ECE 435 – Network Engineering
Lecture 33

Vince Weaver

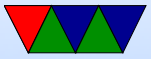
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

18 April 2025

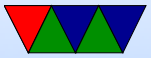
Announcements

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



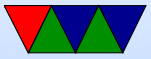
Question from Last Time

- Question from last time, earbuds, broadcast
- Bluetooth 5.2 (2019) added "Auracast" which allows broadcasting to more than one device
- Airpods, apparently one acts as primary, and then sends audio via bluetooth to the secondary



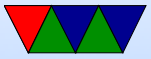
Cellphones

- Today most people's interactions with computer networks are through cellphones
- Have gotten increasingly complex
- What was life like before cellphones?
- Hard to keep up as things are constantly changing

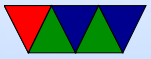


Cellphone Hardware

- RF hardware
  - Antennas – possibly many on modern phone
    1-2 Wifi, 1 bluetooth, 1 for GPS, 1-4 for 4G LTE
  - DSP
  - Baseband processor, with own RAM, running RTOS
- Application Processor
  - Separate from the RF side, for both security and regulatory reasons, don't want rogue code having access to transmitter

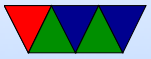


  - These days powerful ARM processor running apps and such
  - Running OS, ios, on Android it's Linux
  - TODO: which is wifi/bluetooth hooked up to?
- Other: camera, battery, etc.



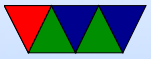
Cellphone SIMs

- Holds info on your account/phone, including phone number, company, billing, etc, encryption keys
- Has room for 8-256k of data, in old days could hold things like contacts and texts (these days, not as much)
- Different sizes, mini, micro, nano
- Some phones can support multiple (two numbers / accounts with one phone)

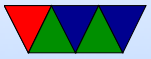


Cellphone eSIMs

- To save space, have permanent SIM soldered to motherboard, programmable via software?
- `https://arstechnica.com/gadgets/2023/04/isim-vs`
- Benefits of eSim
  - No card to lose
  - Hard to damage
  - Smaller
- Downsides
  - Cannot change w/o tech support

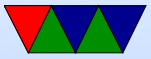


- If broken phone can't just swap to new one
- Have to wipe before sell phone



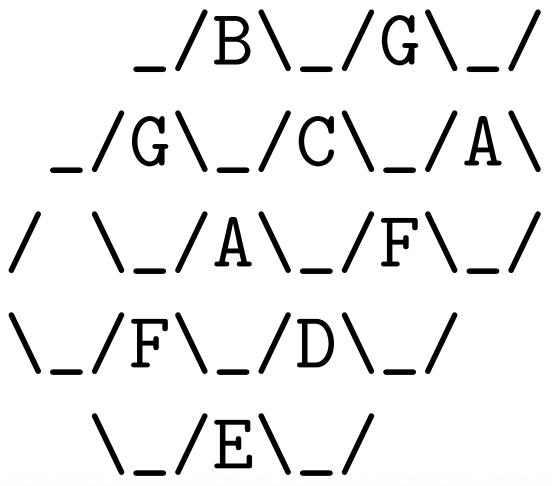
Phone Numbers

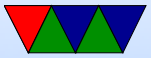
- How do you identify phone? Unique ID?
- Phone number history
  - 5 digits (old fashioned KL5-1234)
  - 7 digits
  - 10 digits with area codes
  - Number portability confuses this all
  - Other countries might be a bit different. Country codes. US is just 1



Cellphones – Cells

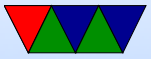
- Geographic area split up into cells
- Each cell uses a frequency different than neighbors
- Smaller cells, lower power more users





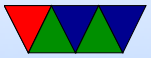
Cellphones – Infrastructure

- Center of each cell is base station
- Maybe seen them. Tower, 3 vertically parallel bars
- Hilltops? Giant towers? Fake Trees? Churches? Side of student union
- Transmitter/Receiver
- Connected to MSC (mobile switching center) or MTSO (Mobile Telephone Switching Office)
- Backup diesel generators



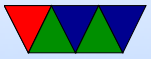
Cellphones – Handoff

- Need to transparently handle moving between cells without dropping call (or noticeable glitch)
- Tricky
- How they do it has changed with newer versions
- 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.



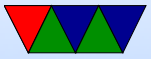
Cellphones – Types of Channels

- 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

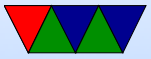


Cellphone – 0G

- 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

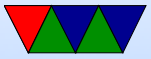


- Due to large transmitter, systems had to be far apart avoid interference



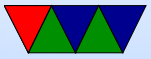
Cellphone 1G – History

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

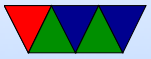


1G – AMPS

- 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

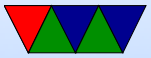


or so freq available at each tower (lose some for control channels too)

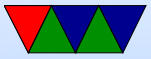


1G – AMPS – Protocol

- 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.

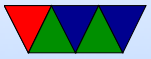


Phone network keeps track of which MSC the phone is in range of. Sends a broadcast on paging channel to see if it there, phone responds saying yes, then MSC sends message saying something like “call on channel 4”



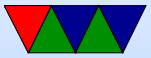
1G – Handoff

- TODO: make sure this is 1G and not 2G
- 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



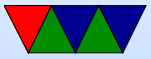
1G – AMPS – Security

- 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.



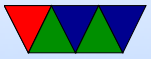
Cellphone 2G – Digital

- 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(?)

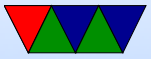


Cellphone 2G – D-AMPS

- TODO: check popularity (mostly in Japan?)
- 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)

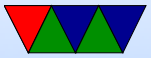


- Control is complicated



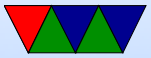
Cellphone 2G – GSM

- 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



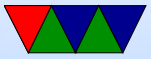
Cellphone 2G – GSM infrastructure

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



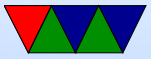
Cellphone 2G – GSM protocol

- 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



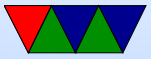
lots and shared

- 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

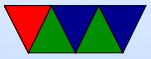


2G GSM – Channels

- 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

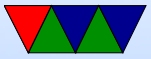


- Access Grant Channel – if negotiate slot successfully



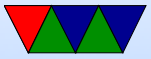
2G GSM – Handoff

- 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)

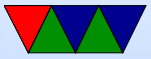


Cellphone 2G – CDMA (IS-95)

- 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

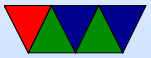


- Chips. Complicated. Sequence of -1, 1. Send sequence for 1, inverse 0. Each device assigned own chip sequence, can mathematically separate



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