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

Peter Steenkiste

Spring Semester 2020

http://www.cs.cmu.edu/~prs/wirelessF20/

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

Rate Adaptation

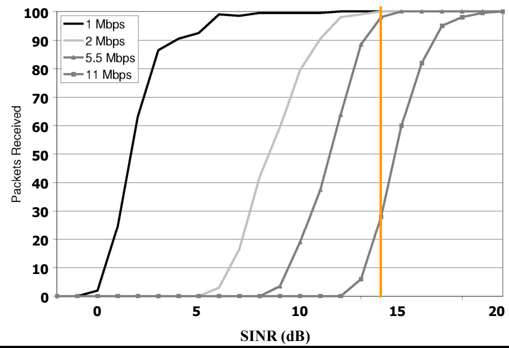
- WiFi supports multiple bit rates but does not standardize bit rate selection
- Outline
  - » Background
  - » RRAA
  - » Charm
  - » MIMO discussion

Bit Rate Adaptation

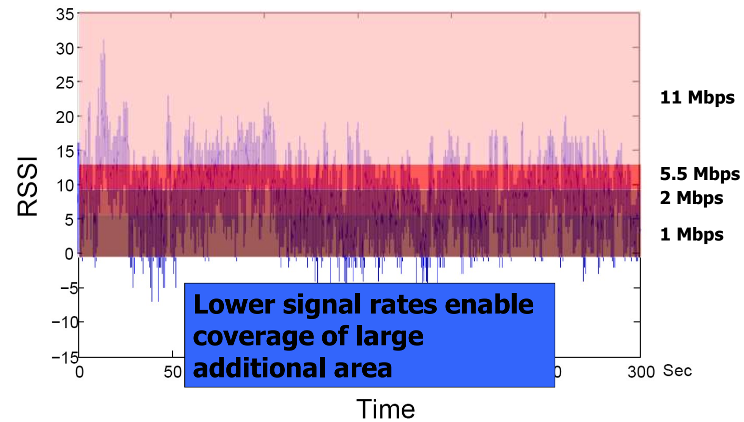
- All modern WiFi standards are multi bit rate
  - » 802.11b has 4 rates, more recent standards have 10s
  - » Vendors can have custom rates!
- Many factors influence packet delivery:
  - » Fast and slow fading: nature depends strongly on the environment, e.g., vehicular versus walking
  - » Interference 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

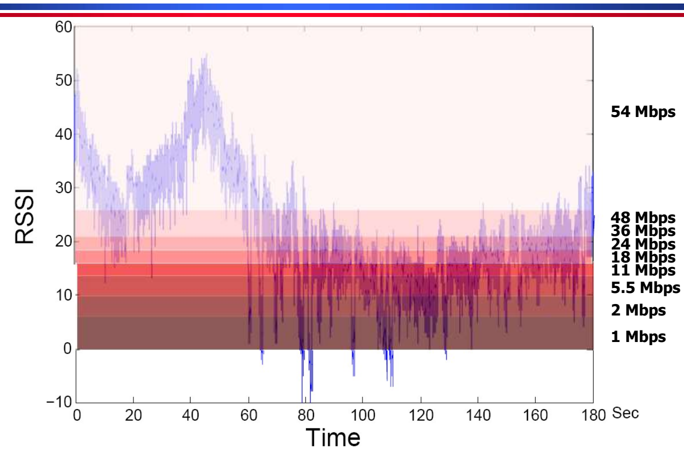
- Goal: pick rate that provides best throughput
  - » E.g. SINR 14 dB → 5.5 Mbps
  - » Needs to be adaptive



"Static" Channel



Mobile Channel – Pedestrian



High Level Designs

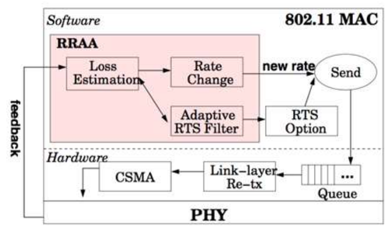
- "Trial and Error": senders use past packet success or failures to adjust transmit rate
  - » Sequence of x successes: increase rate
  - » Sequence of y failures: reduce rate
  - » Hard to get x and y right
  - » Random losses can confuse the algorithm
- Signal strength: stations use channel state information 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

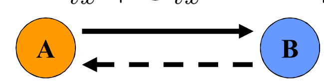
SINR: Noise and Interference

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

- 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

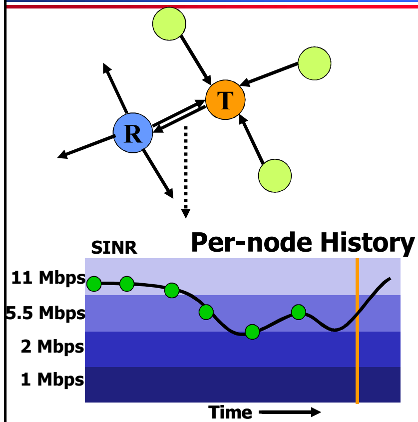
$$RSS = P_{tx} + G_{tx} - PL + G_{rx} \quad (1)$$



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

- 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
- Today's algorithms use CSI but are much more sophisticated
  - » E.g., have to deal with more many more rates, MIMO, etc.

