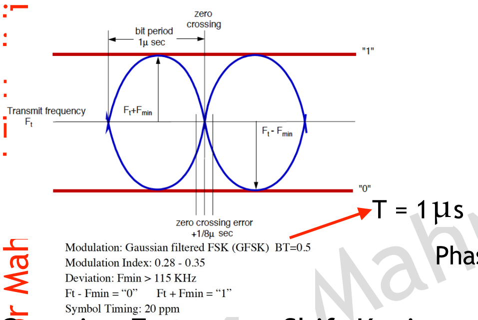


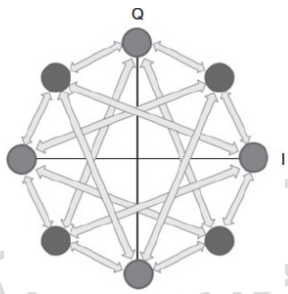
- Bluetooth Radio operates in the 2.4 GHz ISM band.
- Uses a frequency hopping mechanism with 79 channels to combat interference. Each channel has 1 MHz BW.

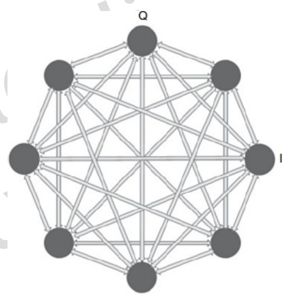




Bluetooth Lower Layers: Bluetooth Radio (Cont'd-3)







Phase differences are chosen from the set {π/4,3π/4,-3π/4,-π/4}

Gaussian Frequency Shift Keying (GFSK)

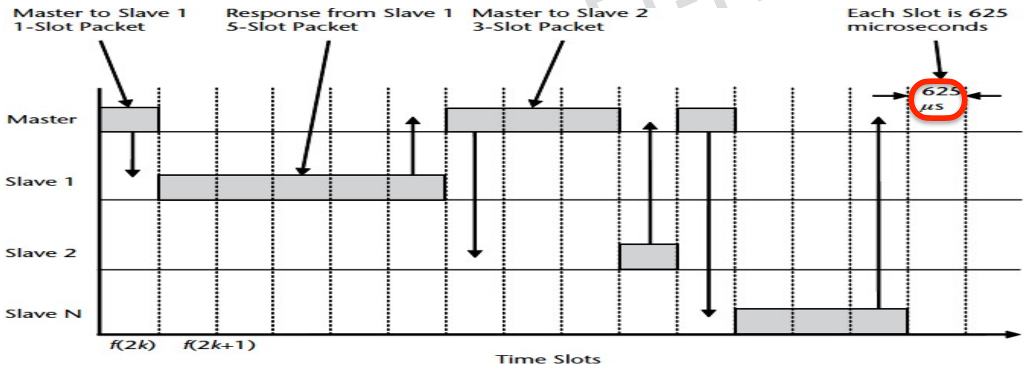
π/4 QPSK & π/4 QDPSK Constellation

8 PSK & 8 DPSK Constellation

- Gross data rate = 2B log M   M = # of symbols
  = 2 x 0.5 MHz x log 2 = 1 Mbps (BR - GFSK)
  = 2 x 0.5 MHz x log 4 = 2 Mbps (EDR - π/4 QDPSK)
  = 2 x 0.5 MHz x log 8 = 3 Mbps (EDR - 8 DPSK)

Bluetooth Lower Layers: Bluetooth Radio (Cont'd-4)

- A Time Division Duplex (TDD) scheme is used for full duplex transmission [Gupta, 2016]



Two types of channels: Asynchronous ConnectionLess (ACL) - used for data - and Synchronous Connection Oriented (SCO) - used for audio. Each channel can utilize 1, or 3, or 5 time slots. Master transmits at EVEN slot #'s while Slave(s) transmit at ODD # slots.

Professor Mahmoud El-Hadidi

Bluetooth Lower Layers: Bluetooth Radio (Cont'd-5)

- Typical technical specifications [Gupta, 2016]

