18-452/18-750
Wireless Networks and Applications
Lecture 15: Wireless and the Internet

Peter Steenkiste

Fall Semester 2018

http://www.cs.cmu.edu/~prs/wirelessF18/

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

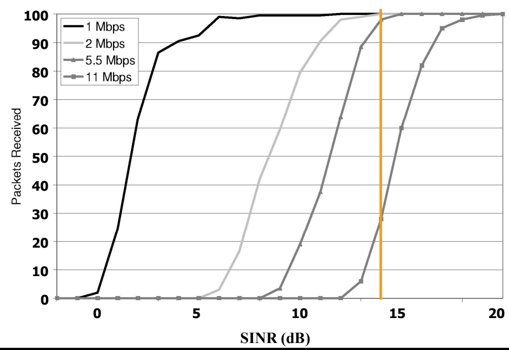
- WiFi supports multiple bit rates but does not standardize bit rate selection
- Outline
  - Background
  - RRAA
  - Charm
  - MIMO discussion

Bit Rate Adaptation

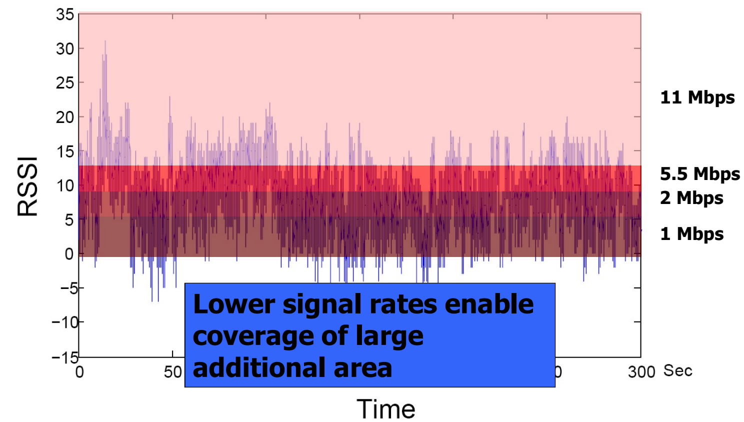
- All modern WiFi standards are multi bit rate
  - 802.11b has 4 rates, more recent standards have 10s
  - Vendors can have custom rates!
- Many factors influence packet delivery:
  - Fast and slow fading: nature depends strongly on the environment, e.g., vehicular versus walking
  - Interference versus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

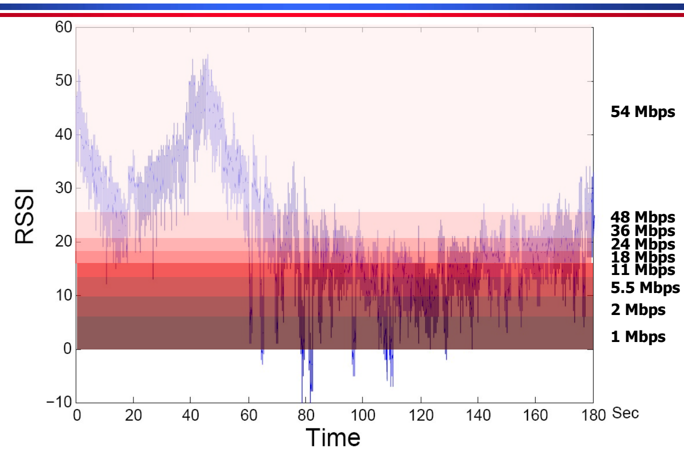
- Goal: pick rate that provides best throughput
  - » E.g. SINR 14 dB → 5.5 Mbps
  - » Needs to be adaptive



"Static" Channel



Mobile Channel – Pedestrian



High Level Designs

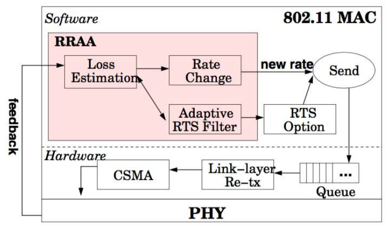
- "Trial and Error": senders use past packet success or failures to adjust transmit rate
  - » Sequence of x successes: increase rate
  - » Sequence of y failures: reduce rate
  - » Hard to get x and y right
  - » Random losses can confuse the algorithm
- Signal strength: stations use channel state information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

