Wireless

Arnav Gupta

December 5, 2024

Contents

1 Wireless Networks

Many more wireless phone subscribers than wired, and same for devices.

Challenges arise from wireless (communication over wireless link) and mobility (handling mobile user who changes point of attachment to network). Wireless $\neq$ mobile.

Base station is typically connected to wired network and relays packets between wired network and wireless hosts in its area.

Wireless link connects mobiles to base station and can be used as a backbone link. Multiple access protocol coordinates link access, and can have various data rates and transmission distance.

Infrastructure mode is how base station connects mobiles into wired network.

With **ad hoc mode**, no base stations and so nodes can only transmit to other nodes within link coverage. With this, nodes organize themselves into a network (route among themselves).

Wireless network taxonomy

- infrastructure, single hop: host connects to base station which connects to larger internet

- infrastructure, multiple hops: host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
- no infrastructure, single hop: no base station, no connection to larger internet (Bluetooth, ad hoc nets)
- no infrastructure, multiple hops: no base station, no connection to larger internet, may have to replay to reach a given wireless node

Long waves mean big antennas and small bandwidth. Best bands are lower ones, since better propagation characteristics and larger antennas. Issue is, more bandwidth on higher frequencies than lower ones, so lower ones are oversubscribed.

Spectrum not always used well and re-allocation often necessary. Spectrum is a scarce resource and hence is heavily reused. This can create **interference**.

Interference management and spectrum reuse are critical problems in wireless.

2 types of bands:

- licensed: used by cellular networks
- unlicensed: used by WiFi (and recently cellular)

Industrial, Scientific, Medical (ISM) wireless bands and is region of EM spectrum available for use without license:

- used for wireless LANs and PANs
- four separate bands

Key words are **rate**, **range**, and **power consumption**.

Lower frequency has longer range.

Half-duplex: a node cannot and receive at the same time

Decreased signal strength: radio signal attenuates as it propagates through matter (path loss), and some cannot cross walls at all

Interference from other sources: ISM bands shared by other devices and so devices can interfere with interference occurring in licensed bands due to reuse

Multipath propagation: radio signals reflects off objects ground, arriving at destination at slightly different times

All these make communication across wireless link difficult, but characteristics depend on the band and are time-varying.

Signal-to-Noise Ratio (SNR): larger means easier to extract signal from noise

Given physical layer, increasing power means increasing SNR and therefore decreasing BER.

Given SNR, choosing modulation and coding scheme that meets BER requirement means giving highest throughput.

SNR may change with mobility, by dynamically adapting physical layer (modulation technique and rate).

By increasing power, interference increases as well.

With multiple wireless senders and receivers, there are additional problems:

- hidden terminal problem: two nodes can talk to some intermediate node but cannot hear each other
- signal attenuation: two nodes have their signal attenuated by some intermediate node

Cellular has:

- wide area coverage, proprietary networks, and more coordination between base stations
- licensed (expensive) spectrum
- high mobility

Wi-Fi has:

- local area coverage, last link for Internet, and little coordination between access points
- unlicensed (free) spectrum (2.4 GHz and 5.3 GHz)
- low/no mobility

In IEEE standards, Ethernet is 802.3, Wi-Fi is 802.11, and Wireless PAN (Bluetooth) is 802.15.

1.1 802.11

802.11 Wireless LAN details:

- 802.11b: 1999, 11 Mbps, 30 m, 2.4 GHz
- 802.11g: 2003, 54 Mbps, 30 m, 2.4 GHz
- 802.11n (WiFi 4): 2009, 600 Mbps, 70 m, 2.4/5 GHz
- 802.11ac (WiFi 5): 2013, 3.47 Gbps, 70 m, 5 GHz
- 802.11ax (WiFi 6): 2020, 14 Gbps, 70 m, 2.4/5 GHz
- 802.11af: 2014, 35-560 Mbps, 1 km, unused TV bands
- 802.11ah: 2017, 347 Mbps, 1 km, 900 MHz

All WiFi use CSMA/CA for multiple access, have access point and ad-hoc network versions, and have a random access mode (DCF: distributed coordinated function) and polling mode (PCF: point coordination function).

