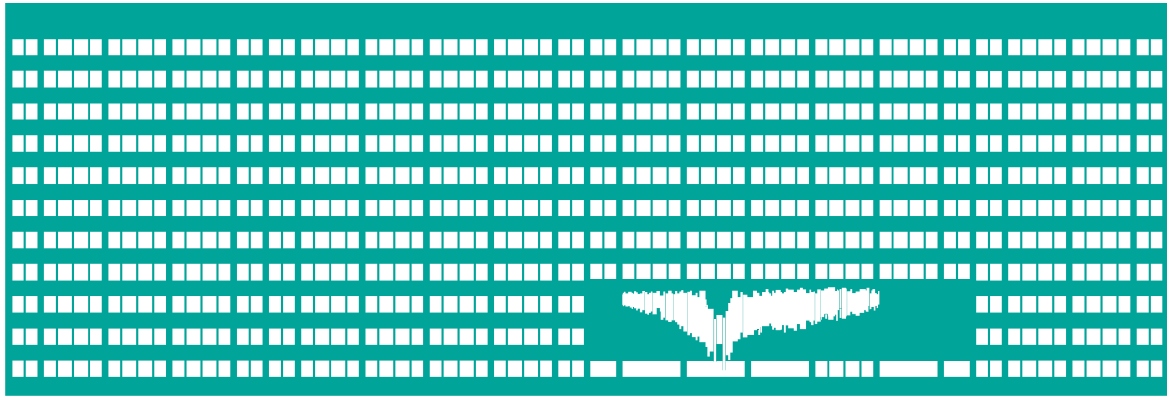
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Multiple Access Protocols



Computer Networks
Lecture 2

Multiple Access to a Shared Channel

- The medium (or its sub-channel) may be shared by multiple stations (dynamic allocation)
  - just one of them may transmit at a particular time
    - otherwise the transmissions collide and the intended receivers can not decode their data
    - all stations need to agree which station will be allowed to transmit
- Various multiple access control (MAC) protocols have been developed for that purpose

Classification of MAC Protocols

- Deterministic (contention-free)
  - a deterministic (distributed) algorithm defines a sequence in that the stations may transmit
  - more than one station will never access the medium at the same time
  - a portion of the channel capacity is consumed by for the MAC protocol
- Probabilistic (contention)
  - A probabilistic algorithm is used to determine which station will be allowed to transmit next
    - e.g random waiting times
  - Multiple stations may try to transmit at the same time which may result in a collision
    - The access control method has to deal with collisions
      - and try to minimize the probability of a collision

