Bluetooth

Acknowledgements

- Based on Jochen Schiller slides

- Supporting text
  » Jochen Schiller, “Mobile Communications”, Addison-Wesley
  » Section 7.5 – Bluetooth
**Bluetooth**

» Universal radio interface for ad-hoc wireless connectivity
» Interconnecting
  
  computer and peripherals, handheld devices, PDAs, cell phones
» Embedded in other devices, goal: 5€/device
» Short range (10 m), low power consumption, license-free 2.45 GHz ISM
» Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).

**Characteristics**

♦ 2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing
  
  – Channel 0: 2402 MHz … channel 78: 2480 MHz
  – G-FSK modulation, 1-100 mW transmit power

♦ FHSS and TDD
  
  – Frequency hopping with 1600 hops/s
  – Hopping sequence in a pseudo random fashion, determined by a master
  – Time division duplex

♦ Voice link – SCO (Synchronous Connection Oriented)
  
  – FEC, no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

♦ Data link – ACL (Asynchronous ConnectionLess)
  
  – Asynchronous, fast acknowledge, point-to-multipoint,
  – Up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

♦ Topology
  
  – Overlapping piconets (stars) forming a scatternet
Piconet

- Collection of devices connected in an ad hoc
- One unit acts as master
  the others as slaves, for the lifetime of the piconet
- Master determines hopping pattern
  each piconet has a unique hopping pattern
  hopping pattern determined by device ID
    48 bit, unique worldwide
  slaves have to synchronize
- Each piconet has
  one master
  up to 7 simultaneous slaves
  Active Member Address: AMA, 3 bit
  200 could be parked
  Parked Member Address: PMA, 8 bit

Scatternet

- Linking multiple co-located piconets
  through the sharing of common master or slave devices

Piconets
(each with a capacity of
< 1 Mbit/s)
Bluetooth Protocol Stack

**Audio**
- Audio apps.
- NW apps.
- vCal/vCard
- TCP/UDP
- IP
- BNEP
- PPP
- RFCOMM (serial line interface)

**Baseband**
- Logical Link Control and Adaptation Protocol (L2CAP)

**Radio**
- Link Manager
- Host Controller Interface

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.

Frequency Selection during Data Transmission

625 µs

\[
\begin{array}{cccccccc}
& f_k & f_{k+1} & f_{k+2} & f_{k+3} & f_{k+4} & f_{k+5} & f_{k+6} \\
M & S & M & S & M & S & M \\
\end{array}
\]

\[
\begin{array}{cccccccc}
& f_k & f_{k+3} & f_{k+4} & f_{k+5} & f_{k+6} \\
M & S & M & S & M \\
\end{array}
\]

\[
\begin{array}{cccccccc}
& f_k & f_{k+1} & f_{k+6} \\
M & S & M \\
\end{array}
\]
Baseband

- Low-level packet definition
  - Access code
  - Packet header
    1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum

SCO Payload Types

```
payload (30)
HV1  audio (10)  FEC (20)
HV2  audio (20)  FEC (10)
HV3  audio (30)  
DV   audio (10)  header (1)  payload (0-9)  2/3 FEC  CRC (2)  
```
ACL Payload types

