Wireless Network Security
CS/IT 818
Spring 2008

Sanjeev Setia

http://www.cs.gmu.edu/~setia/cs818/

Acknowledgements

- Slides adapted or borrowed from
  - *Computer Networking: A Top Down Approach* 4th edition. Jim Kurose, Keith Ross, Addison-Wesley, July 2007
  - *Security & Cooperation in Wireless Networks.* Levente Buttyan, Jean-Pierre Hubaux, Cambridge University Press, January 2008.

Outline

- Survey of Wireless Networks
  - Read Kurose, Ross Ch 6 (or any recently published networking textbook)
  - Buttyan, Hubaux Ch 1, 2
- Security Issues for Wireless Networks
- Class Logistics
- Overview of Cryptographic Protocols
  - Appendix 1, Buttyan & Hubaux
  - Any book on security/cryptography
  - Security chapter of any networking textbook

Wireless Networks are ubiquitous

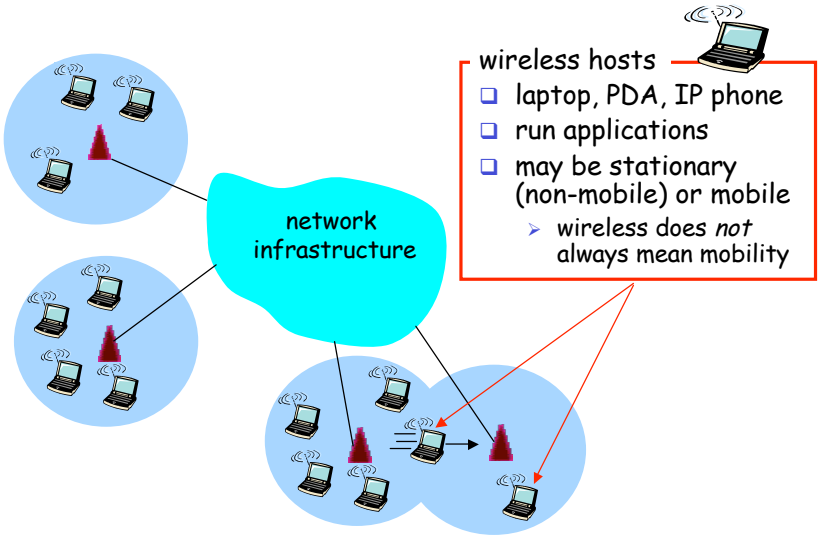
- Existing wireless networks
  - Cellular networks
  - Wi-Fi (802.11)
  - Bluetooth (802.15)
- Emerging networks
  - Ad hoc networks
    - Wireless sensor networks
    - Mesh Networks
    - Mobile Ad hoc networks (MANETs)
    - Vehicular Networks (VANETs)
  - Wi-MAX
  - RFID

Wireless and Mobile Networks

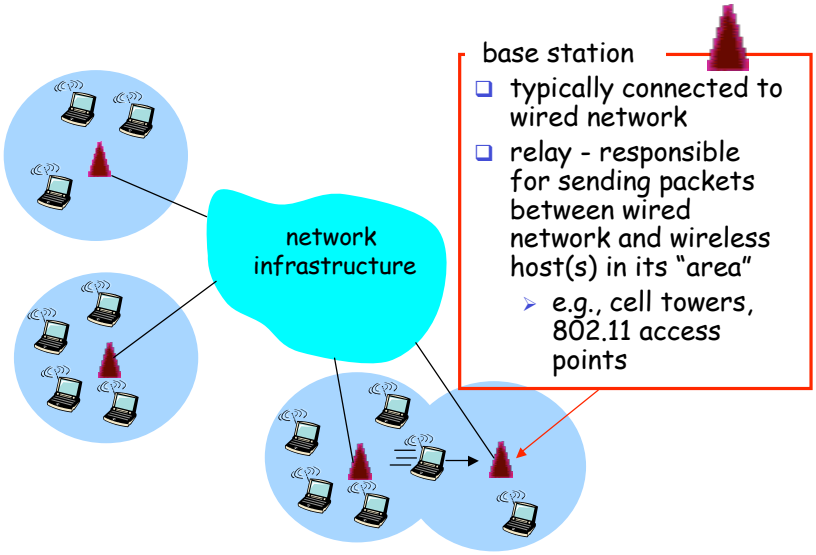
Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers!
- computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