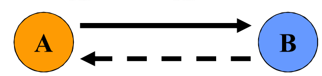
SINR: Noise and Interference

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

- 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

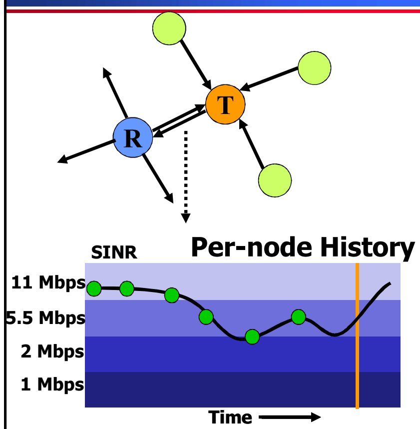
$$RSS = P_{tx} + G_{tx} - PL + G_{rx} \qquad (1)$$



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

- 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

Outline

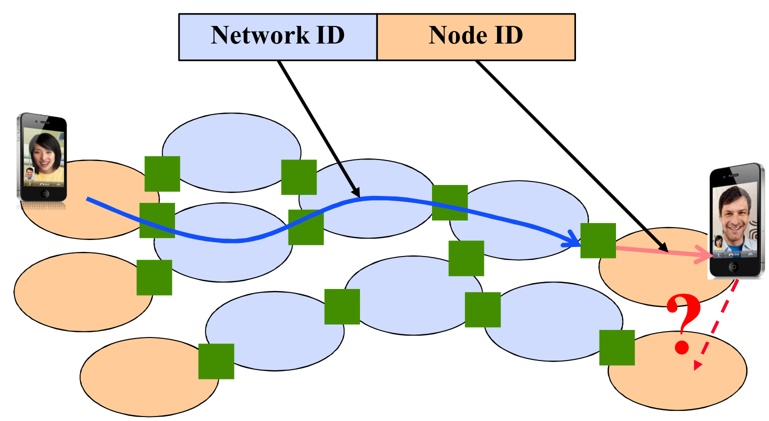
- WiFi deployments
  - » Planning
  - » Channel selection
  - » Rate adaptation
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

IP Address Structure

Network ID	Node ID

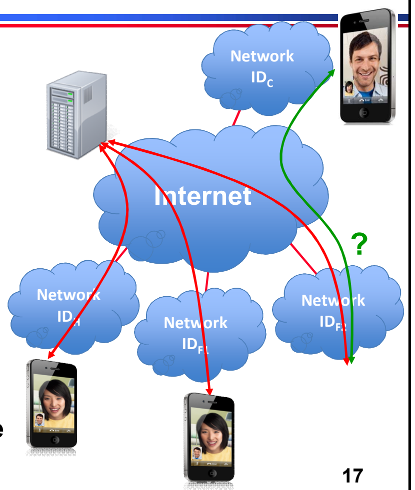
- Network ID identifies the network
  - » CMU = 128.2
- Node ID identifies node within a network
  - » Node IDs can be reused in different networks
  - » Can be assigned independently by local administrator
- Size of Network and Node IDs are variable
  - » Originally Network IDs came in three sizes only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

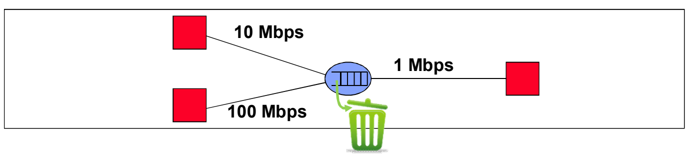
- When a host moves to a new network, it gets a new IP address
- How do other hosts connect to it?
  - » Assume you provide services
  - » They have old IP address
- How do peers know you are the same host?
  - » IP address identifies host
  - » Associated with the socket of any active sessions
- What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