Wireless Network Security
Spring 2016

Patrick Tague

Class #2 – Wireless Security Basics & Threat Models

Class #2

- Brief review of wireless networks

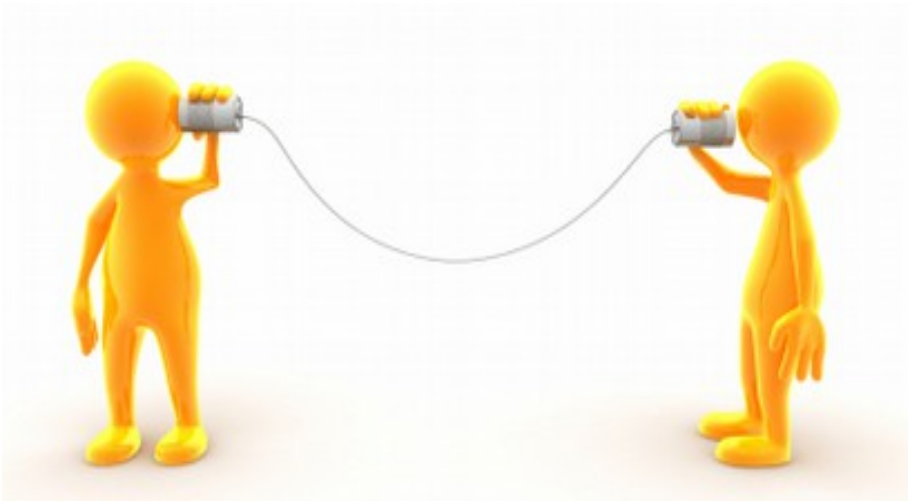
- Wireless security basics, threat models

Welcome to the Party

Wireless networking is analogous to a cocktail 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...
- Party conditions 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

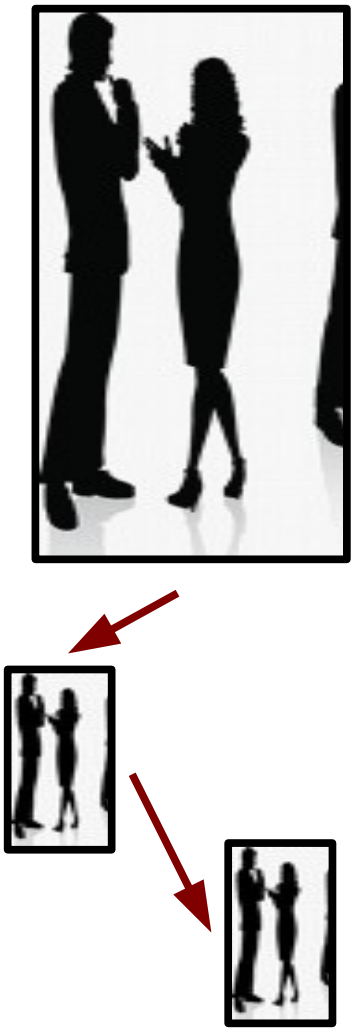
- Competition among (in)dependent sub-groups
  - Think of how many WiFi APs you've seen at once...

How do we deal with these challenges?

“Simplify, Simplify, Simplify”

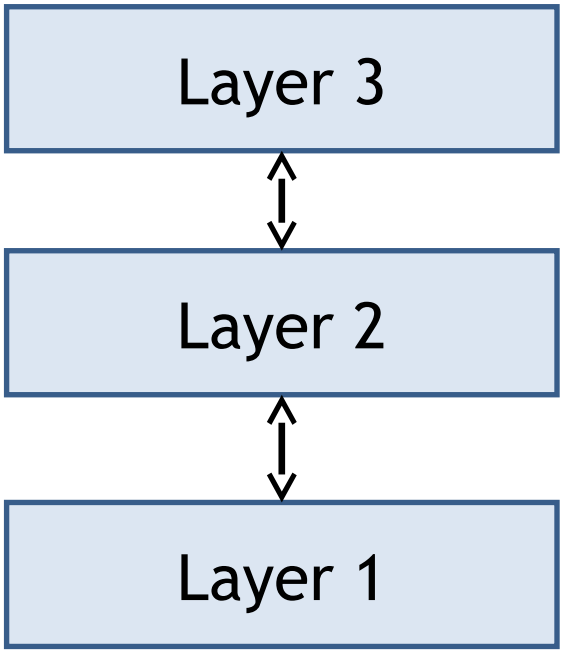
- Thoreau

- 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:

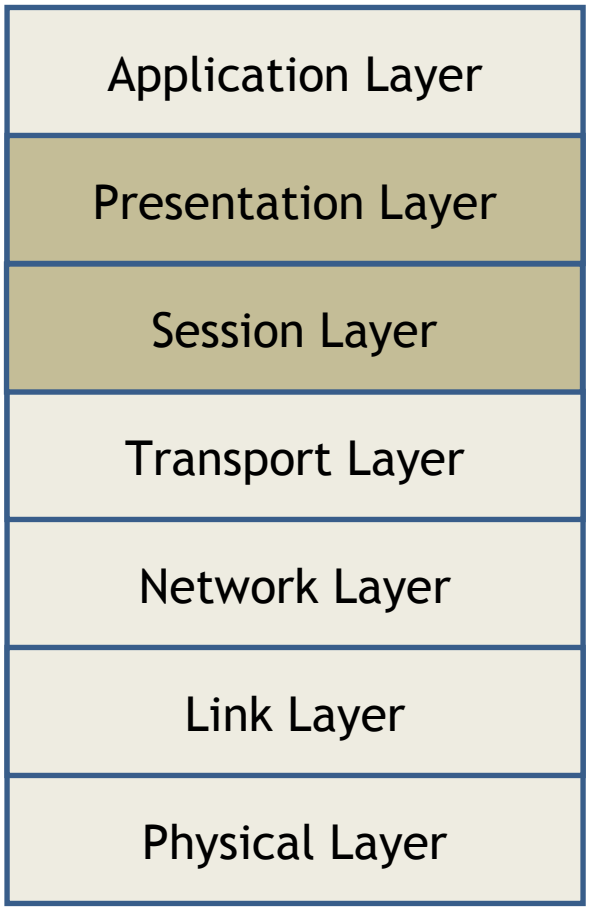


Lower layer provides a service to higher layer

Higher layer doesn't care (or even know, sometimes) how service is implemented: **lack of transparency**

