Ah-Hoc, PAN, WSN, ...

→ **Introduction**
→ **Bluetooth (802.15.1)**
→ **Zigbee (802.15.4)**

Renato Lo Cigno
www.dit.unitn.it/locigno/

Ad-Hoc Networks

- Built by the userse themselves to support specific (in time, space, applications) needs
  - Example: using 802.11 BSS as you did in the lab
- Are generally closed, but "gateways" are coming into play to connect them to the resto fo the world
- The key point is the requirement to build and support dynamically the topology "on-th-fly"
  - No network planning
  - No hierarchy
  - No engineering

Sensor/Actuators Networks

- Ad-Hoc networks whose goal is specifically making some kind of measure (sensing) and, in case, react to some change/event (actuating)
- Normally battery powered: one more problem on energy consupmption
- Are the backbone of "Ambient Intelligence" concepts

Personal Networks

- PAN "personal area network"
- IEEE 802.15 sub-project
- Very short range (1-5m) and extremely low power (< 10mw EIRP)
- The goal is connection of devices for "cable replacement"
  - Earphone with cell/HiFi/TV
  - PDA, cell phone, clock, alarm, laptop
  - mouse, keyboard, laptop
  - ...

Technologies

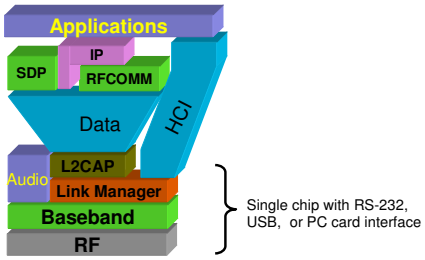
- 802.11
  - Do you know it? ☺
- Bluetooth (802.15.1)
  - Master/Slave architecture
  - Optimized for low bandwidth (< 1Mbit/s), real time communications
- ZigBee (802.15.4)
  - Meshed architecture
  - Low power consumption
  - Suitable for sporadic communications with very low throughput (channel capacity 25 kbit/s)
- All use the same ISM bands

Open (Not Yet Standard) Issues

- Routing
  - How to find the best route across a "temporary" network?
  - Coordination of multi-hop transfer
  - Stability of routes
- Topology Management
  - Cooperation among nodes
  - How to reward nodes that use resources for others
- Usage context
  - Ad Hoc Networks were born for military applications
  - Their civilian use is appealing, but do we really need them?

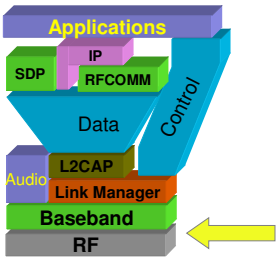
Bluetooth

Bluetooth Specifications

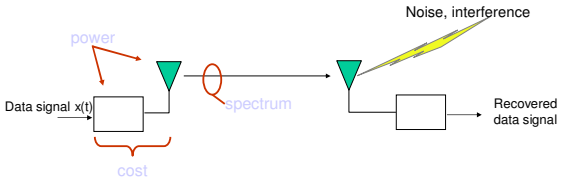


- A hardware/software/protocol description
- An application framework

Bluetooth Radio Specification



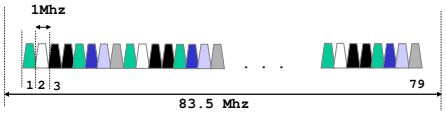
Design considerations



Goal

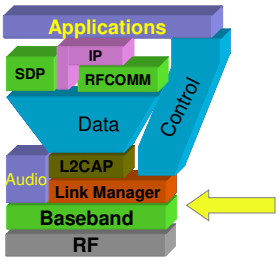
- high bandwidth
- conserve battery power
- cost < $10

Bluetooth radio link



- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dbm (up to 20dbm with power control)

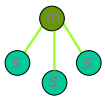
Baseband



Bluetooth Physical link

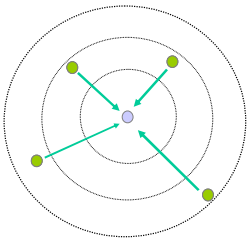
- Point to point link
  - master - slave relationship
  - radios can function as masters or slaves

