15-441 15-641 Computer Networking

Lecture 26: Wireless and the Internet

Justine Sherry
Peter Steenkiste

Fall 2017

www.cs.cmu.edu/~prs/15-441-F17

Overview

- Internet mobility
- Cellular

Routing to Mobile Nodes

- Obvious solution: have mobile nodes advertise route to mobile address/32
  - Should work!!!
- Why is this bad?
  - Consider forwarding tables on backbone routers
    - Would have an entry for each mobile host
    - Not very scalable
- What are some possible solutions?

How to Handle Addressing for Mobile Nodes?

- Simple existing solution: Dynamic Host Configuration (DHCP)
- Host gets new IP address in new locations
  - No impact on Internet routing
- Problems for the mobile host
  1. Host does not have constant name/address → how do others contact host?
  2. Transport connections are tied to src/dest IP addresses → What happens to active connections when a host moves?

We Can Fix the Naming Problem

- Use DNS and update name-address mapping whenever host changes address
  - An awkward solution, at best
  - Increases “write” load on DNS
  - What about caching?
  - Also raises security issues
- Fixes first contact problem but the broken transport connection problem remains

How to Handle Transport Connections for Mobile Nodes?

- TCP currently uses 4 tuple to describe connection
  - <Src Addr, Src port, Dst addr, Dst port>
- Solution: Modify TCP to allow peer’s address to be changed during connection
- Security issues
  - Can someone easily hijack connection?
- Difficult to deploy → both ends must support mobility

How about Link Layer Mobility?

- Link layer mobility is easier
- Learning bridges can handle mobility → this is how it is handled at CMU
- Wireless LAN (802.11) also provides some help to reduce impact of handoff
  - Reduce latency, packet loss
- Problem is with inter-network mobility, i.e. Changing IP addresses
  - Want host to always have the same IP address

Mobile IP Goals

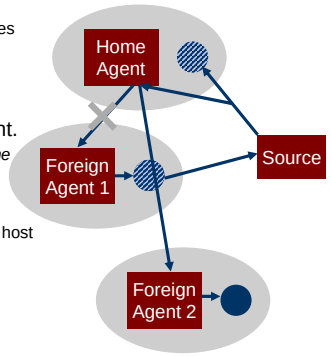
- Communicate with mobile hosts using their “home” IP address
  - Target is “nomadic” devices: do not move while communicating, i.e., laptop, not cellphone
  - Allows any host to contact mobile host using its “usual” IP address, as if it where in its “normal” location
- Mobility should be transparent to applications and higher level protocols
  - No need to modify the software
- Minimize changes to host and router software
  - No changes to communicating host
- Security should not get worse

Mobile IP Overview

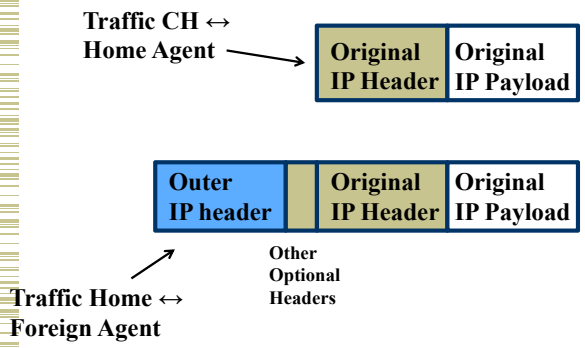
- Home network has a home agent that is responsible for intercepting packets and forwarding them to the mobile host.
  - E.g., router at the edge of the home network
  - Forwarding is done using tunneling
- Remote network has a foreign agent that manages communication with mobile host.
  - Point of contact for the mobile host
- Binding ties IP address of mobile host to a “care of” address in the foreign network.
  - binding = (IP address, foreign agent address)
  - binding includes time stamp

Mobile IP Operation

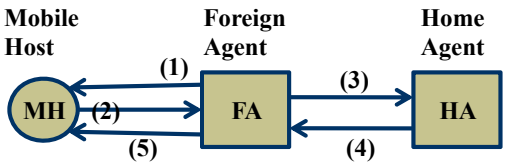
- Agents advertise their presence.
  - Using ICMP or mobile IP control messages
  - Mobile host can solicit agent information
  - Mobile host can determine where it is
- Registration process: mobile host registers with home and foreign agent.
  - Set up binding valid for *registration lifetime*
- Tunneling
  - forward packets to foreign agent
  - foreign agent forwards packets to mobile host
- Supporting mobility
  - invalidating old caches in a lazy fashion



Tunneling IP-in-IP Encapsulation



Registration via Foreign Agent

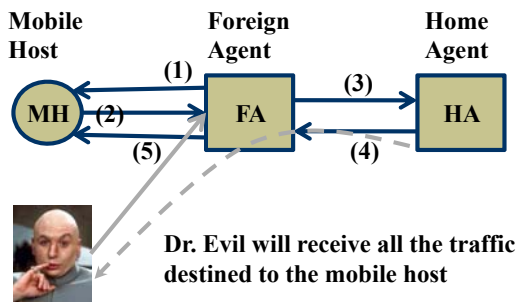


1. FA advertizes service
2. MH requests service
3. FA relays request to HA
4. HA accepts (or denies) request and replies
5. FA relays reply to MH

