CSE160: Computer Networks

Lecture #06 – Wireless and Contention Free Protocols

2020-09-15

Professor
Alberto E. Cerpa

Last time…

- The Medium Access Control (MAC) portion of the Link Layer
- Static Partitioning:
  1. TDM
  2. FDM
- Randomized access protocols:
  1. Aloha
  2. CSMA variants
  3. Classic Ethernet

Application
Presentation
Session
Transport
Network
Data Link
Physical

This Lecture

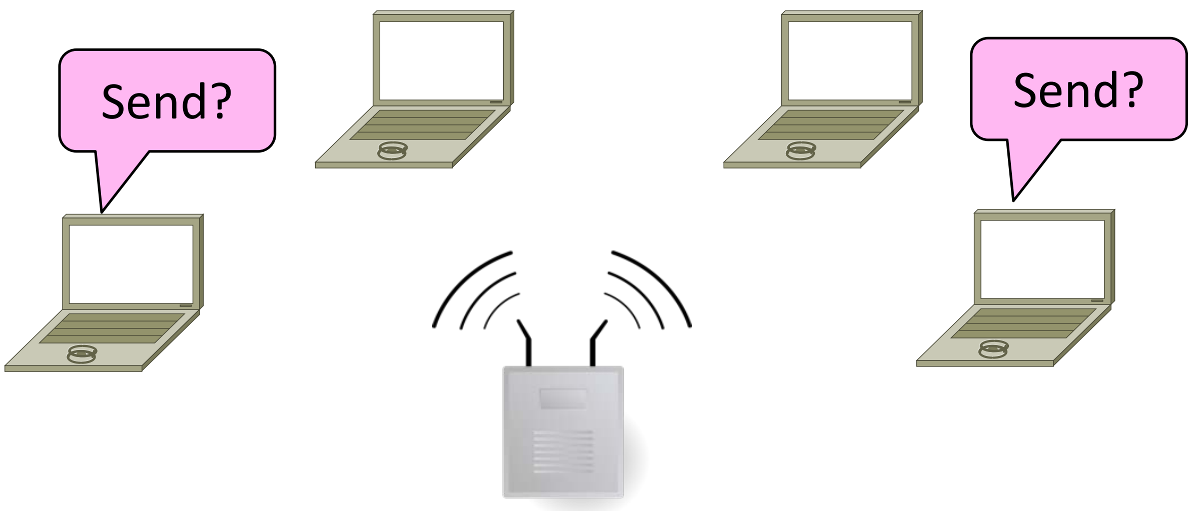
More on multiple-access schemes:

1. Wireless schemes
2. Contention-free protocols

Application
Presentation
Session
Transport
Network
Data Link
Physical

1. Wireless Communication

- How do wireless nodes share a single link? (Yes, this is WiFi!)
  - Build on our simple, wired model



Wireless Complications

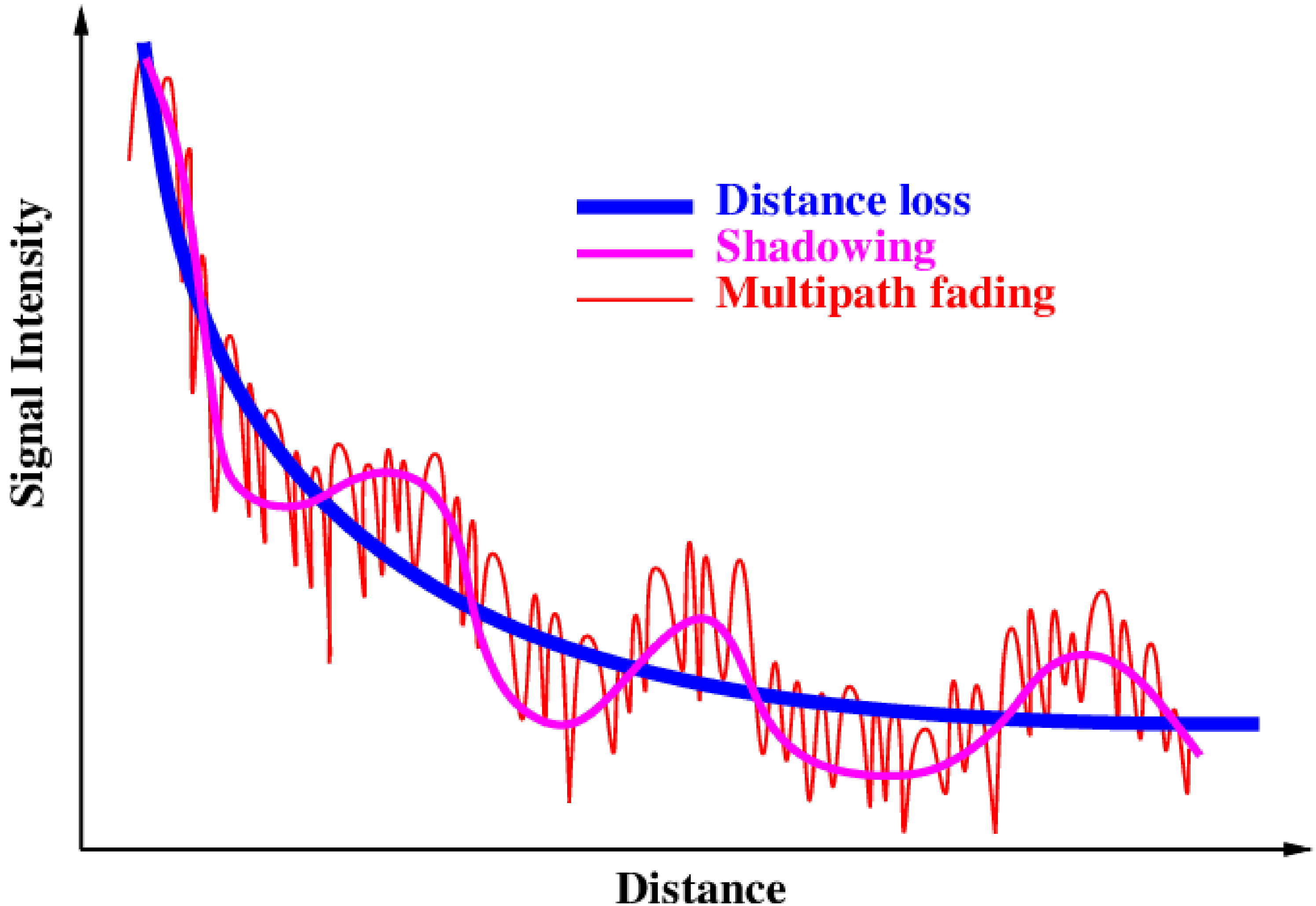
- Wireless is more complicated than the wired case (Surprise!)
  1. Nodes have different areas of coverage – doesn't fit Carrier Sense
     - Asymmetries lead to hidden/exposed terminal problems
  2. Nodes can't hear while sending – can't Collision Detect
     - Transmitter swamps co-located receiver