- Piconet
  - Master can connect to 7 slaves
  - Each piconet has max capacity =1 Mbps
  - hopping pattern is determined by the master



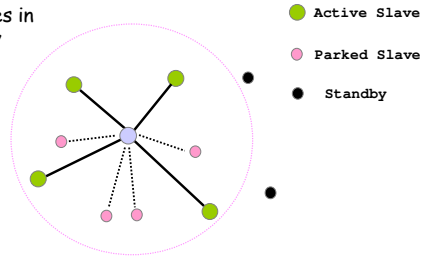
Connection Setup

- Inquiry - scan protocol
  - to learn about the clock offset and device address of other nodes in proximity



Piconet formation

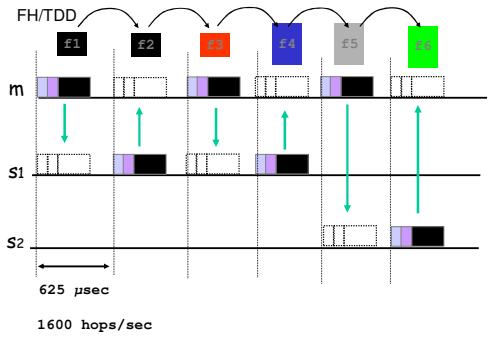
- Page - scan protocol
  - to establish links with nodes in proximity



Addressing

- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address
- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address
- Parked Member address (PM_ADDR)
  - 8 bit parked slave address

Piconet channel



1600 hops/sec

Packet Header

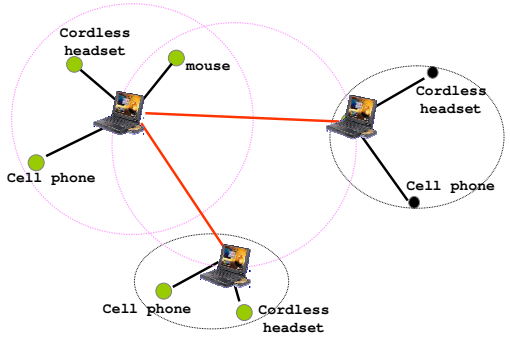
Purpose

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

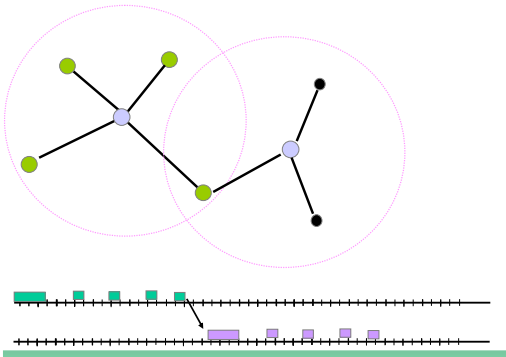
total 18 bits

Encode with 1/3 FEC to get 54 bits

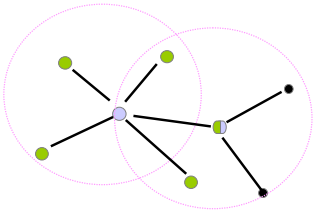
Inter piconet communication



Scatternet



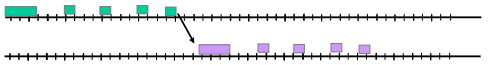
Scatternet, scenario 2



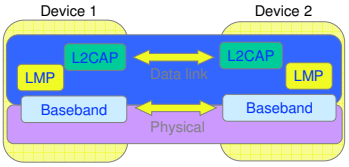
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?

