Wireless Network Security
14-814 - Spring 2014

Patrick Tague

Class #2 – Wireless Review & Systems of Interest

Assignment #1

- First assignment has been posted online
  - Please get started as soon as possible
  - Brian will lead an OMNET++ tutorial in class on Tuesday, so please bring your laptop **with OMNET++ and INET already installed**
    - If you're familiar with Linux, probably best to go that route
    - If you're not good with Linux, Windows is a good option
    - If you prefer OSX, it should work, but we haven't tested it

Welcome to the Party

Wireless networking is much like trying to have a conversation at a party

Open Invitation

- Anyone can “talk”, anyone nearby can “listen”
  - We can control connectivity in wired networks, but not in wireless

A Dynamic Occasion

- Everyone is free to move around as they please
  - Physical mobility - that's why we lost the wires, right?
  - Logical mobility – connecting with different peers at different times
- Conversation quantity/load/demand varies
  - Nobody really talks constantly all the time...
- Air conditions at the party change over time
  - Noise, humidity/temperature, obstacles, reflections
- Others: services, roles, energy, …

Limited Engagement

- Each attendee has a limited amount of energy
  - Wireless devices are ideally battery-powered, otherwise why go wireless?

- Not all attendees have the same capabilities:
  - Some are less capable of processing what others say (e.g., less computation capability, 8-bit processors)
  - Some have limited memory (e.g., less storage)
  - Some have a limited vocabulary or speak a different language (e.g., different communication standards)
  - Some are quieter than others (e.g., shorter range of communication)

MC or No MC?

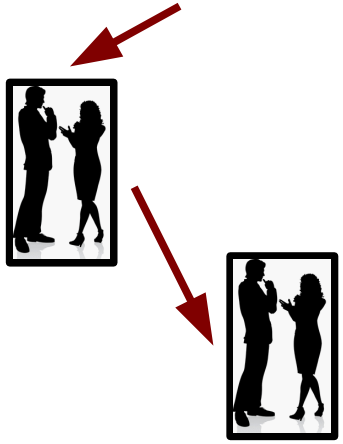
- Larger social gatherings probably don't have a single MC in charge of controlling conversations
  - This type of control is usually more distributed, if existent at all
  - In wireless, APs and gateways act as local controllers, providing access to the cloud, but not controlled by it
- Competition among (in)dependent sub-groups
  - Think of how many WiFi APs you've seen at once...

How do we deal with these challenges?

“Simplify, Simplify, Simplify”

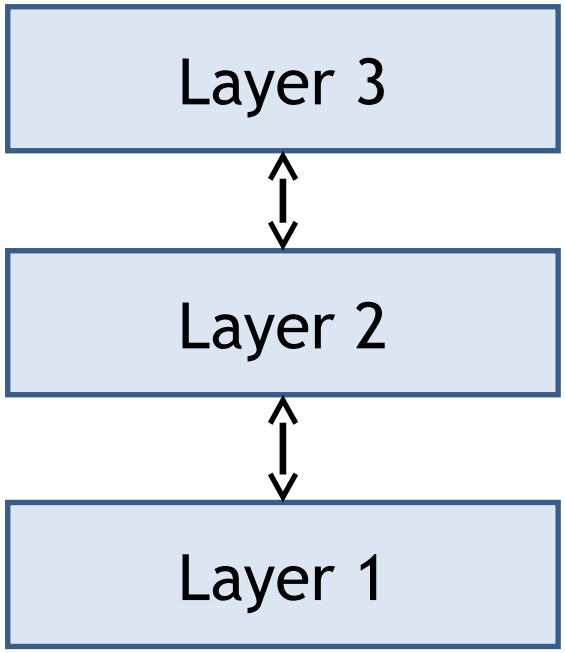
- Thoreau

- Instead of trying to solve all of the possible problems of cocktail party conversation, we decompose the problem into manageable steps
  - Communicating efficiently and effectively to a neighbor
  - Correcting mistakes, repeating, or re-stating
  - Relaying messages to a distant person
  - Making sure messages reach the intended recipient quickly, correctly, efficiently, etc. without annoying the messenger



Layering

- **Layering simplifies network design**
- Layered model:

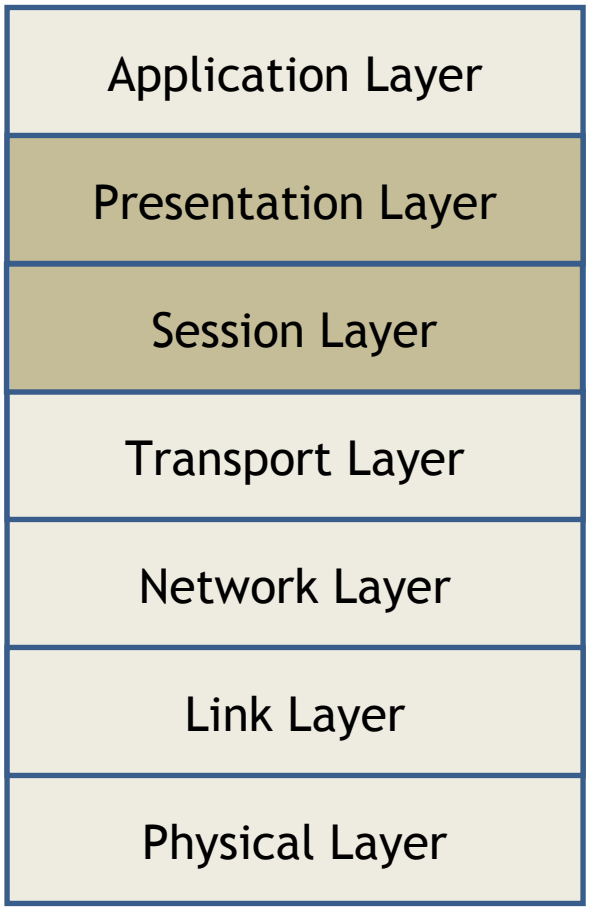


Lower layer provides a service to higher layer

Higher layer doesn't care how service is implemented: **transparency**

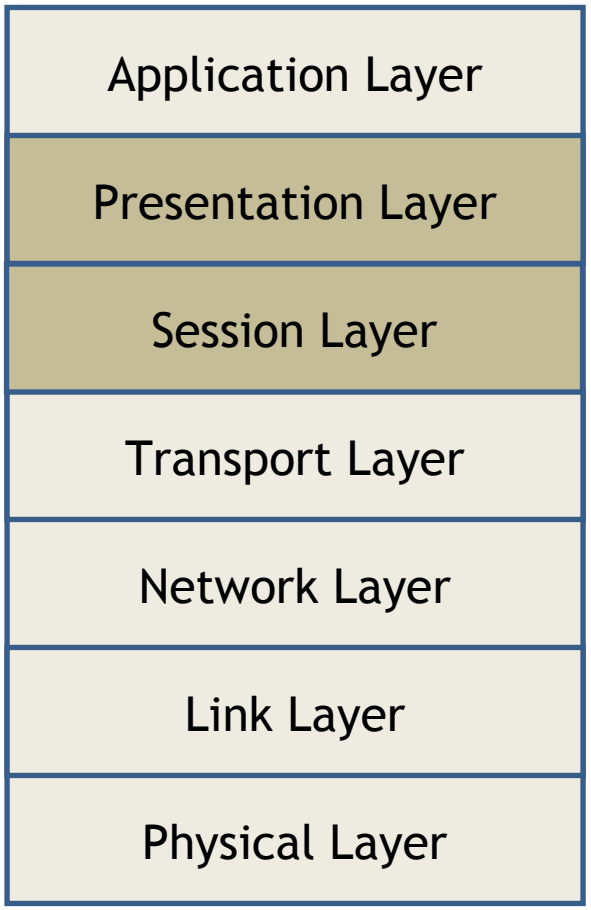
Layering Standards

- Standard layered model
  - Typically we talk about network layering using the 7-layer ISO Open Standards Interconnection (OSI) Model
  - Other models exist, but everyone seems to like ISO OSI



