# Medium Access Control

# Fundamental Problem

- *N* nodes in vicinity want to transmit (to, say, *N* other nodes).
- How to do this "interference free"?
  - Interference free means SINR $\geq \beta$
- Otherwise, we say that packets collide.
- Assume a simple but common scenario: All nodes are so close that *two simultaneous transmissions will always collide*. Also, assume that they are all in the same channel.

# General Solution

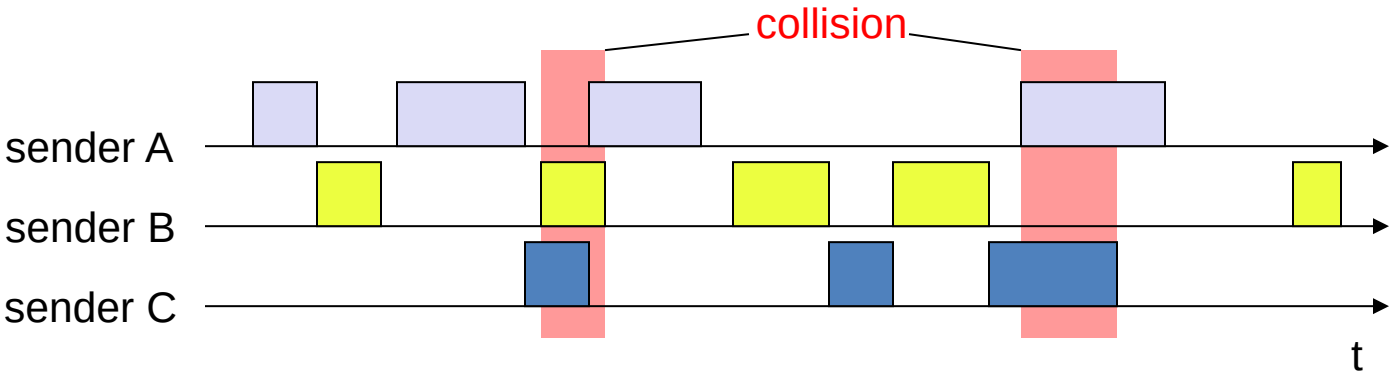
- *Multiplex* transmissions over time.
- Coordinated access:
  - Each node is somehow "scheduled" to transmit in certain intervals of time.
  - Schedule chosen to avoid collision of simultaneous transmissions.
  - Problem: Who does the coordination? How? Need a "coordinator". Need to know who has packet when and who collides with whom.
- Random access:
  - Simple alternative. Nodes transmit at random times.
  - Simply hope that they do no collide.
  - We discuss random access first.

# Aloha Protocol (Slotted and Unslotted)

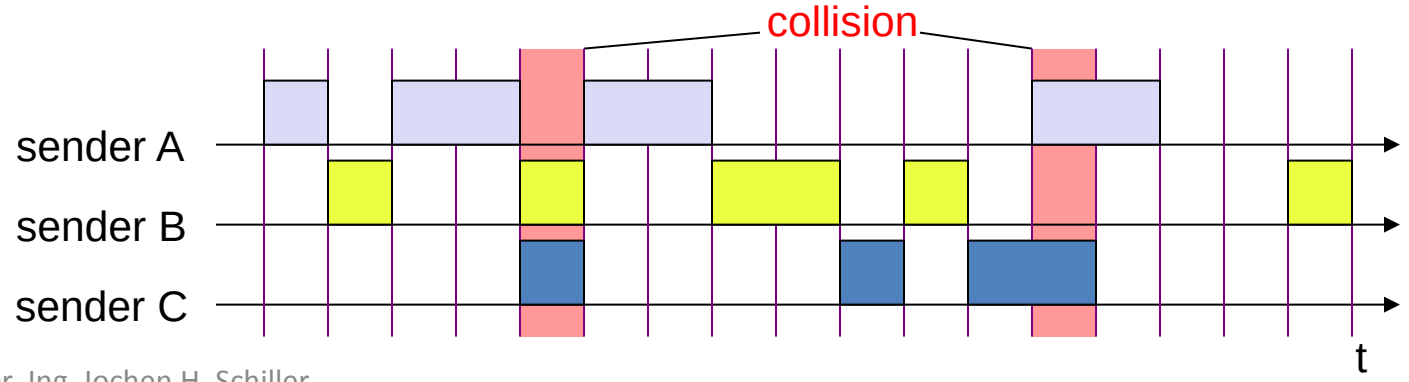
- The most primitive random access protocol
  - Originally invented in the 70s and a pre-cursor of many advanced designs later.
  - Still used in modified form in ultra low –power communications, e.g., RFID.
- Protocol: Transmit packets immediately (if not transmitting already).
- Appears random as packets are generated randomly.
- Slotted version assumes that packet transmissions are synchronized with time slots.

