18-452/18-750
Wireless Networks and Applications
Lecture 20: PAN

Peter Steenkiste
Carnegie Mellon University

Spring Semester 2020
http://www.cs.cmu.edu/~prs/wirelessS20/

Announcements

- Sign up for project meetings
  - » Goal is to discuss your topic(s) and identify questions that you should focus on first
  - » Meetings are this week and hopefully this week
  - » Sign up!
- Midterm preparation
  - » There is a discussion thread on Canvas where you can list questions for the review on Friday
  - » I will have extra office hours Monday 11-noon
- Survey topics/teams are due now!
  - » E-mail
- Return P1 equipment to Justin

Outline

- 802.15 protocol overview
- Bluetooth
- Personal Area Networks – 802.15
  - » Applications and positioning
  - » Bluetooth
  - » High speed WPAN
  - » Zigbee
  - » Other
- UWB

IEEE 802.15: Personal Area Networks

- Target deployment environment: communication of personal devices working together
  - » Short-range
  - » Low Power
  - » Low Cost
  - » Small numbers of devices
- Four groups of standards:
  - » IEEE 802.15.1 – "Bluetooth"
  - » IEEE 802.15.2 – Interoperability (e.g. Wifi)
  - » IEEE 802.15.3 – High data rate WPAN (WiMedia)
  - » IEEE 802.15.4 – Low data rate WPAN (ZigBee)
  - » IEEE 802.15.6 – Body Area Networking
  - » IEEE 802.15.7 – Visible Light Communication

Some Common Themes

- Master/slave notion
  - » Or simple node versus coordinator
- Use of "piconets"
  - » Small groups of devices managed by a master or coordinator
  - » Scalability is not a concern
- Support for QoS
  - » Want to support voice and other media
- But many variants in how this functionality is supported

Bluetooth

- Think USB, not Ethernet
  - » Cable replacement technology
- Originally defined as IEEE 802.15.1, but standard is now maintained by the Bluetooth Special Interest Group
  - » Created by Ericsson
- Some features:
  - » Up to 1 Mbps connections (original version)
  - » 1600 hops per second FHSS
  - » Includes synchronous, asynchronous, voice connections
  - » Piconet routing
- Small, low-power, short-range, cheap, versatile radios
- Used as Internet connection, phone, or headset
- Master/slave configuration and scheduling

IEEE 802.15.1

- Adopted the Bluetooth MAC and PHY specifications
- IEEE 802.15.1 and Bluetooth are almost identical regarding physical layer, baseband, link manager, logical link control and adaptation protocol, and host control interface
- Range of up to 30 feet, uses FHSS
- Data transfer rates of up to 1 Mbps
  - » Up to 3 Mbps for version 2
- Not designed to carry heavy traffic loads

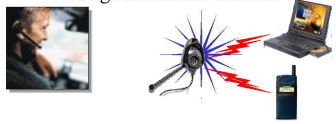
Bluetooth Standards

- Core specifications: defines the layers of the Bluetooth protocol architecture
  - » Radio - air interface, txpower, modulation, FH
  - » Baseband - power control, addressing, timing, connections..
  - » Link manager protocol (LMP) - link setup & mgmt, incl. authentication, encryption, …
  - » Logical link control and adaptation protocol (L2CAP) - adapts upper layer to baseband
  - » Service discovery protocol (SDP) – device info, services and characteristics.

Bluetooth "Profiles"

- Profile specifications describe the use of BT in support of various applications
  - » Includes which parts of the core specification are mandatory, optional or not applicable
- Data and voice access points
  - » Real-time voice and data transmissions
- Cable replacement
  - » Eliminates need for numerous cable attachments for connection

Usage scenarios: Headset



Usage scenarios: Synchronization

Some Example Profiles

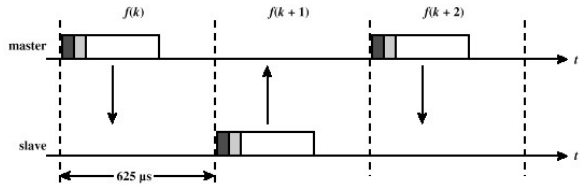
- Audio/video profile
- Fax profile
- Basic printing profile
- Serial port profile
- PAN profile
- Phone book access profile
- Headset profile
- LAN access profile
- Service discovery profile
- Cordless phone profile

Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Total bandwidth divided into 79 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
  - » Remember that all communication is with the master, i.e., only one transmitter at any time