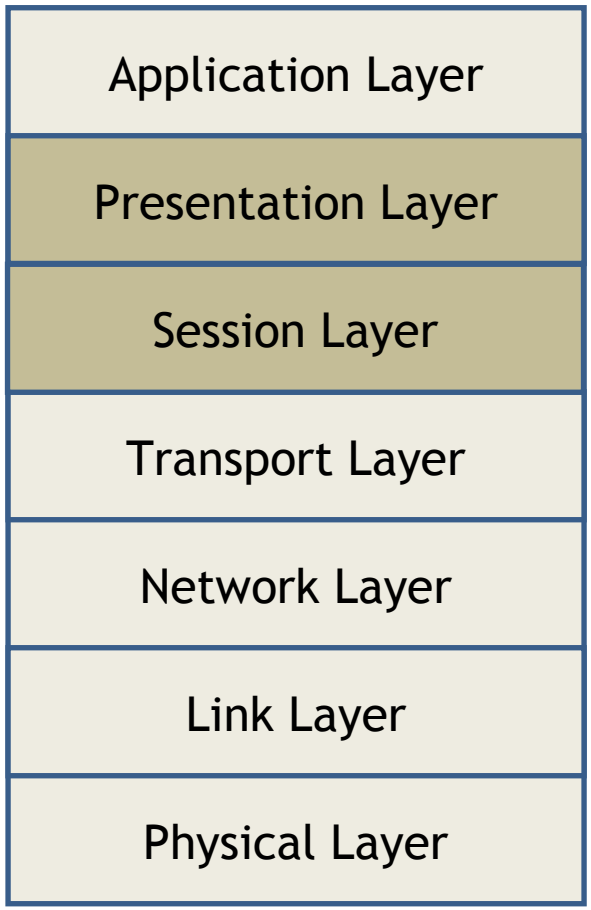
Layer Functionality

- Application Layer – support network applications
  - Presentation Layer – Compression, encryption, data conversion
  - Session Layer – Establish & terminate sessions
- Transport Layer – *Reliable* end-to-end data transfer
  - Multiplexing, error control, flow and congestion control



Layer Functionality

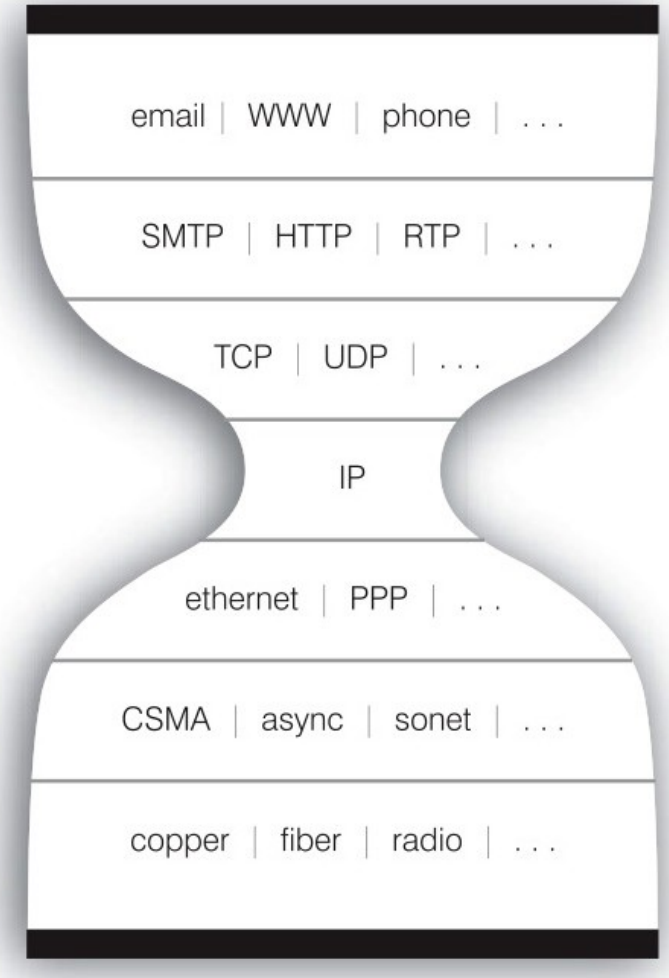
- Network Layer – Addressing and routing
- Link Layer – *Reliable* single-hop data transfer
  - Framing, error detection, medium access control (MAC) sub-layer
- Physical Layer – Moves bits
  - Bit synchronization, modulation & demodulation, physical connections



Internet Layering

- Layered protocols have been the basis of network design for decades

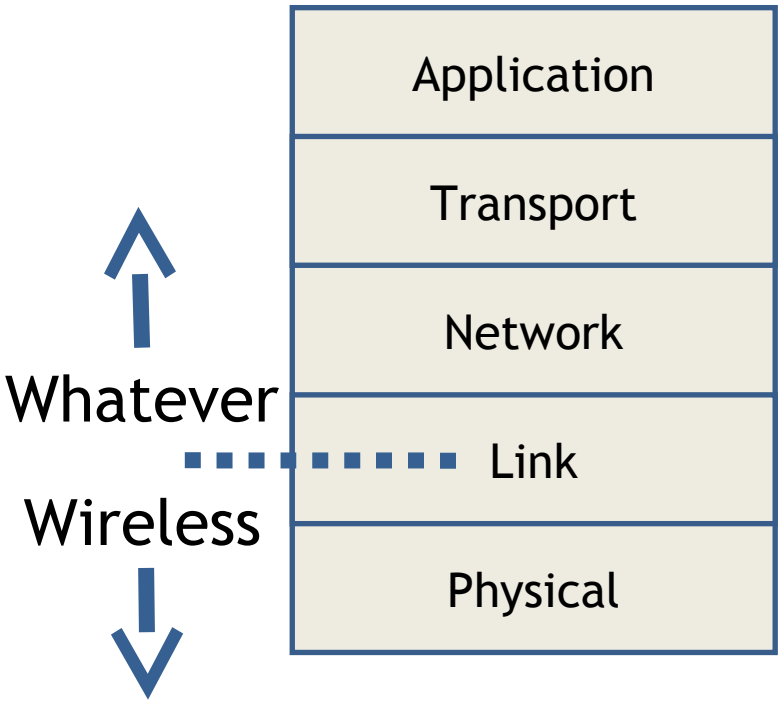
- Layers work great in some scenarios



Layering in Wireless

- Below a certain point, things can be designed for wireless communication

- Above that point, the medium doesn't matter…
  - Or does it?
  - Or should it?



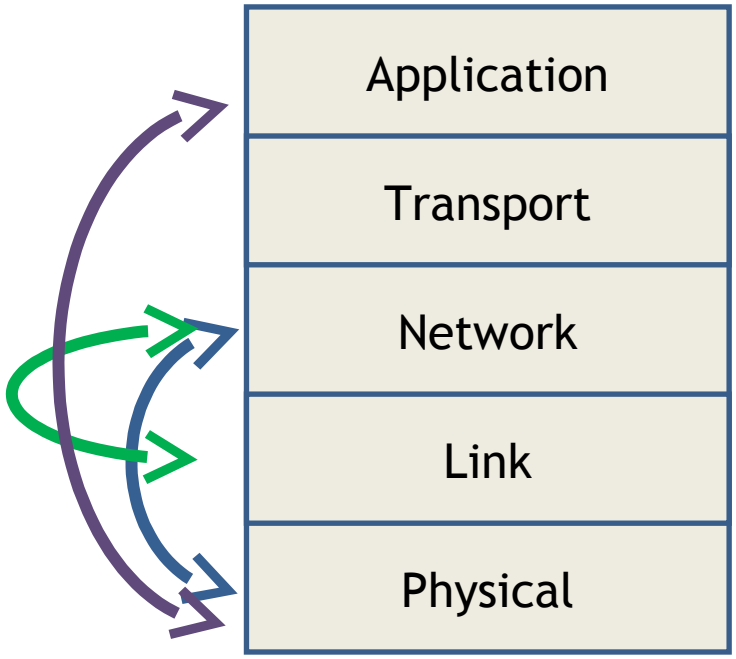
To Layer or Not to Layer?