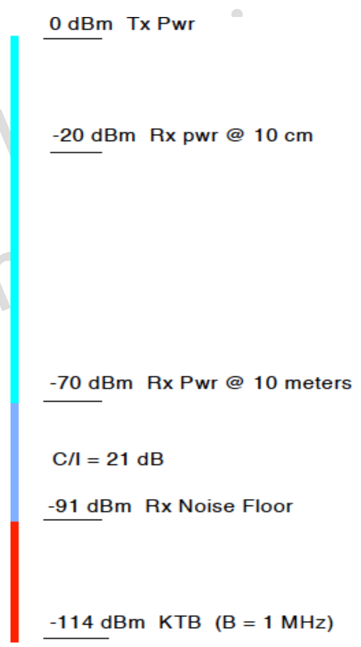
Connection Type	*Frequency Hopping Spread Spectrum*
Spectrum	2.4 GHz ISM Band. Regulatory range: 2400–2483.5 MHz.
Frequency Hopping	1600 hops per second across 79 RF channels. The channels are separated by 1 MHz.
Modulation	Gaussian Frequency Shift Keying (GFSK). ← BR system
Maximum Output Power	1 mW to 100 mW.
Transmit Power	Nominal = 0dBm. Goes up to 20 dBm with power control.
Receiver Sensitivity	–70 dBm at 0.1% Bit Error Rate
Maximum Data Rate	721.2 kbps for Basic Rate. ← < 1 Mbps (due to channel guards)
	2.1 Mbps with Enhanced Data Rate (BT Spec 2.0+EDR).
	24 Mbps with High Speed (BT Spec 3.0+HS).
Typical Range	10 m to 100 m.
Topology	Up to 8 devices in a piconet including 1 Master and up to 7 Slaves.
Voice Channels	3
Data Security: Authentication Key	128 bit key.
Data Security: Encryption Key	8-128 bits (configurable).
Applicability	Does not require line of sight.
	Intended to work anywhere in the world since it uses unlicensed band.

Bluetooth Lower Layers: Bluetooth Radio (Cont'd-6)

- Link Budget

TX power of 0 dBm
C/I = 21 dB
NF = 23 dB

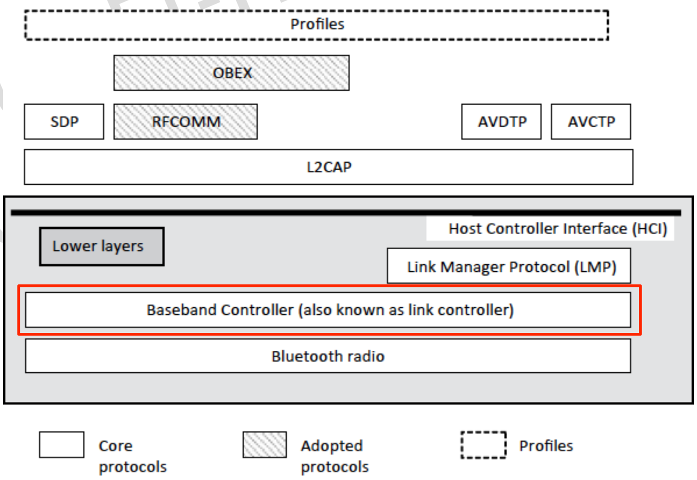
Results in a radio with very relaxed specifications
==> Simpler HW
==> Less Cost



Bluetooth Lower Layers: Baseband Controller

Functions of Baseband Controller (called Link Controller) [Gupta, 2016]

- Management of ***physical channels*** and ***links*** for single or multiple links
- Selection of the next hopping frequency for transmitting and receiving packets.
- Formation of ***piconet*** and ***scatternet***.
- Formation of ***packets*** and then giving them to the Bluetooth radio for transmission.
- ***Inquiry*** and ***Inquiry Scan***.
- ***Connection*** and ***Page Scan***.
- Security (including data encryption).
- Power management (including low power modes).



Bluetooth Lower Layers: Baseband Controller (Cont'd-1) [Gupta, 2016]

