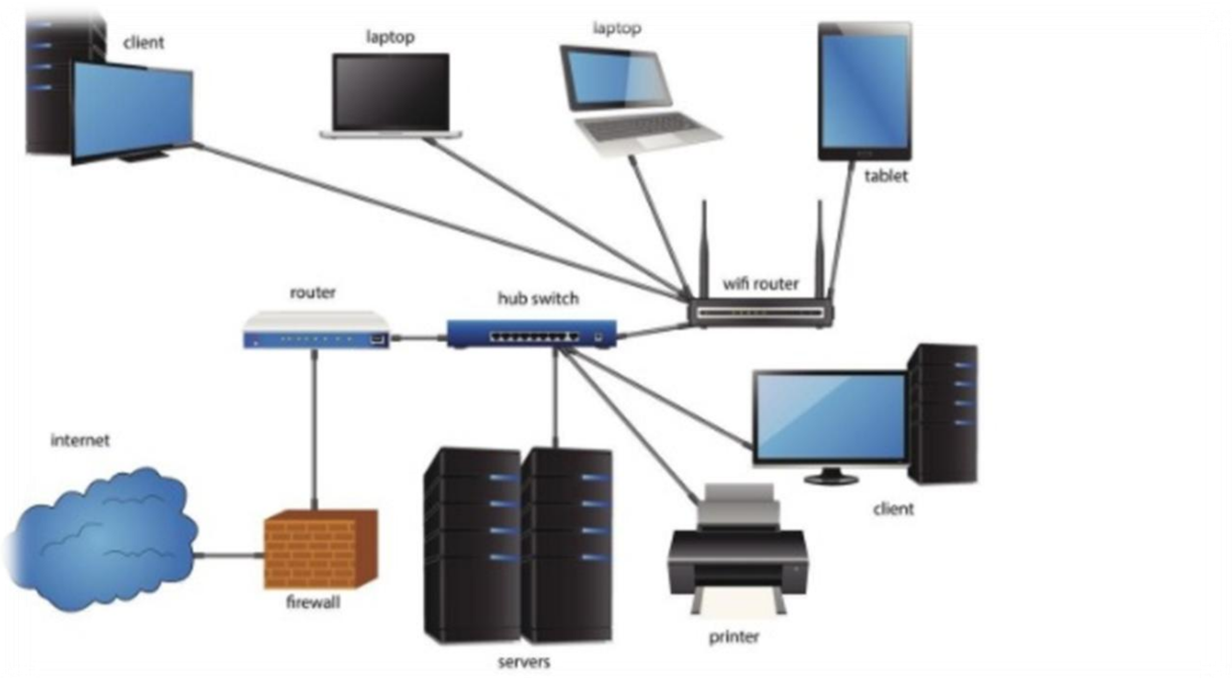
COMPUTER NETWORKS



Instructor: Mr. B. V. Sathish Kumar, Assistant Professor

Department of Electronics and Communication Engineering

UNIT – III
Medium Access Control Sub-layer

Figure: Seven layers of OSI Model

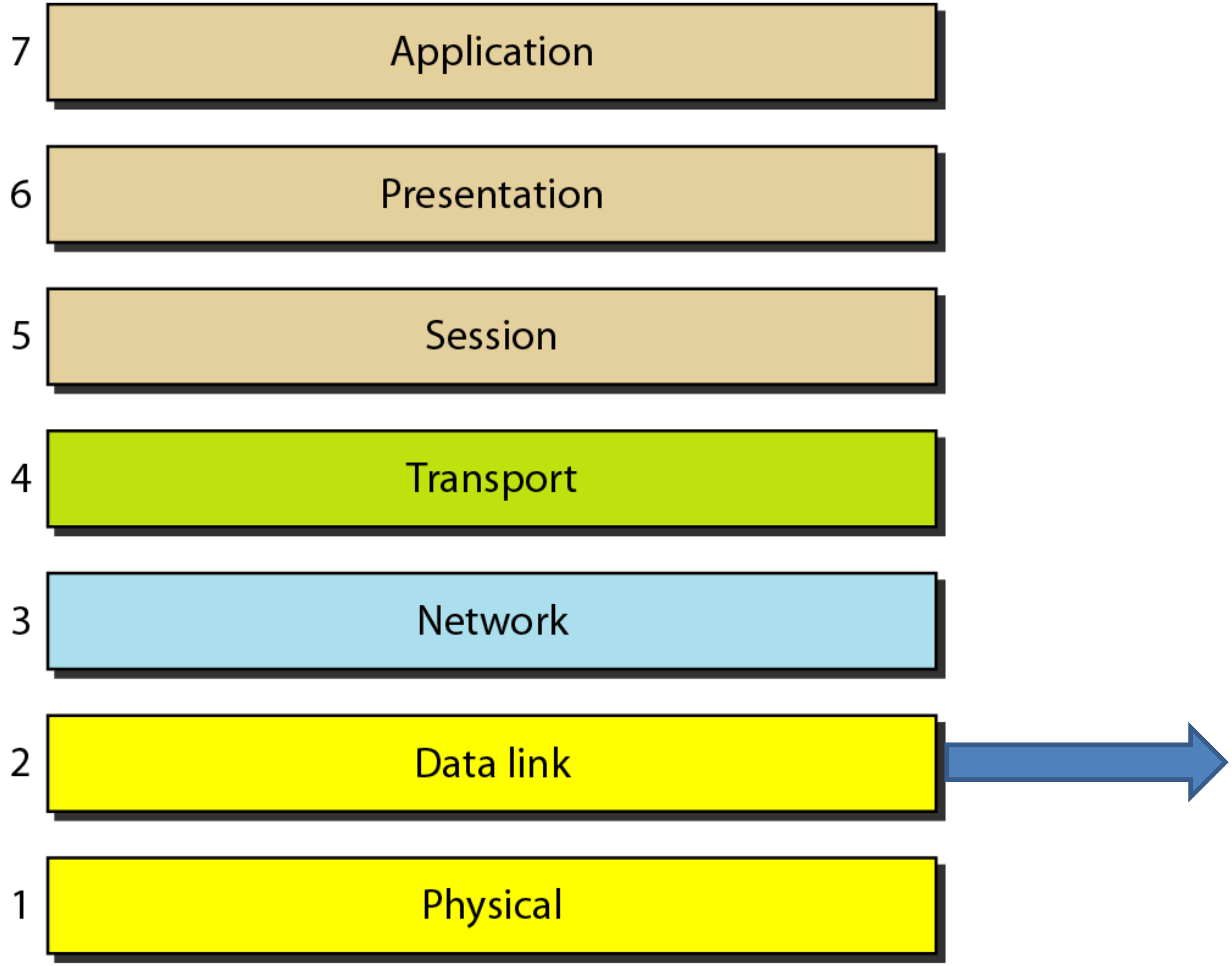


Figure: Data link layer divided into two sub layers

Network	
Data Link	**LLC Sublayer** *(Logical Link Control)*
	MAC Sublayer *(Media Access Control)*
Physical	

Data Link Layer (DLL)

Functions of DLL

1. Framing
2. Physical Addressing or MAC Addressing
3. Error Control
4. Access Control

MAC Sublayer

5. Flow Control

LLC Sublayer

Logical Link Control (LLC)

- It permits multiple network layers to share the same data link layer at the same time(multiplexing).
- Prepares data for transmission .
- Can provide flow control and error notification. Takes the network protocol data and adds control information to help deliver the packet to the destination.

Medium Access Control (MAC)

- Provides layer-2 addressing of devices.
- Detects or avoids frame collisions.
- Determines where frame start & end.
- Implemented by hardware, typically in the computer NIC.

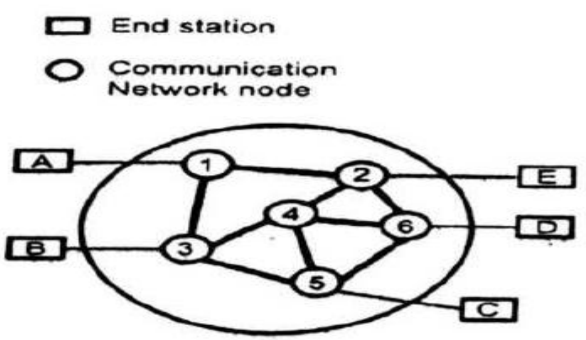
Syllabus

- Channel Allocation Problems, Multiple Access Protocols
- IEEE standards for Local Area Networks
- IEEE standards for WLAN, Bluetooth

NETWORK CATEGORIES

Based on the transmission technology

- Point to Point networks
- Broadcast networks(Multipoint Networks)



Communication network based on Point-to-Point Communication

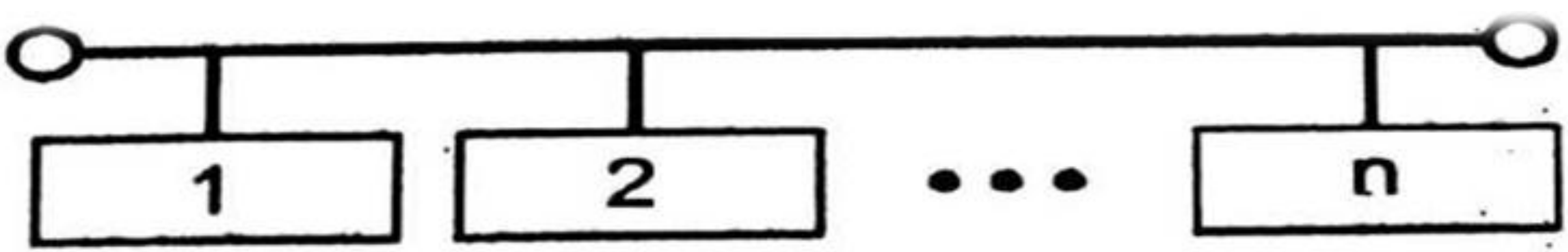
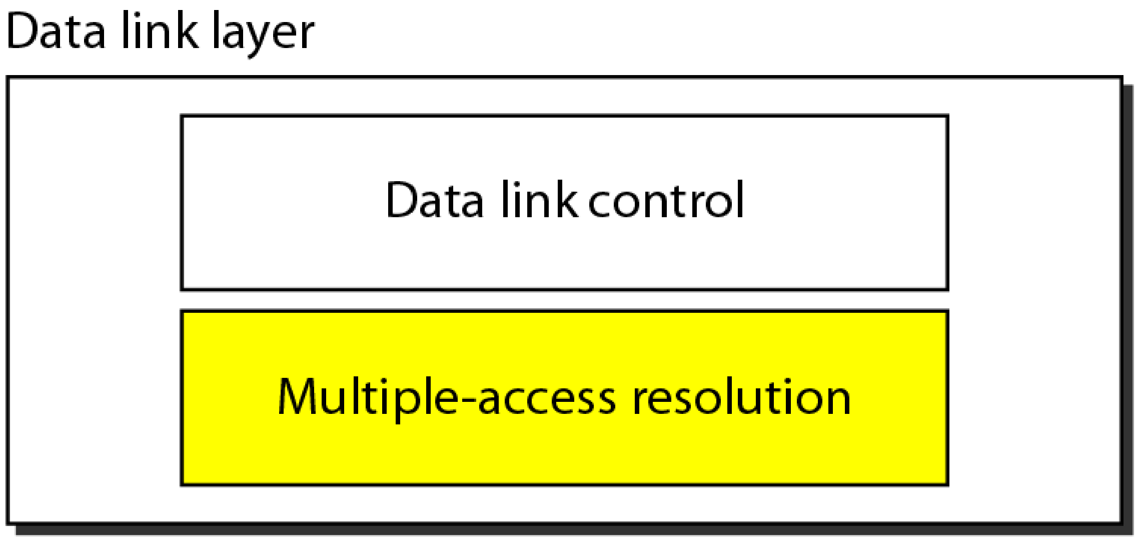


