Bluetooth

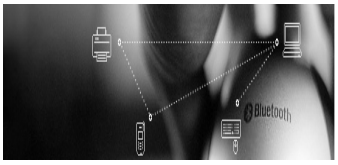
Babak Kia
Adjunct Professor
Boston University
College of Engineering
Email: bkia -at- bu.edu

What is Bluetooth

- **It is an always on, low power, short ranged radio link for communication between mobile devices**
- **Developed in 1994 by the Swedish company Ericsson to enable laptops make calls over mobile phones**
- **Also known as 802.15, it employs the 2.4 GHz unlicensed band, the same as 802.11b wireless, but does not interfere with it**
- **Provides data rates of up to 720 Kbps**
- **Power output is around 1 milliwatt, compared to the average cell phone's 500 milliwatt power output**

Bluetooth Applications

- **Major use in consumer electronics**
- **Embedded in a whole slew of electronic products ranging from on PDAs, cellphones and printers, to automobiles**



Bluetooth Characteristics

- Allows up to 8 devices to communicate in a local network called a Piconet, also known as a Personal Area Network or PAN
- Because of its low power consumption, its range is limited to 10 m.
- However, range can be increased to 100 m by employing a scatternet topology or a higher powered antenna
- Three classes of Bluetooth devices
  - Class 1 – 100 m ≤ 20 dBm power
  - Class 2 – 10m ≤ 4 dBm power
  - Class 3 – 10 cm @ 0 dBm power

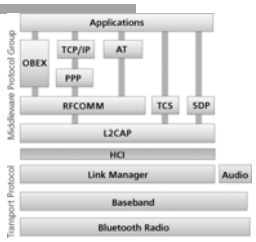
4

The Bluetooth Standard

- The Bluetooth standard is maintained and published by the Bluetooth Special Interest Group (SIG)
- Includes thousands of member companies
- Covers topics such as interoperability, testing and qualification of bluetooth devices
- Most important, outlines the specifications for:
  - Bluetooth Radio
  - Baseband
  - LMP – Link Manager Protocol
  - HCI – Host Controller Interface
  - L2CAP – Logical Link Control & Adaptation Protocol
  - RFCOMM
  - Profiles

5

The Bluetooth Stack



Note: Baseband really means Baseband + Link Controller
•LC is responsible for carrying out link level operations over several data packet duration
•Baseband is responsible for channel codec and management of the link over a single data packet

6

Bluetooth Radio

- Bluetooth uses a 74 MHz slice of the 2.4 GHz radio band.
- This is shared by not only 802.11 WiFi, but also by garage door openers and baby monitors!
- Does this mean that baby monitors interfere with bluetooth?
  - Unlike a baby monitor, bluetooth employs a Frequency Hopping strategy
- Frequency Hopping is a method where the signal is switched from one channel to another in accordance with a pre-established pseudo-random pattern
- This not only reduces interference from other sources, but also provides security by preventing eavesdropping

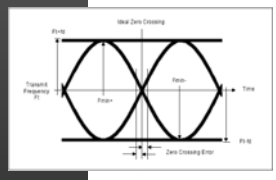
7

Frequency Hopping

- The Bluetooth bit rate is 1Mbps ±1ppm
- However, headers and handshaking overhead take up about 20% of this bandwidth
- Frequency Hopping happens at 1600 times a second over 79 channels (United States and Europe) or 23 channels (Japan)
- Each time-slot is 625 μs long
- Packets can take up to 5 time-slots
- Data packets can be up to 2745 bits long
- Two modes for transmission
  - SCO – Synchronous Connection Oriented
  - ACL – Asynchronous Connectionless

8

Bluetooth Radio



- Bluetooth uses a TDD (Time Division Duplex) protocol to transmit information in one time-slot and receive in another
- Employs a Gaussian Frequency Shift Keying (GFSK) modulation mechanism to transmit bits, where:
  - Binary 0 is represented by a negative frequency deviation
  - Binary 1 is represented by a positive frequency deviation

