Bluetooth

Guevara Noubir

Northeastern University

noubir@ccs.neu.edu

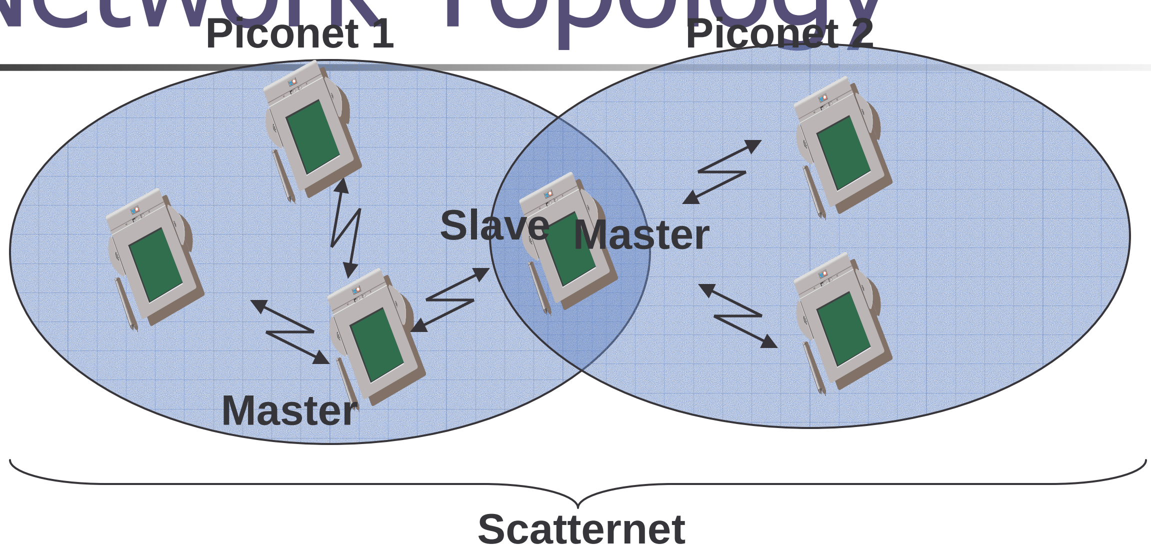
Textbook: William Stallings, “Mobile Communications and Networks”, Prentice Hall, 2005.

Bluetooth

- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba - many other members
- Scenarios:
  - connection of peripheral devices
    - loudspeaker, joystick, headset
  - support of ad-hoc networking
    - small devices, low-cost
  - bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop

- Simple, cheap, replacement of IrDA, low range, lower data rates, low-power
  - Worldwide operation: 2.4 GHz,
  - Resistance to jamming and selective frequency fading:
    - FHSS over 79 channels (of 1MHz each), 1600hops/s
  - Coexistence of multiple piconets: CDMA
  - Links: synchronous connections SCO (e.g., voice) and asynchronous connectionless ACL
  - Interoperability: protocol stack supporting TCP/IP, OBEX, SDP
  - Range: 10 meters, can be extended to 100 meters
- Documentation: over 1000 pages specification:
- www.ccs.neu.edu/course/com3525/ or from www.bluetooth.com