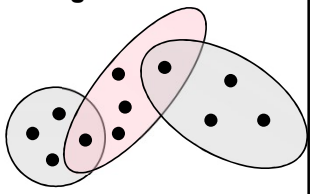
Sharing the Channel

- Bluetooth devices use time division duplex (TDD)
- Access technique is TDMA
- FH-TDD-TDMA

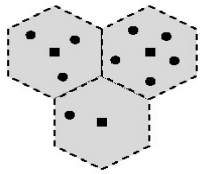


Piconets are Basis for Topology

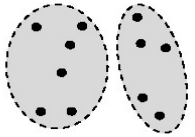
- Master with up to 7 active slaves
  - Slaves only communicate with master
  - Slaves must wait for permission from master
- Master picks radio parameters
  - Channel, hopping sequence, timing, …
- Scatternets can be used to build larger networks
  - A slave in one piconet can also be part of another piconet
  - Either as a master or as a slave
  - If master, it can link the piconets



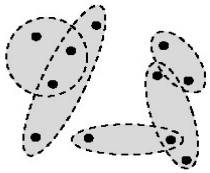
Wireless Network Configurations



(a) Cellular system (squares represent stationary base stations)



(b) Conventional ad hoc systems



(c) Scatternets

Bluetooth Piconet

- A collection of devices connected via Bluetooth technology in a master-slave network
  - Master functions as the piconet coordination (PNC)
- The piconet starts with two connected devices, and may grow to eight connected devices
  - Devices are added by the master
- All Bluetooth devices are peer units and have identical implementations, but they play a master or slave role when connecting
  - Roles can be reversed
  - Example: headsets connects as master to phone but then becomes slave

Forming a piconet

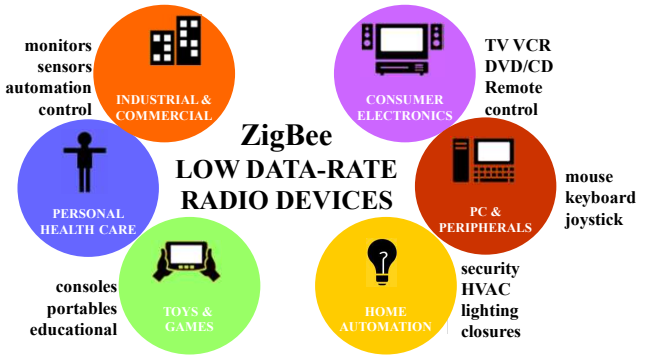
- Needs two parameters:
  - Hopping pattern of the radio it wishes to connect.
  - Phase within the pattern i.e. the clock offset of the hops.
  - Effectively defines a channel that must be unique to the piconet – master must scan for other piconets first
- The global ID defines the hopping pattern.
- The master shares its global ID and its clock offset with the other radios which become slaves.
- The global ID and the clock parameters are exchanged using a FHS (Frequency Hoping Synchronization) packet.

IEEE 802.15.4 - Overview

- Low Rate WPAN (LR-WPAN)
- Simple and low cost
- Low power consumption
  - » Years on lifetime using standard batteries
- Mostly in sensor networks
- Data rates: 20-250 kbps
- Operates at multiple frequencies
  - » 868 Mhz, 915 Mhz, 2.4 GHz
- Blends elements from 802.15.3 and 802.11
- Many versions exist for difference application domains

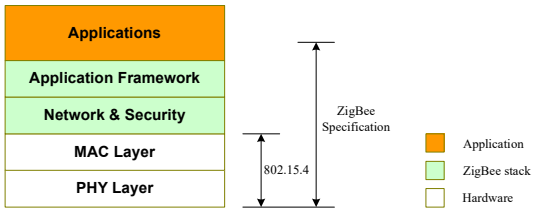
http://www.csie.nctu.edu.tw/~yctseng/WirelessNet06-02/zigbee-802-15-4.ppt

802.15.4 applications



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
  - PHY based on DSSS – runs at 250 Kbps in 2.4 GHz band
  - Links are encrypted