# Aloha Protocol Example

- Aloha




- Slotted Aloha



# Slotted Aloha

- One slot = one packet
- Each slot has one of three states
  - Successful (S): Exactly one node transmits.
  - Collision (C): More than one node transmits.
  - Idle (I): No node transmits.
- Assume that each node transmits in a slot with probability $p$. The #nodes is $n$.
- Normalized throughput

  = throughput / capacity

  = #successful slots/ total #slots (think why?)

  = Prob. of a slot being successful.

# Performance

- Max. possible normalized throughput is 36% (18%) for slotted (unslotted) Aloha when #nodes is very large.
- This is obviously too poor.
- However, the protocol is still very attractive in IoT devices when
  - device is resource constrained and simple protocols are favored.
  - Poor throughput is acceptable.

# Carrier Sense Multiple Access (CSMA)

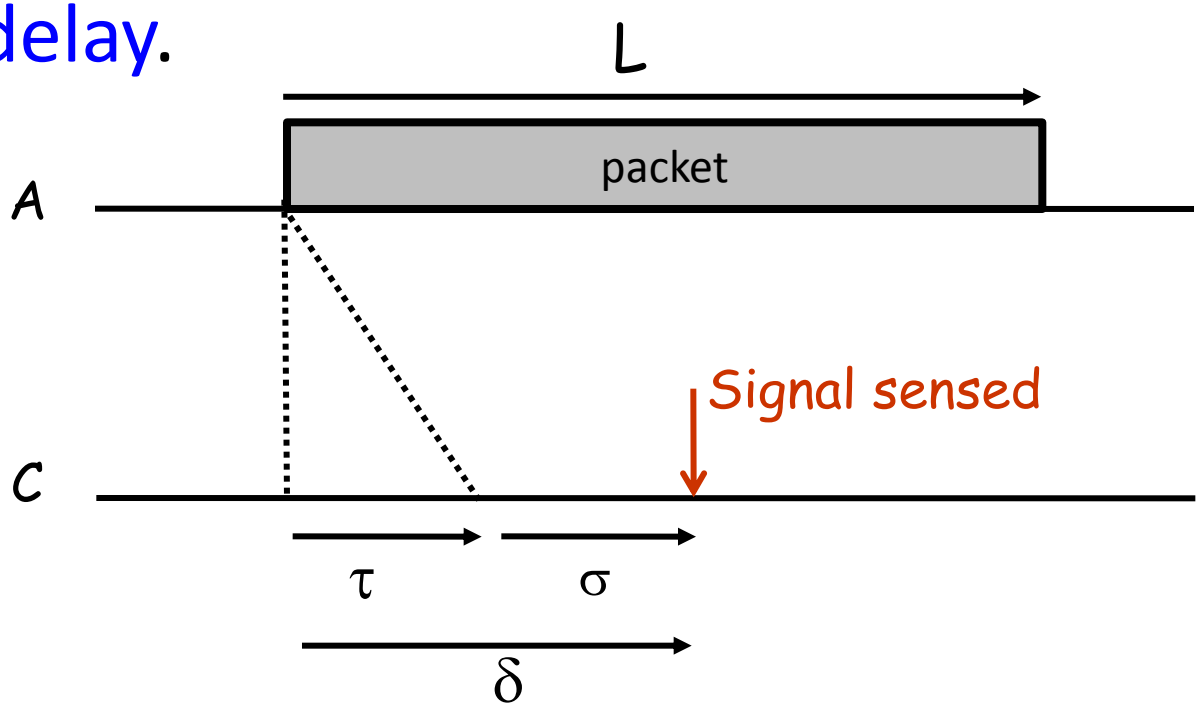
- How to improve throughput?
- Avoid collision. Listen before talk. A node may transmit only when the medium is sensed idle.
- Need to implement channel sensing. Also, called carrier sensing. In standards, sometimes also called clear channel assessment (CCA).

