MOBILE COMPUTING
CSE 40814/60814
Spring 2021

Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, very cheap
  - Short range (10m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s data rate
Bluetooth

• History
  • 1994: Ericsson (Mattison/Haartsen), “MC-link” project
  • Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  • 2001: first consumer products for mass market, spec. version 1.1 released
  • 2005: 5 million chips/week

• Special Interest Group
  • Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  • Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  • > 10000 members
  • Common specification and certification of products

Characteristics

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

• FHSS and TDD
  • Frequency hopping (spread spectrum) with 1600 hops/s
  • Hopping sequence in a pseudo random fashion, determined by a master
  • Time division duplex for send/receive separation

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

• Data link – ACL (Asynchronous Connection Less)
  • Asynchronous, acknowledgments, 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
Bluetooth Piconets

- Up to 7 slaves can be active in the piconet; many more slaves can remain connected in a parked state.
- Parked slaves are not active on the channel, but remain synchronized to the master and can become active without using the connection establishment procedure.
- If multiple piconets cover the same area, a device can participate in two or more overlapping piconets via time multiplexing.
- A device can act as a slave in several piconets, but as a master in only one piconet.
- Piconets with the same master are synchronized and use the same hopping sequence and are therefore considered the same piconet.
- A group of piconets in which connections exist between different piconets is called a scatternet.

Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).
Bluetooth Piconet

- All devices in a piconet hop together
- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

M=Master  P=Parked  S=Slave  SB=Standby
Bluetooth Scatternet

- Piconets that have common devices are called a scatternet.
- Each piconet has one master. Slaves can participate in different piconets on a time-division multiplex basis.
- A master in one piconet can be a slave in other piconets.
- Piconets are not frequency synchronized and each piconet has its own hopping sequence.

Scatternet

Piconets (each with a capacity of 720 kbit/s)

M=Master
S=Slave
P=Parked
SB=Standby
**Frequency Selection**

- \( f_k \), \( f_{k+1} \), \( f_{k+2} \), \( f_{k+3} \), \( f_{k+4} \), \( f_{k+5} \), \( f_{k+6} \)

**Bluetooth Packets**

- **Packet structure**
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum

- **Packet format**
  - 68(72) bits
  - 54 (3*18) bits
  - 0-2745 bits

- **Fields**
  - Preamble (64) bits
  - Sync. (4) bits
  - AM address (3) bits
  - Type (4) bits
  - Flow (1) bit
  - ARQN (1) bit
  - SEQN (1) bit
  - HEC (8) bits
### SCO payload types

<table>
<thead>
<tr>
<th>Type</th>
<th>Payload (30)</th>
<th>FEC (20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HV1</td>
<td>audio (10)</td>
<td></td>
</tr>
<tr>
<td>HV2</td>
<td>audio (20)</td>
<td>FEC (10)</td>
</tr>
<tr>
<td>HV3</td>
<td>audio (30)</td>
<td></td>
</tr>
<tr>
<td>DV</td>
<td>audio (10)</td>
<td>Header (1)</td>
</tr>
</tbody>
</table>

### ACL Payload types

<table>
<thead>
<tr>
<th>Type</th>
<th>Payload (0-343)</th>
<th>CRC (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM1</td>
<td>header (1/2)</td>
<td>payload (0-339)</td>
</tr>
<tr>
<td>DH1</td>
<td>header (1)</td>
<td>payload (0-17)</td>
</tr>
<tr>
<td>DH3</td>
<td>header (2)</td>
<td>payload (0-27)</td>
</tr>
<tr>
<td>DM5</td>
<td>header (2)</td>
<td>payload (0-121)</td>
</tr>
<tr>
<td>DH5</td>
<td>header (2)</td>
<td>payload (0-183)</td>
</tr>
<tr>
<td>AUX1</td>
<td>header (1)</td>
<td>payload (0-29)</td>
</tr>
</tbody>
</table>
## Data rates

