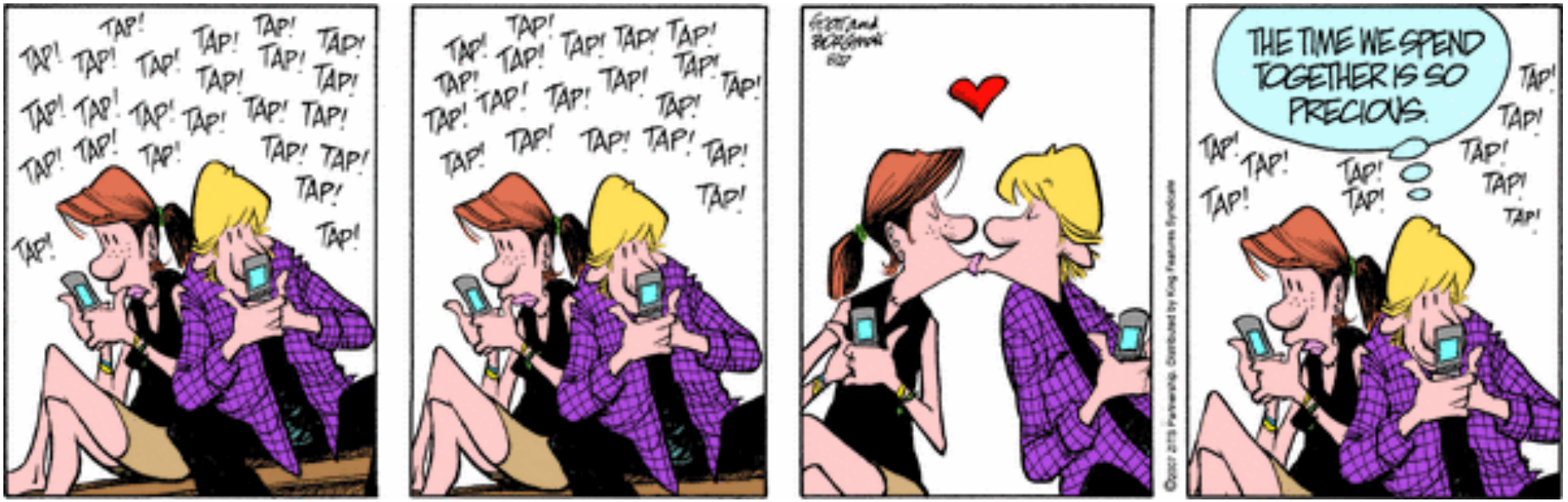
Lecture 22
Wireless systems



Wireless systems

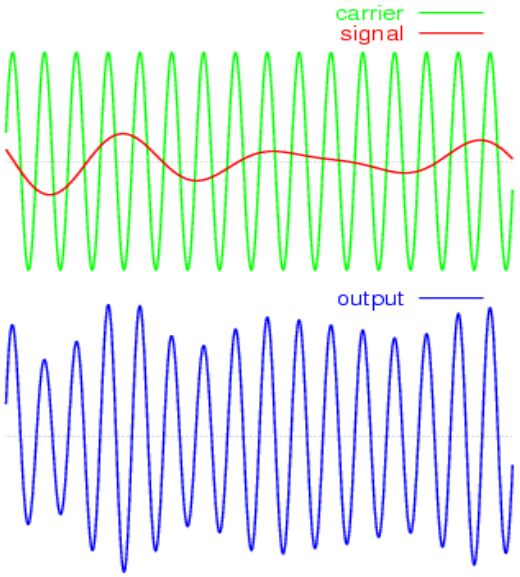
- how radio works
- radio spectrum allocation
- examples of wireless systems
  - cell phones
  - Wi-Fi
  - Bluetooth
  - RFID: prox cards, E-ZPass, store tags, passports, ...
  - GPS

- tradeoffs
  - spectrum, power, range, size, weight, mobility, ...

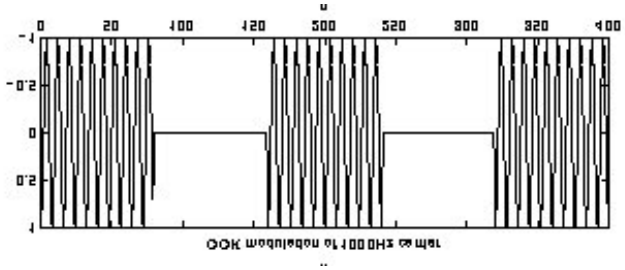
- non-technical issues
  - privacy, security, regulation, competition, ...