# Carrier Sensing

- Typically performed via energy (or power) detection.
- Potential implementation:
  - Listen to channel and measure the received power.
  - If power exceeds given threshold, channel busy.
  - This threshold is called carrier sense threshold $P_{CS}$
- It takes non-zero time to sense carrier. Called carrier sensing delay.

# Slotted CSMA Protocol

- Packet size = *L* (in time units).
- Slot size = $\delta = \tau + \sigma$, where $\tau$ is worst case propagation delay and $\sigma$ is worst case carrier sensing delay.



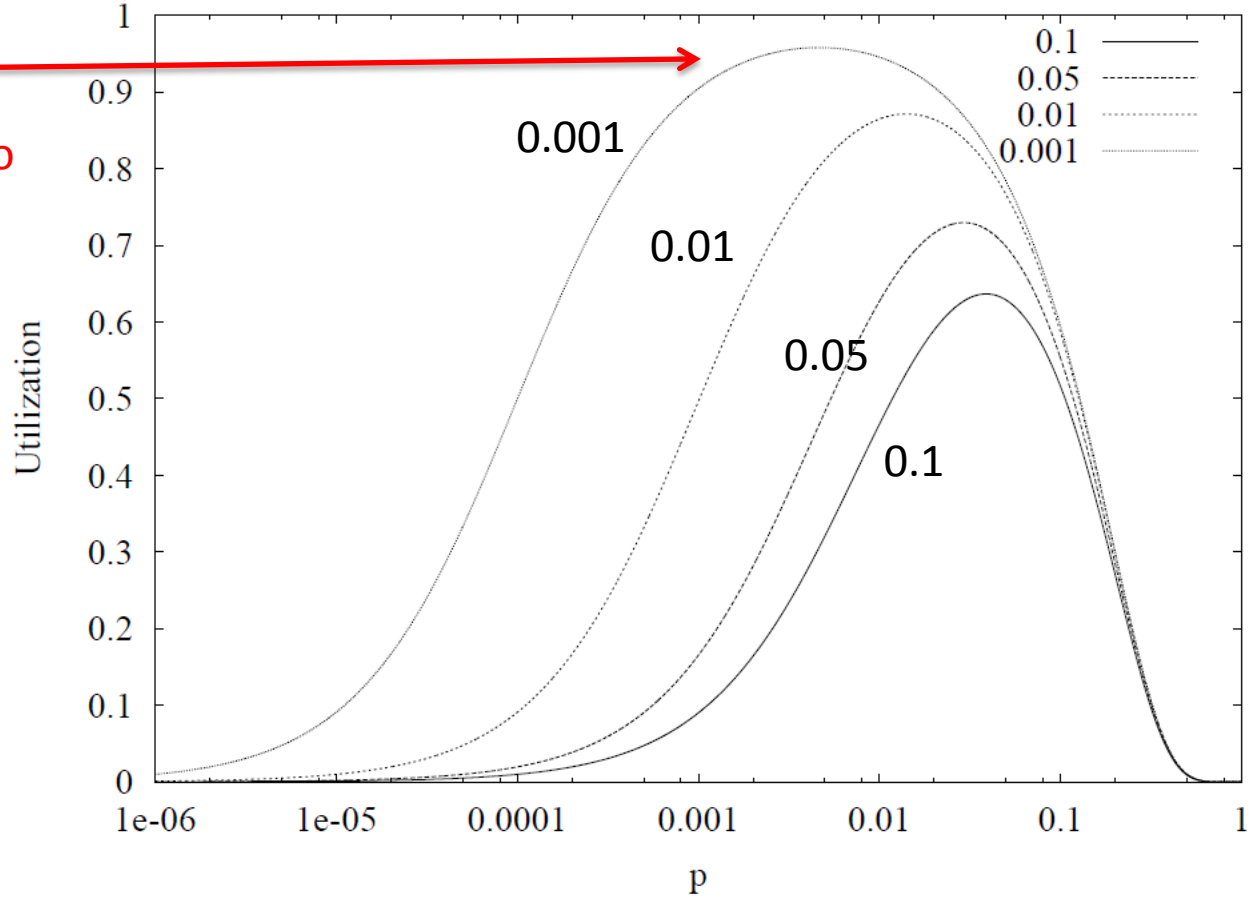
# *P*-persistence

1. If wish to transmit in a slot *i*, sense carrier first.
2. Channel busy -> go to next slot *i+1*.
3. Channel idle -> still go to next slot *i+1*. (Note channel sensing can take a whole slot.) Transmit with probability *p* in slot *i+1*.

