Random Access Protocols

- Assumption
  - Overlap in time and space of two or more transmissions causes a collision and the destruction of all packets involved.

    [No capture effects]
  - One channel
  - For analysis no station buffering
  - Time
    - Synchronization between users (Slotted time)
    - No synchronization between users (unsloted time)
  - Knowledge of the channel state
    - Carrier sensing
    - Collision detection

Random Access Protocols Strategies

- Aloha
  - On coordination between users
  - Send a PDU, wait for acknowledgment,

    if no acknowledgment then **backoff** and retransmit
- Slotted Aloha
  - Same as Aloha only time is slotted

Random Access Protocols Strategies

- *p*-persistent CSMA
  - Listen to channel, on transistion from busy to idle transmit with probability *p*
  - After sending the PDU, wait for acknowledgment,

    if no acknowledgment then **backoff** and retransmit
    - Non-persistent, if channel busy then reschedule transmission
    - 1-persistent, Transmit as soon as idle
- CSMA/CD
  - 1-persistent but continue to sense the channel, if collision detected then stop transmission.

Limitations on Random Access Protocols

- Distance
- Speed

Random Access Protocols

Analysis of Aloha

- Description
  - Packet of length L (sec) arrives at station i
    - Station i transmits immediately
    - Station i starts an acknowledgment timer
  - If no other station transmits while i is transmitting then **success**
  - Else a collision occurred
  - Stations i learns that a collision occurred if the acknowledgment timer fires before the acknowledgment arrives

Random Access Protocols

Analysis of Aloha

  - If collision detected then station i retransmitts at a later time, this time is pseudo-ramdom and is determined by a **backoff** algorithm
- Design Issue:
  - Determine the maximum normalized throughput for an Aloha system

Random Access Protocols

Analysis of Aloha

Assumptions

1. λ = Average number of new message arrivals to the system
2. Λ= Average number arrivals to the system, i.e., new arrivals + retransmissions
3. The total arrival process is Poisson

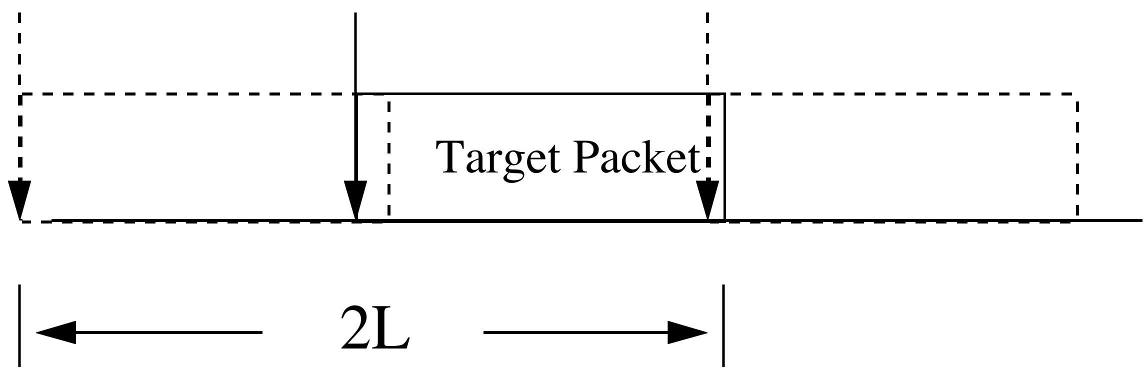
$$S = \lambda L \leq 1$$

$$S = \text{throughput}$$

Random Access Protocols

Analysis of Aloha

Collision Mechanism



Target packet is vulnerable to collision for 2L Sec.