9

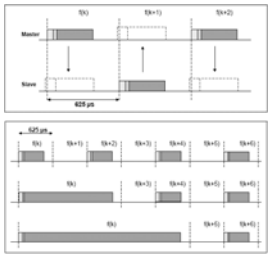
Baseband

- **Baseband is the Physical Layer of Bluetooth and manages the following. We will discuss only the highlighted items:**
  - ✓ **Physical Channels**
  - ✓ **Physical Links**
  - ✓ **Packets**
  - • **Error Correction**
  - • **Logical Channels**
  - • **Data Whitening**
  - • **Transmit/Receive Routines & Timing**
  - • **Channel Control & Hop Selection**
  - • **Bluetooth Audio**
  - ✓ **Bluetooth Addressing**
  - • **Bluetooth Security**

10

Baseband – Physical Channel

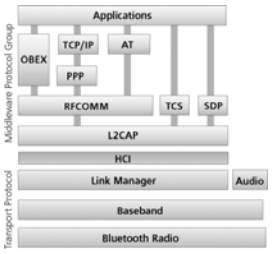
- **Each channel is represented by a pseudo-random hopping frequency, determined by the master, through 79 or 23 RF channels**
- **The channel is divided into time slots, each 625 µs in length**
- **Time slots are numbered according to the bluetooth clock of the master ranging from 0 to 2^{27}-1 cyclically**
- **Master transmits on even time-slots, while slaves transmit on odd time-slots**



11

Baseband – Physical Link

- **Baseband is the physical link of the Bluetooth protocol**
- **It handles two types of links:**
  - **SCO – Synchronous Connection Oriented**
  - **ACL – Asynchronous Connectionless**



12

Baseband - SCO

- SCO is a symmetric point-to-point link between a master and a single slave in the piconet
- The SCO link is maintained by the master by its use of timeslots at regular intervals
- The Master can support up to 3 simultaneous SCO links, while the slaves can support 2 or 3 links
- SCO packets are never retransmitted, and are typically employed in time constraint applications such as voice
- Are used in 64Kbps speech transmission
- A SCO link can be considered as a circuit-switched connection

13

Baseband - ACL

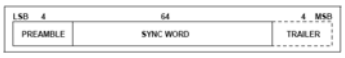
- Point-to-multipoint link between master and all slaves in the piconet
- ACL link can be established on per slot basis
- In the slots which are not reserved for SCO transmission, the master can establish an ACL link with any slave, including the slaves which are already engaged in SCO communication
- Unlike SCO where multiple SCO links can be established, only one ACL Link can be established between two nodes
- ACL packets which are lost are always retransmitted

14

Baseband - Packets

- The Bluetooth general packet format is comprised of three parts: Access Code, Header, and Payload

- Access Code
  - Can be 68 or 72 bits wide, depending on whether a packet header follows or not
  - Used for synchronization, DC offset compensation, and identification



15

Baseband - Packets

- There are three categories of Access Codes:
  - Channel Access Code (CAC): Defines a piconet
  - Device Access Code (DAC): Used for paging
  - Inquiry Access Code (IAC): There are two variations of General (GIAC) and Dedicated (DIAC), the latter is used only in identifying Bluetooth devices sharing a common characteristic
- Payload data is dependent on the Bluetooth application (voice, data, …)
- The Packet Header consists Link Control (LC) and is comprised of 6 fields:

16

Baseband - Packets

- The 6 fields are as follows:
  - AM_ADDR is a 3-bit active member address used to distinguish between the active members of a piconet
  - Type is a 4-bit type code used to distinguish between one of 16 different packet types, such as ID Packet, POLL packet, or NULL Packet.
  - Flow is a bit used for flow control over ACL. When the receiver buffer is full, a STOP indication is returned by means of FLOW = 0 to prevent further transmission
  - ARQN is the acknowledgement bit for CRCed packets
  - SEQN provided sequencing for multiple data packets
  - HEC is the Header Error Check used to verify header integrity

17

Link Controller

- The Link Controller carries out higher level operations such as paging and inquiries
- It is responsible for device discoverability, as well as establishing and maintaining connections with other devices
- Handling corrupted data:
  - Each packet has an ARQN flag which indicates the status of the previously received packet
  - ARQN value of 1 is an ACK, and 0 is a NAK
- All new packets change the value of SEQN, however retransmitted packets maintain SEQN