   (Note that *p =1* may result in a lot of collisions).
4. If no transmission, still sense carrier. Repeat.

# Numerical Results

Very good performance provided packets are large compared to slot




Various values of $\delta/L$ are chosen from 0.001 to 0.1

Of note, $L/\delta$ is packet size in slots

$n = 10$

[Utilization is same as normalized throughput]

[From Nitin Vaidya's notes]

# Backoff

- Backoff is a simple way to implement p-persistence in practical protocols.
- Backoff = number of valid transmission opportunities skipped before actual transmission.
- Randomly chosen, but bounded.
- Example:
  - Backoff interval is chosen uniformly at random in range [Bmin, Bmax].
  - Initialize a counter by this value.
  - Decrement counter after each slot at each valid transmission opportunity (i.e., slot detected idle).
  - On a valid opportunity, if counter 0, transmit.

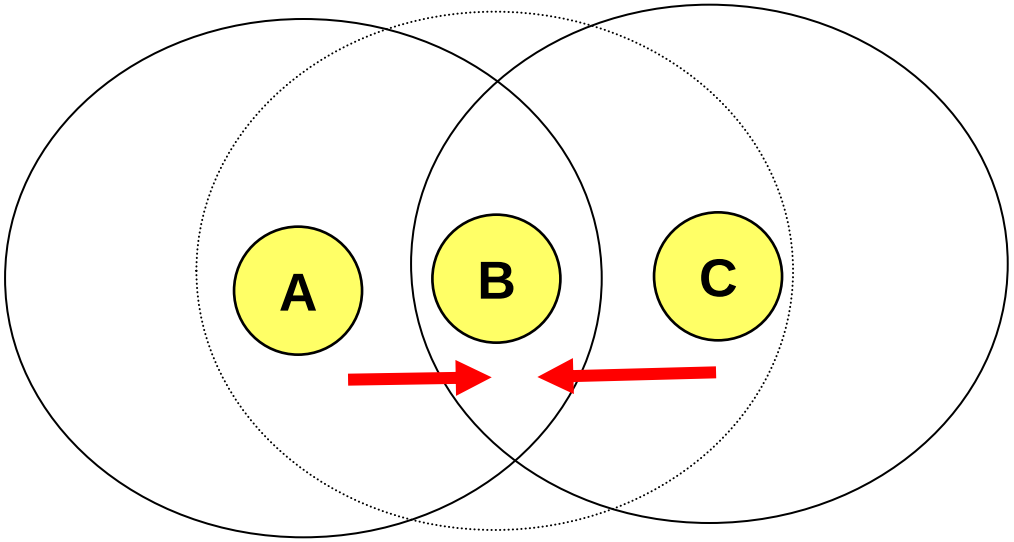
# Responding to Packet Losses

- Packet losses can occur due to collisions. Multiple nodes can decide to start transmission in the same slot.
- To reduce collision, access probability (p) must be reduced.
  - Can be achieved by increasing the window over which the backoff interval is chosen.
  - Exponential backoff: [0,cw-1] -> [0,2*cw-1] on packet loss.