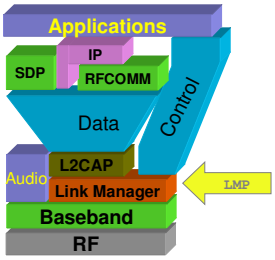


Baseband: Summary



- TDD, frequency hopping physical layer
- Device inquiry and paging
- Two types of links SCO (Sync. Connection Oriented) and ACL (Async. ConnectionLess) links
- Multiple packet types (multiple data rates with and without FEC)

Link Manager Protocol

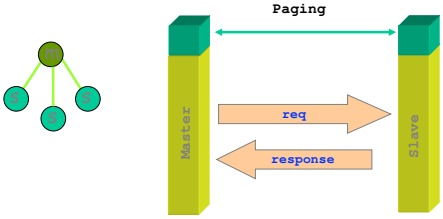


Setup and management of Baseband connections

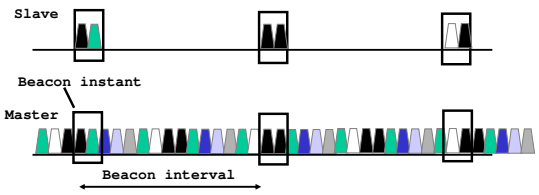
- Piconet Management
- Link Configuration
- Security

Piconet Management

- Attach and detach slaves
- Master-slave switch
- Establishing SCO links
- Handling of low power modes (Sniff, Hold, Park)



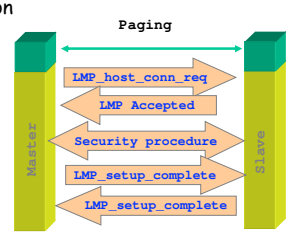
Low power mode (Park)



- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages

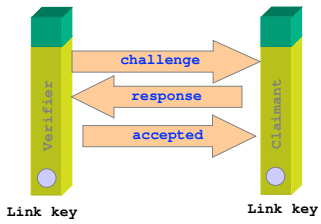
Connection establishment & Security

- Goals
  - Authenticated access
    - Only accept connections from trusted devices
  - Privacy of communication
    - prevent eavesdropping
- Constraints
  - Processing and memory limitations
    - $10 headsets, joysticks
  - Cannot rely on PKI
  - Simple user experience

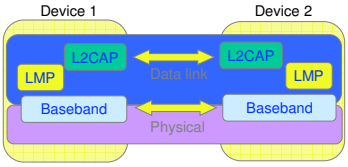


Authentication

- Authentication is based on link key (128 bit shared secret between two devices)
- How can link keys be distributed securely ?

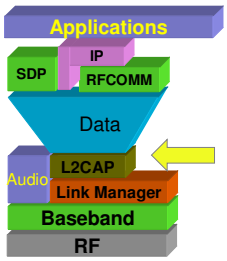


Link Manager Protocol Summary



- Piconet management
- Link configuration
  - Low power modes
  - QoS
  - Packet type selection
- Security: authentication and encryption

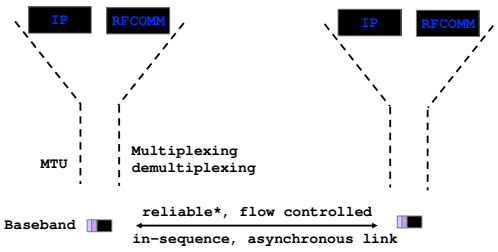
L2CAP



Logical Link Control and Adaptation Protocol

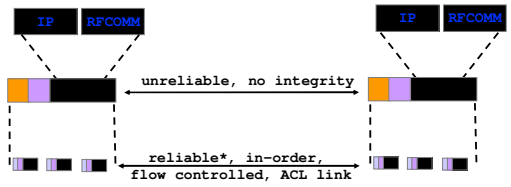
L2CAP provides
- Protocol multiplexing
- Segmentation and Re-assembly
- Quality of service negotiation

Why baseband isn't sufficient



- Baseband packet size is very small (17min, 339 max)
- No protocol-id field in the baseband header

Need a multiprotocol encapsulation layer

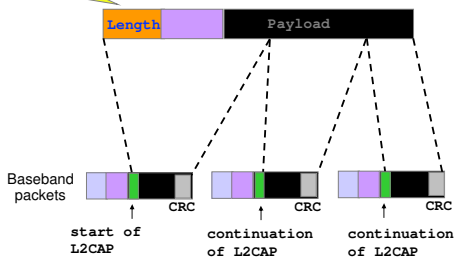


Desired features
- Protocol multiplexing
- Segmentation and re-assembly
- Quality of service

What about
- Reliability?
- Connection oriented or connectionless?
- integrity checks?