Probabilistic (Contention) MAC Protocols

Collision Slot

A maximum time interval unusable for data transfer in case of a collision

- the time of the collision slot duration is wasted

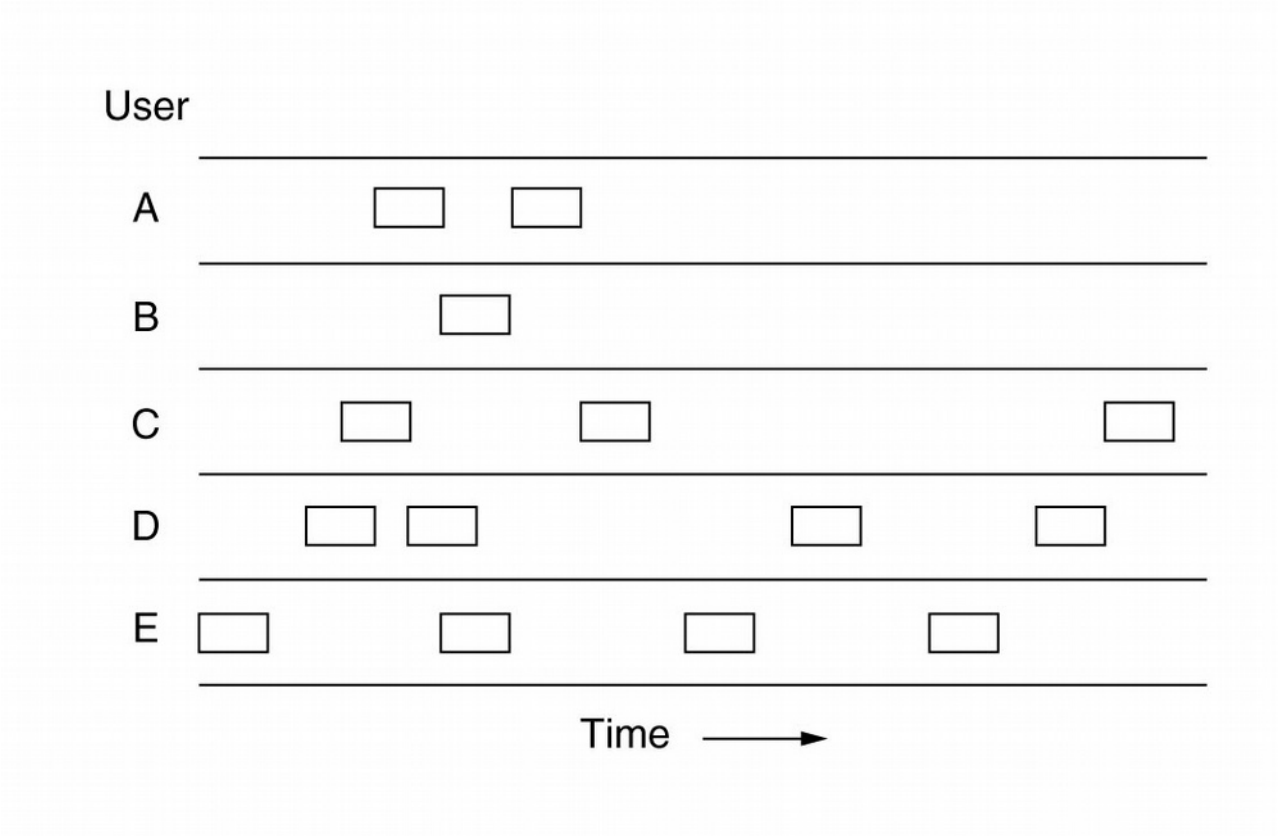
Aloha (1)

- Developed in the wireless network of the University of Hawaii
  - not very heavy traffic
- The station does not check if the medium is busy, it just starts to transmit
- The collision is detected by failing to receive a packet acknowledgment in a timeout
  - packet is retransmitted after the timeout expires
  - random pauses are necessary before packet retransmission to avoid synchronization of multiple transmitters and repeating of the collision

Aloha (2)

- Still used in some wireless networks and communication over satellites where the long propagation delay does not allow to detect presence of signal on the medium before starting the transmission
  - Moreover, we cannot detect the collision by checking our own transmitted signal in radio networks as in wired network segments

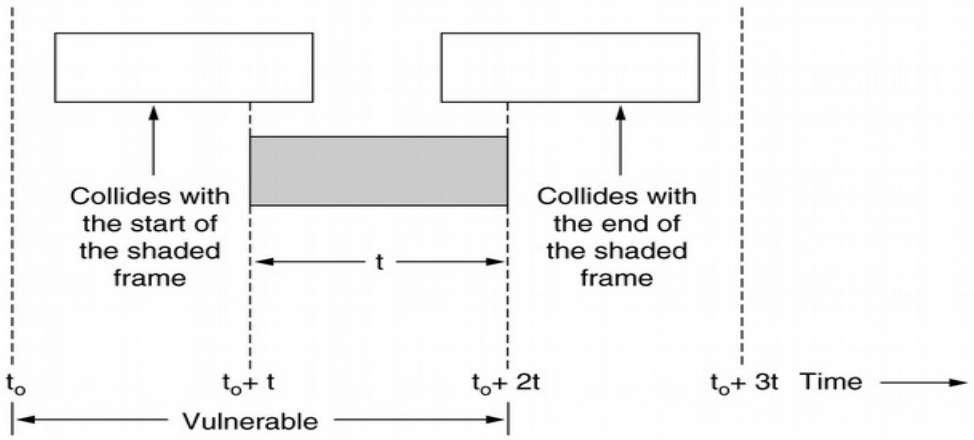
Pure Aloha



The acknowledgments contends for the channel access the same way as the data packets do