# Network Assumptions

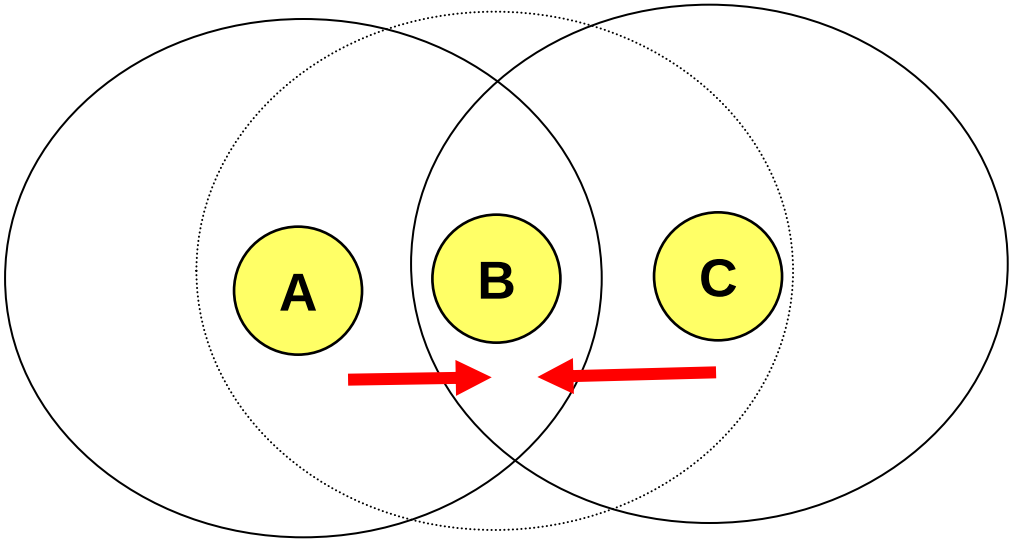
- Recall our assumption so far has been that nodes are close such that two simultaneous transmissions will always collide.
- This also means that any two nodes that may collide also carrier sense each other.
- We have seen that collisions are still possible.
  - But randomization was used to reduce this possibility.
- Now, we consider the possibility that two nodes may not be able sense each other's carrier, but their transmissions could still collide.

# Hidden Terminals



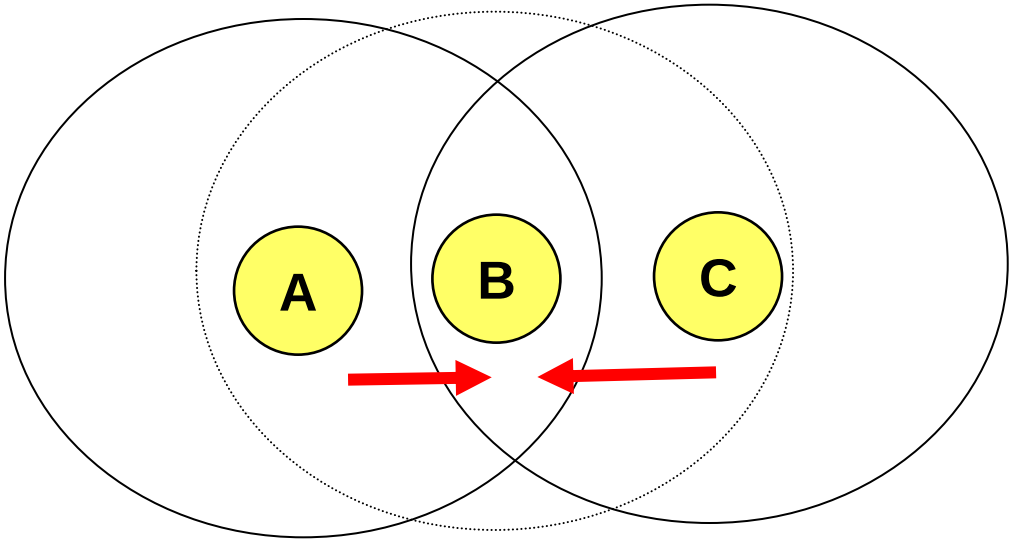

- A and C cannot carrier sense each other. But their transmissions can collide at B.
- A and C are hidden terminals.
- A CSMA-based protocol will cause frequent collisions.

# Observation



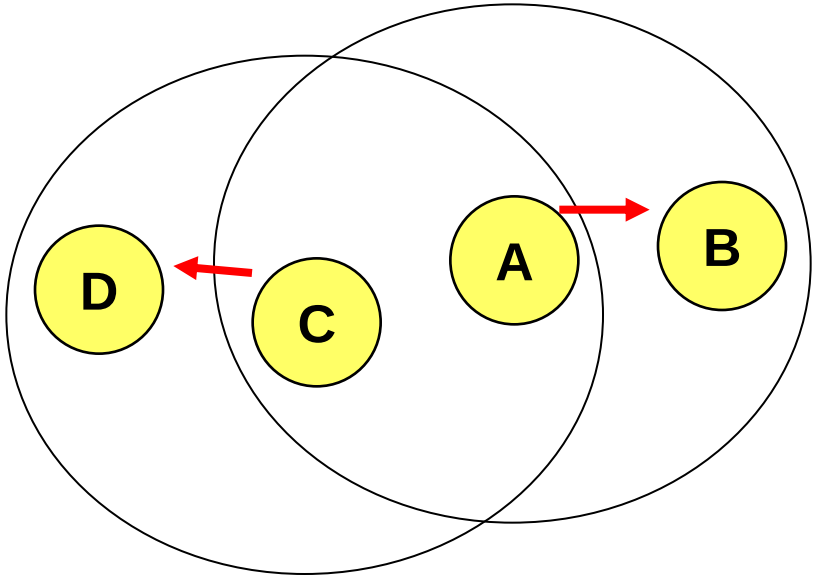

- The real issue is that carrier sensing is done at transmitter. But collision happens at the receiver.
- Information asymmetry: Information available at transmitter and receiver are not the same.