≠ CSMA/CD

Wireless Propagation

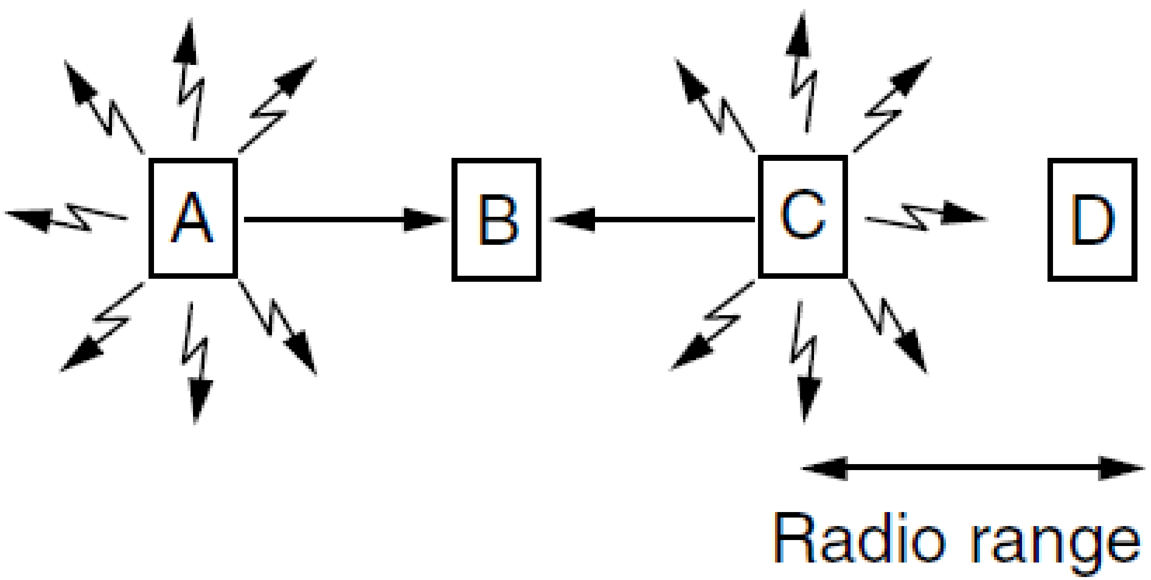
- Difficult due to random, time-varying phenomena
  - The result of signal reflections, diffractions and scattering (multi-path), relative motion (mobile), and shadowing.
- Main Components:
  - Path Loss: attenuation due to distance
  - Shadowing (slow fading): long-term variation of signal caused by obstructions (hills, buildings, mountains, foliage, and for indoor wireless, walls, furniture)
  - Multipath (fast fading): short-term signal variations due to multiple reflections from buildings, walls, and ground.

Wireless Signal

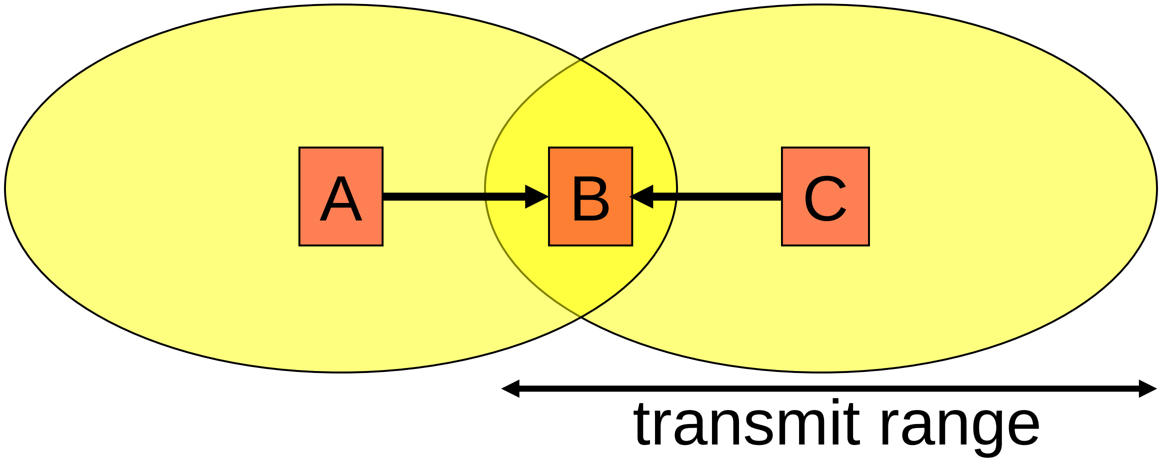


Different Coverage Areas

- Wireless signal is broadcast and received nearby, where there is sufficient SNR

