ECE 435 – Network Engineering
Lecture 23B

Vince Weaver

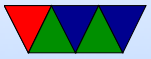
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

11 April 2024

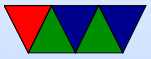
Announcements

- HW#10 will be posted
- Look up ECT-2020 NR? 1.9GHz?



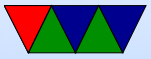
Bluetooth

- Personal Area Network (PAN)



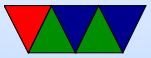
Bluetooth Applications

- Headsets
- Wireless controllers (Wii, PS3)

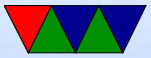


Bluetooth

- 1994 Ericsson. With IBM, Intel, Nokia and Toshiba formed a SIG.
- Named after Harald Blaatand (Bluetooth II (940-981) a Viking king who "united" (conquered) Denmark and Norway. Unite various standards.
- Symbol is runes for HB.
- Get rid of cables, specifically serial cables
- Interferes with 802.11
- IEEE came in an decided to take standard and make it

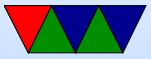


802.15.1 but no longer maintains it

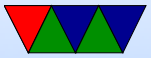


Bluetooth Architecture

- Basic unit: piconet, master node and up to seven *active* slave nodes within 10m
- Many can exist in an area, and can be connected by a bridge. Connected piconets are called a scatternet
- There can also be up to 255 “parked” nodes in a picnoet
- When parked, can only respond to activation on beacon
- Hold and siff?
- Slaves designed to be cheap, so dumb. Master is smart and runs them. slave/slave communication not possible



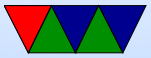
- Master broadcasts clock 312.5us. Master transmits in even, slave in odd.



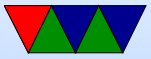
Bluetooth Applications – Profiles

Bluetooth V1.1 has 13 different application protocols.

- Required
  - generic access – link management
  - service discovery – discovering services
- - Serial port
  - Object exchange
- Networking
  - LAN access
  - Dial-up

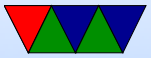


  - Fax
- Telephony
  - Cordless phone
  - Intercom
  - Headset
- File exchange
  - Object push
  - File transfer
  - Synchronization

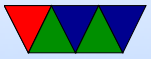


Bluetooth Layering

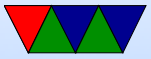
- Radio layer
  - 2.4GHz, 10 meters. 79 channels of 1MHz.
  - Frequency shift keying, 1 Mbps but consumed by overhead
  - Frequency hopping spread spectrum, 1600 hops/sec dwell of 625 usec. All nodes in piconet hop at once, with master controlling this (PRNG) 1,3, or 5 slots/packet
  - Interferes with 802.11. Bluetooth hops faster so causes



more trouble.
  - power output class: 100mW class 1, 2.5mW class 2, 1mW class 3.
- Baseband layer
  - Asynchronous Connection-less link (ACL) packet-switch data at irregular info, no guarantees. one per slice
  - Synchronous Connection Oriented (SCO) – for real time data.
  - Three per slave. Error correction. Each can send 64kpbs PCM audio

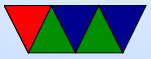


- L2CAP layer
  - accept packets of 64kB and break into frames.
  - Handles multiplexing.



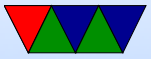
Bluetooth Frames

- Several different formats
- 72 bits access (identify master, as can be in range of multiple)
- 54 bit header
  - (addr(3) frame type(4), flow [buffer full](1), Ack (1) seq(1) checksum(8)
  - This is repeated 3 times.
  - Majority wins (redundancy, cheap small protocol)
- Data 0-2744 bits. SCO always 240 bits.



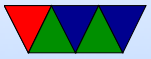
Bluetooth 1.1 (2002)

- First stable version
- Gaussian Freq-shift Keying (GFSK). Smooths signal instead of abrupt 1/0 transition
- 1Mbps peak in theory



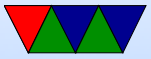
Bluetooth 1.2

- Adaptive frequency hopping, skip busy frequencies
- Up to 721kbps
- eSCO allow retransmitting corrupted packets, at expense of audio latency
- HCI host controller interface, three wire



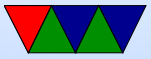
Bluetooth 2.0 (2004)

- 2.0
  - EDR = Enhanced Data Rate
  - BR/EDR 2 and 3Mbps
  - Pi/4 DQPSK – differential quadrature phase-shift keying
- 2.1
  - Secure simple pairing
  - Extended inquiry response



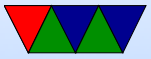
Bluetooth 3.0 (2009)

- Up to 25Mbps "HS" (high speed)
- Alternative MAC, bluetooth set up connection but 802.11 used to transmit data?



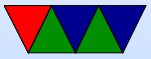
Bluetooth 4.0 (2010)

- Splits things in three, Classic, High-speed (wifi related), and the new Bluetooth Low Energy (BLE)
- BLE
  - Entirely new stack, designed for low power rapid setup links
  - 40 2MHz channels, 1Mbit/s
  - Max power 10mW
  - Not backwards compatible, but same frequency range
  - New profiles



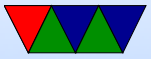
Bluetooth 5.0 (2017)

- Internet of things
- 2MBit/s
- 5.1 (2019) various things including angle of arrival
- 5.2 (2019)
- 5.3
- 5.4



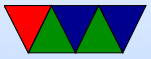
Setting up Connections

- In discoverable mode, will transmit name, class, services, etc on demand
- Has unique 48 bit number but that's rarely seen
- Bonding/Pairing – to avoid people stealing info from your device, require some sort of user interaction to connect for the first time. Before 2.1 it was a 16-byte pin code
- Secure simple pairing, pub key crypto



Security

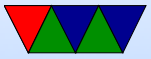
- Prior to 2.1 security can be turned off, and only good for 23.5 hours
- Exploits
  - "Bluejacking" – people walk around sending unwanted pictures/text to unsecured devices
  - Lots of issues over the years do to pairing



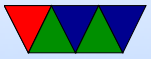
Linux Bluetooth

- Competing implementations (bluez, Affix)
- Install bluez
- bluetoothctl

```
[NEW] Controller B8:27:EB:05:9D:BB pi3 [default]
[bluetooth]# exit
[DEL] Controller B8:27:EB:05:9D:BB pi3 [default]
root@pi3:/home/vince# bluetoothctl
[NEW] Controller B8:27:EB:05:9D:BB pi3 [default]
[bluetooth]# scan on
Discovery started
[CHG] Controller B8:27:EB:05:9D:BB Discovering: yes
[bluetooth]# power on
```



```
Changing power on succeeded
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InProgress
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InProgress
[NEW] Device 64:8A:44:9D:DC:FD 64-8A-44-9D-DC-FD
[NEW] Device D3:E8:9D:CA:71:63 D3-E8-9D-CA-71-63
[CHG] Device D3:E8:9D:CA:71:63 RSSI: -89
```



Linux Bluetooth Investigation

- Can use tcpdump on it