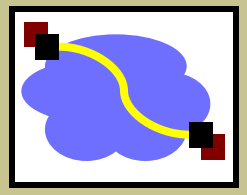
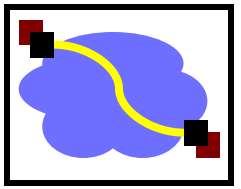


15-441: Computer Networking

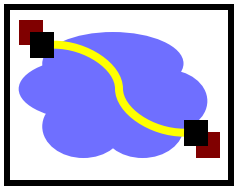
Wireless Networking

Outline



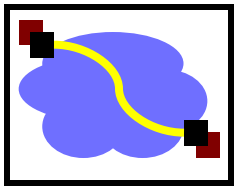
- Wireless Challenges
- 802.11 Overview
- Link Layer
- Ad-hoc Networks

Assumptions made in Internet



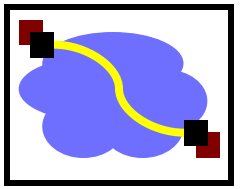
- Host are (mostly) stationary
  - Address assignment, routing
- Links in the network are fairly homogeneous
  - Transport protocols, applications
- Hosts are fairly powerful
  - End to end principle: push functionality to end points
- Security is an end host issue
  - No security inside the network (architecturally)

Mobility



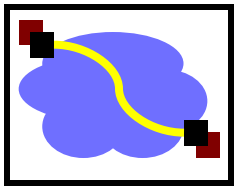
- Many clients today are mobile
- Mobility inside a subnet is supported
  - E.g. moving across APs that are part of a single EBSS
- Mobility across subnets is harder because the IP address is used as address and identifier
  - Identifier: who you are
  - Address: where you can be found
- Keep IP address: network gets confused
  - Delivers packets to wrong “old” subnet
- New IP address: host gets confused
  - Transport protocols, applications, etc.

Link Heterogeneity



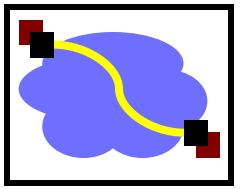
- Original links were basically telephone lines
- Today: huge diversity
  - Optical fiber (wavelengths) … copper … wireless
- Need to share airwaves rather than wire
  - Don’t know what hosts are involved
  - Host may not be using same link technology
  - Wireless is generally slow
  - Error characteristics: higher on wireless - attenuation, interference, multipath
  - Latency: absolute delay and variance in delay
- Mobility adds to diversity
  - E.g. hand off can cause delays and sudden changes in available bandwidth

Device Capabilities



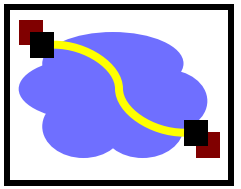
- Originally: mainframes and personal computers
- Today: sensors … supercomputers
- Note: almost any networked device today is more capable than early computers!
  - But our requirements and expectations have increased
  - Anything at or above “PC class” is very capable
- Laptop: view as mobile PC
- PDA: view as 5 year old PC (kind of)
- Cell phone: not even close to a PC
- Sensors: often run as private networks

Security



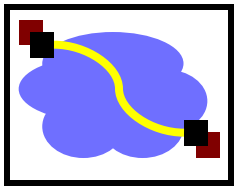
- Access to the network enables all kinds of attacks
  - Argues for pushing security inside the network
  - Firewalls are a very ad hoc way of doing this
- Wireless creates unique challenges
  - Do not need physical connection to sniff or send
  - WEP, 802.1x, etc.
- But wireless security needs to be linked into system wide security

Overview



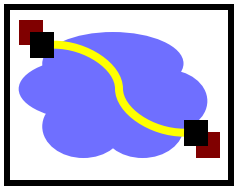
- Wireless Challenges
- 802.11 Overview
- Link Layer Challenges
- Ad-hoc Networks

IEEE 802.11 Wireless LAN



- 802.11b
  - 2.4-2.5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
  - widely deployed, using base stations
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-2.5 GHz range
  - up to 54 Mbps
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

