ECE 435 – Network Engineering
Lecture 23

Vince Weaver

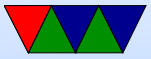
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

13 April 2023

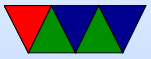
Announcements

- Don't forget status updates, I will send out preliminary schedule
- Will post HW#10 (Wifi)
- Finally figured out how to scan wifi



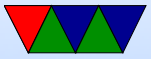
Cellphones

- What was life like before cellphones?
- Hard to keep up as things are constantly changing



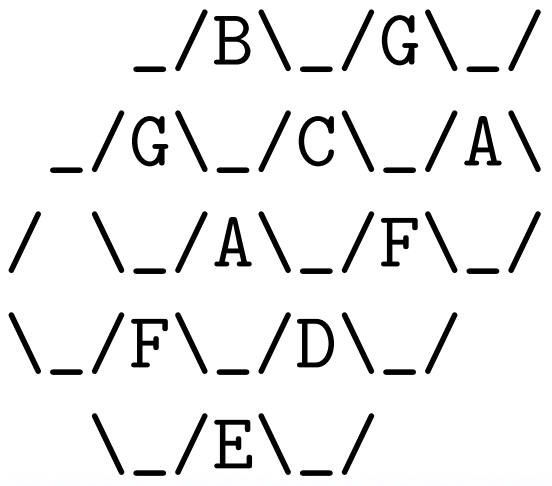
Phone Numbers

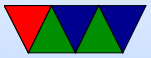
- 10 digits?
- Number portability?



Cellphones – Cells

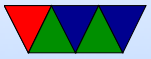
- Geographic area split up into cells
- Each cell uses a frequency different than neighbors
- Smaller cells, lower power more users





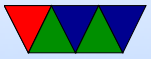
Cellphones – Infrastructure

- Center of each cell is base station
- Hilltops? Giant towers? Fake Trees? Churches?
- Transmitter/Receiver
- Connected to MSC (mobile switching center) or MTSO (Mobile Telephone Switching Office)

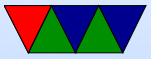


Cellphones – Handoff

- Basic idea (more complex with later versions)
- Phone communicates with tower when in cell
- When signal gets weak, asks surrounding towers about signal strength
- The one with strongest signal takes over control
- Has to switch frequencies
- This handoff takes about 300ms
- soft handoff: connects to new before switching off old. no loss, but needs to be able to receive two freq

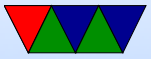


- hard handoff, old drops before new. If something goes wrong, lose connection.



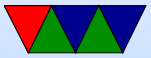
Cellphones – Types of Channels

- Control (base to phone)
- Paging (base to phone) alerts phone for incoming call
- Access (bidirectional) call setup and channel assign
- Data (bidirection) carry data/voice

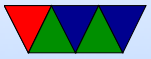


Cellphone – 0G

- 1946 first car phones
  - Only a few per city, more similar to a 2-way radio that an operator used to connect you to the phone network
  - Single channel for send/receive, push to talk
- 1960s Improved Mobile Telephone System (IMTS)
  - High-power (200W) base station on hill
  - Two frequencies for send/receive
  - 23 channels spread from 150MHz to 450MHz
  - Had to wait a while for dial tone if busy

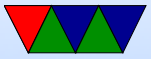


- Due to large transmitter, systems had to be far apart avoid interference



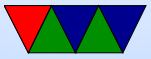
Cellphone 1G

- Analog – decommissioned in 2008
- 1982 AMPS – Advanced Mobile Phone System
  - Bell Labs, deployed in US in 1983
  - Also England (TACS) and Japan (MCS-L1)

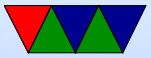


1G – AMPS

- Cells 10-20km across (larger than modern digital)
- FDM (Frequency Division Multiplexing)
- 832 full duplex channels, each a pair of simplex channels
  824MHz to 849MHz mobile to base
  869MHz to 894MHz base to mobile
- Each channel 30kHz wide
- 40cm, straight lines but blocked by trees and plants and bounce
- Since adjacent cells cannot use same freq, only maybe 40

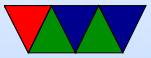


or so freq available at each tower (lose some for control channels too)

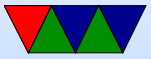


1G – AMPS – Protocol

- Phone had 32-bit serial number and 10-digit phone number.
- On power it scans the list of 21 control channels and picks strongest . The tower gets this, logs it.
- Phone re-registers every 15 mins.
- Press send, tries to send. If collision wait. Tower finds idle channel for call, then notifies phone which one.
- Incoming, constantly monitors to paging channel to see if one is incoming.