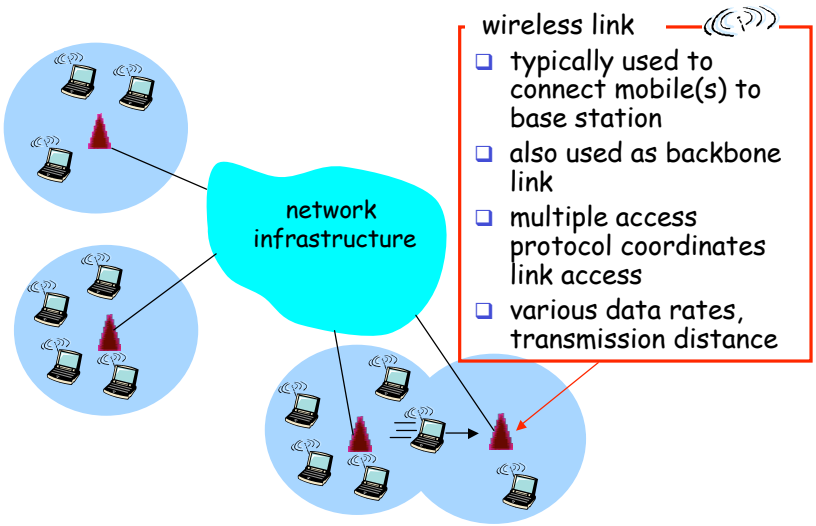
Elements of a wireless network



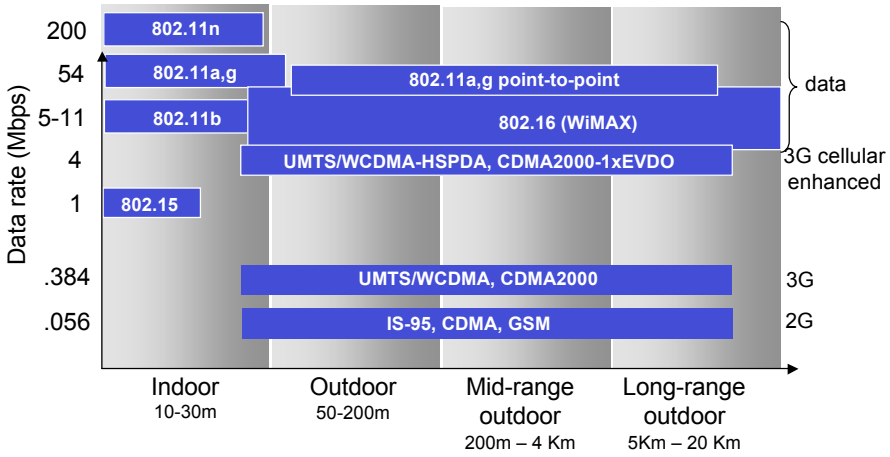
Elements of a wireless network



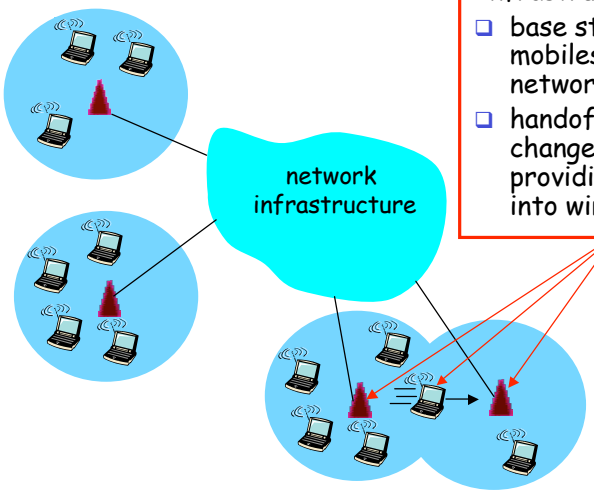
Elements of a wireless network



Characteristics of selected wireless link standards



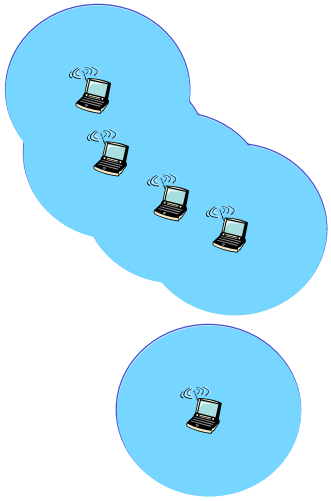
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics (1)

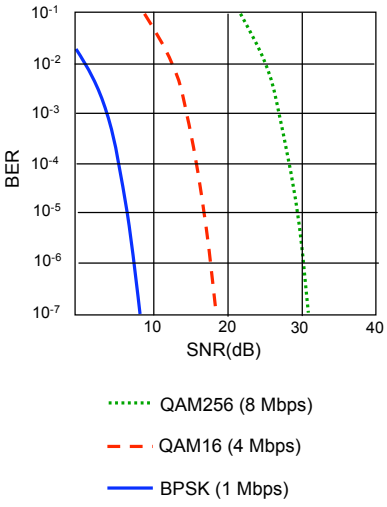
Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

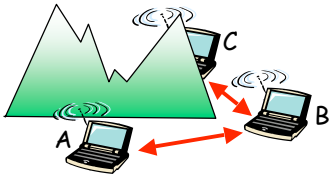
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



Wireless network characteristics

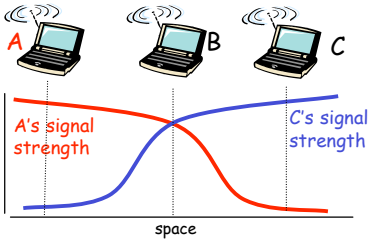
Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B



Signal attenuation:

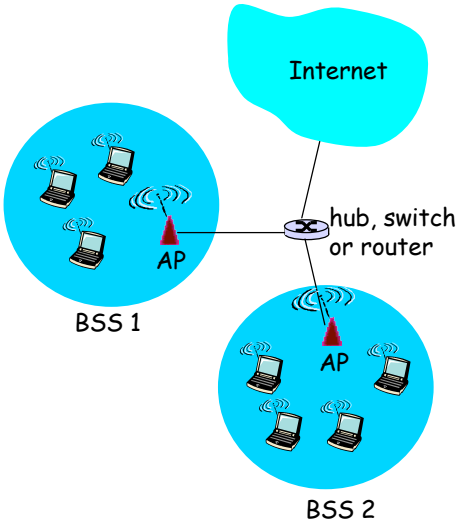
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

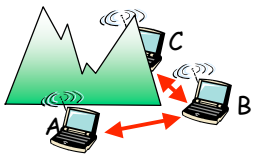
802.11 LAN architecture

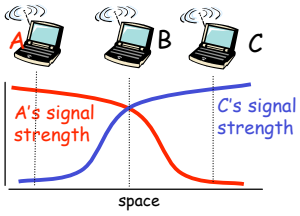


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

IEEE 802.11: multiple access

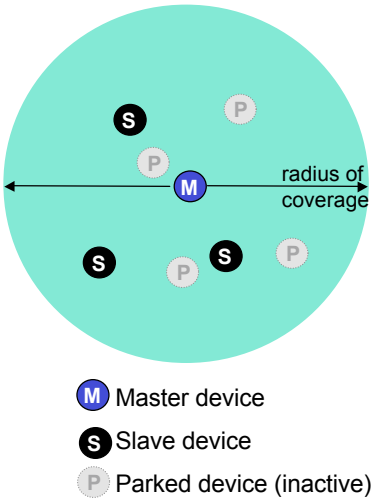
- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