Outline

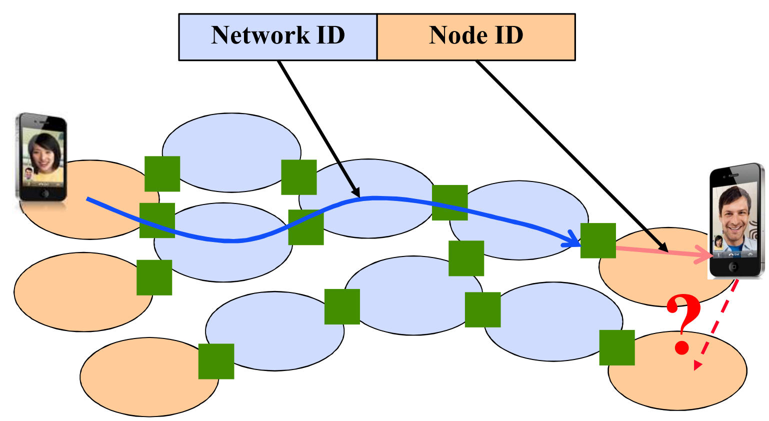
- WiFi deployments
  - » Planning
  - » Channel selection
  - » Rate adaptation
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

IP Address Structure

Network ID	Node ID

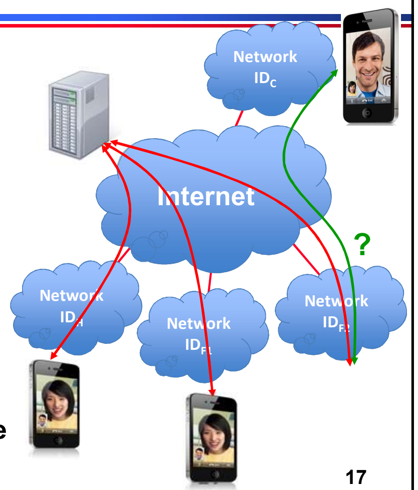
- Network ID identifies the network
  - » CMU = 128.2
- Node ID identifies node within a network
  - » Node IDs can be reused in different networks
  - » Can be assigned independently by local administrator
- Size of Network and Node IDs are variable
  - » Originally Network IDs came in three sizes only
  - » 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

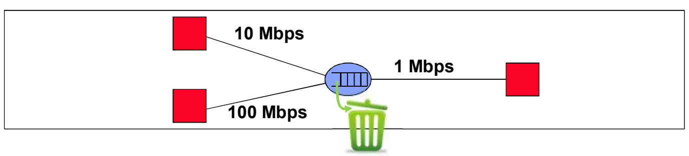
- When a host moves to a new network, it gets a new IP address
- How do other hosts connect to it?
  - » Assume you provide services
  - » They have old IP address
- How do peers know you are the same host?
  - » IP address identifies host
  - » Associated with the socket of any active sessions
- What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

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
  - » The two access points coordinate to reduce latency, packet loss
- Problem is with inter-network mobility, i.e. Changing IP addresses
  - » Want host to always have the same IP address

Network Mobility: Two Simple Solutions

- Routing: mobile nodes keep "home" IP address and advertise route to mobile address as /32 in BGP
  - » Leverages LPM semantics - should work!!
  - » Bad idea: scalability
- DNS: mobile nodes get "local" IP address and update name-address binding in DNS
  - » DNS allows updates of the address – should work!!
  - » Bad idea: results in a lot of write traffic to DNS
  - » DNS is not designed for this and reduces caching benefit

More Practical Way to Support Mobility

- Host gets new IP address in new "foreign" network
  - » Simple: use Dynamic Host Configuration (DHCP)
  - » No impact on Internet routing
- Raises two challenges:
  1. Maintaining a TCP connection while mobile: Transport connections are tied to src/dest IP addresses → What happens to active connections when a host moves?
  2. Finding the host: Host does not have constant address → how do other devices contact the host?

How to Handle Transport Connections for Mobile Nodes?

- Hosts use a 4 tuple to identify a TCP connection
  - » <Src Addr, Src port, Dst addr, Dst port>
  - » Change your IP address breaks the connection – hard to fix
- Best approach: add a level of indirection using two IP addresses
  - » A "identifier" IP address that identifies the connection on end-points
  - » A "locator" IP address that is used in the packets and can change
  - » Host does a mapping
- Security issue: Can someone easily hijack connection?
- Difficult to deploy → both ends must support mobility
- Even better approach: keep the same IP address!