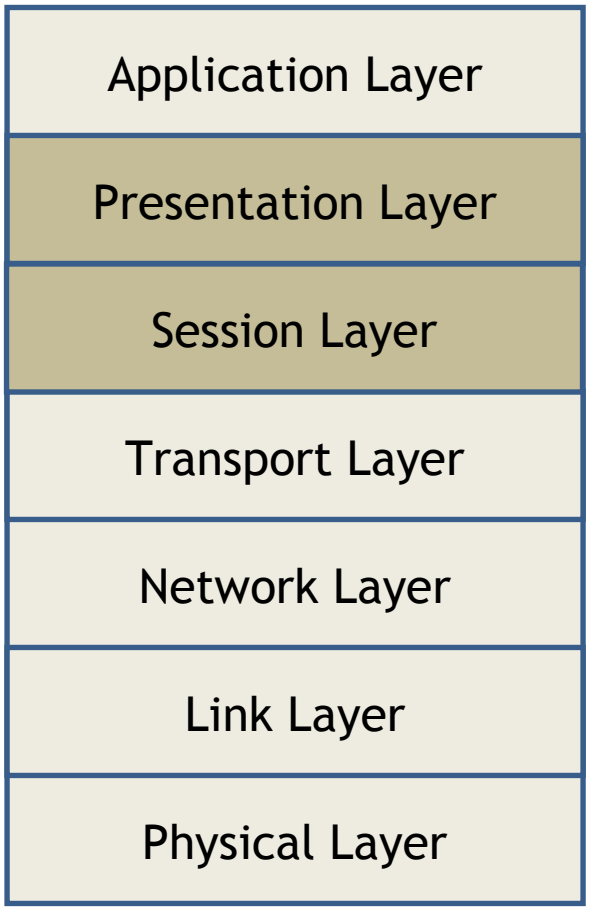
Layering Standards

- 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



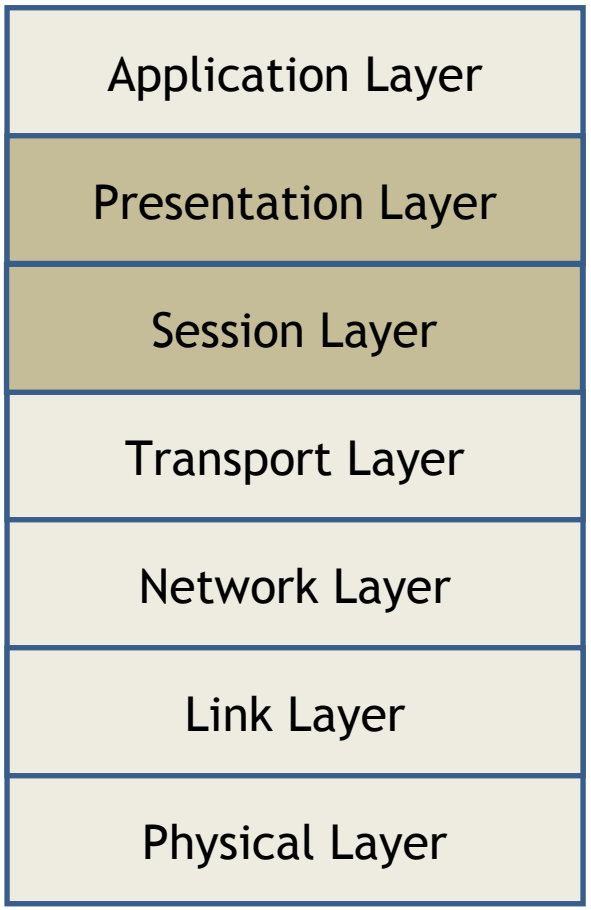
Layer Functionality

- 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

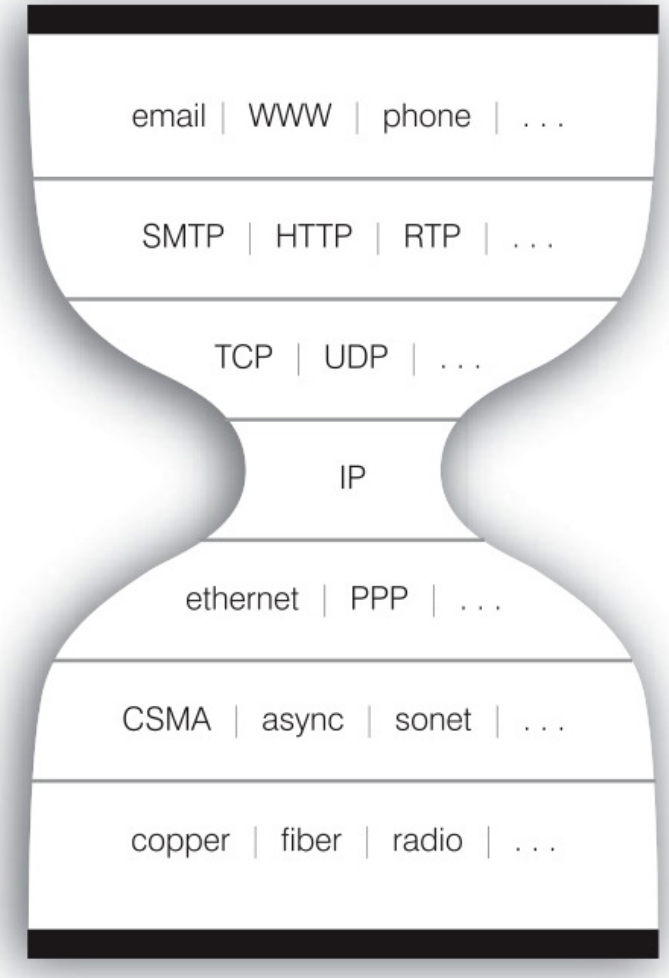
- Network Layer – Addressing and routing
- Link Layer – *Reliable* single-hop data transfer
  - Framing, error detection, medium access control (MAC) sub-layer
- Physical Layer – Moves bits
  - Bit synchronization, modulation & demodulation, physical connections



