eecs 489 COMPUTER NETWORKS

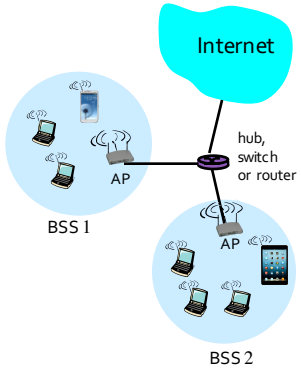
Lecture 39:
Wireless Air Interface: Multiple Access, WiFi

MAC Protocols: a Taxonomy

Three broad classes:

1. Channel Partitioning
   - divide channel into smaller "pieces" (time slots, frequency, code)
   - allocate each piece to a node for exclusive use, no collision
   - TDMA, FDMA, CDMA
2. Polling, reservation, "taking turns"
   - nodes take turns, but nodes with more to send can take longer turns
   - token ring, OFDMA
3. Random Access
   - channel not divided, allow collisions
   - must "recover" from collisions
   - CSMA/CD, CSMA/CA

802.11 LAN Architecture



Wireless host communicates with base station/access point (AP)

Basic Service Set (BSS) (a.k.a. "cell") in infrastructure mode contains:
- wireless hosts
- access point (AP): base station

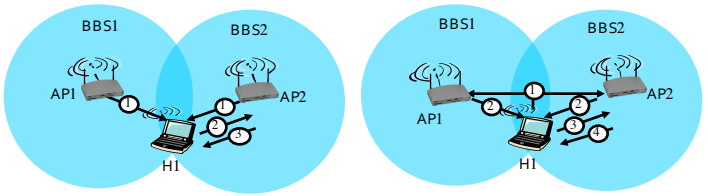
Ad hoc mode contains only hosts

802.11: Channels and Association

802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
- AP admin sets AP at a certain channel/frequency
- interference if channel chosen is same as that of neighboring AP(s)!

Host: must associate with an AP
- AP sends periodic beacon frames containing AP's name (SSID) and MAC address
- hosts scans channels, listening for beacon frames
- host selects an AP to associate with
- AP may perform authentication
- DHCP typically used to assign IP addresses in AP's subnet

802.11: Passive/Active Scanning



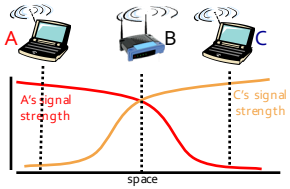
Passive Scanning:
1. beacon frames sent from APs
2. association request frame sent from H1 to selected AP2
3. association response frame sent from selected AP2 to H1

Active Scanning:
1. probe request frame broadcast from H1
2. probe response frames sent from APs
3. association request frame sent from H1 to selected AP2
4. association response frame sent from selected AP2 to H1

Wireless Network Characteristics

Multiple wireless senders and receivers create additional problems (beyond shared access):

Hidden terminal problem
- B, A can hear each other
- B, C can hear each other
- but A, C can't hear each other (obstacles block signal) ⇒ A, C unaware of their interference at B



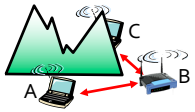
Signal fading:
- B, A can hear each other
- B, C can hear each other
- but A, C can't hear each other (signal has faded) ⇒ interfering at B

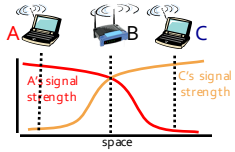
IEEE 802.11: Multiple Access

Collision: two or more nodes transmitting at same time

CSMA - sense before transmitting
CD – collision detection
- listens for collision while transmitting
- aborts and tries again if collision "detected"

But no collision detection in wireless environment!
- difficult to sense collisions when transmitting: strength of received signals is much smaller, expensive to build hardware that detects collisions
- can't sense all collisions in any case: hidden terminal, fading
- instead, avoid collisions: CSMA/CollisionAvoidance

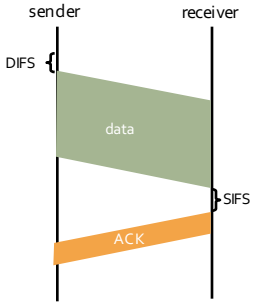




IEEE 802.11 CSMA

802.11 sender:
1. if sense channel idle for Distributed Inter-Frame Spacing (DIFS) time, transmit entire frame (no CD)
2. if sense channel busy start DIFS+random backoff time (why the random part?)
   - timer counts down while channel is idle
   - transmit when timer expires
3. if no ACK, increase random backoff interval, repeat step 2 (a few times)

802.11 receiver:
- if frame received OK, return ACK after Short IFS time (why do we need to ACK?)