- Layering Pros
  - Simplification
  - Transparency
  - Modularity
  - Upgradability
  - …
- Layering Cons
  - Layers aren't actually independent
  - Layers hide inherently useful information
  - Transparency → reliance → trust?
  - …

Question for later: how does layering affect security?

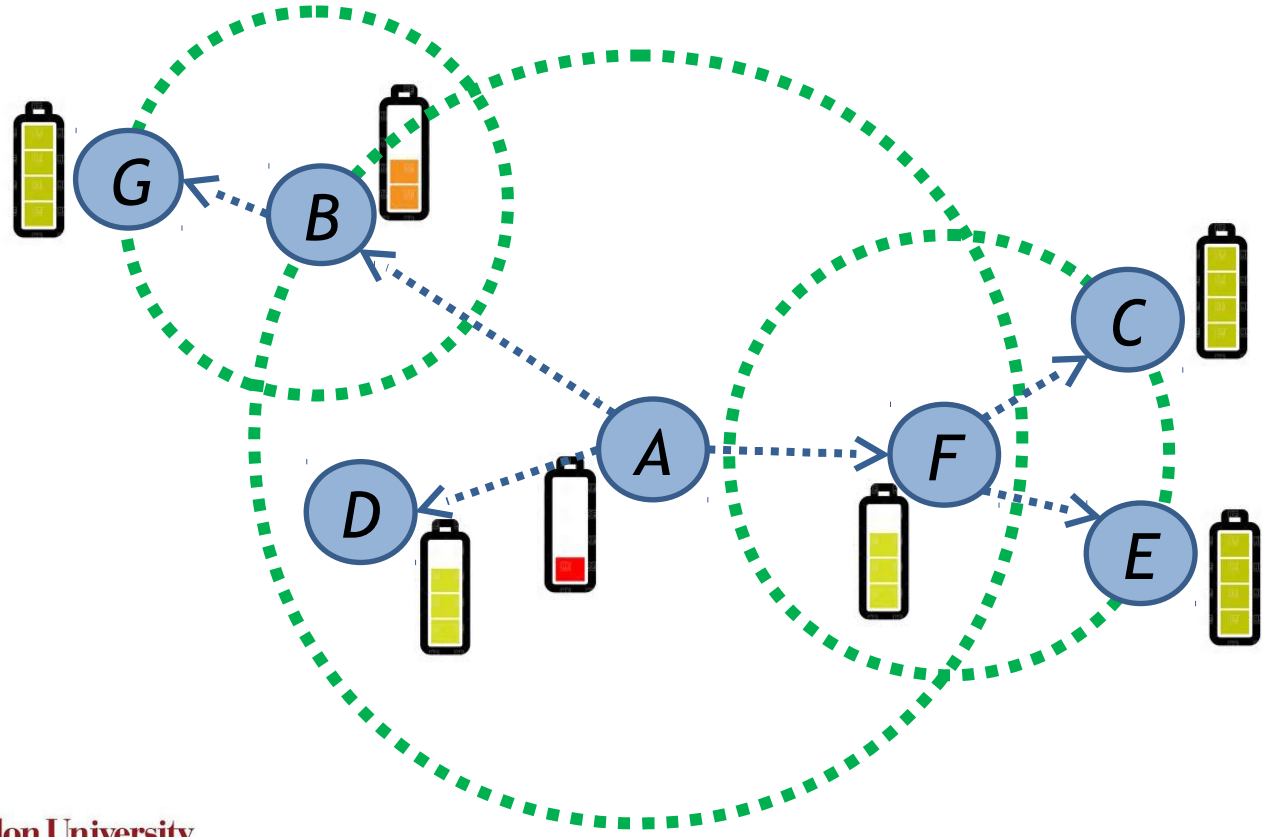
Cross-Layer Design

- Cross-layer design
  - Sharing info helps performance
  - **Transparency lost**
  - Design is more challenging



Max-Lifetime Broadcast Routing

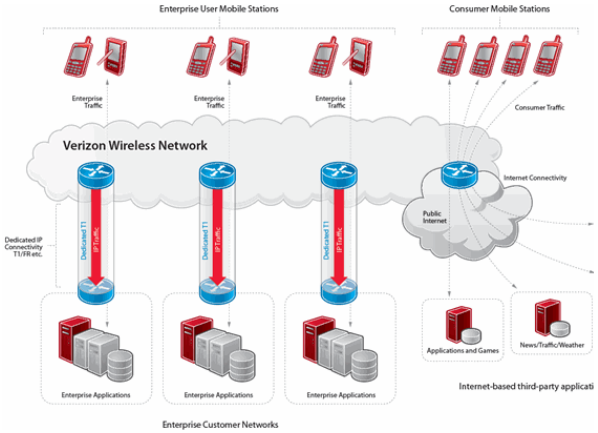
- **Cross-layer example:**
  - How to broadcast to everyone to balance network lifetime given that wireless allows "overhearing"?



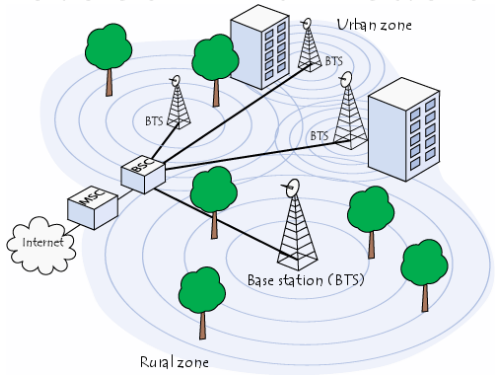
What types of wireless networks are we going to talk about?

