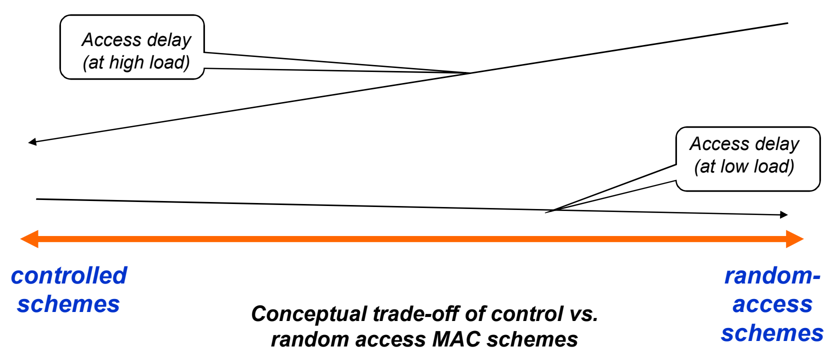
The Medium Access Control problem

⌘ The main function of a MAC layer protocol is to coordinate access to a *shared medium,* while in the r*andom access* protocol type, there is little (or no) coordination among the stations.



Conceptual trade-off of control vs. random access MAC schemes

The ALOHA protocol

- We will start our discussion of the evaluation of communication protocols with the simplest MAC layer protocol, of the *random access* type, the *ALOHA* protocol.
- To reiterate, the main function of a MAC layer protocol is to coordinate access to a *shared medium,* while in the r*andom access* protocol type, there is little (or no) coordination among the stations.
- The simplest random access MAC protocol is based on <u>no coordination</u> among the stations; a station that is *ready* simply transmits.

The ALOHA protocol

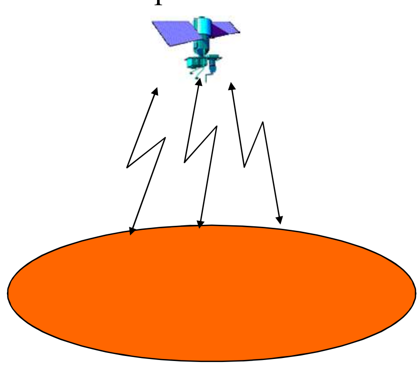
- The concept of ALOHA network was developed and published 1970 by Norman Abramson [N. Abramson, The Aloha System, Another Alternative for Computer Communications, in *Proc. of Fall Joint Comput. Conf., AFIP Conf.,* pp. 37].
- The idea in Abramson work was to develop a protocol to interconnect terminals at the various campuses of the University of Hawaii to a central computer.
- Pure ALOHA is based on a simple algorithm: *a station accesses the channel whenever it becomes ready.* Colliding packets are retransmitted.

The ALOHA protocol (con't)

- In the Slotted ALOHA scheme, *a ready station can access the channel at the first slot after it becomes ready.*
- ALOHA schemes are particularly useful in cases where the propagation delay is much larger than the packet transmission time.
- As we will see, ALOHA scheme have low channel utilization: 18% for Pure ALOHA and 36% for Slotted ALOHA.
- In our model, we will assume that there are very many (infinitely many) stations and that each station generate can generate a packet, which is stored in the station until it is transmitted.

The ALOHA protocol (con't)

- We will assume that the *aggregate* arrival rate from all the nodes is Poisson with rate λ *[packets/packet transmission time]* and we will normalize all times to "packet transmission time."

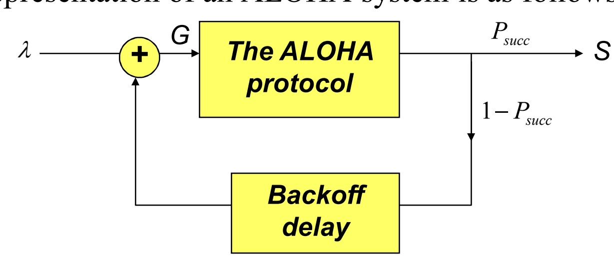


The ALOHA protocol (con't)

- Collisions: when two stations transmit "at the same time," collision will occur. Any colliding packets are destroyed and do not reach their destinations.
- Instantaneous feedback: The feedback about collision is immediate.
- No transmission errors: Lacking collisions, any transmitted packet is received correctly.No channel "capture" is assumed.
- Retransmissions: if a packet is destroyed, the transmitter will reschedule the retransmission to a later time, by putting the packet in a *backlog*.
- First, we will assume a *slotted* system (thus the name, *Slotted ALOHA*. We will relax this assumption later.