# Simple Solution



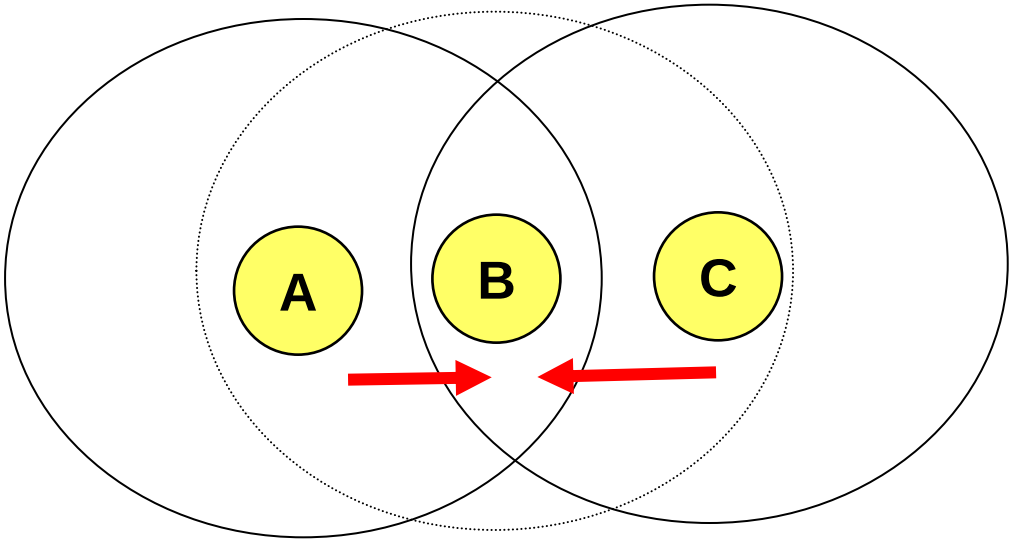

- Make carrier sensing more sensitive.
- Thus, both A and C will actually sense each other.
- Works, but this worsens another problem.

# Exposed Terminal Problem




- In principle, A->B and C->D transmissions can go in parallel without collisions.
- But A and C can hear each other. C will wait for A->B to end before starting C->D.
- A and C are “exposed” terminals.
- More sensitive carrier sensing increases exposed terminal problem.