<table>
<thead>
<tr>
<th>ACL Type</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>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>AUX1</td>
<td>1</td>
<td>0-29</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>185.6</td>
<td>185.6</td>
</tr>
<tr>
<td>SCO</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>SCO</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>SCO</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>SCO</td>
<td>DV</td>
<td>1 D</td>
<td>10+(0-9)</td>
<td>D</td>
<td>yes</td>
<td>64.0+57.6 D</td>
<td></td>
</tr>
</tbody>
</table>

_Data Medium/High rate, High-quality Voice, Data and Voice_

## 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
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

Bluetooth Versions

- Bluetooth 1.1
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard

- Bluetooth 1.2
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference

- Bluetooth 2.0 + EDR (2004, no more IEEE)
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle

- Bluetooth 2.1 + EDR (2007)
  - better pairing support, e.g., using NFC
  - improved security
Bluetooth Versions

- Bluetooth 3.0 + HS (2009)
  - speeds up to 24Mbps (using co-located Wi-Fi link!)
- Bluetooth 4.0
  - Classic Bluetooth
  - Bluetooth High Speed
  - Bluetooth Low Energy
- Bluetooth Low Energy (BLE):
  - Marketed as Smart Bluetooth
  - Lower power, lower cost
  - Use in healthcare, fitness, security, entertainment devices
  - 40 channels
- Bluetooth Profiles (different types of applications)

Energy Consumption in Classic BT

- Traditional Bluetooth is connection oriented. When a device is connected, a link is maintained, even if there is no data flowing
- Sniff modes allow devices to sleep, reducing power consumption to give months of battery life (e.g., wake up every 100ms)
- Peak transmit current is typically around 25mA
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough for coin cells and energy harvesting applications
Bluetooth Low Energy (BLE)

- Bluetooth low energy is a new, open, short range radio technology
  - Blank sheet of paper design
  - Different to Bluetooth classic (BR/EDR)
  - Optimized for ultra low power
  - Enable coin cell battery use cases
    - < 20mA peak current
    - < 5uA average current

BLE Basic Concepts

- Everything is optimized for lowest power consumption
  - Short packets reduce TX peak current
  - Short packets reduce RX time
  - Fewer RF channels to improve discovery and connection time
  - Simple state machine
  - Single protocol
  - ...
BLE Fact Sheet

• Data Throughput
  • For Bluetooth low energy, data throughput is not a meaningful parameter. It does not support streaming.
  • It has a data rate of 1Mbps, but is not optimized for file transfer.
  • It is designed for sending small chunks of data (exposing state).

“Exposing State” (Example: IoT)

• 23.2°C
• 60.5 km/h
• 12:23 pm
• Gate 10 BOARDING
• 3.2 kWh
• Network Available

• It’s good at small, discrete data transfers
• Data can triggered by local events
• Data can be read at any time by a client
• Interface model is very simple (GATT)
BLE Device Modes

• Dual Mode
  • Bluetooth BR/EDR and LE
  • Used anywhere BR/EDR is used today

• Single Mode
  • Implements only Bluetooth low energy
  • Will be used in new devices / applications

BLE Architecture
BLE Device Modes

- Dual mode + single modes

<table>
<thead>
<tr>
<th>BR/EDR stack</th>
<th>Dual-mode stack</th>
<th>Single-mode stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port Profile</td>
<td>Serial Port Profile</td>
<td>Attribute Profile</td>
</tr>
<tr>
<td>RFCOMM Protocols</td>
<td>RFCOMM Protocols</td>
<td>Attribute Protocol</td>
</tr>
<tr>
<td>L2CAP</td>
<td>L2CAP</td>
<td>L2CAP</td>
</tr>
<tr>
<td>Link Manager</td>
<td>Link Manager</td>
<td>Link Layer</td>
</tr>
<tr>
<td>Basic Rate RF</td>
<td>Basic Rate RF + low energy</td>
<td>low energy RF</td>
</tr>
</tbody>
</table>

BLE Physical Layer

- 2.4 GHz ISM band
- 1Mbps GFSK
  - Larger modulation index than Bluetooth BR (which means better range)
- 40 Channels on 2 MHz spacing
BLE Physical Layer