Internet Layering

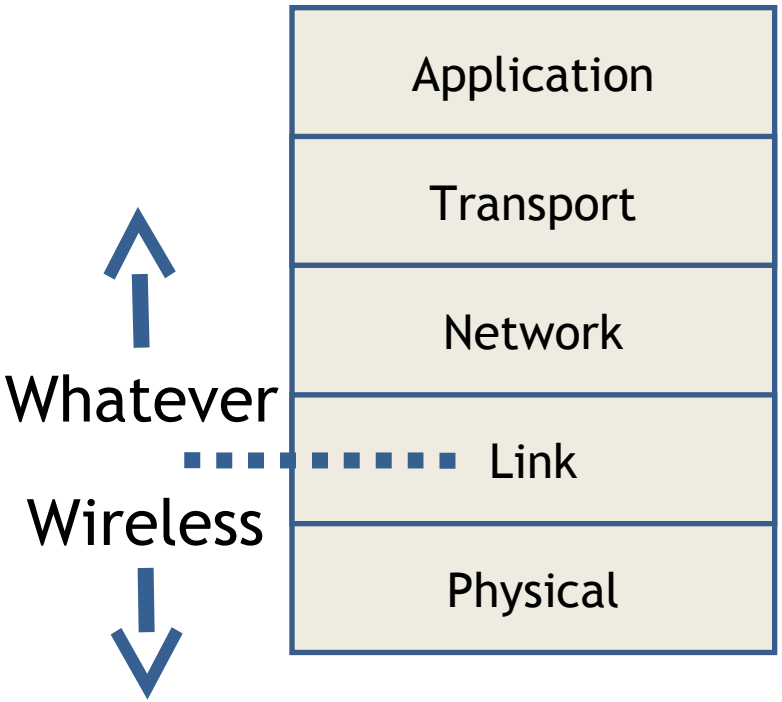
- Layered protocols have been the basis of network design for decades

- Layers work great in some scenarios



Layering in Wireless

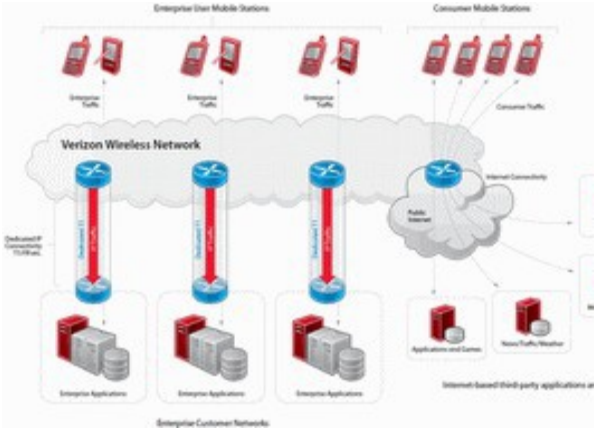
- Below a certain point, things can be designed for wireless communication
- Above that point, the medium doesn't matter…
  - Or does it?
  - Or should it?
- Trade-offs...



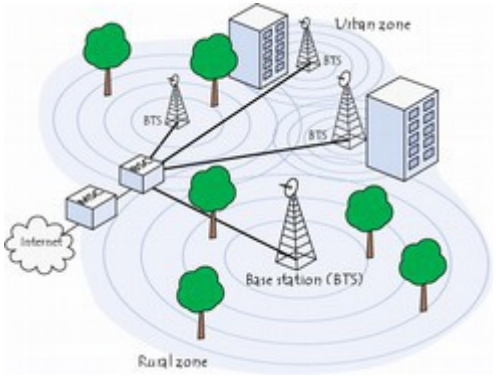
What types of wireless networks are we going to talk about?