18

Link Controller

- **At any given time, the Link Controller is in one of several states**
  - ***Standby*: The device is inactive, the radio is switched off, and no data is being transferred**
  - ***Inquiry*: The device attempts to discover all BT devices in its local vicinity**
  - ***Inquiry Scan*: Another part of the inquiry procedure. Devices listen for a long time, which is important because they don't have knowledge of the frequency hop or timing of an inquiring device, for GIAC and DIAC inquiry packets**

19

Link Controller

- ***Page*: For a device to establish connection and become master, it needs to transmit page messages until a slave device acknowledges the pages**
- ***Paging Scan*: Consequently, a device needs to enter page scan periodically to allow paging devices to establish connection with it**
- ***Connection*: Connection has four states: *active, hold, sniff*, and *park*.**
  - **In Active mode, the bluetooth module is actively participating in channel communication. The master schedules transmissions based on its traffic demands, but also maintains regular transmissions to keep synchronized slaves alive**

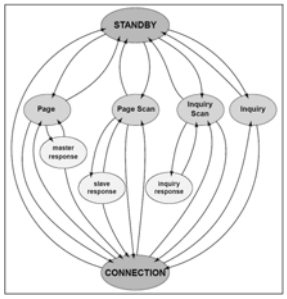
20

Link Controller

- **Hold mode is a low power mode where only the internal timer of the slave is running. Slave units can demand to be put into hold mode, but only the master can put a slave into hold mode**
- **In sniff mode the slave device simply listens to all packets on a predefined time slot until a time out occurs. This occurs at a reduced rate than it would normally listen to traffic.**
- **The sniff interval is is programmable**
- **Park mode is used for low power modes where the device only occasionally listens for traffic, but is still synchronized to the channel**

21

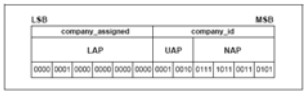
Link Controller State Diagram



22

Bluetooth Addressing

- **Each Bluetooth transceiver is allocated a unique 48-bit device address (BD_ADDR)**
  - **LAP is the 24-bit Lower Address Part**
  - **UAP is the 8-bit Upper Address Part**
  - **NAP is the 16-bit Non-significant Address Part**



23

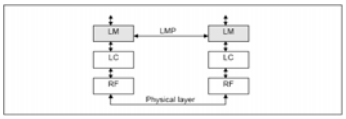
Bluetooth Addressing

- **Asides from the BD_ADDR there are three other addressing functions**
  - **<u>AM_ADDR</u> is the 3-bit Active Member address assigned to each slave in a Piconet. It is only valid while the slave is Active (not parked, or disconnected)**
  - **The all-zero AM_ADDR is the broadcast packet**
  - **The Piconet Master does not have an AM_ADDR. It is distinguishable by its transmit time-slot**
  - **<u>PM_ADDR</u> is an 8-bit Parked Member Address that differentiates between parked slaves**
  - **<u>AR_ADDR</u> is the Access Request Packet used in slave activated unparking**

24

Link Manager Protocol (LMP)

- The Link Manager provides messages that are used in link setup, security and control
- Link Manager Protocols take a higher priority over data traffic
- Messages are interpreted at the LM level and are not passed further up through the stack



- The LMP is a collection of Protocol Data Units (PDUs) sent from one device to another:

25

Link Manager Protocol

- The LM manages:
  - Attaching and detaching slaves to a piconet, and allocating active member addresses
  - Establishing ACL or SCO links
  - Putting a connection into low power mode (hold, sniff, or park)
- A Link Manager communicates with another Link Manager on a different device via the Link Manager Protocol (LMP), and transmitted as Protocol Data Units (PDUs)

26

Link Manager Protocol - PDUs

- General Response
- Authentication
- Pairing
- Change Link Key
- Change Current Link Key
- Encryption
- Slot Offset Request
- Clock Offset Request
- Timing Accuracy Info Req.
- LMP Version
- ✓ Supported Features
- Switch Master/Slave
- Paging Scheme
- ✓ Name Request
- ✓ Detach
- ✓ Hold Mode
- Sniff Mode
- ✓ Park Mode
- ✓ Power Control
- Channel Quality-Driven Change
- Quality of Service
- SCO Links
- Control of Multi-Slot Packets
- Connection Establishment
- Test Mode
- Error Handling
- Link Supervision