Link Controller States

THREE main states

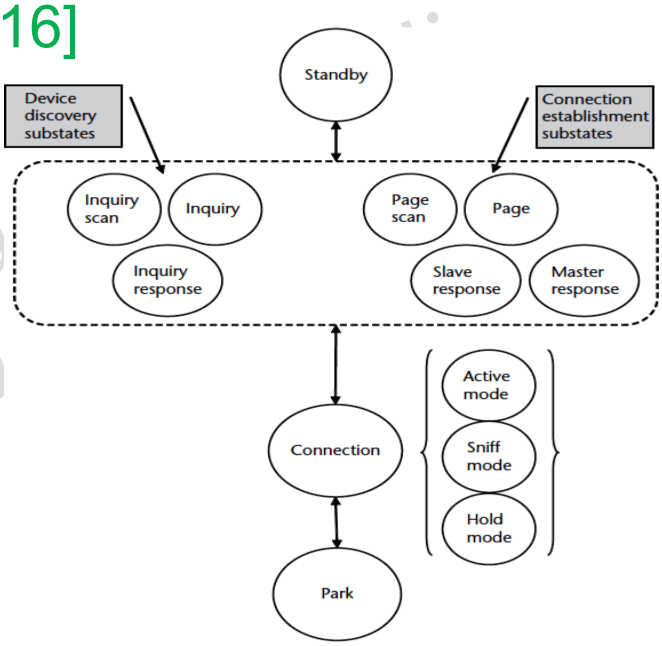
Standby - Connection - Park

+ Device Discovery Sub-States

Inquiry Scan - Inquiry - Inquiry Response

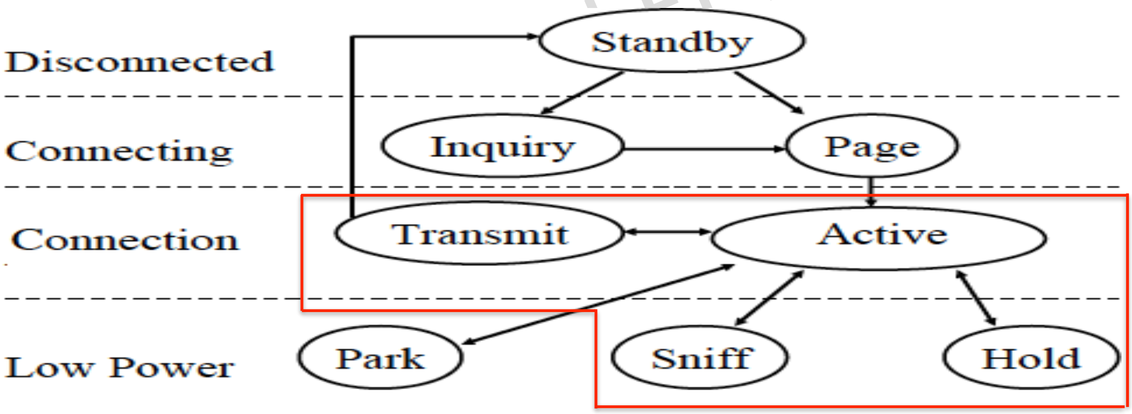
+ Connection Establishment Sub-States

Page Scan - Page - Master Response- Slave Response



Bluetooth Lower Layers: Baseband Controller (Cont'd-2)

State Transition Diagram



Bluetooth Lower Layers: Baseband Controller (Cont'd-3) [Gupta, 2016]

3 Modes of Connection State

In "Connection" state, a device can be in one of three modes:

Active: During this mode, master keeps scheduling the salves by sending POLL packets

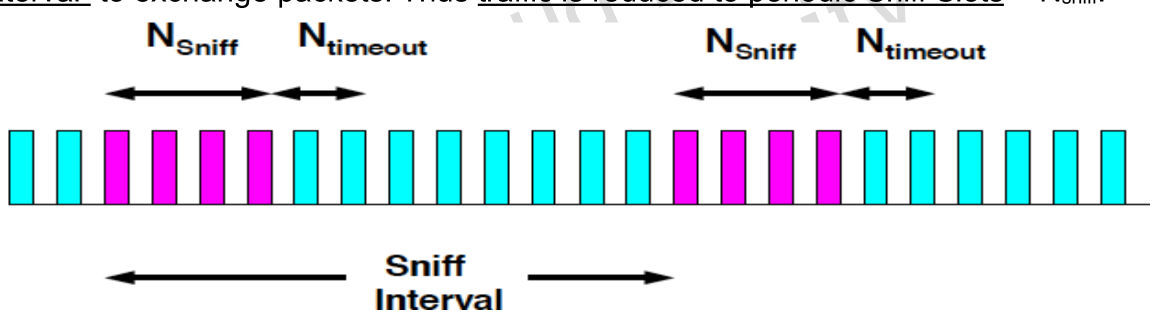
Hold: During this mode, ***master*** stops sending POLL, and both master and slaves are notified of the duration of time they need to hold (hold time is assigned by Master). No Asynchronous Connectionless (ACL) channels are active. Only Synchronous Connection Oriented (SCO) channels continue. Node can do something else: e.g. scan, page, inquire, attend another piconet, or go to low power sleep. Slave keeps 3-bit AM_ADDR (Active Member ADDRess).

After "Hold Time", slave wakes up and synchronizes with traffic on the channel.

Professor Mahmoud El-Hadidi

Bluetooth Lower Layers: Baseband Controller (Cont'd-4)

Sniff: During this mode, a ***device*** can be temporarily absent from piconet (as in case of idle mouse), in order to save battery. Like **Hold**, a Slave in the **Sniff** state retains its AM_ADDR, remains active, but in a low power mode. It wakes up at assigned "Sniff Interval" to exchange packets. Thus traffic is reduced to periodic Sniff Slots = N_{sniff}.