Use of SIFS and DIFS prioritize ACKs over data frames

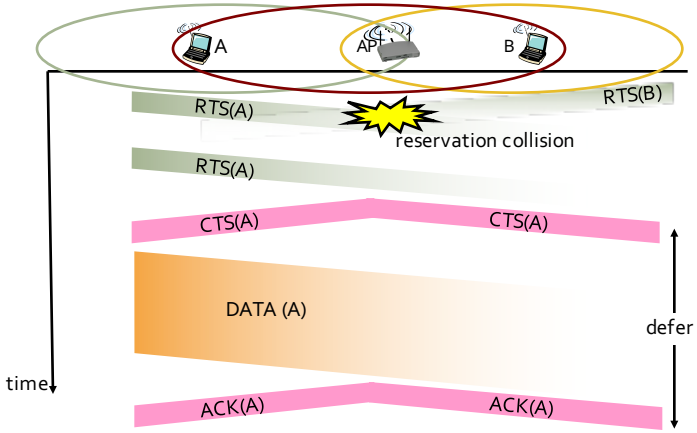
IEEE 802.11 Collision Avoidance

Sender "reserves" channel: transmits a small request-to-send (RTS) packet, including length of data, to AP using CSMA
- RTSs may collide with each other, but they're short

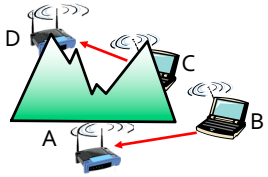
AP broadcasts clear-to-send (CTS) in response to RTS
RTS heard by all nodes
- sender transmits data frame
- other nodes defer transmissions

Avoid data frame collisions completely by using small reservation packets!

RTS-CTS Solves Hidden Terminal

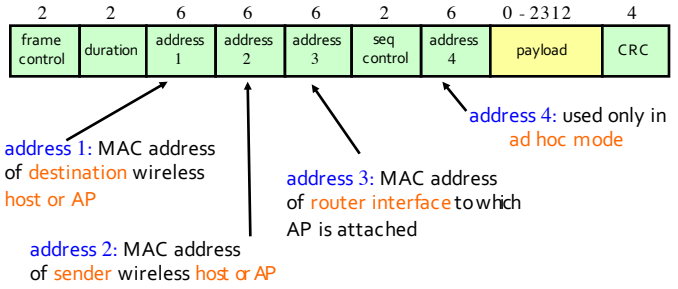


RTS-CTS Solves Exposed Terminal

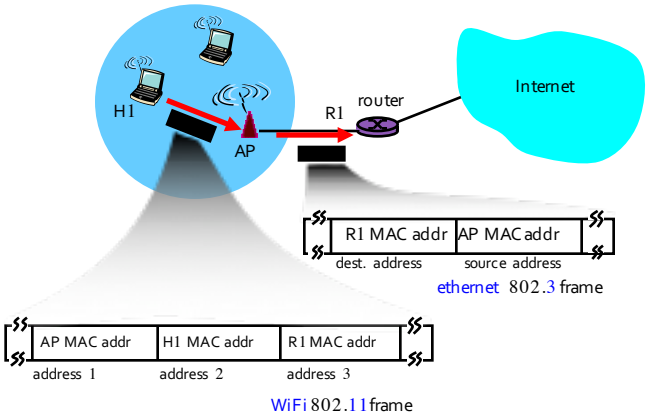


Exposed terminal problem:
- B sends to A
- C can send to D without interfering with B's transmission to A, but CSMA would prevent it from sending (A is unnecessarily "exposed" to C)
- Solution: if C hears B's RTS but not A's CTS, C knows its transmission won't interfere with A's and can send to D