The ALOHA protocol (con't)

- The representation of an ALOHA system is as follows:



- From this representation, we can arrive at the following *characteristic equation of slotted ALOHA:*

$$P(k\ arrivals\ in\ a\ slot\ |arrival\ intensity\ of\ G) = e^{-G} \cdot \frac{G^k}{k!}$$

$$P_{succ} = S/G; \quad P_{succ} = \exp(-G); \quad \Rightarrow \quad S = Ge^{-G}$$

The ALOHA protocol (con't)

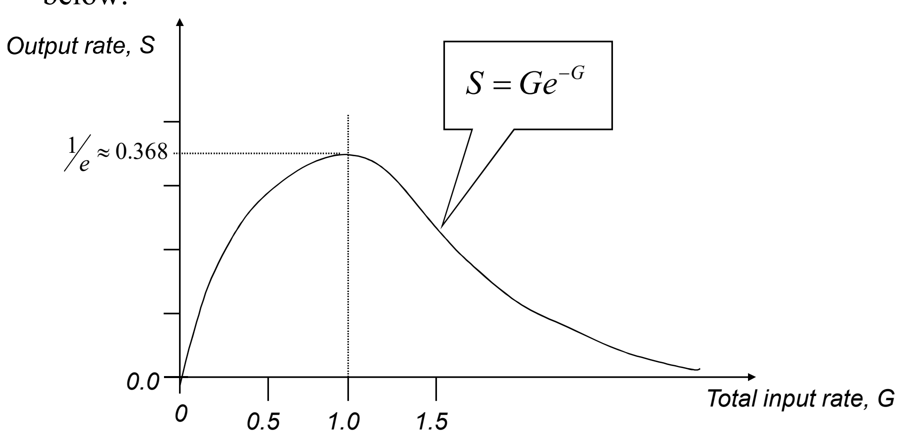
- To calculate the maximum throughput (i.e., the network *capacity*), equate the derivative of the throughput with respect to *G:*

$$\frac{dS}{dG}=0; \quad G=1.0; \quad S_{\max}^{slotted} \equiv C_{\max}^{slotted} = 1/e \approx 36.8\%$$

- In other words, the maximum throughput of slotted ALOHA is 36.8%. The rest of the link capacity is wasted on collisions.
- Note that this is an upper bound; in practical systems, there is usually a finite (often small) number of stations. In such cases, the capacity of slotted ALOHA can be considerably larger.
- Note slotted ALOHA is used in a number of cellular air interfaces; e.g., access to the control channels in GSM.

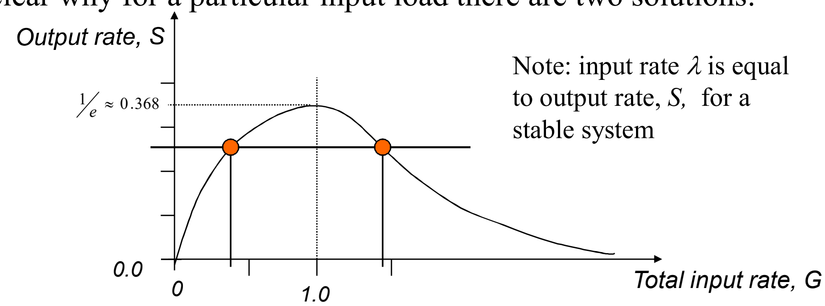
The ALOHA protocol (con't)

- The *characteristic equation* of ALOHA, $S=Ge^{-G}$ is plotted below:



The ALOHA protocol (con't)

- Note, the above derivation is a static solution; it "hides" the dynamic behavior of the system.
- In particular, it is not clear what happens when the input load increases above the *1/e* capacity of the system. Likewise, it is not clear why for a particular input load there are two solutions:

