COMP4310/6310 Wireless Mobile Computing
Bluetooth and ZigBee
Reviews

- **GSM**
  - Key components:
    - MS (mobile station)
    - BSS (Base Station Subsystem):
      - BTS (Base Transceiver Station): sender and receiver
      - BSC (Base Station Controller): controlling several transceivers
    - MSC (mobile switching center)
    - LR (location register)
    - SS7 (Signaling System 7)
  - FDMA/TDMA
  - Comprehensive and successful
    - Handover, security, ....
Reviews

- Satellite

- HEO

- LEO (Globalstar, Irdium)

- MEO (ICO)

- GEO (Inmarsat)

- 1000 km

- 10000 km

- 35768 km
WiFi vs Cellular vs Satellite

- Service
- Coverage
- Data Rate
- Reliability
Bluetooth

• Cable replacement technology.
  - Connect devices such as phone handsets, headsets, computer peripherals, etc.

• Industry standard.
  - Allows wireless communication between devices.
Applications: Cable Replacement

- 1 Mb/s.
- Range ~10 meters.
- Personal Area Network (PAN)
- Single chip radio.
  - Low power & low cost.

Q: Why not just use WiFi?
Applications: Synchronization

- Automatic synchronization of calendars, address books, business cards.
Applications: Cordless Headset

- Multiple device access.
- Hands-free operation.
More applications...

- Conference table.
- Cordless computer.
- Instant photo transmission.
- Cordless phone.
Bluetooth Origins

• Study by Ericsson Mobile Communications in 1994.
  - Alternatives to cables connecting mobile phones to accessories.
  - Use of radio links instead of infrared.
    • Why?
  - Transmission of data and voice.

• Result: Bluetooth spec.
  - Named after Harald Blatand (Danish for Bluetooth).
  - 10th century Viking king who united Denmark and Norway.
More History...

- Recently, IEEE 803.15.1 standard for Wireless PANs (WPANs)
  - Only MAC and PHY.
Goals

- Open spec.
- Low cost.
  - In order to replace cables, should have similar cost.
  - Cell phone cable is ~ $10.
- Power efficiency.
- Lightweight and small form factor.
- Easy to use.
- Reliable and resilient to failures.
The Bluetooth Standard

- Defines a protocol stack to enable heterogeneous devices to communicate.
- The Bluetooth stack includes protocols for the radio layer all the way up to device discovery, service discovery, etc.
Bluetooth Protocol Stack

- RF
- Baseband
- Link Controller
- Link Manager
- Host Controller Interface
- L2CAP
- RFCOMM/SDP
- Applications

- Application
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- PHY
- OSI/ISO
Radio Band

- 2.4 GHz license-free ISM band.
- Available worldwide.
- Industrial, Scientific, Medical (ISM) band.
  - Unlicensed, globally available.
  - Centered around 2.4 GHz.
- Resilient to interference.
- Frequency hopping.
- Range: 10, 20, and 100m.
- 1MB/s.
BT Radio Link (Cont’d)

• Time-division duplex (TDD)
  - Separation of transmission and reception in time.
  - Units alternate transmits and receives.

• Gaussian Frequency Shift Keying (G-FSK) modulation.
  - ‘1’s as positive frequency deviations from carrier frequency; ‘0’s as negative deviations.
Multiple Access

- 79 frequency channels
  - But not FDMA

- **MA scheme:** Frequency hopping spread spectrum.
  - 2.402 GHz + k MHz, k=0, ..., 78
  - 1,600 hops per second.
  - 1 Mb/s data rate.
Frequency hopping

- Frequency hopping vs FDMA
  - Advantages, disadvantages?
Piconets

- BT communication takes place over piconets.
- Piconet formation initiated by master.
- All other participants are slaves.
- Number of participants limited to 8 (1 master and 7 slaves).
  - Channel capacity and addressing overhead.
  - Each slave assigned a locally unique ID.
- Master/slave roles last for the duration of the piconet.
Master and Slaves

- Communicating devices must agree on hopping sequence.
- BT devices can operate as masters or slaves.
- Master node defines sequence to be used.
- Slave units use master id to pick sequence.
- Master also controls when devices are allowed to transmit.
  - Master allocates slots to slaves.
  - Allocates total available bandwidth among slaves.
More on Piconets

- On a piconet, slaves only have direct links to master.
- Point-to-point or point-to-multipoint connections.
Contestation-Free MA

- Master and slaves.
- Master performs medium access control.
  - Schedules traffic through polling.
- Time slots alternate between master and slave transmission.
  - Master-slave: master includes slave address.
  - Slave-master: only slave chosen by master in previous master-slave slot allowed to transmit.
  - If master has data to send to a slave, slave polled implicitly; otherwise, explicit poll.
Inquiry

• Device discovery
  • Listeners respond with their address.
Paging

- Device enters paging to invite others to join its piconet.
- Establishes links with nodes in proximity.
- Paging message unicast to selected receiver.
- Receiver sends ACK.
- Sender becomes master, receiver slave.
Packet Format

72 bits  |  54 bits  |  0 - 2744 bits

Access code | Header | Payload

Voice

No CRC
No retries
FEC (optional)

ARQ
FEC (optional)

625 µs

master

slave
Access Code

- Address of piconet master.