Random Access Protocols
Analysis of Aloha

Probability of Collision $= 1 -$ Prob[no arrivals in 2L sec]

$$= 1 - e^{-2L\Lambda}$$

But

$$\Lambda = \lambda + \Lambda(1 - e^{-2L\Lambda})$$

Let

$$G = \Lambda L = \text{Offered load} \quad (S = \lambda L)$$

Then

$$G = S + G(1 - e^{-2L\Lambda}) \text{ or } S = Ge^{-2L\Lambda}$$

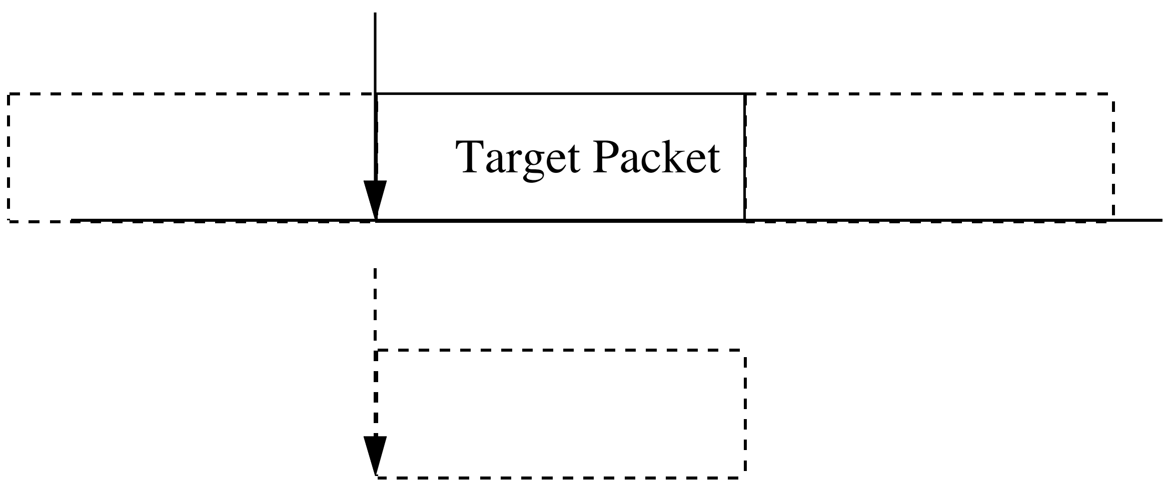
Find S_{max}

$$\frac{dS}{dG} = 0 \text{ when } G = \frac{1}{2} \text{ or } S_{max} = \frac{1}{2e} = 0.18$$

The Maximum throughput for Aloha is 18%

Random Access Protocols

Analysis of Slotted Aloha



Synchronization reduces the vulnerable period from 2L to L so the maximum throughput is increases to 36%

Random Access Protocols

Delay Analysis of Aloha

Let

τ_{ack} = acknowledgment time

T_b = backoff time

N_r = Average number of retransmissions

T = Average delay

Assume $T_b \sim U[1, K_b]$

$$\frac{T}{L} = \frac{\tau_{ack}}{L} + 1 + N_r\left(\frac{\tau_{ack}}{L} + \frac{K_b + 1}{2}\right)$$

with

$$N_r = \frac{G}{S} - 1 = e^{2G} - 1$$

Random Access Protocols

CSMA Protocols

- Listen to the channel before transmitting to reduce the vulnerable period
- Let D = maximum distance between nodes
- Let R = the transmission rate (b/s)
- Let c = speed of light = 3×10^8 m/s
- The end-to-end propagation time = D/kc

k is a constant for the physical media:

k = .66 for fiber, k=.88 for coax

Random Access Protocols
CSMA Protocols

- Assume node A transmits at time *t* and node B at *t -x*, where *x*--> 0
  (That is, Node B transmits right before it hears A)
- If after 2D/kc sec. no collision occurred, then none will occur
- Let *a*= (D/kc)/L = normalized length of the bus
- Remember L = (Packet Length [bits])/R [b/s]
- As *a* --> 1, CSMA --> Aloha

Random Access Protocols
CSMA Protocols

- Limits on *a*
  - Want *a* small to keep vulnerable period short
    - Short bus
    - Lower speeds
    - Long packets
      - Minimum packet length to keep *a* large
      - Maximum packet length to be fair
- Example: Ethernet
  - Rate = 10 Mb/s
  - Minimum packet size = 512 bits
  - Maximum packet size = 12144 bits