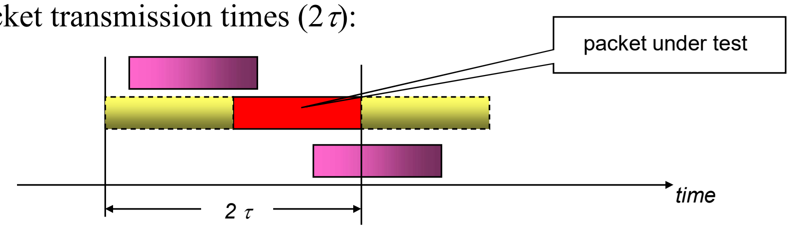


The ALOHA protocol: a Backoff Algorithm

- A *backoff algorithm* is used in ALOHA to avoid repetitious collisions; i.e., if two colliding packets were to be retransmitted in the following slot, they would collide again.
- The most popular backoff algorithm is the *Binary Exponential Backoff (BEB).*
- According to BEB, an arriving packet is transmitted immediately (with probability 1) in the next slot.
- A packet that underwent *i* collisions is retransmitted in the following slots with probability $q_{retransmission} = 2^{-i}$. Alternatively, the backoff interval is uniformly distributed in $[1, 2^{-i}]$.
- The idea behind BEB is for a node to "sense" the size of the backlog by the number of pact collisions and adjusting the "spread" of the retransmission interval accordingly.

The ALOHA protocol: Pure ALOHA

- Slot synchronization may be complex in some circumstances.
- In the pure ALOHA system, a ready station transmits its packet immediately. Upon collision, the packet is retransmitted after a random delay.
- The *characteristic (static) equation* of pure ALOHA can be derived based on the observation that a packet will be successful if and only if no other transmission started in an interval of <u>two</u> packet transmission times (2τ):



The pure ALOHA protocol (con't)

- Thus, the probability of a successful transmission of the "packet under test" is that there is no arrival in the interval of 2τ:

$$P(k\ arrivals\ in\ a\ \text{"}packet\ tx\ time\text{"}\ |arrival\ intensity\ of\ G) = e^{-G} \cdot \frac{G^k}{k!}$$

$$P_{succ} = S/G; \quad P_{succ} = \exp(-2G); \quad \Rightarrow \quad S = Ge^{-2G}$$

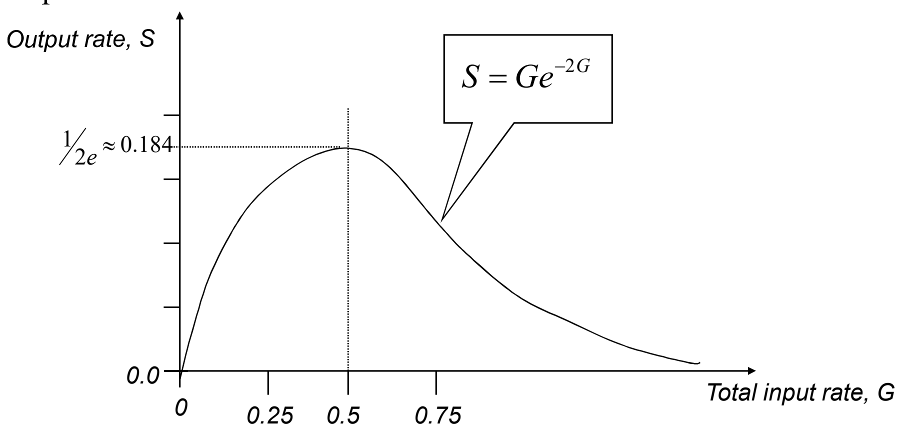
- To find the capacity of the pure ALOHA protocol, we proceed as in the case of slotted ALOHA by taking the derivative of S w.r.t G:

$$\frac{dS}{dG} = 0; \quad G = 0.5; \quad S_{\max}^{slotted} \equiv C_{\max}^{slotted} = 1/2e \approx 18.4\%$$

- So, the capacity of pure ALOHA is 18.4%, half of that of slotted ALOHA.

The pure ALOHA protocol (con't)

- The *characteristic equation* of pure ALOHA, $S = Ge^{-G}$ is plotted below:



The ALOHA protocol (con't)

- Comparison of the ALOHA protocol with TDMA:
  - ALOHA has significantly lower access delay at the expense of some collisions:

    ALOHA: immediate access, TDMA: *m/2* slots
  - ALOHA has significantly lower capacity than TDMA; under high load, TDMA can achieve close to 100% utilization, while ALOHA is limited to 36.8% (slotted) or 18.4% (pure).
- As such, one can say that ALOHA is better used under *low-load* conditions, when the reduced capacity is not an issue, resulting in lower access delay.
- TDMA on the other hand, should be used under *heavy-load* conditions, when capacity is an important consideration.