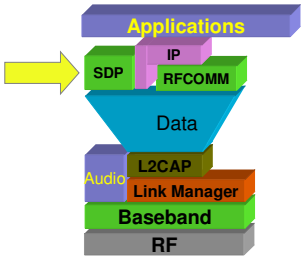
Segmentation and reassembly

min MTU = 48
672 default



- cannot cope with re-ordering or loss
- mixing of multiple L2CAP fragments not allowed
- If the start of L2CAP packet is not acked, the rest should be discarded

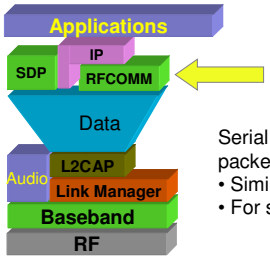
Bluetooth Service Discovery Protocol



Example usage of SDP

- Establish L2CAP connection to remote device
- Query for services
  - search for specific class of service, or
  - browse for services
- Retrieve attributes that detail how to connect to the service
- Establish a separate (non-SDP) connection to use the service

Serial Port Emulation using RFCOMM



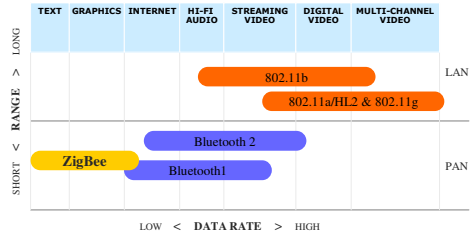
Serial Port emulation on top of a packet oriented link
• Similar to HDLC
• For supporting legacy apps

ZigBee and 802.15.4 for Personal Area and Sensor Networks

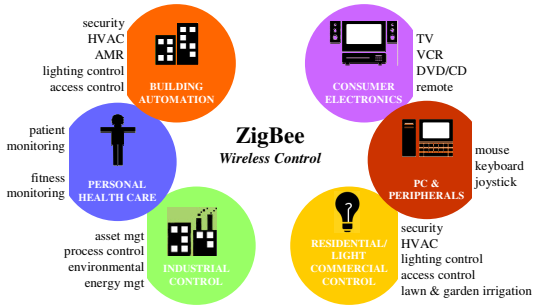
The ZigBee Alliance Solution

- Targeted at home and building automation and controls, consumer electronics, PC peripherals, medical monitoring, and toys
- Industry standard through application profiles running over IEEE 802.15.4 radios
- Primary drivers are simplicity, long battery life, networking capabilities, reliability, and cost
- Alliance provides interoperability and certification testing

The Wireless Market

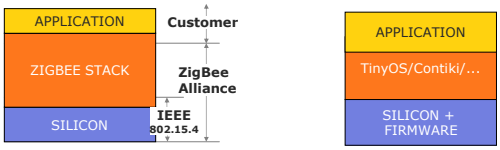


Applications



Development of the Standard

- **ZigBee Alliance**
  - **50+ 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**
  - **Not much used**
- **IEEE 802.15.4 Working Group**
  - **Defining lower layers of protocol stack: MAC and PHY released May 2003**
- **802.15.4 hardware and framing plus Open Source O.S. (TinyOS ...)**



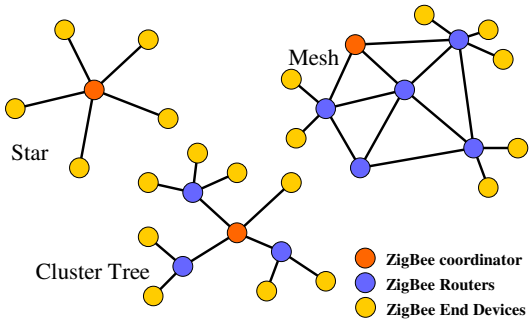
IEEE 802.15.4 Basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi-level security
  - Three bands, 27 channels specified
    - **2.4 GHz: 16 channels, 250 kbps**
    - 868.3 MHz : 1 channel, 20 kbps
    - 902-928 MHz: 10 channels, 40 kbps
  - Works well for
    - 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