Collision Slot Pure Aloha

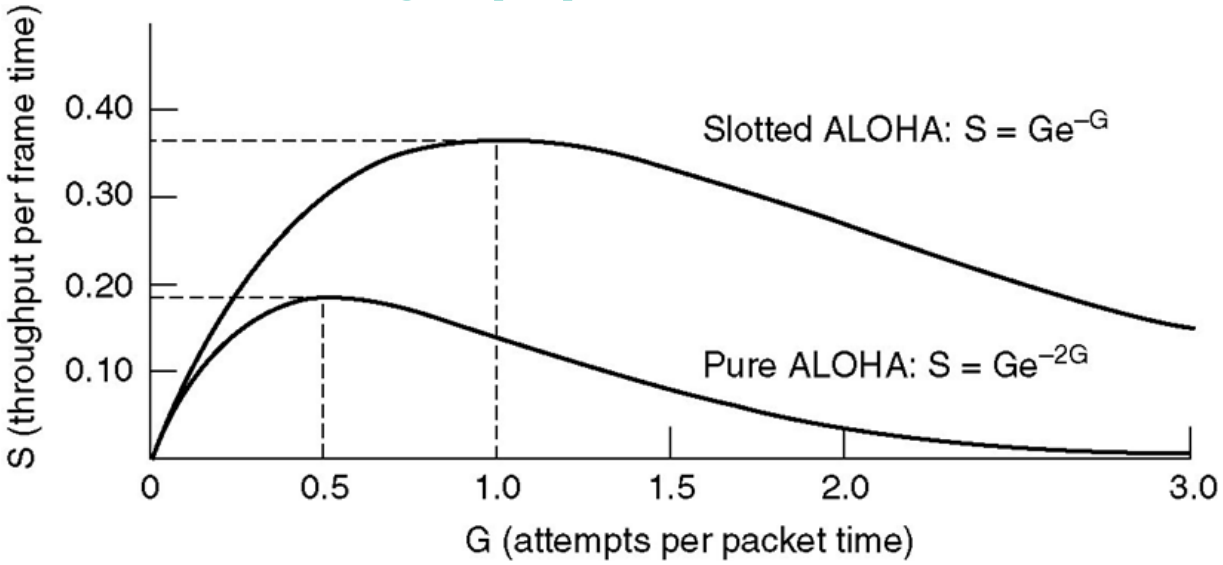
- The collision slot is 2 times longer than the frame timeslot
  - The frame may collide with the ending part of the other frame that started in a previous timeslot or with the beginning part of the other frame if it starts within the current timeslot



Slotted Aloha

- Any transmitter may start the transmission just in particular (globally synchronized) time instants
  - (beginnings of the timeslots)
- The transmission of the packet will be successful if just one station starts to transmit at the beginning of the timeslot
  - a collision occurs if multiple stations start to transmit
  - at most one timeslot will be wasted in case of a collision
- The length of the collision slot is a half of that in the pure Aloha
  - which means the double efficiency

Aloha Efficiency (1)



- The channel capacity may be utilized up to 18.4% (Aloha) or up to 37% (slotted Aloha)
- Every packet has to be repeated 3 times in average when the channel is fully utilized

Aloha Efficiency (2)

- As the total number of packets transmitted (by all transmitters) increases, the overall throughput starts to decrease
- Due to the exponential dependency, just a small increase of the injected traffic may significantly increase the average number of retransmissions and decrease the overall throughput
  - If the total injected traffic increases over the limit, the channel becomes blocked, i.e. the probability of a successful packet transmission rapidly falls to zero
  - Because of that, it is necessary to control the behavior of the method by intelligent modification of its parameters