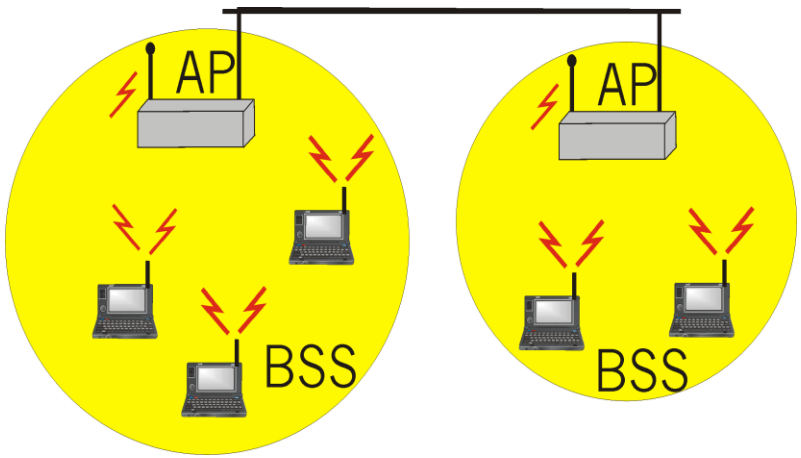
IEEE 802.11 Wireless LAN



- IEEE 802.11a
  - PHY Standard : 8 channels : up to 54 Mbps : some deployment
- IEEE 802.11b
  - PHY Standard : 3 channels : up to 11 Mbps : widely deployed.
- IEEE 802.11d
  - MAC Standard : support for multiple regulatory domains (countries)
- IEEE 802.11e
  - MAC Standard : QoS support : supported by many vendors
- IEEE 802.11f
  - Inter-Access Point Protocol : deployed
- IEEE 802.11g
  - PHY Standard: 3 channels : OFDM and PBCC : widely deployed (as b/g)
- IEEE 802.11h
  - Suppl. MAC Standard: spectrum managed 802.11a (TPC, DFS): standard
- IEEE 802.11i
  - Suppl. MAC Standard: Alternative WEP : standard
- IEEE 802.11n
  - MAC Standard: MIMO : standardization expected late 2008

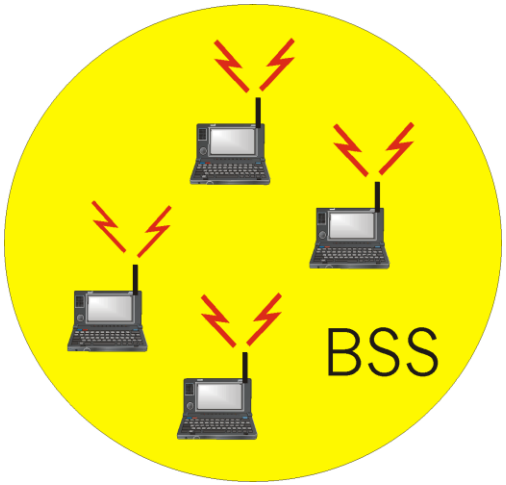
IEEE 802.11 Wireless LAN

- Wireless host communicates with a base station
  - Base station = access point (AP)
- **Basic Service Set (BSS) (a.k.a. “cell”) contains:**
  - **Wireless hosts**
  - **Access point (AP): base station**
- **BSS’s combined to form distribution system (DS)**

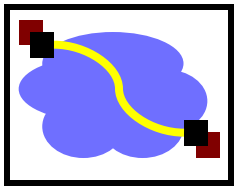


Ad Hoc Networks

- Ad hoc network: IEEE 802.11 stations can dynamically form network *without* AP
- Applications:
  - Vehicles exchange information (VANET)
  - Laptops meeting in conference room, car
  - Interconnection of “personal” devices

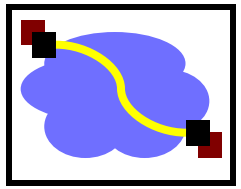


Overview

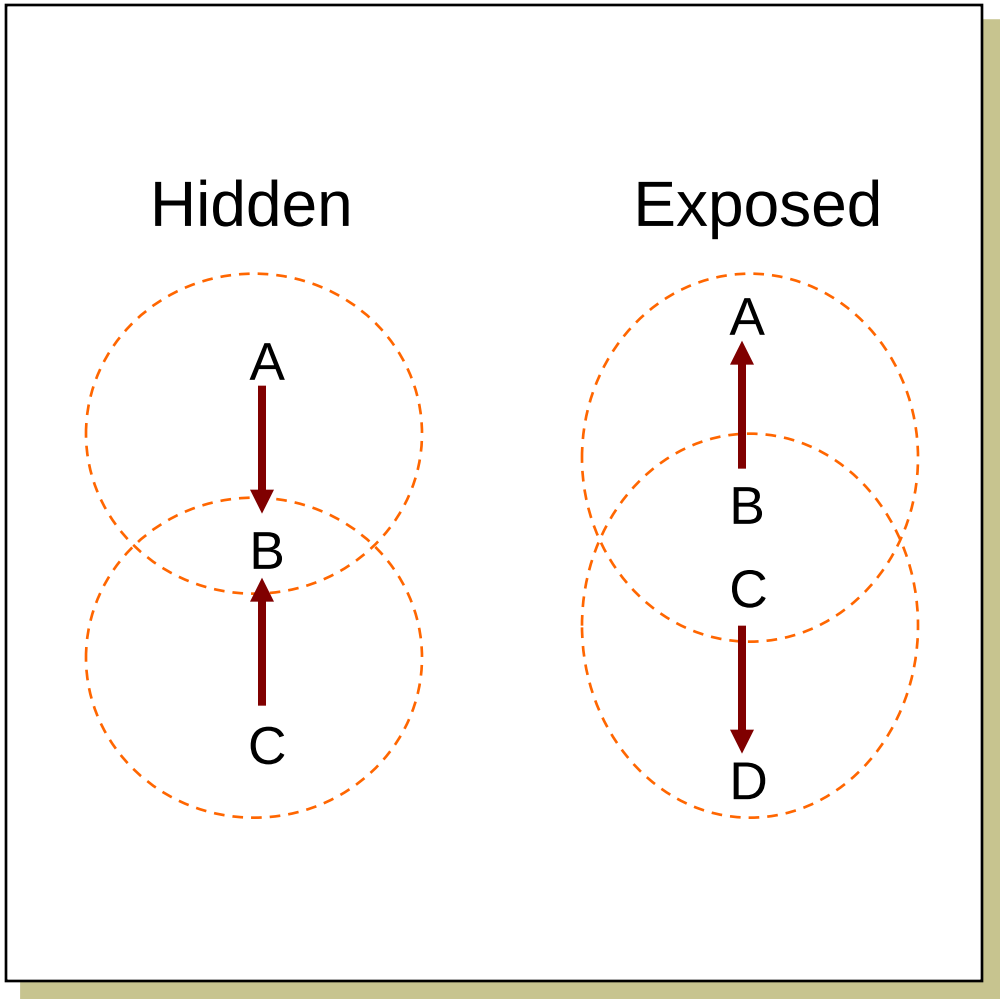


- Wireless Challenges
- 802.11 Overview
- Link Layer Challenges
- Ad-hoc Networks

