# ECE 435 – Network Engineering
# Lecture 34

Vince Weaver

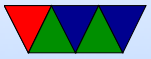
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

21 April 2025

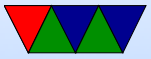
# Announcements

- HW#11 was posted
- Don't forget course reviews

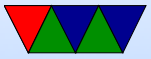


# Cellphone 3G

- 1998 - 2001
- Digital Voice and Data
- IMT-2000 standard (International Mobile Telecommunicatio
  - started planning 1992
  - 2000 was year to come out, frequency, and bandwidth
  - did not make any of those
- Wanted 2GHz worldwide but only China reserved
- 2Mbps stationary, 384kbps walking speed, 144kbps cars
- Security, more secure than 2G, better ciphers (KASUMI)

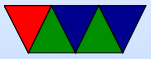


- Mix of connection and packet based
- Decommissioned, supposed to be early 2022 but Sprint held on to December 2022
- Why decommission? Using valuable frequencies wanted for 4G/5G, also cell companies not want to maintain all the equipment for fewer legacy users



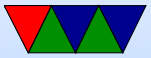
# 3G – W-DCMA vs CDMA2000

- differences mostly politics
- both based on CDMA
- EU wanted GSM compatibility
- US wanted IS-95 compat
- UMTS include both



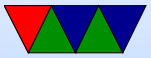
# 3G – More on advanced CDMA

- Chips
  - Chip is a +1 or -1V signal that has been modified by the carrier and actual bit
  - Called chip to distinguish from raw bits
  - 3.84Mchips/sec, sending code 4-256 chips
  - 256 chip code, 12kpbs (enough for voice)
  - 4 chip code, 1Mbps
- Chip sequences, but hard when not all arrive at same time, need some orthogonal with any start time



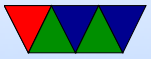
Instead use pseudo-random values, low cross-correlation

- For this to work handset power signals have to be regulated so roughly same reaching receiver (1500 times/sec)
- In order to be faster use more than one channel



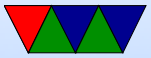
# 3G – CDMA Benefits

- Can take advantage of time when silent (60% of time)
- TDM and FDM can't do this, CDMA more channels can be used if there's quiet time
- CMDA only one frequency, don't have to hand out separate
- Can use directional (sectored) rather than omni-directional antenna
- Soft-handoff, on same frequency so can associate with new antenna before disconnecting from old



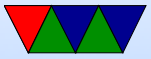
# 3G – Wideband CDMA (W-CDMA)

- Ericsson / EU UMTS (Universal Mobile Telecommunications System)
- 5MHz channels
- Different users can send data at different rates



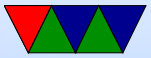
# 3G – CDMA2000

- Qualcomm
- 1.25MHz channels



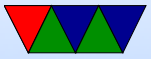
# Cellphone 4G

- Developed late 2000/early 2010s
- Digital Voice and Data, packet switched, often IPv6
- The "G" has become a marketing term
- The final spec was to be 4G needed 1Gbps (1Gbps stationary, 100Mbps mobile)
- Some companies jumped the gun and called things 4G that technically weren't



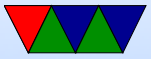
# First came 3.5G / 3.75G / 3.9G

- First implementations declared not really 4G
- Mobile WiMAX (Worldwide interop for microwave access) (IEEE 802.16e)
- LTE (Long Term Evolution)
- HPSA+ – evolved high speed packet access (3.75G)

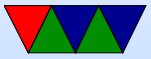


# Actual 4G

- IMT announced requirements for 4G
- All IP packet switch networks (calls via VOIP)
- Peak 100 Mbits (high mobility) 1Gbits (low mobility)
- More frequencies, 700MHz, 800MHz, 850MHz (some of these old analog TV)
- Channels 5-20MHz, optionally 40MHz
- Smooth handovers with heterogeneous networks
- Need for "good spectral efficiency" of 15bit/s/Hz down, 6.75 up



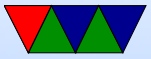
# 1GBit/s in less than 67MHz



# 4G Other

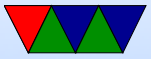
- IPv6
- MIMO antennas
- SDR (software defined radio) because so many frequency ranges
- OFDMA – OFDM combined with TDMA replaced CDMA

  Why no CDMA anymore? Reduced need for it when packet-switched?



