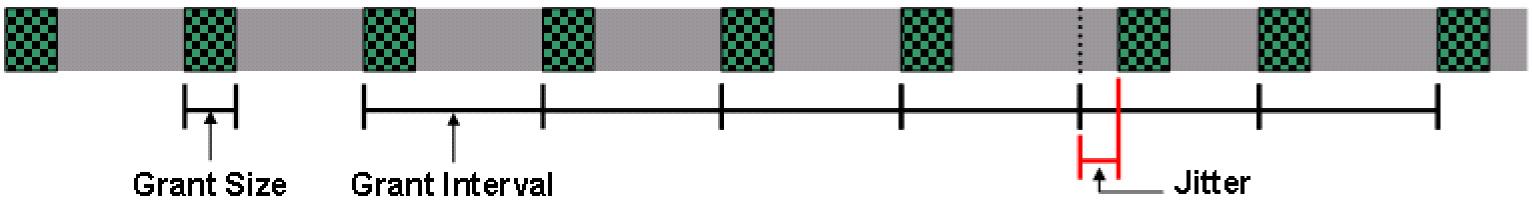
Networking Technologies and Applications

Rolland Vida
BME TMIT

October 2, 2019

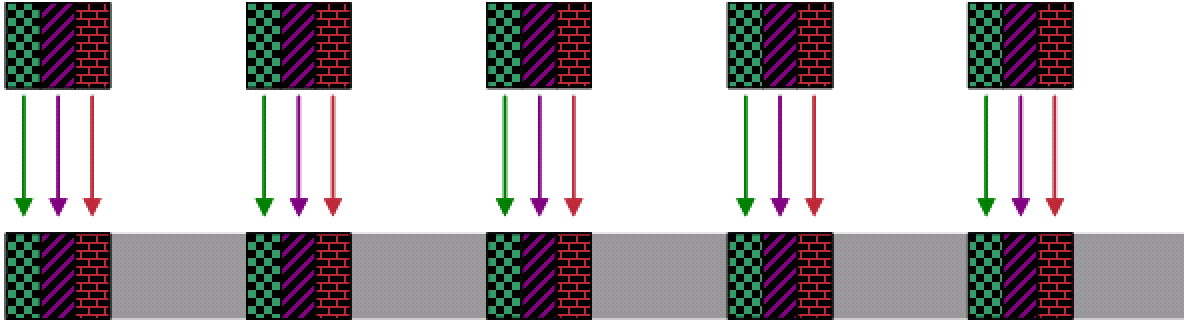
Providing Quality of Service

- Different applications have different QoS requirements
- CBR – Constant Bit Rate (pl. VoIP)
  - **Unsollicited Grant Services (UGS)**
    - No need to sollicit uplink slots all the time
    - Tolerated jitter in grant allocation



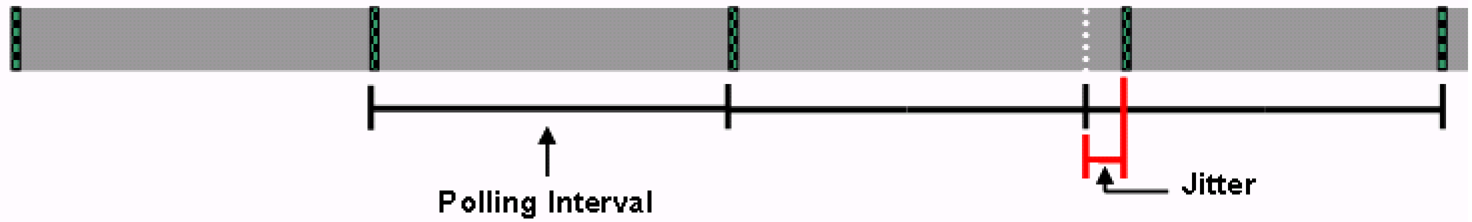
Admission Control

- UGS demands are accepted only in limited number
  - You have to leave room for other traffic types as well



Providing QoS

- rt-VBR (Real Time Variable Bit Rate)
  - E.g., live video stream
  - **Real Time Polling Service (RTPS)**
    - Bandwidth Request Slot dedicated to one specific application / modem
    - Can send his request for sure, no collision
    - Tolerated jitter in polling

