Mobile Security
Fall 2015

Patrick Tague

#8: Location Services

Class #8

- Location services for mobile phones
  - Cellular localization
  - WiFi localization
  - GPS / GNSS

Mobile Location

- Mobile location has become a critical element of smartphone usage
  - One of the major differentiators from laptops
  - Enables a wealth of new services (location-based services)

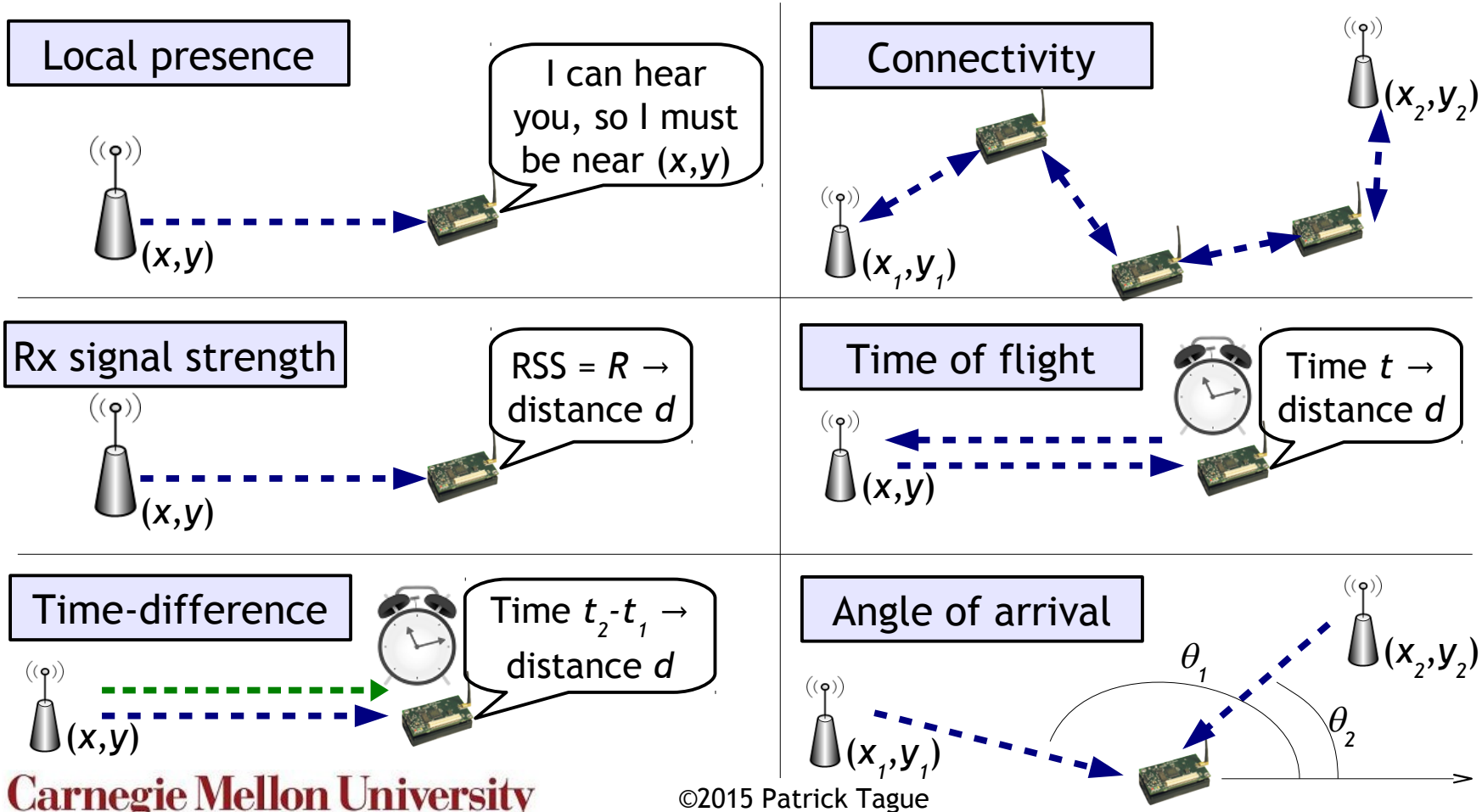
- How does it work?

