18-452/18-750
Wireless Networks and Applications
Lecture 13: Wireless and the Internet

Peter Steenkiste

Spring Semester 2018

http://www.cs.cmu.edu/~prs/wirelessS18/

Outline

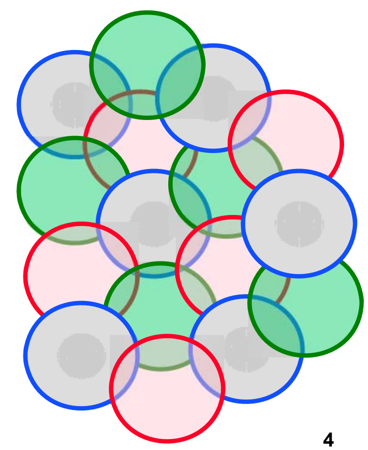
- WiFi deployments
  - » Planning
  - » Channel selection
  - » Rate adaptation
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

Outline

- WiFi deployments
  - » Planning
  - » Channel selection
  - » Rate adaptation

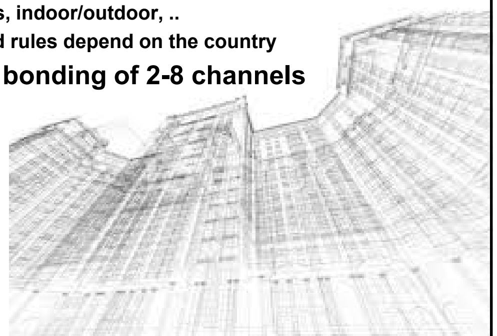
Infrastructure Deployments Frequency Reuse in Space

- Set of cooperating cells with a base stations must cover a large area
- Cells that reuse frequencies should be as distant as possible to minimize interference and maximize capacity
  - » Hidden and exposed terminals are also a concern



Frequencies are Precious

- 2.4 Ghz: 3 non-overlapping channels
  - » Plus lots of competition: microwaves and other devices
- 5 GHz: 20+ channels, but with constraints
  - » Power constraints, indoor/outdoor, ..
  - » Exact number and rules depend on the country
- 802.11n and ac: bonding of 2-8 channels
- And the world is not flat!

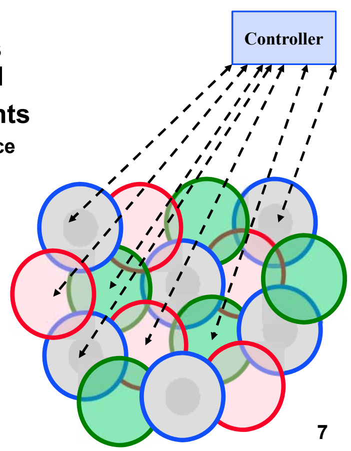


Frequency Planning

- Campus-style WiFi deployments are very carefully planned:
- A lot of measurements to determine where to place the AP
  - » What is the coverage area?
  - » What set of APs has good coverage with few “dead spots”
  - » What level of interference can we expect between cells
  - » What traffic loads can we expect, e.g., auditorium vs office
- Frequencies are very carefully assigned
  - » Can use the above measurements
- Must periodically re-evaluate infrastructure
  - » Furniture is moved, remodeling, …

Centralized Control

- Many WiFi deployments have centralized control
- APs report measurements
  - » Signal strengths, interference from other cells, load, …
- Controller makes adjustments
  - » Changes frequency bands
  - » Adjusts power
  - » Redistributes load
  - » Can switch APs on/off
  - » Very sophisticated!



Monitoring the Spectrum

- FCC (in the US) controls spectrum use
  - » Rules for unlicensed spectrum, licenses for other spectrum, what technologies can be used
- … but there is an special clause for campuses
  - » They have significant control over unlicensed spectrum use on the campus
  - » They can even use some “licensed” spectrum if it does not interfere with the license holder
- Network management carefully monitors spectrum use to make sure it is used well
  - » Shut down rogue APs – interference, security
  - » Non-approved equipment - interference
  - » Discourages outdated standards - inefficient

How about Small Networks?

