Mobile Sensor Systems

Background

12 billion mobile devices – almost everyone has phones, now sensors and IOT etc. is gaining traction.

The internet is only available to most people through phones, no computers.

Mobile data traffic is ≈0.5 **exabytes** per day.

In the US, >50% of internet access is through WiFi, rest is mostly 4G. In Nigeria 75% is through 3G. Geographic areas have vastly different access patterns based on the infrastructure available and economics.

Phones have a multitude of sensors:

- Camera
- Microphone
- Fingerprint
- Accelerometer
- Gyroscope
- Heart Rate

Mobile devices are resource- and energy-constrained. Connectivity is highly variable in **performance** and **reliability**. Mobile devices are inherently **less secure** (wireless communication means broadcast, which is snoopable).

Types of connectivity, with energy/reliability/rate limits:

- Cellular (SMS, 3G, 4G, ...)
- WiFi
- Bluetooth
- NFC
- Generic other radio communication

Wireless communication is generally organised as either:

- Infrastructure: Mobile devices connect to static base stations which are wired together into a trunk network. Handoff devices between base stations.
- Ad-hoc: No base stations, devices communicate between themselves when they're in range or available. Node organise themselves into a network.

Medium (radio spectrum) is generally multiplexed between multiple devices:

- Time: fixed or dynamic.
- Frequency: each communication gets a disjoint frequency band.

Multiplexing as above doesn't scale well with lots of devices or if communication is sparse. Ad-hoc approaches allow more statistical multiplexing:

- CSMA/CD: transmit if nothing else is, jam if you detect a collision, random binary exponential backoff.
  - Hidden Terminal: