15-441 15-641 Computer Networking

Lecture 25 – CSMA Protocols

Peter Steenkiste

Fall 2016

www.cs.cmu.edu/~prs/15-441-F16

Outline

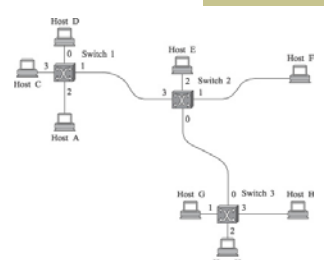
- Ethernet
- Wireless networking
  - Wireless Ethernet
  - Aloha
  - 802.11

Reminder: Datalink Functions

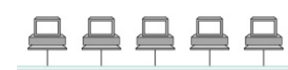
- Framing: encapsulating a network layer datagram into a bit stream.
  - Add header, mark and detect frame boundaries, …
- Error control: error detection and correction to deal with bit errors.
  - Based on error coding or retransmissions
- Flow control: avoid sender overrunning receiver.
- Media access control (MAC): which frame should be sent over the link next.
  - Easy for point-to-point links
  - Harder for multi-access links: who gets to send?

Datalink Architectures

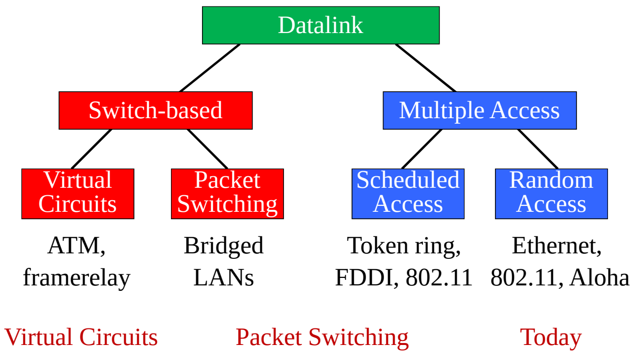
- Switches connected by point-to-point links -- store-and-forward.
  - Used in WAN, LAN, and for home connections
  - Conceptually similar to "routing"
    - But at the datalink layer instead of the network layer
  - MAC = (local) scheduling



- Multiple access networks - - contention based.
  - Multiple hosts are sharing the same transmission medium
  - Used in LANs and wireless
  - Access control is distributed and much more complex



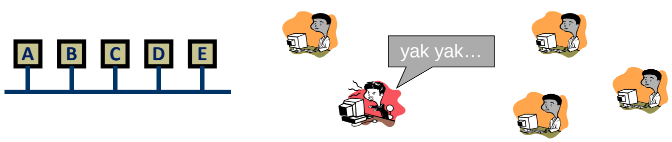
Datalink Classification



Random Access Protocols

- When node has packet to send
  - Transmit at full channel data rate R
  - No *a priori* coordination among nodes
- Two or more transmitting nodes → "collision"
- Random access MAC protocol specifies:
  - How to detect collisions
  - How to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - CSMA and CSMA/CD
  - Wireless protocols

Problem: Sharing a Wire



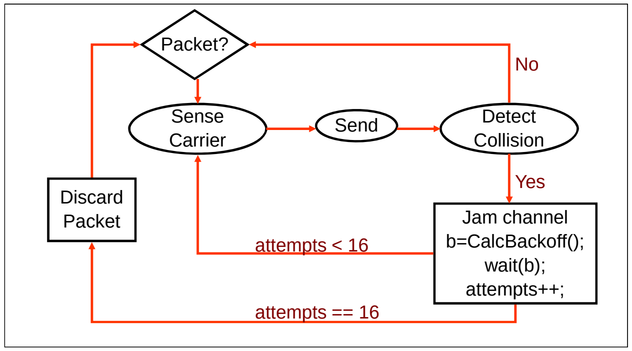
- Just send a packet when you are ready
  - Does not work well: collisions! More on this later
- Natural scheme – listen before you talk …
  - Works well in practice
  - A cheap form of coordination
- But sometimes this breaks down
  - Why? How do we fix/prevent this?