Fig . Broadcast network based on shared bus

Figure: **Data link layer divided into two functionality-oriented sub layers**



The protocols used to determine who goes next on a multi-access channel belong to a sub-layer of the data link layer called the MAC (Medium Access Control) sub-layer.

The MAC sub-layer is especially important in LANs, many of which use a multi-access channel as the basis for communication.

The Channel Allocation Problem

The central theme is how to allocate a single broadcast channel among competing users.

The channel connects each user to all other users who makes full use of the channel interferes with other users who also wish to use the channel.

Topics discussed in this section:

Static Channel Allocation

Assumptions for Dynamic Channel Allocation

Static Channel Allocation

In this method a single channel is allocated among multiple competing users by using the

- Frequency Division Multiplexing (FDM)

If there are N users, the bandwidth is divided into N equal-sized portions and each user being assigned one portion.

Pros:

- Each user has a private frequency band, there is no interference between users.

Cntd…

Cons:

- However, when the number of senders is large and continuously varying or the traffic is bursty, FDM presents some problems.
- If the spectrum is cut up into N regions and users (<N) are currently using the channel then the channel will be wasted.
- If more than N users want to communicate, some of them do not communicate due to the lack of bandwidth. It is hard to remaining users to transmit or receive data.

When there is a small and constant number of users, FDM is a simple and efficient allocation mechanism.

Cntd...

❑ Time Division Multiplexing (TDM)

Each user is statically allocated every N^{th} time slot. If a user does not use the allocated slot, it just lies fallow.

The mean delay using TDM is N times worse than if all the frames were somehow magically arranged orderly in a big central queue.

Conclusion:

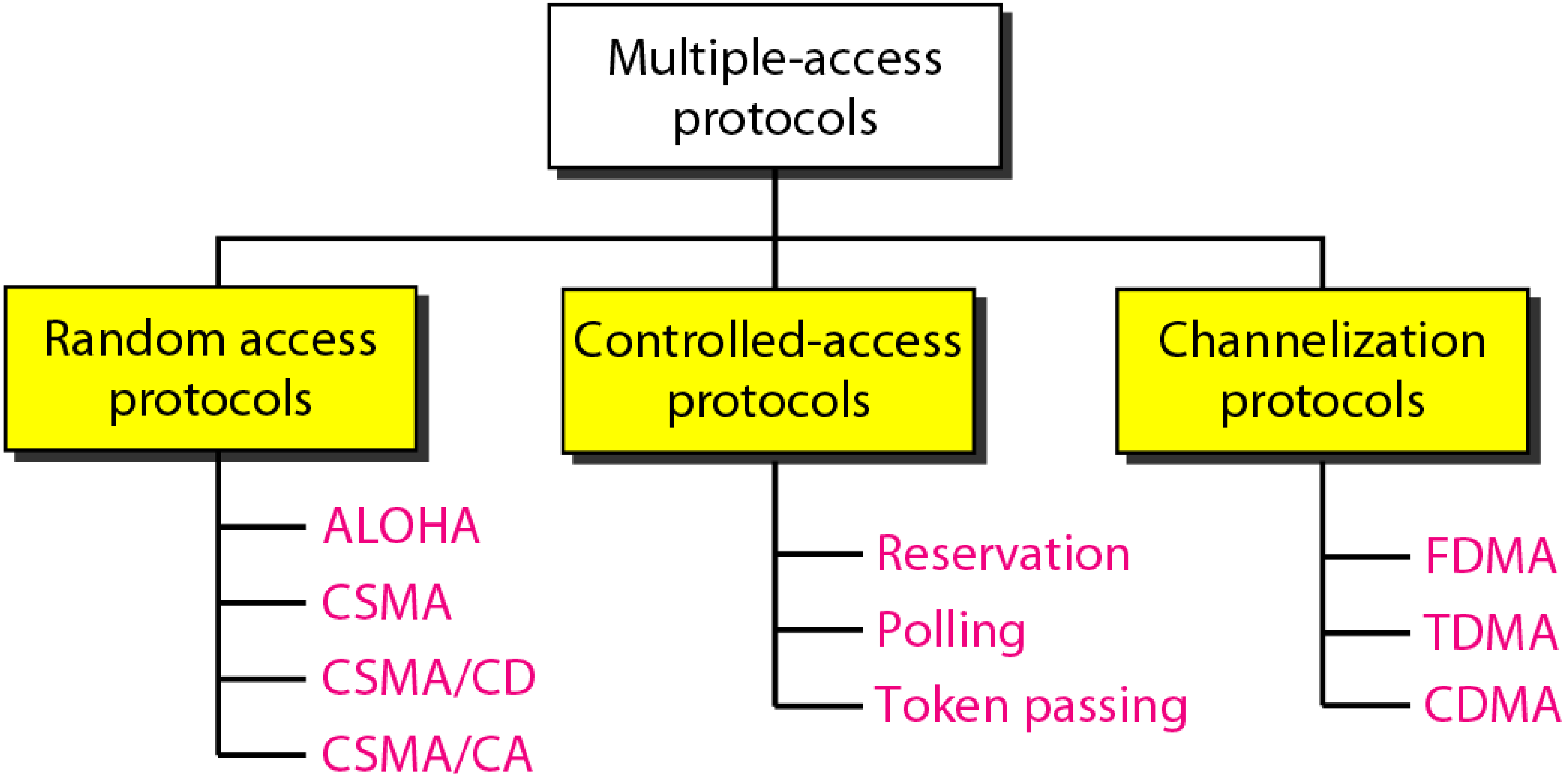
Since none of the traditional static channel allocation methods work well with bursty traffic, we will now explore dynamic methods.

Dynamic Channel Allocation

Multi-access protocols are based on the Dynamic Channel Allocation. The basic assumptions needed for channel allocation are

1. Independent Traffic
2. Single Channel
3. Observable Collisions
4. Continuous or Slotted Time
5. Carrier Sense or No Carrier Sense

Figure: **Taxonomy of multiple-access protocols**



RANDOM ACCESS

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

Two features give this method its name:

- First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called *random access*.

- Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called *contention methods*.

Topics discussed in this section:

1. **ALOHA**

2. **Carrier Sense Multiple Access (CSMA)**

3. **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

4. **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**

1. ALOHA

Aloha is a random access protocol.

It has been derived from a compound of the Hawaiian words:

- ***ALO*** means "share".
- ***HA*** means "essence of life".

History of ALOHA

Development of the ALOHA network was begun in 1968 at the University of Hawaii under the leadership of Norman Abramson. Their work has been extended by many researchers since then.

The goal was to use low-cost commercial radio equipment to connect users on Oahu(an island of Hawaii) and the other Hawaiian islands with a central time-sharing computer on the main Oahu campus.

ALOHAnet became operational in June, 1971, providing the first public demonstration of a wireless packet data network.

Although ALOHAnet was designed for wireless communication, there were two other media available for the application of an ALOHA channel – cables and satellites.

Cntd…

In the 1970s ALOHA random access was employed in the widely used Ethernet cable based network and then in the satellite network.

In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

There are two versions of ALOHA:

i. ***Pure Aloha***
ii. ***Slotted* Aloha**

They differ with respect to whether time is divided into discrete slots into which all frames must fit. Pure ALOHA does not require global time synchronization; slotted ALOHA does.

i). Pure Aloha

It allows stations to transmit whenever they have data to be sent.

When a station sends data it waits for an acknowledgement.

If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (T_B) and resends the data.

Since different stations wait for different amount of time, the probability of further collision decreases.