• Two types of channels

![3 Advertising Channels and 37 Data Channels](image)

BLE Physical Layer

• Advertising channels avoid 802.11

![9 LL Data Channels still available](image)
BLE Link Layer

- Link Layer state machine

![Diagram of BLE Link Layer state machine]

BLE Link Layer

![Diagram of BLE Link Layer state machine with different states and transitions]

![Diagram of BLE Link Layer state machine with different roles and connections]
BLE Link Layer

- Possible states:
  - **Standby**: not transmitting or receiving any data, and is not connected to any other device
  - **Advertiser**: periodically broadcasting advertisements
  - **Scanner**: actively looking for advertisers
  - **Initiator**: actively trying to initiate a connection with another device
  - **Master**: connected to another device as a master
  - **Slave**: connected to another device as a slave

BLE Advertising

- Devices can advertise for a variety of reasons:
  - To broadcast promiscuously
  - To transmit signed data to a previously bonded device
  - To advertise their presence to a device wanting to connect
  - To reconnect asynchronously due to a local event
BLE Advertising

- Four types of advertisements:
  - **Connectable undirected**: any scanner device can initiate a connection with this advertiser
  - **Connectable directed**: only one specific device can initiate a connection with this advertiser
  - **Non-connectable undirected**: no devices can initiate a connection with this advertiser; primarily used for general broadcast of data (up to 31 bytes of payload)
  - **Discoverable undirected**: any scanner device can request more information from the advertising device, but no devices can initiate a connection with it

BLE Data Transfer

- Once a connection is made:
  - Master informs slave of hopping sequence and when to wake up
  - All subsequent transactions are performed on the 37 data channels
  - Transactions can be encrypted
  - Both devices can go into deep sleep between transactions
Link Layer Connections

- Very low latency connection

![Diagram of Link Layer Connections]

ZigBee

- IEEE 802.15.4 (similar to Bluetooth and IEEE 802.15.1)

- Pushed by Chipcon (now TI), Ember, Freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung...

- More than 260 members
  - about 15 promoters, 133 participants, 111 adopters
  - must be member to commercially use ZigBee spec

- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications
ZigBee

- Design goal
  - Low power consumption
  - Simple Design
  - Few costs
- History
  - ZigBee-style networks began ~1998
  - IEEE 802.15.4 was first completed in 2003
  - ZigBee Alliance was established in 2002

ZigBee Core Market

- Industrial and Commercial
  - Monitors
  - Movement Sensors
  - Automation
- Personal Healthcare
  - Patient monitors
  - Remote Diagnosis
  - Data loggers
- Building Automation
  - Security
  - Lighting
  - Fire and Safety systems
- Automotive
  - Service controls
  - Inventory tracking
ZigBee Protocol Stack

- **Application**
  - Application Layer (AL)
    - Application Framework (AF)
    - ZigBee Device Objects (ZDO)
    - Application Support Sublayer (ASP)

- **Network (NWK)**
  - Star / Mesh / Cluster-Tree

- **MAC**
  - Device Types, Channel Access

- **PHY**
  - 868 MHz / 915 MHz / 2.4 GHz

Customer → ZigBee Alliance → IEEE 802.15.4

Device Type

- **Full Function Device (FFD)**
  - Network router function
  - Any Topology

- **Reduced Function Device (RFD)**
  - Easy and cheap to implement
  - Limited to star topology

- **Personal Area Network (PAN) Coordinator**
  - Maintains overall network knowledge
  - Needs most memory and computing power
Basic Topology

