Announcements

- Project proposals:
  - Written proposal due in 1 week
  - Presentation in class in 1 week
  - Contact me to discuss project topics, topics must be approved prior to proposal
Agenda

• Overview of systems of interest
• Brief highlights of standards, protocols, etc.
• Discussion of challenges, issues, constraints
• Discussion of potential security concerns
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
Security in MANETs

- What aspects of information, network, and system security are harder in MANETs?
  - Addressing/naming/identity management issues
  - Device/user authentication
  - Routing/discovery
  - Accountability
  - Access / entry to network
  - Intrusion detection/prevention system
  - Trusted information management
Lack of Infrastructure

- Implies that security mechanisms are decentralized / distributed
- Who do you trust?
- What if you don't trust anyone?
- What services are no longer secure?
Mobility

- Network is fluid
  - Security associations are dynamic or short-lived
  - Members can join and leave network or groups
  - Observing behaviors over a long period (e.g., for monitoring or intrusion detection) is not possible
  - Dynamic connectivity and reachability
Opportunities for Misbehavior

• With no authority, controller, or coordinator, attackers can misbehave arbitrarily!
  – Layered attackers
    • Targeted misbehavior at the PHY, MAC, NET, TRANS, or APP layers
  – Cross-Layer attackers
    • Can incorporate information from multiple network layers for various attack gains
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
Wireless Mesh Networks

• Pure ad hoc network
  – No infrastructure, completely flat architecture

• Mesh network
  – Adding dedicated nodes which connect ad-hoc network to a wireless backbone
  – Hierarchical architecture

• However, there’s no strict boundary between the ad hoc network and the mesh network.
Wireless Mesh Networks

- Mesh networks provide multi-hop wireless connections to a backhaul
  - Mesh routers can be fixed or mobile, serve as multi-hop connectivity for Internet traffic to/from users
  - End users.getHosts are typically mobile, hand-off to numerous mesh routers
  - Alternatively, a mobile mesh has hosts/routers only and a few fixed APs
## Standards for Mesh Network

<table>
<thead>
<tr>
<th>Type of mesh networks</th>
<th>Corresponding standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMAN mesh (WiMAX)</td>
<td>IEEE 802.16a (mesh option), IEEE 802.16j (multihop relay)</td>
</tr>
<tr>
<td>WLAN mesh (Wi-Fi)</td>
<td>IEEE 802.11s</td>
</tr>
<tr>
<td>WPAN mesh (ZigBee)</td>
<td>IEEE 802.15.5</td>
</tr>
</tbody>
</table>
WMAN Mesh

(a) point-to-multipoint mode
(b) mesh mode

[Lee et. al, 06]
WLAN Mesh

[Lee et. al, 06]
Where's the boundary between MANETs and WMNs? Can protocols, standards, designs, etc. for one be applied to the other?
Tethering to the Cloud

• Extension of the ad hoc vision
  – Leveraging occasional connections to the Internet through mesh or DTN may have advantages and disadvantages

  – Sensor networks are connected through base stations to relay sensed information, but typically operate independent of the cloud

  – What are the opportunities for leveraging that possible connection?
Detaching from the Cloud

- Convergence of the WLAN/cell/MANET domains can also move the other way
  - Cell services don't always require the cloud, so why not take those services off?
    - Save bandwidth, reduces risk of information leakage, etc.
  - e.g. home energy management systems
    - Why is all my private home and energy use/management information stored on the cloud when I access it from my couch?
    - Billing issues?
Sensor Networks

- Mostly use 802.15.4 / ZigBee, but architecture and topology are different
  - 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
  – So?

  – Control systems have much tighter time constraints than data/computing systems
    • What happens if your video stream is delayed? Fire alarm?
  – Control information can be operation/safety critical
    • Authentic control signal vs. correct control signal
Unattended Operation

- Unlike many of the systems we've talked about so far, sensing/actuation devices aren't associated with people
  - Completely autonomous operation
  - No user interface
  - All debugging, reporting, re-programming, data dissemination, control, etc. has to happen over a wireless interface (in any practical setting)
Context

- Sensor data usually requires some additional contextual meta-data to describe the data
  - Location of the sensor device
  - Types of sensors on the device
  - Granularity of each data field
  - Time-stamp of measurements
  - ...

- Context information relates to various types of network services (e.g., synchronization, localization, db, etc.)
Home Networking
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.)
Heterogeneity

- Home networks comprise many different wireless technologies, including:
  - WiFi
  - PAN
  - Mesh networking
  - Sensors and actuators

- Interoperability adds new dimensions to the challenges and security concerns
Interoperability Issues

- In a home network, security properties should be provided across protocol domains
  - Not only do protocols need to interoperate, but security mechanisms need to be composable across interoperating domains
    - Ex: how to guarantee data deliver across a network using ad hoc WiFi, ZigBee mesh, ...
  - Interoperability highlights the difference between “network security” and “system security”
Usable Security

• One thing we definitely know about home network security is that we shouldn't assume that users will understand it
  – How many people understand WiFi security on their home WiFi AP/router?
  – Adding a new laptop to a home WiFi network is hard enough...imagine adding new appliances, sensors to every outlet, heating duct, and so on
  – How to automate security to the point that people can use it in various scenarios?
VANET
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.”
Subsystems / Subnetworks

• VANETs include different subsystems
  – These subsystems need to interoperate, either directly or through APIs
  – Different components are developed by different vendors, not always with standards
  – As with home networks, interoperability has major implications, but now the different devices are highly dynamic / mobile
Example Components

- User devices interact with the vehicle using WiFi, Bluetooth, NFC, visual comms, etc.
- On-board sensors communicate with a controller using ZigBee, e.g., TPMS
- Telematics unit (e.g., 4G) for car-to-cloud
- Safety messaging systems between vehicles
802.11p and DSRC

- 802.11p extends the 802.11 standard to include vehicular communications in the 5.9 GHz band
  - Allows dynamic comms without setting up a BSS (i.e., no SSID) for fast decentralized operation
  - No association, no authentication, no access control...
  - Also includes mechanisms for channel management and synchronization

- Dedicated Short Range Communication
  - One- and two-way communication based on the 802.11p standard
  - Builds on the older ASTM E2213-03 standard
WAVE

• Wireless Access in Vehicular Environments
  – Wireless stack for vehicle-to-vehicle and vehicle-to-infrastructure communications
  – Based on IEEE 1609 standard family
  – Built on top of the 802.11p / DSRC foundation
  – Think of it as:
    • 802.11p + DSRC = PHY/MAC
    • WAVE / 1609 = layers 3+
  – Envisioned for 100s-1000s of applications
    • Safety messaging, autonomous driving, assisted braking, etc.
    • Sensing road conditions, traffic, etc.
    • Payment systems (tolls, parking, etc.)
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
Issues

• Very large, very dynamic control system, sort of like a giant sensor/actuator network
• Failure → outage
• Better data and controls → more $$$

• Misbehavior:
  – DoS, where service = \{power, billing, sensing, communication, ...\}
  – Selfish service manipulation
  – Price manipulation, mis-charging, fraud
  – ?
Some General Questions

• Smart Grid is very new, so there aren't any firm standards yet...but many standards bodies are in progress
  – What aspects of the Smart Grid should be wireless?
    • This is a pretty hot topic of debate. Some people say none, some people say as much as possible.
  – What value can be provided by wireless?
  – What risks does wireless introduce?
Next Time

• Wireless link security
  – General wireless link layer issues

  – WiFi link security