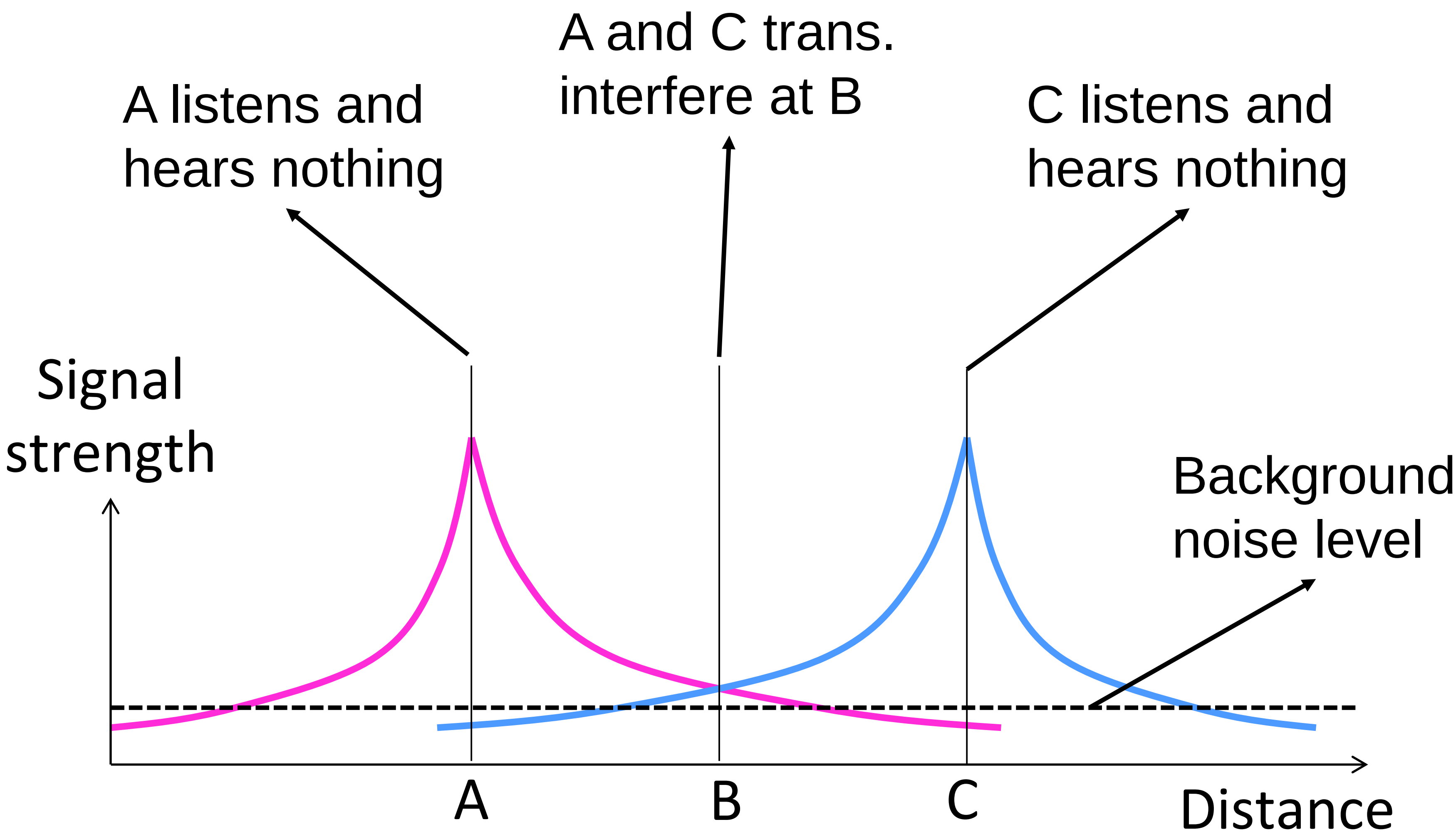


Hidden Terminals

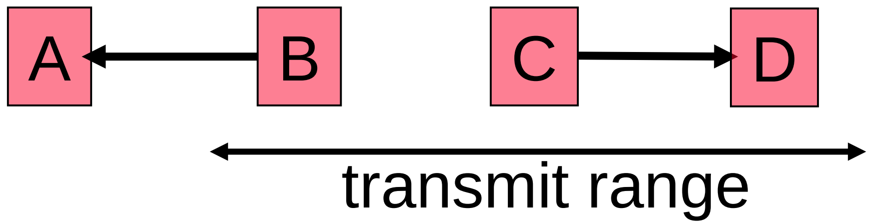


- Nodes A and C are hidden terminals when sending to B
  - Can't hear each other (to coordinate) yet collide at B
  - We want to avoid the inefficiency of collisions
- CSMA will be ineffective – want to sense at receiver

Hidden Terminals (2)