Device Localization

- How does a device figure out its location?
  - Another device/system tells it
    - Ex: cell provider tells the device where it is
  - Another device/system provides reference points that allow it to estimate a location
    - Ex: GPS
  - It learns from a set of known landmarks
    - I just took a picture of the statue of liberty...where am I?
  - It figures it out using other information

Relative Localization

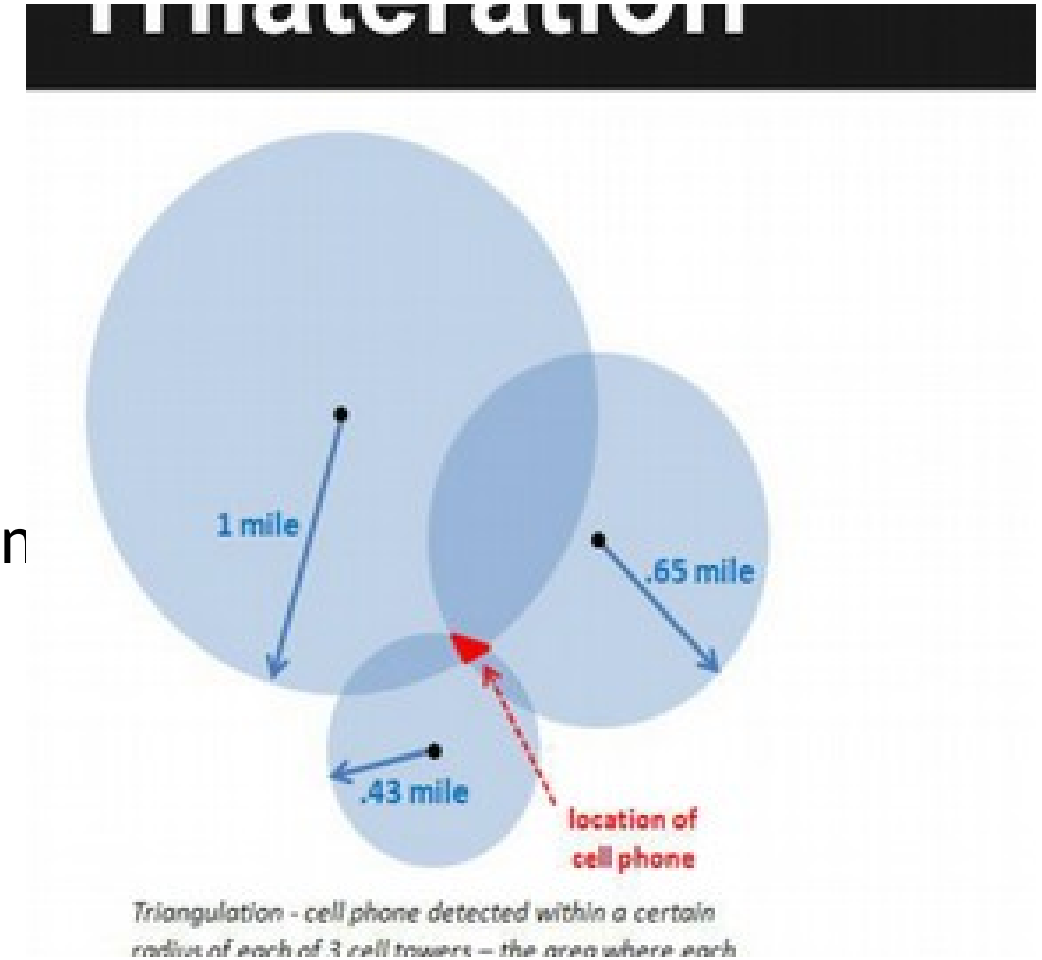
Each localizing device collects geometric relationships relative to several reference points (x_i,y_i)



Location from Cell Towers

Trilateration

- Requirements:
  - At least three reference points
  - Reference points with known location
  - Line-of-sight communication