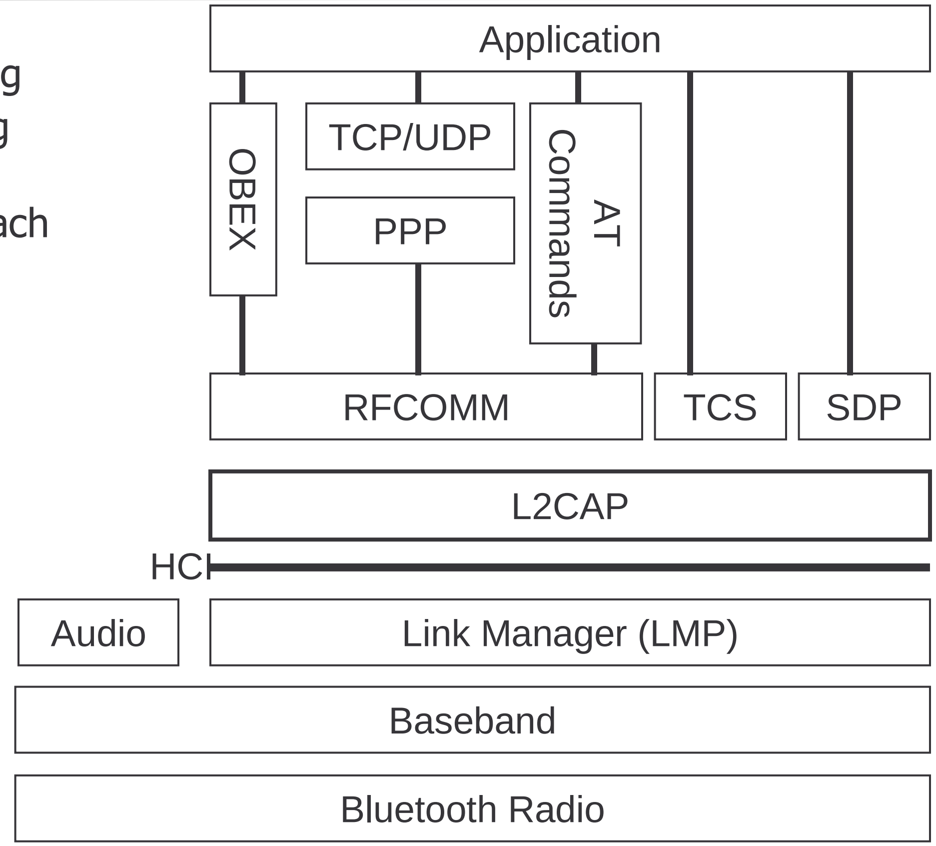
Network Topology



- Piconet = set of Bluetooth nodes synchronized to a master node
  - The piconet hopping sequence is derived from the master MAC address (BD_ADDR IEEE802 48 bits compatible address)
- Scatternet = set of piconet
- Master-Slaves can switch roles
- A node can only be master of one piconet. Why?

Protocol Architecture

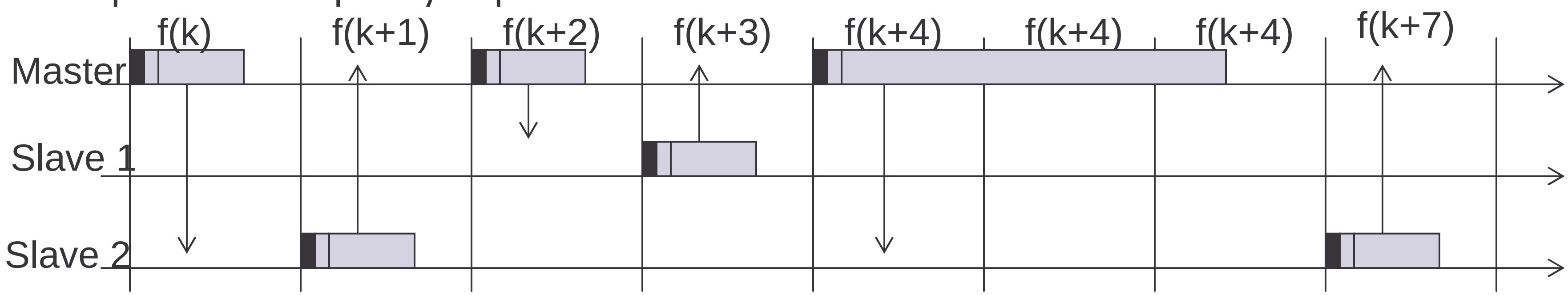
- **BT Radio** (2.4 GHZ Freq. Band):
- Modulation: Gaussian Frequency Shift Keying
- **Baseband**: FH-SS (79 carriers), CDMA (hopping sequence from the node MAC address)
- **Audio**: interfaces directly with the baseband. Each voice connection is over a 64Kbps SCO link. The voice coding scheme is the Continuous Variable Slope Delta (CVSD)
- Link Manager Protocol (**LMP**): link setup and control, authentication and encryption
- Host Controller Interface: provides a uniform method of access to the baseband, control registers, etc through USB, PCI, or UART
- Logical Link Control and Adaptation Layer (**L2CAP**): higher protocols multiplexing, packet segmentation/reassembly, QoS
- Service Discover Protocol (**SDP**): protocol of locating services provided by a Bluetooth device
- Telephony Control Specification (**TCS**): defines the call control signaling for the establishment of speech and data calls between Bluetooth devices
- **RFCOMM**: provides emulation of serial links (RS232). Upto 60 connections