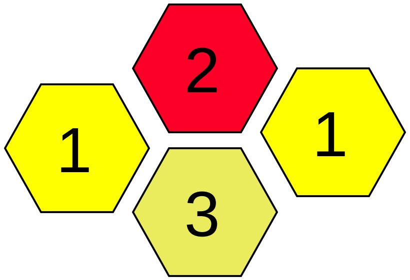


Exposed Terminals



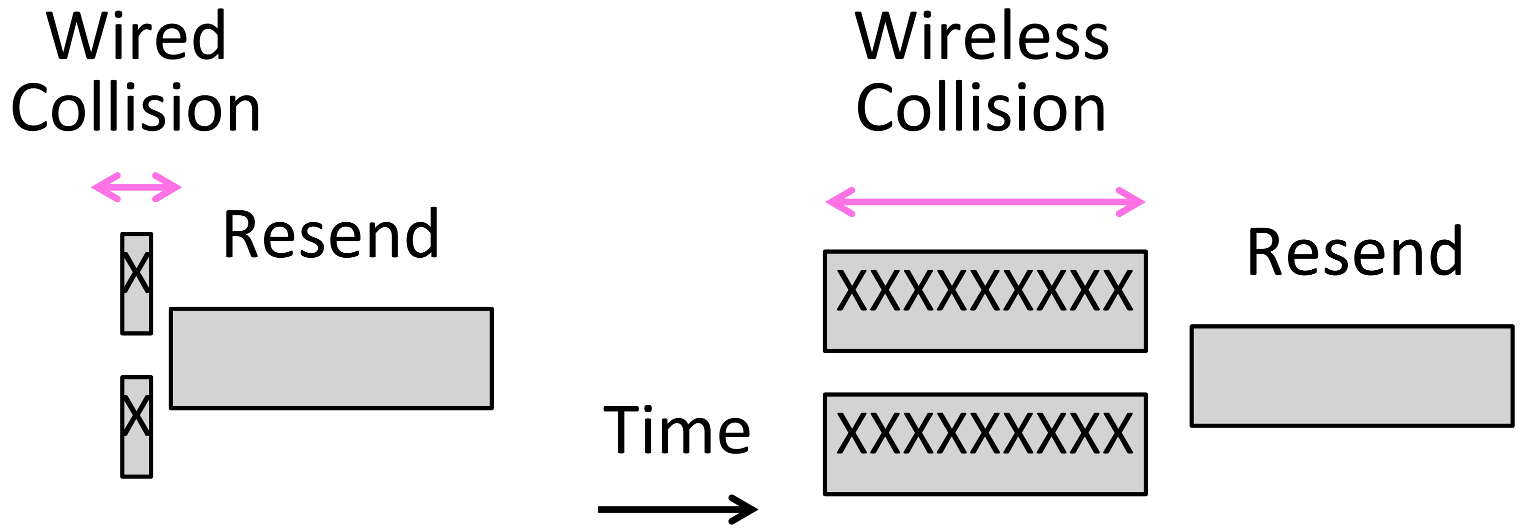
- B and C are <u>exposed terminals</u> when sending to A and D
  - Can hear each other yet don’t collide at receivers A and D
  - We want to send concurrently to increase performance

- Compare to spatial reuse in cell phones:



Nodes Can't Hear While Sending

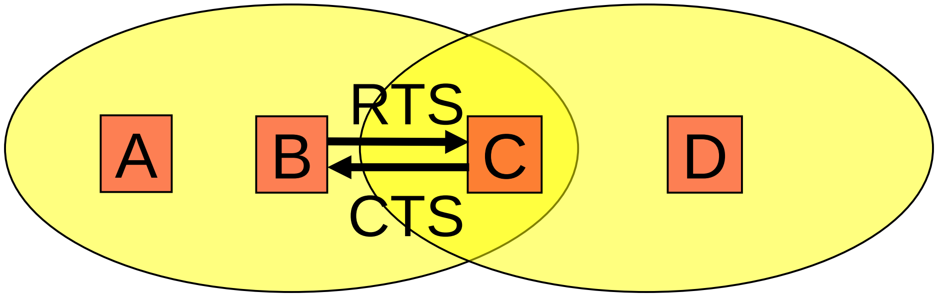
- With wires, detecting collisions (and aborting) lowers their cost
- More wasted time with wireless



CSMA with Collision Avoidance (CA)

- Since we can't detect collisions, we avoid them
  - CSMA/CA as opposed to CSMA/CD
  - Not greedy like Ethernet
- CD: listen before transmitting
  - When medium busy, choose random backoff interval
  - Wait for that many idle timeslots to pass before sending
- CA: transmit short "jamming" signal before sending frame
  - essentially reserves medium, let's others know your intent to transmit
- Collisions can be inferred
  - Use CRC and ACK from receiver to infer "no collision"
  - on collision, binary exponential backoff like Ethernet

RTS / CTS Protocols (MACA)