Figure: Frames in a pure ALOHA network

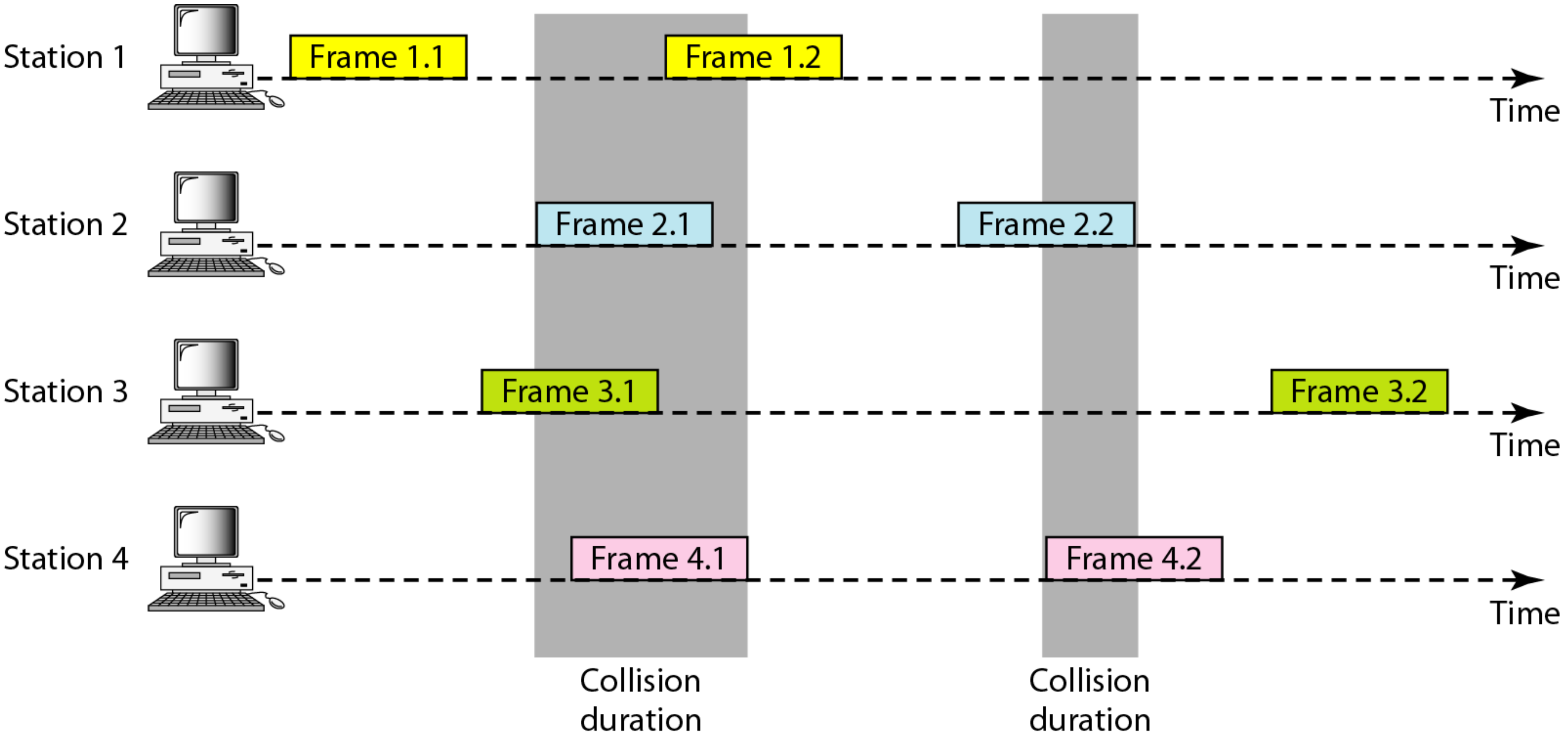
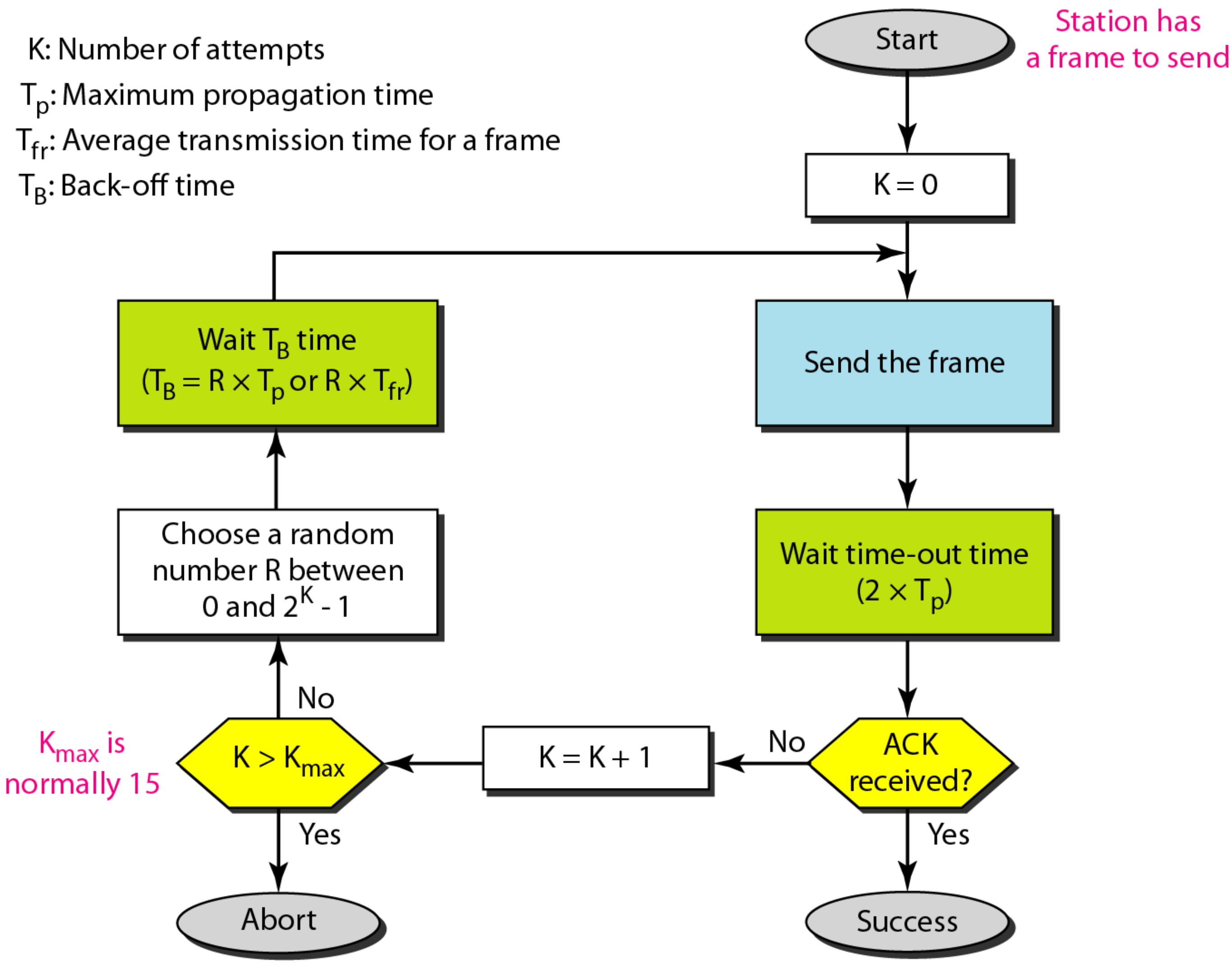


Figure: Procedure for pure ALOHA protocol



Example 4.1

The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s, we find

$$T_p = (600 \times 10^3) / (3 \times 10^8) = 2 \text{ ms.}$$

Now we can find the value of T_B for different values of K.

a. *For $K = 1$, the range is {0, 1}. The station needs to generate a random number with a value of 0 or 1. This means that T_B is either 0 ms (0 × 2) or 2 ms (1 × 2), based on the outcome of the random variable.*

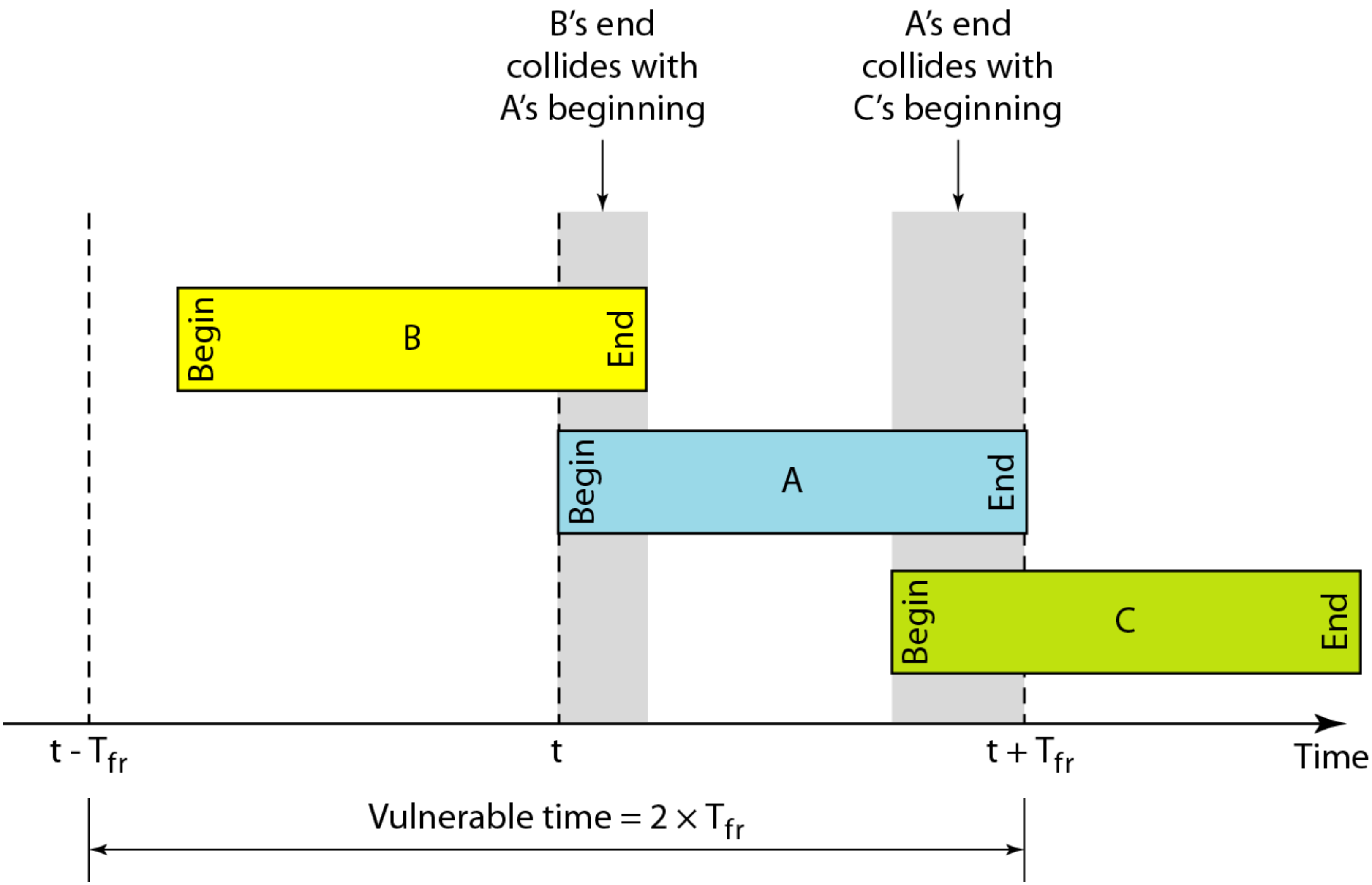
Example 4.1 (continued)

***b.** For K = 2, the range is {0, 1, 2, 3}. This means that T_B can be 0, 2, 4, or 6 ms, based on the outcome of the random variable.*

***c.** For K = 3, the range is {0, 1, 2, 3, 4, 5, 6, 7}. This means that T_B can be 0, 2, 4, . . . , 14 ms, based on the outcome of the random variable.*

***d.** We need to mention that if K > 10, it is normally set to 10.*

Figure: Vulnerable time for pure ALOHA protocol



Example 4.2

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

The frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the one 1-ms period that this station is sending.