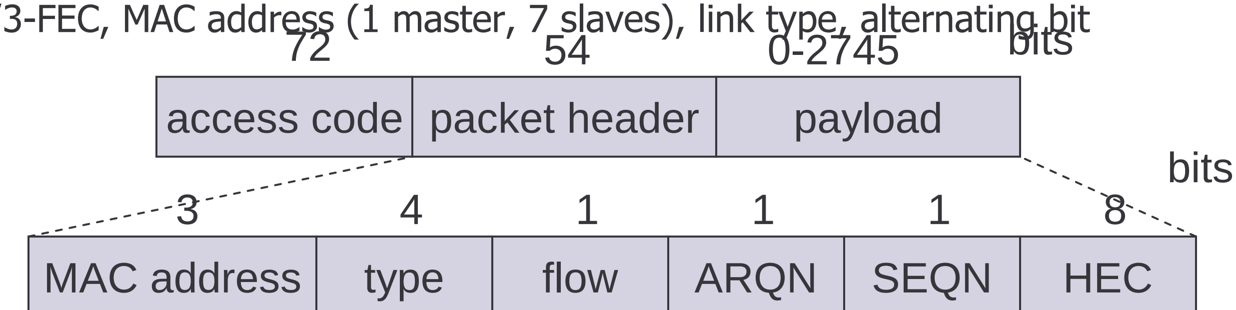
OBEX: OBject EXchange (e.g., vCard)

Bluetooth Piconet MAC

- Each node has a Bluetooth Device Address (BD_ADDR). The master BD_ADDR determines the sequence of frequency hops



- Types of connections:
  - Synchronous Connection-Oriented link (**SCO**) (symmetrical, circuit switched, point-to-point)
  - Asynchronous Connectionless Link (**ACL**): (packet switched, point-2-multipoint, master-polls)
- Packet Format:
  - Access code: synchronization, when piconet active derived from master
  - Packet header (for ACL): 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Types of packets

- SCO packets: Do not have a CRC (except for the data part of DV) and are never retransmitted. Intended for High-quality Voice (HV).

Type	Payload (bytes)	FEC	CRC	Symm. max-rate kbps
HV1	10	1/3	No	64
HV2	20	2/3	No	64
HV3	30	No	No	64
DV	10+(1-10)D	2/3D	Yes D	64+57.6D

- ACL packets: Data Medium-rate (DM) and Data High-rate (DH)

Type	Payload (bytes)	FEC	CRC	Symm. max-rate kbps	Asymm. max-rate (DL/UL)
DM1	0-17	2/3	Yes	108.8	108.8/108.9
DM3	0-121	2/3	Yes	258.1	387.2/54.4
DM5	0-224	2/3	Yes	286.7	477.8/36.3
DH1	0-27	No	Yes	172.8	172.8/172.8
DH3	0-183	No	Yes	390.4	585.6/86.4
DH5	0-339	No	Yes	433.9	723.2/185.6