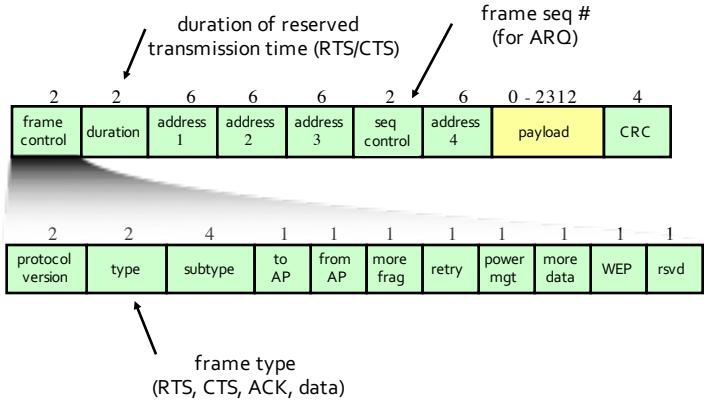
802.11 Frame: Addressing



802.11 Frame: Addressing



802.11 Frame: More



802.11: Power Management

Power management

- host-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if it has frame incoming; otherwise sleep again until next beacon frame

802.11i: Improved 802.11 Security

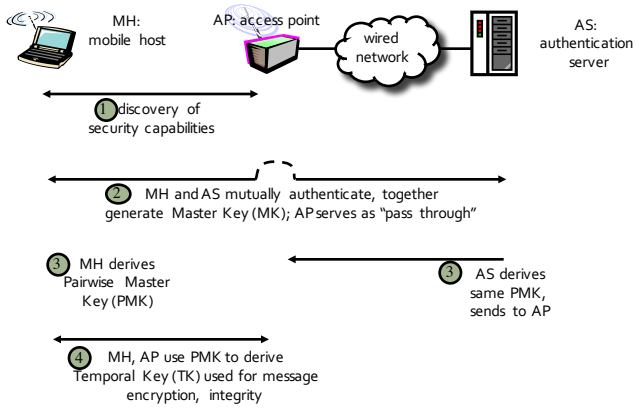
WPA2 or RSN (Robust Security Network): a 2004 amendment to the original 802.11 standard, incorporated into the 2007 updated 802.11 standard

- replaces Wireless Equivalent Privacy (WEP)
  - broken: reused key stream can be easily detected
- subsumes WPA (Wi-Fi Protected Access)

Provides key distribution

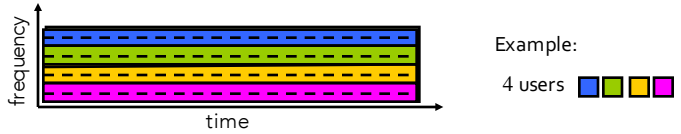
Uses authentication server separate from AP

802.11i Encryption Key Distribution

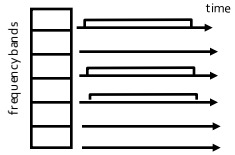


FDMA: Frequency DMA

- channel spectrum divided into frequency bands
- each node assigned a fixed frequency band
- well-known example: broadcast radio



- unused transmission time in frequency bands go idle
- example: 6-node LAN, only nodes 1, 3, 4 have packets, frequency bands 2, 5, 6 idle



Frequency Hopping (FH)

Multiple carrier frequencies used over the course of a transmission

Two reasons for frequency hopping:

1. frequency diversity: independent fading characteristics
2. interference avoidance:
   - very unlikely that all channels in the band experience interference; FH averages interference
   - dynamically detect persistently busy channels and avoid them

Two kinds of FH:

1. slow hopping: change of carrier frequency happens at the rate slower than the symbol rate
   - e.g., GSM, carrier frequency changed once per time slot
2. fast hopping: carrier frequency changes faster than the symbol rate