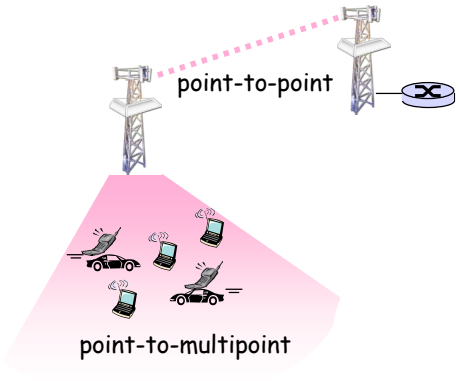
802.15: personal area network

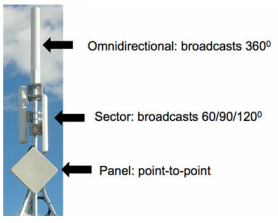
- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps



802.16: WiMAX

- like 802.11 & cellular: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps

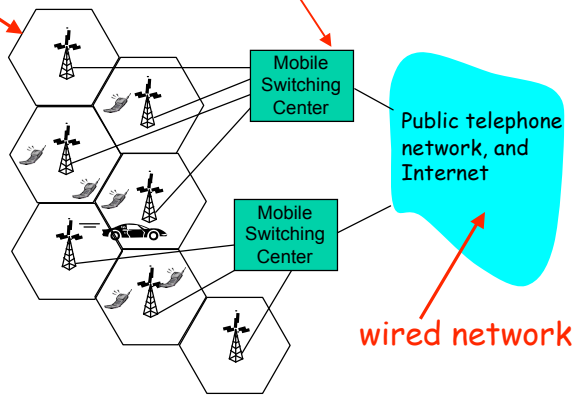




Components of cellular network architecture

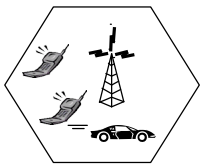
MSC
- connects cells to wide area net
- manages call setup
- handles mobility

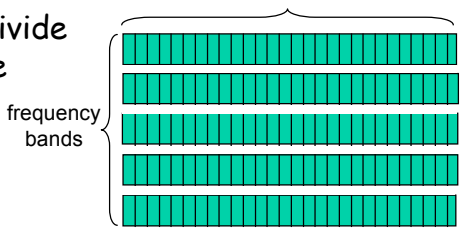
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum
- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access

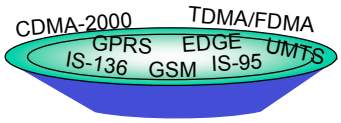




Cellular standards: brief survey

2G systems: voice channels

- IS-136 TDMA: combined FDMA/TDMA (north america)
- GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed
- IS-95 CDMA: code division multiple access



Don't drown in a bowl of alphabet soup: use this for reference only

Cellular standards: brief survey

2.5 G systems: voice and data channels

- for those who can't wait for 3G service: 2G extensions
- general packet radio service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
- enhanced data rates for global evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - data rates up to 384K
- CDMA-2000 (phase 1)
  - data rates up to 144K
  - evolved from IS-95

Cellular standards: brief survey

3G systems: voice/data

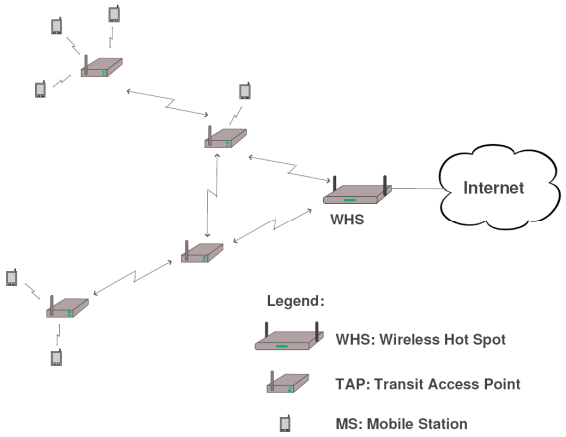
- Universal Mobile Telecommunications Service (UMTS)
  - data service: High Speed Uplink/Downlink packet Access (HSDPA/HSUPA): 3 Mbps
- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvlution Data Optimized (1xEVDO) up to 14 Mbps

Upcoming wireless networks

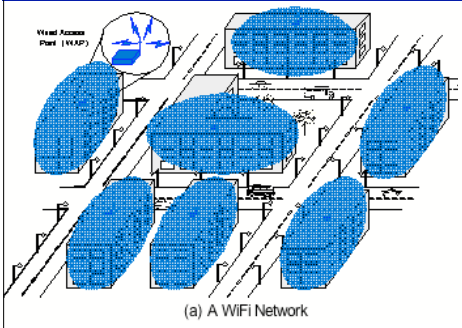
- Wireless mesh networks
- Hybrid ad hoc networks
- Mobile ad hoc networks
- Vehicular networks
- Sensor networks
- RFID

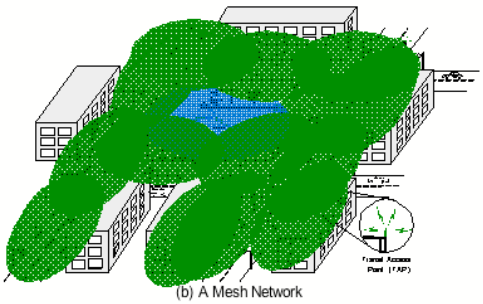
Wireless mesh networks

- Mesh network:
  - One Wireless Hot Spot (WHS)
  - Several Transit Access Points (TAPs)
  - Mobile Stations