Throughput or Efficiency

We will make the following assumptions:

- All frames are of constant length.
- The channel is noise-free; the errors are only due to collisions.
- Frames do not queue at individual stations.
- The channel acts as a Poisson process.

Since S represents the number of "good" or "succeed" transmissions per frame time, and G represents the total number of attempted transmissions per frame time, then we have:

$$S = G \quad * \text{ (Probability of good transmission)}$$

For Pure ALOHA, the probability of a successful transmission is e^{-2G} .

Cntd...

The relation between the offered traffic and the throughput is shown

$$S = G e^{-2G}$$

Which means that a small increase in the channel load, that is G, can drastically reduce its performance.

The maximum throughput occurs at G = 0.5, with S = 1/2e, which is about 0.184.

In other words, the best we can hope for is a channel utilization of 18.4%. This result is not very encouraging.

Note

The throughput for pure ALOHA is
$S = G \times e^{-2G}$.
The maximum throughput
$S_{max} = 0.184$ **when G= (1/2).**

Example 4.3

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. *1000 frames per second* **b.** *500 frames per second*

c. *250 frames per second.*

Solution

The frame transmission time is 200/200 kbps or 1 ms.

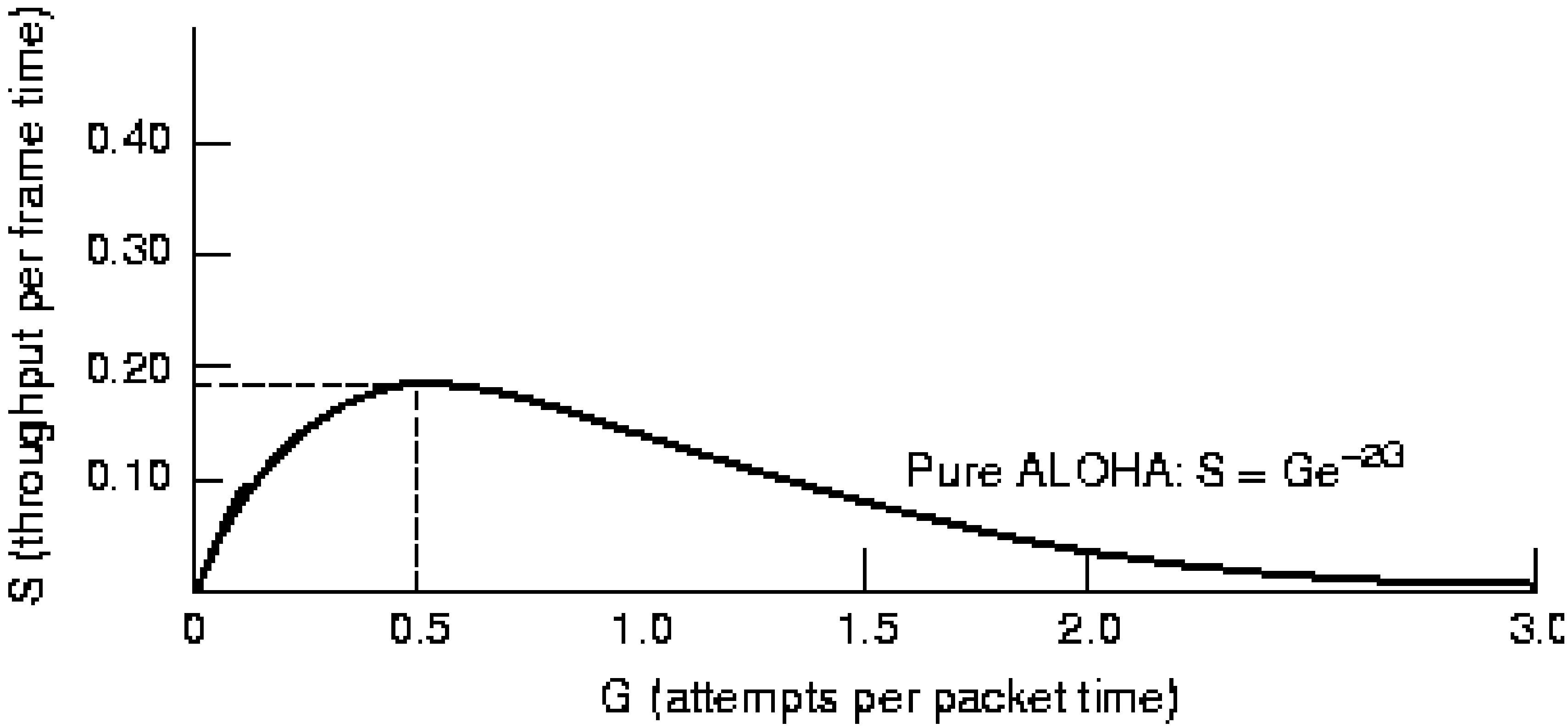
a. *If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.*

Example 4.3 (continued)

b. *If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.*

c. *If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.*

Figure: Pure ALOHA Offered Load vs. Throughput



Max at G = 0.5, S = 1/2e, only about 0.184 (18.4%)!

– Can we do better?

ii). Slotted Aloha

In 1972, Roberts published a method for doubling the capacity of Abramson's pure ALOHA system (Robert,1972).

His proposal was the time of shared channel is divide time into discrete intervals called slots.

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot.

Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

Cntd...

Assumptions made in Slotted ALOHA

- All frames consist of exactly L bits.
- Time is divided into slots of size L/R seconds (i.e., a slot equals the time to transmit one frame).
- Nodes start to transmit frames only at the beginnings of slots.
- The nodes are synchronized so that each node knows when the slots begin.
- If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.

Procedure for slotted ALOHA

While there is a new frame A to send do

1.Send frame A at a slot boundary and wait for ACK

2.If after "some" time ACK is received, successful transmission of frame.

3.If there is a collision, the node detects the collision before the end of the slot.

4.Wait a random amount of time and go to 1

End

The node retransmits its frame in each subsequent slot with probability P until the frame is transmitted without a collision.

Figure: ***Frames in a slotted ALOHA network***

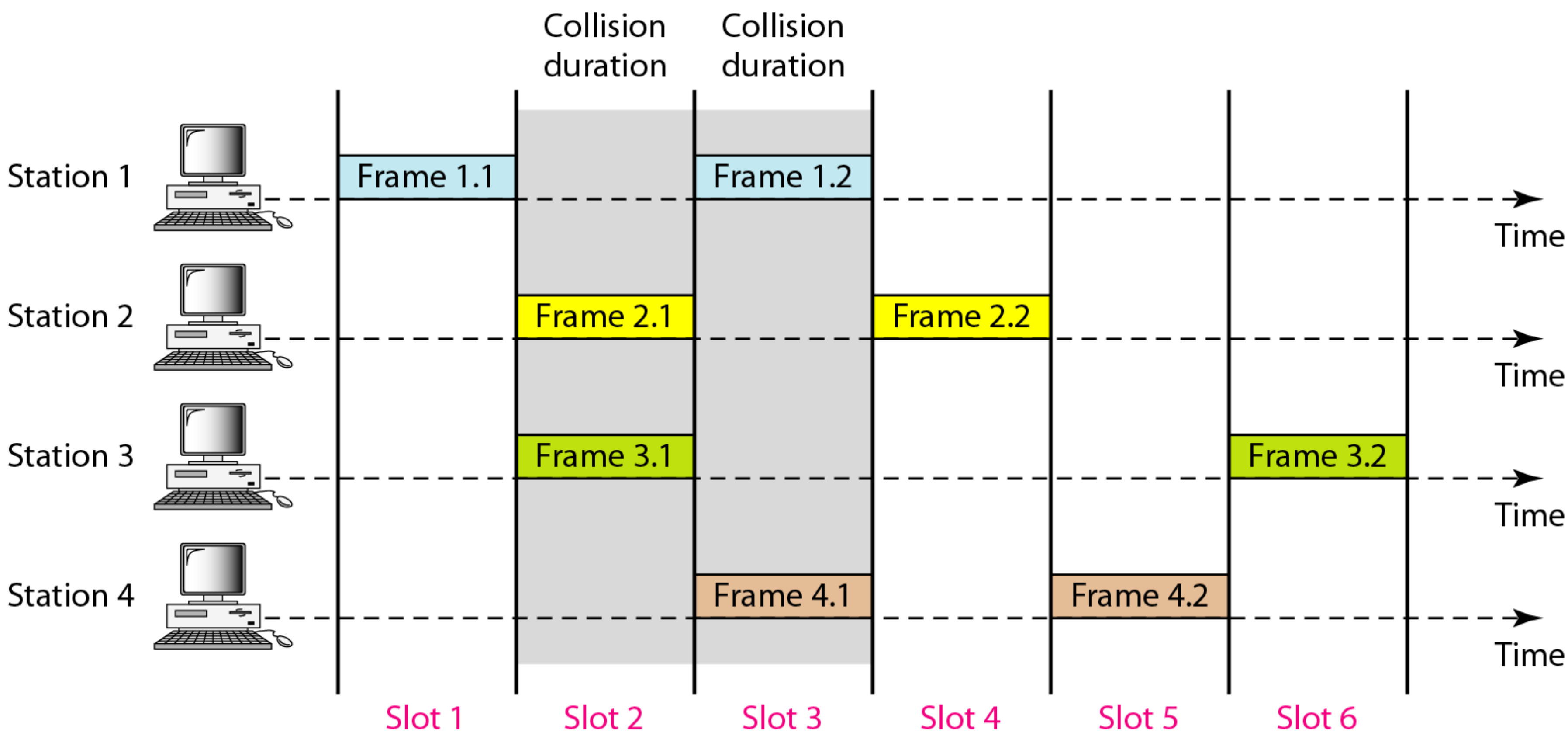
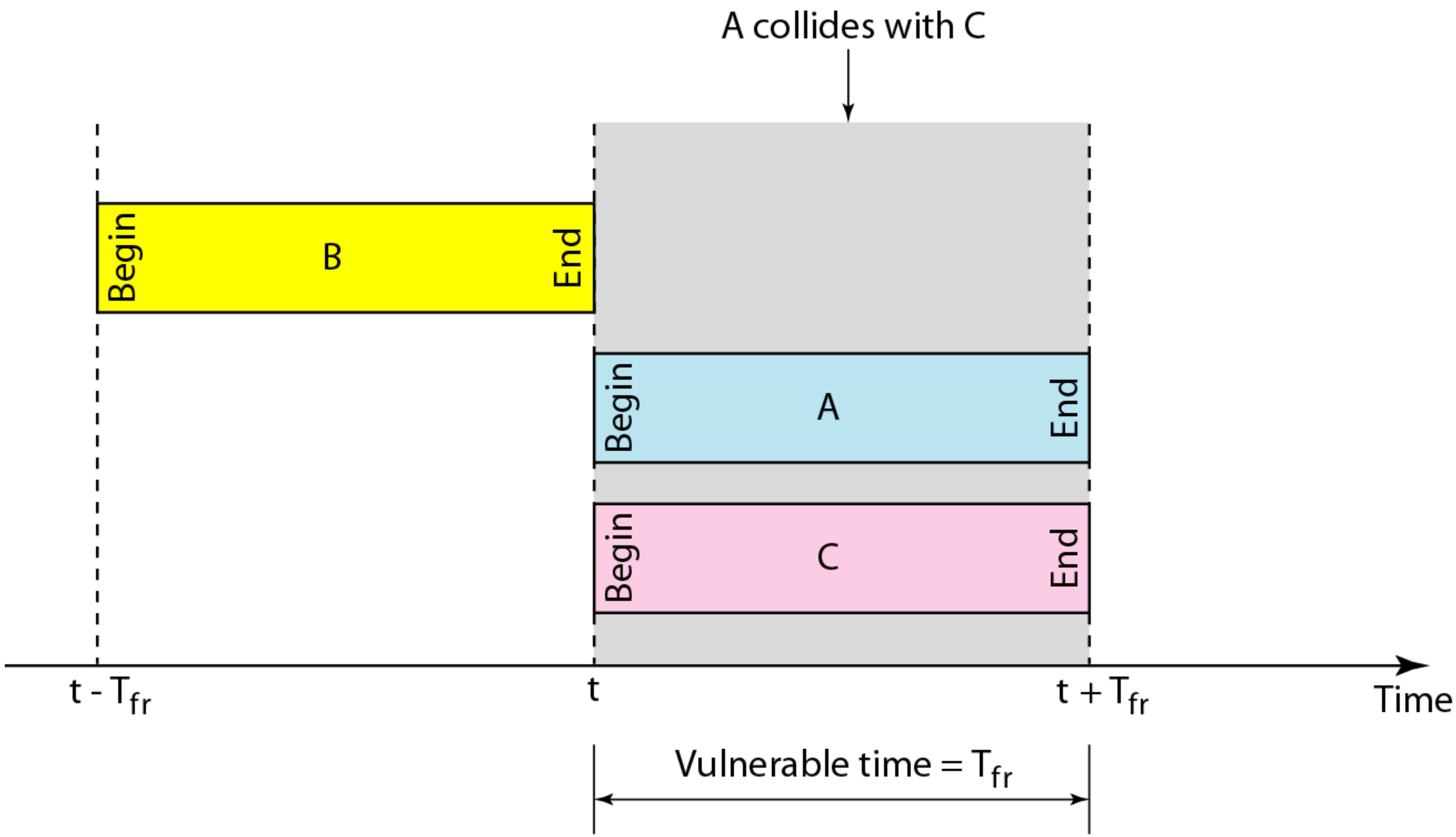