Triangulation - cell phone detected within a certain radius of each of 3 cell towers – the area where each

More Trilateration

- GPS
- WiFi
- Bluetooth
- …

Bluetooth®

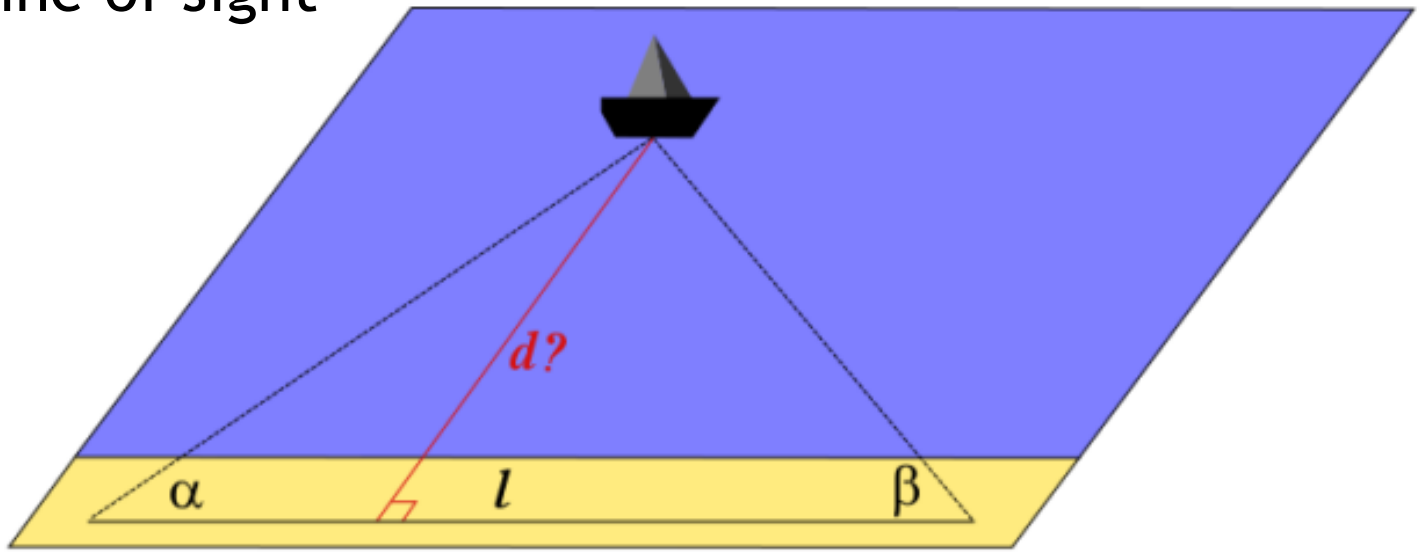
You Mean Triangulation?

- Trilateration ← Using 3 or more distance measurements to identify a point

- Triangulation ← Uniquely defining a triangle from two angle measurements and a known length

Triangulation

- Requirements:
  - At least two angle measurements
  - At least one known distance
  - Ability to measure angle-of-arrival (not as easy as it sounds)
  - Line of sight