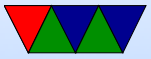
# 3.9G: Long-term Evolution Advanced (LTE)

- First release on 3.9G (need peak of 1Gbps to be 4G)
- Finalized 2008
- 300Mbps down, 75Mbps up
- Low latency (sub 5ms)
- Can handle mobile at up to 220mph to 310mph (depends on frequency)
- Flexible spectrum widths, 1.4, 3, 5, 10, 15, 20 MHz wide bads
- 20 active devices per cell



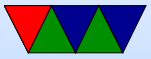
# 4G: Long-term Evolution Advanced (LTE-A)

- 2011
- Carrier aggregation (multiple channels for more speed in connection)
- 4x4 MIMO, 256 QAM
- 1Gbps
- Also an LTE Advanced Pro (4.5G), 3Gbps, 32-carrier aggregation

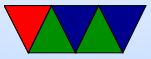


# Fixed WiMax

- IEEE 802.16
- Worldwide Interoperability for Microwave Access
- Fixed or mobile. Originally designed for "last mile" setup, (metropolitan area network) but used as 4G phone (mobile wi-max)
- Distance of miles
- Base station allocates time slot, good for VOIP and QoS
- Licenses spectrum from 2-11GHz and 10GHz-66GHz

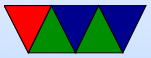


- can run in mesh mode where nodes can act as relays
- OFDM and OFDMA



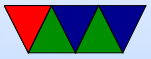
# WiMax mobile (pre-4G)

- 802.16e-2005
- handoffs and roaming
- Lower freq, 2.3 - 2.5GHz
- up to 75Mbps, can cover 30 mile radius
- soft and hard handoff



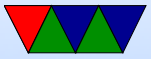
# WiMax Scheduling

- Unsolicited Grant Service (UGS) – voip w/o silence suppression
- Real-time Polling Service (rtPS) – video, voip w silence suppression
- Non-real-time Polling (nrtPS) – web browsing
- Best Effort (BE) – e-mail, message based
- Extended Real-Time Polling (ertPS) – video, voip w silence suppression



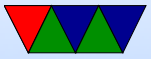
# 4G: WiMax2 (802.16m)

- 4G
- There's also a WiMax2+



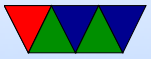
# Cellphone 4G – Radio Access Network (RAN)

- access node eNodeB – performs actions in physical layer
- Medium Access Control (MAC), Radio Link Control (RLC) Packet Data Control Protocol (PDCP)



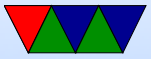
# VoLTE (Voice over LTE)

- Standard for Voice and SMS over LTE
- Smaller headers/packets than plain VoIP?
- Sometimes called “HD Voice” but that’s something different
- More complicated than you’d think



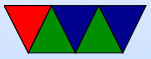
# Cellphone 4G – LTE, EPC

- Serving Gateway (S-GW) forwards packets when moving between eNodeBs
- Mobility Management Entity (MME) – tracks/pages the device and chooses SGW
- Packet Data Network Gateway (P-GW) – interfaces between user and pack data network (provide IP address, etc)
- Home Subscriber Server (HSS) – determines if user a valid subscriber



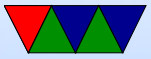
# Cellphone 5G

- 4G finally mature around 2014, working on next
- Whatever is used for faster access, 5G
- Goal is increase area capacity of network by 1000 times that of 4G
  - Ultra-densification. More cells per area. picocells (less than 100m diameter) or femtocells (Wi-fi like range). More complicated handoff
  - Increased bandwidth, millimeter waves. Current in MHz to GHz, so wavelength centimeters to a meter.



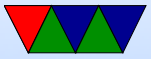
Crowded. Lots of unused in mm wave 20-300GHz. Do not penetrate well. Better antennas?