<table>
<thead>
<tr>
<th>ACL</th>
<th>Type</th>
<th>Payload Header [byte]</th>
<th>User Payload [byte]</th>
<th>FEC</th>
<th>CRC</th>
<th>Symmetric max. Rate [kbit/s]</th>
<th>Asymmetric max. Rate [kbit/s]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Forward</td>
<td>Reverse</td>
</tr>
<tr>
<td>1 slot</td>
<td>DM1</td>
<td>1</td>
<td>0-17</td>
<td>2/3</td>
<td>yes</td>
<td>108.8</td>
<td>108.8</td>
</tr>
<tr>
<td></td>
<td>DH1</td>
<td>1</td>
<td>0-27</td>
<td>no</td>
<td>yes</td>
<td>172.8</td>
<td>172.8</td>
</tr>
<tr>
<td>3 slot</td>
<td>DM3</td>
<td>2</td>
<td>0-121</td>
<td>2/3</td>
<td>yes</td>
<td>258.1</td>
<td>387.2</td>
</tr>
<tr>
<td></td>
<td>DH3</td>
<td>2</td>
<td>0-183</td>
<td>no</td>
<td>yes</td>
<td>390.4</td>
<td>585.6</td>
</tr>
<tr>
<td>5 slot</td>
<td>DM5</td>
<td>2</td>
<td>0-224</td>
<td>2/3</td>
<td>yes</td>
<td>286.7</td>
<td>477.8</td>
</tr>
<tr>
<td></td>
<td>DH5</td>
<td>2</td>
<td>0-339</td>
<td>no</td>
<td>yes</td>
<td>433.9</td>
<td>723.2</td>
</tr>
<tr>
<td></td>
<td>AUX1</td>
<td>1</td>
<td>0-29</td>
<td>no</td>
<td>no</td>
<td>185.6</td>
<td>185.6</td>
</tr>
<tr>
<td></td>
<td>HV1</td>
<td>na</td>
<td>10</td>
<td>1/3</td>
<td>no</td>
<td>64.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HV2</td>
<td>na</td>
<td>20</td>
<td>2/3</td>
<td>no</td>
<td>64.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HV3</td>
<td>na</td>
<td>30</td>
<td>no</td>
<td>no</td>
<td>64.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DV</td>
<td>1 D</td>
<td>10+(0-9) D</td>
<td>2/3 D</td>
<td>yes</td>
<td>D</td>
<td>64.0+57.6 D</td>
</tr>
</tbody>
</table>

Data Medium/High rate, High-quality Voice, Data and Voice
Baseband Link Types

- Polling-based TDD packet transmission
  625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint

Master

Slave 1

Slave 2

Robustness

- Slow frequency hopping with hopping patterns determined by a master
  Protection from interference on certain frequencies
  Separation from other piconets
  Retransmission    ACL only, very fast
- Forward Error Correction
  SCO and ACL

Error in payload
(not header!)

Master

Slave 1

Slave 2
**Baseband States of a Bluetooth Device**

- **Standby**: do nothing
- **Inquire**: search for other devices
- **Page**: connect to a specific device
- **Connected**: participate in a piconet
- **Transmit AMA**
- **Park PMA**
- **Hold AMA**
- **Sniff AMA**
- **Low power**
- **Connecting**
- **Active**
- **Unconnected**

**L2CAP – Logical Link Control and Adaptation Protocol**

- **Simple data link protocol on top of baseband**
- **Connection oriented, connectionless, and signaling channels**
- **Protocol multiplexing**
  - RFCOMM, SDP, telephony control
- **Segmentation & reassembly**
  - Up to 64kbyte user data
- **QoS specification per channel**
  - Delay, jitter, bursts, bandwidth
- **Group abstraction**
  - Create/close group, add/remove member
### L2CAP logical channels

![Diagram of L2CAP logical channels]

### L2CAP packet formats

**Connectionless PDU**

- **2 bytes**
- **CID=2**
- **PSM ≥2**
- **payload 0-65533**

<table>
<thead>
<tr>
<th>length</th>
<th>CID=2</th>
<th>PSM</th>
<th>payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>≥2</td>
<td></td>
</tr>
</tbody>
</table>

**Connection-oriented PDU**

- **2 bytes**
- **CID**
- **payload 0-65535**

<table>
<thead>
<tr>
<th>length</th>
<th>CID</th>
<th>payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Signalling command PDU**

- **2 bytes**
- **CID=1**
- **One or more commands**

<table>
<thead>
<tr>
<th>length</th>
<th>CID=1</th>
<th>One or more commands</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Code**
- **ID**
- **Length**
- **Data ≥0**
Security

- PIN (1-16 byte)
  - $E_2$
  - Link key (128 bit)
  - $E_3$
  - Encryption key (128 bit)
  - Keystream generator
  - Payload key