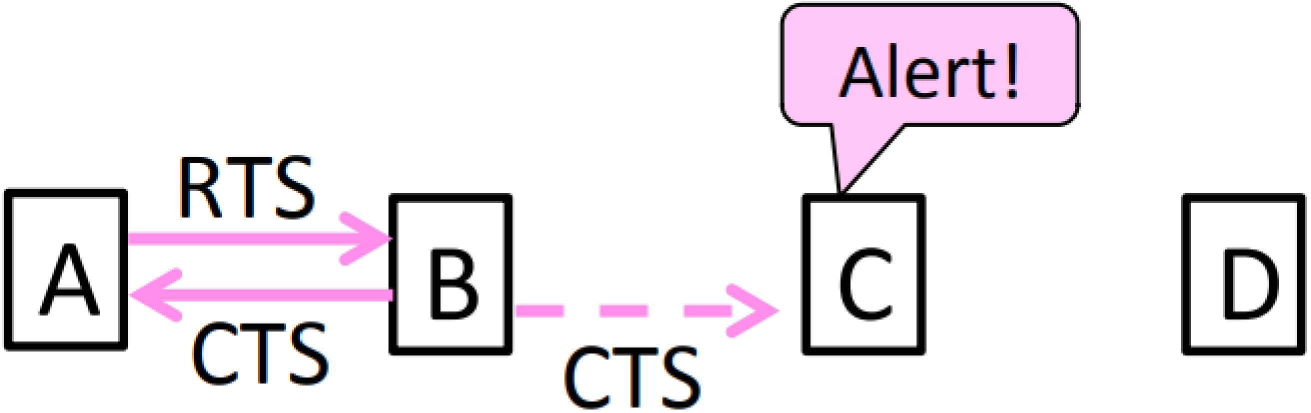
- MACA uses a short handshake instead of CSMA (Karn, 1990)
  - 802.11 uses a refinement of MACA (later)
- Protocol rules:
  1. A sender node transmit a RTS (Request-To-Send, with frame length)
  2. The receiver replies with a CTS (Clear-To-Send, with frame length)
  3. Sender transmits the frame while nodes hearing the RTS or CTS stay silent
  - Collisions on RTS/CTS are still possible, but less likely; RTS/CTS ***ameliorates*** hidden terminal problems

MACA – Hidden Terminals

- A → B with hidden terminal C
  1. A sends RTS, to B

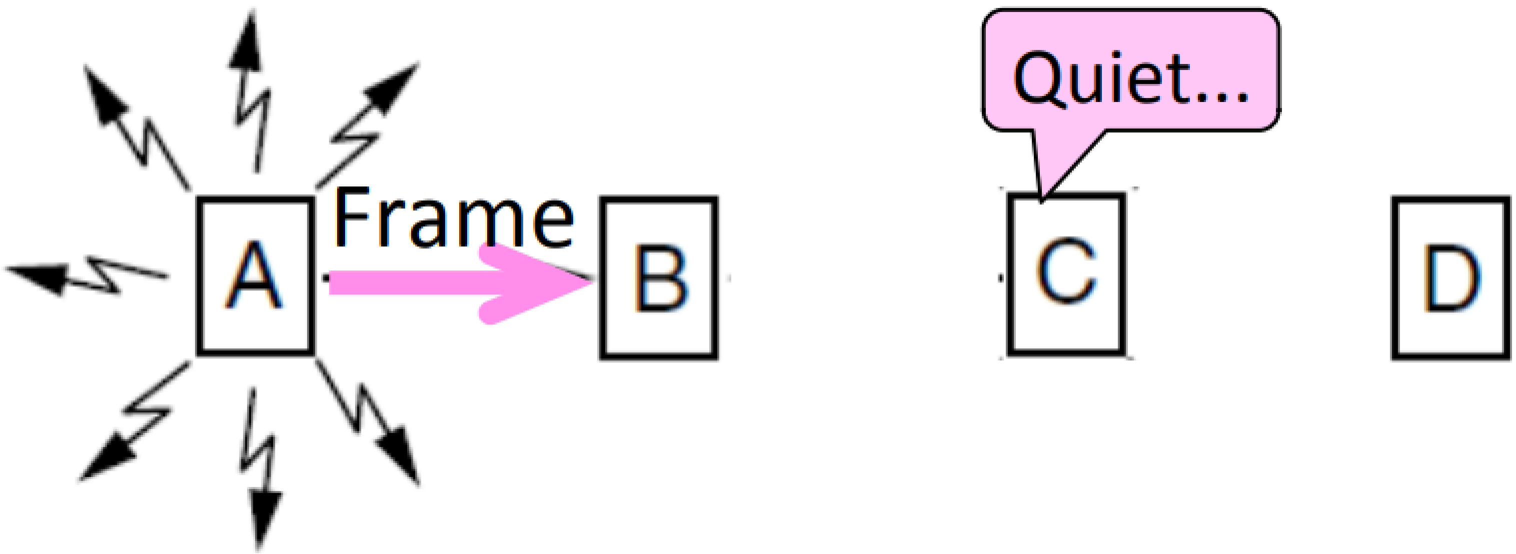
MACA – Hidden Terminals (2)

- A → B with hidden terminal C
  2. B sends CTS to A, and C too



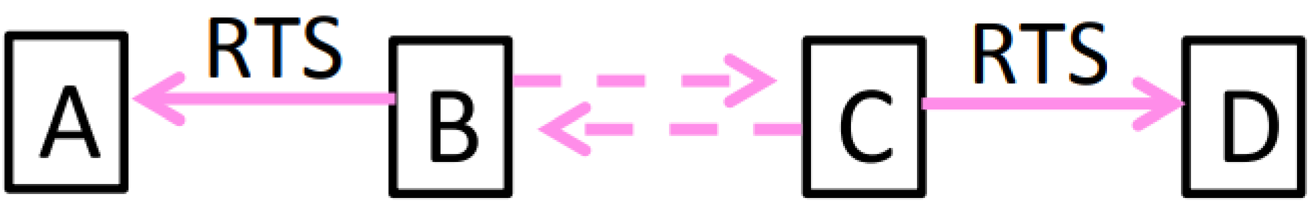
MACA – Hidden Terminals (3)