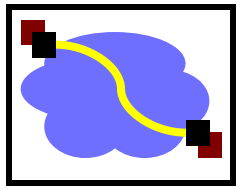
CSMA/CD Does Not Work



- Collision detection problems
  - Relevant contention at the receiver, not sender
    - Hidden terminal
    - Exposed terminal
  - Hard to build a radio that can transmit and receive at same time

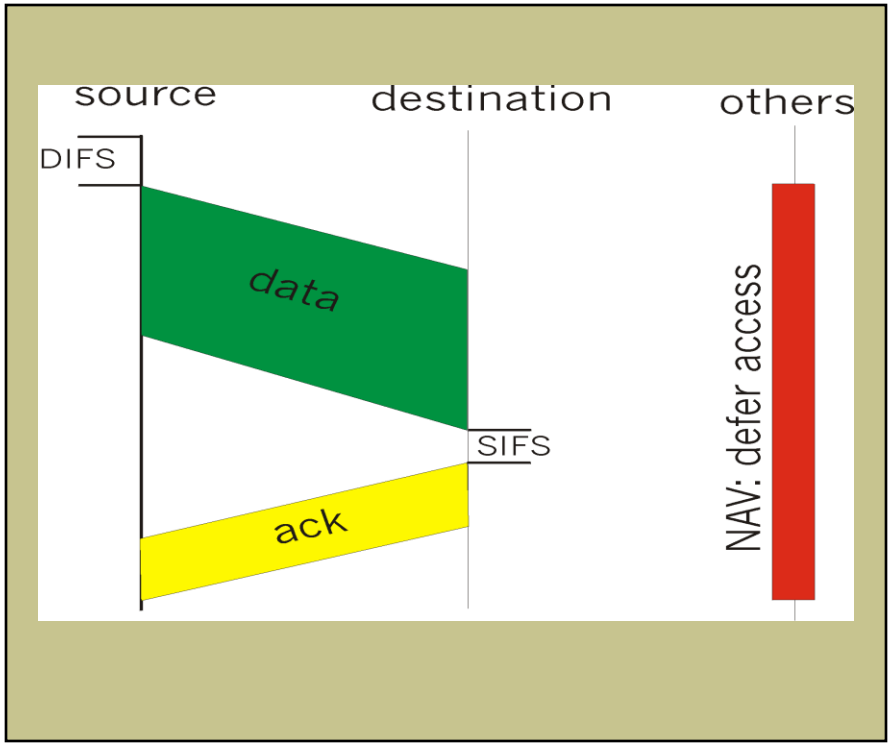


IEEE 802.11 MAC Protocol: CSMA/CA



802.11 CSMA: sender

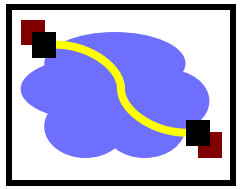
- If sense channel idle for **DISF (Distributed Inter Frame Space)**
  then transmit entire frame (no collision detection)
- If sense channel busy
  then binary backoff



802.11 CSMA receiver:

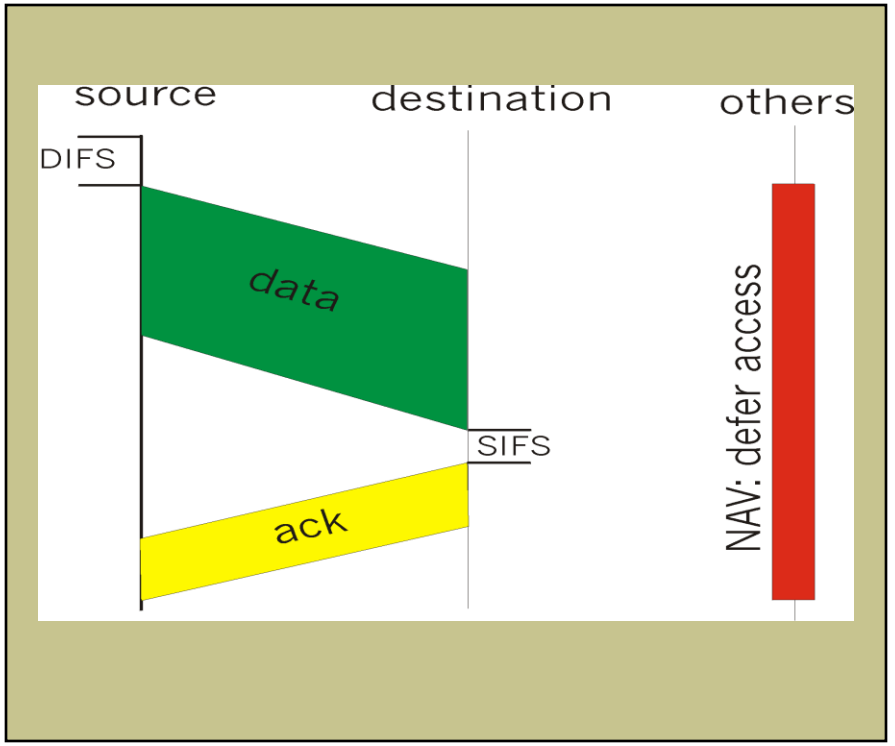
- If received OK
  return ACK after **SIFS (Short IFS)**
  (ACK is needed due to lack of collision detection)