Ethernet MAC Features

- Carrier Sense: listen before you talk
  - Avoid collision with active transmission
- Collision Detection during transmission
  - Listen while transmitting
  - If you notice interference → assume collision
  - Abort transmission immediately – saves time
- Why didn't ALOHA have this?
  - Signal strength is reduced by distance for radio
    - May not hear remote transmitter – hidden terminal
  - Very difficult for radios to listen and transmit
  - More on this later in the course

Ethernet MAC – CSMA/CD

- Carrier Sense Multiple Access/Collision Detection



Ethernet CSMA/CD: Making it work

Jam Signal: make sure all other transmitters are aware of collision; 48 bits;

Exponential Backoff:

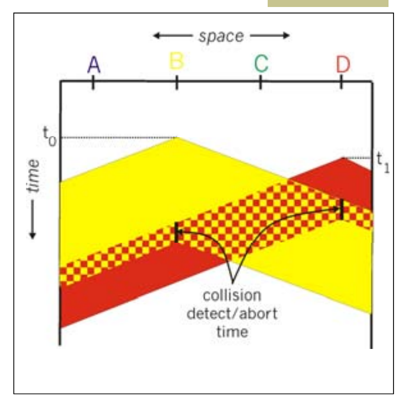
- If deterministic delay after collision, collisions will occur again in lockstep
- Why not random delay with fixed mean?
  - Few senders → needless waiting
  - Too many senders → too many collisions
- *Goal*: adapt retransmission attempts to estimated current load
  - heavy load: random wait will be longer

Ethernet Backoff Calculation

- Delay is set as K slots – control K
- Exponentially increasing random delay
  - Infer senders from # of collisions
  - More senders → increase wait time
- First collision: choose K from {0,1}; delay is K x 512 bit transmission times
- After second collision: choose K from {0,1,2,3}…
- After ten or more collisions, choose K from {0,1,2,3,4,…,1023}

Minimum Packet Size

- Packets must be long enough to guarantee all nodes observe collision
- Depends on packet size and length of wire
  - Propagation delay
- Min packet length > 2x max prop delay



Delay & Collision Detection

- Speed in cable ~= 60% * c ~= 1.8 x 10^8 m/s
- 10Mb Ethernet, 2.5km cable
  - ~= 12.5us delay
  - +Introduced repeaters (max 5 segments)
  - Worst case – 51.2us round trip time!
  - Corresponds to 512 bits
- Also used as slot time = 51.2us for backoff
  - After this time, sender is guaranteed sole access to link
  - Specifically, will have heard any signal sent in the previous slot

Scaling Ethernet

- What about scaling? 10Mbps, 100Mbps, 1Gbps, ...
  - Use a combination of reducing network diameter and increasing minimum minimum packet size
- Reality check: 40 Gbps is 4000 times 10 Mbps
  - 10 Mbps: 2.5 km and 64 bytes -> silly
  - Solution: switched Ethernet – see lecture 3
- What about a maximum packet size?
  - Needed to prevent node from hogging the network
  - 1500 bytes in Ethernet = 1.2 msec on original Ethernet
  - For 40 Gps -> 0.3 microsec -> silly and inefficient

Things to Remember

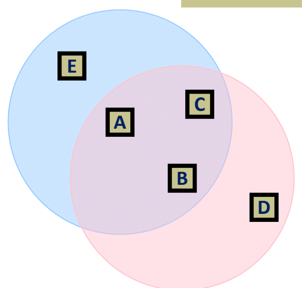
- Trends from CSMA networks to switched networks
  - Need for more capacity
  - Low cost and higher line rate
- Emphasis on low configuration and management complexity and cost
  - Fully distributed path selection
- Trends are towards "Software Defined Networks"
  - Network is managed by a centralized controller
  - Allows for the implementation of richer policies
    - Easier to manage centrally
  - Already common in data centers

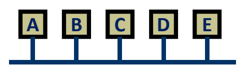
Outline

- Ethernet
- Wireless networking
  - Wireless Ethernet
  - Aloha
  - 802.11

Wireless Communication

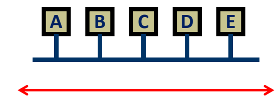
- Wireless communication is based on broadcast
  - A, B, and C can all hear each other's signal
- Looks like Ethernet!
- Why not use CSMA/CD?
  - Carrier-sense Multiple Access / Collision Detection
- Well, it is not that easy

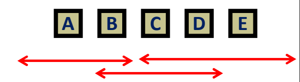




What is the Problem? There are no Wires!