- A → B with hidden terminal C
    3. A sends frame while C defers



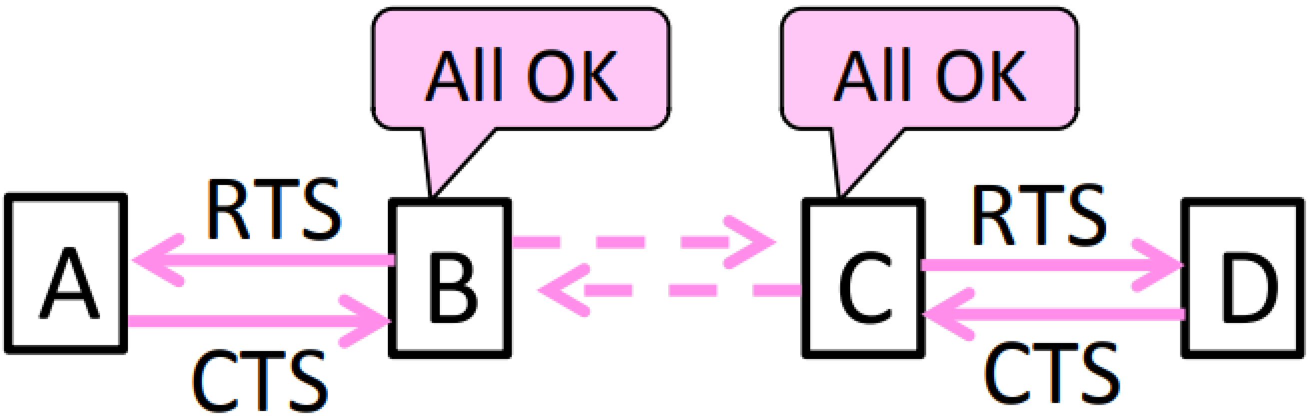
MACA – Exposed Terminals

- B → A, C → D as exposed terminals
  1. B and C send RTS to A and D



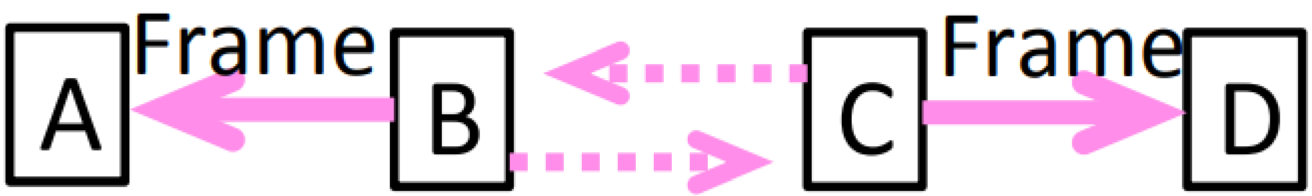
MACA – Exposed Terminals (2)

- B → A, C → D as exposed terminals
  2. A and D send CTS to B and C



MACA – Exposed Terminals (3)

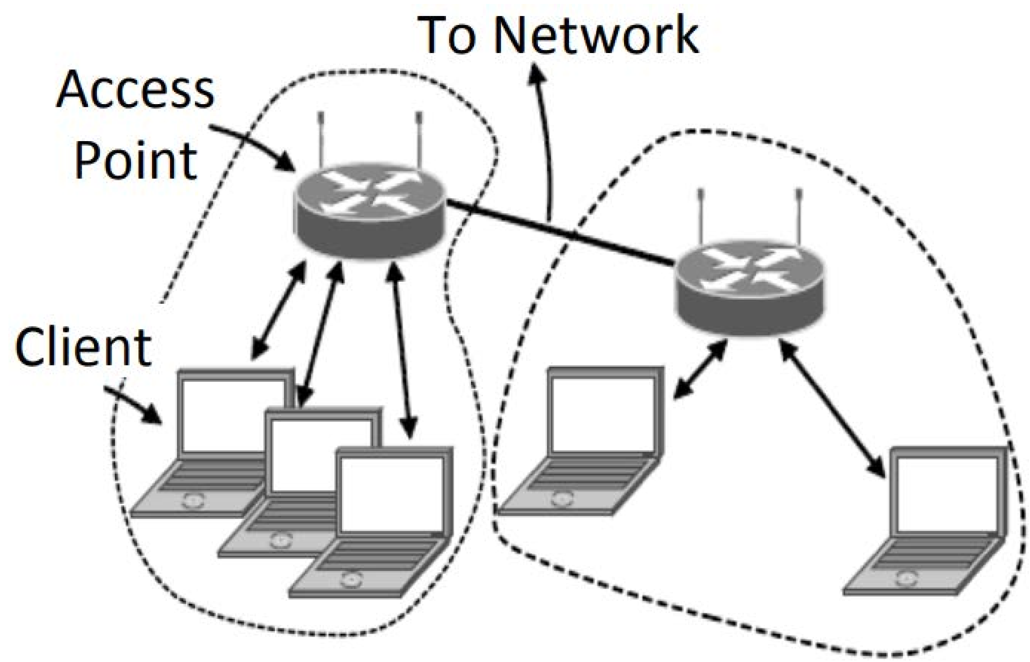
- B → A, C → D as exposed terminals
    3. B and C send frames to A and D



- What is the main assumption? May it break?