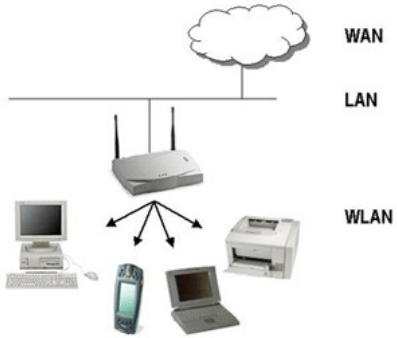
Wireless Networks

Enterprise Wireless

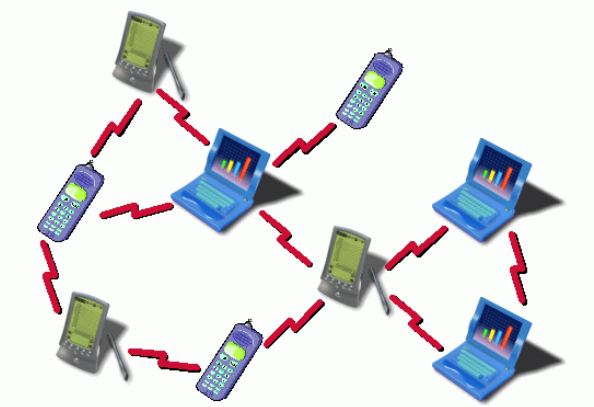


Telecommunications

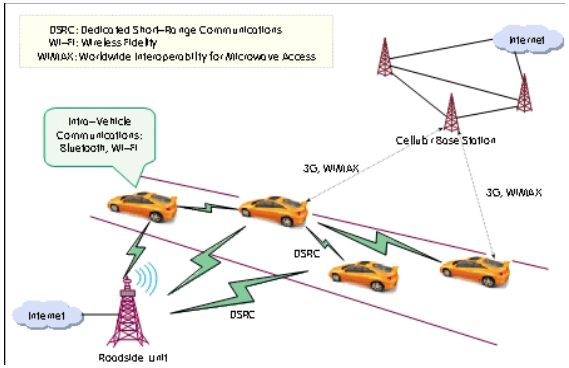




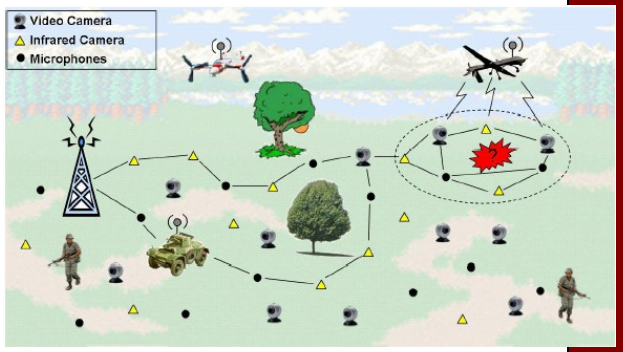
Wireless Internet



Ad Hoc / Mesh



Vehicular Networks



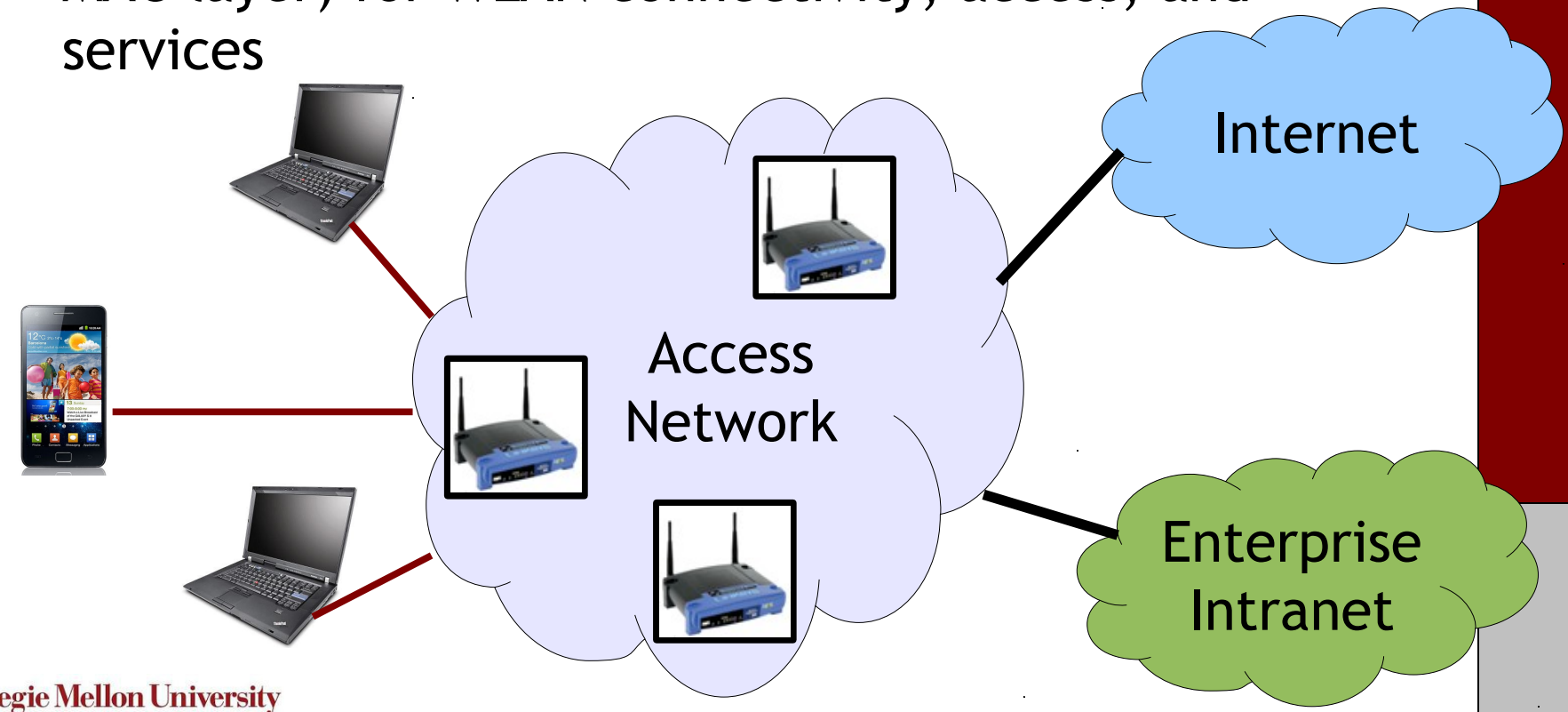
Sensing / Control Systems

And more...

WLAN

WLAN Systems

- Almost every WLAN system in existence uses the IEEE 802.11 “WiFi” standard
  - 802.11 defines lower-layer services (physical, link, MAC layer) for WLAN connectivity, access, and services



WiFi Physical Layer

- The WiFi PHY is responsible for transmission of raw bits/symbols between host and AP
  - Manages transmission and reception, perform bit-to-symbol (and inverse) mappings, and bit-stream hand-off with layer 2
  - Radio interface management: spectrum allocation, signal strength, bandwidth, phase sync, carrier sensing, etc.
  - Signal processing: equalization, filtering, training, pulse shaping, etc.
  - Modulation and coding (FEC, channel, etc.)

802.11 Standard PHY

- 802.11 defines a number of different PHY specifications
  - You've probably heard of 11b, 11g, and 11n
  - There are quite a few others, including upcoming 11ac and 11ad
  - Most of them use OFDM and/or DSSS

WiFi Link/MAC Layer

- The WiFi link layer is responsible for managing interaction between mobile terminal and AP

- Link layer has to manage:
  - Channel / link formation and management
  - Medium access ("MAC sublayer")
  - Network access control: authentication, authorization, etc.

  - 802.11i and 802.11w describe the link security architecture and protections (more later)

WiFi Extensions

- 802.11p: SSID-less comms for vehicles
  - Extension of WiFi to vehicular (V2V, V2I) networking, often used with DSRC, WAVE, and IEEE 1609
- 802.11s: WiFi mesh networking
  - Introduces link layer forwarding and extended service set to allow multi-hop WiFi, primarily among APs
- 802.11u: 3rd party authorization, cellular network offload
  - Aids in 4G by allowing seamless authorization of mobile devices to coordinated WiFi systems

Telecom

Early Cell Systems - "1G"

- Most well known system is AMPS (advanced mobile phone system)
  - Analog mobile phone system introduced in 1978 (FCC-approved and first used in 1983)
  - First use of the hexagonal cell structure (W. R. Young @ Bell Labs)

2G

- 2G is essentially the digital version of what 1G was in analog – referred to as digital PCS
  - GSM – global system for mobile communication
  - CDMA Cellular (IS-95A)
- 2.5G (IP-based)
  - GPRS (general packet radio service): adds IP-overlay over GSM circuits, provides packet data service, uses additional support node as Internet gateway
  - CDMA2000: wider-band, higher capacity CDMA
- 2.75G (IP-based)
  - EDGE (enhanced data rates for GSM evolution): modifies physical layer, no other changes

From 2G to 3G

- GSM and CDMA technologies have started to converge in 3G, with UMTS basically representing this convergence
  - UMTS = universal mobile telecom system, comes in many different flavors
  - TD-CDMA combines TDMA and CDMA
  - WCDMA (similar to EDGE with CDMA)
  - CDMA2000-3xRTT (three times the channel usage as 1xRTT)

3G

- 3G is when GSM and CDMA started to converge: mixed switching, MMS, location services, faster
  - UMTS, TD-CDMA, WCDMA, CDMA-3xRTT, TD-SCDMA
- 3.5G: increased download speeds
  - HSDPA (high speed downlink packet access)
- 3.75G: increased upload, multimedia
  - HSUPA (" uplink ") → HSPA
  - Multimedia broadcast → mobile TV
- 3.9G: ~2x UL/DL rates
  - HSPA+
  - Sometimes marketed as 4G, but it's not