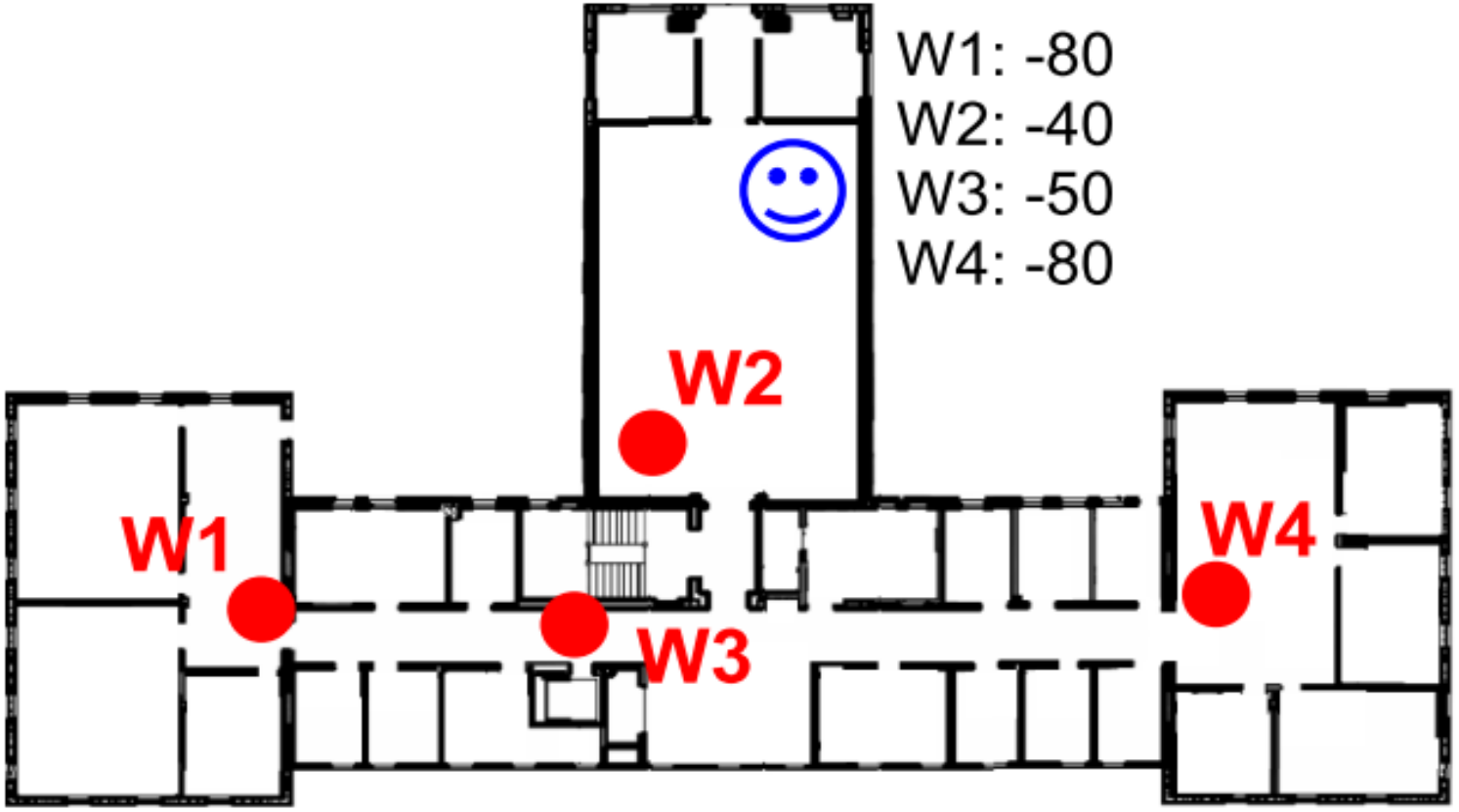
Triangulation v. Trilateration

- Trilateration
  - Receiver (e.g., phone) is locating itself based on measurements from several transmitters (e.g., cell towers) with known locations

- Triangulation
  - Two receivers (e.g., cell towers) are locating a transmitter (e.g., phone) by measuring angle-of-arrival of transmitted signal
    - Requires special hardware or really fancy software