IEEE 802.11 MAC Protocol

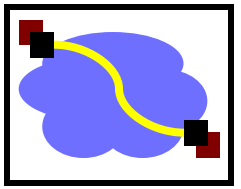


802.11 CSMA Protocol: others

- **NAV**: Network Allocation Vector
- 802.11 frame has transmission time field
- Others (hearing data) defer access for NAV time units



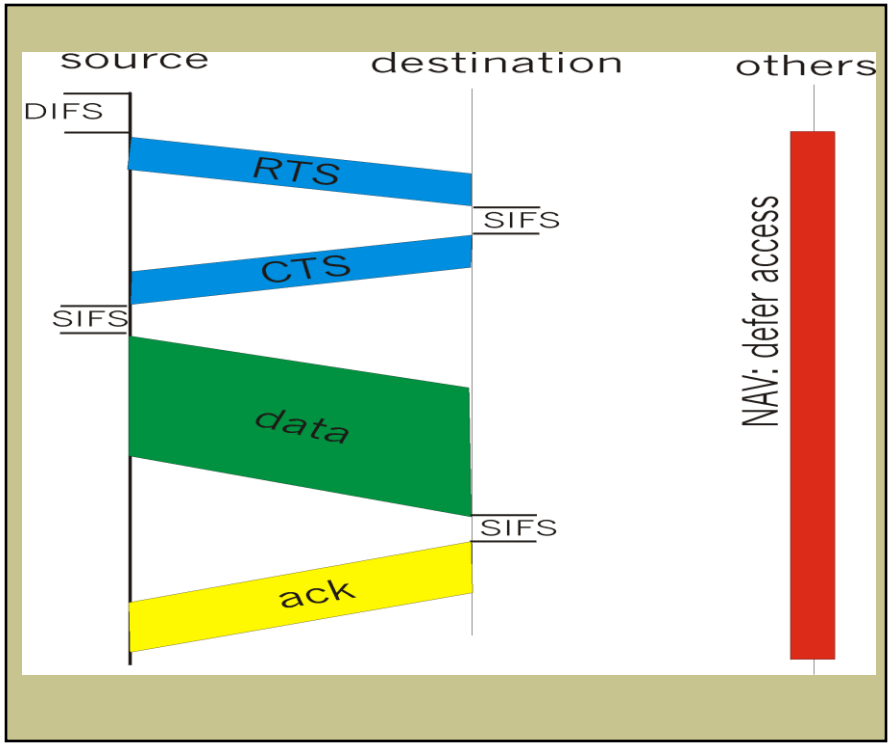
Collision Avoidance Mechanisms



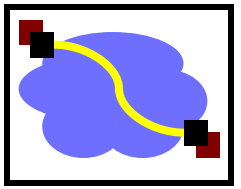
- Problem:
  - Two nodes, hidden from each other, transmit complete frames to base station
  - Wasted bandwidth for long duration !
- Solution:
  - Small reservation packets
  - Nodes track reservation interval with internal “network allocation vector” (NAV)

Collision Avoidance: RTS-CTS Exchange

- Explicit channel reservation
  - Sender: send short RTS: request to send
  - Receiver: reply with short CTS: clear to send
  - CTS reserves channel for sender, notifying (possibly hidden) stations
- RTS and CTS short:
  - collisions less likely, of shorter duration
  - end result similar to collision detection
- Avoid hidden station collisions
- Not widely used/implemented
  - Consider typical traffic patterns

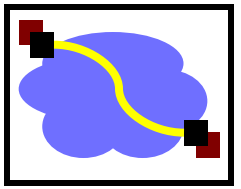


Overview



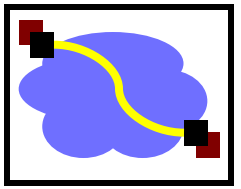
- Wireless Challenges
- 802.11 Overview
- Link Layer Challenges
- Ad-hoc Networks

Ad Hoc Networks



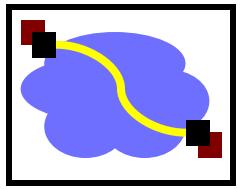
- All the challenges of wireless, plus some of:
  - No fixed infrastructure
  - Mobility (on short time scales)
  - Chaotically decentralized (:-)
  - Multi-hop!
- Nodes are both traffic sources/sinks and forwarders
- The big challenge: Routing