Intelligent Control of Aloha Protocol Behavior

- The packet transmission rate have to be regulated according the current load of the shared media
  - The higher rate results in more faster transfers but the rate have to be limited if the channel starts to be blocked
- Heuristics are applied to control transmission rate
  - exponential backoff method exponentially lowers the transmission rate as the number of unsuccessful attempts grows
- We may eventually observe the current ratio of the busy and free slots on the channel and limit the packet transmission rate so that the maximum total load of the channel is bellow G=1

Carrier Sense Multiple Access (CSMA)

- A group of random access methods that listen the (carrier) signal present on the channel to detect whether the channel is busy
- The necessary assumptions:
  - stations may hear each other well
  - low signal propagation delay
- Typically met in wired LANs
- If the assumptions are not met, CSMA protocols perform worse than the pure Aloha.

Persistent CSMA (1) (1-persistent CSMA)

- The channel is checked before the start of the transmission
- If the channel is busy, the transmission is deferred until the previous transmission finishes
  - The station senses the medium continually
- There is a risk that multiple stations waiting for the free channel will start to transmit at the same time
- If the collision is detected (packet is not acknowledged in a timeout), the transmitter has to wait for a random time before the next attempt
  - to avoid global synchronization

Non-persistent CSMA

- If the station detects the busy channel, it waits for a random time before it repeats the check if the medium is still busy
- The time to wait is commonly chosen as a random multiple of the signal propagation time
- Reduces the risk of collision after the end of the previous transmission
  - but may waste time by underutilization of the channel

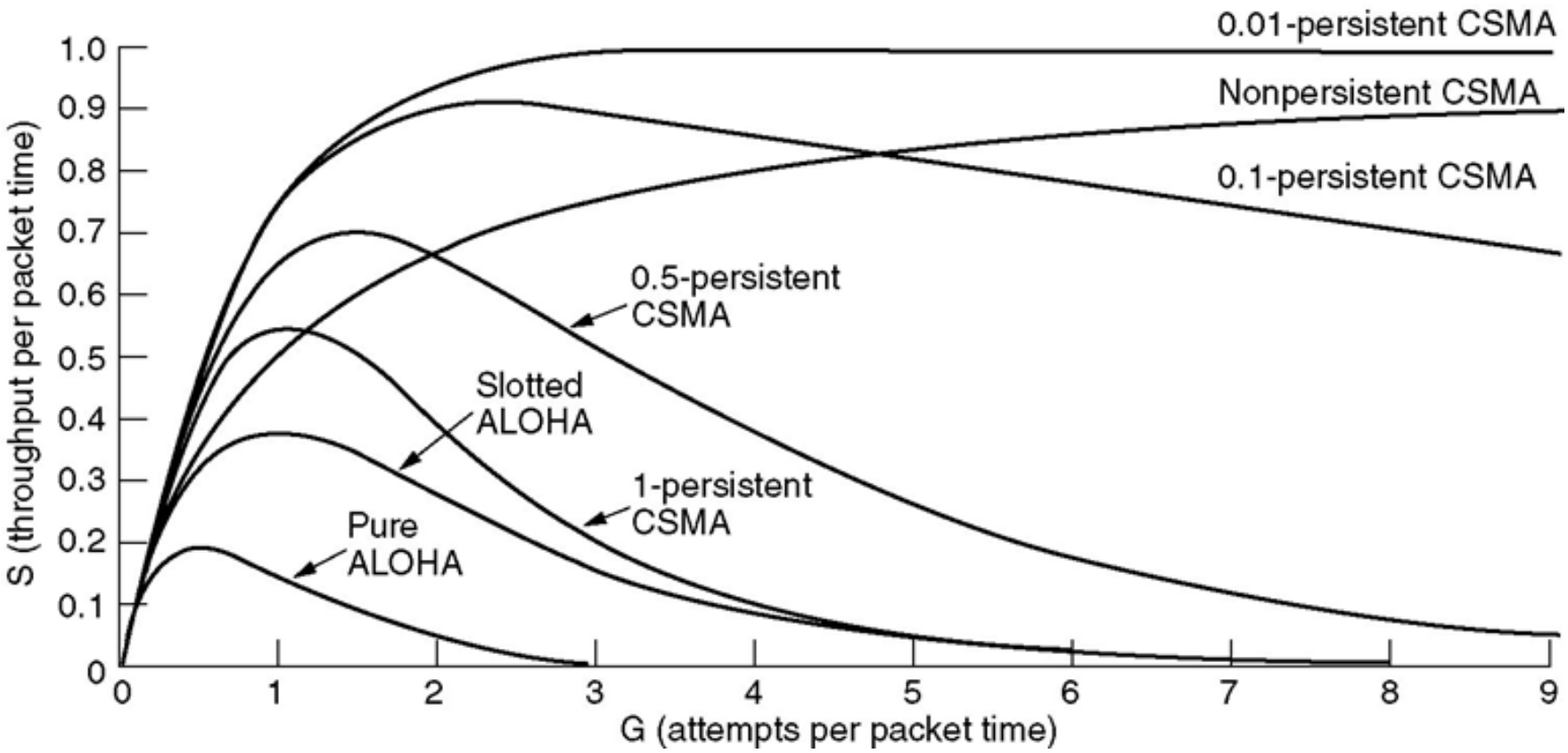
p-Persistent CSMA (1)