WMAN

Metro Area Networks

- MANs are an attempt at convergence between WLAN and Telecom
  - WiMAX and LTE are the basis of 4G systems
  - Both independent Internet access systems and cellular components are being deployed
    - WiMAX as an alternative to DSL/Cable high-speed internet
    - LTE as the next-generation high-speed mobile data
  - MANs can also serve as the high-speed backhaul for WiFi and other wireless networks

802.16 Standard

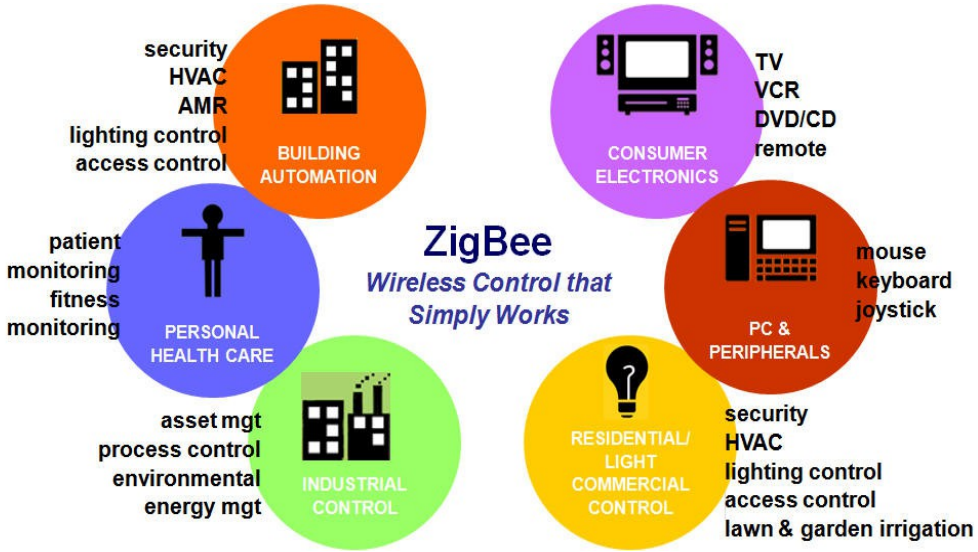
- IEEE 802.16 describes the physical and link/MAC layer for MANs as well as associated services
  - Essentially, it's a hybrid between what WiFi provides, what early cell infrastructures tried to do, and what is desired in the ITU 4G standard

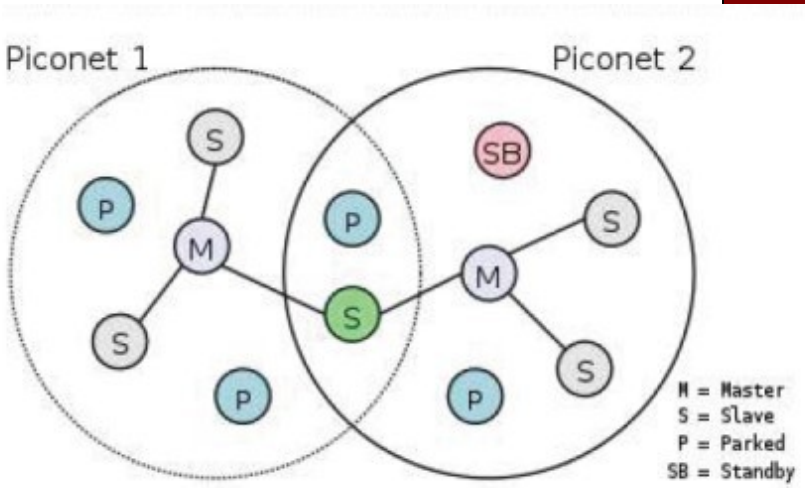
- More or less analogous to WiFi PHY and Link

WPAN

Personal Area Networks

- Local “device-to-device” networking
- Typically short range, few devices, low power
- Commonly used for home, personal, office





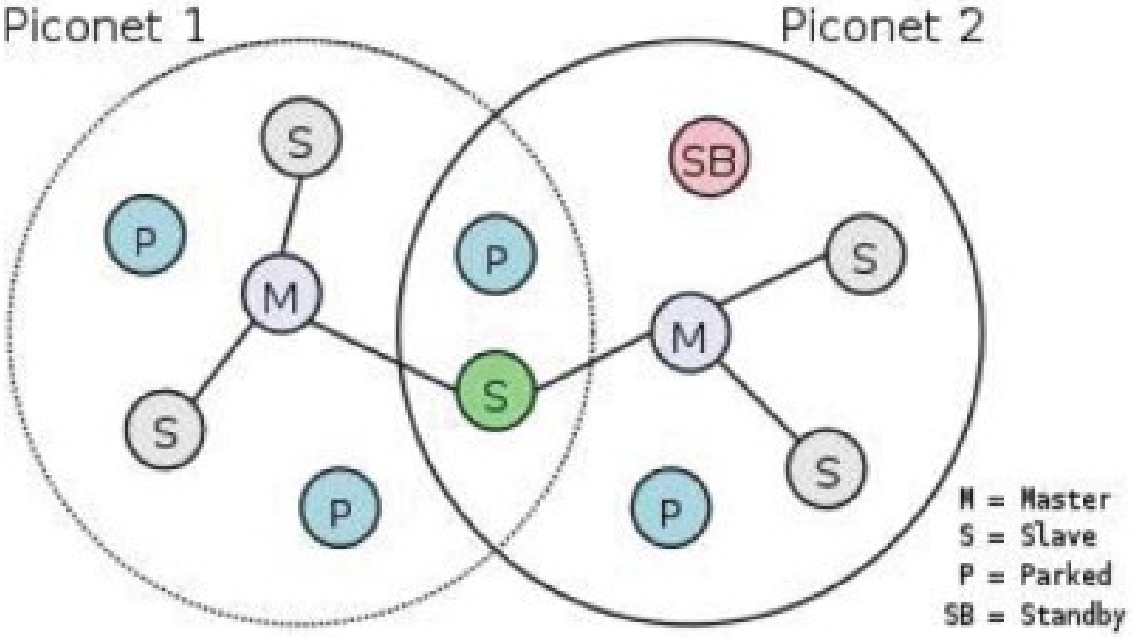
802.15 Standard

- Personal area networks enable device-to-device communication without relying on the Internet

- IEEE 802.15 family
  - 802.15.1: Bluetooth
  - 802.15.3: High-rate WPAN, including UWB
  - 802.15.4: Low-rate WPAN, including ZigBee
  - 802.15.6: body area networks (BAN)
  - 802.15.7: visible light communication (VLC)

Bluetooth

- 802.15.1 provides Bluetooth PHY
  - Short range, few devices, low power, cheap
  - Commonly used for home, personal, office networks
  - Bluetooth piconet is similar to WLAN (1 server, n clients) → (1 master, n slaves), only no back-end