Ad Hoc Routing

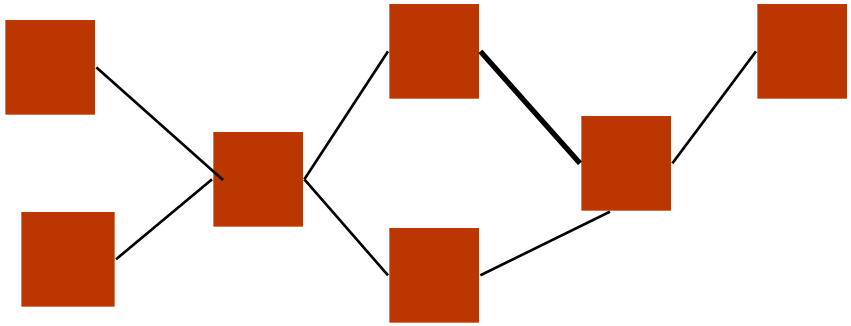


- Find multi-hop paths through network
  - Adapt to new routes and movement / environment changes
  - Deal with interference and power issues
  - Scale well with # of nodes
  - Localize effects of link changes

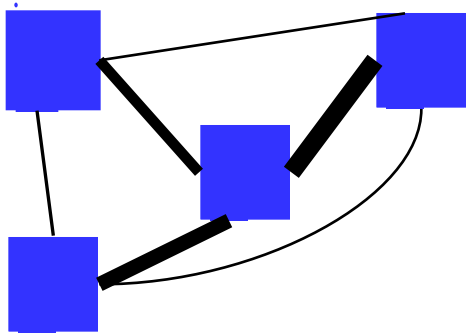
Traditional Routing vs Ad Hoc



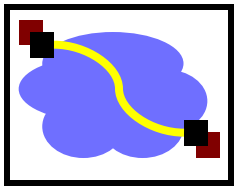
- Traditional network:
  - Well-structured
  - ~O(N) nodes & links
  - All links work ~= well



- Ad Hoc network
  - N^2 links - but many stink!
  - Topology may be really weird
    - Reflections & multipath cause strange interference
  - Change is frequent

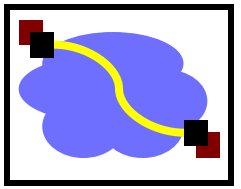


Problems using DV or LS



- DV loops are very expensive
  - Wireless bandwidth << fiber bandwidth…
- LS protocols have high overhead
- N^2 links cause very high cost
- Periodic updates waste power
- Need fast, frequent convergence

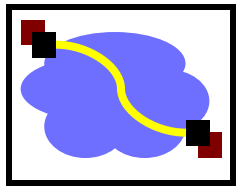
Proposed protocols



- Destination-Sequenced Distance Vector (DSDV)
- Dynamic Source Routing (DSR)
- Ad Hoc On-Demand Distance Vector (AODV)

- Let's look at DSR

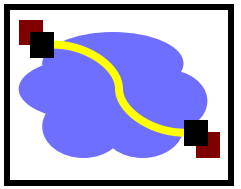
DSR



- Source routing
  - Intermediate nodes can be out of date
- On-demand route discovery
  - Don’t need periodic route advertisements

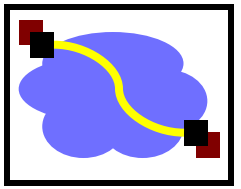
- (Design point: on-demand may be better or worse depending on traffic patterns…)

DSR Components



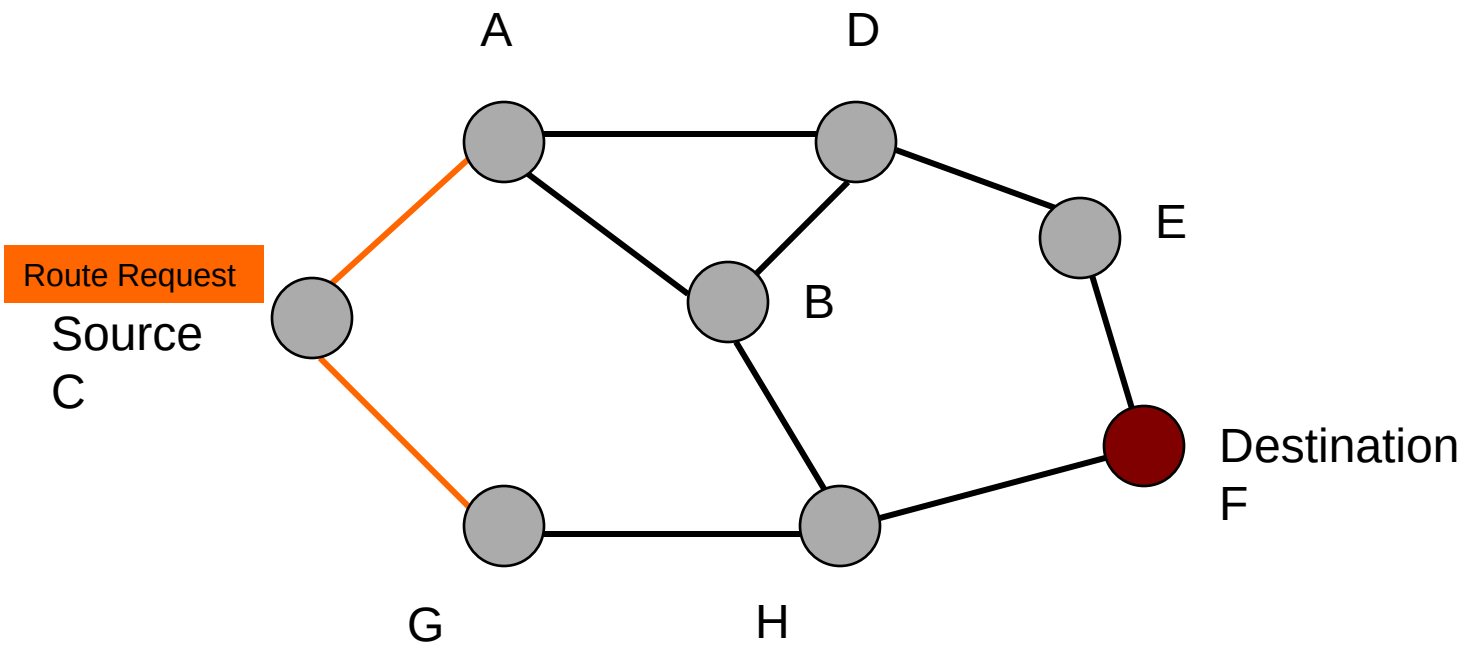
- Route discovery
  - The mechanism by which a sending node obtains a route to destination
- Route maintenance
  - The mechanism by which a sending node detects that the network topology has changed and its route to destination is no longer valid