Optimizations

- Mobile host can be its own the foreign agent.
  - Mobile host acquires local IP address using DHCP
  - Performs tasks of the mobile agent
- Short circuit the home location by going directly to the foreign agent.
  - Routers in the network store cache bindings and intercept and tunnel packets before they the mobile host's home network
  - Need a protocol to update/invalidate caches
  - Raises many security questions and is not in the standard

Authentication



Mobile IP Authentication

- Without security, an adversary on any network with a FA could issue a registration request for a host on any network (with a HA)
  - HA would begin to forward datagrams to the bad guy
- Registration messages between a mobile host and its home agent must be authenticated
  - Uses mobile-home authentication extension
- Mobile hosts, home agents, and foreign agents must maintain a mobility security association for mobile hosts, indexed by…
  - Security Parameter Index (SPI)
  - IP address (home address for mobile host)

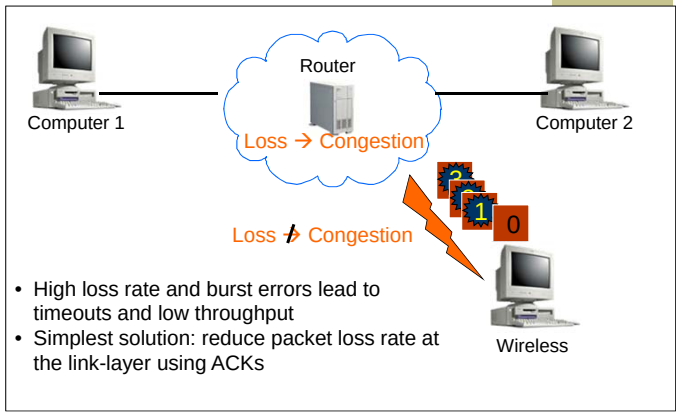
Discussion

- Mobile IP not used in practice
- Not designed for truly mobile users
  - Designed for nomadic users, e.g. visitors to a remote site
  - Only solves the initial contact problem, but …
- Mobile devices are typically clients, not servers, i.e., they initiate connections
  - Problem Mobile IP solves not common in practice
- IETF defined solutions that are more efficient
  - But they are move heavy weight: effectively creates overlay with tunnels and special "routers"
- Ultimately all solutions are similar: need a "relay" that knows location of the device

Overview

- Internet mobility
- Cellular

Wireless Bit-Errors



- High loss rate and burst errors lead to timeouts and low throughput
- Simplest solution: reduce packet loss rate at the link-layer using ACKs

Overview

- Internet mobility
- Cellular

Cellular versus WiFi

	Cellular	WiFi
Spectrum	Licensed	Unlicensed
Service model	Provisioned "for pay"	Unprovisioned "free" – no SLA
MAC services	Fixed bandwidth SLAs	Best effort no SLAs

Implications WiFi

	WiFi	Implication
Spectrum	Unlicensed	No control – open, diverse access
Service model	Unprovisioned "free"	No guarantees maximize throughput, fairness
MAC services	Best effort no SLAs	FCC rules to avoid collapse

Implications Cellular

	Cellular	Implication
Spectrum	Licensed	Provider has control over interference
Service model	Provisioned "for pay"	Can and must charge + make commitments
MAC services	Fixed bandwidth SLAs	TDMA, FDMA, CDMA; access control

But There are Many Similarities

- Cellular and WiFi face the same fundamental physical layer challenges
  - Interference, attenuation, multi-path, …
- Spatial frequency reuse based on "cells"
  - Adjacent cells use different frequencies
- Over time, they use similar modulation schemes
  - Each generation uses the best technology available at that time
- Rapid improvements in throughputs
  - Better modulation and coding, increasingly aggressive MIMO, …

23

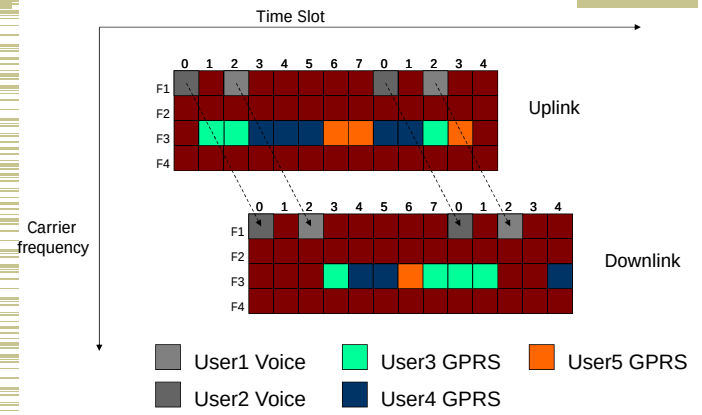
The Advent of Cellular Networks

- Mobile radio telephone system was based on:
  - High power transmitter/receivers
  - Could support about 25 channels
  - in a radius of 80 Km
- To increase network capacity:
  - Multiple low-power transmitters (100W or less)
  - Small transmission radius -> area split in cells
  - Each cell with its own frequencies and base station
  - Adjacent cells use different frequencies
  - The same frequency can be reused at sufficient distance

