**THESE NOTES ARE NOT COMPLETE/CHECKED AND COULD DO WITH UPDATING. I’LL GET ROUND TO IT OVER THIS WEEKEND BUT ANYONE FEEL FREE TO AMEND/ADD TO THEM**

**Broadcast Networks- multiple access protocols**

1. Station model - N independent stations - generating packets at random times
2. Single Channel - All stations can transmit/receive on it
3. Collision Assumption - If two frames overlap in time, they are both lost
4. Can stations detect current transmission? Yes, if using carrier sense we can detect busy channel. Otherwise no carrier sense
5. Time model - Continuous or slotted

Communications usually provide access to several users concurrently.

* FDMA
* TDMA
* CDMA
* OFDMA - Orthogonal
* Spatial division multiple access

**Pure Aloha**

Stations transmit whenever they have data to transmit (completely arbitrary). Success is detected by listening to the channel, or by acknowledgement. If the frame is destroyed, re-transmit after a **random** delay, to prevent continuous collisions. Aloha is a ***contention*** (fighting?) system, as everything has to fight for the channel. Pure ALOHA uses a continuous time model.

**Slotted Aloha**

Uses a slotted time model by synchronizing. Much more throughput than pure aloha.

Fewer collisions occur.

ALOHA overall works well with a small load, but not suited for intensive networks.

**Carrier-Sense Multiple Access**

Listen before you speak!

Aggressive transmission algorithms:

* If someone is talking, wait to finish before speaking. If collision occurs, wait a random time, and transmit again, unconditionally- **1-persistent CSMA**
* If the channel is busy, we wait a random time and then check again - **Non-persistent CSMA**

Approach between 1 and non-persistent CSMA modes:

* Continues to try and speak in the next slot with probability p - **p-persistent CSMA**

0.01 persistent CSMA gets near 100% network utilization, but will be VERY SLOW for a single user

CSMA Collision Detection

Transmitter monitors its own transmissions. Abort a transmission as soon as a collision is detected. Used only by wired Ethernet. Saves time, power and transmission capacity.

CSMA Collision Avoidance

For wireless systems.

A wireless transmitter cannot easily monitor its own transmissions.

With wireless, the emphasis is on avoiding collisions in the first place.

(networks notes) If packets aren’t being ACK’ed, then stop sending as it’s assumed to be a collision.

Transmission Modes -

Non-Contention - Centralized control

Contention - CSMA CD/CA

**Wi-FI Contention**

Uses real channel sensing - Sense the channel just before transmission, if it’s free transmit. Collisions sensed at receiver end

Virtual Channel sensing - Uses control frames. Request to send and Clear to send.

Hidden device problem - If A B C, C is out of the range of A, B may get talked to by both

Exposed device problem - B wants to transmit to A, who cannot hear transmissions from C. C may be transmitting to D, B will assume channel is not free, does not transmit. However it can transmit to A without interfering with a transmission from C to B.

**Bluetooth Architecture**

Basic unit of a bluetooth system is a piconet. The network consists of 1 master node and up to 7 slaves. Piconets can be connected into a “Scatternet” by using one of the slaves as a bridge.

Uses frequency hopping. Transmit on a varying sequence of frequencies defined by a pseudo-random sequence (must have the same seed)

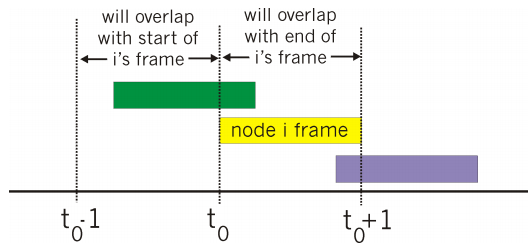
**Power Modulation**

Use minimum power necessary. Don’t want to reduce battery life. Also need to be careful with interfering with other cells.

**Notes copied straight from COMP28411 computer networks:**

(Random) Aloha - Random

When a packet is ready, send it. This means that each frame is vulnerable to interference for twice it’s length:

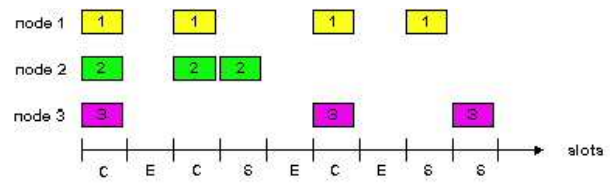


Efficiency is based on the probability of:

* A node transmitting
* Another node transmitting in time [t0-1, t0]
* Another node transmitting in time [t-, t0+1]

It comes out to be very low, 18% by some fancy maths.

(Random) Slotted Aloha

Like aloha, but reduce the perio...d that a frame is vulnerable by only allowing transmission at the start of a “slot”.

When a node transmits, it detects if there is an error, it tries to retransmit. Eventually it will succeed.

By slotting up time there are more problems introduced though.

* Assume frames are of equal size
* Assumes time can be divided up
* Assumes nodes can detect a collision has happened
* Node synchronization (probably most important/difficult)

Efficiency is slightly better at 36% ish

(Random) CSMA - Carrier Sense multiple access

Listen to the wire/air/medium before transmitting. If its free then transmit, otherwise don’t. Collisions can still occur though, due to propagation delays of other party’s messages.

(Random) CSMA/CD … with collision detection

Used in the ethernet protocol. Was required when the wire was shared. When a collision is detected after transmitting, then stop sending message to reduce channel use wastage.

(Random) CSMA/CA … with collision avoidance

Used in wireless stuff when it’s harder to listen to the medium to detect errors. If packets aren’t being ACK’ed, then stop sending as it’s assumed to be a collision.

(Turn Taking) Polling

Have a master and slaves. The master controls who sends stuff and how much they can send. Master is a point of failure.

(Turn Taking) Token Passing (Ring Networks?)

A send token is passed around. Only the person with the sending token can send at that time. Token must be recoverable if client holding it (the token) crashes.