Mobilkommunikation - Mobile Communications

Lecture 9: Bluetooth

Prof. Dr.-Ing. Markus Fidler

Institute of Communications Technology
Leibniz Universität Hannover

June 24, 2016

Previous lecture: WLAN

Wireless local area networks (WLAN)

- IEEE 802.11
- 2.4 GHz and 5 GHz ISM bands
- gross data rate up to 600 Mb/s and beyond
- infrastructure mode but also ad-hoc mode possible
- application: replace wiring and support (nomadic) mobility
  - at home
  - in the office
  - on campus
- range
  - indoor: 30 m
  - outdoor: 300 m

Bluetooth

- IEEE 802.15.1 PHY and MAC
- 2.4 GHz ISM band
- piconets, range of 10 m or less
- gross data rate 1 Mb/s and beyond
- ad-hoc communication
- small low cost devices, less than 5 €
- application: replace wiring and provide easy ad-hoc connectivity, e.g.
  - mobile phone to hands-free equipment e.g. earphone, car
  - mobile phone to computer
  - wii and playstation 3 controller

Outline

Bluetooth
- Architecture
- Radio layer
- Baseband layer
- Link manager protocol
- Logical link control and adaptation protocol (L2CAP)

Outlook: IEEE 802.15 WPAN standards

History

Bluetooth

- 1994: Ericsson started studies on a so-called multi-communicator link
  - the project was renamed Bluetooth later after
  - Harald "Blåtand" Gormsen, king of Denmark, 10th century
- 1998: Bluetooth consortium founded
  - by Ericsson, Intel, IBM, Nokia, Toshiba
  - goal: single-chip, low-cost, radio-based network technology
- 2001: first mass market products

IEEE 802.15.1

- at the same time the IEEE 802.11 working group started to investigate WPANs
- IEEE founded the 802.15 working group for WPANs
- close cooperation with Bluetooth consortium: 802.15.1

Characteristics

- 2.4 GHz ISM band
- channels with 1 MHz carrier spacing
  79 channels from 2402 to 2480 MHz
- Gaussian frequency shift keying (GFSK) modulation
- time division duplexing (TDD) for send/receive separation
- frequency hopping spread spectrum (FHSS)
  - 1600 hops/second
  - different pseudo random hopping sequence (FH-CDMA)
- piconets
  - different piconets are separated by different pseudo random hopping sequences
  - master/slave configuration
  - hopping sequence is determined by the master
  - each piconet has a gross capacity of < 1 Mb/s (Bluetooth 1.x)

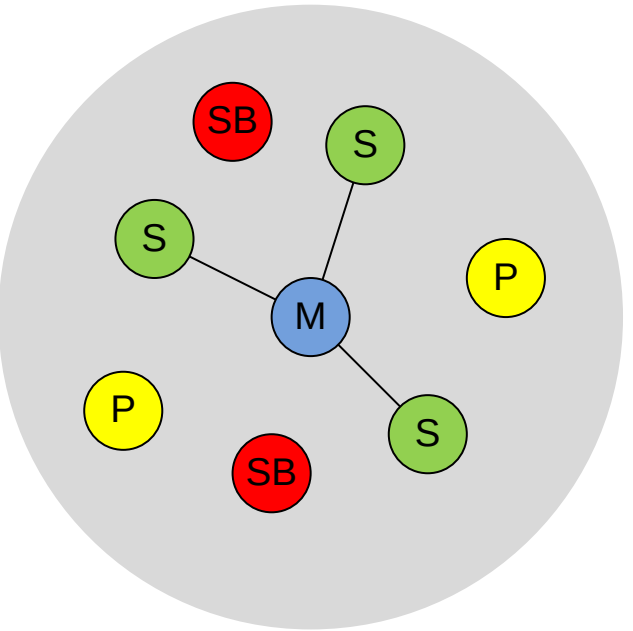
Piconets

Piconet: collection of connected devices

- each piconet has a unique hopping sequence
  - one master, up to seven slaves ($>$ 200 can be parked)
  - master determines pseudo random hopping sequence
  - slaves have to synchronize to the hopping sequence
  - participation in a piconet is by synchronization

Devices can be in any of four states

- M: master
- S: slave
- P: parked
  - not actively participating
  - but known to the piconet
  - can be activated shortly
- SB: standby



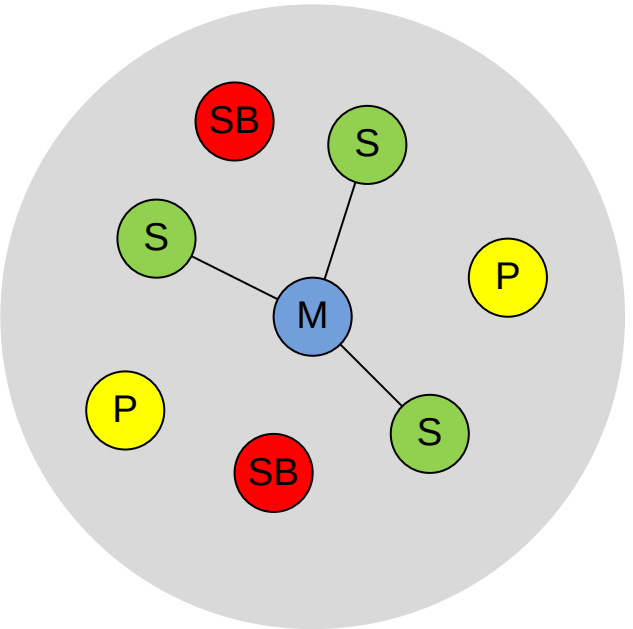
Forming a piconet

All devices in a piconet hop together

- master provides its clock and its device identifier to slaves
  - device ID: 48 bit, worldwide unique
  - the device ID determines the unique hopping sequence
  - the phase in the hopping sequence is determined by the clock