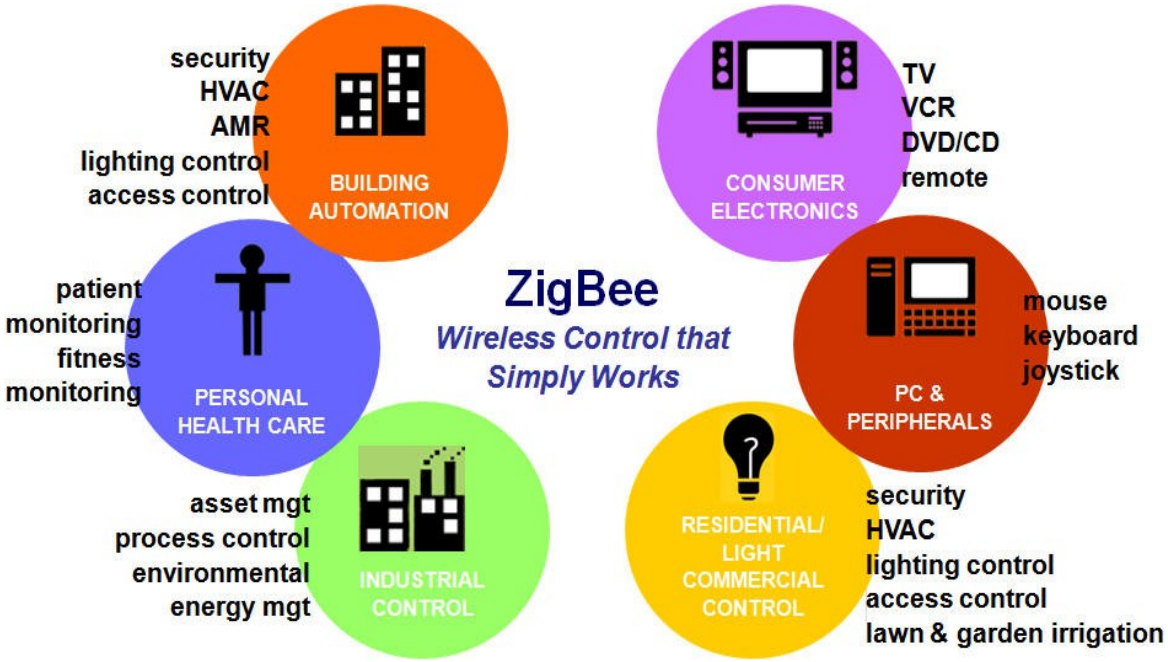


Ultra-Wideband

- Based on 802.15.3 standard
  - Very high data rate (~Gbps), very low power, very short distances (10-100cm)
    - High-rate file transfer, streaming audio/video, wireless display, wireless printing, …
  - Coexists with other wireless protocols

ZigBee

- Based on (and building on) 802.15.4
  - Designed for home automation, low-rate control systems, sensor networks, etc.
  - ZigBee builds a full network stack on top of the 802.15.4 PHY/MAC

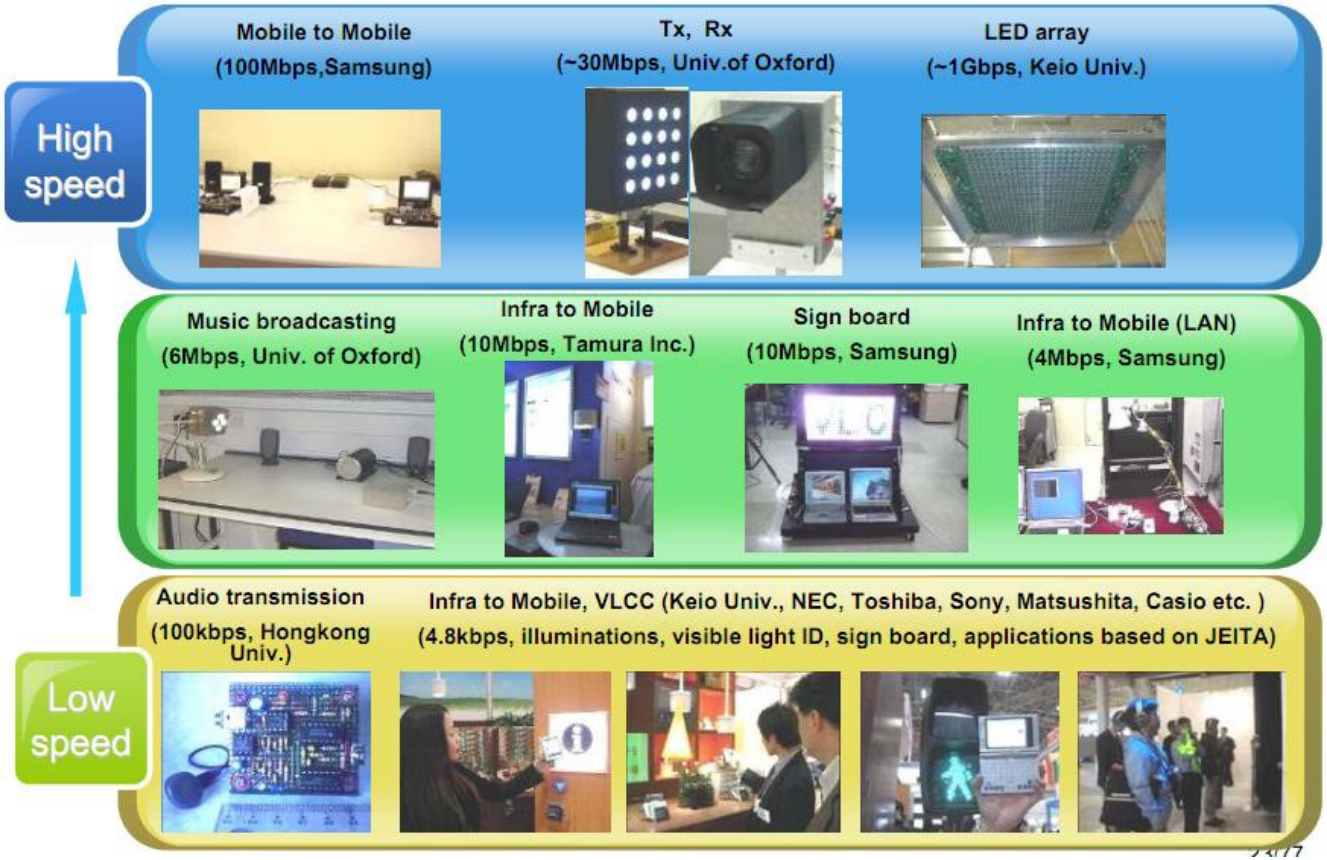


Body Area Networks

- Described in the 802.15.6 standard
  - Data collection from and control of medical sensors and implanted medical devices
  - Incredibly low power, esp. implanted devices

Visible Light Communication

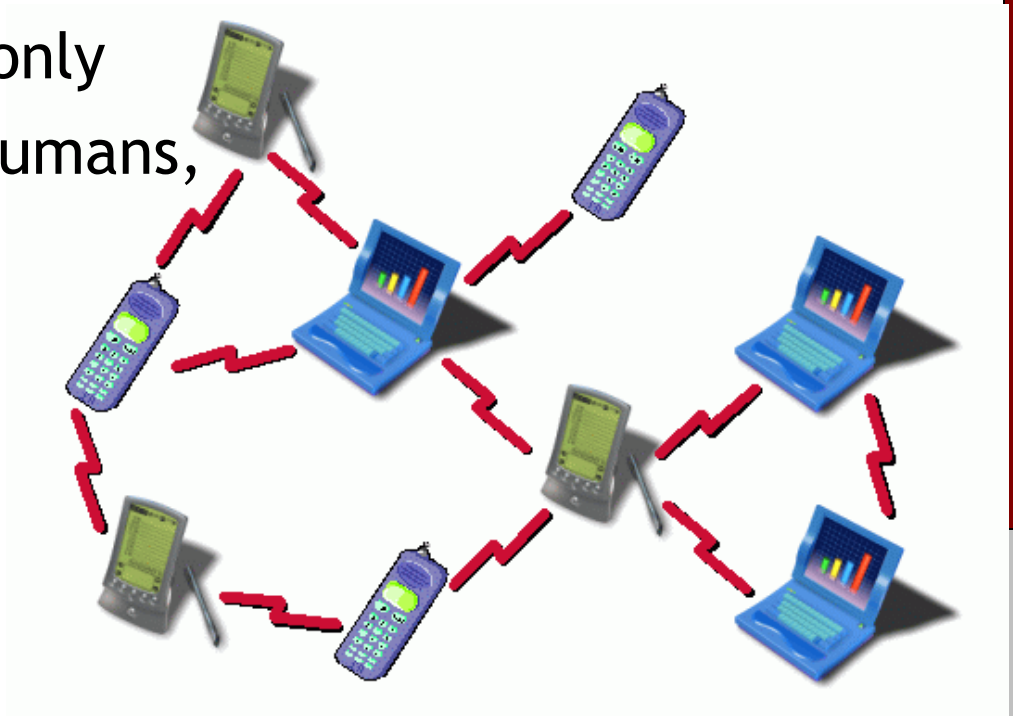
- 802.15.7 provides PHY/MAC for short-range comms using visible LEDs / sensors
  - 428-750 THz, unregulated, potential for high-rate and low-rate communication