Wireless Mesh Networks


(a) A WiFi Network


(b) A Mesh Network

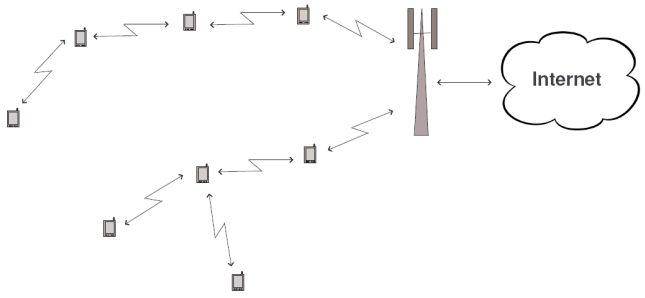
- Wireless Mesh Network (WMN): Same coverage as with WiFi networks but with only one WAP (and several TAPs).
- WMNs allow a fast, easy and inexpensive network deployment.
- However, the lack of security guarantees slows down the deployment of WMNs

Wireless mesh networks

- Easy to deploy:
  - Single connection point to the Internet
- Providing Internet connectivity in a sizable geographic area:
  - Much lower cost than classic WiFi networks
- Fairness and security are closely related
- Not yet ready for wide-scale deployment:
  - Severe capacity and delay constraints
  - Lack of security guarantees

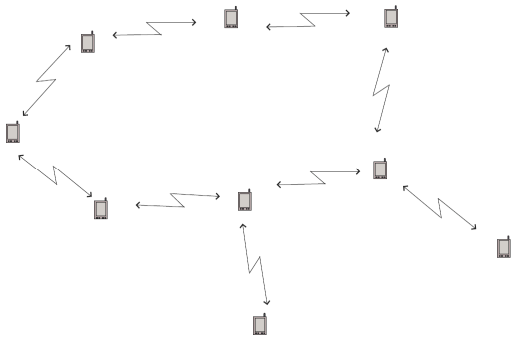
Hybrid ad hoc networks

- Hybrid ad hoc networks or multi-hop cellular networks:
  - No relay stations
  - Other mobile stations relay the traffic
- Problem of power management

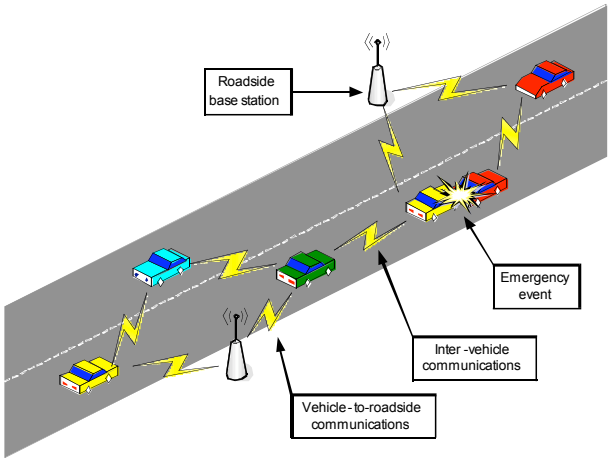


Mobile ad hoc networks

- Mobile ad hoc networks:
  - Mobile ad hoc networks in hostile environments
  - In self-organized mobile ad hoc networks



What is a VANET (Vehicular Ad hoc NETwork)?

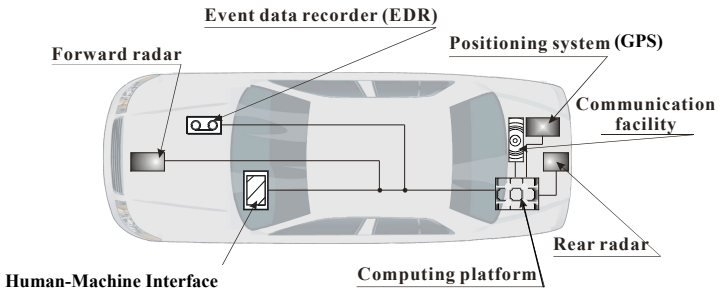


- Communication: typically over the Dedicated Short Range Communications (DSRC) (5.9 GHz)
- Example of protocol: IEEE 802.11p
- Penetration will be progressive (over 2 decades or so)

Vehicular communications: why?

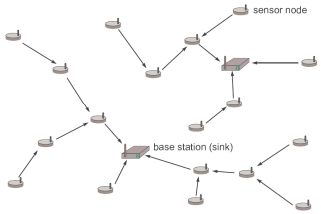
- Combat the awful side-effects of road traffic
  - In the EU, around 40'000 people die yearly on the roads; more than 1.5 millions are injured
  - Traffic jams generate a tremendous waste of time and of fuel
- Most of these problems can be solved by providing appropriate ***information*** to the driver or to the vehicle

A smart vehicle



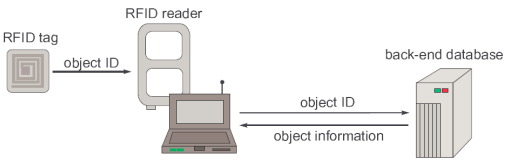
Sensor networks

- Large number of sensor nodes, a few base stations
- Sensors are usually battery powered:
  - Main design criteria: reduce the energy consumption
- Multi-hop communication reduces energy consumption:
  - Overall energy consumption can be reduced, if packets are sent in several smaller hops instead of one long hop
  - Fewer re-transmissions are needed due to collisions



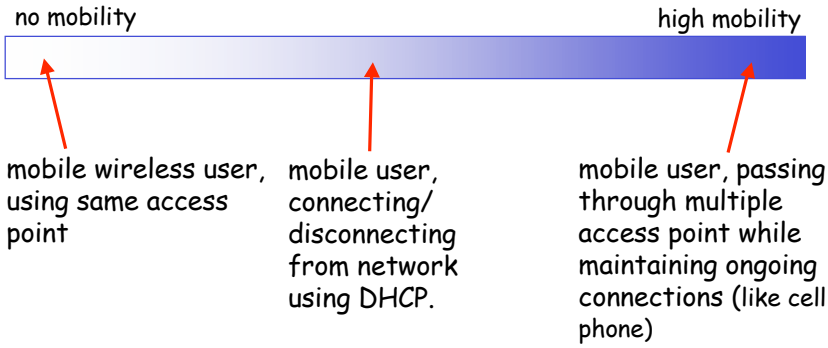
RFID

- RFID systems:
  - RFID tags
  - RFID readers
  - Back-end databases
- RFID tag: microchip and antenna
  - Active: have battery
  - Passive: harvest energy from the reader's signal