- Most WiFi networks are small and (largely) unmanaged
  - » Home networks, hotspots, …
- Traditional solution: user-chosen frequency of their AP or a factory set default
  - » How well does that work?
- Today, APs pick a channel automatically in a smart way
  - » Monitors how busy channels are or how strong the signals are and then picks the best channel
  - » Can periodically check for better channels

Outline

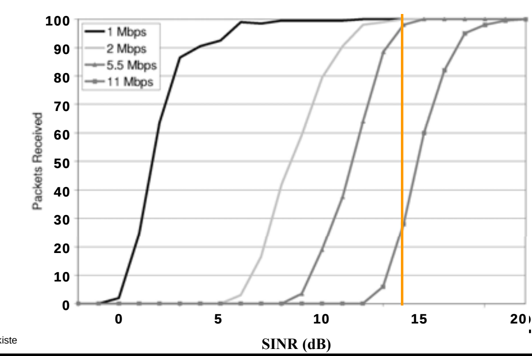
- WiFi deployments and channel selection
- Rate adaptation
  - » Background
  - » RRAA
  - » Charm

Bit Rate Adaptation

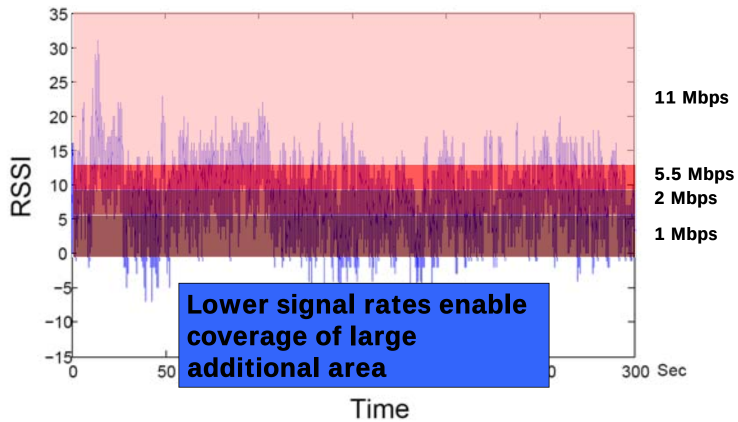
- All modern WiFi standards are multi bit rate
  - » 802.11b has 4 rates, more recent standards have 10s
  - » Vendors can have custom rates!
- Many factors influence packet delivery:
  - » Fast and slow fading: nature depends strongly on the environment, e.g., vehicular versus walking
  - » Interference versus WiFi contention: response to collisions is different
  - » Random packet losses: can confuse “smart” algorithms
  - » Hidden terminals: decreasing the rate increases the chance of collisions
- Transmit rate adaptation: how does the sender pick?

Transmit Rate Selection

- Goal: pick rate that provides best throughput
  - » E.g. SINR 14 dB → 5.5 Mbps
  - » Needs to be adaptive

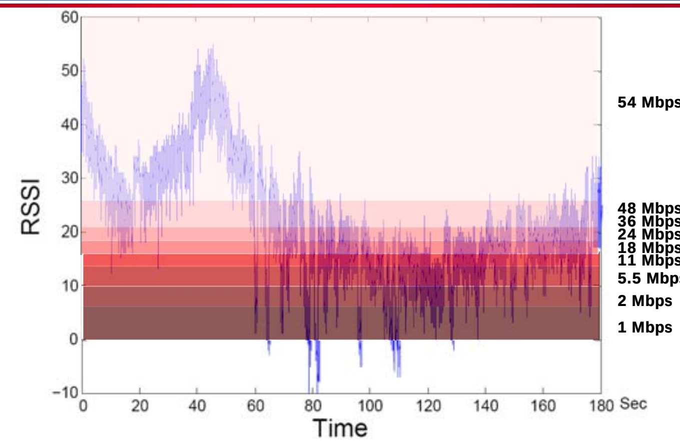


"Static" Channel



Lower signal rates enable coverage of large additional area

Mobile Channel – Pedestrian



High Level Designs

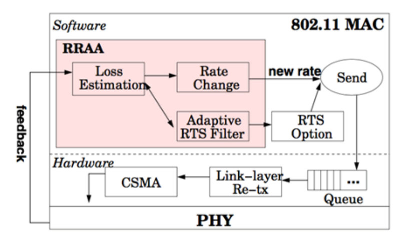
- "Trial and Error": senders use past packet success or failures to adjust transmit rate
  - » Sequence of x successes: increase rate
  - » Sequence of y failures: reduce rate
  - » Hard to get x and y right
  - » Random losses can confuse the algorithm
- Signal strength: stations use channel state information to pick transmit rate
  - » Use path loss information to calculate "best" rate
  - » Assumes a relationship between PDR and SNR
    - – Need to recover if this fails, e.g., hidden terminals
- Newest class: context sensitive solutions
  - » Adjust algorithm depending on, e.g., degree of mobility, ..