# More Involved Solutions to Hidden Terminal Problem



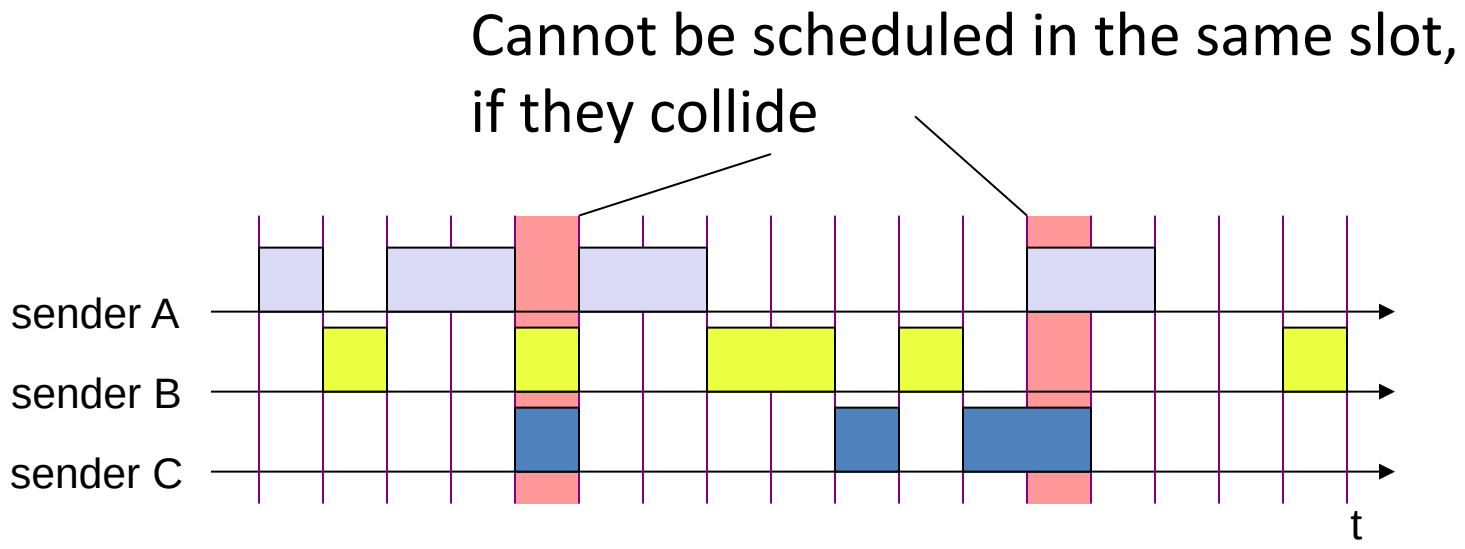

- Virtual carrier sensing – implement carrier sensing at the receiver via additional control messaging.
- Busy tone approach – a receiver when busy receiving emits a tone. Transmitters carrier sense on this tone.

# Summary So Far

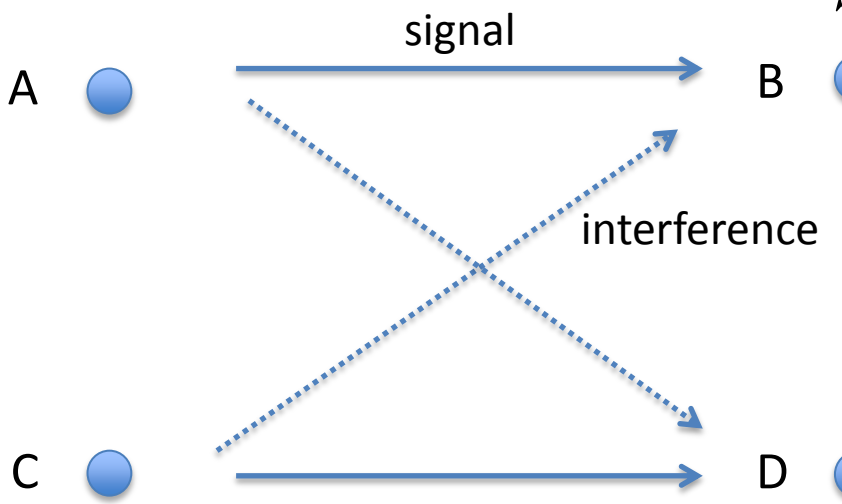
- Random access protocols are attractive for IoT for simplicity of implementation and completely distributed operation.
- Standard: IEEE 802.15.4 personal area network standard is based on CSMA protocol ideas discussed.
  - Zigbee is based on this.

# Alternative: Scheduled Access

- Suppose time is slotted. Schedule transmissions in slots so that they do not collide.



# Recall Example




$$SINR = \frac{\frac{KP_A}{d_{AB}^{\alpha}}}{N + \frac{KP_C}{d_{CB}^{\alpha}}}$$

$$\alpha = 2$$

$$SINR = \frac{\frac{KP_C}{d_{CD}^{\alpha}}}{N + \frac{KP_A}{d_{AD}^{\alpha}}}$$

If the SINR condition is not satisfied, we say that packets “collide.”

If A->B and C->D transmissions collide, they must be scheduled in a different slot.

# TDM Scheduling

- TDM = Time Division Multiplexing
- There must be a central scheduler – e.g., an access point that must know
  - Who can collide with whom
  - Who has packets to send

  and allocate slots accordingly.
- Advantages: No collisions at all. Also, can conserve power easily – just switch off when no slots scheduled.
- Disadvantage: Need a scheduler that must know interference and traffic information.

# Summary So Far

- We covered
  - Physical layer
  - Medium access protocols

  targeting wireless short range networks
- In the next lecture, we will cover
  - Routing layer
  - Localization
  - RF-powered backscatter networks