IEEE 802.15.4 Device Types

- Three device types
  - Network Coordinator
    - Maintains overall network knowledge; most sophisticated of the three types; most memory and computing power
  - Full Function Device
    - Carries full 802.15.4 functionality and all features
    - Additional memory, computing power make it ideal for a network router function
    - Could also be used in network edge devices (where the network touches the real world)
  - Reduced Function Device
    - Carriers limited (as specified by the standard) functionality to control cost and complexity
    - General usage will be in network edge devices
- All of these devices can be no more complicated than the transceiver, a simple 8-bit MCU and a pair of AAA batteries!

ZigBee Topology Models



MAC Options

Two channel access mechanisms

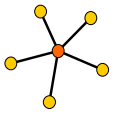
- Non-beacon network
  - Standard CSMA-CA communications
  - Positive acknowledgement for successfully received packets
- Beacon-enabled network
  - Superframe structure
    - For dedicated bandwidth and low latency
    - Set up by network coordinator to transmit beacons at predetermined intervals
      - 15ms to 252sec (15.38ms*2n where $0 \leq n \leq 14$)
      - 16 equal-width time slots between beacons
      - Channel access in each time slot is contention free

Non-Beacon vs Beacon Modes

- Non-Beacon Mode
  - A simple, traditional multiple access system used in simple peer and near-peer networks
  - Think of it like a two-way radio network, where each client is autonomous and can initiate a conversation at will, but could interfere with others unintentionally
  - However, the recipient may not hear the call or the channel might already be in use
- Beacon Mode
  - A powerful mechanism for controlling power consumption in extended networks like cluster tree or mesh
  - Allows all clients in a local piece of the network the ability to know when to communicate with each other
  - Here, the two-way radio network has a central dispatcher who manages the channel and arranges the calls
- As you'll see, the primary value will be in system power consumption

Example of Non-Beacon Network

- Commercial or home security
  - Client units (intrusion sensors, motion detectors, glass break detectors, standing water sensors, loud sound detectors, etc)
    - Sleep 99.999% of the time
    - Wake up on a regular yet random basis to announce their continued presence in the network ("12 o'clock and all's well")
    - When an event occurs, the sensor wakes up instantly and transmits the alert ("Somebody's on the front porch")
  - The ZigBee Coordinator, mains powered, has its receiver on all the time and so can wait to hear from each of these station.



Example of Beacon Network

- Now make the ZigBee Coordinator battery-operated also
  - All units in system are now battery-operated
  - Client registration to the network
    - Client unit when first powered up listens for the ZigBee Coordinator's network beacon (interval between 0.015 and 252 seconds)
    - Register with the coordinator and look for any messages directed to it
    - Return to sleep, awaking on a schedule specified by the ZigBee Coordinator
    - Once client communications are completed, ZigBee coordinator also returns to sleep

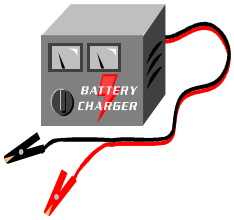
ZigBee and Bluetooth

Optimized for different applications

- **ZigBee**
  - **Smaller packets over large network**
  - **Mostly Static networks with many, infrequently used devices**
  - **Home automation, toys, remote controls, etc.**
- **Bluetooth**
  - **Larger packets over small network**
  - **Ad-hoc networks**
  - **File transfer**
  - **Screen graphics, pictures, hands-free audio, Mobile phones, headsets, PDAs, etc.**

ZigBee and Bluetooth

Address Different Needs



- Bluetooth is a cable replacement for items like Phones, Laptop Computers, Headsets
- Bluetooth expects regular charging
  - Target is to use <10% of host power

ZigBee and Bluetooth

Address Different Needs

- ZigBee is better for devices where the battery is 'rarely' replaced
  - Targets are :
    - Tiny fraction of host power
    - New opportunities where wireless not yet used

An Application Example

Battery Life & Latency in a Light Switch

- **Wireless Light switch**
  - Easy for Builders to Install
- **A Bluetooth Implementation would:**
  - use the inquiry procedure to find the light each time the switch was operated.