Addressing

- AMA: active member address
  - 3 bit
  - 7 slaves
- PMA: passive member address
  - 8 bit
  - $>$ 200 parked

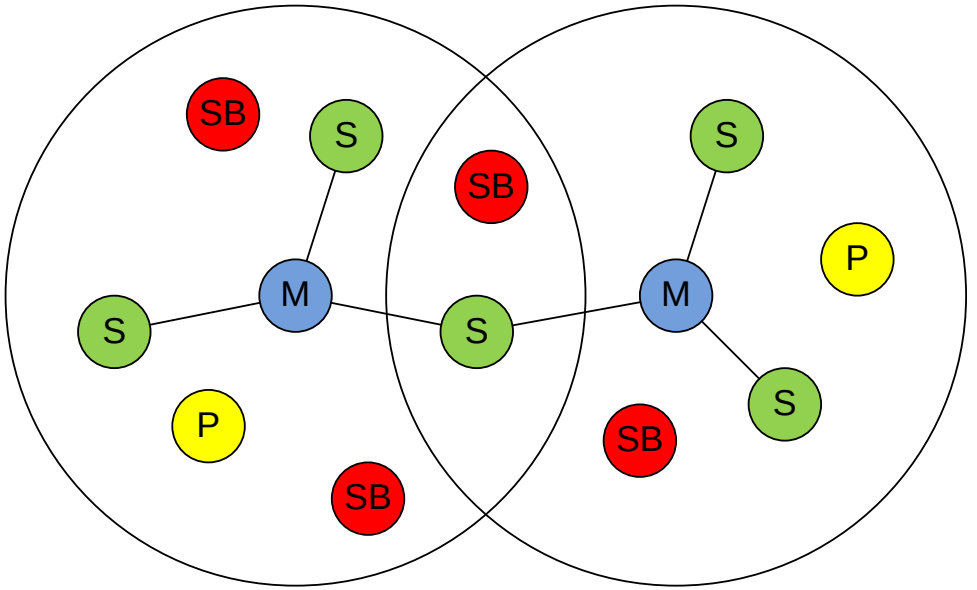


Scatternets

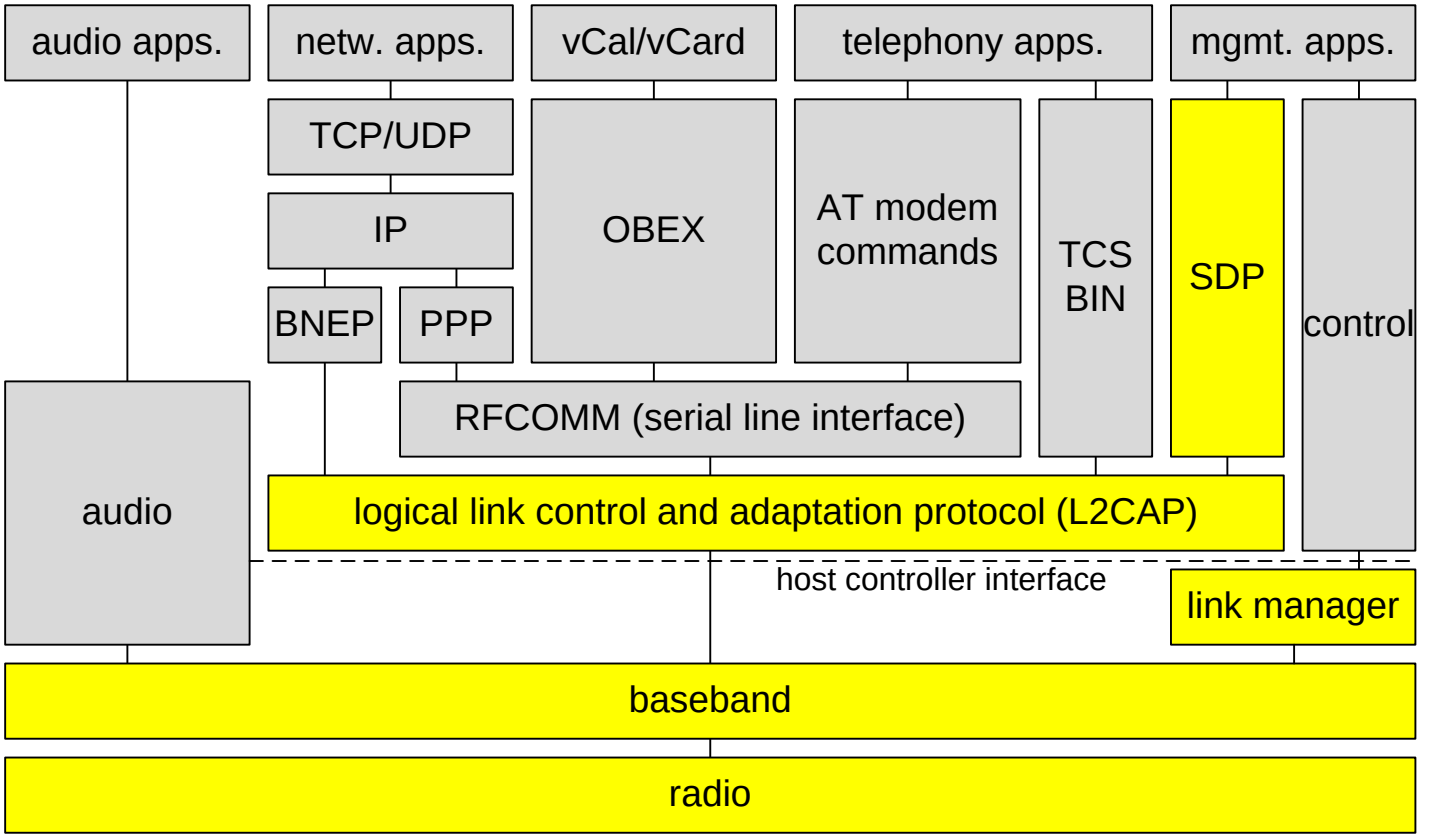
Scatternet: co-located piconets that share a common device

- common device can be
  - slave in both piconets
  - master in one and slave in another piconet
  - why can a device not be master of two piconets?
- communication between piconets
  - devices jump back and forth between piconets

- M: master
- S: slave
- P: parked
- SB: standby



Protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM radio frequency comm.