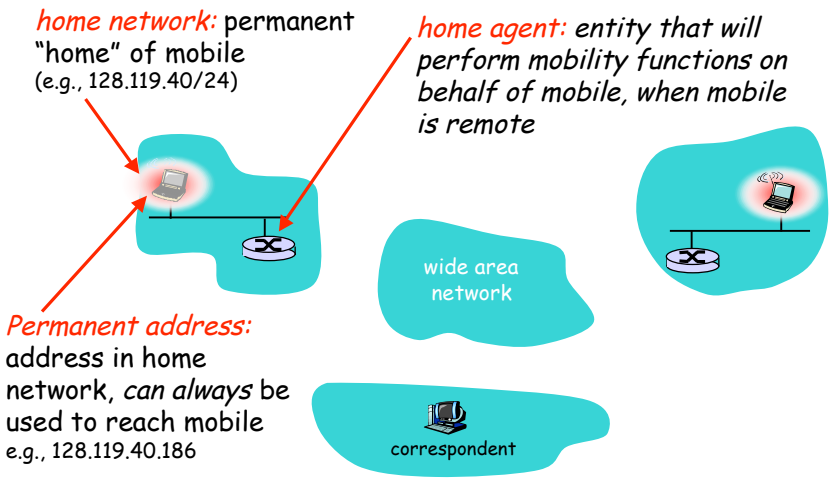


What is mobility?

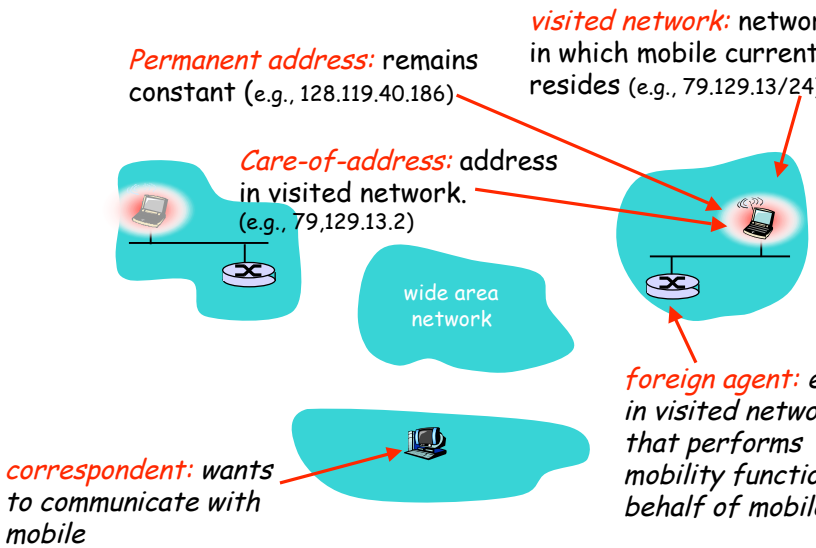
- spectrum of mobility, from the *network* perspective:



Mobility: Vocabulary



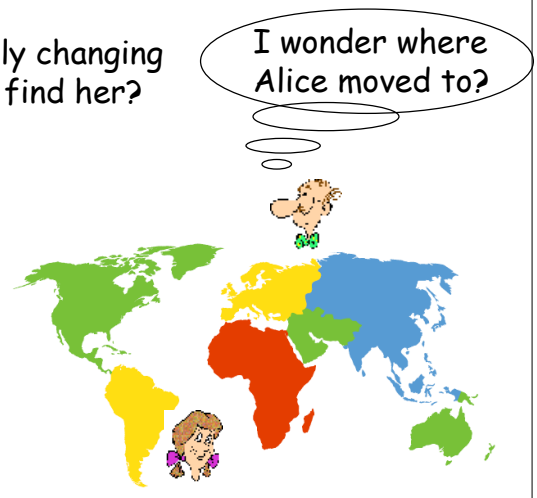
Mobility: more vocabulary



How do *you* contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents?
- expect her to let you know where he/she is?

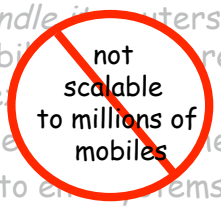


Mobility: approaches

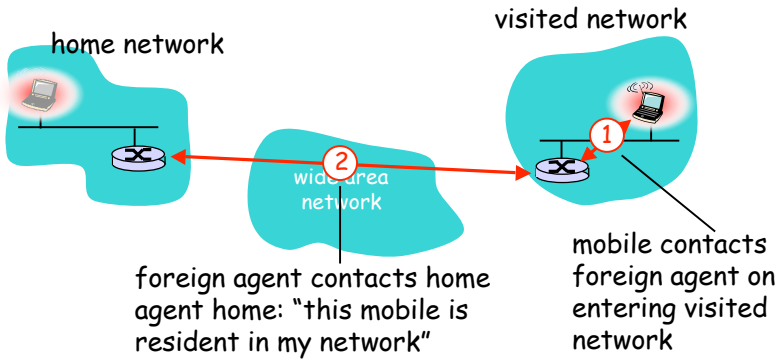
- *Let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *Let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: approaches