Figure: *Vulnerable time for slotted ALOHA protocol*



Note

The throughput for slotted ALOHA is

$$S = G \times e^{-G}\ .$$

The maximum throughput

$S_{max} = 0.368$ when G = 1.

Example 4.4

A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second *b. 500 frames per second*

c. 250 frames per second.

Solution

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 386 frames out of 1000 will probably survive.

Example 4.4 (continued)

b. *If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.*

c. *If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.*

Figure: Throughput vs. offered traffic for ALOHA systems

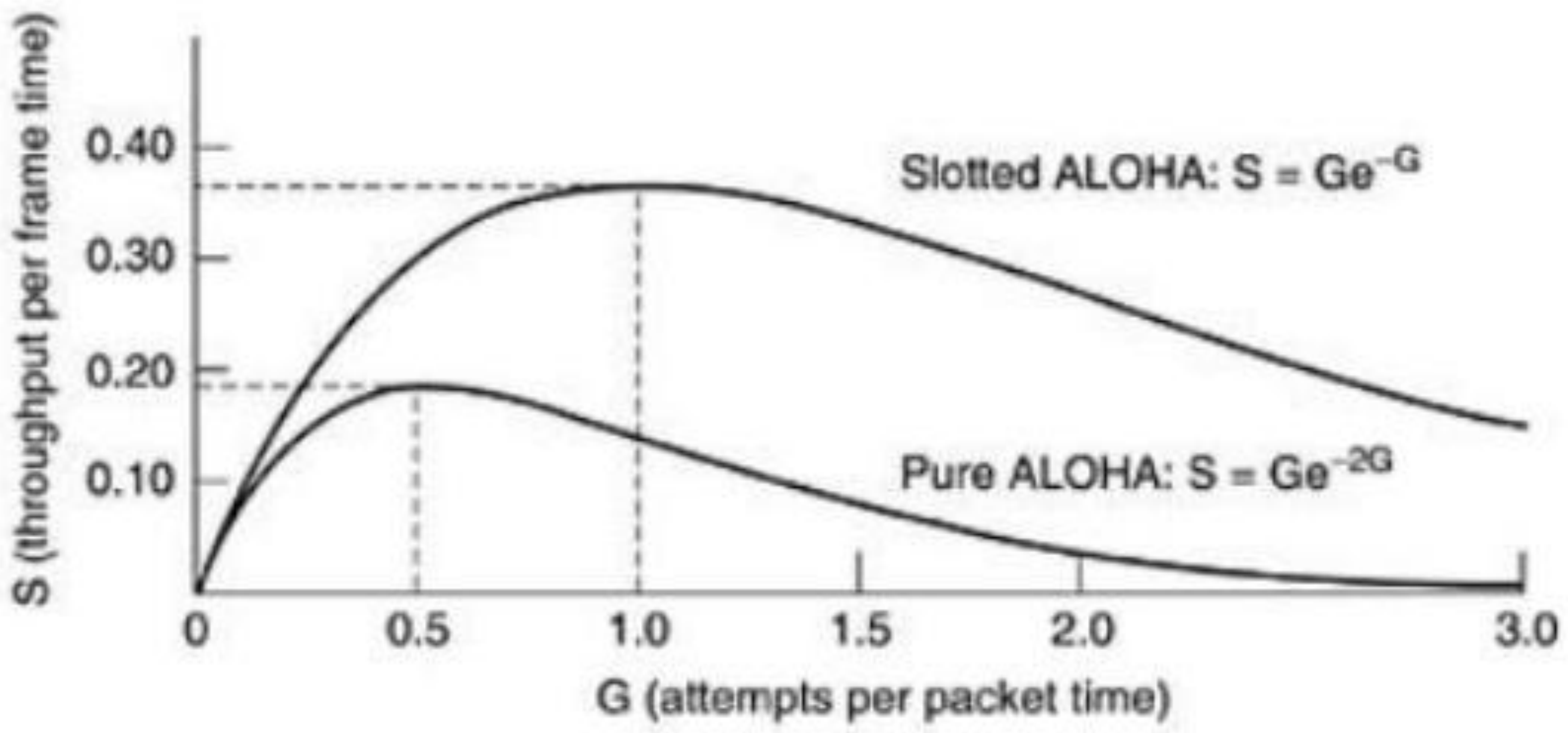


Table: Comparison of ALOHA systems

S.No	Pure ALOHA	Slotted ALOHA
1	Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
2	The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
3	Vulnerable time $= 2 \times T_{fr}$	Vulnerable time $= T_{fr}$
4	Probability of successful transmission of data pack $= G \times e^{-2G}$	Probability of successful transmission of data packet $= G \times e^{-G}$
5	Maximum efficiency = 18.4%	Maximum efficiency = 36.8%

Summary

- ALOHAis one of the random access protocol implemented at MAC Sublayer of data link layer.
- Chances of collisions are more in pure ALOHA as compared to Slotted ALOHA , but still it is least efficient as compared to other random access protocol such as CSMA(CD/CA).
- These protocols works efficiently when there are less active nodes.
- Modified versions of ALOHA are being used in some services such as Mobile Slotted ALOHA.

2. CSMA

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.

Principle of CSMA: “Sense before transmit” or “listen before talk”.

Carrier busy = Transmission is taking place.
Carrier idle = No transmission currently taking place.

The possibility of collision still exists because of propagation delay; a station may sense the medium and find it is idle, only because the first bit sent by another station has not yet been received.