Protocol stack continued

Bluetooth core protocol specification

- **radio:** air interface, i.e. frequencies, modulation, transmit power
- **baseband:** connection establishment, packet formats, timing, hopping, automatic repeat request, channels, quality of service
- **link manager protocol (LMP):** link setup and management between devices, security
- **logical link control and adaptation protocol (L2CAP):** adaptation layer, connectionless or connection-oriented
- **service discovery protocol (SDP):** device discovery, querying service characteristics

Host controller interface (HCI)

- command interface
- can be viewed as hardware/software boundary

Protocol stack continued

Profile specifications (adaptation of Bluetooth to legacy apps.)

- **audio:** encoded audio signals are directly supported by the baseband layer
- **telephony control protocol specification - binary (TCS BIN):** call control signalling for voice and data calls
- **radio frequency comm. (RFCOMM):** emulates a serial line interface (RS-232), allows Bluetooth to act as a cable replacement
  - **AT modem commands:** telephony applications can use standard modem commands
  - **object exchange protocol (OBEX):** exchange of calender and business card objects (as in IrDA)
  - **point-to-point protocol (PPP):** Internet applications running over the TCP/IP stack
- **Bluetooth network encapsulation protocol (BNEP):** more efficient than PPP

Radio layer

Specification (ten pages) of carrier frequency and transmit power

Requirements for Bluetooth radio interface

- low power consumption, size, weight, prize
- world-wide usage

Characteristics

- 2.4 GHz ISM band, GFSK modulation
- TDD, FHSS with FH-CDMA
- 79 carriers with 1 MHz spacing
- 1600 hops/second, 625 μs time slots
- 3 power classes
  - class 1: 1...100 mW with power control, up to 100 m range
  - class 2: 0.25...2.5 mW, typically 10 m range
  - class 3: less than 1 mW, about 1 m range

Baseband layer

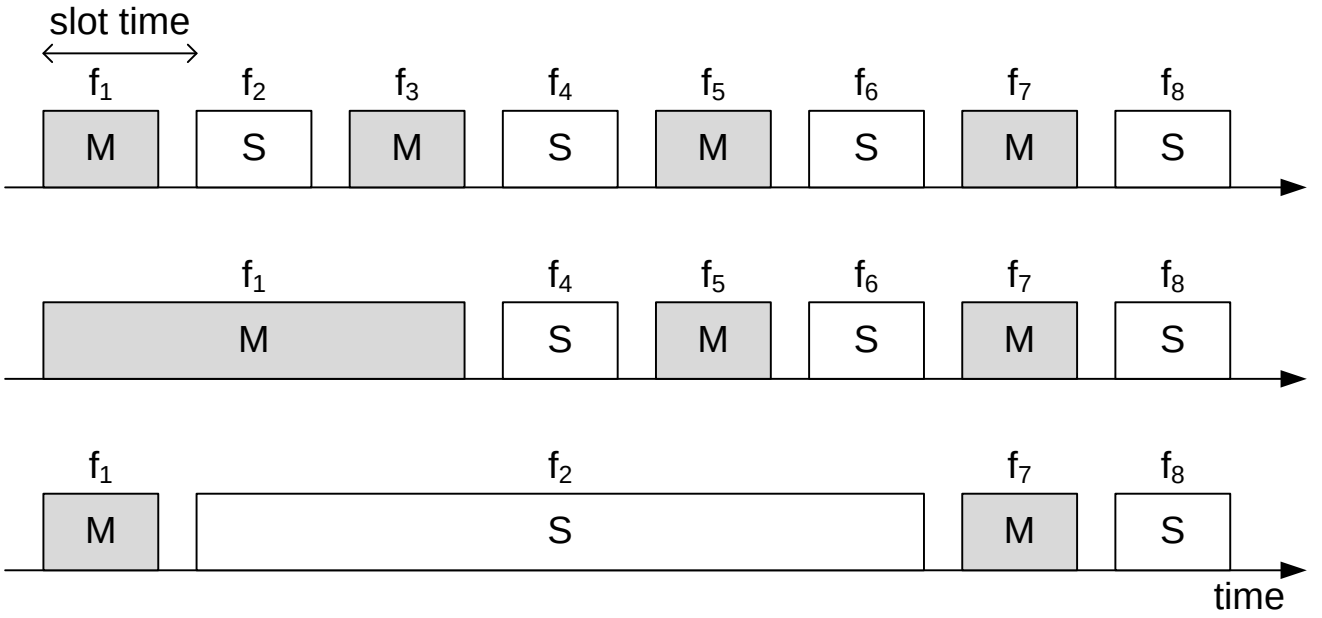
Complex functionality

- frequency hopping for
  - interference mitigation
  - medium access
- definition of physical links
- many packet formats