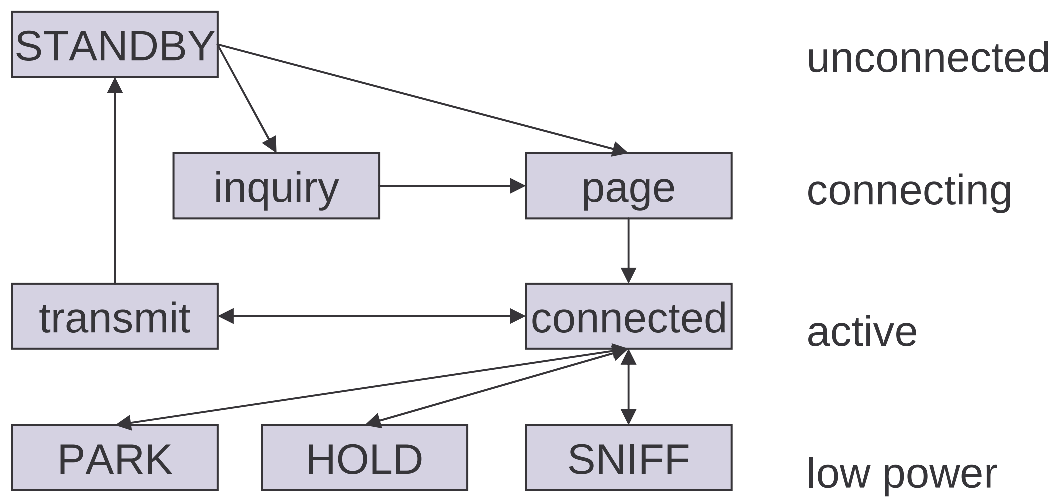
States of a Bluetooth Device (PHY layer)

ACTIVE (connected/transmit): the device is uniquely identified by a 3bits AM_ADDR and is fully participating

SNIFF state: participates in the piconet only within the SNIFF interval

HOLD state: keeps only the SCO links

PARK state (low-power): releases AM_ADDR but stays synchronized with master



BT device addressing:
- BD_ADDR (48 bits)
- AM_ADDR (3bits): ACTIVE, HOLD, or SNIFF
- PM_ADDR (8 bits): PARK Mode address (exchanged with the AM_ADDR when entering PARK mode)
- AR_ADDR (8 bits): not unique used to come back from PARK to ACTIVE state

Bluetooth Device Operation [Page 105 of 1084]

- Inquiry:
  - Goal: aims at discovering other neighboring devices
  - Inquiring node:
    - Sends an inquiry message (packet with only the access code: General Inquiry Access Code: GIAC or Dedicated IAC: DIAC). This message is sent over a subset of all possible frequencies.
    - The inquiry frequencies are divided into two hopping sets of 16 frequencies each.
    - In inquiry state the node will send upto $N_{INQUIRY}$ sequences on one set of 16 frequencies before switching to the other set of 16 frequencies. Upto 3 switches can be executed. Thus the inquiry may last upto 10.24 seconds.
  - To be discovered node:
    - Enters an inquiry_scan mode: listens over one frequency for $T_{w\_inquiry\_scal}$ time
    - When hearing the inquiry_message (and after a backoff procedure) enter an inquiry_response mode: send a Frequency Hop Sync (FHS) packet (BD_ADDR, native clock)
  - After discovering the neighbors and collecting information on their address and clock, the inquiring node can start a page routine to setup a piconet

Bluetooth Device Operation (Cont'd) [Page 102 of 1084]

- Page:
  - Goal: e.g., setup a piconet after an inquiry
  - Paging node (master):
    - Sends a page message (i.e., packet with only Device Access Code of paged node) over 32 frequency hops (from DAC and split into 2*16 freq.)
    - Repeated until a response is received
    - When a response is received send a FHS message to allow the paged node to synchronize
  - Paged node (slave):
    - Listens on its hopping sequence
    - When receiving a page message, send a page_response and wait for the FHS of the pager

Link Manager Protocol

- Security: shared secret key
  - Authentication: challenge response
  - Weak Encryption: combination of (Linear Feedback Shift Registers) LFSR

- Connections setup/release (SCO/ACL)
- Master-slave switch
- Power-control
- Scheduling

Scatternets

- Each piconet has one master and up to 7 slaves
- Master determines hopping sequence, slaves have to synchronize
- Participation in a piconet = synchronization to hopping sequence
- Communication between piconets = devices jumping back and forth between the piconets