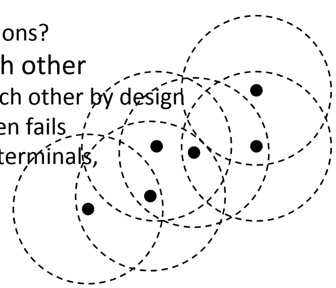
- Attenuation is very high!
  - Signal is not contained in a wire
  - Attenuation is $1/D^2$ for distance D
- In addition, there is significant noise and interference
  - No wire to protect the signal
- It is much harder for nodes to communicate
  - Much higher error rates
  - Not all nodes in the wireless network can hear each other



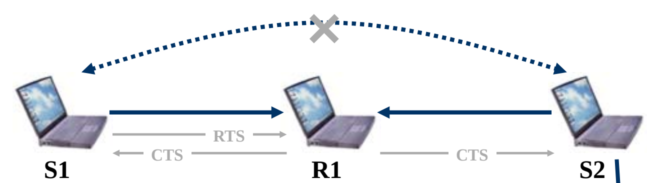


Implications for Wireless Ethernet

- Collision detection is not practical
  - Ratio of transmitted signal power to received power is too high at the transmitter
  - Transmitter cannot detect competing transmitters (is deaf while transmitting)
  - So how do you detect collisions?
- Not all nodes can hear each other
  - Ethernet nodes can hear each other by design
  - "Listen before you talk" often fails
  - Hidden terminals, exposed terminals,
  - Capture effects
- Made worse by fading
  - Changes over time!

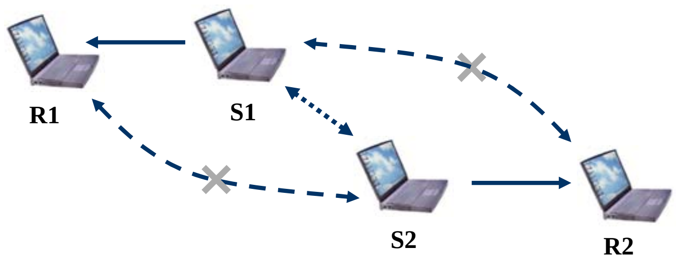


Hidden Terminal Problem



- Lack signal between S1 and S2 and cause collision at R1
- Severity of the problem depends on the sensitivity of the carrier sense mechanism
  - Clear Channel Assessment (CCA) threshold

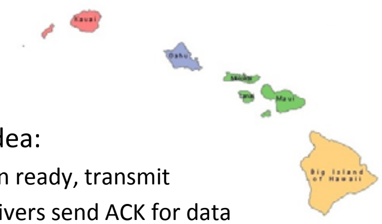
Exposed Terminal Problem



- Carrier sense prevents two senders from sending simultaneously although they do not reach each other's receiver
- Severity again depends on CCA threshold
  - Higher CCA reduces occurrence of exposed terminals, but can create hidden terminal scenarios

Aloha – Basic Technique

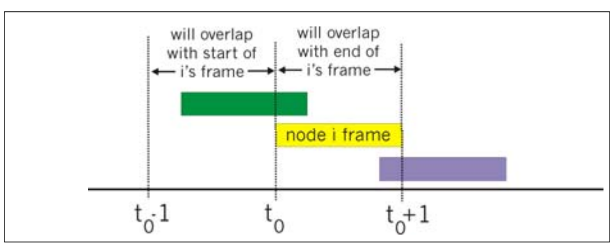
- First random MAC developed
  - For radio-based communication in Hawaii (1970)



- Basic idea:
  - When ready, transmit
  - Receivers send ACK for data
  - Detect collisions by timing out for ACK
  - Recover from collision by trying after random delay

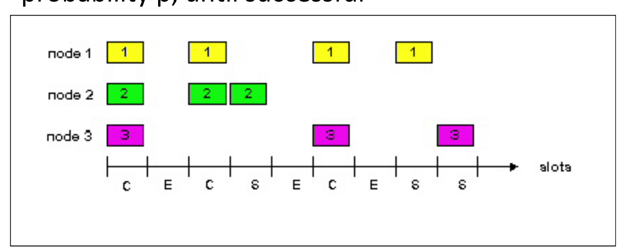
Collisions in ALOHA

- Original ALOHA had no synchronization
- Pkt needs transmission:
  - Send without awaiting for beginning of slot
- Many chances for collision
  - Pkt sent at t_0 collide with other pkts sent in $[t_0-1, t_0+1]$



Slotted Aloha

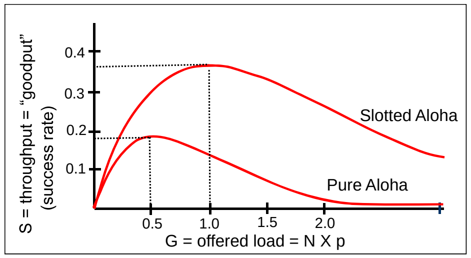
- Time is divided into equal size slots
  - Equal to packet transmission time
- Node (w/ packet) transmits at beginning of next slot
- If collision: retransmit pkt in future slots with probability p, until successful



Aloha Throughput Comparison

- It is possible to calculate throughput for Aloha
  - Many assumptions: exponential arrival, transmitters independent, …
- Bad news: maximum throughput is low
- Slotted Aloha (a variant) can achieve higher throughput
  - But has higher latency, especially under low load

protocol constrains effective channel throughput!



