Bluetooth Technology

Sources:

BLUETOOTH, J Bray and C. F. Sturman
Bluetooth Baseband Specification
Bluetooth

• Low-power, short range, wireless radio system (BT SIG: Ericsson, Nokia, IBM, …)
• 10 m, 1-Mbps links to 7 BT devices, 2.4 GHz,
• Both isochronous and asynchronous traffic
Bluetooth Protocol Stack

Radio
  ↓
Baseband
  ↓
LMP
  ↓
L2CAP
  ↓
RFComm
  ↓
PPP
  ↓
IP
  ↓
TCP/UDP
  ↓
AT
  ↓
SDP
  ↓
TCS
  ↓
PPP
  ↓
Audio
  ↓
OBEX
  ↓
0x0003
BT Protocol Stack

- Radio+Baseband: Frequency hopping radio platform.
- LMP: Data link setup, authentication
- L2CAP: Multiplexed comm. (conn./less), proprietary
- RFComm: Emulates RS-232 serial interface
- OBEX: Object exchange protocol
- SDP: Service discovery protocol
BT Service Discovery Protocol (SDP)

• API for enumerating and browsing
• Stop rules to limit duration of searches
• Applications use API to search devices
  • By service classes (printer, storage, …)
  • By matching attributes (model #, protocol, …)
• Service attributes are managed as a record by the devices SDP server
• No mechanism for using discovered service
Radio (ISM band)
• 2.4000—2.4835 GHz frequency range
• 2 MHz Lower Guard Band
• 3.5 MHz Upper Guard Band
• Available channels 79

-----------------------------
2.4465—2.4835 GHz freq range
7.5 MHz lower guard, 7.5 MHz upper guard,
23 channels
Device Address

- Bluetooth device address: 48 bits
  - BD_ADDR[23-:0] \(\Leftarrow\) LAP[23:0] : freq hop
  - BD_ADDR[31-24] \(\Leftarrow\) UAP[7:0] : freq hop
  - BD_ADDR[47-32] \(\Leftarrow\) NAP[15:0] : encryption
Masters, Slaves, and Piconets

- BT is a TDM system
- Basic unit of op. is a 625 microsec slot
- In pre-connection stage (inquiry/page.scan), Tx and Rx can occur in half slots.
- In connection state, Tx and Rx can occur in multiple slots: 1, 3, 5.
BT Piconet

• Piconet: An ad hoc net of up to 8 BT devices
• Master:
  – The device which initiates an exchange of data
  – Coordinates devices in a piconet
• Devices can be a part of several piconets at the same time: scatternet
Device state

• Device state:
  • Standby (waiting to connect to another device)
  • Inquire (searching for nearby devices), Inq. Scan
  • Page (connecting to another device), Page Scan
  • Connect
  • Hold and park (Connected to a piconet, power saving)
    – Hold ➔ no ACL traffic, free up bandwidth for other ops.
      (scanning, paging, inquiry, low-power sleep ….)
Bluetooth Clock

- Every device has a free-running “native” clock that controls the timing and op of that device: **CLKN**
Physical Links: ACL, SCO

• ACL
  • It exists as soon as a connection is established.
  • 1 ACL link between a Master ↔ Slave
  • View it as a packet-switched connection.
  • Under the control of the Master: a Slave can only respond if it has been addressed by the Master in the preceding M-to-S slot.
  • Broadcast packets are ACL packets.
Physical Link: ACL, SCO

- **SCO**
  - Provides a symmetric link between Master/Slave
  - Reserved channel bandwidth (reserved slots)
  - Up to 3 SCO links between Master ↔ 1 or more slaves.
  - SCO packets are never retransmitted
  - A SCO link is set up by a Link Manager (LM) command from Master to Slave
  - Master transmits SCO packets to Slave at regular intervals, defined by $T_{SCO}$. 
Packet Structure

• Packet
  – Access code: packet presence, from address
  – Header: control info (slave id)
  – Payload
Access Code

• CAC: derived from LAP of Master. Used by all in the piconet.
• DAC: derived from a device’s LAP. Used by a paging device.
• GIAC: Used by all during inquiry. 0x9E8B33 ← fixed
• Dedicated IAC: 0x9E8B00—0x9E8B3F
Packet Header (18 bits)

- **AM_ADDR (3 bits)**: 7 slaves, 1 bcast, at paging.
- **Packet Type (4 bits)**: NULL, POLL, FHS, DM1.. 
- **Flow (1 bit)**: Set by a device when it is unable to receive more data due to lack of local buffer.
- **ARQN (1 bit)**: Set by a device to indicate that the previous reception was OK.
  (Lost ARQN \(\rightarrow\) NACK)
- **SEQN (1 bit)**: toggles for each new packet
- **HEC (8 bits):**
ACL Payload

• Payload Header
  • L_CH (2 bits): Start/continuation of L2CAP message or an LMP message
  • Flow (1 bit): L2CAP flow control
  • Length (9 bits): payload data length in bytes
  • Unused (3 bits)

• Payload: Up to 341 bytes

• CRC: 16 bits
SCO Packet Structure

- Access Code: similar to ACL packet’s
- Header: similar to ACL packet’s
- Payload: fixed 30 bytes (source data of 10, 20, or 30 bytes with 1/3, 2/3, or none encoding)
## Packet Type Summary