Robust Rate Adaptation Algorithm

- RRAA goals
  - » Maintain a stable rate in the presence of random loss
  - » Responsive to drastic channel changes, e.g., caused by mobility or interference
- Adapt rate based on short term PDR

$$R_{new} = \begin{cases} R^{+} & P > P_{MTL} \\ R_{-} & P < P_{ORT} \end{cases}$$

  - » Thresholds and averaging windows depend on rate
- Selectively enable RTS-CTS



CHARM

- Channel-aware rate selection algorithm
- Transmitter passively determines SINR at receiver by leveraging channel reciprocity
  - » Determines SINR without the overhead of active probing (RTS/CTS)
- Select best transmission rate using rate table
  - » Table is updated (slowly) based on history
  - » Needed to accommodate diversity in hardware and special conditions, e.g., hidden terminals
- Jointly considers problem of transmit antenna selection

SINR: Noise and Interference

$$\text{SINR} = \frac{\text{RSS}}{\text{Noise} + \sum \text{Interference}}$$

- Noise
  - » Thermal background radiation
  - » Device inherent
    - – Dominated by low noise amplifier noise figure
  - » ~Constant
- Interference
  - » Mitigated by CSMA/CA
  - » Reported as "noise" by NIC

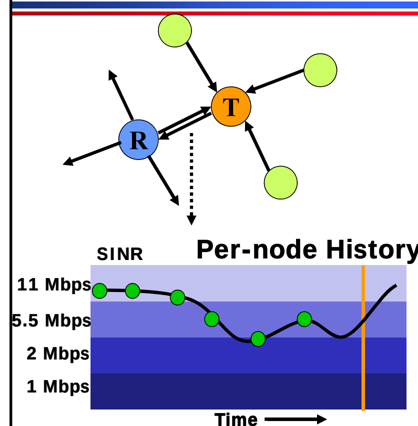
SINR: RSS

$$RSS = P_{tx} + G_{tx} - PL + G_{rx} \qquad (1)$$

$$PL = P_{tx} + G_{tx} + G_{rx} - RSS \qquad (2)$$

- By the reciprocity theorem, at a given instant of time
  - » $PL_{A \rightarrow B} = PL_{B \rightarrow A}$
- A overhears packets from B and records RSS (1)
- Node B records P_{tx} and card-reported noise level in beacons and probes, so A has access to them
- A can then calculate path-loss (2) and estimate RSS and SINR at B

CHARM: Channel-aware Rate Selection



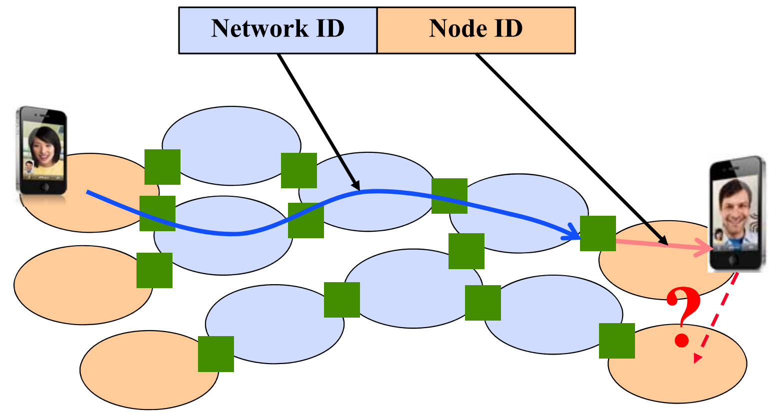
- Leverage reciprocity to obtain path loss
  - » Compute path loss for each host: P_{tx} - RSSI
- On transmit:
  - » Predict path loss based on history
  - » Select rate & antenna
  - » Update rate thresholds