Outline

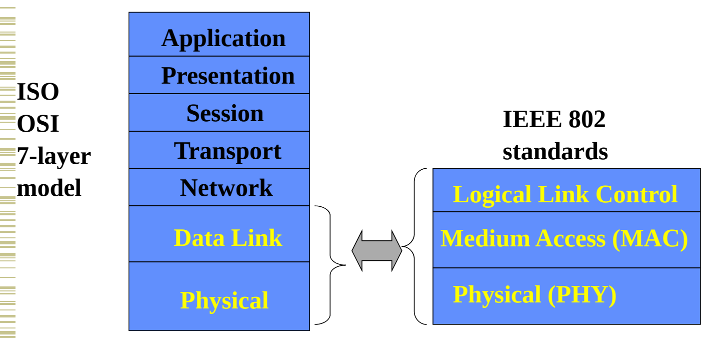
- Ethernet
- Wireless networking
  - Wireless Ethernet
  - Aloha
  - 802.11

History

- Aloha wireless data network
- Car phones
  - Big and heavy "portable" phones
  - Limited battery life time
  - But introduced people to "mobile networking"
  - Later turned into truly portable cell phones
- Wireless LANs
  - Originally in the 900 MHz band
  - Later evolved into the 802.11 standard
  - Later joined by the 802.15 and 802.16 standards
- Cellular data networking
  - Data networking over the cell phone
  - Many standards – throughput is the challenge

Standardization of Wireless Networks

- Wireless networks are standardized by IEEE
- Under 802 LAN MAN standards committee



The 802 Class of Standards

- List on next slide
- Some standards apply to all 802 technologies
  - E.g. 802.2 is LLC
  - Important for inter operability
- Some standards are for technologies that are outdated
  - Not actively deployed anymore
  - E.g. 802.6

- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
  - 802.3a Contention Bus Standard 10base 2 (Thin Net)
  - 802.3b Broadband Contention Bus Standard 10broad 36
  - 802.3d Fiber-Optic InterRepeater Link (FOIRL)
  - 802.3e Contention Bus Standard 1 base 5 (Starlan)
  - 802.3i Twisted-Pair Standard 10base T
  - 802.3j Contention Bus Standard for Fiber Optics 10base F
  - 802.3u 100-Mb/s Contention Bus Standard 100base T
  - 802.3x Full-Duplex Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
  - 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
  - 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard

WiFi Family

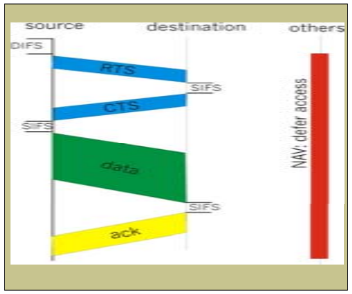
Bluetooth, Zigbee, ..

Wireless Collision Avoidance

- Problem: two nodes, hidden from each other, transmit complete frames to base station
- Wasted bandwidth for long duration !
  - Plus also exponential backoff before retransmissions
- Solution: small reservation packets
  - Nodes track reservation interval with internal “network allocation vector” (NAV)
- Note that nodes still do “physical” carrier sense
  - “Listen before you talk” often works and is cheap

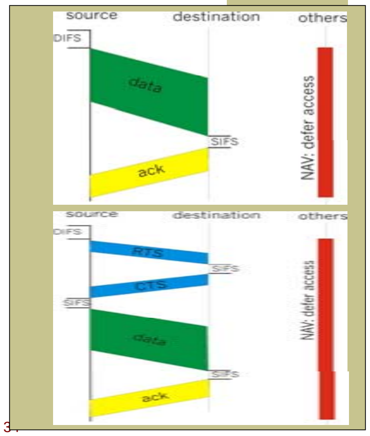
Collision Avoidance: RTS-CTS Exchange

- 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 (not used really)
  - Overhead is too high
  - Not a serious problem in typical deployments



IEEE 802.11 MAC Protocol

- RTS/CTS implemented using **NAV**: Network Allocation Vector
  - Also used with data packets
- 802.11 frame has transmission time field
- Others (hearing data) defer access for NAV time units
- How do we ensure the node can send



How About Exposed Terminal?

- Can increase the “carrier-sense” threshold
  - Signal needs to be stronger before node defers
- Could this create other problems?
  - Yes - not really practical
- Exposed terminals are difficult to deal with
  - Even hard to detect them!
- Good news – they are
  - So we live with them