Light switch using Bluetooth

- **Inquiry procedure to locate light each time switch is operated**
  - Bluetooth 1.1 = up to 10 seconds typical
  - Bluetooth 1.2 = several seconds even if optimized
  - **Unacceptable latency**

Light switch using ZigBee

- With DSSS interface, only need to perform CSMA before transmitting
  - Only 200 µs of latency
  - Highly efficient use of battery power

ZigBee offers longer battery life and lower latency than a Bluetooth equivalent

Wireless Keyboard

- Battery-operated keyboard
  - Part of a device group including a mouse or trackball, sketchpad, other human input devices
  - Each device has a unique ID
  - Device set includes a USB to wireless interface dongle
    - Dongle powered continuously from computer
  - Keyboard does not have ON/OFF switch
  - Power modes
    - Keyboard normally in lowest power mode
    - Upon first keystroke, wakes up and stays in a "more aware" state until 5 seconds of inactivity have passes, then transitions back to lowest power mode

Keyboard Usage

- Typing Rates
  - 10, 25, 50, 75 and 100 words per minute
- Typing Pattern
  - Theoretical: Type continuously until battery is depleted
    - Measures total number of hours based upon available battery energy

Wireless Keyboard Using 802.15.4

- 802.15.4 Operation Parameters
  - Star network
  - Non-beacon mode (CSMA-CA)
  - USB Dongle is a PAN Coordinator Full Functional Device (FFD)
  - Keyboard is a Reduced Function Device (RFD)
  - Power Modes
    - Quiescent Mode used for lowest power state
      - » First keystroke latency is approx 25ms
    - Idle mode used for "more aware" state
      - » Keystroke latency 8-12 ms latency

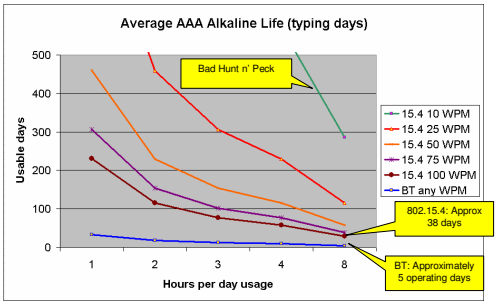
Wireless Keyboard Using 802.15.4

- 802.15.4 Chipset Parameters
  - Motorola 802.15.4 Transceiver and HCS08 MCU
  - Battery operating voltage 2.0 – 3.6 V
    - All required regulation internal to ICs
    - Nearly all available energy usable with end of life voltage at 2.0 volts

Wireless Keyboard Using Bluetooth

- Bluetooth Operation Parameters
  - Piconet network
  - USB Dongle is piconet Master
  - Keyboard is a piconet Slave
  - Power Modes
    - Park mode used for lowest power state
      - » 1.28 second park interval
      - » First keystroke latency is 1.28s
    - Sniff mode used for "more aware" state
      - » 15ms sniff interval
      - » 15ms latency

BT vs. 15.4 Keyboard Comparison



Why BT and ZigBee are so different?

- Bluetooth and 802.15.4 transceiver physical characteristics are very similar
- Protocols are substantially different and designed for different purposes
- 802.15.4 designed for low to very low duty cycle static and dynamic environments with many active nodes
- Bluetooth designed for high QoS, variety of duty cycles, moderate data rates in fairly static simple networks with limited active nodes
- Bluetooth costs and system performance are in line with 3rd and 4th generation products hitting market while 1st generation 15.4 products will be appearing only late this year