802.11, or WiFi

- Very popular wireless LAN started in the 1990s
- Clients get connectivity from a (wired) AP (Access Point)
- It's a multi-access problem ☺
- Various flavors have been developed over time
  - Faster, more features



802.11 Physical Layer

- Uses 20/40 MHz channels on ISM bands
  - 802.11 b/g/n on 2.4 GHz
  - 802.11 a/n on 5 GHz

- OFDM modulation (except legacy 802.11b)
  - Different symbols use different amplitude/phases for varying SNRs
  - Rates from 6 to 54 Mbps plus error correction (FEC)
  - 802.11n uses multiple antennas; See “802.11 with Multiple Antennas for Dummies” by Halperin et. al.

802.11 Link Layer

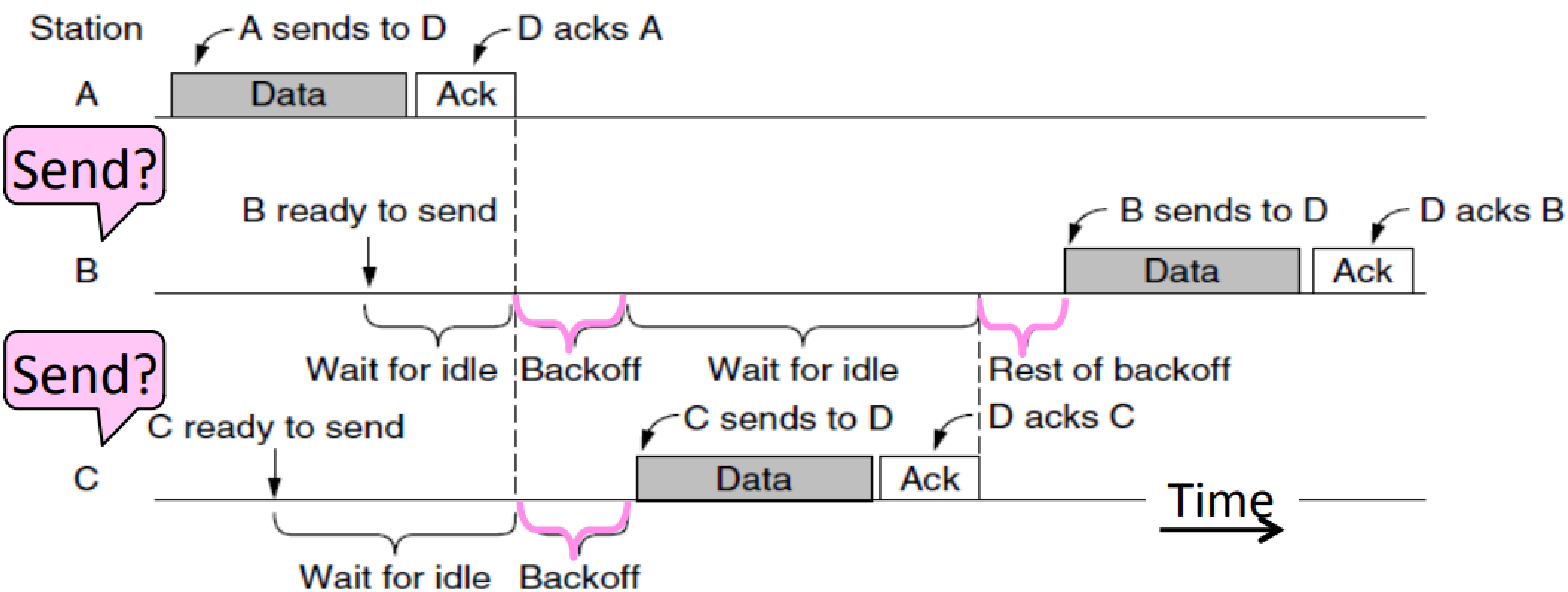
- Multiple access uses CSMA/CA (next); RTS/CTS optional
- Frames are ACKed and retransmitted with ARQ
- Funky addressing (three addresses!) due to AP
- Errors are detected with a 32-bit CRC
- Many, many features (e.g., encryption, power save)

Packet from Network layer (IP)

	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence
Bytes	2	2	6	6	6	2	0–2312	4

802.11 CSMA/CA for Multiple Access

- Sender avoids collisions by inserting small random gaps (p-persistence)
  - E.g. when both B and C send, C picks a smaller gap, goes first



The Future of 802.11 (Guess)

- Likely more ubiquitous for Internet connectivity
  - Greater diversity, from low- to high-end devices

- Innovation in physical layer drives speed
  - And power-efficient operation too

- More seamless integration of connectivity
  - Too manual now, and limited (e.g., device-to-device)

Issues with Random Multiple Access

- CSMA is good under low load:
  - Grants immediate access
  - Little overhead (few collisions)
- But not so good under high load:
  - High overhead (expect collisions)
  - Access time varies (luck/unlucky)
- We want to do better under load!

2. Contention-free Protocols

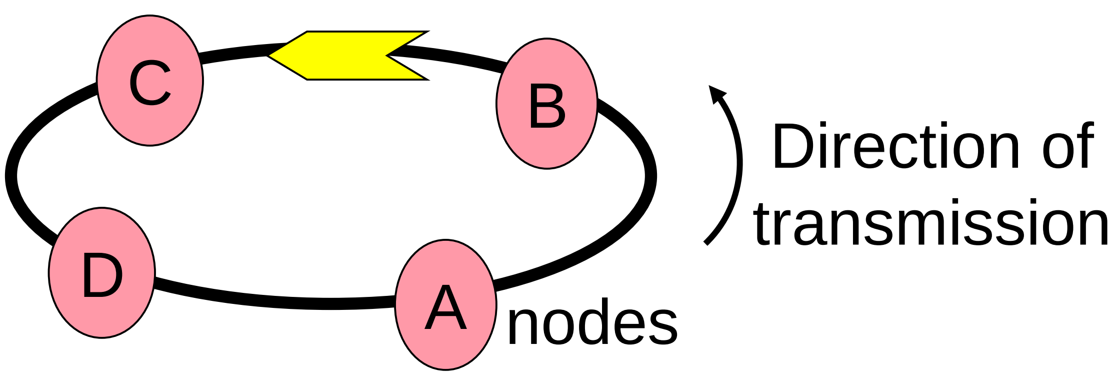
- Collisions are the main difficulty with random schemes
  - Inefficiency, limit to scalability