- *Let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile



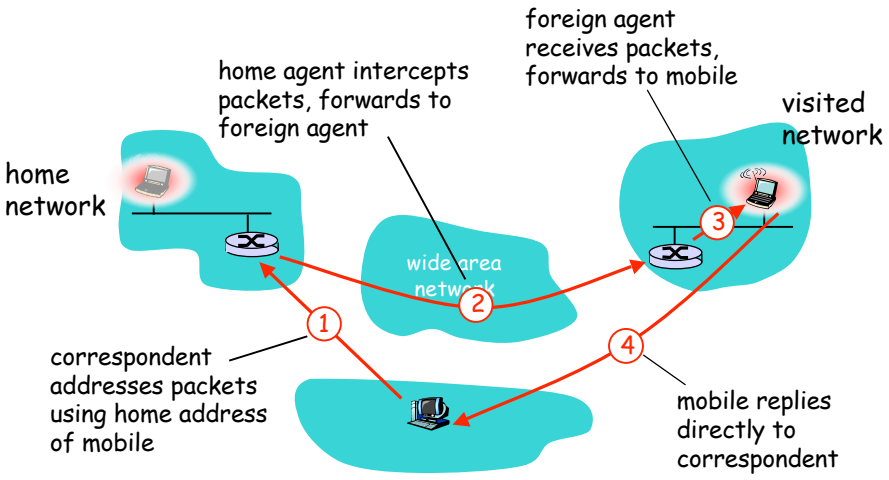
Mobility: registration



End result:

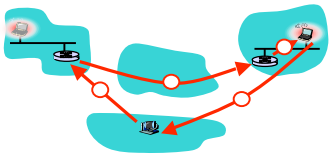
- Foreign agent knows about mobile
- Home agent knows location of mobile

Mobility via Indirect Routing



Indirect Routing: comments

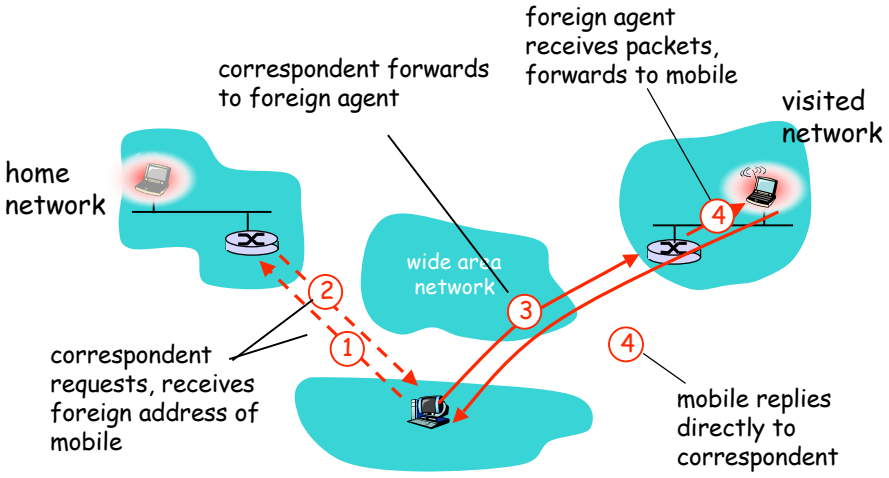
- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Indirect Routing: moving between networks

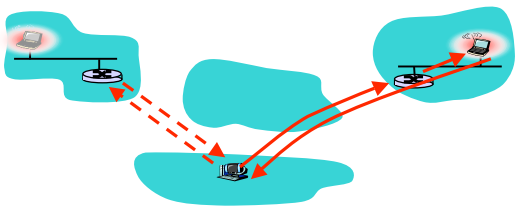
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

Mobility via Direct Routing



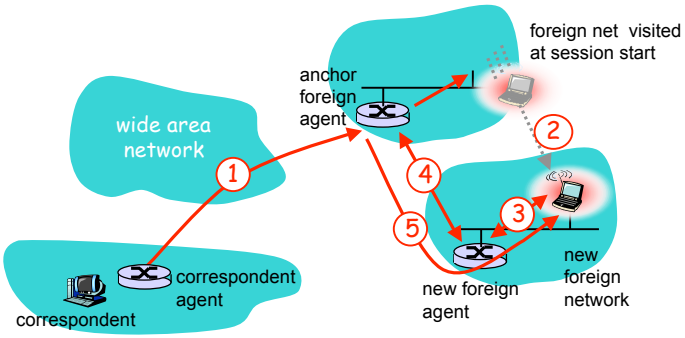
Mobility via Direct Routing: comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



Accommodating mobility with direct routing

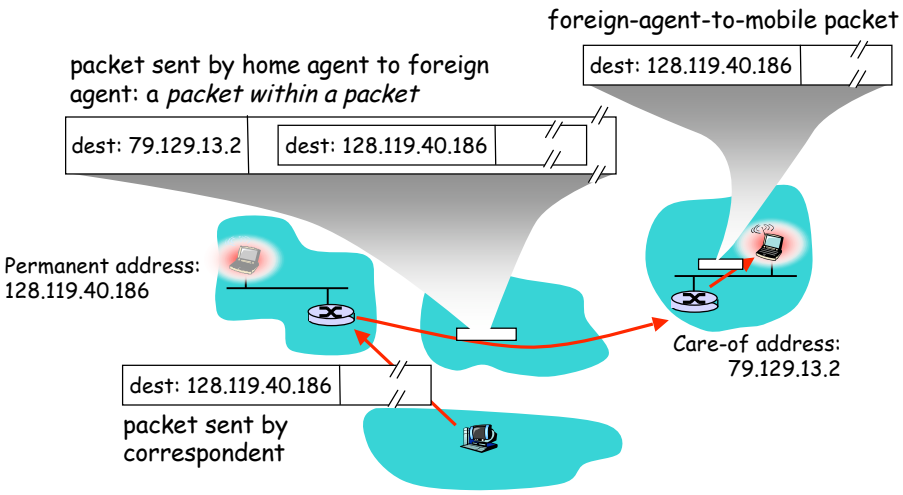
- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Mobile IP