Fingerprinting

Wi-Fi Fingerprinting for indoor positioning

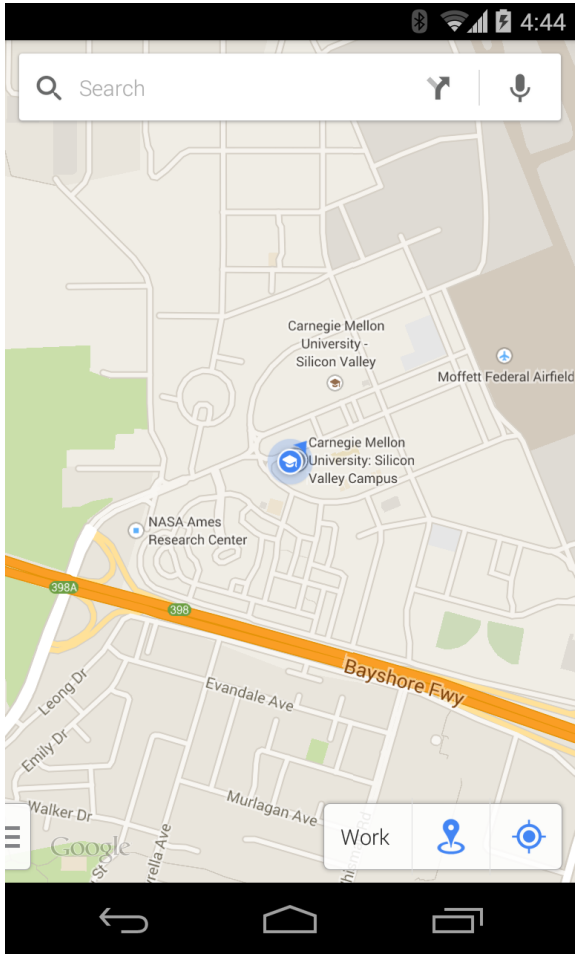


Fingerprinting

- Advantages
  - Resistant to multipath and attenuation
- Disadvantages
  - Requires data collection / site survey

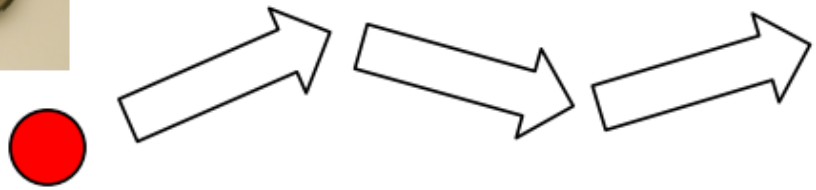
Crowd-Sourced WiFi Fingerprints

- WiFi fingerprinting can be done at large scale by recording which WiFi networks (SSID+MAC) are nearby (maybe +RSSI)
  - Location service providers such as Skyhook can take this info, look up the networks in a giant database, and perform trilateration for you



Location from Sensors

- Many sensors on the phone can be helpful in determining location, especially due to mobility
- Dead reckoning



- Advantage:
  - Needs no infrastructure
- Disadvantage:
  - Error accumulates over time

Let's focus on GPS, arguably the most prominent location source for smartphones

GPS

- Global Position System was developed by the US DoD initially in the 1970s and completely operational in 1994
  - Similar to other systems deployed by Russia, EU, China, India, and others

- Satellites broadcast current time and location to allow any receiver on Earth to localize

Things using GPS

- GPS is used for:
  - Automobile navigation (and autonomous driving)
  - Mobile geo-location (for LBS, etc.)
  - Livestock / wildlife tracking
  - Aircraft and ship navigation and autopilot

  - Power grid synchronization
  - Financial transactions & trading
  - Telecom system operations
  - ...