- If the station is ready to transmit, it waits for the free medium
  - Checks the medium continually
- After the idle medium is detected, the station will transmit with a probability p or waits one timeslot with a probability (1-p)
  - typical timeslot length corresponds to 2x maximum signal propagation delay
- If the station detect any other station's transmission after the waiting timeslot ends, it waits for a random time and repeats the attempt as in case of a collision
- The process is repeated until the frame is transmitted

p-Persistent CSMA (2)

- The utilization of the channel may be optimized for a given load by a proper selection of p parameter
- Behaves as persistent-CSMA if p=1
- If p is very small, there are almost no collisions but the average packet delivery time grows significantly

Efficiency of CSMA and Aloha Protocols



CSMA/CD (1)
(CSMA with Collision Detection)

- The station detects a collision by listening the signal on the medium during its own transmission
  - The hardware has to allow the collision detection
    - e.g. by shift of DC component on coax Ethernet (property of Manchester encoding) or by a presence of a foreign signal on RX pair of TP Ethernet
- Before starting of the transmission, the medium has to be idle for a duration of the collision slot
- The subsequent steps correspond to persistent CSMA

CSMA/CD (2)

- If the collision is detected, the transmission is stopped immediately
  - to avoid wasting of channel capacity by unusable collided packets
    - To ensure faster and more reliable detection of a collision by all transmitting stations, the station that detected the collision sends the special collision („jam“) signal
  - all stations whose transmissions collided have to wait for a random time before the next attempt
    - backoff algorithm
    - Ethernet
      - After the k-th collision the stations choses a random number of timeslots to wait from the interval <0 , 2^k-1) (max. 1023)
      - The transmission is given up after 16 unsuccessful attempts