<table>
<thead>
<tr>
<th>Code</th>
<th>Slots</th>
<th>SCO</th>
<th>ACL</th>
<th>PLHB</th>
<th>UPLB</th>
<th>FEC</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>0.5</td>
<td>ID</td>
<td>ID</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000</td>
<td>1</td>
<td>NULL</td>
<td>NULL</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0001</td>
<td>1</td>
<td>POLL</td>
<td>POLL</td>
<td>0</td>
<td>0</td>
<td>2/3</td>
<td></td>
</tr>
<tr>
<td>0010</td>
<td>1</td>
<td>FHS</td>
<td>FHS</td>
<td>0</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0011</td>
<td>1</td>
<td>DM1</td>
<td>DM1</td>
<td>1</td>
<td>0-17</td>
<td>2/3</td>
<td>Yes</td>
</tr>
<tr>
<td>0100</td>
<td>1</td>
<td>DH1</td>
<td>1</td>
<td>0-27</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>0101</td>
<td>1</td>
<td>HV1</td>
<td></td>
<td>No</td>
<td>10</td>
<td>1/3</td>
<td></td>
</tr>
<tr>
<td>0110</td>
<td>1</td>
<td>HV2</td>
<td></td>
<td>No</td>
<td>20</td>
<td>2/3</td>
<td></td>
</tr>
<tr>
<td>0111</td>
<td>1</td>
<td>HV3</td>
<td></td>
<td>No</td>
<td>30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Packet Type Summary (Contd.)

<table>
<thead>
<tr>
<th>Code</th>
<th>Slots</th>
<th>SCO</th>
<th>ACL</th>
<th>PLHB</th>
<th>UPLB</th>
<th>FEC</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>1</td>
<td>DV</td>
<td>1</td>
<td>10</td>
<td>10 (0-9)</td>
<td>2/3</td>
<td>Yes</td>
</tr>
<tr>
<td>1001</td>
<td>1</td>
<td>AUX1</td>
<td>1</td>
<td>0-29</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1010</td>
<td>3</td>
<td>DM3</td>
<td>2</td>
<td>0-121</td>
<td>2/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1011</td>
<td>3</td>
<td>DH3</td>
<td>2</td>
<td>0-183</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>1100</td>
<td>3</td>
<td>xxxxx</td>
<td>xxxx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>3</td>
<td>xxxxx</td>
<td>xxxx</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1110</td>
<td>5</td>
<td>DM5</td>
<td>2</td>
<td>0-224</td>
<td>2/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>5</td>
<td>DH5</td>
<td>2</td>
<td>0-339</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Data Rates (ACL packets)

<table>
<thead>
<tr>
<th>Type</th>
<th>UPLB</th>
<th>Symmetric Max rate (kb/s)</th>
<th>Asym. Max Rate Forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM1</td>
<td>0-17</td>
<td>108.8</td>
<td>108.8</td>
</tr>
<tr>
<td>DH1</td>
<td>0-27</td>
<td>172.8</td>
<td>172.8</td>
</tr>
<tr>
<td>DM3</td>
<td>0-121</td>
<td>258.1</td>
<td>387.2</td>
</tr>
<tr>
<td>DH3</td>
<td>0-183</td>
<td>390.4</td>
<td>585.6</td>
</tr>
<tr>
<td>DM5</td>
<td>0-224</td>
<td>286.7</td>
<td>477.8</td>
</tr>
<tr>
<td>DH5</td>
<td>0-339</td>
<td>433.9</td>
<td>723.2</td>
</tr>
<tr>
<td>AUX1</td>
<td>0-29</td>
<td>185.6</td>
<td>185.6</td>
</tr>
</tbody>
</table>
Calculation of data rates

Consider DM1 packet type:
User Payload (bytes) = 0-17
Symmetric Max. rate = 108.8 kb/sec
# Data Rates (SCO packets)

<table>
<thead>
<tr>
<th>Type</th>
<th>UPLB</th>
<th>Symmetric Max Rate (kb/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HV1</td>
<td>10 (FEC = 1/3)</td>
<td>64.0</td>
</tr>
<tr>
<td>HV2</td>
<td>20 (FEC = 2/3)</td>
<td>64.0</td>
</tr>
<tr>
<td>HV3</td>
<td>30 (no FEC)</td>
<td>64.0</td>
</tr>
<tr>
<td>DV</td>
<td>10 + (0-9) D</td>
<td>64.0 + 57.6 D</td>
</tr>
</tbody>
</table>
Logical Channels (Use of different packets)

- Link Control data: Packet header, ARQ, SEQ
- Link Manager data: Carried via DM1. L_CH = 11
- User Async data: Carried via ACL payload and contains L2CAP user data.
- User Sync data: Carried via SCO channel payload
Link Controller Operation

- Standby
- Page
- Page Scan
- Inq. Scan
- Inquiry
- Master Resp.
- Slave Resp.
- Inq. Resp.
- Conn.
To be discussed in class

- Frequency hopping mechanism
- Inquiry protocol
- Paging protocol
- Some performance data