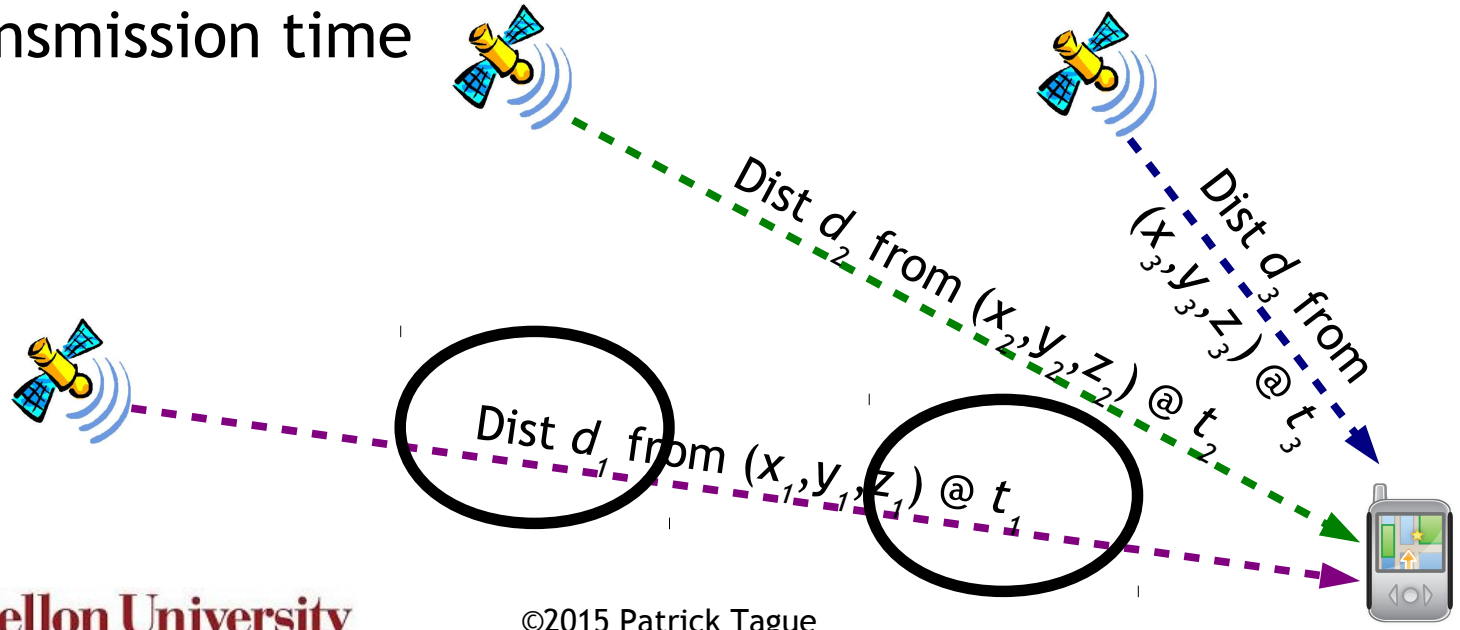
So, how does GPS actually work?

GPS Signals

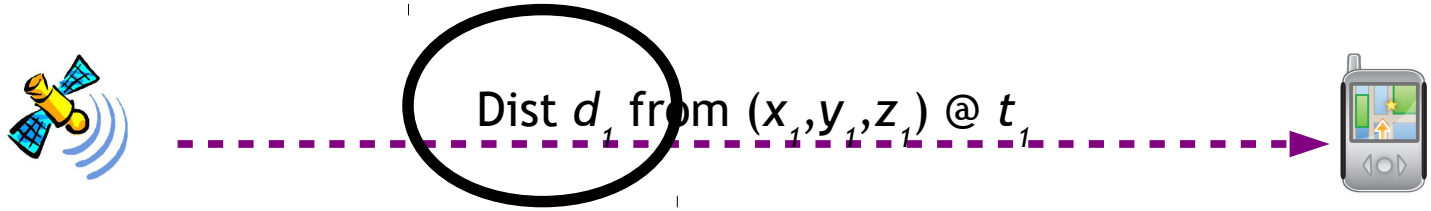
- GPS satellites send several different signals
  - On the L1 band (1575.42 MHz), coarse-acquisition (C/A) signal, encrypted precision (P(Y)) signal, L1 civilian (L1C) and military (M) codes
  - On the L2 band (1227.60 MHz), P(Y) code, L2C and M
  - Three other bands (L3, L4, L5) used for other purposes
    - Nuclear detonation detection, atmospheric correction, civilian safety-of-life

Multilateration

- GPS satellites serve as mobile reference points for Earth-based receivers
  - All satellites have high-precision, tightly synchronized clocks and precisely known locations
  - Each receiver hears a coordinate and timestamp from each transmitter, measures the distance based on the transmission time