The Family of Carrier Sensing Protocols

- The source of capacity degradation of ALOHA are the collisions.
- An obvious approach to reduce the number of collisions is to "sense" the state of the shared channel before access.
- This type of sensing is commonly referred to as: *carrier sensing;* the station that wants to access the shared medium senses the presence of carrier energy on the medium. If energy is detected, the channel is declared busy and the station defers from accessing the channel.
- Note that the actual mechanism for "carrier sensing" does not need to involve actual "carrier" detection. All is required is detection of an idle medium.

The Family of Carrier Sensing Protocols (con't)

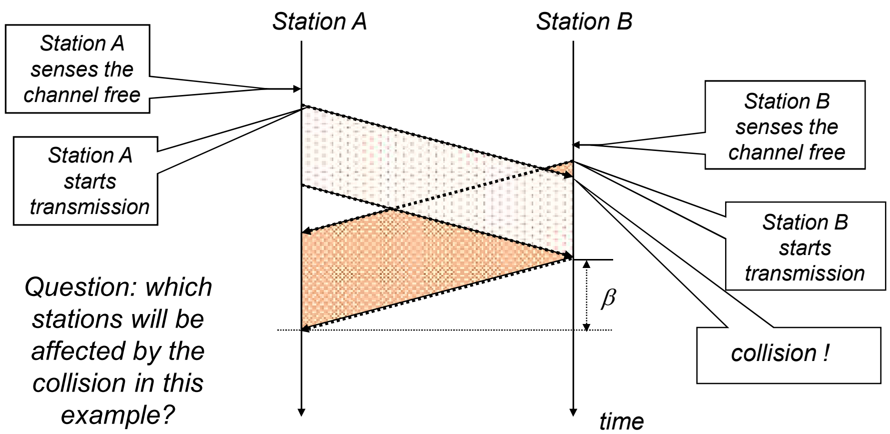
- The channel sensing usually involves some delay. This delay is usually small (compared to other delays) and will be ignored in our discussion here.
- However, even if we senses the channel, collisions are still possible. The culprit is the network propagation delay.
- Assume that the max network propagation delay is β *[packet transmission time]:*

$$\beta = \tau \cdot C / L$$

where τ is the propagation time [sec], C is the channel raw bit rate, and L is the average packet length [bits].

The Family of Carrier Sensing Protocols (con't)

⌘ The following example show how collision can occur with CSMA:



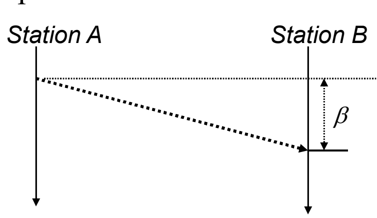
Question: which stations will be affected by the collision in this example?

The Family of Carrier Sensing Protocols (con't)

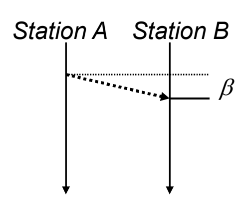
⌘ What is the culprit? - the network propagation delay (i.e., the fact that there is some time until all the stations can detect that another station started transmission.

⌘ In other words, as $\beta \rightarrow 0$, the feedback becomes more immediate and the chances of collision are reduced.

⌘ The "vulnerability period" is β; the larger the β is, the more probable a collision is:



Vulnerability to collisions as a function of the propagation delay, β



The Family of Carrier Sensing Protocols (con't)

- The CSMA is actually a family of protocols. They differ mainly in the action taken upon detecting a busy channel.
- *1-persistent CSMA* will transmit the packet immediately upon discovering an idle channel. If the channel is found busy, the ready node will wait until the end of the current transmission (detection of idle channel) and immediately transmit the packet.
- *Non-persistent CSMA* will transmit the packet immediately upon discovering an idle channel. If the channel is found busy, the ready node will wait until the end of the current transmission (detection of idle channel) and reschedule the transmission of the packet into the future.