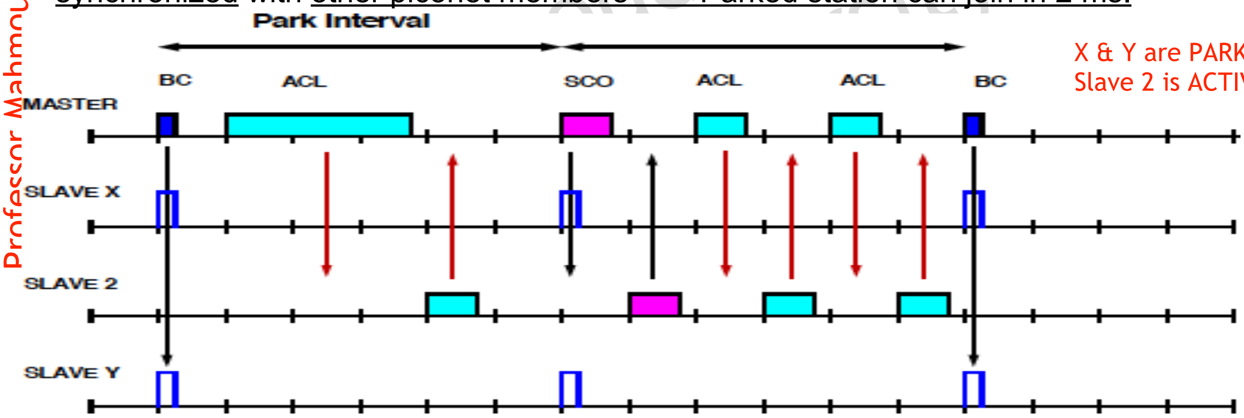


Slave listens for traffic with Slave AM_ADDR or N_{sniff} whichever is longer. After traffic ceases, Slave continues to listen for $N_{timeout}$.

Link Management Protocol (LMP) sets Sniff Mode parameters.

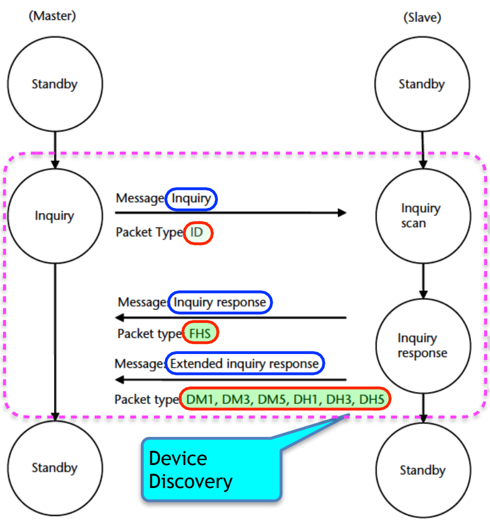
Bluetooth Lower Layers: Baseband Controller (Cont'd-5)

Remark: In "Park" state:
Device is in very low-power mode. It gives up its 3-bit AM-ADDR and gets an 8-bit parked member address. It wakes up periodically and listens to beacons.
Master broadcasts a train of beacons sent periodically by the Link Manager. It remains synchronized with other piconet members ==> Parked station can join in 2 ms.

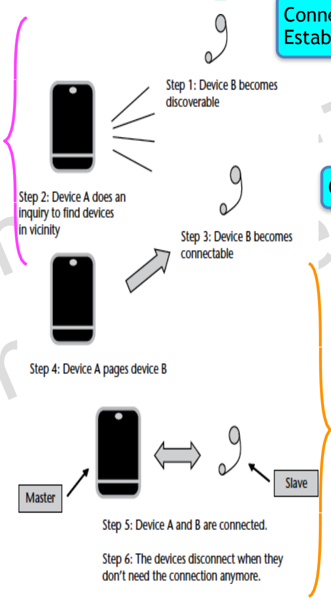


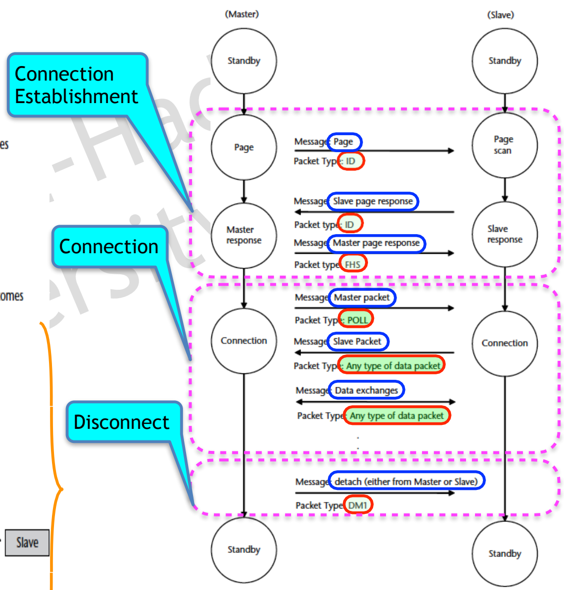
X & Y are PARKED
Slave 2 is ACTIVE

Bluetooth Lower Layers: Baseband Controller (Cont'd-6) [Gupta, 2016]



Link Controller Messages & States during inquiry





Link Controller Messages & States during connection & disconnection