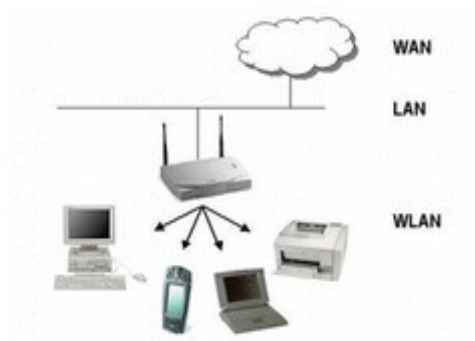
Wireless Networks

Enterprise Wireless

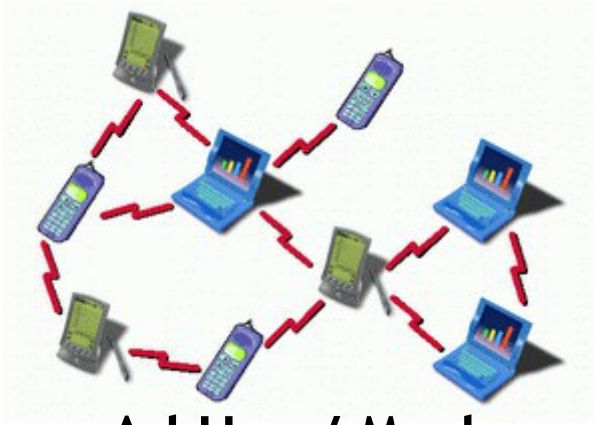


Telecommunications

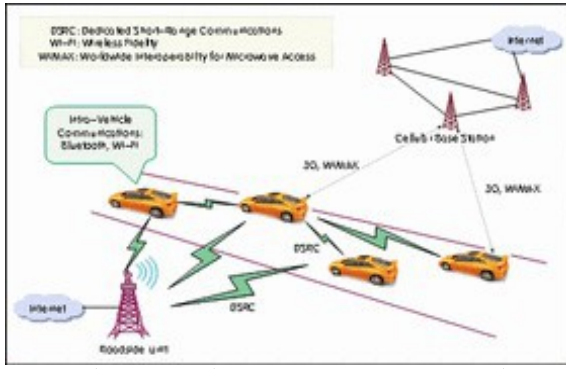




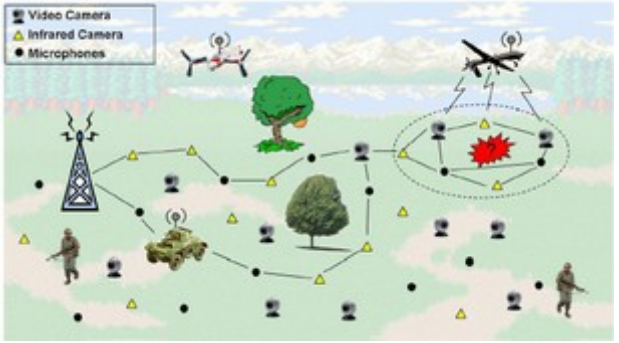
Wireless Internet



Ad Hoc / Mesh



Vehicular Networks

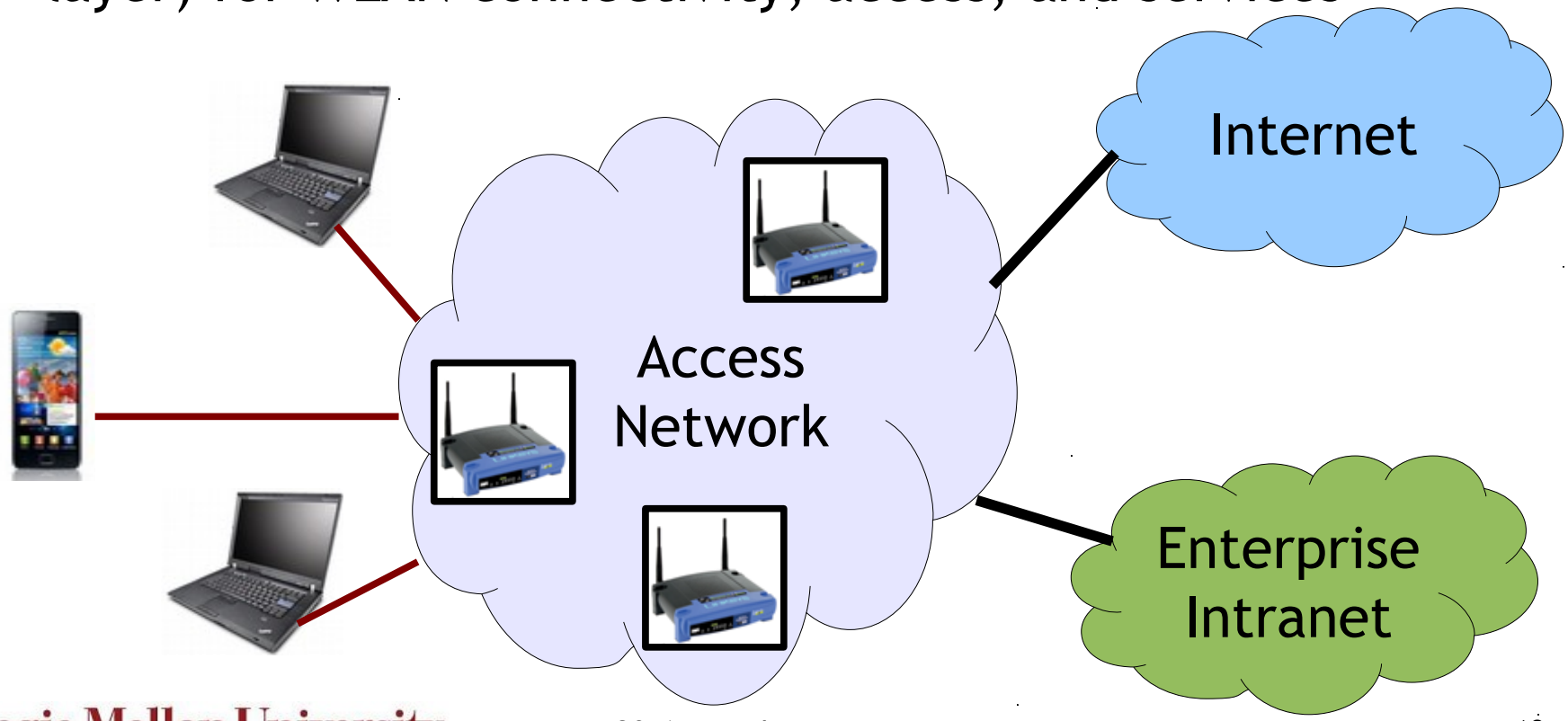


Sensing / Control Systems

And more...