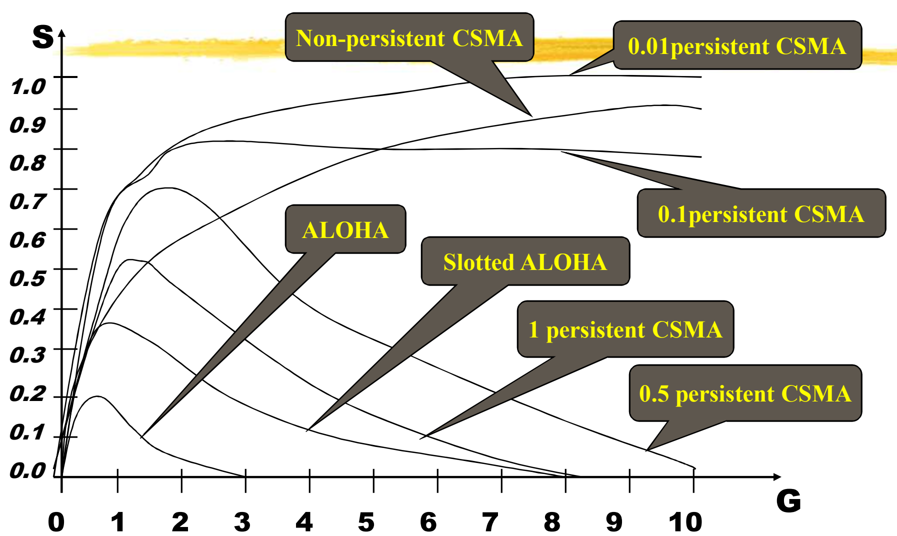
The Family of Carrier Sensing Protocols (con't)

- *p-persistent CSMA* is always slotted. It will transmit the packet in a slot with probability *p,* and defer from transmission with probability *(1-p).*
- The choice of a protocol depends on the actual operational conditions of the network.
- In low load, when collisions are less probably, *1-persistent CSMA* offers lower delay than either *non-* or *p-persistent CSMA*
- However, at higher load, the throughput of the *1-persistent CSMA* scheme is significantly lower than the the two other schemes.
- The advantage of the *p-persistent CSMA* is that its behavior can be <u>adapted to the network conditions,</u> by modifying the value of the parameter *p.*

The Family of CSMA Schemes

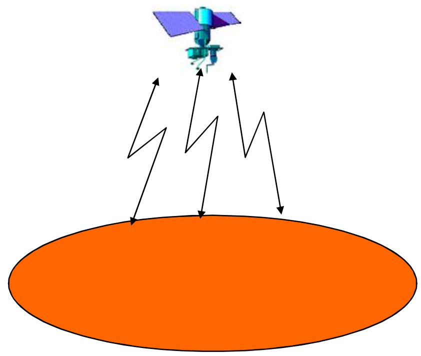
- In 1-persistent CSMA and in non-persistent CSMA, if a channel is idle upon access, the station transmits its packets.
- If a channel is busy, the 1-persistent scheme waits until the channel is released and then transmits its packets.
- If a channel is busy, the non-persistent scheme sets up a backoff counter that determines when the station will revisit the channel again.
- The p-persistent CSMA scheme is slotted. If a current slot is idle, the station transmits with probability p, otherwise, it defers with probability p until the next slot, where the same algorithm is performed again.

Comparison of the Traditional MAC Schemes



The ALOHA protocol (con't)

- We will assume that the *aggregate* arrival rate from all the nodes is Poisson with rate λ *[packets/packet transmission time]* and we will normalize all times to "packet transmission time."