[Kostanic

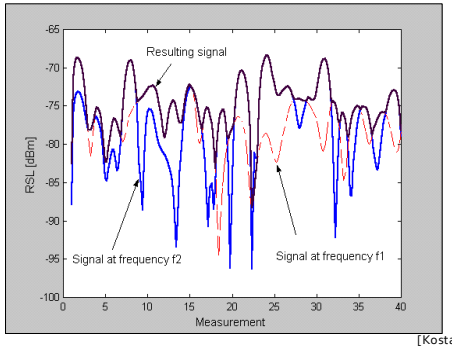
Frequency Diversity

Mobile environment is characterized by small scale fading

The depth of signal fade is a function of frequency

If two signals are sufficiently separated in frequency domain they fade independently

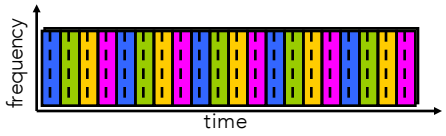
Frequency diversity gain diminishes for fast moving mobiles



[Kostanic

TDMA: Time DMA

- channel divided into N time slots, one per node
- access to channel in "rounds"
- each node gets fixed length slot (length = packet transmission time) in each round



Example:

4 users

- inefficient with light load: unused slots go idle
- example: 6-node LAN, nodes 1, 3, 4 have packets, time slots 2, 5, 6 go idle

CDMA: Code DMA

Unique "code" (c) assigned to each node; i.e., code set partitioning

All nodes share the same frequencies, but each node has its own "chipping" sequence (i.e., code) to encode data

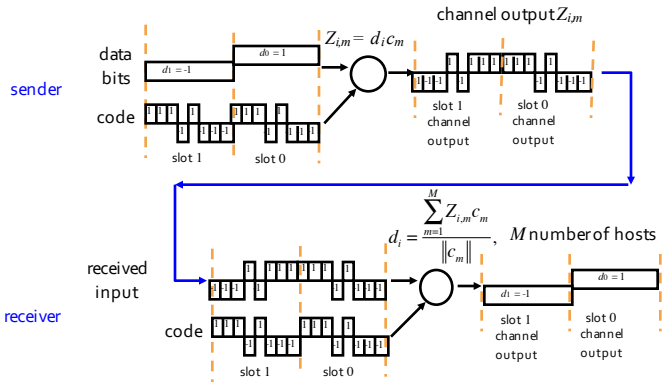
Codes are orthogonal or have low cross correlation

Encoded signal for bit i with node's code, of length M: $Z_{i,m} = d_i\, c_m$; d_i: bit i of data; c_m: bit m of code, $1 \le m \le M$

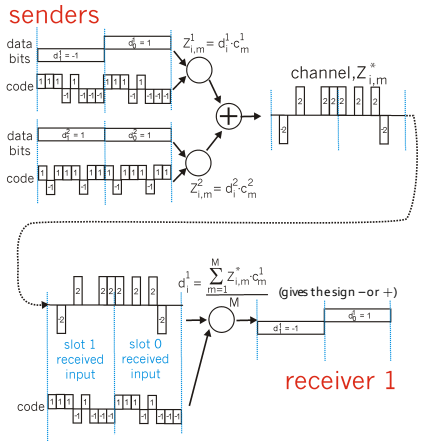
Decoding: dot-product of encoded signal and chipping sequence divided by $\|c_m\| = d$

Allows multiple users to "coexist" and transmit simultaneously with minimal interference (because codes are orthogonal or have low cross correlation)

CDMA Encode/Decode



CDMA: Two-Sender Case



CDMA Decoding

Receiver extraction works because each bit of code (c_m) is equally likely to be -1 or $+1$

So if the wrong code (c'_m) is used to decode, $\sum c_m c'_m$ is likely to be 0

If the right code is used, the sign of $\sum c_m c'_m$ determines whether data is $+1$ or -1

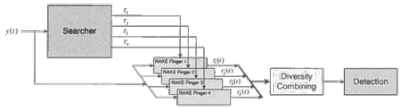
Instead of low-cross correlation random code per sender, can use orthogonal codes which guarantees $\sum c_m c'_m = 0$ if the wrong code is used to decode

CDMA: Issues

Code choice: Barker (802.11), Walsh (cdmaOne), Orthogonal Variable Spreading Factor (WCDMA/UMTS)