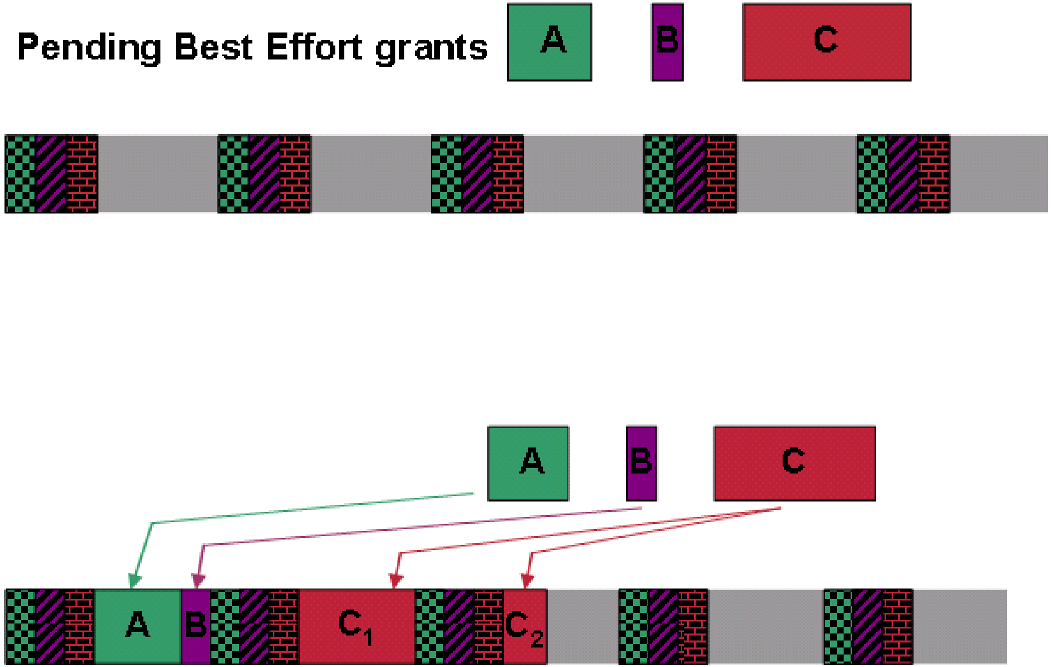


Providing QoS

- **Unsollicited Grant Service with Activity Detection (UGS-AD)**
  - Operates in UGS mode only if it has data to be sent
  - If temporarily no data, switches to RTPS mode
  - If needed, can switch back to UGS mode
  - E.g., VoIP with Voice Activity Detection (VAD)
- **Non-Real Time Polling Service (nRTPS)**
  - For nrt-VBR traffic
  - The polling intervals are not uniform

Providing QoS

- **Best Effort Grants (BEG)**
  - No strict requirements for delay or jitter
  - Fragmentation – if needed, the slot requests can be split in time
    - More headers, but sometimes it is worth doing it



No contention in the downstream traffic

- Downstream traffic is sent only by the CMTS
  - No contention, no need for mini timeslots
    - No collisions, lower probability for bit errors, no need for retransmission
  - Large packets in the downstream traffic
    - Typical packet length: 204 bytes
      - Includes Reed-Solomon error correcting code
      - 184 bytes for user data

Secure communication

- Shared cable
  - Anyone can read the traffic that passes by
- Two way traffic encrypted, to avoid the eavesdropping of the neighbors
  - Agreement between the modem and the CMTS on a common encryption key
    - Between two strangers, on a shared, eavesdropped link
  - Diffie-Hellman algorithm
    - Alice and Bob agree on two large prime numbers n and g
      - Public values, e.g., Alice chooses them, and send them to Bob, without encryption
    - Alice chooses a large (512 bit long) number: x
    - Bob chooses a similar one: y
    - Alice starts the key exchange, and sends the triplet $(n, g, g^x \bmod n)$ to Bob
    - Bob sends back the value $g^y \bmod n$
    - Both of them calculate the shared key:
      - $(g^x \bmod n)^y = (g^{xy} \bmod n) = (g^{yx} \bmod n) = (g^y \bmod n)^x$
    - Carol knows g and n, but cannot obtain x and y
      - It would take too much time, even with a supercomputer

MITM attack

- Diffie-Hellman does not protect against a MITM attack
  - Man-In-the-Middle
  - How do I know that Alice is really Alice?
    - Carol chooses a number z
    - It intercepts the triplet (n, g, g^x mod n) sent by Alice, and replaces it with her own triplet (n, g, g^z mod n)
    - It intercepts Bob's answer g^y mod n and replaces it with her own g^z mod n
    - Carol agrees with Alice in the shared key (g^{xz} mod n), and with Bob in a different key (g^{yz} mod n)
    - Alice and Bob think they talk to each other, but in reality they talk to Carol
- Some authentication scheme is required
  - Digital signature - public/private keys
    - Alice knows Bob's public key
      - Certificate authority – trusted third party
    - Bob attaches a digital signature to its packet, using his private key
    - Alice verifies if the packet was really sent by Bob or not, using his public key

Aloha

- Hawaii – no telephone network at the end of the 70's
  - How to connect the computers on different islands to a network, containing the central computer in Honolulu?
- Solution: **ALOHANET** – low range radio
  - Norman Abramson, University of Hawaii
  - Each user terminal had a small radio device
    - Operated on two frequencies
      - One for the downstream, one for the upstream traffic
    - Downstream data broadcasted by the central computer, no problem
    - Contention on the upstream channel
      - If data reached correctly the central computer, it retransmitted it on the downstream channel
      - If the original sender did not receive it back, it was probably lost
        - » Retransmission required
  - If low upstream traffic, the solution is quite efficient
  - If higher traffic, the solution is unusable