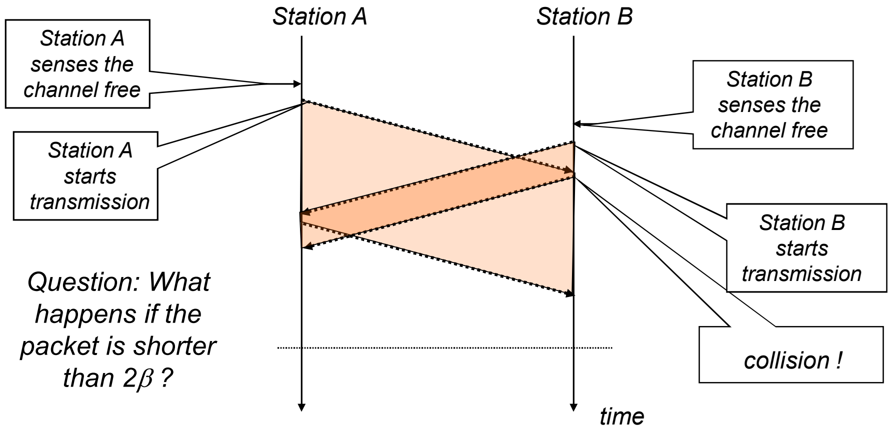


CSMA with Collision Detection: CSMA/CD

- In CSMA/CD, it is assumed, as in CSMA, that a node can listen to the channel before it transmits. However, it is also assumed that a transmitting node can continue to monitor the shared medium to determine whether a collision has occurred.
- When a collision is detected, all the nodes involved in the collision immediately cease all transmission.
- Of course, if no node attempted to access the channel after a node started its transmission during the time period equal to the medium propagation time, then no collision will occur.
- We will analyze the CSMA/CD performance assuming a slotted system.

CSMA/CD – Collision Resolution

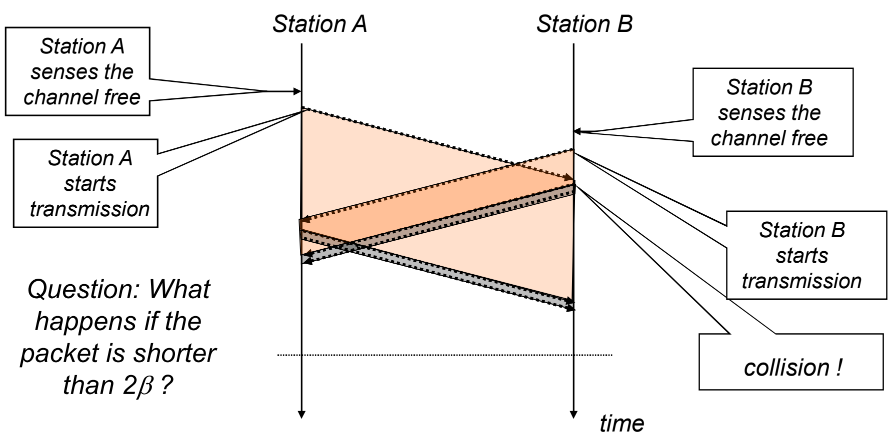
- The following example show how collision can occur with CSMA/CD:



Question: What happens if the packet is shorter than 2β ?

CSMA/CD – Collision Resolution

- The following example show how collision can occur with CSMA/CD:



Question: What happens if the packet is shorter than 2β ?

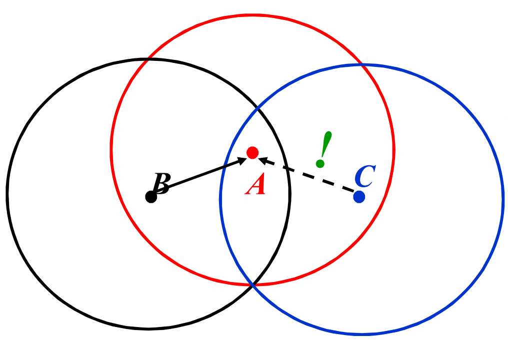
MAC-based Carrier-Sensing: Discussion

- Carrier-Sense (CS) schemes have been the traditional method of controlling access to a shared medium in radio packet networks.
- The CS schemes rely on sensing the power of the channel and deferring from accessing the channel until the channel becomes idle.
- The main observation is that the effectiveness of the CS schemes is reduced because:

collisions occur at the receiver, while CS monitors the status of the channel at the transmitter.

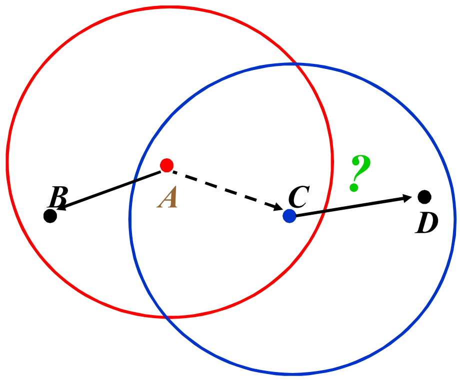
MAC for Radio Networks

- The above observation results in two access problems:
  - the hidden terminal problem, and
  - the exposed terminal problem



The hidden-terminal problem

MAC for Radio Networks (con't)