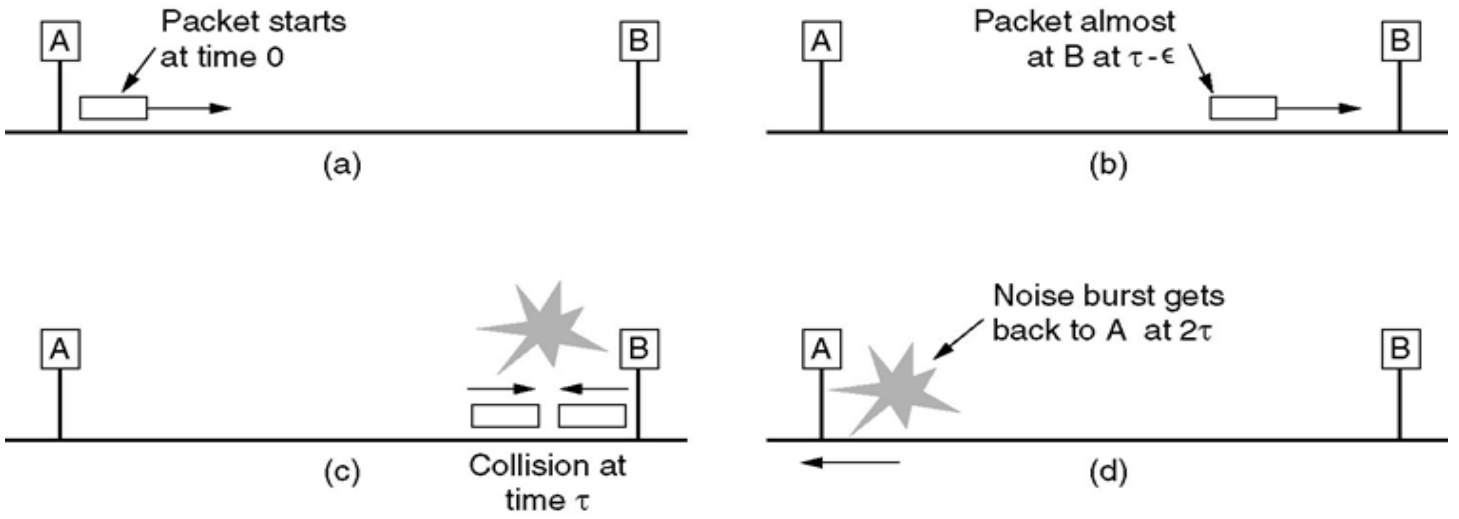
CSMA/CD Timing

There is a close relation between

- The velocity of the signal propagation on the medium
  - includes delays caused by repeaters
- Maximum allowed segment length
- The minimum time of the frame transmission duration
  - and thus the minimum frame length

The Minimum Frame Length

- The transmission time of a frame has to be at least as long as the time to detect the collision in the worst case
  - 2 times of the time of the signal propagation delay between the stations on the opposite ends of the segment



The Maximum Length of the Cable Segment

- The signal propagation time between the opposite segment ends is given by
  - The segment length
  - The signal propagation velocity
  - Delay introduced by repeaters/hubs

- To ensure detection of a collision, the back and forth propagation time may not be longer than the transmission time of the shortest allowed frame
    - The Ethernet standard specifies 51.2 μs

The Maximum Cable Length on (half duplex) Ethernet

- The longest allowed delay on the segment is set to 51.2 μs, i.e. 512 bit intervals at 10 Mbps
  - Corresponds to 2.5 km of coax cable + 4 repeaters (10Base5)

Deterministic (Contention-Free) MAC Protocols

General Classification

- Centralized Control
- Distributed Control

Centralized Control

- A master station is dedicated to assign the capacity of the channel to the other (slave) stations
- Introduces a single point of failure

Centralized Control
Polling

- The central station polls (offers the right to transmit to) the other stations
- The polled station either sends the data frame or informs that there are no data to send
  - or remains silent
- Round-robin polling scheme
  - Applicable for channels with a small signal propagation delay
  - Behaves well when the most of stations want to transmit equally and all the time
    - Inefficient for large number of stations and a light of unbalanced load
- Other polling schemes may be also applied

Centralized Control Request Arbitration

- Stations use the separate (narrow-band) channels to ask the access to the data channel
- The central station arbitrates the requests and assigns the channel
  - the channel assignment message is transmitted on the common data channel
- Used in radio networks
  - low-speed TDM channel commonly used for access requests