Finding Mobile Hosts: Mobile IP

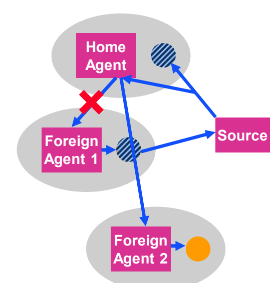
- Communicate with mobile hosts using their "home" IP address
  - » Target is "nomadic" devices: do not move while communicating, i.e., laptop, not cellphone
  - » Allows any host to contact mobile host using its "usual" IP address, as if it where in its "normal" location
- Mobility should be transparent 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

Finding Mobile Hosts: Mobile IP

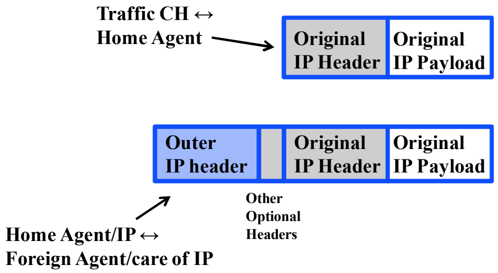
- Any host can contact mobile host using its usual "home" IP address
  - » Target is "nomadic" devices: do not move while communicating, i.e., laptop
- Home network has a home agent that is responsible for intercepting packets and forwarding them to the mobile host.
  - » E.g., router at the edge of the home network
  - » Forwarding is done using tunneling
- Remote network has a foreign agent that manages communication with mobile host.
  - » Module that runs on mobile and the point of contact for the mobile host
- Binding ties home IP address of mobile host to a "care of" address in the foreign network.
  - » binding = (home IP address, foreign IP addess)

Mobile IP Operation

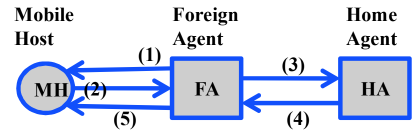
- Registration process: mobile host registers with home agent.
  - » Home agents needs to know that it should intercept packet and forward them
- In foreign network, foreign agent gets local "care of" address and notifies home agent
  - » Home agent knows where to forward packets
- Tunneling
  - » Home agent forward packets to foreign agent
  - » Return packets are tunneled in the reverse direction
- Supporting mobility
  - » Update binding in home and foreign agents.



Tunneling
IP-in-IP Encapsulation

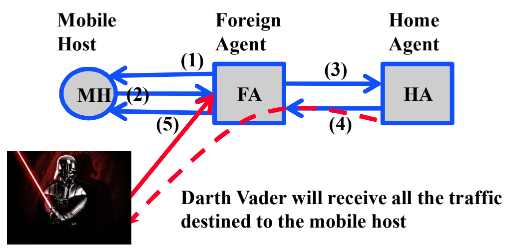


Registration via Foreign Agent



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

Authentication



Solution: Registration messages between a mobile host and its home agent must be authenticated

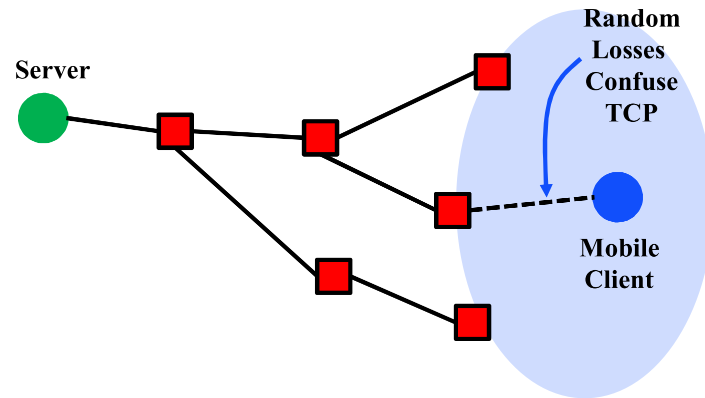
Mobility Discussion

- Obvious optimization: mobile host send return packet directly to communicating host – not through home agent
  - » Problem: may look like spoofed traffic to the foreign network
- Mobile IP not used in practice
- Mobile devices are typically clients, not servers, i.e., they initiate connections
  - » The problem Mobile IP solves rare in practice
- Mobile IP is not designed for truly mobile users
  - » Designed for nomadic users, e.g. visitors to a remote site
- IETF defined several solutions that are more efficient
  - » Also more heavy weight: creates overlay with tunnels and special "routers"
- 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