Power control: powerful signal interferes with others

- open-loop: mobile observe received signal, adjust its own transmit signal, works for TDD, not so well for FDD
- closed-loop: base station tells mobile to increase/decrease power; requires fast feedback time



RAKE receiver:

- takes advantage of multipathing: multiple copies of streams arrive at the receiver as signal is bounced off the environment; with RAKE receiver, late arriving copies used to help strengthen the signal
- enables soft handoff: a mobile receives copies from multiple base stations during handoff

[Kwok & Lau]

Orthogonal Frequency Division Multiplexing (OFDM)

Modulation: changing/modulating the carrier frequency, phase, and/or amplitude to carry information

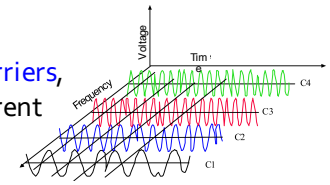
Multiplexing: mixing information from multiple sources to share a channel

Despite its name, OFDM is a modulation method, not a multiple access method; but it's a multi-carrier modulation method, i.e., signal is split into sub-signals that are then multiplexed onto the channel

[Langton]

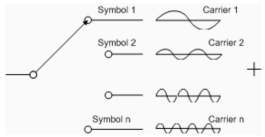
OFDM

Carrier is split into sub-carriers, $C1, \ldots, Cn$, each of a different frequency



Each sub-carrier is modulated by data, in sequence, using a conventional modulation scheme (QAM, PSK, etc.) at a low, $1/n$, symbol rate

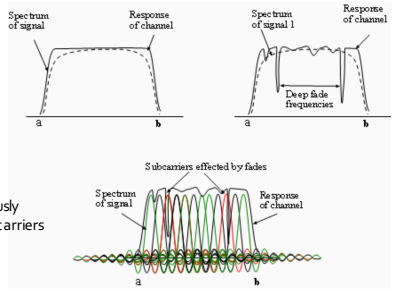
- besides, fast symbol rates are more susceptible to multi-path distortion



[Langton]

OFDM

FDM: data is transmitted over only one carrier



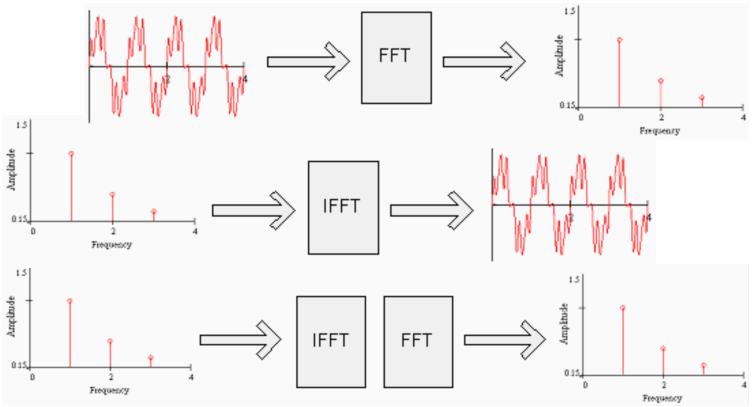
OFDM: data is simultaneously transmitted over several carriers

Advantages of OFDM:

- robust against multi-path distortion: fading and inter-symbol interference (ISI)
- robust against narrow-band interference
- high spectral efficiency, no need for band guards

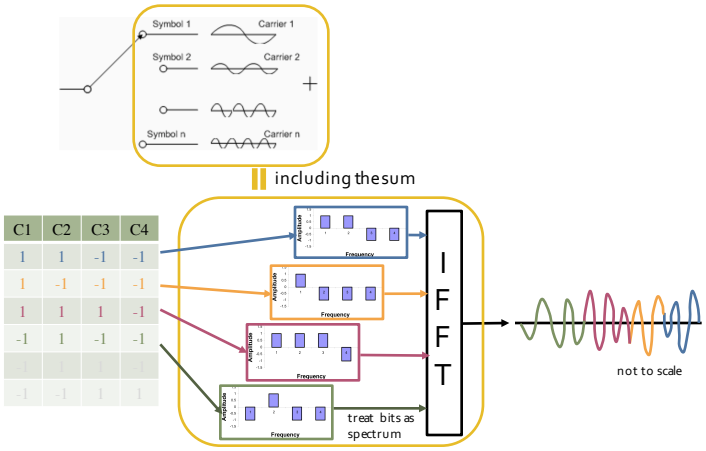
[Dahlman, Keithley]