Basic principle: FH-CDMA

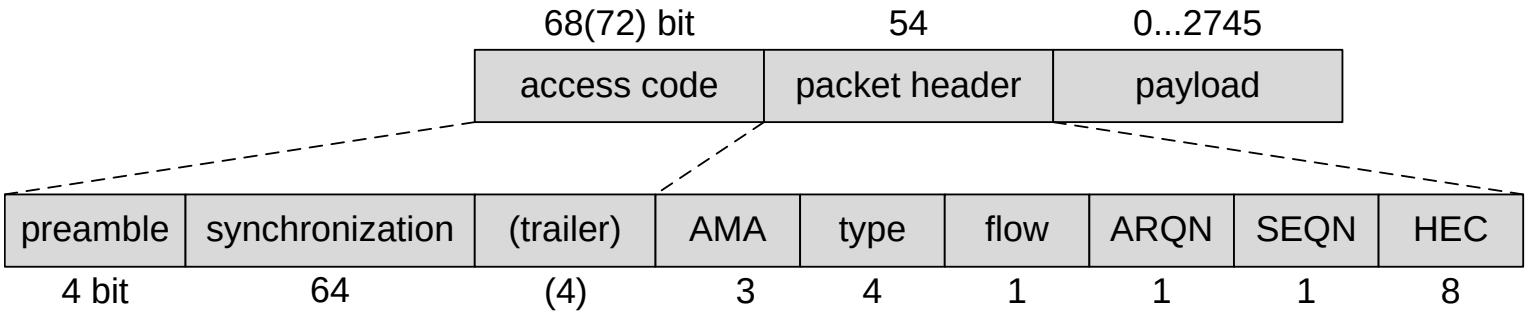
- each piconet uses a unique hopping sequence
- the hopping sequences of several piconets can overlap, i.e. devices that belong to different piconets may transmit at the same time on the same frequency (no carrier sense is used)
  - result: interference and possibly collisions
  - however, usually only a small number of slots are affected
  - Bluetooth uses a fast retransmit mechanism
  - at the time of the retransmission stations have hopped again

Transmission scheme



- frequency hopping sequence f_i
- master's and slaves' transmissions alternate (TDD)
- 1-, 3-, and 5-slot packets for higher data rates
  - frequency hopping is suspended for the duration of a packet
  - frequency hopping is resumed afterwards using the original sequence (otherwise the piconet would break apart)

Baseband packet format



- access code
  - e.g. derived from the master's globally unique 48-bit address
- packet header
  - 3-bit active member address (AMA) of a slave
    - slave is either source or destination (all communication is via the master)
  - 4-bit type field determines the type of the packet
  - 1-bit flow for flow control (if flow=0 transmission must stop)
  - 1-bit sequence number (SEQN) and ack. number (ARQN)
    - alternating bit protocol (stop and wait ARQ)
  - 8-bit header error check (HEC)
  - one third rate forward error correction (FEC), i.e. plus 36 bit

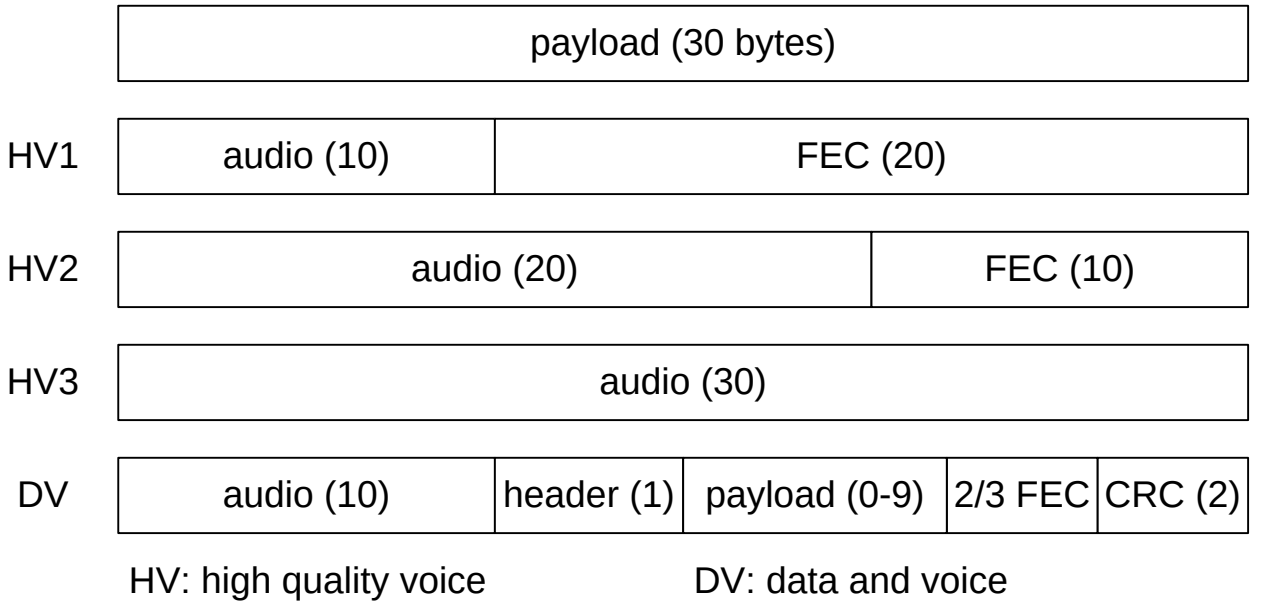
Physical links

- **synchronous connection-oriented link (SCO):**
  - for classical telephone (voice) connections
  - symmetrical, circuit-switched point-to-point connection
  - master reserves two consecutive time slots at fixed intervals (forward and reverse)
  - can use forward error correction (FEC)
  - does not use automatic repeat request (ARQ)
- **asynchronous connectionless link (ACL):**
  - for data applications
  - symmetrical or asymmetrical packet-switched traffic
  - point-to-point or point-to-multipoint communications
  - the master uses a polling scheme, clients may only answer if polled in the preceding slot
  - can use forward error correction (FEC)
  - uses fast automatic repeat request (ARQ)
  - can use multi-slot packets