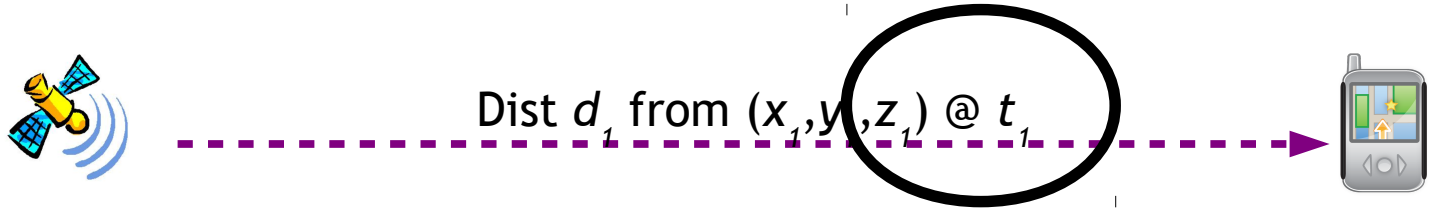
Measuring Distance



- How to measure distance from the satellite?

- Well, *distance* = *speed of light* * *time*, so just measure time...

Receiver Timing

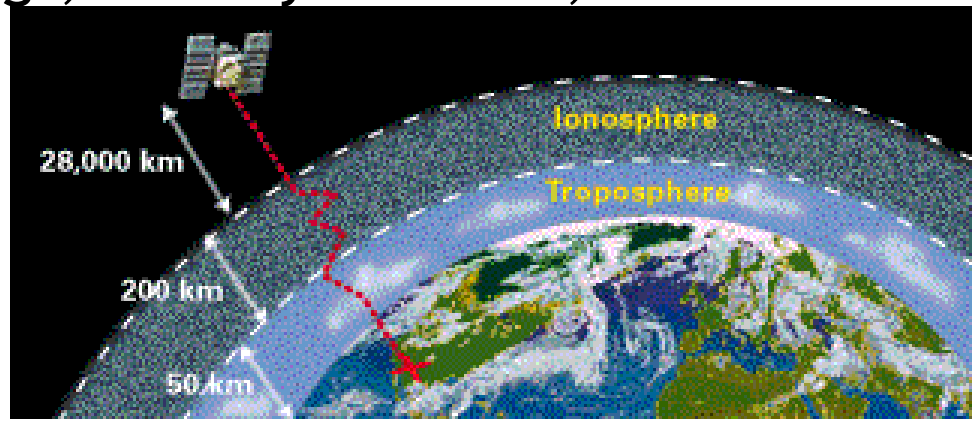


- Satellites themselves use atomic clocks to maintain ground truth
  - Receivers have to synchronize with the satellites
  - Remember, 1ns time error → 1ft distance error

- With clever processing, an extra satellite signal provides required synchronization
  - 3 satellites for space, 4 for space+time

Errors

- Errors arise for many different reasons
  - Scattering through Earth's atmosphere, reflection off buildings, time sync errors, etc.



  - Much of this can be handled by incorporating proper models in the distance estimation process
    - But, no longer just *distance = rate * time*
  - Some receivers get diversity from using military & civilian signals

Military v. Civilian GPS

- Civilian GPS uses an unencrypted and unauthenticated signal for location and time synchronization

- Military GPS devices can be keyed to use an encrypted and authenticated signal for high assurance location and timing
  - Military GPS requires key management, often in the form of manually entering long keys into handsets
  - Use of the military signal can provide much higher accuracy, error correction, etc.

Military GPS Rumors

- Since manual key management is often an impediment to mission-critical activities, there have been reports that a large number of soldiers use GPS in civilian mode

Selective Availability

- When GPS was originally designed, it was intended to provide coarse-grained location for civilians and fine-grained location for military
  - Does anyone remember when GPS accuracy was 30-50 meters and that was good enough for most things?

- Selective Availability was eliminated around 2000 to provide higher accuracy for civilian applications
  - Usually, we can get ~10 meter accuracy

Differential GPS

- For applications that require even better accuracy
  - Differential GPS uses an additional signal sent from a ground station to compensate for errors in data sent by satellites
  - E.g., DGPS stations can send difference between location claimed by satellite and its observed location
  - Accuracy of ~10cm can be achieved using DGPS
    - Appropriate for autonomous / swarm vehicle applications

What are the possible security issues with GPS?