DSR Route Discovery

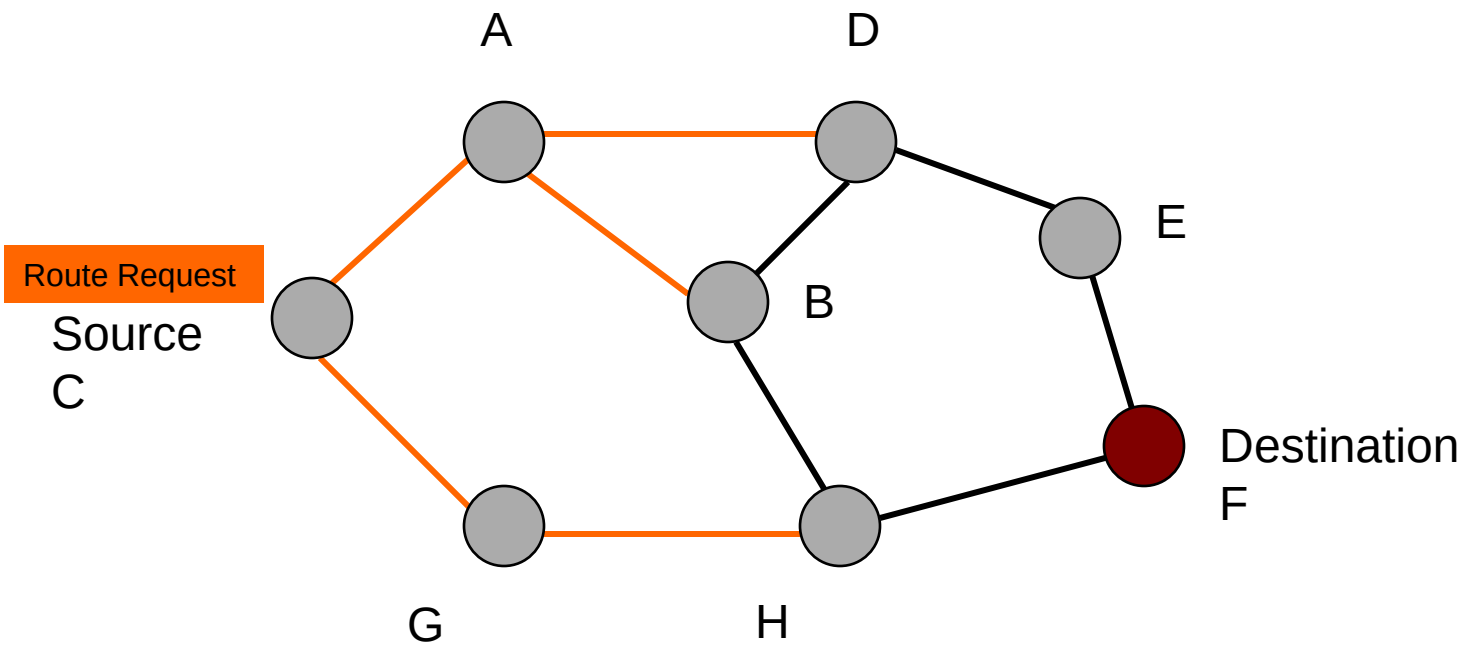


- Route discovery - basic idea
  - **Source** broadcasts route-request to **Destination**
  - Each node forwards request by adding own address and re-broadcasting
  - Requests propagate outward until:
    - Target is found, or
    - A node that has a route to Destination is found