SCO payload types

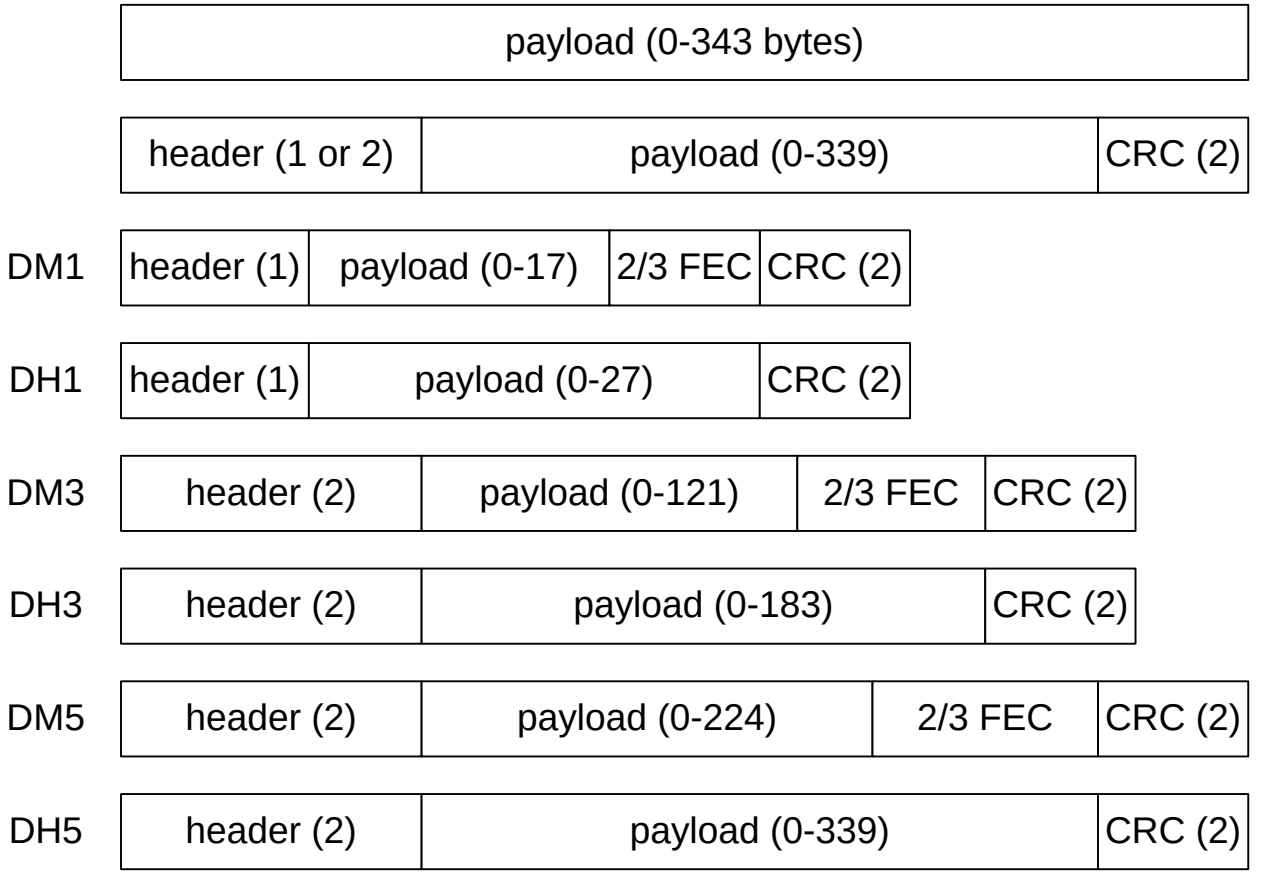
Synchronous connection-oriented link payload types

- voice data at 64 kb/s
- FEC: no, 2/3, or 1/3



ACL payload types

Asynchronous connectionless link payload types



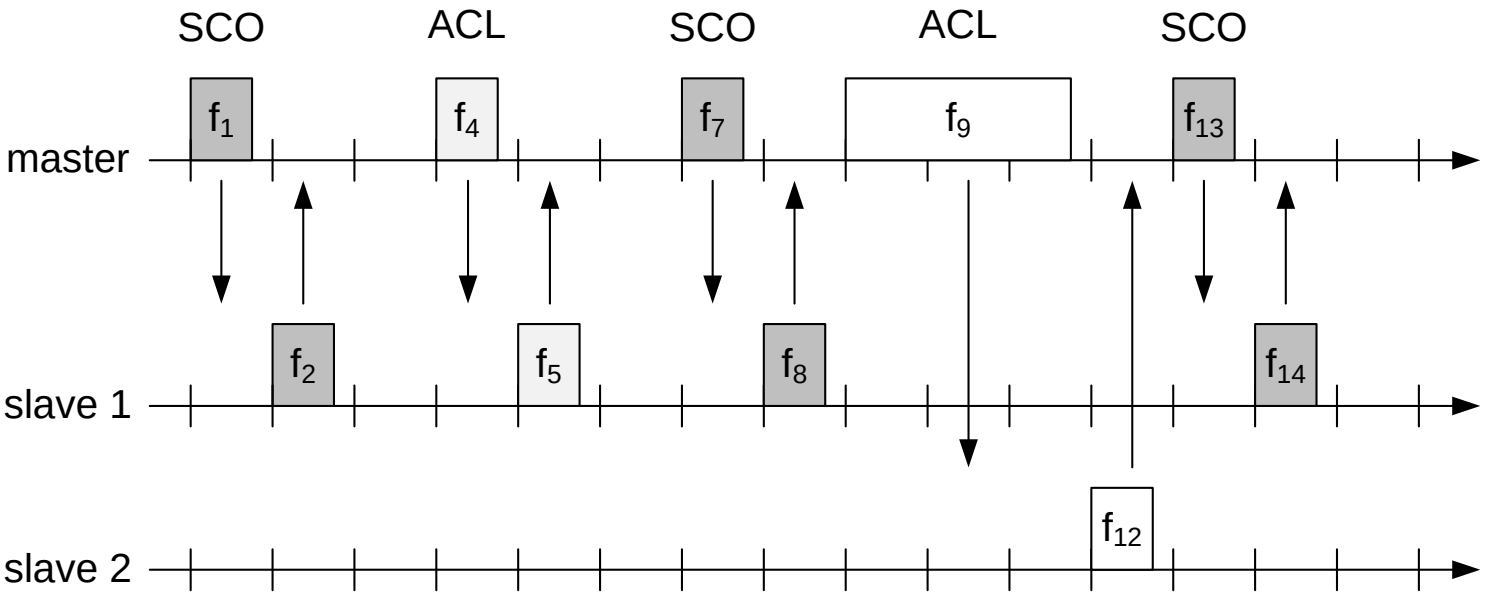
DM: data medium rate
1,3, or 5 slot packets