Jamming

- GPS is based on wireless communication, so it's subject to interference

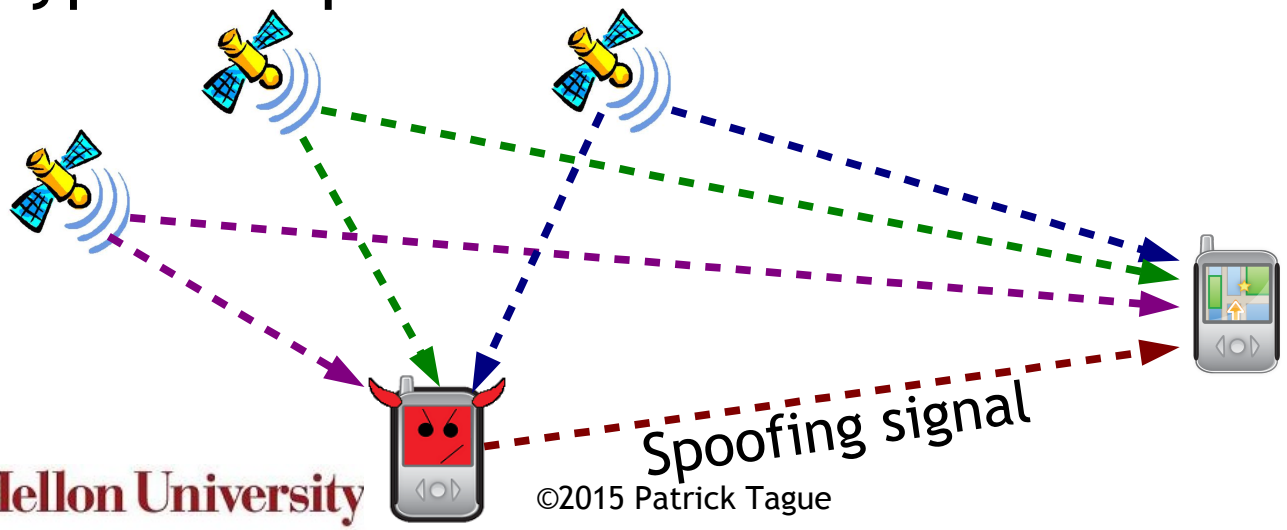
- GPS signals can be as quiet as -160dBm (10^{-19}W)
  - Jamming is pretty easy

Replay Attacks

- Replay of GPS transmissions would involve stale timestamps and location information
- The content of the message would be good
- But the time sync step would fail and most likely give unreasonable results
  - Unless the timing is precisely controlled...more in a minute

GPS Spoofing

- Instead of replaying old GPS signals, fabricate new ones and pretend to be a satellite
  - Spoofing leverages lack of authentication in civilian GPS signals
- Provides invalid information to the receiver to force it to compute an incorrect location
- Two types of spoofers have been demonstrated



Timed Replay as Spoofer

- Humphreys et al. built a spoofer (see [Humphreys et al., ION GNSS 2008])
  - It receives signals, analyzes them, and replays them after a precise delay
  - The delay affects the distance measurement, thereby affecting the location result
  - Precise control of delay allows gradual error accumulation or “drifting”, so detection is difficult

Many More Attacks

- GPS receivers are also vulnerable to a number of signal- and software-based attacks
  - e.g., Middle-of-the-Earth attack
  - See [Nighswander et al., CCS 2012]

How could you protect against these GPS attacks / threats...

without replacing or upgrading the satellite systems?

Deployment Constraints

- Because of the deployment cost, upgrading or replacing satellites is not really an option
  - Maybe very slowly over time, but not any time soon
  - So authentication is out

- GPS receivers have to respect what the GPS transmitters are sending even if they cannot authenticate them

Alternatives

- Several defense / mitigation strategies have been proposed by the GNSS community
  - Modifying GPS receivers to use multiple antennas to verify angle of arrival consistency
  - Augment receiver software to compare changes in location over time
  - Incorporate sensor data (GPS says you're moving but gyro says you're not → ?)
  - Incorporate other GNSS systems for diversity

What about Privacy?

- Location privacy is a huge problem

- We'll talk about it more a bit later in the semester

Oct 13 & 15:
SoW Presentations

Oct 20:
NFC & Mobile Payment