- Q: Can we avoid collisions?
- A: Yes. By taking turns or with reservations
  - They define an order in which nodes get a chance to send
    - Or pass, if no traffic at present
  - We just need some ordering …
    - E.g., Token Ring / FDDI, DQDB
    - E.g., node addresses (from lowest to highest)

- More generally, what else might we want?
  - Deterministic service, priorities/QOS, reliability

Token Ring (802.5)

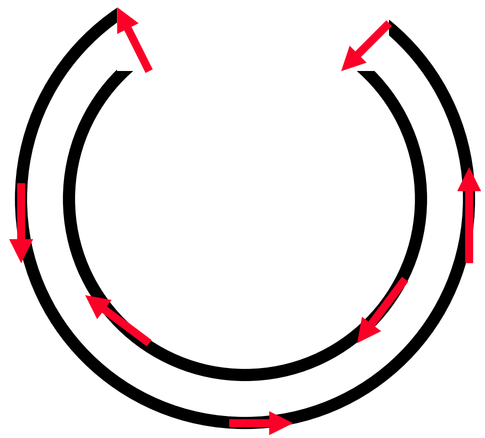
- Arrange nodes in a ring
- Token rotates “permission to send” to each node in turn
- Sender injects packet into ring and removes later
  - Maximum token holding time (THT) bounds access time
  - Early or delayed token release
  - Round robin service, acknowledgments and priorities
- Monitor nodes ensure health of ring



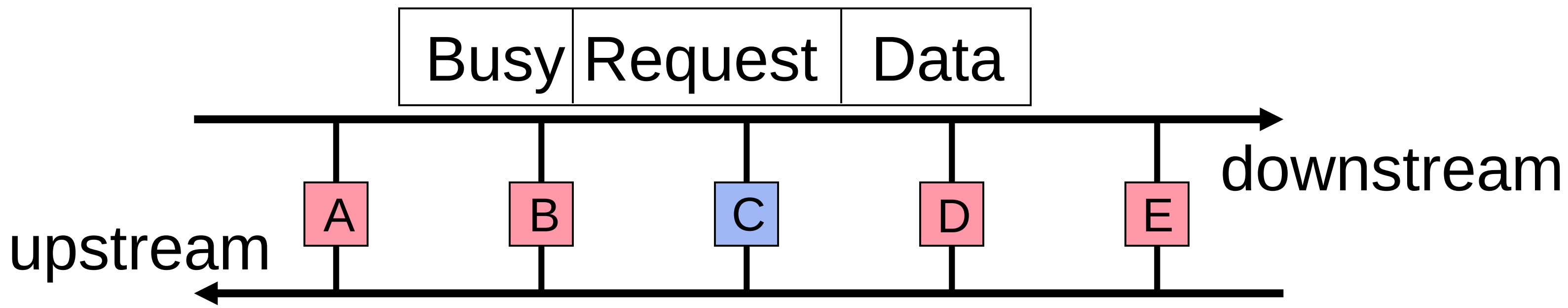
FDDI (Fiber Distributed Data Interface, 802.4)

- Roughly a large, fast token ring
  - At the time (circa 80's-90's),100 Mbps and 200km vs 4/16 Mbps and local (802.5)
  - Dual counter-rotating rings for redundancy
  - Complex token holding policies for voice and video traffic
  - It is really a token bus, i.e. a virtual token ring
    - implies knowledge of neighbors and addressing scheme

Break!



DQDB (Distributed Queue Dual Bus, 802.6)



- Two unidirectional buses that carry fixed size cells
  - Cells are marked busy/free and can signal a request too
- Nodes maintain a distributed FIFO queue
  - By sending requests they are reserving future access

DQDB Algorithm

- Two counters per direction (UP, DN)
  - RC (request count), CD (countdown)
- Consider sending downstream (DN):
  - Always have RC count UP requests, minus free DN cells if larger than zero
  - This is a measure of how many others are waiting to send
  - To send, copy RC to CD and set RC to zero, then decrement CD for each free DN cell, send when zero
  - This waits for earlier requests to be satisfied before sending
- Highly scalable, efficient, but not perfectly fair. Why?

Turn-Taking Advantages

- Fixed overhead with no collisions
  - More efficient under load
- Regular chance to send with no unlucky nodes
  - Predictable service, easily extended to guaranteed quality of service
  - Priorities and reservations

Turn-Taking Disadvantages

- Complexity
  - More things that can go wrong than random access protocols!
    - E.g., what if the token is lost?
  - Higher overhead at low load

Turn-Taking in Practice

- Regularly tried as an improvement offering better service
  - E.g., qualities of service
- But random multiple access is hard to beat
  - Simple, and usually good enough
  - Scales from few to many nodes

Key Concepts

- Wireless communication is relatively complex
  – No collision detection, hidden and exposed terminals
- There are contention-free MAC protocols
  – Based on turn taking and reservations, not randomization