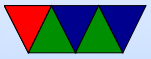


Phone network keeps track of which MSC the phone is in range of. Sends a broadcast on paging channel to see if it there, phone responds saying yes, then MSC sends message saying something like “call on channel 4”



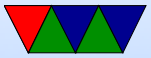
1G – AMPS – Security

- none. Plain analog, could listen on scanner (government made it illegal to sell scanners that could listen on those frequencies)
- Cloning – could listen and capture phone ID when it sends to tower. Then reprogram your own phone to steal the phone's account, make calls for free, etc.



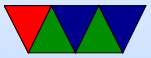
Cellphone 2G – Digital

- Roughly 1991
- Sometimes term PCS (Personal Communications Services) used, originally meant in 1900MHz band
- Digital, Encrypted, Data+SMS, Voice
- Benefits
  - Can be digitized and compressed, less bandwidth
  - Can be encrypted, better security
- Being decommissioned, starting 2017 with T-mobile last in the US not until December 2022(?)



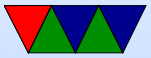
Cellphone 2G – D-AMPS

- Co-exist with AMPS, 1G and 2G could operate in same cell.
- Same freq, can change on fly which channels digital, which analog.
- Freq in 1800-1900 waves are 16cm, 0.25 wave antenna 4cm so can have smaller phones.
- Compression of signal, so much that typically 3 can use same channel via TDMA (time-division multiplex)
- Control is complicated



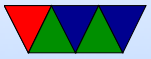
Cellphone 2G – GSM

- Original European, Groupe Specialé Mobile, but when popular Global System for Mobile
- everywhere but US and Japan.
- Standard 5000 pages long.
- FDM used
- GSM channels wider, higher data rate.
- In theory up to 900 channels available
- Simplex, cannot send and receive at same time.
- 33kbps, but after overhead only 13kbps



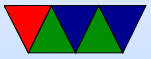
Cellphone 2G – GSM infrastructure

- SIM card (Subscriber Identity Module)
- Network ID follows the SIM, not the phone
- Has encryption
- Cell base stations have BSC (Base Station Controller)



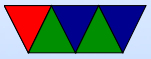
Cellphone 2G – GSM protocol

- MSC maintains list of nearby phones, VLR (Visitor Location Register)
- Also database last known location of each phone HLR (Home Location Register)
- Runs at 900, 1800, 1900MHz. More spectrum than AMPS to allow more phones
- Frequency Division Duplex like AMPS (transmits on one freq, receive on 55MHz higher)
- Freq pair split up with time-division multiplexing in time



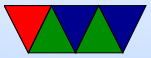
lots and shared

- GSM channels much wider than AMPS (200kHz vs 30kHz)
- Up to 992 channels, but many not available due to neighbor cells
- Transmit/Receive not at same time as GSM transmitters cannot and takes time to switch from send to receive
- Assigned a time slot to transmit in
- Each channel in theory 270kbps, split 8 ways 24.7kps but error correction takes down to 13kbps

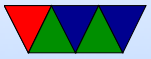


2G GSM – Channels

- Broadcast Control Channel – continuous stream from tower give ID and status, is how you determine signal strength
- Dedicated Control Channel – location update, registration, call setup
- Common Control Channel
  - Paging channel – announce incoming calls
  - Random Access Channel – request a slot on dedicated control

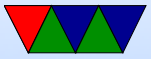


- Access Grant Channel – if negotiate slot successfully



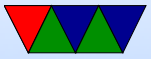
2G GSM – Handoff

- Handoff in AMPS was done entirely in base station
- In GSM most of time idle between slots
- It can notice if signal needs handoff and setup itself
- MAHO (Mobile Assisted HandOff)

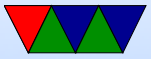


Cellphone 2G – CDMA (IS-95)

- code division multiple access
- Qualcomm
- At first people thought it was crazy
- Instead of having channels, tower broadcast throughout the spectrum. Coding theory.
- Noisy room analogy:
  TDM is people taking turns talking.
  FDM, people in clumps talking to each other.
  CDMA everyone talking at once, but different language

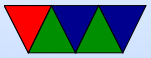


- Chips. Complicated. Sequence of -1, 1. Send sequence for 1, inverse 0. Each device assigned own chip sequence, can mathematically separate

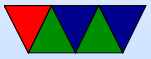


Cellphone 2.5/2.75G

- Newer phones started needing more bandwidth for data
- 2.5G (original iPhone)
  - GPRS
  - General Packet Radio Service
  - Packet vs Switched
  - Speed 50kbps (40kbps achievable)
- 2.75G
  - EDGE (Enhanced Data Rate for GSM Evolution) in 2003

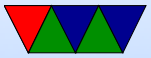


- 8PSK encoding
- 500kbps

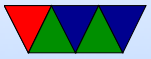


Cellphone 3G

- 1998 - 2001
- Digital Voice and Data
- IMT-2000 standard (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 if stationary, but 384kbps walking speeds 144kbps cars
- 200kbps (3.5 and 3.75G provide "broadband" speed)