DH: data high rate

Baseband data rates

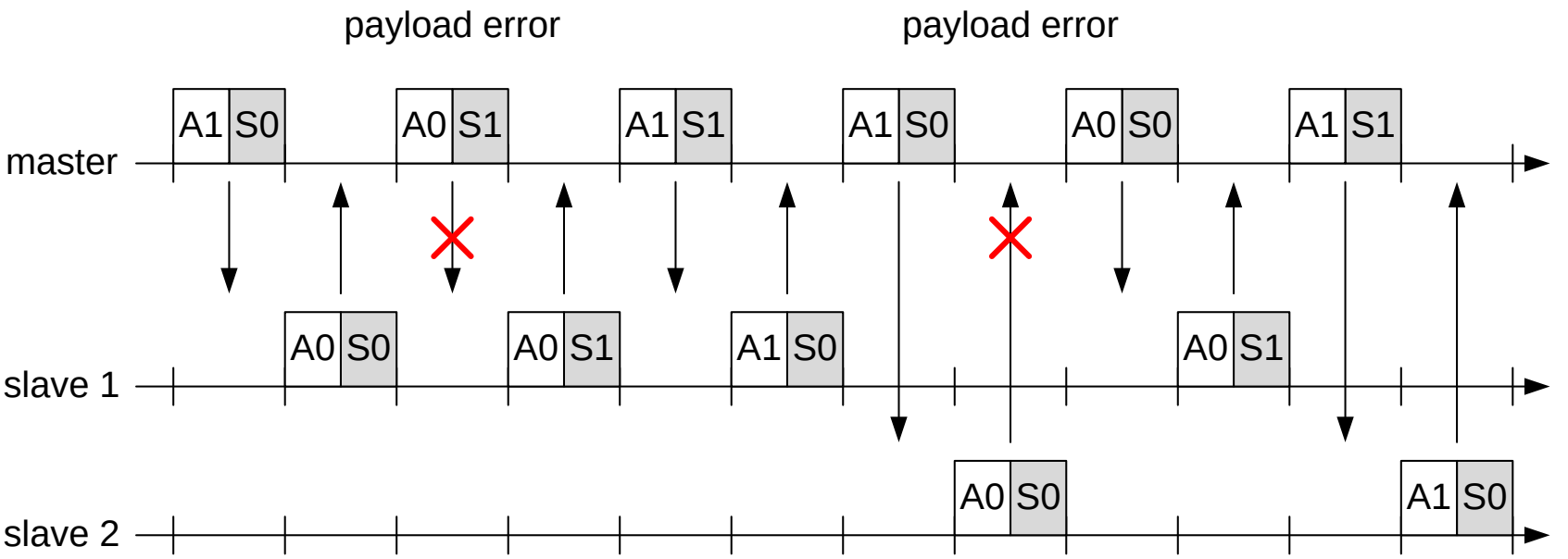
type	payload header [byte]	user payload [byte]	FEC	CRC	symmetric max rate [kb/s]	asymmetric forward [kb/s]	asymmetric reverse [kb/s]
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
HV1	-	10	1/3	no	64.0	-	-
HV2	-	20	2/3	no	64.0	-	-
HV3	-	30	no	no	64.0	-	-

Example: data transmission



- TDD with 625 μs slots: master polls slaves
- synchronous connection-oriented (SCO): periodic single-slot assignment with 64 kb/s
- asynchronous connectionless (ACL): variable packet size with 1, 3, or 5 slot packets