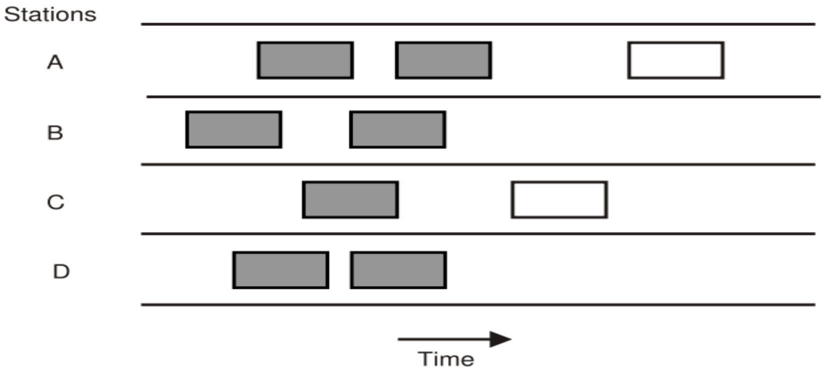
Aloha

Advantages:

- Different size packets
- No need for synchronization
- Simple operation

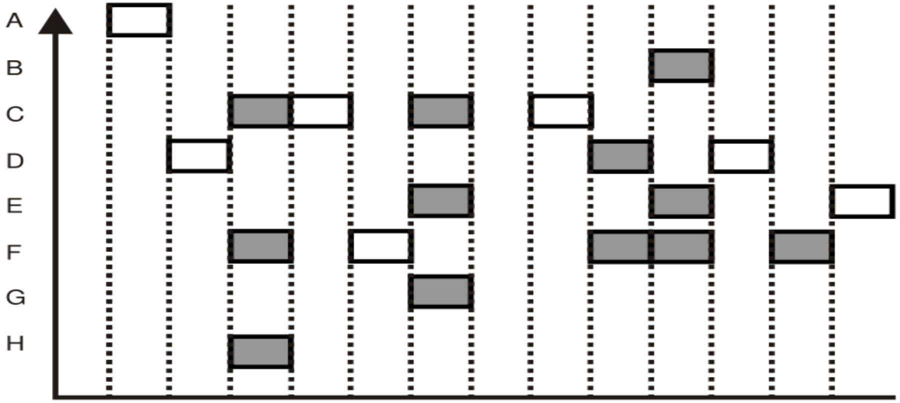
If low upstream traffic, the solution is quite efficient

If higher traffic, the solution is unusable



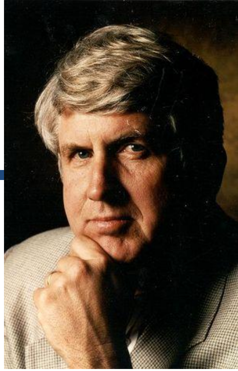
Slotted Aloha

- Time is divided into **slots**
  - Fixed length slots to transmit fixed size packets
- If a node wants to send, waits until a new slot begins
  - Need to **synchronize** the nodes
- If nobody else sends in the same slot, then the sending is successful
  - Otherwise collision, the packet is resent after waiting for a random amount of time

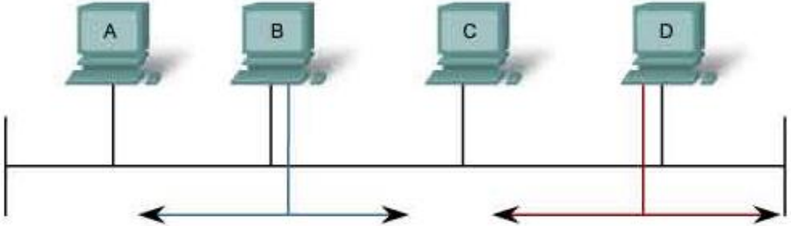


Slotted ALOHA protocol (shaded slots indicate collision)

Ethernet



- Bob Metcalfe (MIT, Harvard) spends his holiday together with Abramson on Hawaii
  - Idea: let's do something similar, but for a wired network (1973)
  - First standard (DEC, Intel, Xerox) in 1982, IEEE 802.3 standard in 1983
- Many stations connected to the same cable segment
  - Everyone hears everyone, but without any central node
  - The Ethernet frames will have to have a destination address
    - Everyone hears it, but the frame will be processed only by the destination



Ethernet = CSMA/CD

- Before transmission, hosts on the same Ethernet cable first listen to the channel (**CSMA – Carrier Sense Multiple Access**)
  - If busy, they wait for the transmission to end
  - If free, start sending
    - Not immediately, but after a **slot time**
      - If there is a signal on the channel, it leaves time for it to be received
    - Slot time = maximum round-trip time on the cable
      - For 10 Mb/s Ethernet it is 51,2 μs, for 100 Mb/s is 5,12 μs
- Two stations might think in parallel that the channel is free
  - Both start sending, a collision occurs
  - If collision, they detect it (**CD – Collision Detection**), and send a jam signal to ensure that others detect the collision as well