72 bits

Access code

Header

Payload
Packet Header

54 bits

Access code | Header | Payload

Purpose

- Addressing (3) → Max 7 active slaves
- Packet type (4) → 16 packet types (some unused)
- Flow control (1)
- 1-bit ARQ (1) → Broadcast packets are not ACKed
- Sequencing (1) → For filtering retransmitted packets
- HEC (8) → Verify header integrity

total 18 bits
Multiple Piconets

• Piconets may overlap in space and time.
• They can work independently.
  - Each with its own hopping sequence.
  - Packets with different access codes.
• Or they can overlap, i.e., nodes can participate in more than 1 piconet.
  - “Time sharing”.
Scatternets

- Interconnection of multiple piconets.
Scatternets (cont’d…)

• Interconnection by bridge nodes.
  - Bridge nodes are members of piconets they interconnect.
  - Bridge node “stay” in a piconet for some time, then switch to another piconet by changing hop sequence.
  - Do this for all member piconets.
  - Send and receive in each piconet.
  - Forward from one piconet to another.
Power Management

- Low-power modes: prolong battery life.
  - Devices can be turned-off when idle.
  - Devices wake up periodically to send/receive data.
Security

• Authentication and encryption.
• LMP provides mechanisms for negotiation of encryption modes, keys, etc.
Summary

- WiFi - Wireless LAN
- Cellular networks
- Satellite networks
- Bluetooth piconets
- ZigBee:
  - A set of applications require simple wireless connectivity, relaxed throughput, very low power, short distance and inexpensive hardware.
What is ZigBee Alliance?

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Alliance provides interoperability, certification testing, and branding
# Comparison between WPAN

<table>
<thead>
<tr>
<th>Project</th>
<th>Data Rate</th>
<th>Range</th>
<th>Configuration</th>
<th>Other Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.15.1</strong> (Bluetooth)</td>
<td>1 Mbps</td>
<td>10M (class 3) 100M (class 1)</td>
<td>8 active device Piconet/Scatternet</td>
<td>Authentication, Encryption, Voice</td>
</tr>
<tr>
<td><strong>802.15.3</strong> High Rate</td>
<td>22, 33, 44, 55 Mbps</td>
<td>10M</td>
<td>256 active device Piconet/Scatternet</td>
<td>FCC part 15.249 QoS, Fast Join Multi-Media</td>
</tr>
<tr>
<td><strong>802.15.4</strong> Low Rate</td>
<td>up to 250Kbps</td>
<td>10M nominal 1M-100M based on settings</td>
<td>Master/Slave (256 Devices or more) Peer to Peer</td>
<td>Battery Life: multi-month to infinite</td>
</tr>
<tr>
<td><strong>802.15.2</strong> Coexistence</td>
<td>Develop a Coexistence Model and Mechanisms Document as a Recommended Practice</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Data Rate**: The data rate is crucial for determining the speed at which data is transmitted.
- **Range**: The range indicates how far devices can communicate with each other.
- **Configuration**: Details about the configuration of the WPAN, including the number of active devices and the type of network (Piconet/Scatternet).
- **Other Features**: Additional features such as authentication, encryption, voice support, FCC compliance, QoS, fast join, multimedia support, battery life, and recommended practices.
ZigBee/IEEE 802.15.4 market feature

- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders (<= 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications
ZigBee network applications

- **PERSONAL HEALTH CARE**: monitors, sensors, automation, control
- **INDUSTRIAL & COMMERCIAL**: LOW DATA-RATE RADIO DEVICES
- **CONSUMER ELECTRONICS**: TV VCR, DVD/CD, Remote control
- **PC & PERIPHERALS**: mouse, keyboard, joystick
- **TOYS & GAMES**: consoles, portables, educational
- **HOME AUTOMATION**: security, HVAC, lighting, closures
ZigBee/802.15.4 architecture

- **ZigBee Alliance**
  - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003

- **IEEE 802.15.4 Working Group**
  - Defining lower layers of protocol stack: MAC and PHY

---

![Diagram of ZigBee architecture](image-url)
How is ZigBee related to IEEE 802.15.4?

- ZigBee takes full advantage of a powerful physical radio specified by IEEE 802.15.4
- ZigBee adds logical network, security and application software
- ZigBee continues to work closely with the IEEE to ensure an integrated and complete solution for the market
IEEE 802.15.4 overview
General characteristics

- Data rates of 250 kbps, 20 kbps and 40 kbps.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access.
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- Channels:
  - 16 channels in the 2.4GHz ISM band,
  - 10 channels in the 915MHz ISM band
  - 1 channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)
IEEE 802.15.4 basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - CSMA/CA
  - Message acknowledgement
  - Optional beacon structure
  - Target applications
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries
Star topology

Network coordinator

Full Function Device (FFD)
Reduced Function Device (RFD)
Communications Flow

Master/slave
Peer to peer topology

Point to point

Tree

Full Function Device (FFD)

Communications Flow
Device addressing

- Two or more devices communicating on the same physical channel constitute a WPAN.
  - A WPAN includes at least one FFD (PAN coordinator)
  - Each independent PAN will select a unique PAN identifier

- Each device operating on a network has a unique 64-bit extended address. This address can be used for direct communication in the PAN

- A device also has a 16-bit short address, which is allocated by the PAN coordinator when the device associates with its coordinator.
Channel Access Mechanism

• Two type channel access mechanism:
  - beacon-enabled networks → slotted CSMA/CA channel access mechanism
  - non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
Slotted CSMA/CA algorithm

• In slotted CSMA/CA
  - The backoff period boundaries of every device in the PAN shall be aligned.
    • i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
  - The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period
Slotted CSMA/CA algorithm (cont.)

- Each device maintains 3 variables for each transmission attempt
  - **NB**: number of times that backoff has been taken in this attempt (if exceeding `macMaxCSMABackoff`, the attempt fails)
  - **BE**: the backoff exponent which is determined by NB
    - When **BE** = 2, becomes binary exponential backoff
  - **CW**: contention window length, the number of clear slots that must be seen after each backoff