IP Address Structure

Network ID	Node ID

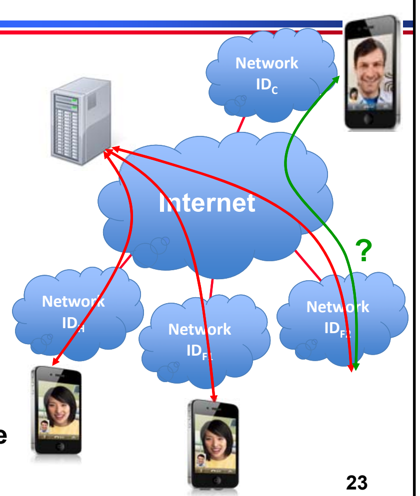
- Network ID identifies the network
  - » CMU = 128.2
- Node ID identifies node within a network
  - » Node IDs can be reused in different networks
  - » Can be assigned independently by local administrator
- Size of Network and Node IDs are variable
  - » Originally Network IDs came in three sizes only
  - » Variable sized Network IDs are often called a prefix
- Great, but what does this have to do with mobility?

Routing and Forwarding in the Internet



Mobility Challenges

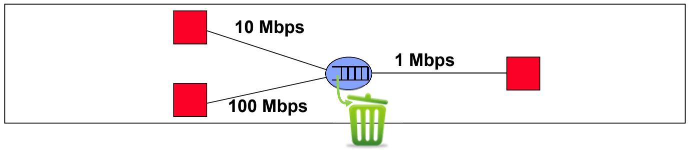
- When a host moves to a new network, it gets a new IP address
- How do other hosts connect to it?
  - » Assume you provide services
  - » They have old IP address
- How do peers know you are the same host?
  - » IP address identifies host
  - » Associated with the socket of any active sessions
- What assumption is made here?



Main TCP Functions

- Connection management
  - » Maintain state at endpoints to optimize protocol
- Flow control: avoid that sender outruns the receiver
  - » Uses sliding window protocol
- Error control: detect and recover from errors
  - » Lost, corrupted, and out of order packets
- Congestion control: avoid that senders flood the network
  - » Leads to inefficiency and possibly network collapse
  - » Very hard problem – was not part of original TCP spec!
  - » Solution is sophisticated (and complex)

TCP Congestion Control



- Congestion control avoids that the network is overloaded
  - » Must slow down senders to match available bandwidth
  - » Routers that have a full queue drop packets – inefficient!
- How does sender know the network is overloaded?
- It looks for dropped packets as a sign of congestion
- What assumption is made here?

Wireless and the Internet Challenges

- IP addresses are used both to forward packets to a host and to identify the host
  - » Active session break when a host moves
  - » Mobile hosts are hard to find
- TCP congestion control interprets packet losses as a sign of congestion
  - » Assumes links are reliable, so packet loss = full queue
  - » Not true for wireless links!
- Applications generally assume that they are continuously connected to the Internet
  - » Can access servers, social networks, …
  - » Mobile apps must support "disconnected" operations

Outline

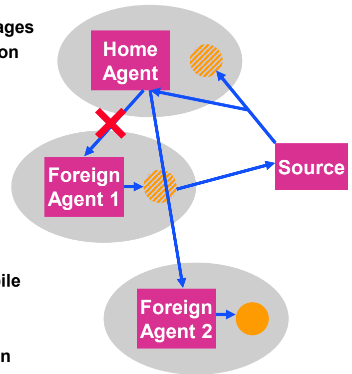
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

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
- 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 Operation

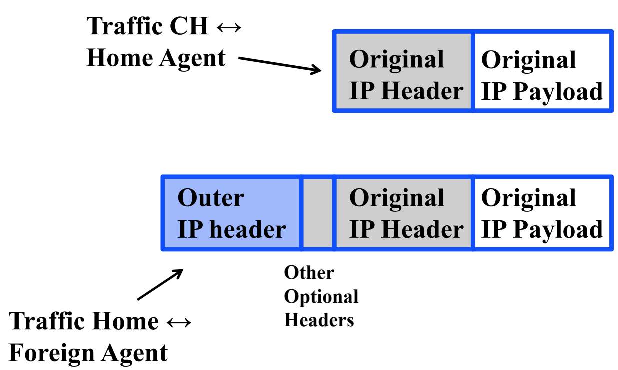
- Agents advertise their presence.
  - Using ICMP or mobile IP control messages
  - Mobile host can solicit agent information
  - Mobile host can determine where it is
- Registration process: mobile host registers with home and foreign agent.
  - Set up binding valid for *registration lifetime*
- Tunneling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