Contention-free Protocols
Distributed Control

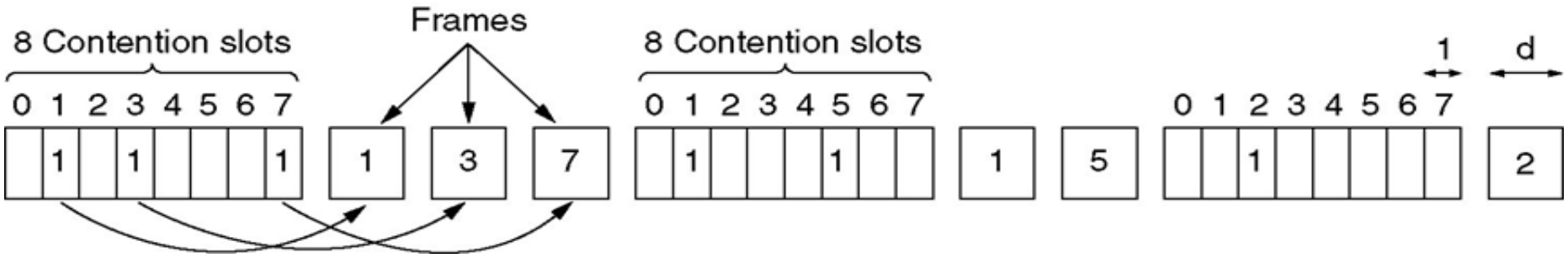
- Independent on a single central control station
- The implementation tends to be more complicated

Distributed Control
Bit-Map Protocol (1)

- The master station periodically generates the reservation frame
  - Number of bits correspond to the number of stations
  - Minimum bit length is twice the propagation delay
- A station may reserve a timeslot for data transmission in a reservation frame
  - using the bit that correspond to the station number
- Data timeslot follows the reservation frame
  - Only for stations that requested to reserve a timeslot
  - If no station have data to transmit, just the reservation frames still repeat on the medium

Distributed Control
Bit-Map Protocol (2)

- Not efficient for a large number of stations, on the media with long propagation delays and for light loads



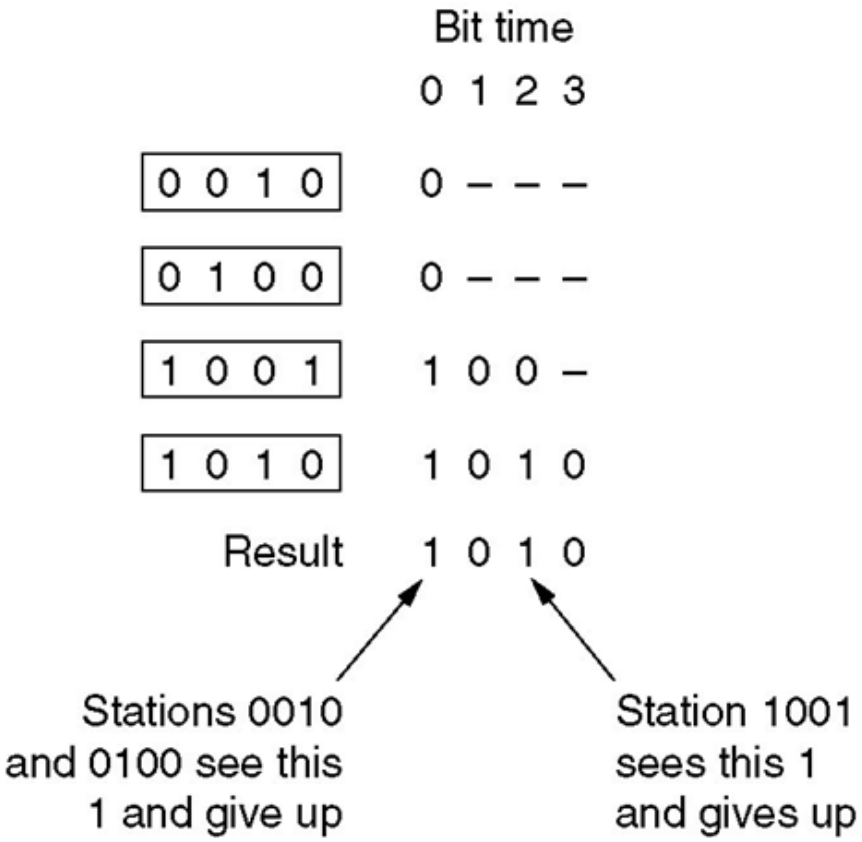
Distributed Control
Binary Countdown (1)