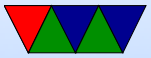


- Security, more secure than 2G, better ciphers (KASUMI)
- Mix of connection and packet based
- Being decommissioned, most right now (early 2022) with last Sprint in December 2022



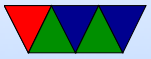
3G – W-DCMA vs CDMA2000

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



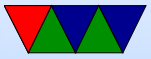
3G – More on advanced CDMA

- 3.84Mchips/sec, sending code 4-256 chips
- 256 chip code, 12kpbs (enough for voice)
- 4 chip code, 1Mbps
- In order to be faster use more than one channel
- 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



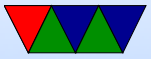
times/sec)

- 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



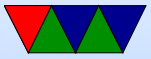
3G – Wideband CDMA (W-CDMA)

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



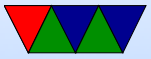
3G – CDMA2000

- Qualcomm
- 1.25MHz channels



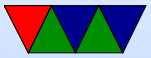
Cellphone 4G

- 2008
- Digital Voice and Data, packet switched
- The “G” has become a marketing term
- To be official supposedly need 1Gbps bandwidth



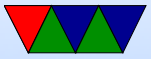
First came Cellphone 3.9G

- 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



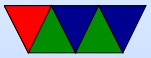
Actual 4G

- IMT announced requirements, advanced standards for 4G
- All IP packet switch networks (calls via VOIP)
- Peak 100 Mbits (high mobility) 1Gbits (low mobility)
- Channels 5-20MHz, optionally 40MHz
- Smooth handovers with heterogeneous networks
- Spectral efficiency of 15bit/s/Hz down, 6.75 up 1GBit/s in less than 67MHz



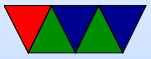
Cellphone 4G

- Packet switched
- EPC (evolved packet core)
- Data and Voice networks. Voice is VoIP (voice over IP)
- 100Mbps upload / 50Mbps download
- More frequencies, 700MHz, 850MHz, 800MHz
- Need good "spectral efficiency", how many bps per frequency
  Should be 15bps/Hz for down and 6.75bps/Hz for up



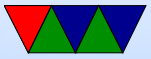
4G Other

- IPv6
- MIMO antennas
- SDR (software defined radio) because so many frequency ranges
- OFDMA



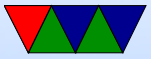
Long-term Evolution Advanced (LTE)

- 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

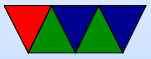


WiMax

- 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 a time slot, good for VOIP and QoS
- Licenses spectrum from 2-11GHz and 10GHz-66GHz

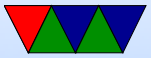


- can run in mesh mode where nodes can act as relays
- OFDM and OFDMA



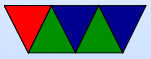
WiMax mobile

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



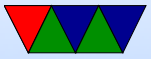
WiMax Scheduling

- 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



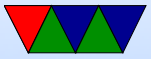
WiMAX2 (802.16m)

- 4G
- TODO



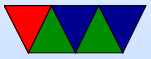
Cellphone 4G – Radio Access Network (RAN)

- 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)



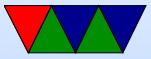
Cellphone 4G – LTE, EPC

- 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



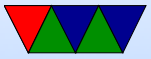
Cellphone 5G

- 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.



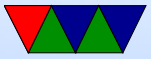
Crowded. Lots of unused in mm wave 20-300GHz. Do not penetrate well. Better antennas?

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

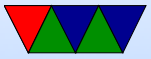


Cellphone 5G – more

- Up to 20Gbps
- Bands
  - Low band – similar to frequency band of 4G
  - Mid band – 1.7GHz - 4.7GHz, towers several km (most common)
  - High-band – Gb/s bandwidth, 24.25-29.5GHz
- Latency, ideal 8-12ms. HARQ retransmissions (FWD error correction, automatic repeat request), 50-500ms during handover

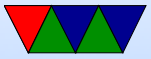


- Error rate, adaptive modulation and coding (MCS) to keep bit error rate low, reduce speed to reduce errors
- Frequency – interference with weather radar? Also some bands 3.7-3.98GHz interfere with poorly made airplane altimeters at 4.2GHz
- Coding change from polar to turbo?
- FCC freeing up bands?
- emBB – enhanced mobile broadband?
- URLLC – ultra-reliable low-latency communication
- mmtc – massive machine ? communication



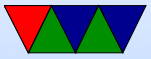
Cellphone 6G?

- They are thinking about it
- Will be faster
- Nothing concrete yet



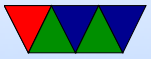
Cellphone Hardware

- Transmitter and application separate
- Antennas
- Sim cards. Multiple?

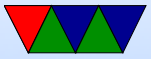


Cellphone Security

- 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



Future

- Cellphones that can talk to satellites? Starlink?