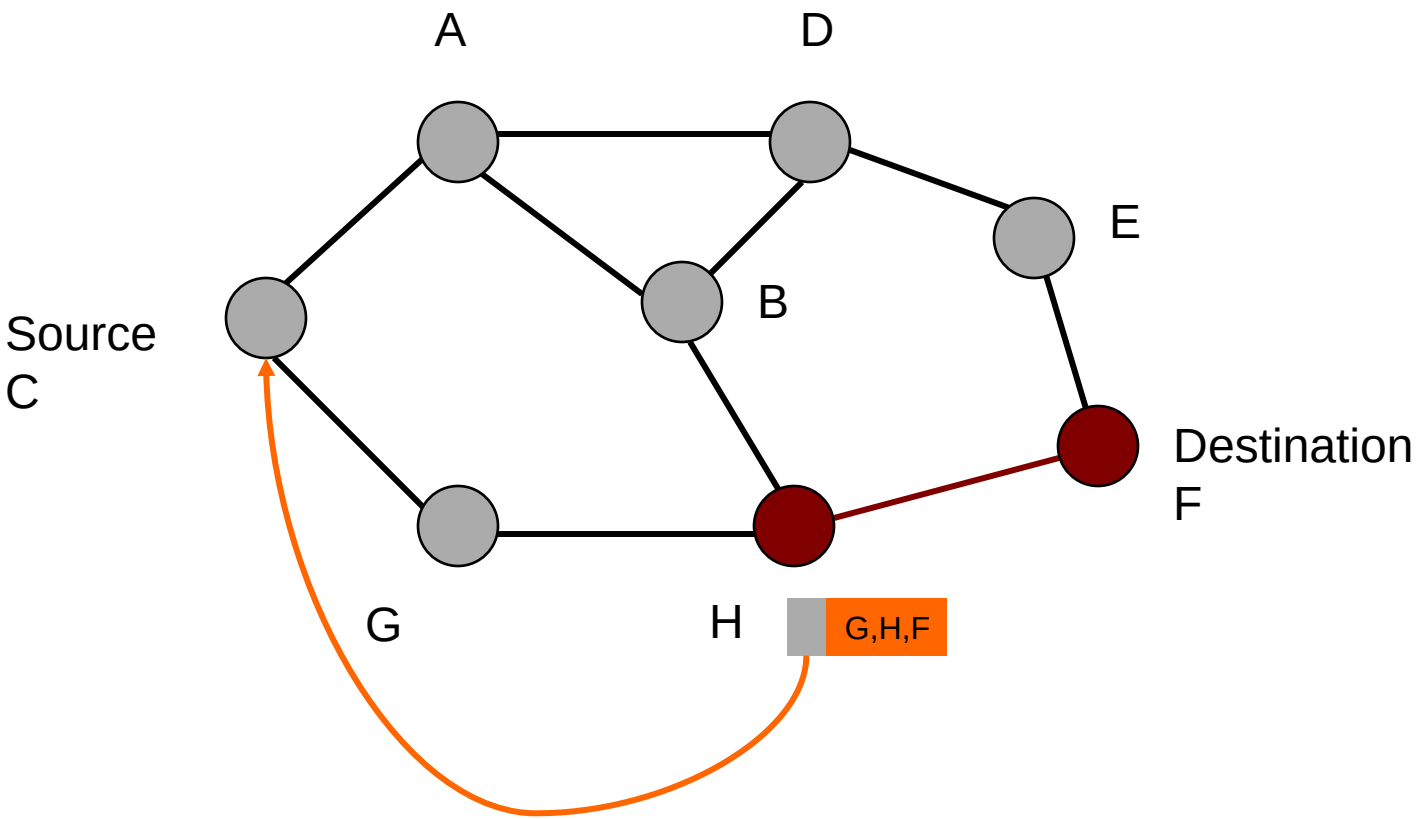
C Broadcasts Route Request to F



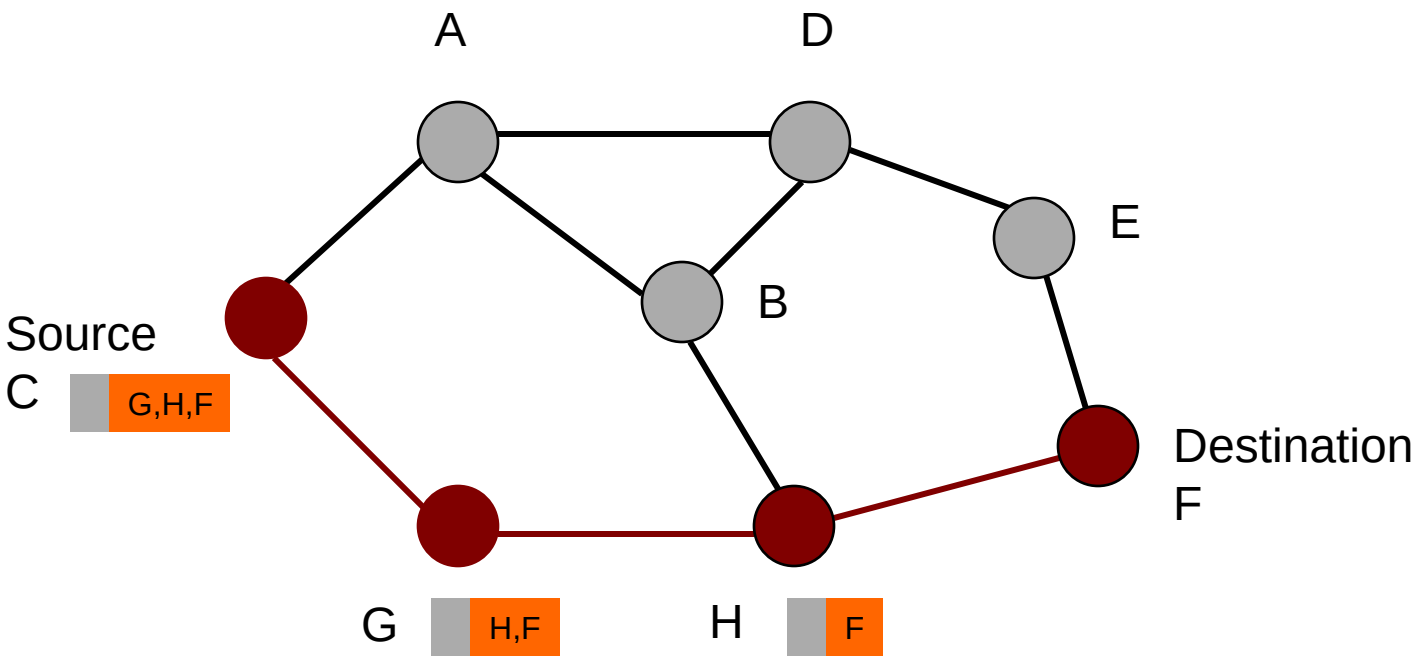
C Broadcasts Route Request to F



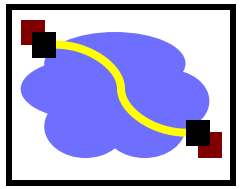
H Responds to Route Request



C Transmits a Packet to F

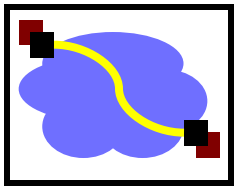


Forwarding Route Requests



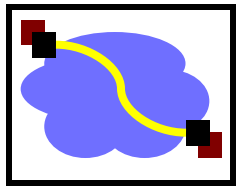
- A request is forwarded if:
  - Node is not the destination
  - Node not already listed in recorded source route
  - Node has not seen request with same sequence number
  - IP TTL field may be used to limit scope
- Destination copies route into a Route-reply packet and sends it back to **Source**

Route Cache



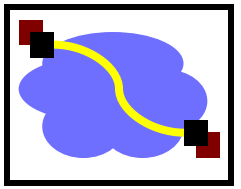
- All source routes learned by a node are kept in Route Cache
  - Reduces cost of route discovery
- If intermediate node receives RR for destination and has entry for destination in route cache, it responds to RR and does not propagate RR further
- Nodes overhearing RR/RP may insert routes in cache

Sending Data



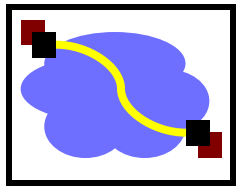
- Check cache for route to destination
- If route exists then
  - If reachable in one hop
    - Send packet
  - Else insert routing header to destination and send
- If route does not exist, buffer packet and initiate route discovery

Discussion



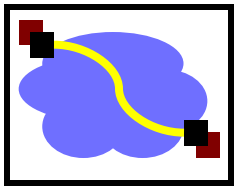
- Source routing is good for on demand routes instead of a priori distribution
- Route discovery protocol used to obtain routes on demand
  - Caching used to minimize use of discovery
- Periodic messages avoided