WLAN 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

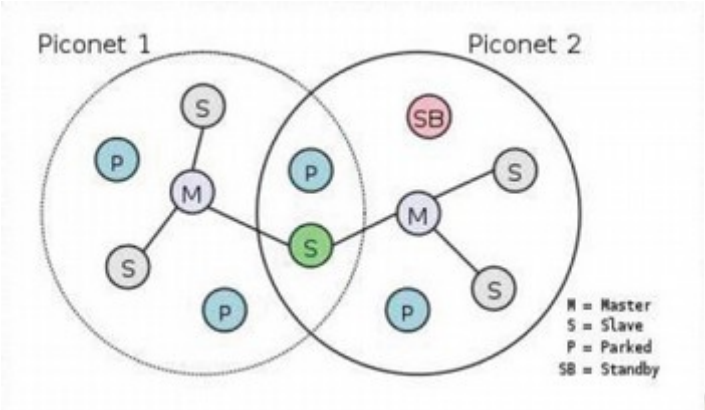


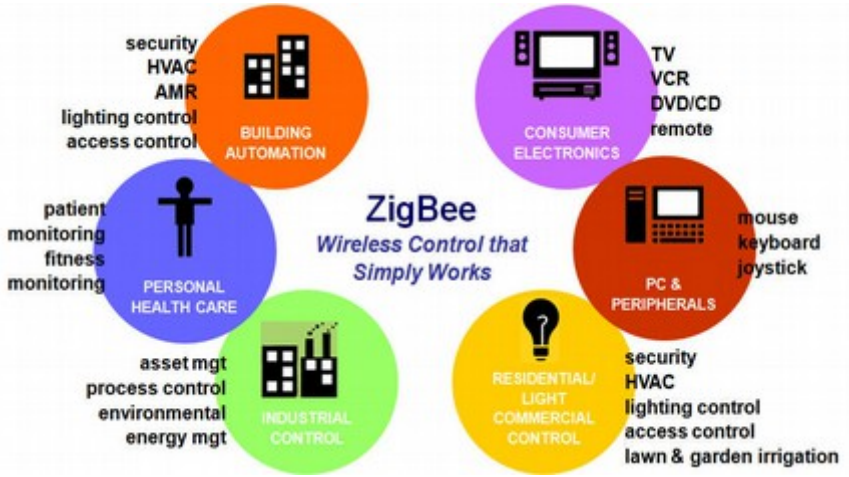
Telecom/Mobile Networks

- Mobile networks have evolved from providing voice connectivity to the PSTN to providing all forms of connectivity to the Internet
  - AMPS first introduced in 1978
  - GSM developed through the 1990s-2000s
  - 3G/4G standards emerged with full data support, looking more like a WLAN/WMAN

Personal Area Networks

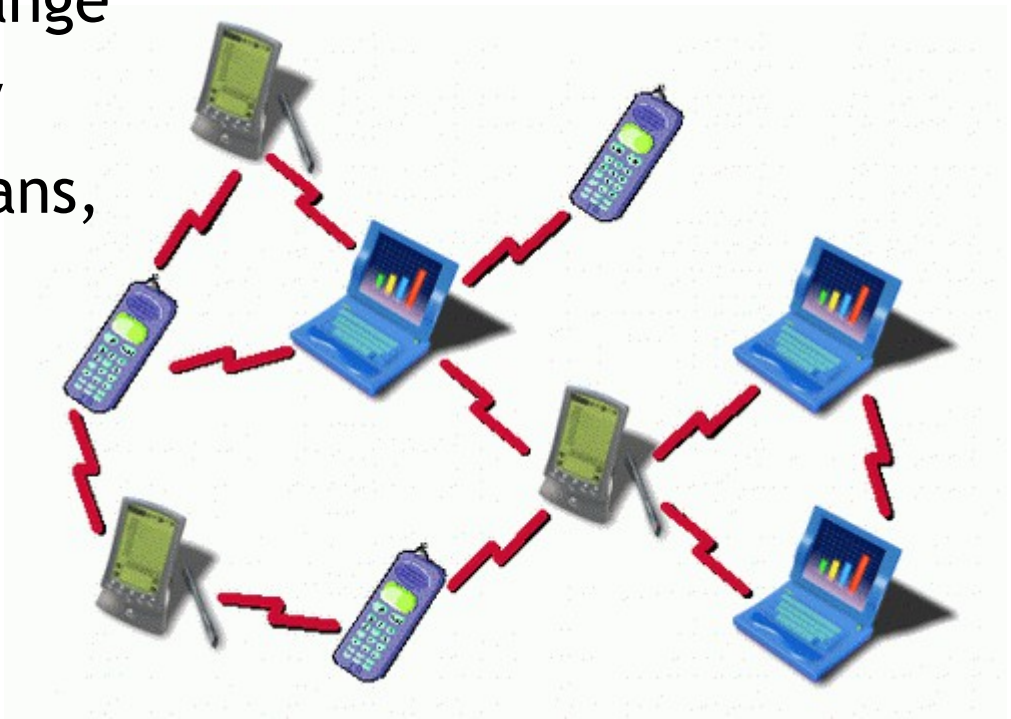
- Local “device-to-device” networking using the 802.15 family of standards
- Typically short range, few devices, low power
- Commonly used for home, personal, office