MANET

Ad Hoc Networks

- Ad hoc networks typically manage “local” or “off-line” traffic, i.e. no Internet connection
  - Device-to-device, no APs
  - Peer-to-peer data exchange
  - In-network services only
  - Sometimes involve humans, but sometimes don't
  - No central server
  - No authority
  - No backhaul



Mobility

- Network is fluid
  - Associations are dynamic or short-lived
  - Members can join and leave network or groups
  - Observing behaviors over a long period (e.g., for modeling, monitoring, detection, etc. is not possible
  - Dynamic connectivity and reachability

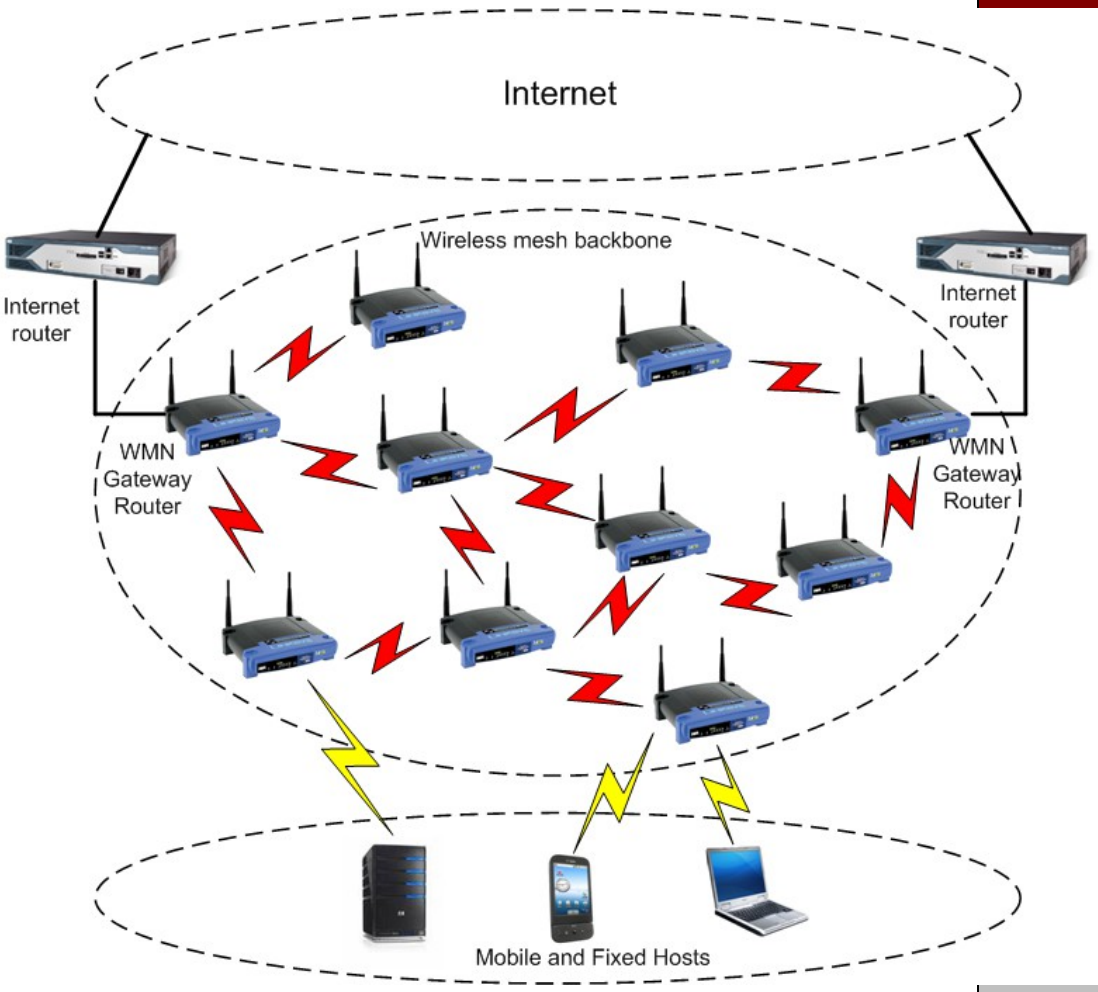
MANET Realities

- Recently claimed that true MANETs have very few good applications
  - Most practical systems end up being tethered to the cloud for one reason or another
  - Adding base stations to a MANET provides shared cloud access
  - Multihop networking among Internet devices allows local communication without cloud services

WMN

Wireless Mesh Networks

- Mesh networks provide multi-hop wireless connections to a backhaul
  - Mesh routers can be fixed or mobile, serve as multi-hop Internet connectivity
  - Hosts are typically mobile, hand-off to mesh routers



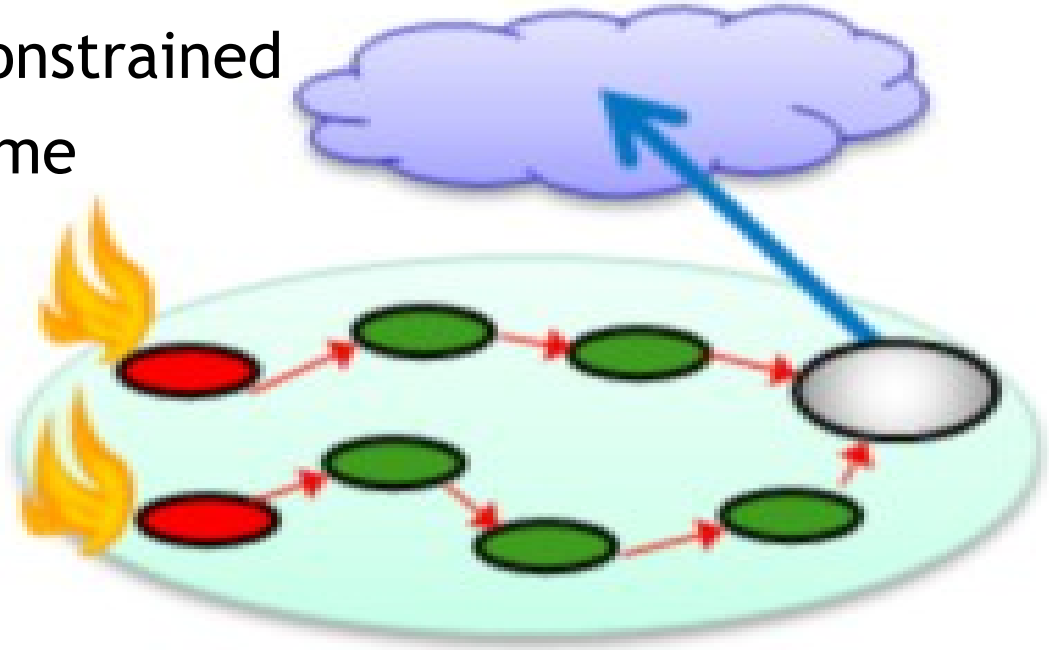
Standards for Mesh Network

Type of mesh networks	Corresponding standards
WMAN mesh (WiMAX)	IEEE 802.16a (mesh option), IEEE 802.16j (multihop relay)
WLAN mesh (Wi-Fi)	IEEE 802.11s
WPAN mesh (ZigBee)	IEEE 802.15.5

WS[A]N

Sensor Networks

- Mostly use ZigBee (based on 802.15.4) or WiFi depending on requirements
  - Sensor networks are typically closer to a mesh architecture: multi-hop to one/many APs
  - Intermittent low-rate traffic, mostly sensor readings from nodes back to APs
  - Heavily resource-constrained
  - Designed for life-time