Example: automatic repeat request

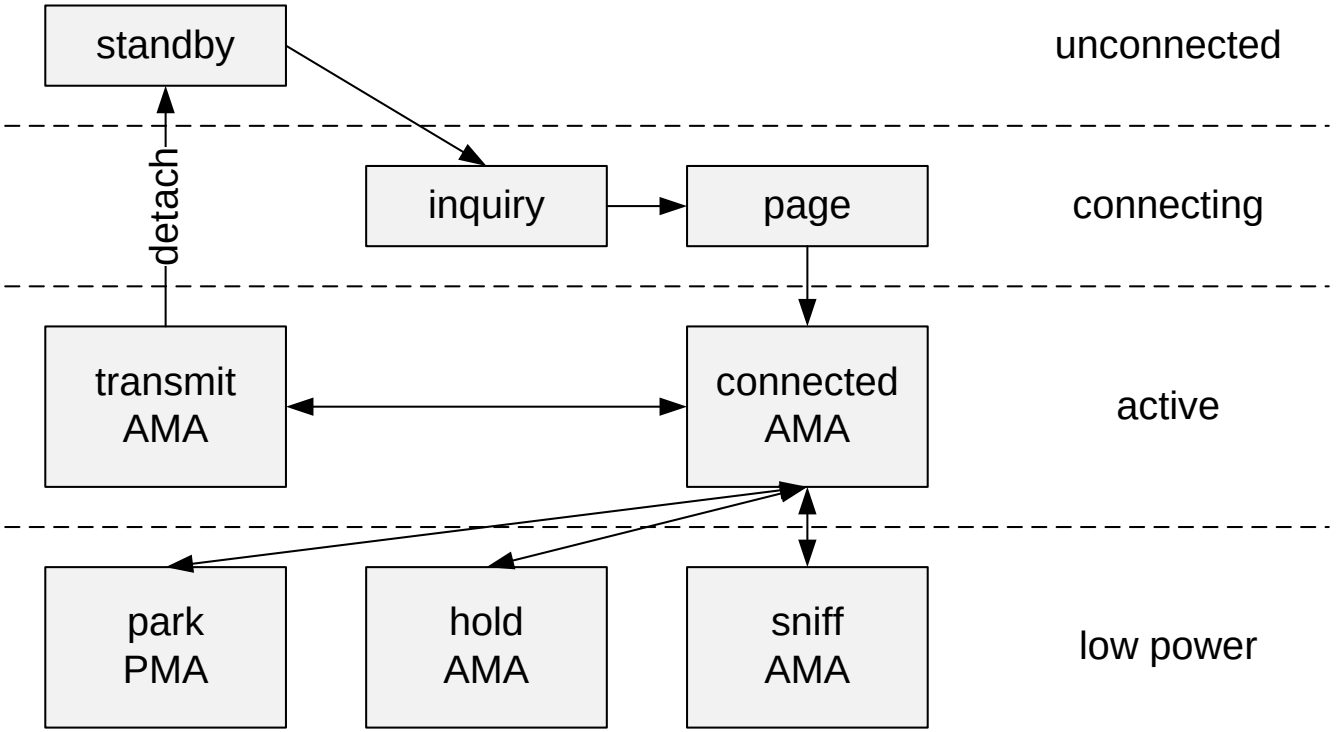


- header uses 1/3 rate FEC
- ACL payload uses CRC plus 2/3 FEC or no FEC
- fast ARQ with alternating bit protocol:
  - ARQN: 1 bit acknowledgement number
  - SEQN: 1 bit sequence number

Link manager protocol (LMP)

- **pairing, authentication, and encryption:** pairing establishes a trust relationship between devices that have never communicated before resulting in a link key that is used as input for authentication and encryption
- **synchronization:** adjust clock offset upon packet reception
- **capability negotiation:** not all devices support all features, e.g. multi-slot packets
- **quality of service negotiation:** e.g. the poll interval determines latency and throughput
- **power control:** depending on the receive power the receiver may request the sender to adapt its send power
- **link supervision:** e.g. setup of SCO links
- **state and transmission mode changes:** e.g. attach to, detach from a piconet; switch master/slave role

State transition diagram



- AMA: 3-bit active member address
- PMA: 8-bit passive member address

State transition diagram continued

- **standby:** any device that is not participating in a piconet
- **inquiry:** devices that want to establish or join a piconet
  - a master that wants to establish a piconet repeatedly sends a specific inquiry access code (IAC) on so-called wake-up carriers
  - a slave that wants to join a piconet periodically searches for IAC messages on the wake-up carriers and if it receives an IAC message it returns its address and timing information
- **page:** after successful inquiry the master pages each slave on its specific hopping sequence; the slaves synchronize with the master and start using the master's hopping sequence
- **connected:** synchronized devices (after paging)
  - **sniff:** device listens to the piconet at reduced rate
  - **hold:** device stops ACL transmissions but may still use SCO
  - **park:** device releases its AMA and receives a PMA; wakes up at certain beacon intervals to stay synchronized

Inquiry

Which hopping sequence has to be used for inquiry?

- usually the hopping sequence is determined from device identifiers
- devices do, however, not yet know each other
- specific hopping sequences (using 32 channels) for
  - inquiry and
  - inquiry response

Which phase (reference clock) has to be used for hopping?

- usually the clocks are synchronized to one reference clock
- clocks are, however, not yet synchronized during inquiry
- devices use different speed for hopping
  - master hops after 312.5 μs
  - slave hops after 1.28 s

Power consumption

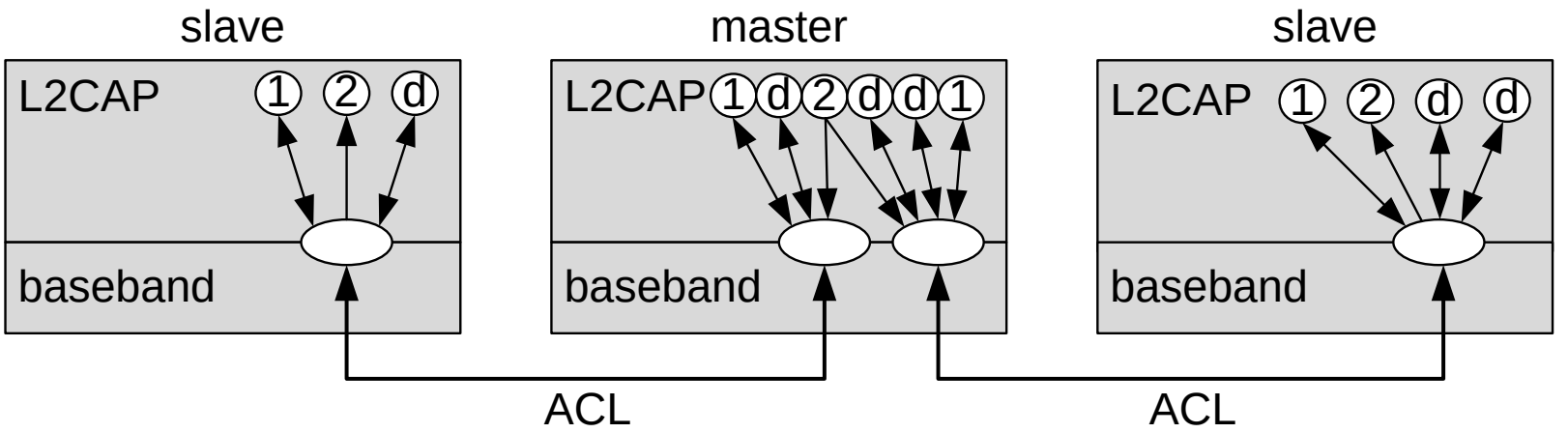
operating mode	average current [mA]
SCO, HV1	53
SCO, HV3	26
ACL, 723.2 kb/s	53
ACL, 115.2 kb/s	15.5
ACL, 38.4 kb/s, 40 ms interval sniff mode	4
park mode, 1.28 s beacon interval	0.6
standby	0.047