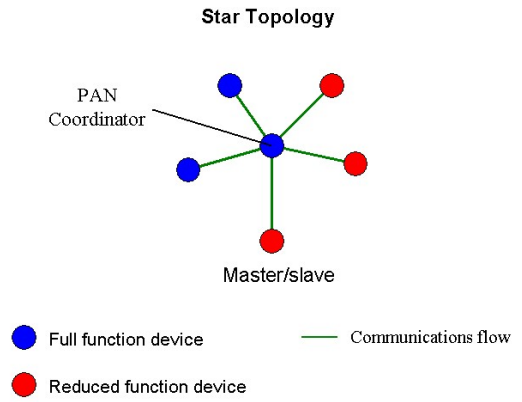
802.15.4 devices

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation

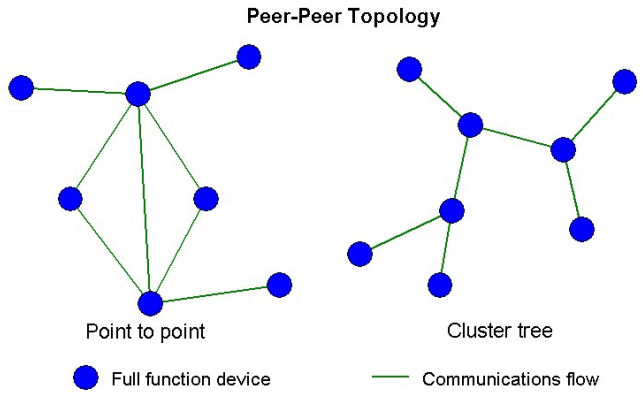
Roles

- **Devices (RFD or FFD)**
  - » must be associated to a coordinator
- **Coordinators (FFD)**
  - » can operate in peer-to-peer mode
  - » can form a PAN coordinated by a PAN coordinator
- **PAN Coordinator (FFD)**
- **Coordinator**
  - » manages a list of associate devices
  - » devices need to associate and disassociate
  - » allocates short addresses
  - » beacon frames (in beacon mode)
  - » processes requests for fixed time slots

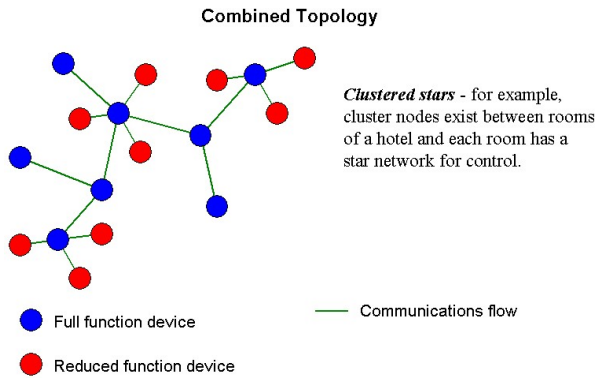
IEEE 802.15.4 - Star



IEEE 802.15.4 – Peer-to-Peer



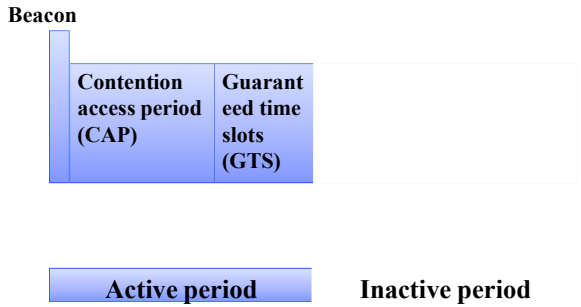
IEEE 802.15.4 - Combined



IEEE 802.15.4 - MAC

- One PAN coordinator & multiple RFDs/FFDs
  - » Association/disassociation
- CSMA-CA channel access
  - » Reliable delivery of data
- Optional superframe structure with beacons
  - » GTS mechanism
- AES-128 security
- QoS – 3 traffic types
  - » Periodic data: e.g. Sensor data
  - » Intermittent data: generated once a while, e.g. light switch traffic
  - » Repetitive low latency data: E.g. Mouse device traffic

802.15.4 superframe structure



Outline

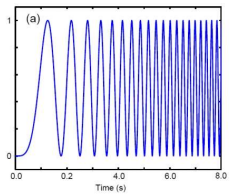
- 802.15 protocol overview
- Bluetooth
- Personal Area Networks – 802.15
  - » Applications and positioning
  - » Bluetooth
  - » Zigbee
  - » Other
- UWB

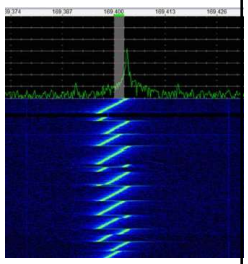
Low Power Technologies

- Battery life times of years or even decades
  - » Ubiquitous deployment of sensors
  - » Internet of Things (IoT), automation, …
  - » Replacing batteries is labor intensive
- Bluetooth Low Energy
  - » Not backwards compatible; deployed in some phones
  - » Profiles for healthcare, proximity sensing, alerts, keyboard/mice/.., ..
  - » 2.4 GHz but simpler modulation schemes