Star Network

Cluster Tree Network
ZigBee PRO: Mesh Network

Bluetooth vs. ZigBee

<table>
<thead>
<tr>
<th></th>
<th>Bluetooth (v1)</th>
<th>ZigBee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol Stack</strong></td>
<td>250 kb</td>
<td>&lt; 32 kb (4kb)</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>10 - 100 meters</td>
<td>30 - 100 meters</td>
</tr>
<tr>
<td><strong>Link Rate</strong></td>
<td>1 Mbps</td>
<td>250 kbps</td>
</tr>
<tr>
<td><strong>Battery</strong></td>
<td>rechargeable</td>
<td>non-rechargeable</td>
</tr>
<tr>
<td><strong>Devices</strong></td>
<td>8</td>
<td>$2^{16}$</td>
</tr>
<tr>
<td><strong>Air Interface</strong></td>
<td>FHSS</td>
<td>DSSS</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>frequently</td>
<td>infrequently</td>
</tr>
<tr>
<td><strong>Network Join Time</strong></td>
<td>long</td>
<td>short</td>
</tr>
<tr>
<td><strong>Extendibility</strong></td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>PIN, 64 bit, 128 Bit</td>
<td>128 bit, AES</td>
</tr>
</tbody>
</table>
## Comparison

<table>
<thead>
<tr>
<th>Technology</th>
<th>Classic Bluetooth Technology (SIG/ECMA)</th>
<th>Bluetooth low energy technology</th>
<th>ZigBee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio Frequency</strong></td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td><strong>Distance / Range</strong></td>
<td>10 to 100 meters²</td>
<td>10 to 100 meters³</td>
<td>10 to 200 meters³</td>
</tr>
<tr>
<td><strong>Over the air Data Rate</strong></td>
<td>1 Mbps</td>
<td>1 Mbps</td>
<td>256 Kbps at 2.4 GHz</td>
</tr>
<tr>
<td><strong>Application Throughput</strong></td>
<td>0.7-2.1 Mbps</td>
<td>0.2 Mbps</td>
<td>&lt;0.1 Mbps</td>
</tr>
<tr>
<td><strong>Nodes/Active Slaves</strong></td>
<td>7 / 147771 (SIG²)</td>
<td>Unlimited¹</td>
<td>65535²</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>64-bit/128-bit and application layer user defined</td>
<td>128-bit AES and application layer user defined</td>
<td>128-bit AES and application layer user defined</td>
</tr>
<tr>
<td><strong>Robustness</strong></td>
<td>Adaptive fast frequency hopping, FEC, fast ACK</td>
<td>Adaptive fast frequency hopping</td>
<td></td>
</tr>
<tr>
<td><strong>Latency (from a non connected state)</strong></td>
<td>100ms</td>
<td>3ms</td>
<td>10ms</td>
</tr>
<tr>
<td><strong>Total time to send data (in battery state)</strong></td>
<td>100ms</td>
<td>3ms</td>
<td>10ms</td>
</tr>
<tr>
<td><strong>Government Regulation</strong></td>
<td>Worldwide</td>
<td>Worldwide</td>
<td>Worldwide</td>
</tr>
<tr>
<td><strong>Certification Body</strong></td>
<td>Bluetooth SIG</td>
<td>Bluetooth SIG</td>
<td>Zigbee Alliance</td>
</tr>
<tr>
<td><strong>Voice capable</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Network topology</strong></td>
<td>Scatternet</td>
<td>Star-bus</td>
<td>Star or Mesh</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>1 as the reference</td>
<td>0.01 to 0.3 (depending on use-case)</td>
<td>2 (router) / 0.1 (end point)</td>
</tr>
<tr>
<td><strong>Peak current consumption (max 15 mA per run on coin cell battery)</strong></td>
<td>&lt;30 mA</td>
<td>&lt;15 mA</td>
<td>&lt;15 mA</td>
</tr>
<tr>
<td><strong>Service discovery</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Profile protocol</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Primary Use Cases</strong></td>
<td>Mobile phones, gaming, headsets, drones, audio streaming, automotive, PCs, consumer electronics, etc.</td>
<td>Mobile phones, gaming, PCs, watches, sports &amp; fitness, healthcare, automotive, consumer electronics, automation, industrial, etc.</td>
<td>Fixed location industrial, building &amp; home automation, AMR/SmartEnergy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ Unrestricted, SIG ¹¹
² Maximum Supportable 30 Nodes With 100% Busy Activity
³ SIG ¹¹ is the reference to the table.