Logical link control and adaptation protocol (L2CAP)

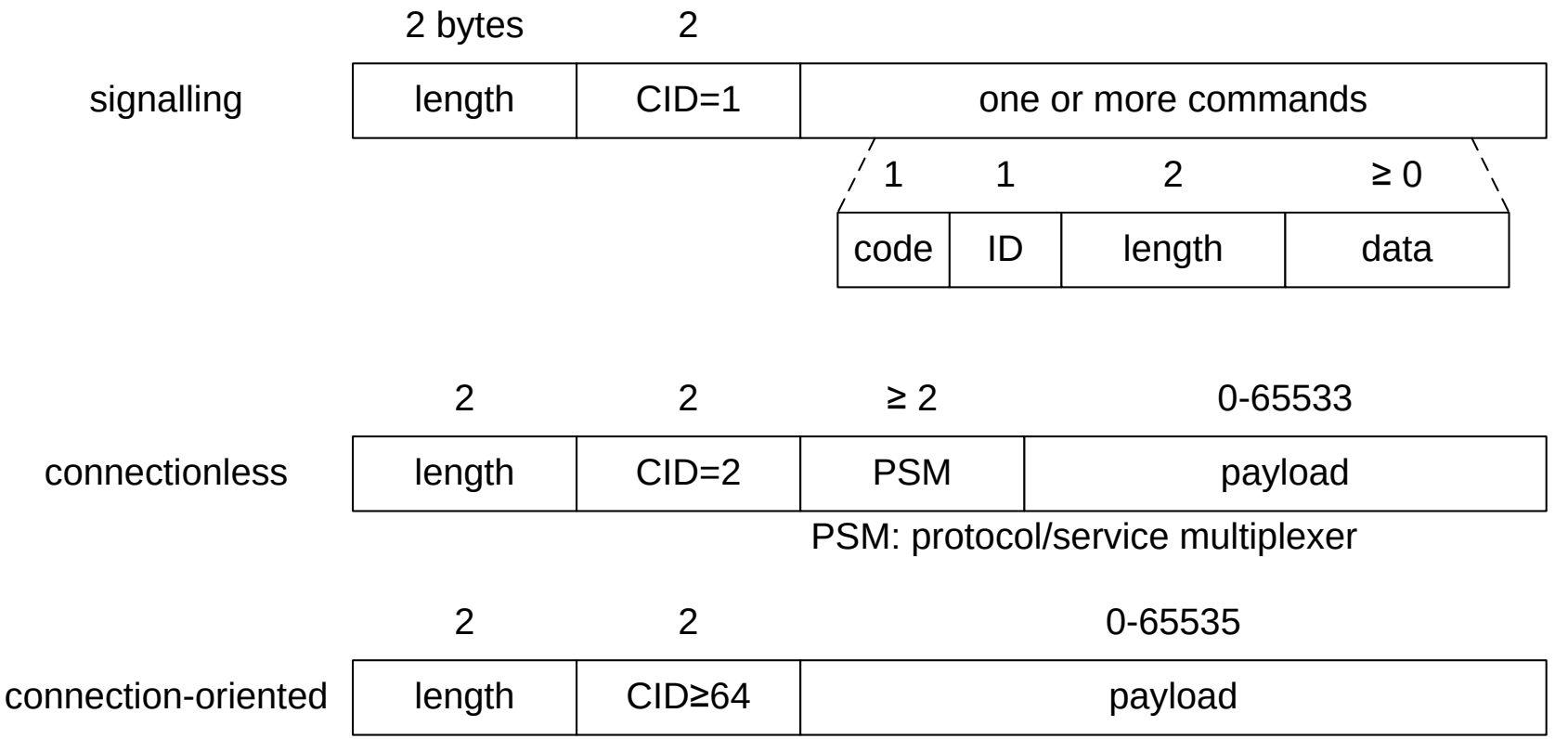
Simple data link protocol on top of the baseband layer

- provides logical channels with unique channel identifier (CID)
  - signaling: CID 1
  - connectionless: broadcast from master to slaves, CID 2
  - connection-oriented: bi-directional with QoS (RFC 1363), CID ≥ 64 (CID $= 3...63$ are reserved)
- protocol multiplexing: e.g. RFCOMM, SDP, etc.
- segmentation and reassembly:
  - L2CAP data units have up to 64 kbyte user data
  - baseband packets carry at most 339 byte user data

Logical channels



Packet format



IEEE 802.15 family of WPAN standards

IEEE 802.15 working groups

- 1: PHY and MAC as used by Bluetooth
- 2: Coexistence of Bluetooth 802.11 WLAN
  - both operate in the 2.4 GHz ISM band
  - interference model
- 3: high bit rates of more than 100 Mb/s
  - 3a: ultra wide band (UWB)
- 4: PHY and MAC as used by ZigBee
  - low data rate, tens of kb/s
  - low complexity
  - multi-month up to multi-year battery life
  - application: sensors, remote control, smart badges etc.
- 5: WPAN mesh networking, i.e. interconnection of WPANs
- 6: body area networks (BAN)
- 7: visible light communications (VLC)

Literature

- Jochen Schiller, Mobile Communications, Second Edition, Addison-Wesley, 2003.