Bluetooth

Part 1: Overview

Outline

- What is Bluetooth?
- The protocol stack
- Using Bluetooth

Bluetooth Defined

- Bluetooth is a low cost, low power, short-range radio technology
- Originally developed as cable replacement to connect mobile phones, headsets, portable computers, and Personal Digital Assistants (PDAs)
- Standardized wireless communication enables **Personal Area Network** (PAN)

Bluetooth Protocol Stack

- Bluetooth stack defined by series of layers (see Figure 1-1)
- Usually implemented partly in hardware and partly in software
- Allows devices from different manufacturers to communicate with one another
- Enables applications to discover other Bluetooth devices, and determine what services they offer

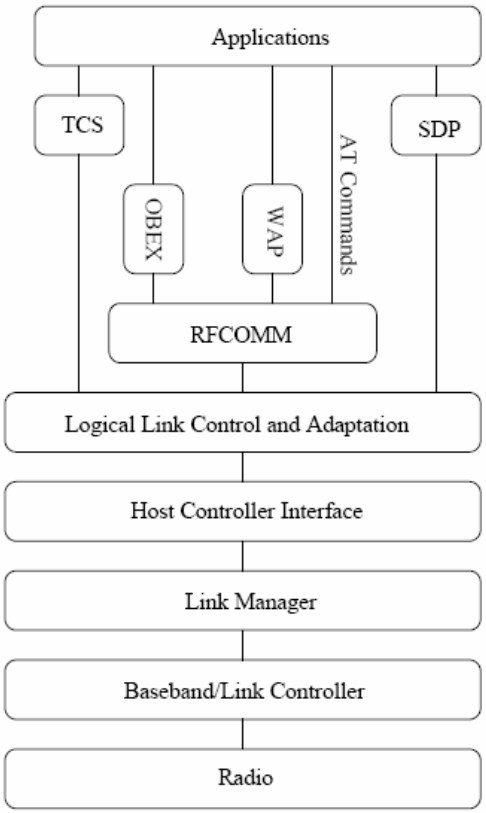

Figure 1-1 Protocol stack

Physical Layer

- Operates at 2.4 GHz in globally available, unlicensed Industrial, Scientific, and Medical (ISM) band
- Handheld Bluetooth devices require antennas which radiate in a pattern close to a sphere, i.e., the performance of the devices should appear to be independent of operating angle
- Bluetooth signalling must be robust since there are many other systems using the same spectrum, thus creating interference

Signalling

- Operating band (2.400–2.4835 GHz) of 83.5 MHz divided into 79 channels with carrier frequencies $f = 2402 + k$ MHz, $k = 0, \ldots, 78$
- Channel spacing is 1 MHz. To comply with out-of-band regulations, 2 MHz and 3.5 MHz lower and upper guard bands are used
- Gaussian Frequency Shift Keying (GFSK) modulation with one bit per symbol

More on Signalling

- Frequency Hopping Spread Spectrum (FHSS) for robust and "secure" communication
- 625 microseconds time slots
- One hop per packet (every slot, every 3 slots, or every 5 slots)
- Re-transmission of lost data packets

Transmit Power Classes

Class	Max. output power	Range	Power control
1	100mW (20 dBm)	100m+	mandatory
2	2.5mW (4 dBm)	10m	optional
3	1mW (0 dBm)	1m	optional

- Most manufacturers are producing Class 3 radios
- Power control reduces interference and power consumption

Masters and Slaves

- Each Bluetooth device is a **Master** or **Slave**. A Master initiates an exchange of data and the Slave responds to the Master
- Communicating Bluetooth devices must use same sequence of frequency hops
- Slaves synchronize to frequency hop sequence used by Master

Frequency Hop Sequence

- Every Bluetooth device has unique device (48 bit IEEE MAC) address and clock
- Each Slave receives Master's address and clock. Slave uses this information to calculate frequency hop sequence