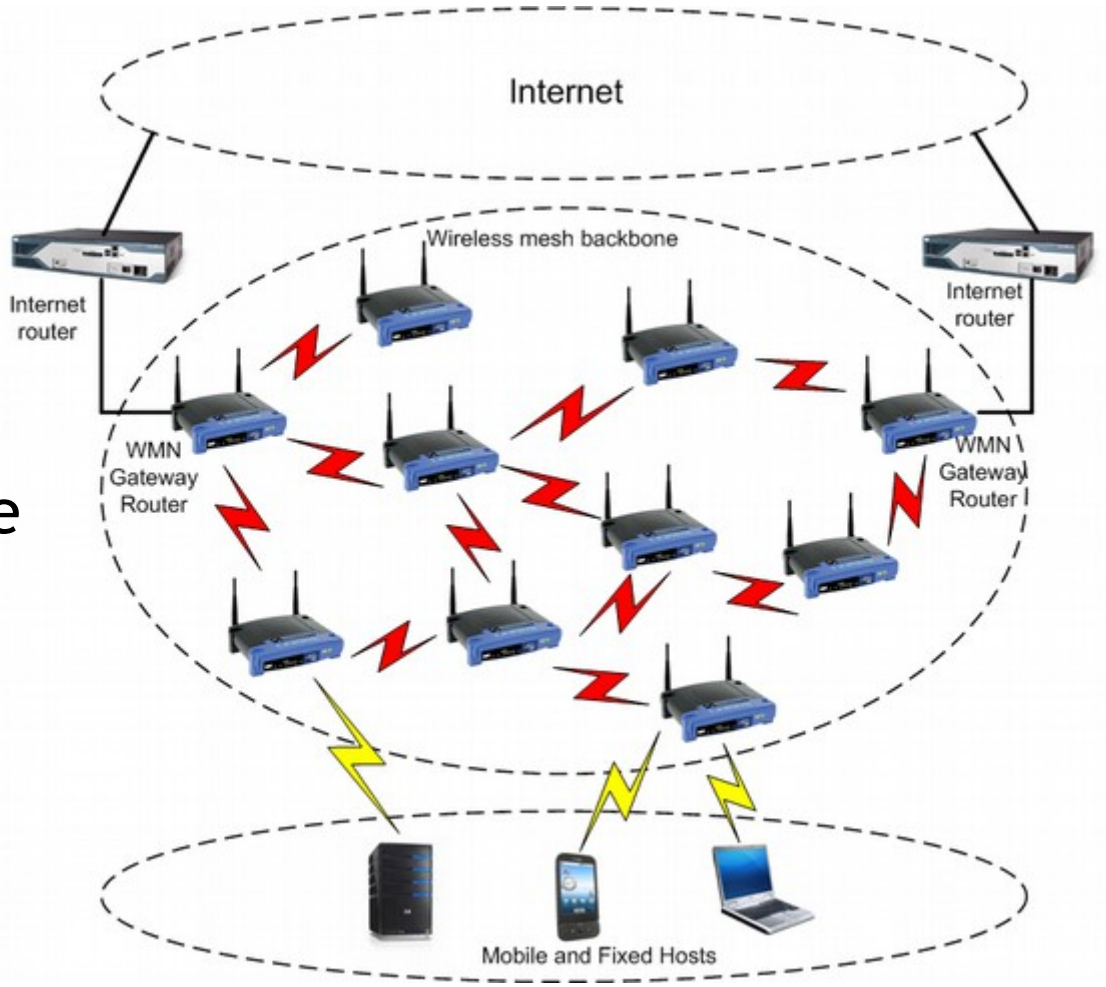
Mobile Ad Hoc Networks

- Mobile ad hoc networks (MANETs) typically connect local/offline devices with 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



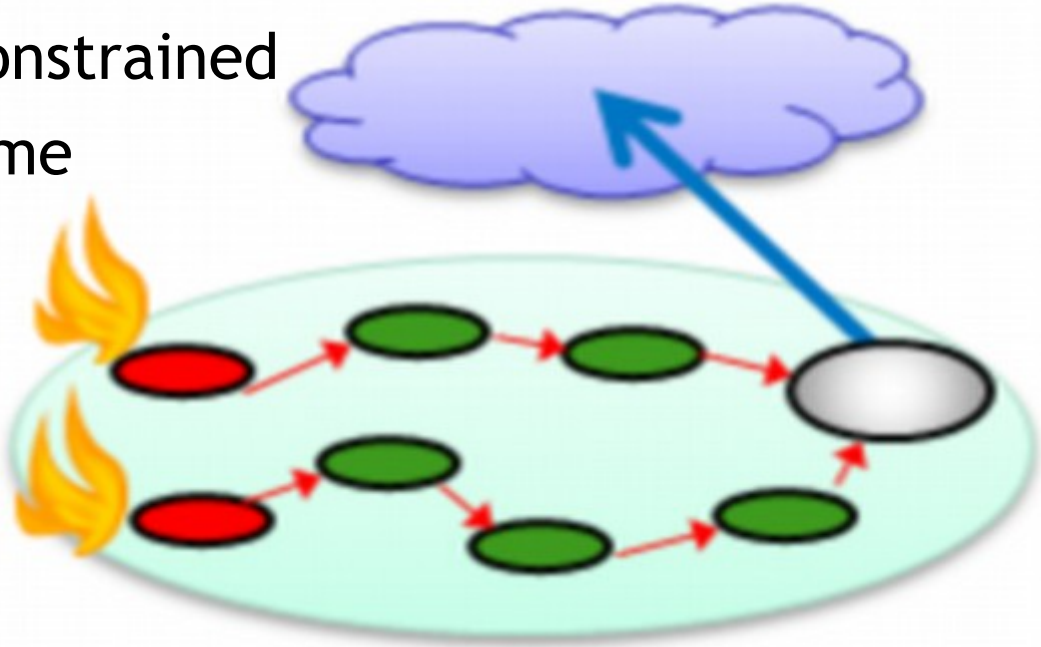
Wireless Mesh Networks

- 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



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



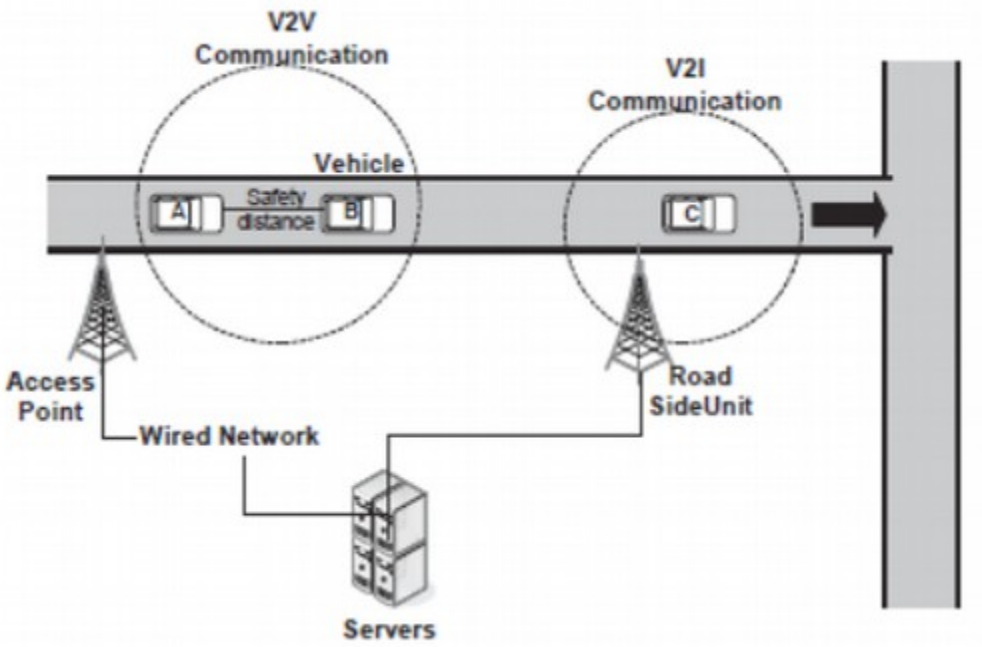
Home Networks

- 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.)

