CS551
Wireless and Mobile Networking
Bill Cheng

http://merlot.usc.edu/cs551-f12
How Is Wireless & Mobile Different From Traditional Networking?

- **Wireless**
  - cellular vs. ad hoc
  - transmission media is air
    - interference from other radios and obstacles ➞ much less reliable
    - higher error rates
    - mitigated by physical level work (coding)
  - not everyone can hear each other
  - slower speed than traditional (limited spectrum)
  - security
    - network may not trust users
    - users may not trust network
How Is Wireless & Mobile Different From Traditional Networking? (Cont...)

- Mobile
  - location change ⇒ routing needs to change
    - what basestation are you talking to
  - limited energy (battery)
  - scaling may not be as important
    - scaling in ad hoc network is open research
  - security, again
    - network may not trust users
    - users may not trust network
Dimensions of Wireless/Mobile

- mobility
  - one-hop to base-station vs. ad hoc/multi-hop

- wireless
  - fixed vs. mobile

- protocols
  - IP vs. cell phone (3G) vs. protocols for sensor networks

- constraints
  - energy
  - radio range
  - antenna directionality

- trust
  - do you trust others to forward your data to overhear your packets

- app-level issues
  - even if you have connectivity, what can you do?
    - Ex: it may be easier to share files with floppies
    - often e-mail must go through a central server
Approach For This Class

Lots of work in mobile/wireless

Look at small sample
- link-layer: MACAW
- routing: Mobile IP and DSR
- transport-layer: SNOOP
- sensor network: Direct Diffusion
- applications (CSci555)
CS551
Mobile IP
[Johnson96b]
Bill Cheng

http://merlot.usc.edu/cs551-f12
Key Ideas

Mobile IP:
- how do people find you if you move around?
- specifically: how do you keep your IP address anywhere you go
Mobile IP

How do we deliver IP packets when endpoints move?

Issues
- Impact on IP addressing
- Impact on routing

Key design considerations
- Scale
- Incremental deployment

Result: Mobile IP [RFC 2290]
- Internet standard for support for mobility in IP
Possible Approaches

- Why not just announce a route to your host?
  - doesn’t scale to millions of hosts
  - breaks hierarchical addressing!

- Why not re-address your host?
  - then people can’t find out
  - but this is what 95% of people do today, because they only run clients, not servers

- Why not separate naming and addressing?
  - too many protocols use IP addresses instead of hostnames, especially for open connections
The IETF Mobile IP Approach

- A location registry
  - keeps track of where you are
  - tunnels packets to you

- Pros:
  - good scalability (many users)
  - incremental deployment easy

- Cons:
  - triangle routing through home
  - must be careful about security
  - is it really necessary? (consider end-to-end argument)
Mobile IP Terminology

- **Corresponding Host (CH)**
- **Mobile Host (MH)**
- **Home Agent (HA)**
- **Home Network (HN)**
- **Foreign Agent (FA)**
- **Foreign Network (FN)**

The diagram illustrates the key components of Mobile IP, including the corresponding host (CH), mobile host (MH), home agent (HA), home network (HN), foreign agent (FA), and foreign network (FN).
Discovering Agents

Q: How do laptops usually figure things out? Why not use that?
A: DHCP... because it didn’t exist when Mobile IP started.
MH moves to foreign network
MH registers with FA and gets temp local IP address
FA informs HA so HA always knows
Registration (Cont...)

HA setups tunnel to FA
Tunneling

- CH sends pkt to MH’s IP address like normal
- HA intercepts pkt (uses same IP network as MH) and tunnels pkt to FA
- FA gets tunneled pkt, decapsulates it, sends it to MH_{temp-local}
- MH’s reply can then go straight back to the CH

- CH does not have to be Mobile IP-aware
- Triangular routing
Other Mobile IP Issues

Route optimality
- resulting paths are not optimal, they all go through the HA
- can be improved with *route optimization*
  - smart senders keep cache of FA & MH
  - one more thing to keep updated

Smooth handoffs
- don’t want to drop pkts when changing FAs

Security issues
- authentication
  - FA may make false claim that MH is in its network
  - don’t want others to claim to be MH
- confidentiality
  - FA may be listening and recording
  - FA may modify messages