27

Link Manager Protocol - PDUs

- **Supported Features**
  - **The Bluetooth radio and Link Controller could support only a limited number of packet types and features**
  - **Therefore a device cannot send any packets other than ID, FHS, NULL, POLL, DM1 and DH1 until a target device capabilities are identified**
- **Name Request**
  - **Name Request receives a user-friendly name associated with a Bluetooth device in a maximum string length of 248 characters encoded in the UTF-8 standard.**
- **Detach**
  - **A command which can be initiated by the master or the slave in order to close a connection. A message can be transferred to indicate the reason as to closure of link.**

28

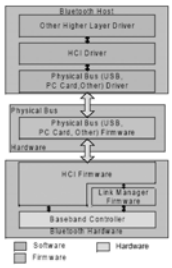
Link Manager Protocol - PDUs

- **Hold Mode**
  - **Used in ACL mode, it is intended to prevent the Master from sending further ACL packets for a specified hold time. The transceiver can then be turned off in order to save power.**
- **Park Mode**
  - **If a slave does not need to participate in a channel, it can be placed in park mode. In this mode all PDUs sent from the Master are broadcast PDUs.**
- **Power Control**
  - **A device can request to increase or decrease another devices transmit power. A request in a multi-slave scenario affects only for the requesting slave.**

29

Host Controller Interface (HCI)

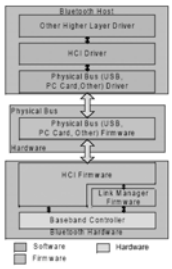
- **HCI's most important function is to provide a uniform method for accessing Bluetooth baseband capabilities**
- **It separates the higher levels of the Bluetooth Stack (software) from the lower levels of the Bluetooth stack (firmware and hardware)**



30

Host Controller Interface (HCI)

- HCI is an interface between higher and lower levels of the protocol, e.g. PCMCIA card
- For example, a PCMCIA card can implement the lower levels of the protocol, and to save cost interface with the host PC for higher levels of the protocol
- Why not implement some of the lower levels on host PC? Because of stringent timing requirements
- However something like a headset needs to implement all levels of the protocol



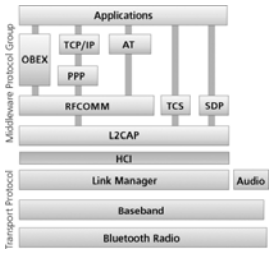
31

Host Controller Interface (HCI)

- HCI employs three different packet types
  - Command Packets – go from Host to the BT module
  - Event Packets –go from the BT module to the Host
  - Data Packets – which travel in both directions
- Through these commands, HCI enables the host to fully control a BT module
  - Control links – configure, setup, teardown
  - Access local & remote modules via LMP exchanges
  - Invoke the BT test module for factory test
- HCI provides three transport layers
  - USB
  - RS232 – which provides error correction
  - UART – which does not provide error correction

32

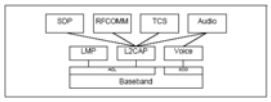
In case you've forgotten…



33

Logical Link Control and Adaptation Protocol (L2CAP)

- L2CAPs function is to take data from a higher level application and to pass it down to the lower stack
- L2CAP supports both connection oriented and connectionless data services to upper protocols
- It allows higher level protocols to transmit and receive data of up to 64 Kbytes.
- L2CAP is in charge of protocol multiplexing as well as Segmentation and Reassembly (SAR) of packets.



