3: Multiple Access

Thursday 26th of October, 2017

Intro

Multiple nodes are trying to access the network at the same time. This only applies on some nodes. Point-to-point nodes never have multiple people transmitting at the same time, but broadcast networks (some ethernet, wifi) will – they need multiple access control.

Most long-distance connections are point-to-point between two machines and full duplex, so both devices can send and receive freely.

Multiple Access Protocols

In a shared broadcast channel, if two or more nodes transmit at once, we get interference. (A collision is when a node receives two or more signals at the same time.)

Ideally you want a distributed algorithm. Communication about channel sharing must use the channel itself – there's no out-of-band channel for co-ordination.

Ideal Multiple Access Protocol

1. When one node wants to transmit, they can send at the data rate of the channel.
2. When M nodes want to transmit, each can send at an average rate R/M
    - R is the data rate
3. Fully decentralised
    - no special node for co-ordination of transmissions
    - no synchronisation of clocks
4. Simple

In general, we won't get this, instead having some level of compromise.

Taxonomy of MAC Protocols

There are three broad classes:

- Channel Partitioning
  - divide channel into smaller pieces (typically time slots)
  - allocate piece to node for exclusive use
- Random Access
  - channel not divided, allow collisions
  - recover from collisions
- [...]

Channel Partitioning

TDMA: time division multiple access

Conceptually simple:

Access to channel is done in *rounds*, which repeat indefinitely. Each station gets a fixed-length slot in each round.

However, it's inefficient – if any stations aren't currently sending, their slots are unused. If only one is sending, it can still only use its own slot.

It's distributed, but it needs synchronised clocks. (Usually there's a guard interval between slots, as it's hard to get clocks perfectly synchronised).

Also large latency with large numbers of slots. Also, how do you decide to allocate slots based on the number of connected devices?

Random Access

Originated in the ALOHA satellite system.

When a node has a packet to send, it transmits at the full channel data rate R. There is no co-ordination among nodes. If two or more nodes transmit at once, there's a collision. Random access MAC protocol specifies how to detect collisions, and how to recover from them (e.g. with delayed retransmissions).

There's a maximum frame length, so that at some point every sender has to move on to a new frame – this facilitates fairness.

ALOHA

Very simple, no co-ordination or synchronisation.

When a frame arrives at the sender's MAC layer, transmit it immediately.

ALOHA suffers from very poor link utilisation for medium to high traffic loads – lots of collisions because there's no co-ordination.

Very good if only one sender is sending – gets full data rate.

Carrier Sensing

Listen before you transmit. If the channel is idle, transmit the frame. If the channel is busy, defer the transmission.

Collisions can still occur – propagation delay means two nodes may not hear each other's transmission in time, and may think the channel is idle. If a collision happens, the entire packet transmission time is wasted.

Link layer technologies have upper bounds on the length between stations, for this reason.

Collision Detection

If you detect a collision, stop sending.

In wired LANs, it's easy to detect collisions – you can compare transmitted and received signal strengths. In wireless LANs, it's much more difficult, because received signals are overwhelmed by transmitted signals. In a wireless network, the distances are harder to define – two people could be in range of an access point but not each other.

CSMA/CD in Classic Ethernet

Classic ethernet isn't used so much anymore.

Jam signal is to point out that the packet is ending prematurely.

Exponential Backoff

Want to introduce non-determinism to prevent repeated collisions.

Wait (K * slot duration), where K is chosen at random. After the first collision, choose K from {0, 1}. After a second collision, choose K from {0, 1, 2, 3}. After each collision, double the range from which K values are chosen.

At some point, if there are still collisions happening, sending will be abandoned, as there are probably problems with the network.

CSMA/CD Efficiency

[...]

Some collisions still can't be detected – take A and B sending very small packets. They stop listening once they're done sending, and the collision happens between when they stop listening and when the packets are received.

Can solve this with a minimum packet size.

CSMA in Wireless Links

There are some problems with using CSMA/CD in wireless networks:

- Signal strength decreases proportionally to the square of the distance between the sender and the receiver.
- The sender could apply carrier sensing and collision detection, but collisions happen at the receiver.
- A sender may not be able to hear other transmissions (so carrier sensing not working)
- A sender may not be able to hear collisions (so collision detection not working)

Hidden Node Problem

Nodes A and C are out of range of each other, but within range of the access point B. They each think the medium is free, and send simultaneously – they can't detect the collision that's happening at the access point.

This doesn't happen in ethernet, because all nodes on an ethernet cable are guaranteed to be within range of one another.

IEEE 802.11 (WiFi)

Very influenced by ethernet, as it was originally a convenient alternative to it.

Devices in a cell communicate with an access point. The access point with the connected devices is called a Basic Service Set. Every BSS has an SSID, and several can share SSIDs.

Wireless Differences from Wired

Communication across even a point-to-point wireless link is much more difficult than a wired link:

- decreased signal strength
- interference from other sources
  - e.g. bluetooth and other devices
- multipath propagation

  - radio signal reflects off objects and the ground, arriving at the destination at slightly different times

802.11 Basics

An inter-frame space is a delay prior to transmitting a frame. There are different IFSs, e.g. DIFS for regular data, and SIFS (which is short) for ACKs.

IFSs can impose a priority – using a shorter space means you get in first.

802.11 CSMA/CA

Uses collision avoidance instead of detection, as detection isn't possible.

Basic mechanism uses Clear Channel Assessment to listen to the medium before transmitting, combined with a random exponential backoff.

If another stations occupies the medium during the back-off time, the back-off timer is paused until the medium is free again. This promotes fairness, as those who've been waiting the longest are most likely to get access to the channel.

This works well, but requires every node to be in range of every other node. We still haven't solved the hidden node problem.

Reservation

The sender reserves a channel, rather than using random access of data frames.

Request-to-send (RTS) packets are broadcast, which are small. They may still collide, but it's less likely. When received, the access point broadcasts a clear-to-send (CTS) packet, showing that someone has reserved the channel. In the hidden node problem, anyone in range of the access point will know that the channel is reserved, so that's solved.

"Taking Turns" MAC Protocols

Channel partitioning MAC protocols share the channel efficiently and fairly at high load, but are inefficient at low load.

Random access MAC protocols are very efficient at low load, but at high load there's overhead from collisions.

"Taking turns" protocols look for the best of both worlds.

Polling

One machine is the controller, and invites/polls other nodes to transmit in turn. Typically the other devices are simple in their logic.

This is fair, but there are some issues:

- overhead of polling
- latency
- single point of failure (controller)

Can detect a controller disappearing by noticing that there haven't been any polling messages in a while, and then use a distributed algorithm to allocate a new controller.

Token Passing

Uses a ring of connected devices.

Control token is passed from one node to the next sequentially. Once a packet has been sent, and makes its way around the ring back to you, you release the token and pass it to the next device in the ring.

Token needs to be regenerated if someone goes offline while holding it, need a distributed algorithm for that. It's also possible, though unlikely, that the token could get corrupted during transmission.

Summary

These do offer kind of the best of both worlds, but are not as efficient at either end as purely random-access or purely […].

They're used in some situations: […]