Radio

- electromagnetic radiation to carry information
  - without wires => "wireless"
- radiation is a wave of a particular frequency (in Hz)



- transmitter "modulates" the wave to impose information on it
  - amplitude (AM): change the power level
  - frequency (FM): change the frequency around a central value
  - digital: on/off
  - …



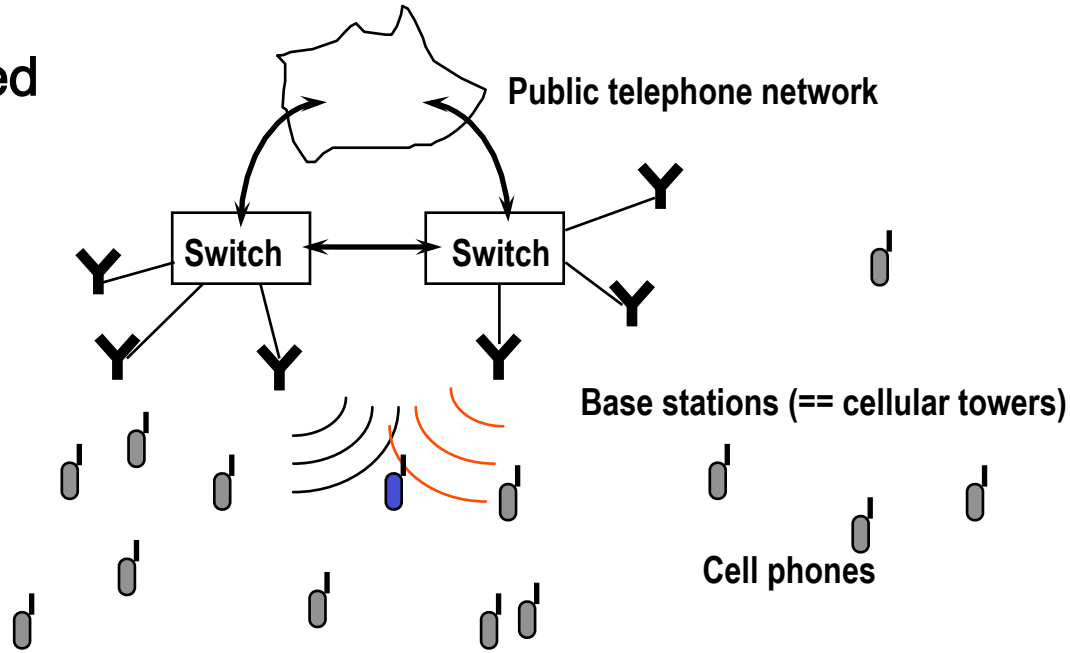
- receiver demodulates to recover the information
  - received signal strength varies directly with power level, and decreases with square of distance ("inverse square")
  - higher frequencies (shorter wavelengths) go shorter distances, penetrate obstacles less well

Cell phones 101

- all phones are part of the public switched telephone network
- a cell phone is connected by radio instead of wires

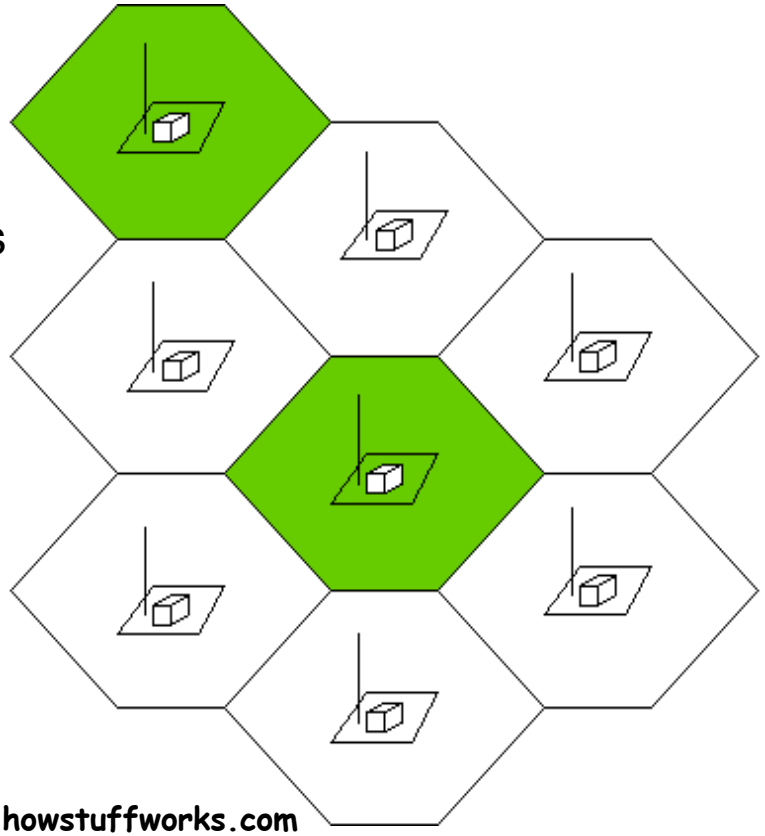
- moves long distances, at high speed, appears out of nowhere
- shares a very limited radio frequency spectrum with others
- operates with low power because it uses batteries

