Outline

Wireless MAC issues
Specific wireless network technologies

Transmission model

Signal strength varies over space, due to:
- Path length
  - e.g. omnidirectional antennas: signal strength proportional to inverse square of path length
- Obstructions (e.g. hidden behind a mountain)

In the following slides, signal strength is shown by the intensity of the colour.
Transmission overwhelms local receiver

Since signals spread as they propagate, $P_{rx} \ll P_{tx}$
- e.g. Cisco 350 series NIC:
  - transmit at 1mW (0dBm) to 100mW (20dBm)
  - receive sensitivity -94dBm (1Mb/s) to -85dBm (11Mb/s)
- $\Rightarrow$ 9 orders of magnitude difference
- local transmission power $\gg$ local power of interference
- (e.g. collision from contending station)
- $\Rightarrow$ can’t detect contention locally.
- $\Rightarrow$ Can’t use Collision Detection.

Solutions:
- Use acks for MAC
  - Lack of ack suggests collision (or noise)
- Collision Avoidance: Reduce probability of collision by:
  - Randomly delaying attempts when collision is likely (immediately after channel is sensed to be free).
  - Exchanging handshake frames (RTS/CTS, whose small size makes them less likely to suffer collisions) before long data frames.

Immediate ACKs for MAC

If the receiver sends an ACK to the source immediately after receiving a frame, then the source can determine if the frame (or the ACK) was lost (e.g. due to a collision).

Notes:
- ACK is not intended for error control, but to help MAC (detect collisions).
- However loss of ACK may also be due to transmission error & this ACK can also be used for error control if needed.
- Receiver must be able to send the ACK without contending for medium access.

Achieve this by using interframe spaces of different lengths, e.g. in 802.11 (numerical examples for 802.11b):
- Short IFS (10µs):
  - Interval between receiver finishing receiving frame and
  - sending ACK.
- DCF IFS (50µs): Minimum time that other prospective sources must wait after source’s transmission before contending for access.
  - $\Rightarrow$ prospective sources contend after ACK is sent
- DIFS > SIFS $\Rightarrow$ prospective sources contend after ACK is sent

Capture effect (aka “near-far problem”)

Signal from far station may have sufficient power to be received if there were no other transmissions, but is “drowned out” by the power of nearby stations.

- $D$ receives strong signal from $S_1$, which overpowers the signal from $S_2$.
- $D$ & $S_1$ are oblivious to $S_2$’s attempt to transmit

Good: Throughout: Don’t waste time on collisions
Bad: Unfair: $D$ & $S_1$ “capture” the channel, preventing access by $S_2$.
Resolve by limiting transmission rates (e.g. $S_1$) to less than channel capacity by introducing random space between frames.

Random delays before data transmission

Contention is likely just after one station finishes transmitting:
- Likely that other stations generated data to transmit during the transmission.
- These stations might politely wait until the end of the current transmission, and then try transmitting simultaneously.

Avoid this by requiring that stations (which sense the channel to be busy) wait a random period of time before each transmission, i.e. non-persistent.

Random $\Rightarrow$ one station with freshly generated info will (probably) transmit first; other will sense activity & defer
Prevent one station deferring indefinitely to others by accumulating time deferred $\Rightarrow$ freeze timer while other stations are transmitting & attempt to transmit when cumulative time reaches selected random period.

Compare with Ethernet, which has random backoff only after collision.
Here, backoff occurs before transmission, but also increases exponentially after collisions.
802.11 implementation of random delays

Time is measured in "slots" (20µs for 802.11b)
Prospective source that senses channel to be busy:
1. Randomly selects a Contention Window, initially in the range \([0,7]\) slots, with range doubling after each collision \([0,15], [0,31], \ldots\).
2. Decrements its CW for each slot time after the channel has been idle for a DIFS.
3. Attempts to transmit when \(\text{CW}=0\)

![Diagram](image)

\[\text{Source 1} \quad \text{Source 2} \quad \text{Source 3}\]

- \(\text{CW}=7\) DIFS 5 4 3 2 1 0
- \(\text{Source 2} \quad \text{Source 3} \quad \text{Source 1}\)

| = transmitting | = generates frame to transmit | = empty slot |

*Varying this range is another way to prioritise sources.*

Time-varying channel

Destination may not be able to receive source's signal:
• If it's mobile, it may move out of range
• Even if it's stationary: May not be able to receive signal because of time-varying channel qualities (e.g. attenuation from passing obstruction)

⇒ Before the source invests time in transmitting a long frame, it might want to check \(\bullet\) that the destination is reachable.
1. Source sends Request To Send (RTS) signal to destination.
2. Destination replies to any RTS that it receives when ready with a Clear To Send (CTS) signal.

Hidden terminal problem

Success of a transmission is determined by interference at the receiver, but MAC decisions are made on the basis of information available at the transmitters.

\(S_1\) and \(S_2\) are out of range of (hidden from) each other, but their transmissions interfere at \(D\).

Because the sources can't detect the collision, they continue transmitting, wasting transmission time.

*Also "Hidden node" or "Hidden station" problem.*

Hidden terminal solutions

An early solution was Busy Tone Multiple Access, in which a receiver would emit a continuous busy tone on a frequency (different from that on which it is receiving) and prospective sources had to check for a busy tone before transmitting.
Hidden terminal solutions: RTS/CTS

Idea: Get the destination to transmit a signal informing stations near it that it needs the channel for a certain interval.

Implementation: Stations record when they shouldn’t transmit because it is needed for local reception. Formal names for this record: "Virtual Carrier"/"Network Allocation Vector".

They learn this information by:
1. Source sends Request To Send (RTS) to destination, indicating expected duration of transmission.
2. Destination sends Clear To Send (CTS) signal (indicating remaining duration) to its locality & source.
3. Other recipients of RTS remain silent long enough for source to receive CTS.
4. Recipients of CTS suppress transmissions for indicated duration.
5. If the source doesn’t receive a CTS, it backs off (waits) for a random duration, and tries again.

Exposed terminal problem

An exposed terminal is within range of the transmitter, but not within range of the receiver.

* S1 wants to transmit to D1, and S2 to D2.
  * S1’s transmission won’t interfere at D1.
  * can be concurrent with S1’s transmission
  * S2 hears carrier from S1 (S2 is exposed).

Dealing with exposed terminals

**Theory:** Modify RTS/CTS
- S2 hears RTS from S1, but not the CTS from D1.
- Deferring tx in response to RTS, causes S2 to unnecessarily defer
- Defer only in response to CTS.

**Practice:** (e.g. 802.11) Use conventional RTS/CTS
- If transmissions are bidirectional (e.g. D1 asks S2), then need to briefly suspend transmission near source.
- 802.11 is conservative & stations defer if they received either RTS or CTS.
Lecture summary

- Spatial variation of wireless signal strength makes it hard to detect collisions (at the receiver – where they count)
- Various solutions, each introducing an overhead that is not always warranted
  - acknowledgements to detect collisions
  - random delays before transmitting after another station
  - RTS/CTS exchanges