Low-Power Wide-Area Networks (LPWAN)

- Longer range to simplify deployment
  - » "Metropolitan" area – cite-wide sensor network
  - » Single base station covers large area and many sensors
- Many competing proprietary technologies
  - » LoRa: chirp spread spectrum
- Sigfox
  - » Star topology, 900 MHz, ..
- LTE-MTC
  - » Machine Type Communication
  - » Defined by 3GPP





https://www.link-labs.com/blog/what-is-lora

Outline

- 802.15 protocol overview
- Bluetooth
- Personal Area Networks – 802.15
  - » Applications and positioning
  - » Bluetooth
  - » Zigbee
  - » Other
- UWB

Ultra WideBand

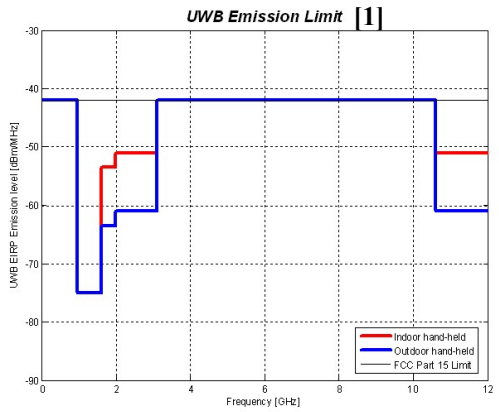
$$C = B\log_2(1+\mathrm{SNR})$$

- Can achieve high throughputs with low SNR by using a high B
- Motivation is the 802.15.3a (high rate PAN) standards effort
  - » Targets high speed, short distance communication
- But where do I find this much spectrum?
- Use a transmit power that is low enough to so it will not affect other users
  - » Can be used in most licensed frequency bands (with FCC permission, of course)

FCC UWB Rules

- UWB technically defined as:
  - » Width of signal > 500 MHz, or $B_f = 2\frac{f_H - f_L}{f_H + f_L} > 0.2$
- Approved for 3.1 GHz to 10.6 GHz
- Power limit is -41.3 dBm/MHz
  - » Note that the limit is not on the total signal but across the part of the spectrum that is used
- Results in a frequency mask that must be satisfied
- Certain narrow bands must be filtered out
  - » E.g. certain radio astronomy bands
  - » Depends on the country

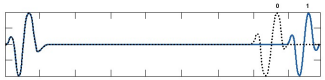
FCC Regulations



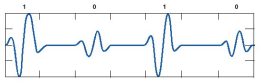
Example Technology: Basic Impulse Information Modulation

Pulse length ~ 200ps; Energy concentrated in 2-6GHz band; Voltage swing ~100mV; Power ~ 10uW

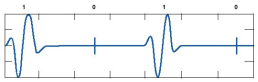
- **Pulse Position Modulation (PPM)**



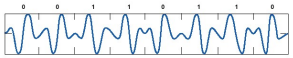
- **Pulse Amplitude Modulation (PAM)**



- **On-Off Keying (OOK)**

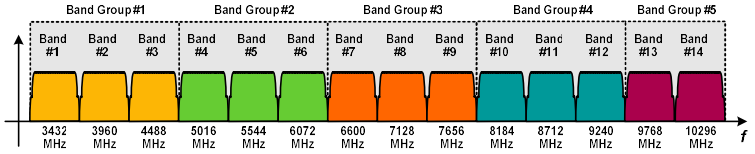


- **Bi-Phase Modulation (BPSK)**



Multi-band OFDM

- **Divide the spectrum into bands of 528 MHz.**



  - » **Transmitter and receiver process smaller bandwidth signals.**
  - » **Can spread symbols across multiple bands (FH)**
  - » **Can avoid bands based on local regulations**
- **Use of OFDM offer additional advantages**
  - » **Proven technology that is known to be efficient**
  - » **Can selectively disable subcarriers to protect narrow band signals**
  - » **For example: 128 tones of 5.125 MHz**

Discussion

- **UWB was included in 802.15 standards**
- **802.15.3a was going to use UWB but never materialized**
  - » **Fight between two competing proposals**
  - » **Example on previous slide is one of them**
- **Also added as 802.15.4a to the low power PAN group**
  - » **Provides for 3 "narrower" bands**
  - » **Not clear it is used**