- User input (initialization)
  - Pairing
  - Authentication key generation (possibly permanent storage)
  - Link key (128 bit)
  - $E_2$
  - Encryption key generation (temporary storage)

- Payload key
  - Ciphering
  - Cipher data

Additional Protocols

- SDP – Service Discovery Protocol
  - Inquiry/response protocol for discovering services in radio proximity
  - Adapted to dynamic environment

- RFCOMM
  - Emulation of a serial port

- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
WPAN: IEEE 802.15-1 – Bluetooth

♦ Data rate
  » Synchronous, connection-oriented
    – 64 kbit/s
  » Asynchronous, connectionless
    – 433.9 kbit/s symmetric
    – 723.2 / 57.6 kbit/s asymmetric

♦ Transmission range
  – 10 m
  – 100 m, with special transceivers
  – Frequency 2.4 GHz ISM-band

♦ Connection set-up time
  – Depends on power-mode
  – max. 2.56s, avg. 0.64s

♦ Quality of Service
  – guarantees, ARQ/FEC

WPAN: IEEE 802.15 – future developments 1

♦ 802.15-2: Coexistance
  – Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

♦ 802.15-3: High-Rate
  – Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  – Data Rates: 11, 22, 33, 44, 55 Mbit/s
  – Quality of Service isochronous protocol
  – Ad hoc peer-to-peer networking
  – Security
  – Low power consumption
  – Low cost
  – Designed to meet the demanding requirements of portable consumer imaging and multimedia applications
WPAN: IEEE 802.15 – future developments 2

♦ 802.15-4: Low-Rate, Very Low-Power
  – Low data rate solution with multi-month to multi-year battery life and very low complexity
  – Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
  – Data rates of 20-250 kbit/s, latency down to 15 ms
  – Master-Slave or Peer-to-Peer operation
  – Support for critical latency devices, such as joysticks
  – CSMA/CA channel access (data centric), slotted (beacon) or unslotted
  – Automatic network establishment by the PAN coordinator
  – Dynamic device addressing, flexible addressing format
  – Fully handshaked protocol for transfer reliability
  – Power management to ensure low power consumption
  – 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

RFID – Radio Frequency Identification (1)

♦ Data rate
  » Transmission of ID only (e.g., 48 bit, 64 bit, 1 Mbit)
  » 9.6 – 115 kbit/s

♦ Transmission range
  » Passive: up to 3 m
  » Active: up to 30-100 m
  » Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

♦ Frequency
  » 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

♦ Security
  » Application dependent, typ. no crypt. on RFID device

♦ Cost
  » Very cheap tags, down to 1€ (passive)

♦ Connection set-up time
  » Depends on product/medium access scheme (typ. 2 ms per device)

♦ Quality of Service
  » none

♦ Manageability
  » Very simple, same as serial interface

♦ Special Advantages/Disadvantages
  » Advantage: extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
  » Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/ transmission of ID)

♦ Availability
  » Many products, many vendors
RFID – Radio Frequency Identification (2)

♦ Function
- Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
- Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)

♦ Features
- No line-of sight required (compared to, e.g., laser scanners)
- RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
- Products available with read/write memory, smart-card capabilities

♦ Categories
- Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
- Active RFID: battery powered, distances up to 100 m

RFID – Radio Frequency Identification (3)

♦ Applications
- Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
- Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
- Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
- Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...

♦ Local Positioning Systems
- GPS useless indoors or underground, problematic in cities with high buildings
- RFID tags transmit signals, receivers estimate the tag location by measuring the signal’s time of flight
ISM band interference

Many sources of interference
- Microwave ovens, microwave lightning
- 802.11, 802.11b, 802.11g, 802.15
- Even analog TV transmission, surveillance
- Unlicensed metropolitan area networks

Levels of interference
- Physical layer: interference acts like noise
  - Spread spectrum tries to minimize this
  - FEC/interleaving tries to correct
- MAC layer: algorithms not harmonized
  - E.g., Bluetooth might confuse 802.11

802.11 vs. 802.15/Bluetooth

802.11b
3 channels (separated by installation)

802.15.1
79 channels (separated by hopping pattern)