FFT and Inverse FFT



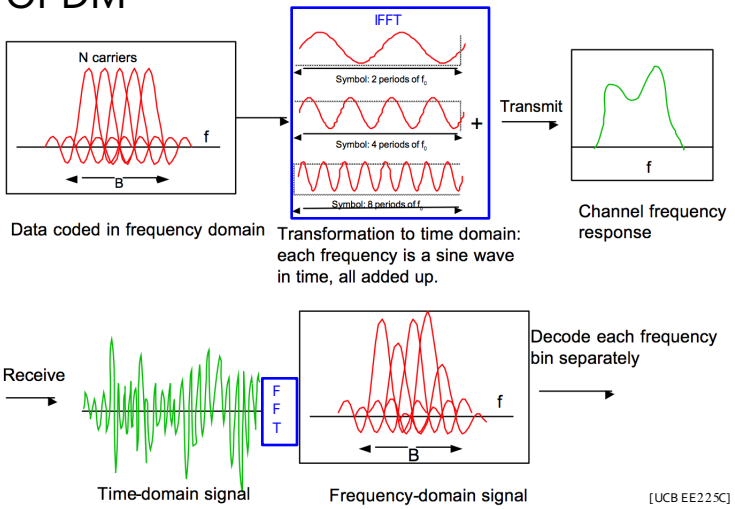
[Langton]

OFDM Encoding



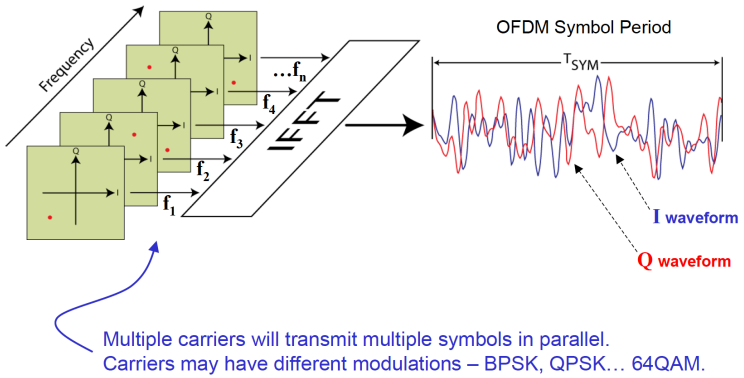
[Langton]

OFDM



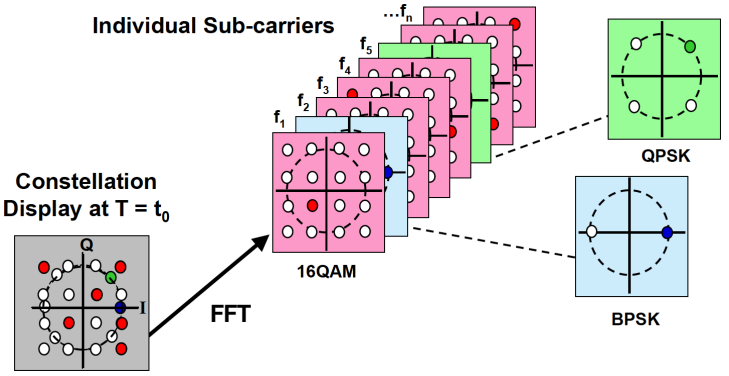
[UCB EE225C]