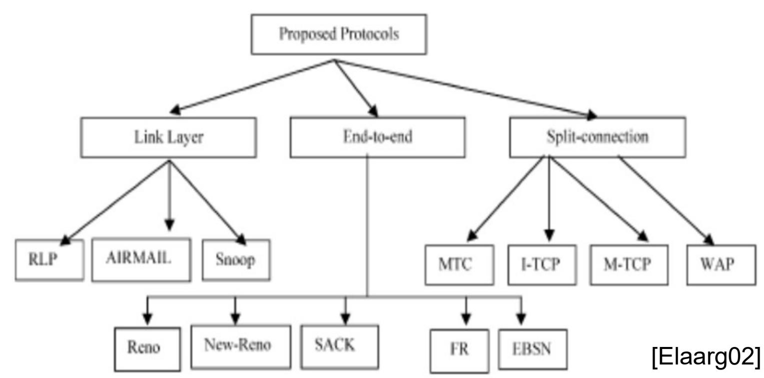
Solution Ideas?



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]

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

Outline

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

Disconnected Operation

- Mobility means that devices will occasionally be disconnected from the network
  - » Seconds ... Minutes … Hours .. Days
  - » Mostly an issue for clients
- This can confuse systems and applications that assume a wired/stationary model
  - » Clients cannot access servers, e.g., mail, calendar applications, …
  - » Distributed file systems
  - » Systems for back up or systems management
- Must adapt the applications and systems to make them "disconnection aware"

Two Examples

- E-mail: users must be able to "work on" e-mail offline and operations are performed when the mobile client is redirected
  - » Compose, read and delete e-mail
  - » Possibly others: manage folders, etc.
- Calendars and tasks are similar: operations performed offline must be executed later
  - » Adding or removing appointment and tasks, …
- Must sometimes resolve conflicts when multiple clients are used offline
  - » E.g., mail is deleted on one client and moved to another folder on another – delete or keep?
  - » Tend to be minor – ask user for help if needed

More Complex Case: File System

- A distributed file system can be accessed from many computers
  - » Files tend to be cached in the computers
- Creates opportunities for inconsistencies
  - » E.g., a file is modified on two different computers – how do you merge the changes? Who is responsible?
- The consistency model depends on the file system
  - » Stronger consistency requires that the system can keep track of all copies and remove/lock them if needed
- Disconnected operation makes the consistency problem harder!
  - » Some file copies my be inaccessible for long periods!

Mobility is Common Today

- Many applications are designed to work on mobile clients so they deal properly with disconnections
  - » Many apps on mobile devices are designed for mobility
  - » Most clients server applications can work offline with at least partial functionality
- Does not work for interactive applications
  - » Games, etc.
- Disconnection can still be very inconvenient
  - » Need state that is not cached on your client device
  - » Things like back ups cannot be performed
  - » Unpredictable delays in communication

Outline

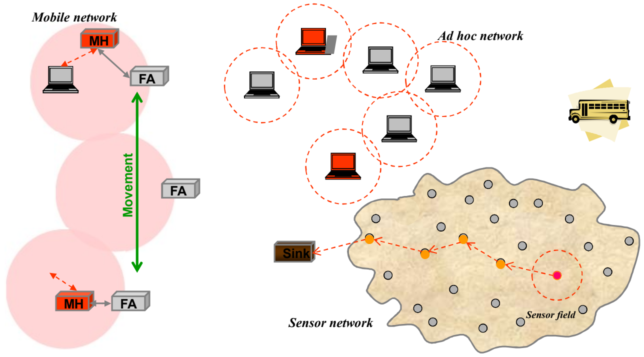
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

Based on slides by Kevin Fall

Challenged Networks

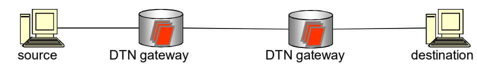
- Violate one or more of Internet's assumptions
  - » End-points may rarely/never be online at the same time
  - » Very long delay path, frequent disconnections, …
  - » Have naming semantics for their particular application domain
  - » Not be well served by the current end-to-end TCP/IP
- Examples
  - » Terrestrial mobile networks
  - » Some ad-hoc networks
  - » Sensor/actuator networks
- Goals for "disruption tolerant" networks
  - » Achieve interoperability between very diverse types networks
  - » Sometimes also called disruption tolerant

Background



High-level Architecture

- Characteristics:
  - » Operate as an overlay above the existing transport layers
  - » Based on an abstraction of message switching
    - – Bundle
    - – Bundle forwarder (DTN gateway)
    - – Store-and-forward gateway function between different networks



- Constituent of DTN architecture
  - » Region: internally homogenous, i.e. same network stack, addressing, …
  - » DTN gateway: Interconnection point between region boundaries
  - » Name Tuple: {Region name, Entity name}

Example DTN