- But need to buffer packets
- How do you decide between links?

Forwarding Packets is expensive



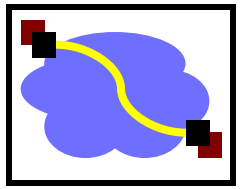
- Throughput of 802.11b =~ 11Mbits/s
  - In reality, you can get about 5.
- What is throughput of a chain?
  - A -> B -> C ?
  - A -> B -> C -> D ?
  - Assume minimum power for radios.
- Routing metric should take this into account

ETX



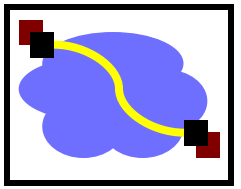
- Measure each link's delivery probability with broadcast probes (& measure reverse)
- P(delivery) = 1 / (df * dr) (ACK must be delivered too)
- Link ETX = 1 / P(delivery)
- Route ETX = sum of link ETX
- (Assumes all hops interfere - not true, but seems to work okay so far)

Capacity of multi-hop network



- Assume N nodes, each wants to talk to everyone else. What total throughput (ignore previous slide to simplify things)
  - O(n) concurrent transmissions. Great! But:
  - Each has length O(sqrt(n)) (network diameter)
  - So each Tx uses up sqrt(n) of the O(n) capacity.
  - Per-node capacity scales as 1/sqrt(n)
    - Yes - it goes down! More time spent Tx'ing other peoples packets…
- But: If communication is local, can do much better, and use cool tricks to optimize

Important Lessons



- Many assumptions built into Internet design
  - Wireless forces reconsideration of issues
- Link-layer
  - Spatial reuse (cellular) vs wires
  - Hidden/exposed terminal
  - CSMA/CA (why CA?) and RTS/CTS
- Network
  - Mobile endpoints – how to route with fixed identifier?
  - Link layer, naming, addressing and routing solutions
    - What are the +/- of each?