TDM

- Time Division Multiplexing (TDM) is used to divide the total bandwidth between Bluetooth devices
- Master assigns time slots to Slaves
- Packets are joined together in transmit and receive pairs; a packet pair can be 2, 4, 6, 8, or 10 slots long

Piconets and Scatternets

Piconet Group of Bluetooth devices joined together into a short-range network by Bluetooth links. The group is synchronized to the timing and hopping sequence of the Master (see Figure 1-2)

Scatternet Group of Bluetooth piconets joined together by devices that are in more than one piconet. (Routing of packets between piconets is not defined in version 1.1 of the Bluetooth standard)

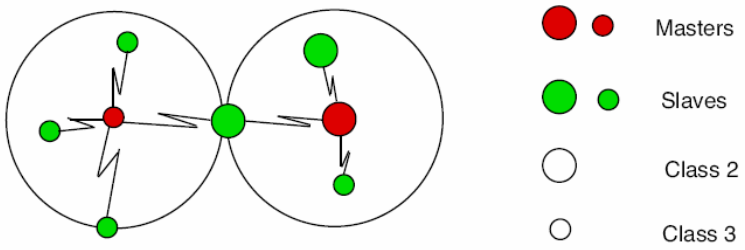

Figure 1-2 Scatternet consisting of two piconets with different power class devices

More on Piconets

- The Slaves in a piconet only have links to the Master; there are no direct links between Slaves in a piconet
- There are no more than seven Slaves in a piconet

More on Scatternets

- A device present in more than one piconet must time-share, spending a few slots on one piconet and a few slots on the other
- A device may not be Master of two different piconets since all Slaves in a piconet are synchronized to the Master's hop sequence
- *Piconets making up a scatternet do not coordinate their frequency hopping*
- Unsynchronized piconets in an area will randomly collide on the same frequency.

Voice and Data Links

- **SCO** (Synchronous Connection Oriented) links for voice communication
- **ACL** (Asynchronous Connectionless) links for data communication

ACL Data Packets

- ACL data packets contain a 72-bit access code, 54-bit header, 16-bit Cyclic Redundancy Checksum (CRC), and varying amount of data
- The largest packet, i.e. the DH5 packet, stretches over five slots
- Maximum data rate at application level is about 650 kb/s

SCO

- SCO links operate at 64 kb/s
- Can have up to three voice links at once
- SCO links are not suitable for delivering CD-quality sound (!)

Security

- High speed, pseudo-random frequency hopping algorithm makes it difficult to listen in on a connection
- Public domain cipher algorithm SAFER+ generates 128-bit cipher keys from 128-bit plain text

Using Bluetooth, Step 1

Three steps are carried out when a Bluetooth device A (*laptop computer*) wants to utilize a service provided by another device B (*cell phone*).

Step 1 Discovering Bluetooth device (see Figure 1-3):

- device A transmits inquiry packets
- device B replies with **Frequency Hop Synchronization** (FHS) packet which contains device class information

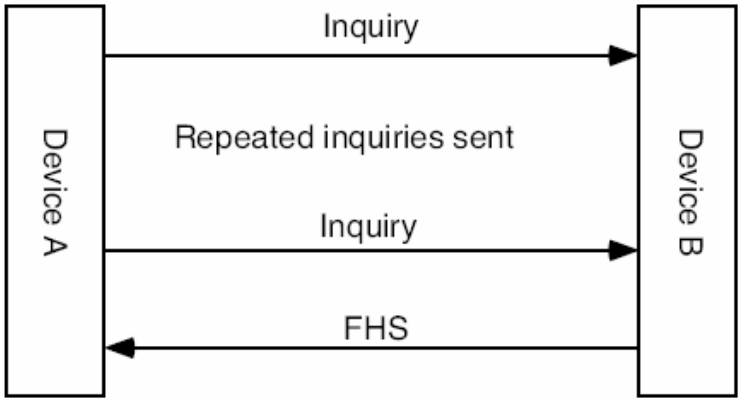

Figure 1-3 Discovering a Bluetooth device

Using Bluetooth, Step 2

Step 2 Connecting to service discovery database (see Figure 1-4):