VANETs

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

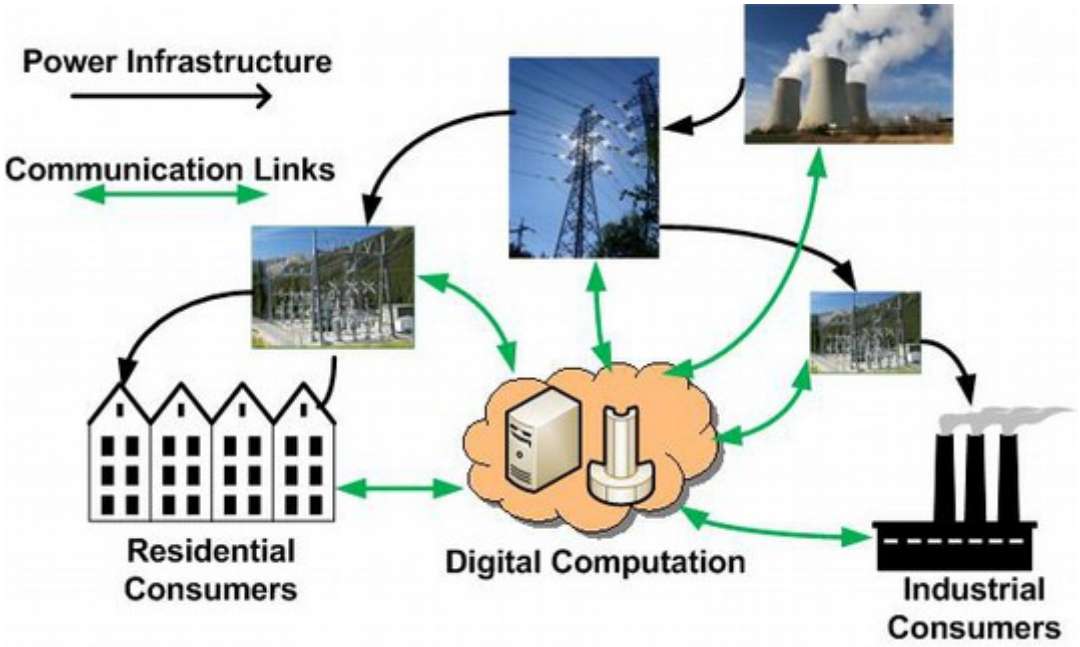


- Applications of interest:
  - Automated driver safety management
  - Passive road quality / condition monitoring
  - In-car entertainment
  - Navigation services
  - Context-aware rec's:
    - "This alternate route would be faster, and it would go past your favorite Primanti Bros."

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



What is Wireless Network Security?

A probabilistic guarantee that a wireless network does a particular job *as expected*, even when faced with *a variety of threats*

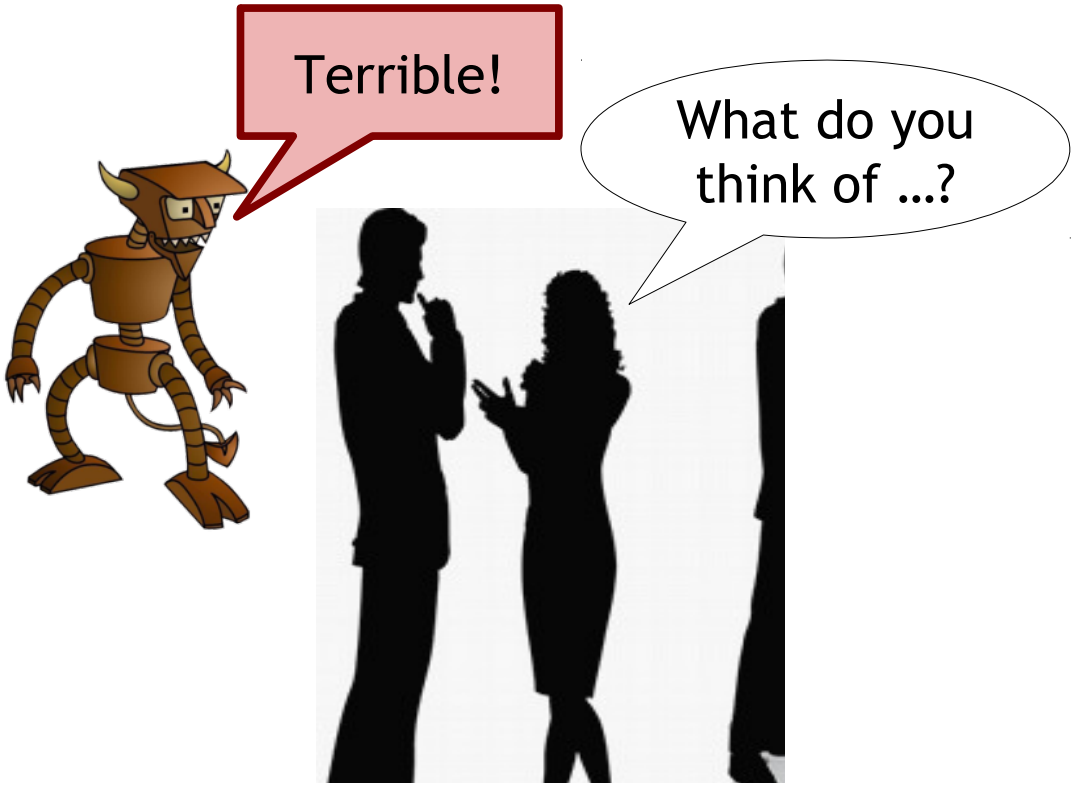
Threats of Interest

- Many different types of threats faced in wireless
- Including (but not limited to) threats to:
  - Information content, source, etc.
  - Availability of wireless connectivity
  - Performance of network protocols
  - Proper use of scarce resources (energy, bandwidth, …)
  - Proper use of command/control messages
  - Correct representation of devices
  - …
- All of these are composed of certain primitives