34

Other L2CAP Functions

- **L2CAP is also in charge of…**
  - Multiplexing between different higher level protocols
  - Segmentation and Reassembly to allow transfer of larger packets than lower levels can support
  - Group management, provides one-way transmission to a group of BT devices
  - QoS management for higher protocols

35

RFCOMM

- RFCOMM is used to emulate the functions of a serial port (RS232) over bluetooth
- RFCOMM provides multiple concurrent connections by relying on the L2CAP services to handle multiplexing over a single connection
- RFCOMM lacks the ability to validate data integrity, and therefore relies on the bluetooth baseband to provide reliable and in-sequence delivery of byte streams

36

RFCOMM

- Traditional serial interfaces rely on a Universal Asynchronous Receiver Transmitters (UARTs) to translate parallel data into a serial stream and vice versa.
- RFCOMM emulates this process
- There are two types of devices:
  - Type 1 is an internally emulated serial port
  - Type 2 is an intermediate device which is actually connected to a serial port

37

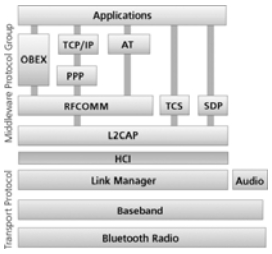
RFCOMM

- RFCOMM needs to first establish an L2CAP connection, after which time the RFCOMM control and data frames can be sent back and forth
- RFCOMM can support up to 30 different data channels at once, however in reality most devices limit the number of channels due to lack of resources

38

Service Discovery Protocol (SDP)

- Service Discovery Protocol is one of the higher level protocols which provides the means for an application to discover which services are available
- Keep in mind that the list of services which are available changes dynamically due to environmental factors (RF proximity), or functional factors…



39

Service Discovery Protocol (SDP)

- The way bluetooth connects to devices is unlike the way devices connected on a LAN
- For example, you can find a printer on the local network and connect to it with a PC. Once connected, this is a connection which remains in place for a very long time
- Bluetooth on the other hand was designed for an environment where connections changed frequently
- Therefore it needs a mechanism to allow it to quickly discover devices, use their services, and forget about them once they have been used
- This is provided by the *Service Discovery Protocol*

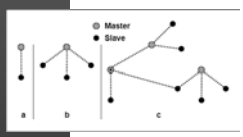
40

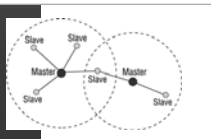
Profiles

- Profiles are specifications which describe how bluetooth should be used in a specific application and as such ensures that all devices from different manufacturers can seamlessly work with one another
- There are about a dozen profiles:
  - Generic Access, Serial Port, Dialup Networking, FAX, Headset, LAN Access Point, Generic Object Exchange (OBEX), File Transfer,Object Push, Synchronization, Cordless Telephony, and Intercom
- More profiles are under discussion within various Bluetooth SIG groups, and there is a whole other spec dedicated to Bluetooth Profiles

41

Piconet





- A Piconet or a Personal Area Network (PAN) is comprised of one master and seven slaves
- A device can be a slave in two different Piconets
- A device can also be a master in one Piconet while a slave in another
- Piconet communication always takes place as point-to-point or point-to-multipoint
- Joining more than one Piconet together forms a scatternet

42

Piconet

- The ability of Bluetooth to setup and tear down piconet networks *ad-hoc* makes it both very flexible, and more complex than traditional wired networks
- This is also why the Bluetooth Link Controller provides specific functions to help detect new in-range devices and to easily establish connection with them

43

Inquiry Example

- The inquiry procedure enables a device to discover which devices are in range, and determine the addresses and clocks for the devices.
  - The inquiry procedure involves a unit (the source) sending out inquiry packets (inquiry state) and then receiving the inquiry reply
  - The unit that receives the inquiry packets (the destination), will hopefully be in the inquiry scan state to receive the inquiry packets.
  - The destination will then enter the inquiry response state and send an inquiry reply to the source.
- After the inquiry procedure has completed, a connection can be established using the paging procedure.

44

Paging Procedure

- It is with the paging procedure that an actual connection can be established.
- The paging procedure typically follows the inquiry procedure. Only the Bluetooth device address is required to set up a connection.
- A unit that establishes a connection will carry out a page procedure and will automatically be the master of the connection.

45

Paging Procedure (cont.)

- **The procedure occurs as follows:**
  - **A device (the source) pages another device (the destination). [Page state]**
  - **The destination receives the page. [Page Scan state]**
  - **The destination sends a reply to the source. [Slave Response state]**
  - **The source sends an FHS packet to the destination. [Master Response state]**
  - **The destination sends it's second reply to the source. [Slave Response state]**
  - **The destination & source then switch to the source channel parameters.**

46

Have a nice weekend!

47