- ACL baseband connection is established
- **Logical Link Control and Adaption Protocol** (L2CAP) connection is set up over ACL channel
- L2CAP adds Protocol and Service Multiplexor (PSM) to L2CAP packets to distinguish between different higher-layer protocols and services (PSM=0x0001 for service discovery)

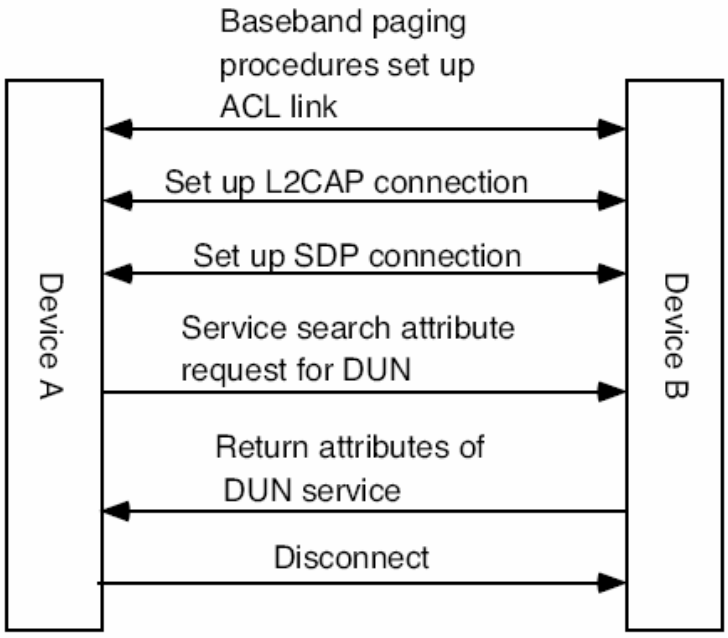

Figure 1-4 Retrieving information on services

Using Bluetooth, Step 2 Continued

- **Service Discovery Protocol** (SDP) connection over L2CAP channel
- device A receives **Dial-Up Networking** (DUN) information from B's service discovery database
- device A disconnects

Using Bluetooth, Step 3

Step 3 Connecting to Bluetooth service (see Figure 1-5):

- ACL link is set up
- device A utilizes **Link Management Protocol** (LMP) to configure link
- L2CAP connection using the RFCOMM protocol for RS-232 serial cable emulation is set up (PSM=0x003)
- DUN connection is set up using RFCOMM connection

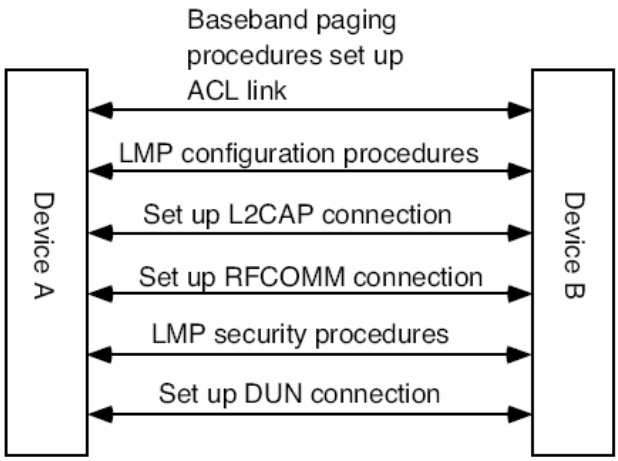

Figure 1-5 Connecting to a Dial Up Networking service

Management

- Device manager needed to manage links. Not defined by Bluetooth specification
- Implementation and complexity of device manager depend on requirements of Bluetooth device
- Device manager can provide fault, accounting, configuration, performance, and *security management*

Summary

- Bluetooth is a low power, short-range radio technology for wireless communications
- Large effort made to ensure
  - high usability
  - low cost
  - interoperability between devices from different manufacturers