Mobile IP

- 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.
  - binding = (IP address, foreign agent address)
  - binding includes time stamp

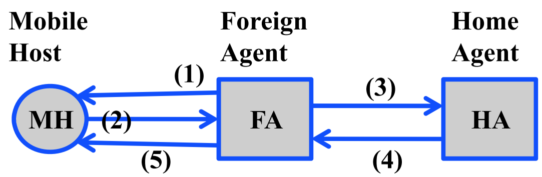
Tunneling IP-in-IP Encapsulation



Optimizations

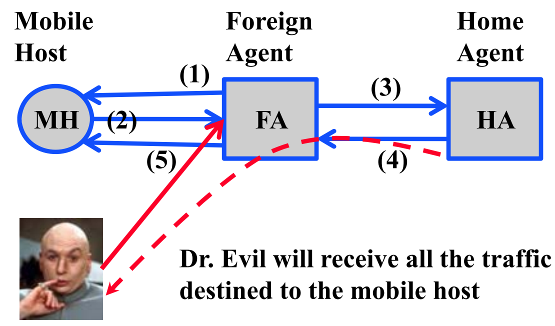
- Mobile host can be its own the foreign agent.
  - Mobile host acquires local IP address
  - performs tasks of the mobile agent
- Short circuit the home location by going directly to the foreign agent.
  - Routers in the network store cache bindings and intercept and tunnel packets before they the mobile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

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

Authentication



Mobile IP Authentication

- Without security, a “bad guy” 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)

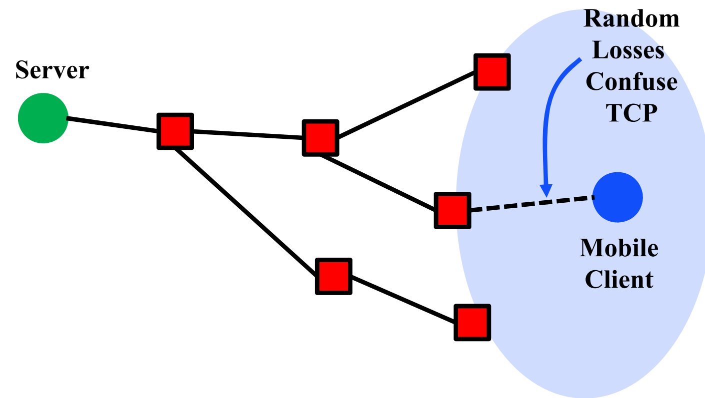
Discussion

- 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 is rare 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

Outline

- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

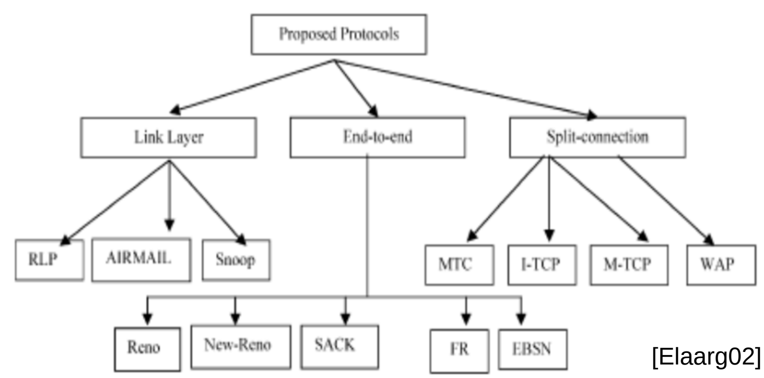
Solution Ideas?