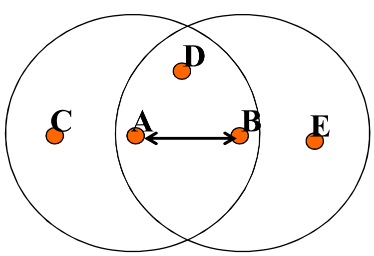


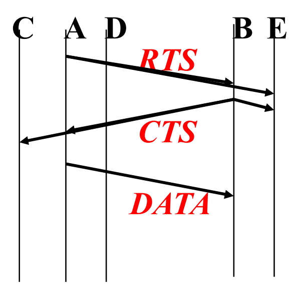
The exposed-terminal problem

Wireless Networks Laboratory Copyright ©by Zygmunt J. Haas, 2017 31

Random-Access MAC for Radio Networks (con't)

- An alternative to Carrier Sensing was proposed in which the coordination among the stations is performed by two basic control messages: Request-To-Send and Clear-To-Send.
- These messages "reserve" spatially and temporarily the channel for the about-to-communicate nodes.

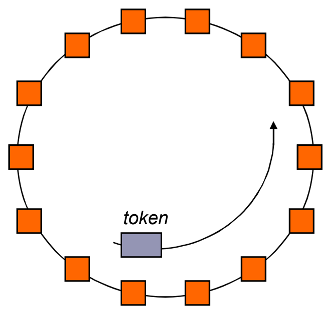




Wireless Networks Laboratory Copyright ©by Zygmunt J. Haas, 2017 32

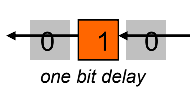
Token Rings

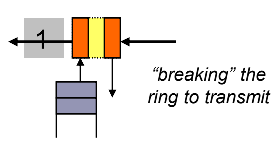
- As opposed to the CDMA-family of *random access* protocols, *token passing* allow for controlled access to a shared medium.
- The most known token-passing protocol is the *token ring,* which is built on top of architecture in which every node connects to exactly to other neighbors.

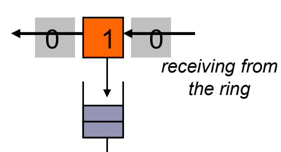


Token Rings (con't)

- In token ring, a token (a set of bits) is used to control access to the medium - only the station that holds the token is allowed to transmit at that time.
- Each station has a one-bit delay, that allows it to examine the incoming transmission.
- A station that wants to transmit onto the ring, waits until it sees a token passing by. The station "remove" the token from the ring, "breaks" the ring, and injects its own transmission. At the end of the transmission (more about this in a moment), the station regenerates the token and "heals" the ring.







Token Rings (con't)

- There are a number of variants of the token ring MAC protocol. In particular, one differentiator is when the token is released back into the medium:
  - at the end of the transmission of the current message, appended to the end of the message
  - when the head of the message emerges from the ring
  - when the whole message was drained from the ring
- Another choice is whether a station sends out a single packet each time or all the packets in its queue. Another choice is to hold the token for some maximum time and release it at the end of this time, even if there are still some unserved packets in the queue.

CSMA vs. Token Rings

- We now make some remarks related to the comparison of Token Ring with CSMA/CD MAC protocols.
- When the propagation delay is small, both CSMA/CD and Token Ring can achieve capacity close to 1.
- When the propagation delay is large (e.g., $\beta>1$), the advantage of CSMA/CD relative to CSMA decreases. However, Token Ring performance degrades as well.
- The main advantage of the Toke Ring technology is that, under some implementation choices, the access time can be bounded, even at high load. This is important for some time-critical applications, such as industrial automation, for example.

Copyright ©by Zygmunt J. Haas, 2017

CDMA vs. Token Rings (con't)

- On the other hand, for the family of CSMA protocols, being random access, the access delay cannot be bounded; all performance are average, rather than maximum. However, at low load, CSMA schemes can achieve substantially lower access delay, relative to Token Ring.
- In general, the access delay of random-access schemes is lower under low load and larger under high load, relative to access-controlled schemes, such as polling.

Other "traditional" MAC schemes

- Collision-Free Schemes:
  - A Bit-Map Protocol
  - BRAM/MSAP (Broadcast Recognition Access Method / Mini Slotted Alternating Priorities)
  - MLMA (the Multi-Level Multi-Access)
  - Binary Countdown
- Limited-Contention Schemes:
  - The Adaptive Tree Walk Protocol
  - The Urn Protocol