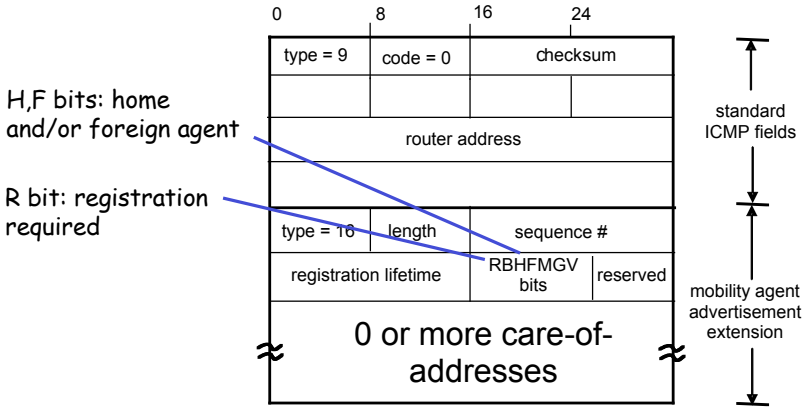
- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: indirect routing

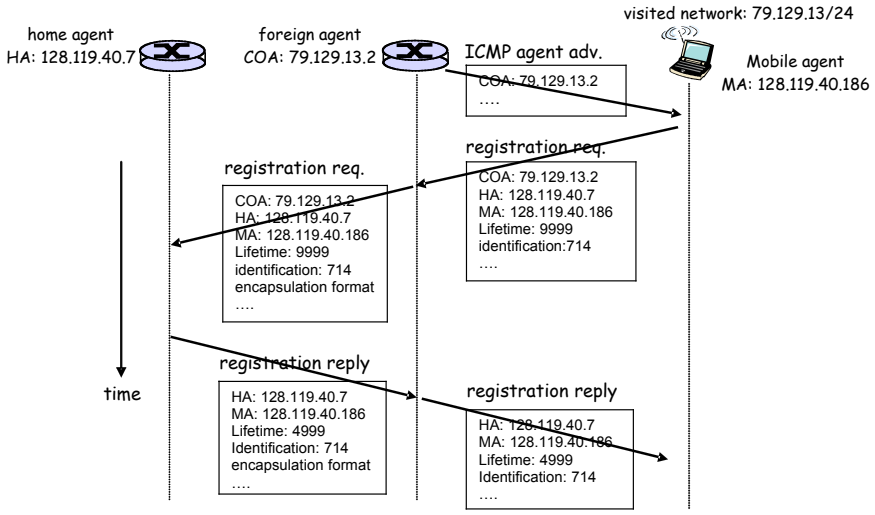


Mobile IP: agent discovery

- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

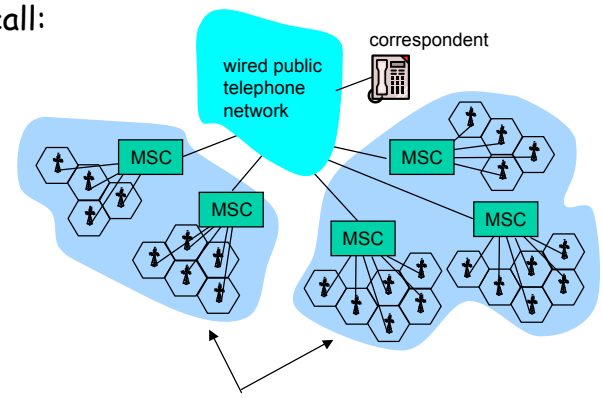


Mobile IP: registration example



Components of cellular network architecture

recall:

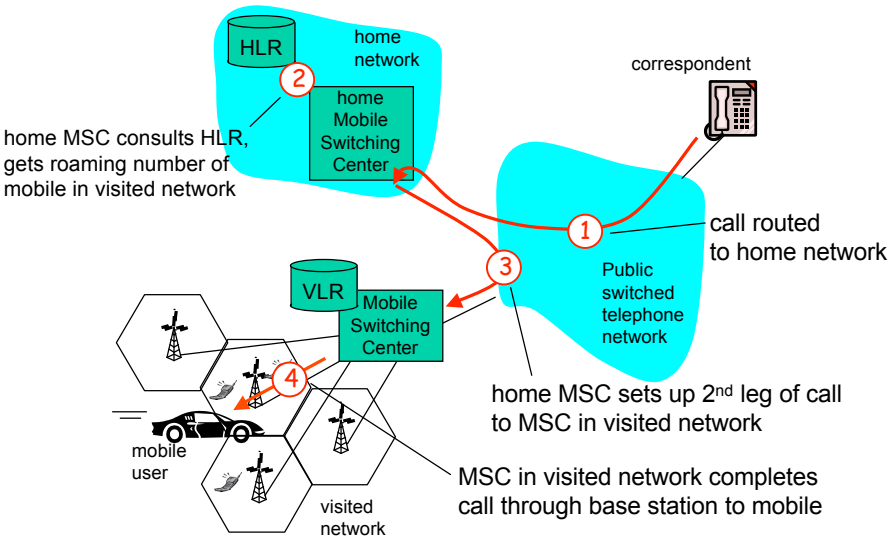


different cellular networks,
operated by different providers

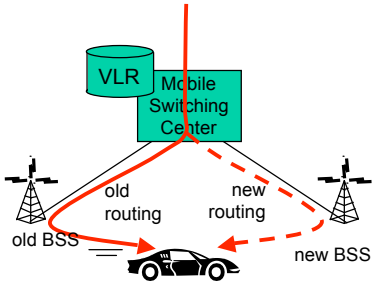
Handling mobility in cellular networks

- *home network:* network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- *visited network:* network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network
  - could be home network