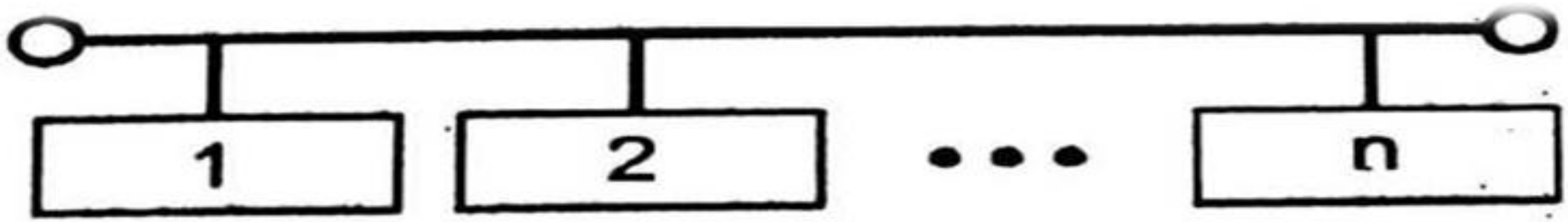


Fig . Broadcast network based on shared bus

Figure: Space/time model of the collision in CSMA

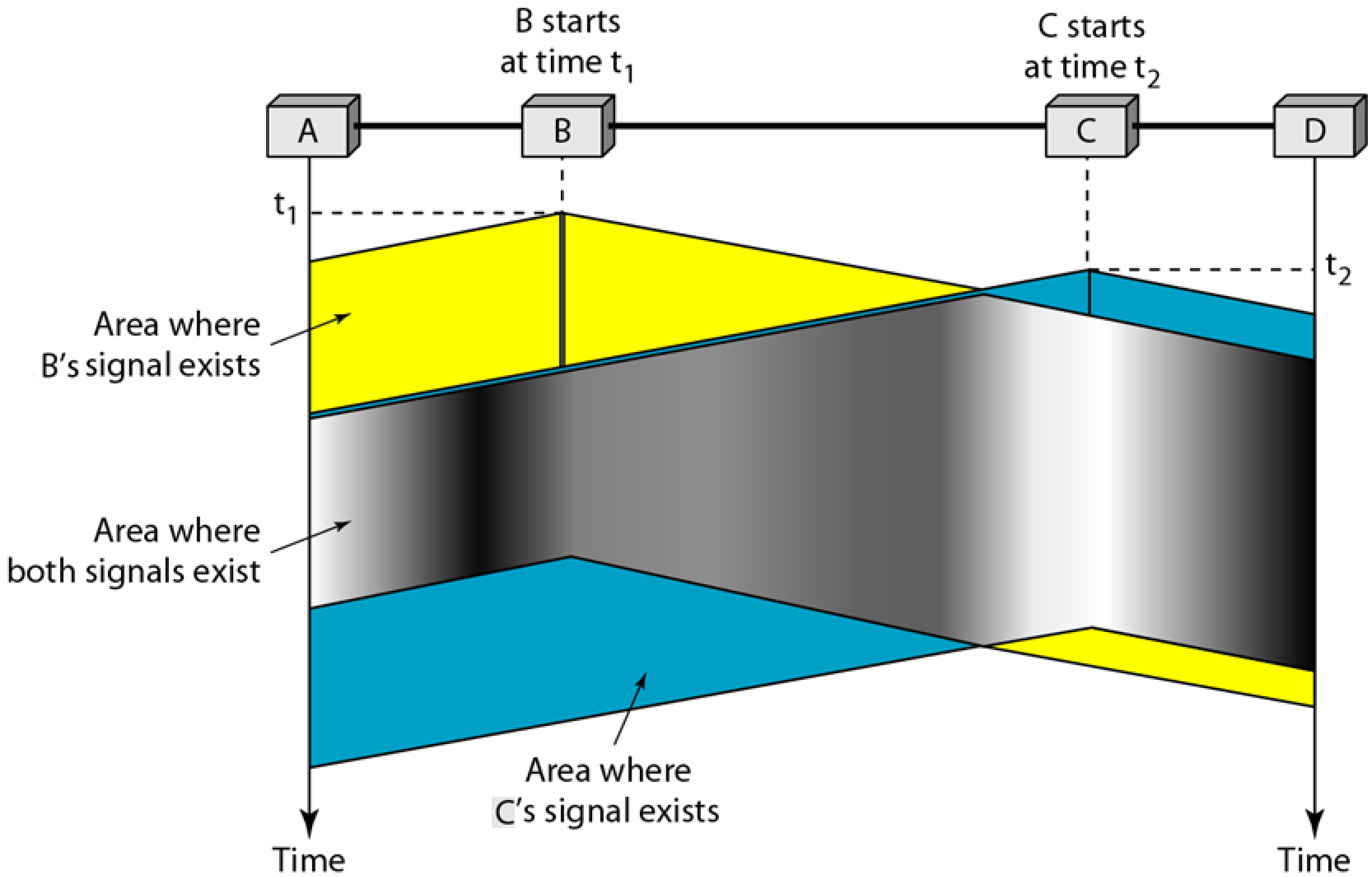
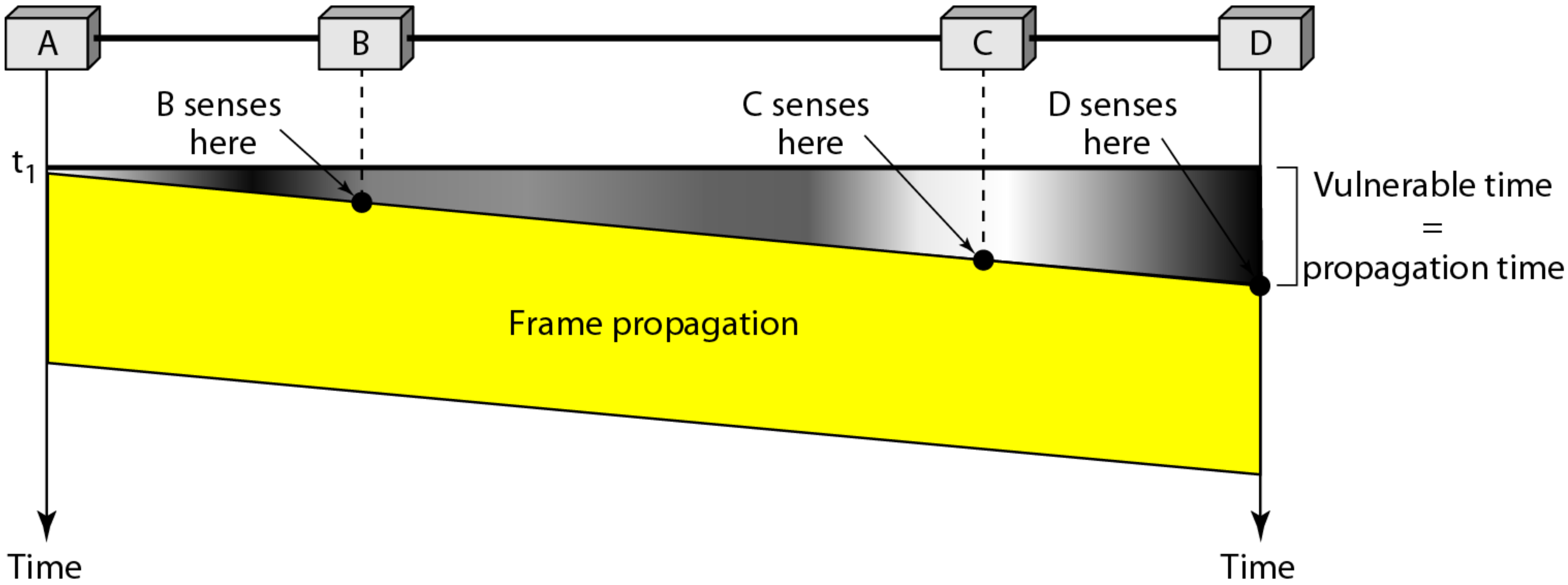


Figure: Vulnerable time in CSMA



Types of CSMA

1) 1-Persistent CSMA

2) Non-Persistent CSMA

3) P-Persistent CSMA

What should a station do if the channel is busy?
What should a station do if the channel is idle?

CSMA/CD (CSMA with Collision Detection)

CSMA/CA (CSMA with Collision Avoidance)

1). 1-Persistence CSMA

Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.

If channel is idle, the station transmits a frame immediately(with probability 1).

If busy, then it seems the transmission medium continuously until it becomes idle.

Since the station transmits the frame with the probability of 1 when the carrier or channel is idle, this scheme of CSMA is called as 1-Persistant CSMA.

Cntd…

The propagation delay has an important effect on the performance of the protocol.

This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

The longer the propagation delay, the more important this effect becomes, and the worst performance of the protocol.

2). Non-Persistence CSMA

Before sending the data, a station senses the channel. If no one else is sending, the station begins doing so itself.

However, if the channel is already in use, the station doesn't continuously sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.

Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

3). P-Persistence CSMA

It applies to slotted channels.

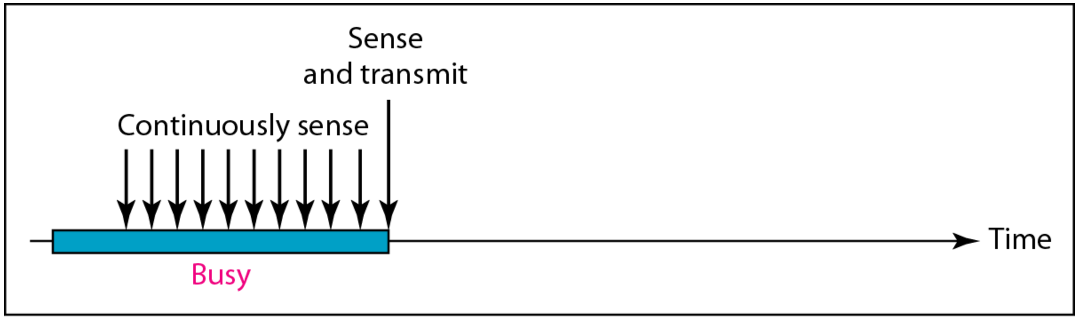
When a station becomes ready to send, it senses the channel.

If the station finds the line idle it follows these steps:

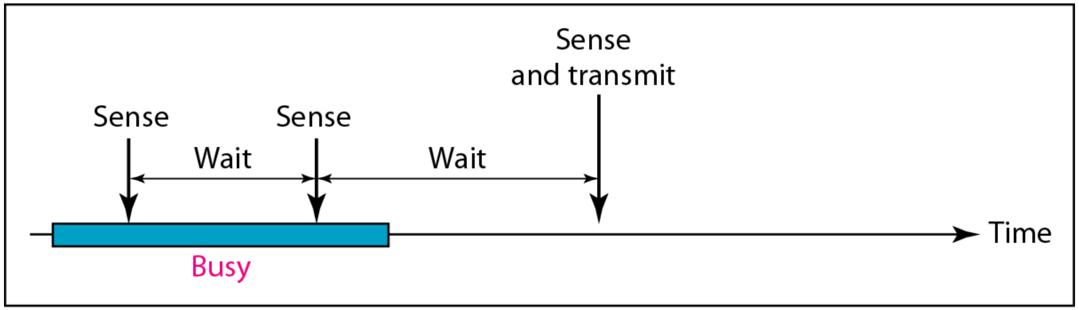
1. With probability P, the station sends its frame.
2. With probability Q = 1- P, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm.