802.11b's 2.4GHz-2.485 GHz spectrum is divided into 14 channels at different frequencies. The access point admin chooses a channel for the access point. Interference is possible since the channel chosen can be the same as the neighbouring access point.

Since channels are at 22MHz bandwidth, channels overlap. Channels 1, 6, and 11 can operate simultaneously with no interference.

At 5GHz, there are 24 non-overlapping channels.

1.1.1 Architecture

Wireless host communicates with access point.

Basic Service Set (BSS) in infrastructure mode contains wireless hosts and access point.

There is an adhoc mode with no access point, but much less used.

A network administrator allocates a name (SSID) to each access point.

Arriving host must associate with an access point:

1. scans channels, listening for beacon frames containing SSID and access point's MAC address
2. selects access point to associate with

3. may perform authentication
4. typically run DHCP to get IP address in access point's subnet

Passive Scanning

1. Beacon frames sent from APs (on different channels)
2. Association Request frame sent: host to selected AP
3. Association Response frame sent: selected AP to host

Active Scanning

1. Probe Request frame broadcast from host (on all channels)
2. Probe Response frames sent from APs
3. Association Request frame sent: host to selected AP
4. Association Response frame sent: selected AP to host

Passive scan generally takes more time, uses less energy, and if client does not wait long enough on a channel, it may miss an AP beacon.

802.11 uses CSMA for multiple access (sense before transmitting, but don't collide with ongoing transmission by other nodes) and no collision detection since difficult to receive when transmitting due to weak received signals:

- cannot sense all collisions in any case due to hidden terminal and fading
- goal: avoid collisions with two CA mechanisms

For CSMA/CA:

- 802.11 sender:
    1. if sense channel idle for DIFS, then transmit entire frame (no CD)
    2. if sense channel busy, then start random backoff time, timer counts down while channel idle, then go to 1 when timer expires
- 802.11 receiver
    1. if frame received OK, return ACK after SIFS<DIFS (ACK needed due to hidden terminal problem and bad channel conditions)
    2. if no ACK, after timeout, increase random backoff interval, try again to transmit starting at the beginning of the process (max 7 trials)

To avoid collisions when hidden terminals, sender reserves channel use for data frames using small reservation packets:

- sender first transmits small request-to-send (RTS) packet to AP using CSMA
  - RTSs may still collide with each other (but short)
- AP broadcast clear-to-send CTS (after SIFS) in response to RTS with NAV
- CTS heard by all nodes (since AP can be heard by everyone)
  - sender transmits data frame
  - other stations defer transmissions

This approach avoids data frame collisions completely using small reservations packets.

802.11 frame has:

- frame control: 2 bytes
  - protocol version → 2 bits
  - type → 2 bits, RTS, CTS, ACK, data
  - subtype → 4 bits
  - to AP → 1 bit
  - from AP → 1 bit
  - more frag → 1 bit
  - retry → 1 bit
  - power management → 1 bit
  - more data AP → 1 bit
  - WEP → 1 bit
  - rsvd → 1 bit
- duration: 2 bytes, duration of reserved transmission time (NAV in RTS/CTS)
- address 1: 6 bytes, MAC address of wireless host to receive this frame

- address 2: 6 bytes, MAC address of wireless host or AP transmitting this frame
- address 3: 6 bytes, MAC address of router interface to which AP is attached
- sequence control: 2 bytes, frame sequence number for reliable data transfer
- address 4: 6 bytes, used only in ad hoc mode
- payload: 0 to 2312 bytes, datagram or ARP packet, rarely greater than 1500 bytes
- CRC: 4 bytes

Issues with mobility are handover and keeping TCP alive (is learning fast enough).

802.11 also has **power management**:

- node-to-AP: AP knows not to transmit frames to this node, so node wakes up before next beacon frame (one beacon frame every 100 ms)
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent, otherwise sleep again until next beacon frame (wakeup is 250 ms)

Personal Area Network (PAN): less than 10 m diameter (short range), low power, low rate, 2.4 GHz, up to 2 Mbps

- evolved from Bluetooth specification
- replacement for cables
- ad hoc: no infrastructure, 8 active devices at a time, 255 parked
- master/slaves: a node becomes master
  - master rules, its clock determine time, transmit in odd-numbered slot (625 μs)
  - slaves only transmit to master on even-numbered slot after being talked to