- MIMO (multiple input/output) – multiple antennas
- Network slicing



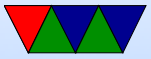
# Cellphone 5G – more

- Up to 20Gbps
- Bands
  - Frequency Range (FR)
  - FR1 Low band – similar to 4G, 600-900MHz
  - FR1 Mid band – 1.7GHz - 4.7GHz, towers several km (most common)
  - FR2 High-band – Gb/s bandwidth, 24.25-47GHz but reduced range
- Latency, ideal 8-12ms. HARQ retransmissions (FWD



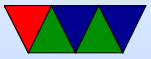
error correction, automatic repeat request), 50-500ms during handover

- Error rate, adaptive modulation and coding (MCS) to keep bit error rate low, reduce speed to reduce errors
- Frequency – interference with weather radar? Also some bands 3.7-3.98GHz interfere with poorly made airplane altimeters at 4.2GHz
- Coding change from polar to turbo
- FCC freeing up bands?



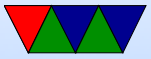
# 5G Applications

- emBB – enhanced mobile broadband – replacing 4G LTE
- URLLC – ultra-reliable low-latency communication
- mmtc – massive machine-type communication – IoT

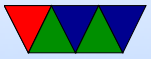


# Other 5G

- In theory up to 10Gbps or 20Gbps (10x faster than 4G)
- More realistically mid-bands 400Mbps - 1Gbps
- Latency 10-30ms? Longer when handover
- Auto drop speed if errors to reduce errors
- Higher density areas
- Higher bandwidth, used for FWA (fixed wireless access)
- 5G can come from satellite too, NTN (non-terrestrial network)
- Edge computing – opposite cloud computing, computing

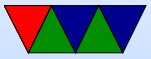


on devices



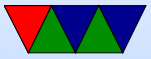
# 5G New Radio (NR) Standard

- 5G NR, OFDM, replace LTE (4G)
  FR1 Frequency Range 1 410MHz - 7.125GHz
  FR2 24.250 GHZ - 71 GHZ
- Dynamic Spectrum Sharing: 5G and 4G in same band
- Non-standalone: use 4G LTE for control, 5G for data
- Standalone, uses 5G both control and data
- NR-Light / RedCap (Reduced Capacity) – for simpler low-power devices, sensors, etc
- Wireless power transmission for IoT



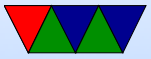
# 5G New Radio (NR) Standard

- Femtocell – 10 people, 10 meters
- Pico Cell – 100 people, 10 meters
- Micro Cell – 200 people, 100 meters
- Macro Cell – 200+people, hundreds meters



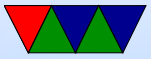
# VoNR (Vo5G)

- Voice over New Radio
- Similar to VoLTE
- All packet switched these days



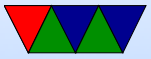
# Fronthaul

- Between Remote Radio Head and Base Band Unit. IEEE 1914.3 standard, new Ethernet frame with special (IQ?) headers?



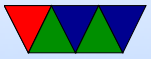
# Other 5.25G / 5.5G

- 5G-Advanced – 5.5. Machine Learning/AI?



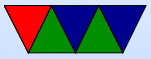
# 5G Security

- Worry about Chinese 5G gear



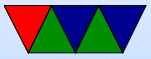
# 5G Interference

- 26GHz near bands used in weather radar
- Near 4GHz bands interfere with airplane altimeters
- 3.4GHz interfere with satellite C-band
- Some could use unlicensed 6GHz band, interfere with Wifi



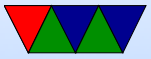
# Cellphone 6G?

- Every 10 years new version, so they are thinking about it
- Will be faster
- Nothing concrete yet
- Terrahertz bands?



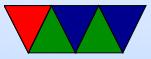
# Cellphones in Space

- 4G on moon?
- Nokia put LTE on moon on Athena probe, but it crashed and landed on side
- rovers and astronauts could use off-the-shelf phones?

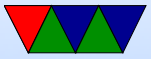


# Cellphone Security

- SIM chip cloning
- False base stations
  - Also rogue base stations, or Stingray
  - Laptop + transmitter impersonates base station
  - Small enough to carry around
  - Broadcast stronger signal than actual base station
  - Often used by law enforcement
  - In older days could force downgrade to 2G to break encryption



- App processor runs regular OSes (Android is Linux for example) so vulnerable to all the regular types of exploits
- Chinese / Huwawei gear banned by the US
- Location tracking by tower triangulation



# Other topics

- Emergency calling. Phones in theory should do this even if no SIM/plan installed
- Apps like wattsap / etc for messaging