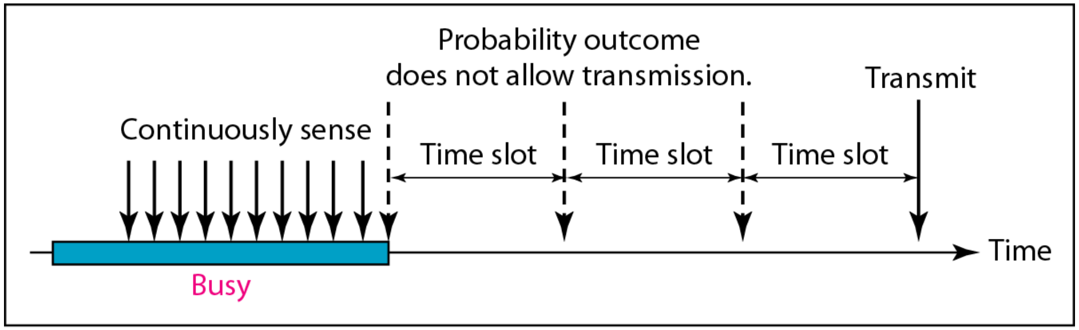
Figure: Behavior of three persistence methods



a. 1-persistent

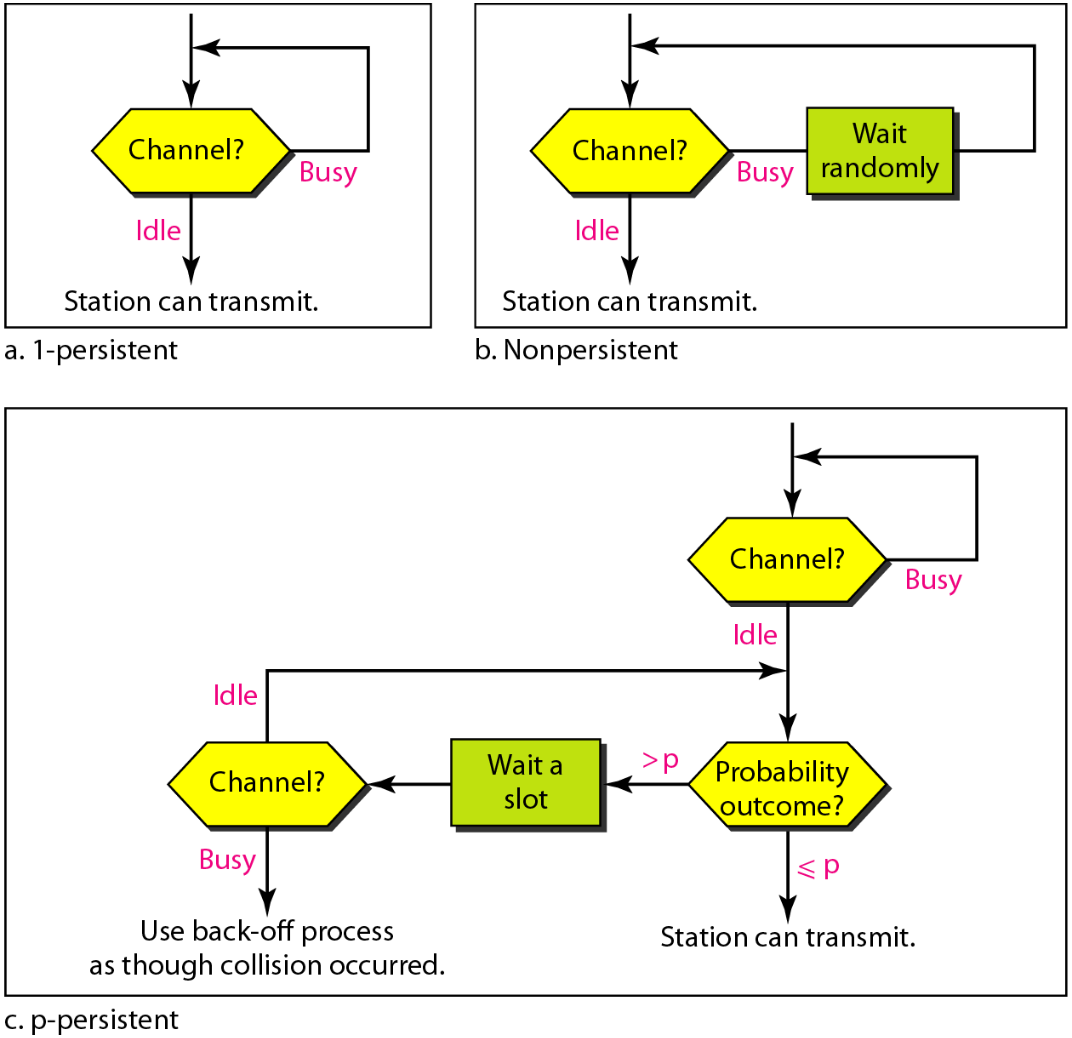


b. Nonpersistent



c. p-persistent

Figure: Flow diagram for three persistence methods



3. CSMA/CD

If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.

Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collision is detected.

Quickly terminating damaged frames saves time and bandwidth.

This protocol, known as CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sub layer.