Eavesdropping

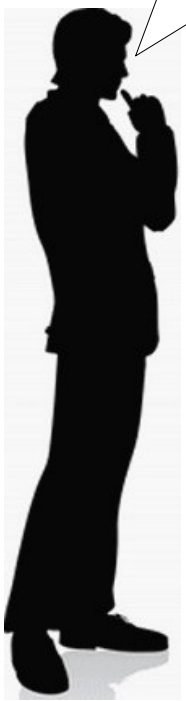
Interference

Msg/Pkt/Signal Injection/Replay



Spoofing

Man-in-the-Middle Attack

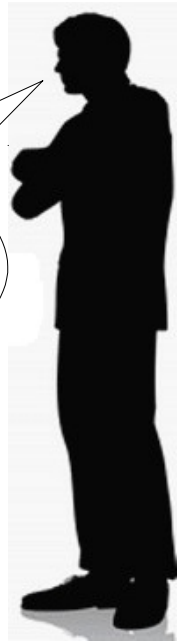


Can you bring a Coke to Table 3?

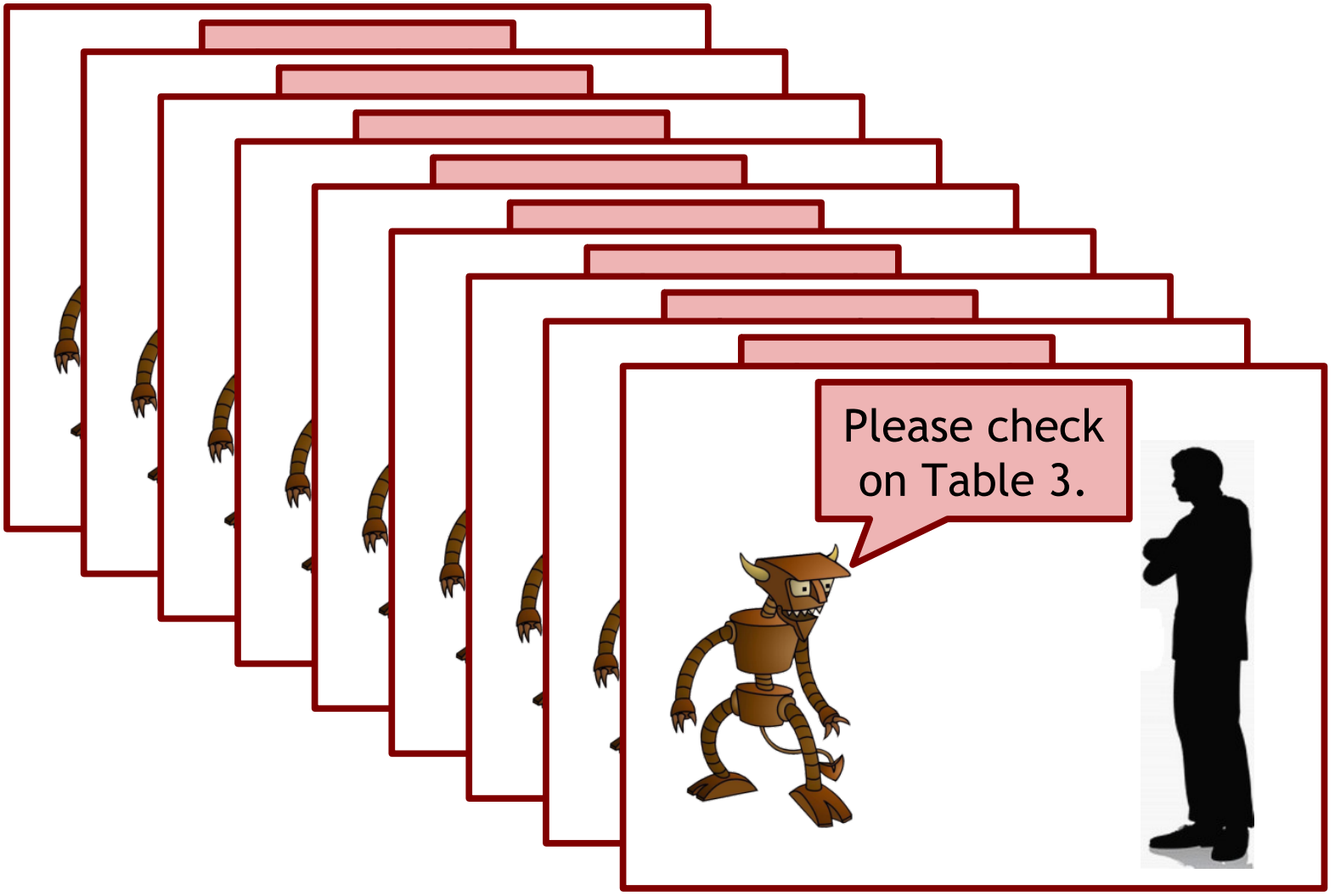
Can you bring a **Diet** Coke to Table 3?

Coke to Table 3, sure thing!

Diet Coke, Table 3, sure thing!



Resource Depletion / Wastage



Byzantine Threats

- Byzantine threat is sort of like insider threat
- Basically, an authenticated / valid / trusted group member stops following the rules

And Many More...

- Denial/Degradation of Service
- Exploiting Composition Issues
- Context Manipulation
- …

Our plan.

We'll study how these various threats manifest at different layers and in different types of wireless systems.

January 19:
Project Discussion;
OMNET++ Tutorial I