Sensing vs. Computing

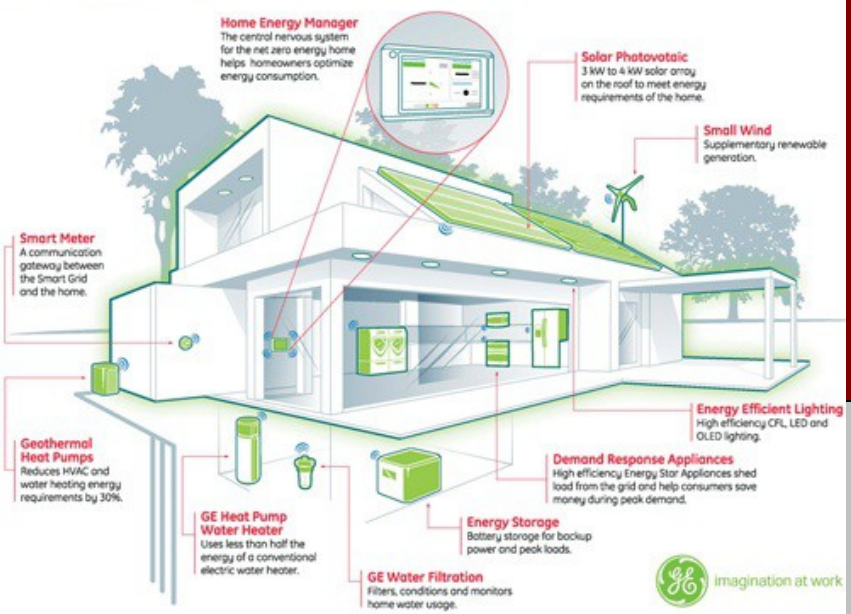
- Primary difference between sensor/actuator networks and typical computer networks is control vs. data
  - Sensors create data used to generate control signals given as input to actuators
  - Control systems have much tighter time constraints than data/computing systems
    - Delayed video vs. delayed fire alarm?
  - Control information can be operation/safety critical
    - Authentic control signal vs. correct control signal

More Specialized Networks

Home Networks

- In-home networked systems (Smart Home)
  - Entertainment/media
  - Appliances, etc.

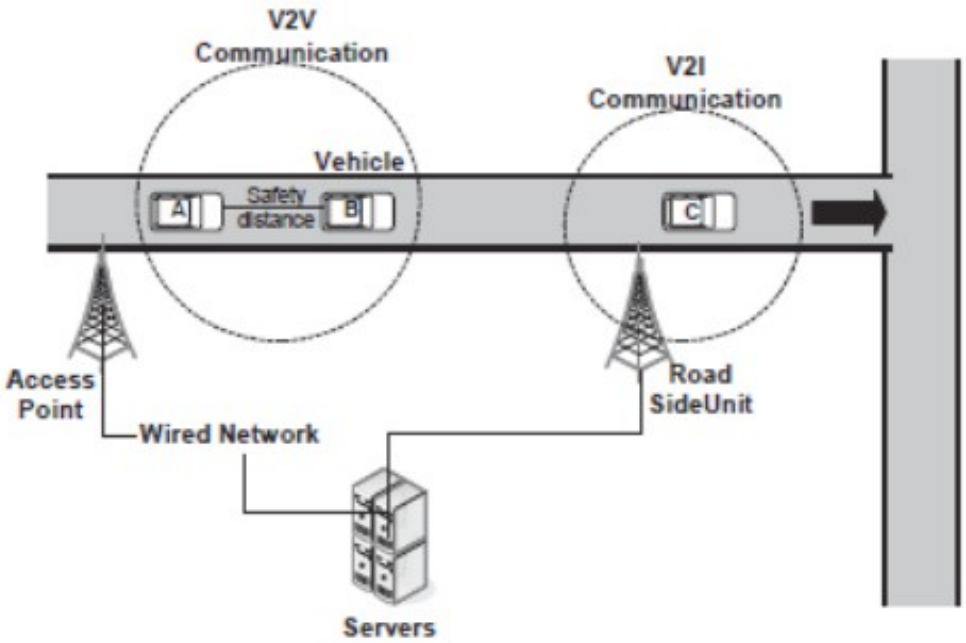
- Home energy networks
  - The home side of the smart grid, between the smart meter and user
  - Mostly wireless (802.15.4, etc.)



Carnegie Mellon University
Silicon Valley

VANETs

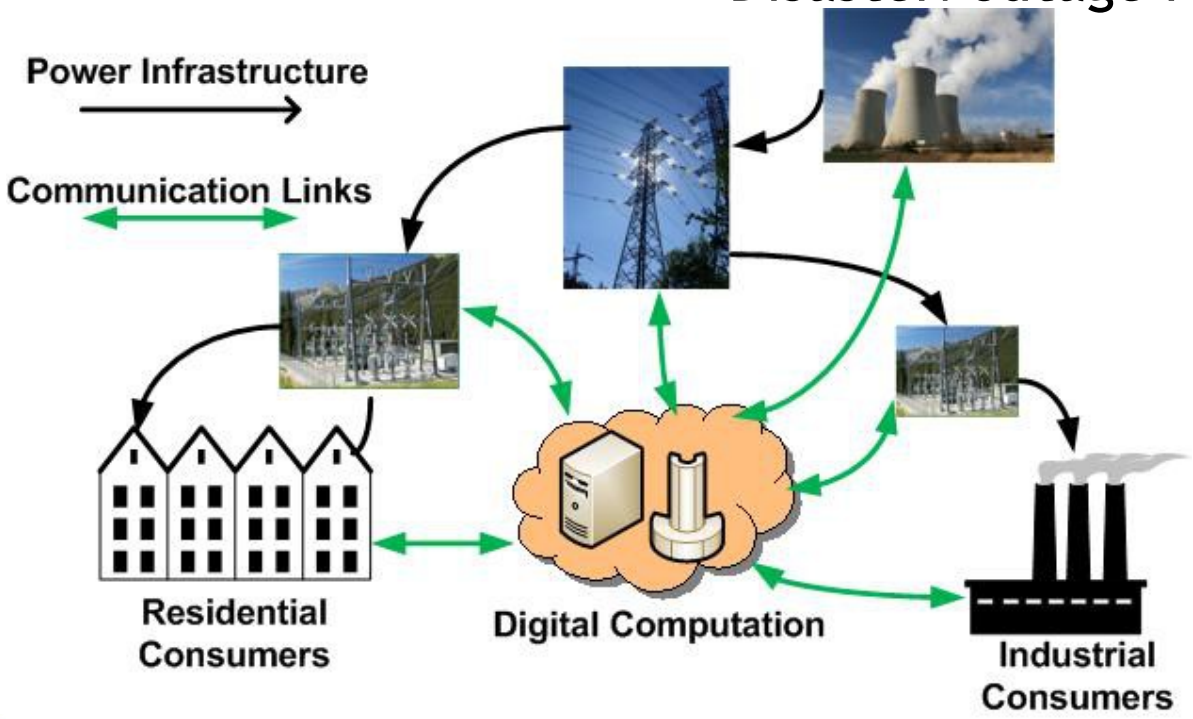
- VANET = Vehicular ad hoc network
  - Cars talk amongst each other and with roadside infrastructure



- Applications of interest:
  - Automated driver safety management
  - Passive road quality / condition monitoring
  - In-car entertainment
  - Navigation services
  - Context-aware rec's:
    - "This alternate route would be faster, and it would go past your favorite Primanti Bros."

Smart Grid

- The Smart Grid incorporates hybrid wired/wireless communications into the energy grid
- Applications of interest:
  - Dynamic pricing
  - Improved efficiency
  - Home energy mgmt.
  - Disaster/outage recovery



January 21:
OMNET++ Tutorial

(please come prepared)

January 23:
PHY Network & Threat Models