- this makes life complicated



Cells (a very idealized and over-simplified picture)

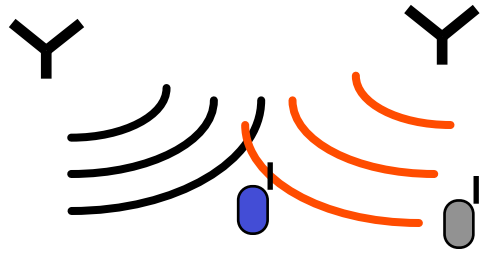
- divide geographical area into cells (notionally hexagonal)
- each cell has an antenna, handles all cell phones in its area
- available radio spectrum is divided into channels
  - two channels for one conversation, one for each direction
  - competing carriers operate on different frequency bands
- each cell gets 1/7 of the channels
  - adjacent cells can't use the same channels because of interference
  - non-adjacent cells can re-use channels



from www.howstuffworks.com

How it works

- **when a phone is turned on, it broadcasts its ID ("registration")**
  - nearest base station notices, validates with home system
    registration uses encryption for fraud prevention
  - phone keeps broadcasting enough to keep in touch
- **when the phone is called, the home system knows where it is**
  - home system contacts base(s) where phone is
  - bases broadcast to where phone was last seen ("paging")
- **phones talk to base with strongest signal**
  - base and phone communicate over 2 agreed-upon channels (up, down)
  - phones continuously adjust power level to signal strength at base
    uses less battery, creates less interference for other phones
- **phones move from base to base and from system to system**
  - base initiates handoff when signal gets weak
  - phone picked up by base with strongest signal
  - elaborate protocols at all levels



How it works, continued

- **multiple frequency bands** (different in different parts of the world)
  - divided into channels (frequency multiplexing)
    - digital phones multiplex several calls on one channel (GSM)
    - or spread calls out over the whole spectrum (CDMA)
  - phones usually support multiple bands
    - may use mulltiple frequency bands concurrently (5G)
- **channels carry both voice and control information** (including data)
  - digital speech is highly compressed (~1 bit/speech sample)
  - elaborate coding & error correction for speech & control information
  - power turned off when nothing is being sent
- **phone stores user info on (usually removable) SIM card**
  - SIM == Subscriber Information Module (flash memory)
  - may be able to replace card to use in a different environment

Mobile phone generations

- technology "generations" are roughly 10 years long
  - lots of overlap in deployed systems
- 3G (~2000)
  - on the way out
- 4G (~2010)
  - typical frequency bands 800-900 MHz, 1700-1900 MHz, 2.5 GHz, 5 GHz
  - supports 100 Mbps moving, 1 Gbps stationary (in theory)
  - 4G LTE ("Long-term evolution")
    a roadmap for evolution from 3G to 4G; a plan, not a strict definition
- 5G (~2020)
  - up to three bands, one of which is very high frequency (25-40 GHz)
  - similar to 4G for normal use
  - higher bandwidth (at short distances), up to 10 Gbps, mainly for data
  - higher density of devices supported (IoT) but at short ranges

GPS (Global Positioning System)

- 31 satellites, each broadcasting time & its location
  - altitude ~ 20 km, frequency ~ 1575 MHz
  - at least 6 are visible at any time

- receiver calculates its position using distances to 3 or more satellites
  - distances computed by careful measurement of time
  - accuracy typically within 15 m for civilian systems
  - additional inputs or use of encrypted info reduces this to < 1 m

- GPS is 1-way, passive

Location services for phones

- cell phones know approximate location by triangulation on base station signals, within about 125 meter radius

- cell phones have GPS receivers so position is known within about 5 to 10 meters
  - this can be augmented with ground-based signals, incuding wi-fi
  - the result is a very accurate computation of phone's location

- the phone knows the accurate location and reports it back to the carrier
  - and potentially lots of others

- if "location services" is turned on, location is available to apps as well

Technology meets politics

- should texting while driving be illegal (and enforced)?
  - how about just talking on a phone while driving? (Walking?)
- who determines where cell phone towers are permitted?
  - property rights versus eminent domain
- should cell phone jammers be legal?
  - in theatres, trains, etc.
- should StingRay devices be legal?

- location tracking and surveillance
  - who can have access to what phone records under what circumstances?
  - FCC mandates that cell phones can be located within 125 meter radius
  - should real-time location info be available to law enforcement, etc.?
  - how should this evolve as cellphones become universal?

Technology meets politics (2)

- should you be forced by law enforcement to unlock your phone?
  - under what circumstances?
    e.g., is entering the country different from a traffic stop?
  - what information can they access?

- should end to end encrypted communications systems like Signal be permitted / regulated?
  - this is the backdoor issue again

- how about end to end encrypted mail?