OFDM Encoding



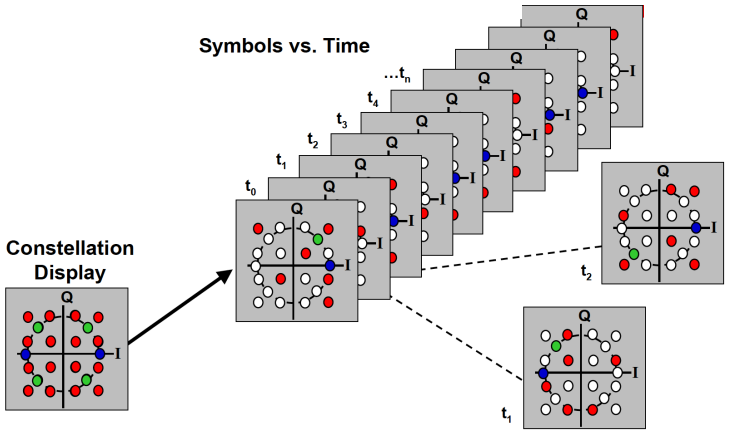
[Keithley]

OFDM Decoding



[Keithley]

OFDM Constellation over Time



[Keithley]

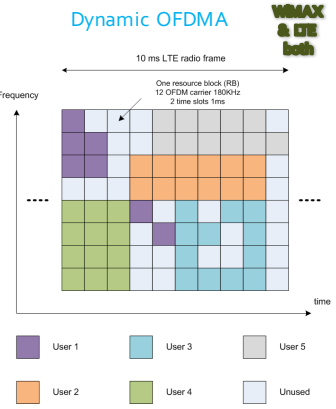
OFD Multiple Access (OFDMA)

OFDM is a modulation method for a single user: all sub-carriers in a channel are used to carry a single user's signal

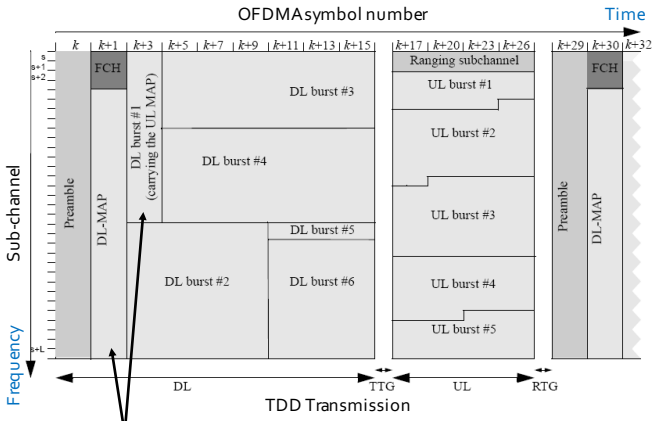
OFDMA is a multiple-access method: it assigns different set of sub-carriers to different users the way CDMA assigns different chipping codes to different users

Dynamic OFDMA: allocation per user is dynamically allocated over time (slotted)
⇒ OFDMA with statistical multiplexing

Scalable OFDMA: number of sub-carriers scales with bandwidth, bandwidth of sub-carriers is fixed



OFDMA: DL, UL Scheduling



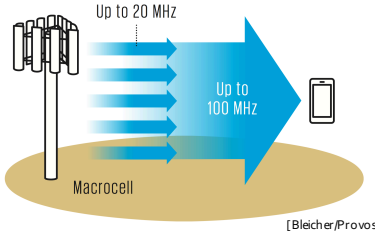
base station tells mobiles who will get to receive (DL map) and who will get to send (UL map), and when

LTE-Advanced

"True 4G": meets the ITU specifications for 4G
download rate: 3 Gbps (vs. 300 Mbps LTE)
upload rate: 1.5 Gbps (vs. 75 Mbps)

Five key features:

1. Carrier aggregation: can combine up to 5 non-consecutive LTE frequency channels, each up to 20 MHz wide

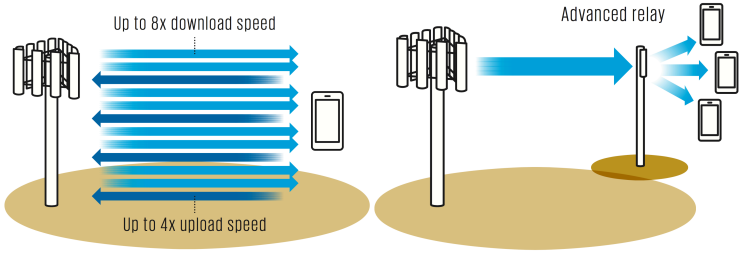


[Bleicher/Provost]