- Stations are given binary addresses
- Before data transmission, the station first starts to send its address bit by bit
- The bits transmitted by different stations are are logically ORed
- If the station sends 0 but hears 1, it has to refrain from the further transmission as there is another station with the higher priority that wants to send data
- The station that successfully transmitted the whole address gets the right to send a frame

Distributed Control
Binary Countdown (2)

- There must exist a mechanism to synchronize stations, i.e. define the instants when stations may start to transmit bits of their addresses
- Lower overhead ($\log_2(N)$) comparing to bit-map protocol (N)
  - N denotes the number of the stations
- Stations may be given priorities using the addressing scheme
- To avoid monopolizing of channel by the highest-priority station, we may identify the stations by addresses independent on the MAC protocol and rotate MAC-protocol addresses after transmission of every frame in a deterministic manner

Distributed Control
Binary Countdown – An Example



Distributed Control
Adaptive Tree-Walk Protocol

- Stations are represented as leaves of a binary tree
- The tree is searched depth-first to find a subtree with just one station that wants to send data:
  - In the first timeslot, all stations are allowed to transmit
  - If a collision occurs the left and right subtrees are searched recursively
  - After data frame was sent without any collision or the channel remained idle (meaning that there is no transmitter in the subtree), another round of the search continues from the root
- There is a timeslot potentially reserved for every single station

Distributed Control - Token Passing

- A right to transmit is represented by a token
  - a station may hold the token only for a limited time
- The token is passed around between nodes
  - every station needs to know its address and the successor address

Necessary supporting mechanisms:

- Ring initialization:
  - stations have to learn their successors
- Attachment of another station to the ring
- Detachment of station from the ring
- Handling of the token loss and duplication

Virtual Token Passing (1)

- Station with address m senses the medium and determines that station with address n just finished its transmission
- The station with address m may start to transmit if the medium is idle for ((m-n) mod N)*t
  - N is the total number of stations
  - t is the longest possible signal propagation time
- After a frame transmission finishes, every other station has a dedicated time interval to start its transmission. If it does not start, the next station gets its chance and so on.

Virtual Token Passing (2)

- The procedure can be seen as passing of an implicit (virtual) token
  - Limits the overhead of passing the real token
- Stations have to hear each other well
- More efficient compared to standard token passing if there is a lot of stations and a light load

Distributed Medium Access Control Access Control on Ring Networks (1)

- Token Ring (Newhall)
  - A station ready to transmit changes the identifier of the arrived token frame to identify the data frame and sends its data frame
  - After the data frame returns back, the token is released to the neighboring station

- Slotted Ring (Pierce ring)
  - Fixed-size frames with a control bit indicating whether the frame is busy or empty circulate around the ring
  - The source station that receives its own frame coming back from the ring resets the busy indicator bit

Distributed Medium Access Control Access Control on Ring Networks (2)

- Register Insertion Ring
  - The station prepares the frame to transmit in a shift register that may be switched into the ring between two frames
  - After the frame rotates round the ring, the switch register is switched out

  The fact that frames return back to the source in the ring networks may be utilized to acknowledge reception by the receiver to the source station using control bits of the frame header

Comparison of the Contention-free and Probabilistic MAC Protocols

- Delay of the packet delivery under the light load
  - The contention-free protocols introduce an overhead of the MAC algorithm
    - grows with a number of involved stations
- Channel utilization under heavy load
  - Probabilistic methods cannot avoid the complete blocking of the channel by collisions