Solution Space

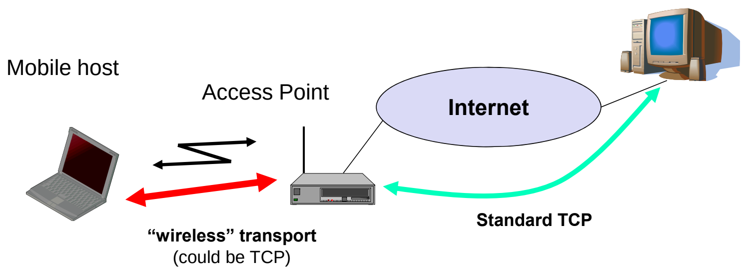
- Modify TCP for wireless paths
  - » Would maintain status quo for wired paths
  - » What would wireless TCP look like?
  - » Difficult to do: there are many Internet hosts
  - » Traditionally, hosts have no information about path properties
- Modify TCP for all paths
  - » Not clear what that modification would be!
  - » Similar problems: need to modify many hosts
- Modify TCP only on the mobile host
  - » A more practical idea – but what would the change be?
- Keep end hosts the same but tweak things at the wireless gateway
  - » Keep end-end TCP happy despite wireless links

Possible Classification of Solutions



[Elaarg02]

I-TCP



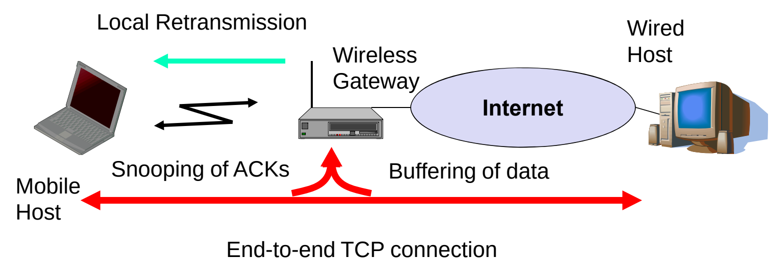
Connection Split: Indirect TCP or I-TCP

- Do not change TCP on the wire-line part
- Split the TCP connection at the wireless gateway into two parts
  - » One optimized for the wireless link
  - » The second for the wire-line communication (TCP)
- No real transport-layer end-to-end connection
  - » Although host on wired network does not know this
- Wired host should not notice the characteristics of the wireless part
  - » This is a challenge since wireless gateway is limited in what it can send and when, e.g. cannot prematurely acknowledge data
  - » Certain things cannot be hidden: delay, dramatic throughput variations

I-TCP Discussion

- I-TCP Advantages
  - » No changes in the fixed network or hosts (TCP protocol), so all current TCP optimizations still work
  - » Wireless transmission errors do not "propagate" to the wire-line network
  - » Simple, effective (in the best case)
- I-TCP Disadvantages
  - » End-to-end semantics become less clear, e.g. what happens if the wireless gateway crashes?
  - » Higher end-to-end delays due to buffering and forwarding to the gateway

Snooping TCP



Snooping TCP

- "Transparent" extension of TCP within the wireless gateway
  - » End hosts are not modified
- Hides wireless losses from wired host
  - » Buffer packets sent to the mobile host
  - » Local retransmission: Lost packets on the wireless link, for both directions, are retransmitted immediately by the mobile host or foreign agent
- Wireless gateway "snoops" the packet flow so it can cover up signs of packet loss
  - » E.g. recognizes acknowledgements in both directions and suppresses duplicate ACKs

Snooping TCP Discussion

- Data transfer to the mobile host
  - » FA buffers data until it receives ACK from the MH
  - » FA detects packet loss via duplicated ACKs or time-out
- Data transfer from the mobile host
  - » FA detects packet loss on the wireless link via sequence numbers
  - » FA answers directly with a NACK to the MH
  - » MH can now retransmit data with only a very short delay
- Integration of the MAC layer
  - » MAC layer often has similar mechanisms to those of TCP
- Problems
  - » Snooping TCP does not isolate the wireless (as I-TCP)
  - » Snooping might be useless if encryption is used

An Internet Style Approach

- Use aggressive retransmission in the wireless network to hide retransmission losses
  - » Most deployed wireless network in fact do that already
  - » Would sell few products if they did not
- Wireless losses translate into increased delay
  - » But TCP roundtrip time estimation is very conservative, e.g. increases if variance is high
- Also: persistent high loss rate results in reduced available bandwidth → congestion response is appropriate and needed
- Works remarkably well!
- Other solutions only needed for "challenged" networks