GSM: indirect routing to mobile

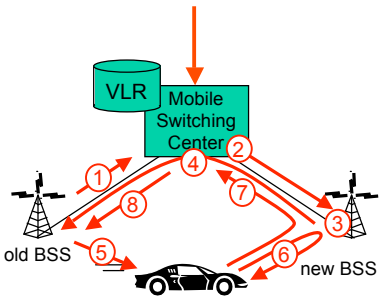


GSM: handoff with common MSC



- Handoff goal: route call via new base station (without interruption)
- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

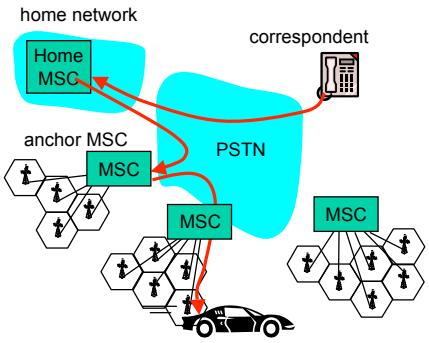
GSM: handoff with common MSC



1. old BSS informs MSC of impending handoff, provides list of 1+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

8 MSC-old-BSS resources released

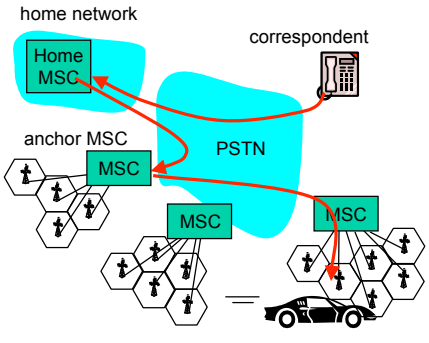
GSM: handoff between MSCs



(a) before handoff

- *anchor MSC:* first MSC visited during cal
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

GSM: handoff between MSCs



(b) after handoff

- *anchor MSC:* first MSC visited during cal
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

Mobility: GSM versus Mobile IP

GSM element	Comment on GSM element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	Home network
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	Home agent
Visited System	Network other than home system where mobile user is currently residing	Visited network
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	Foreign agent
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	Care-of-address

Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links

Why is security more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
- broadcast communications
  - wireless usually means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

- ➢ eavesdropping is easy
- ➢ injecting bogus messages into the network is easy
- ➢ replaying previously recorded messages is easy
- ➢ illegitimate access to the network and its services is easy
- ➢ denial of service is easily achieved by jamming

Wireless communication security requirements

- confidentiality
  - messages sent over wireless links must be encrypted
- authenticity
  - origin of messages received over wireless links must be verified
- replay detection
  - freshness of messages received over wireless links must be checked
- integrity
  - modifying messages on-the-fly (during radio transmission) is not so easy, but possible …
  - integrity of messages received over wireless links must be verified
- access control
  - access to the network services should be provided only to legitimate entities
  - access control should be permanent
    - it is not enough to check the legitimacy of an entity only when it joins the network and its logical associations are established, because logical associations can be hijacked
- protection against jamming

Class Logistics: a research seminar

Q: Is a seminar just like a course?

NO!

- I will lecture for the first 5-6 weeks
- Second half of the semester: student-presentations
  - 2 presentations per class
  - Each presentation based on 1-2 papers
  - student-led discussions
- no well-defined body of knowledge to impart
  - seminar is about searching for answers (and questions)
- great opportunity to find interesting research projects

Requirements

Workload:

- Reading assigned papers
- Write short reviews of papers to be discussed in class (20% of grade)
  - Email them to me before class.
  - Template for reviews is on class web site
- Participate in class discussions
- Make a class presentation (25%)
- Assist others in preparing their presentations (5%)
  - Each presenter will be assigned a partner who will go over the presentation with them
- Course project (50%)

Pre-requisites:

- previous class on networking (CS 555) and operating systems (CS 571)
- Background in security, cryptography helpful

Presentations

- after first six weeks:
  - *student-led* presentations and discussions
- *you* will need to:
  - read, think deeply about paper, topic area
  - look for additional outside material
  - prepare ~60 minute class presentation
  - Go over presentation with partner, instructor
  - lead in-class discussion of material
- everyone wants your presentation to be well-prepared, interesting, thoughtful

Presentations (more)

Preparing your presentation in advance:

- read documents about preparing a good talk (on web site)
- 1 week in advance: meet with presentation partner
  - Practice your talk!
- meet with instructor about presentation
- post overheads in advance of class

What's in a presentation?

- paper contents
- additional material you have found
- *critical analysis:* questions, strengths, weaknesses, improvements, future work
  - For every paper find:
    - 3 most important points
    - 3 weaknesses (flaws with the assumptions/methodology/etc.)

Class Project

- Various Options
  - Explore an open topic
    - Read literature, find open problem, propose a new solution, evaluate it
    - Could be the beginning of a MS/Ph.d. thesis
  - Re-evaluate/Validate the conclusions of a previous study
    - do experiments that have been reported in a paper
    - Measurement, Implementation, Simulation
  - Programming-oriented project
    - Implement a secure wireless application/service, e.g. using a platform such as TelosB "motes"
    - Identify project by end of Sept.
  - Discuss with instructor
  - Make a presentation in class (5-10 minutes)

Schedule

- First 5-6 weeks
  1. Course Intro (Week 1)
  2. Intro to Cryptographic Mechanisms (Week 1)
  3. Securing Existing Wireless Networks (Weeks 2)
  4. Challenges in Securing New Wireless Networks (Week 3)
  5. Thwarting Malicious Behavior
     1. Naming & Addressing
     2. Establishing Security Associations
     3. Securing Neighbor Discovery
     4. Secure Routing in Multi-hop Networks
     5. Privacy Protection
- Next 7 weeks – student presentations, guest lectures
  - See reading list on class web site (soon!)
- Last week + Finals week
  - Project Presentations

Readings

- Survey of Wireless Networks
  - Read Kurose, Ross Ch 6 (or any recently published networking textbook)
  - Buttyan, Hubaux Ch 1, 2