CMPE 257: Wireless and Mobile Networking

Katia Obraczka
Computer Engineering
UCSC Baskin Engineering

Lecture 3

CMPE 257 Spring’15
Announcements

• Next week
  – April 14: ICN (Spencer Sevilla)
  – April 16: DTN (Aloizio Silva)
• Projects
  – Project ideas
  – Project proposal
• Student presentations
• Class calendar updated
Today

• Medium access control (MAC).
Medium Access Control

- MAC protocols.
- Aka, multiple access protocols.
When do we need MAC?

• 2 types of links:
  – Point-to-point.
  – Shared.

- Shared wire (e.g., cabled Ethernet)
- Shared RF (e.g., 802.11 WiFi)
- Shared RF (satellite)
- Humans at a cocktail party (shared air, acoustical)
Shared Links

• If more than 1 node transmits at the same time:
  – Collision at receiver!

• MAC protocol:
  – Arbitrate access to medium.
  – Determine who can transmit when.
Expanded Data Link Layer

• Sublayers of data link layer:
  – **Logical Link Control (LLC):** framing, flow and error control.
  – **Medium Access Control (MAC):** multiple access resolution.
Types of MAC

• Who makes decision?
  – Centralized versus distributed MACs.
• Channel access policy.
Types of MAC

Channel Access Policy

- **Random access (or contention-based)**
  - No scheduled time for transmissions.
  - No order for transmissions.

- **Controlled access**
  - Stations coordinate access to channel.
  - Station only transmits when it has right to send.

- **Channelization (channel partitioning)**
  - Bandwidth of channel is statically partitioned.
Another way to look at it…

• Control:
  – Distributed.
  – Centralized.

• How they coordinate access to medium:
  – Round-robin.
  – Scheduled-access.
  – Contention-based.
  – A-priori channel partitioning.
Contention-Based Protocols

• Aka, Random-Access MAC:
  • ALOHA
  • Slotted Aloha
  • CSMA
  • CSMA/CD (Ethernet IEEE 802.3)
  • CSMA/CA (WiFi IEEE 802.11)
CSMA

• Carrier sense:
  – Stations listen first whether another transmission is in progress.
  – If medium in use, wait.
  – If not, transmit.

• Can collisions still occur?
CSMA Variants

• 1-persistent (IEEE 802.3):
  – If medium idle, transmit.
  – If medium busy, keep listening; when medium idle, transmit with probability 1.

• $p$-persistent:
  – Same as above but with probability $p$.

• Non-presistent:
  – If medium idle, transmit.
  – If medium busy, wait a random period before retrying.
CSMA/CD

• CSMA + collision detection.
  – Performance improvement over CSMA.
  – How?
    • Listen while transmitting.
    • If collision, transmit brief jamming signal and abort transmission.
      – How does this improve performance?
    • Wait random time and try again.
Collision Avoidance (CA)

• CSMA/CD assumes stations can detect collision.
• Not valid in all contexts (e.g., wireless):
  – Attenuation too great to detect collision at all stations.
  – Hard for transmitter to distinguish its own transmission from incoming weak signals and noise.
  – Radios are usually half-duplex ($$$).

CSMA/CA tries to avoid collisions.
CSMA/CA

Tries to avoid collisions by avoiding the “hidden terminal” problem.

How?

But, first, what's hidden terminal?
Hidden-Terminal Problem

B and C are hidden from each other with respect to A.
Hidden- and Exposed Terminals

A wants to send to B but cannot hear that B is busy

B wants to send to C but mistakenly thinks the transmission will fail

(a) Hidden Terminals

(b) Exposed Terminals
CSMA/CA: RTS-CTS Solution

“Channel reservation”

- With collision avoidance, stations exchange small control packets to determine which sender can transmit to a receiver.
CSMA-CA

• CSMA/CA means both physical- and virtual carrier sensing.
  – Physical: CS.
  – Virtual: CA.
How does CSMA-CA work?
IEEE 802.11

- Provides 2 types of medium access:
  - DCF: distributed coordination function.
  - PCF: point coordination function.
- DCF is contention-based.
- PCF is polling-based.
  - Collision free.
  - Implemented atop DCF.
IEEE 802.11 DCF

• Physical carrier sensing:
  – Stations listen to channel before transmitting (CS of CSMA/CA).

• Virtual carrier sensing:
  – CA OF CSMA/CA.
  – “Reserve” channel for transmission.
  – Use RTS/CTS handshake.
IEEE 802.11 MAC Protocol: CSMA (no CA)

**802.11 sender**

1. if sense channel idle for DIFS then
   transmit entire frame (no CD)

2. if sense channel busy then
   start random backoff time
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random backoff interval,
   repeat 2

**802.11 receiver**

- if frame received OK
  return ACK after SIFS (ACK needed due to hidden terminal problem)
IEEE 802.11 MAC Protocol: CSMA/CA

- Physical CS + virtual CS.
  - Sense channel for DIFS.
- RTS/CTS handshake before sending data.
  - RTS is 20 bytes and CTS is 16 bytes.
  - Maximum data frame is 2,346 bytes.

Note: This is only for unicast transmissions. Broadcast transmissions do not use virtual carrier sensing.
CSMA-CA Examples

Scenario: A wants to transmit to C.
  . A sends RTS.
  . D defers.
  . C sends CTS.
  . B defers.
IEEE 802.11 Wireless LAN

- **802.11b**
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code

- **802.11a**
  - 5-6 GHz range
  - up to 54 Mbps

- **802.11g**
  - 2.4-5 GHz range
  - up to 54 Mbps

- **802.11n**: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network modes.
MAC: A Bird’s Eye View
Solutions to Hidden/Exposed Nodes in CSMA

• Use control packets:
  – RTS/CTS (Request-To-Send/Clear-To-Send)
  – Used by MACA (Multiple Access Control Avoidance) and MACAW (MACA for Wireless LANs).

• Use both control packets and carrier sense:
  – CSMA/CA, IEEE 802.11
Dynamic Reservation Approaches: Sender- vs. Receiver-initiated

• Sender-initiated:
  – A node wanting to send data takes the initiative of setting up the reservation.
  – Most existing schemes.

• Receiver-initiated:
  – A receiving node polls a potential transmitting node for data.
  – A node can send data after being polled.
  – E.g., MACA-By Invitation.
Single vs. Multiple Channel Protocols

• Single channel protocols: control and data use the same channel.

• Multiple channel protocols: separate channels for control & data transmission; data transmission on separate channels.
Other criteria for classification

• Power-aware.
  – E.g., PAMAS.

• Directional or omnidirectional antennas.

• QoS-aware
  – End-to-end (E2E) delay
  – Packet loss rate (or the probability)
  – Available bandwidth
  – Challenges: lack of centralized control, limited bandwidth, node mobility, power/computational constraints, error-prone nature of wireless media.