Cellular Standards

- 1G systems: analog voice
  - Not unlike a wired voice line (without the wire)
  - Pure FDMA: each voice channel gets two frequencies
- 2G systems: digital voice
  - Many standards
  - Example: GSM - FDMA/TDMA, most widely deployed, 200 countries, a billion people
- 2.5G systems: voice and data channels
  - Example: GPRS - evolved from GSM, packet-switched, 170 kbps (30-70 in practice)
  - Use some of the “voice slots” for data

GPRS Radio Interface

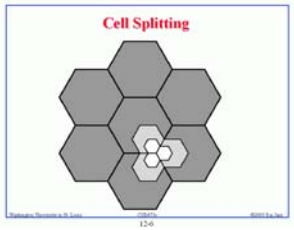


Cellular Standards

- 3G: voice (circuit-switched) and data (packet-switched)
  - Several standards
  - Most use Code Division Multiple Access (CDMA)
- 4G: 10 Mbps and up, seamless mobility between different cellular technologies
  - LTE the dominating technology
  - Completely packet switched, including voice
  - Uses Orthogonal Frequency Division Multiplexing (OFDM) for increased robustness wrt. frequency selective fading and mobility

How to Increase Capacity?

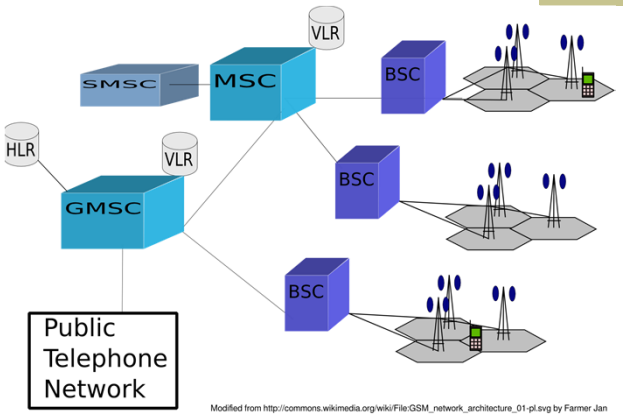
- Adding new channels
  - More spectrum – spectrum auctions
- Frequency borrowing
  - More flexible sharing of channels across cells
- Sectoring antennas
  - Split cell into smaller cells using directional antennas – 3-6 per cell
- Microcells, picocells, …
  - Antennas on top of buildings, lamp posts
  - Form micro cells with reduced power
  - Good for city streets, roads and inside buildings



Mobility with GSM

- Mobile Station – MS
  - A device connecting to the cellular network
- Base Station Controller - BSC
  - In charge of a group of cells
  - Sometimes called a Location Area (LA)
- Mobile Switching center – MSC
  - In charge of several clusters of cells
- Gateway Mobile Switching center – GMSC
  - Connects to the wired telephone networks
- Location registries
  - Home Location Registry (HLR)
  - Visitor Location Registry (VLR)

GSM Core Architecture



Modified from http://commons.wikimedia.org/wiki/File:GSM_network_architecture_01-pl.svg by Farmer Jan

Home Location Register

- One per "operator"
- Contains entries for every subscriber and every mobile ISDN number that is homed in the respective network
- Permanent subscriber data and relevant temporary information
- Current location of the mobile station
- All administrative activities of the subscriber happen here!

Visitor Location Register

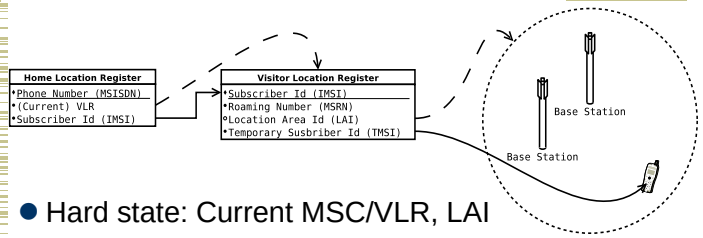
- Stores data on all mobile stations that are currently in the administrative area of the MSC
  - Roughly a large region
- 1 VLR could be responsible for more than 1 MSC
- A roaming MS will be registered in a VLR of its home network or the foreign network depending on its location
- MS registers upon entering a LA. The MSC passes the identities of the MS and LA to VLR

GSM Addressing Hierarchy

- Device
  - IMEI (International Mobile Equipment Identifier)
- User
  - IMSI (International Mobile Subscriber Identifier)
  - MSISDN (Mobile Subscriber IDSN Number)
    - "Real phone number"
  - MSRN (Mobile Station Roaming Number)
  - TMSI (Temporary Mobile Subscriber Identity
  - LMSI (Local Mobile Subscriber Identity)
- Other
  - LAI (Location Area Identity)
  - CI (Cell Identity)

Just for your entertainment – do not memorize

GSM Address Lookup ("registers")



- Hard state: Current MSC/VLR, LAI
  - (Necessary to page phone, updated whenever mobile moves)
- Soft-ish state:
  - MSRN, cell ID, TMSI

Again: Grossly simplified for your safety and sanity!