LTE-Advanced

2. Spatial multiplexing: uses MIMO to send parallel streams

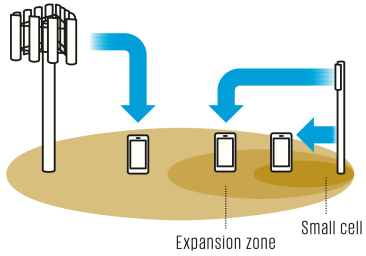
3. Advanced relays: relays decode signals and forward only those intended for nearby users



[Bleicher/Provost]

LTE-Advanced

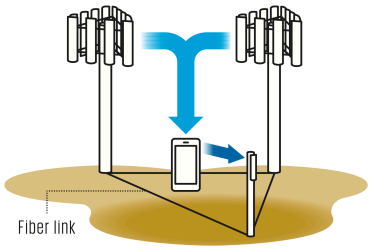
4. Enhanced inter-cell interference coordination (eICIC): supports lower-power small cell within a traditional macrocell: the two cells dynamically coordinate use of spectrum, allowing the small cell to expand its range



[Bleicher/Provost]

LTE-Advanced

5. Coordinated multipoint (CoMP) transmission: allows several base stations to serve a single cell: a mobile connects to all of them simultaneously, e.g., mobile could download from high-power towers while uploading to a nearby small cell



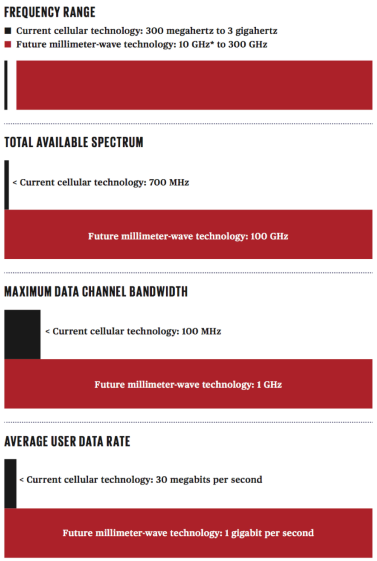
[Bleicher/Provost]

5G

Standards . . . still evolving

Goals and means:

- higher bandwidth: 20 Gbps indoor (vs. 1 Gbps 4G), order of 10 Mbps for order of 10^3 users outdoor
  - 8 GB HD movie in 6 seconds, vs. 7 minutes for 4G, >1 hour for 3G
  - can use millimeter-wave frequencies (10 to 300 GHz vs. 300 MHz to 3 GHz)



[Young15, Rappaport14]

5G

Other goals:

- higher spectral efficiency: 4.5 bps/Hz (vs. 1.5 bps/Hz 4G)
- higher data density: 10 Mbps/m^2 (vs. 0.1 Mbps/m^2)
- higher device density: 1 M/km^2 (vs. 100K/km^2): Internet of Things (IoT), machine-to-machine (M2M) sensor network
- ultra-low latency: 1 ms (vs. 50 ms)
- higher mobility: 500 km/h (vs. 350 km/h)
- lower energy: 100 Kbits/millijoule (vs. 1Kbits/millijoule)

[Young15]

5G

Other means:

- massive MIMO: e.g., 64 antennae on a Post-It note-sized area
- heterogeneous network architectures: combination of pico cells, small cells, macro cells: mobile can use all of them
- radio-access network virtualization: RAN processor virtualized into the cloud
  - content cached close to user

	CURRENT CELLULAR TECHNOLOGY	FUTURE MILLIMETER-WAVE TECHNOLOGY
Single antenna length in free space	At 700 MHz: 21.3 centimeters	At 28 GHz: 0.5 cm
Maximum urban-transmission range	At 700 MHz: 3 kilometers	At 28 GHz: 300 meters
Signal attenuation	At 700 MHz *Air:* .005 decibels per kilometer *Heavy rain:* .02 dB/km	At 28 GHz *Air:* 0.1 dB/km *Heavy rain:* 10 dB/km

[Young15, Rappaport14]