Access method used by Ethernet: CSMA/CD

Figure: Energy level during transmission, idleness, or collision

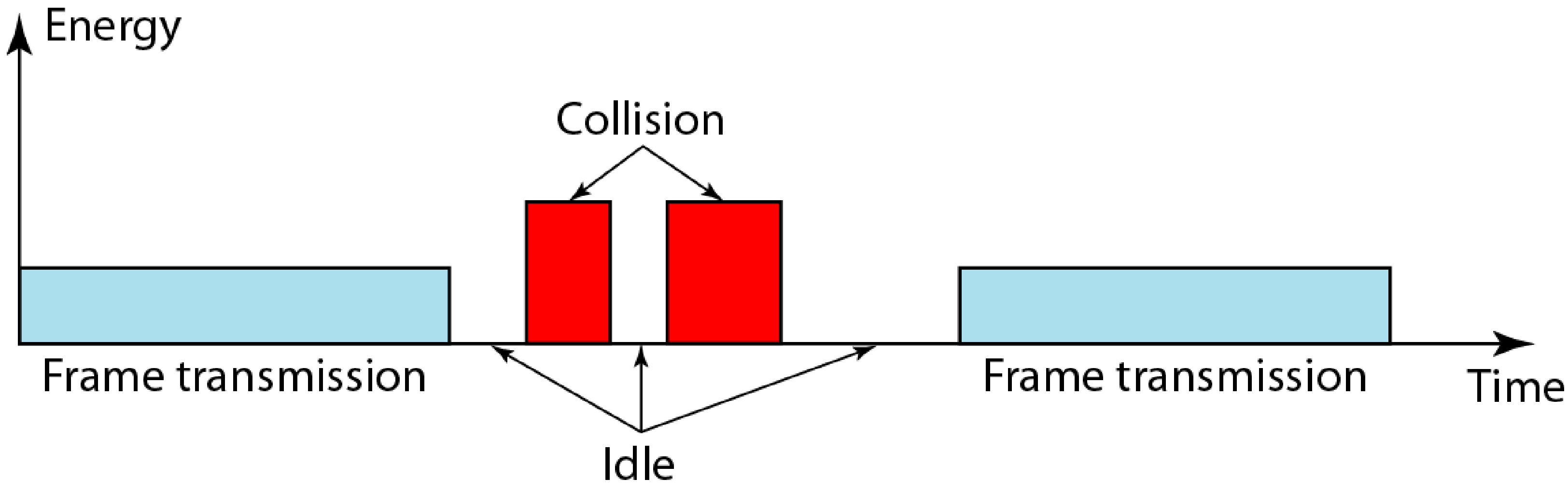


Figure: Collision of the first bit in CSMA/CD

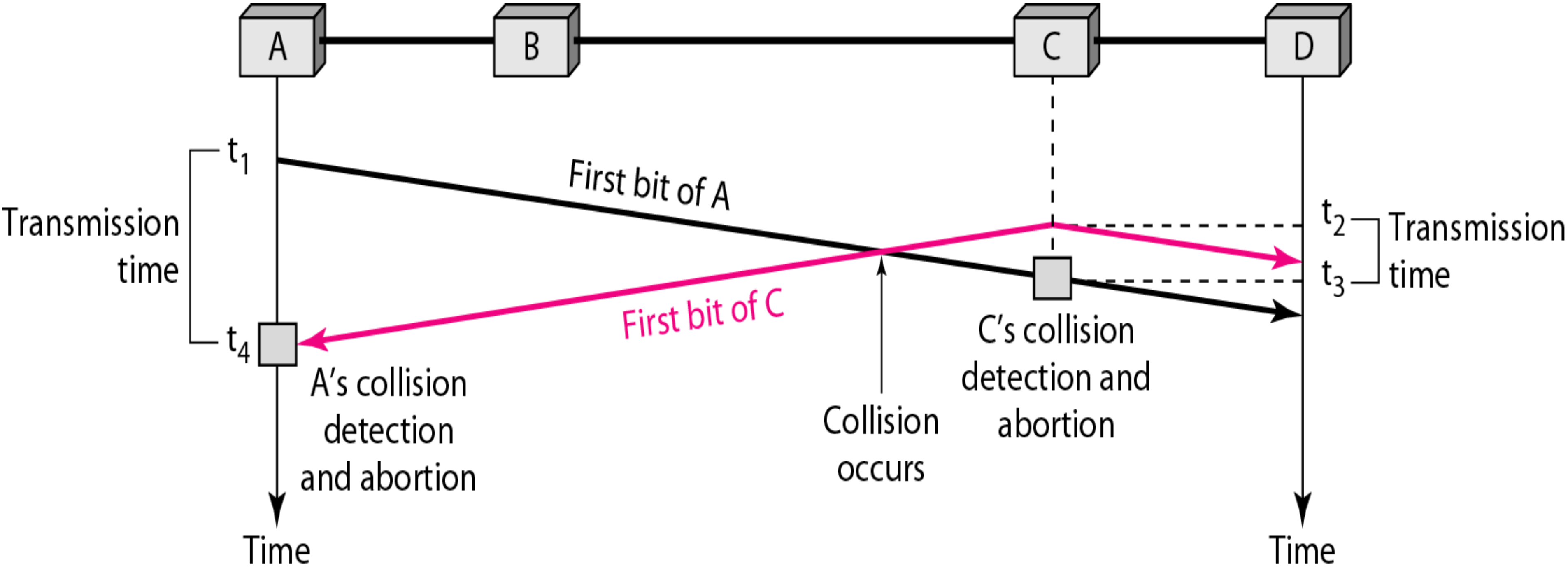


Figure: **Collision and abortion in CSMA/CD**

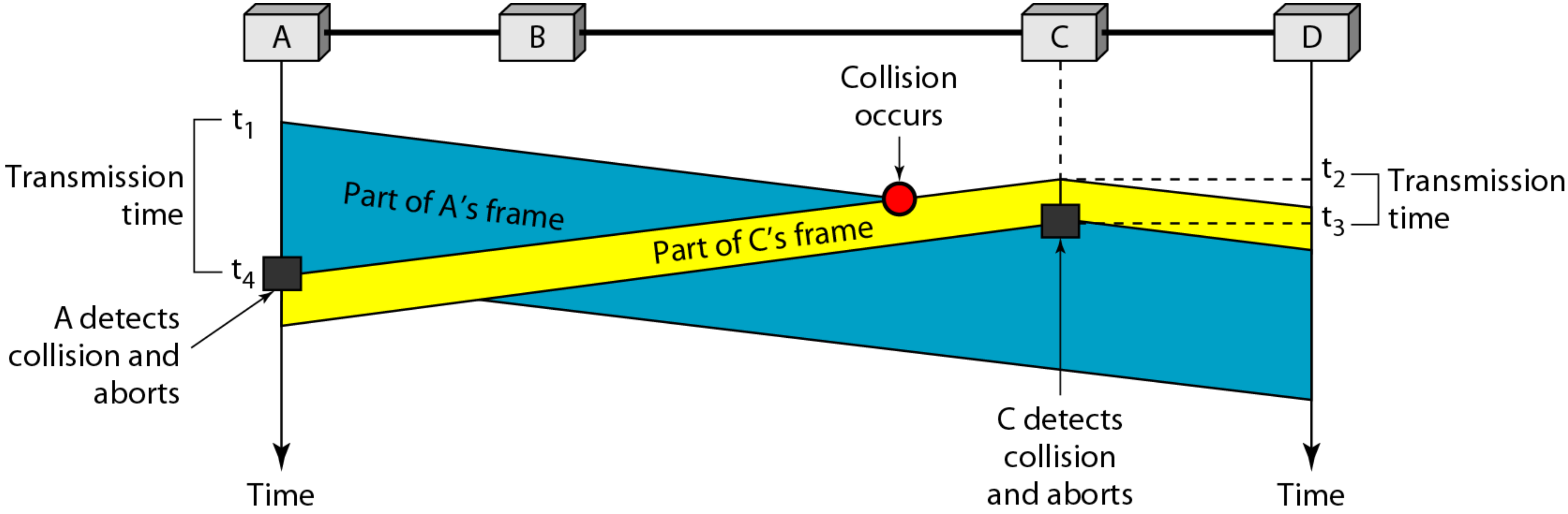


Figure: Minimum Frame size-Case Study example

Example 4.5

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2\ \mu s$. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

Figure: Flow diagram for the CSMA/CD

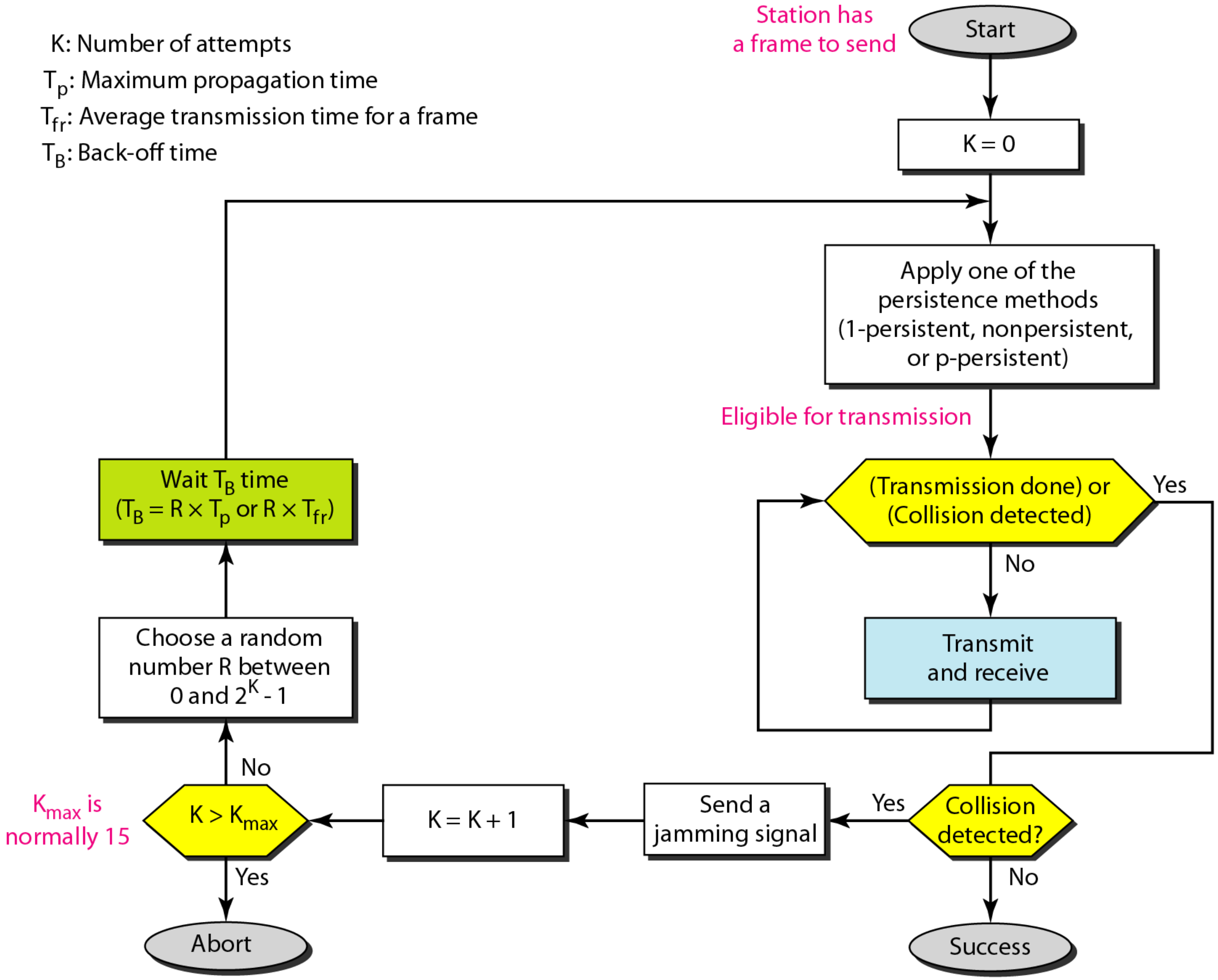
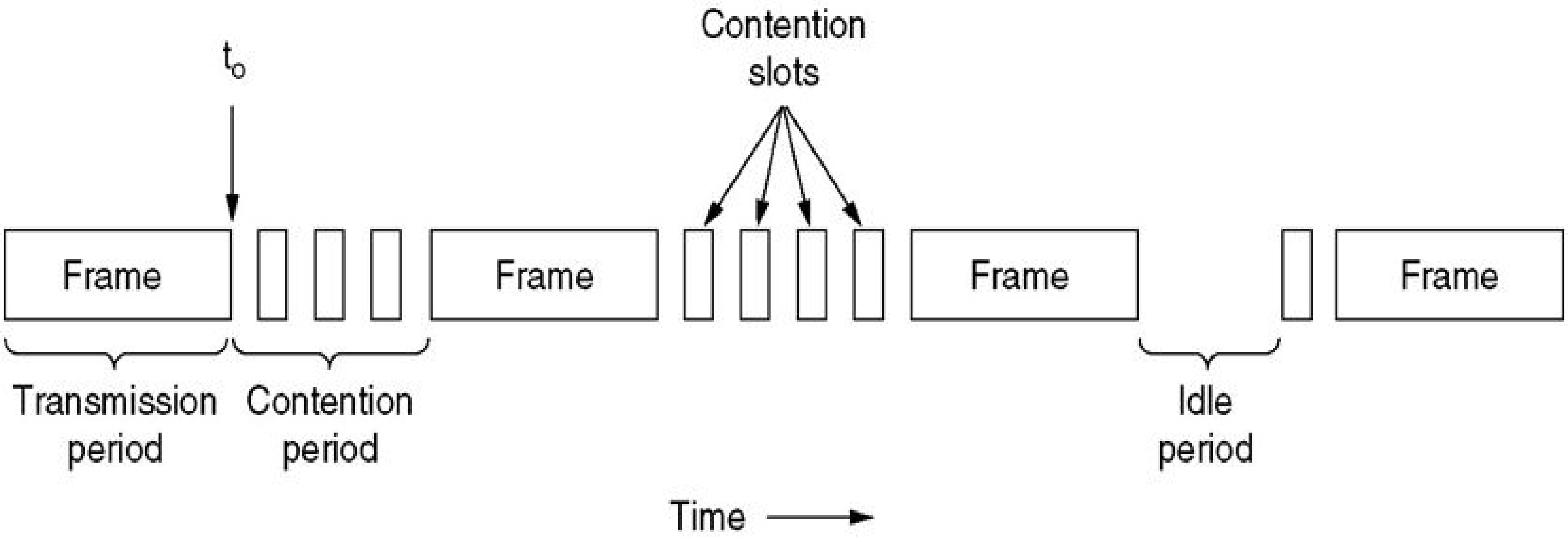


Figure: Timing in CSMA/CD



CSMA/CD can be in one of three states: contention, transmission, or idle.

4. CSMA/CA

Carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be 'idle'.

CSMA/CA was invented for wireless networks.

Collisions are avoided through the use of CSMA/CA's three strategies:

i. Inter Frame Space (IFS)
ii. Contention window
iii. Acknowledgments.

i). Inter Frame Space (IFS)

First, collisions are avoided by deferring transmission even if the channel is found idle.

When an idle channel is found, the station does not send immediately. It waits for a period of time called the inter frame space or IFS.

After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window (described next).

The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned shorter IFS has a higher priority.

ii). Contention Window

The contention window is an amount of time divided into slots.

A station that is ready to send chooses a random number of slots as its wait time.

The number of slots in the window changes according to the binary exponential back off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle.

iii). Acknowledgement

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission.

The positive acknowledgment and the time- out timer can help guarantee that the receiver has received the frame.

Figure: Timing in CSMA/CA

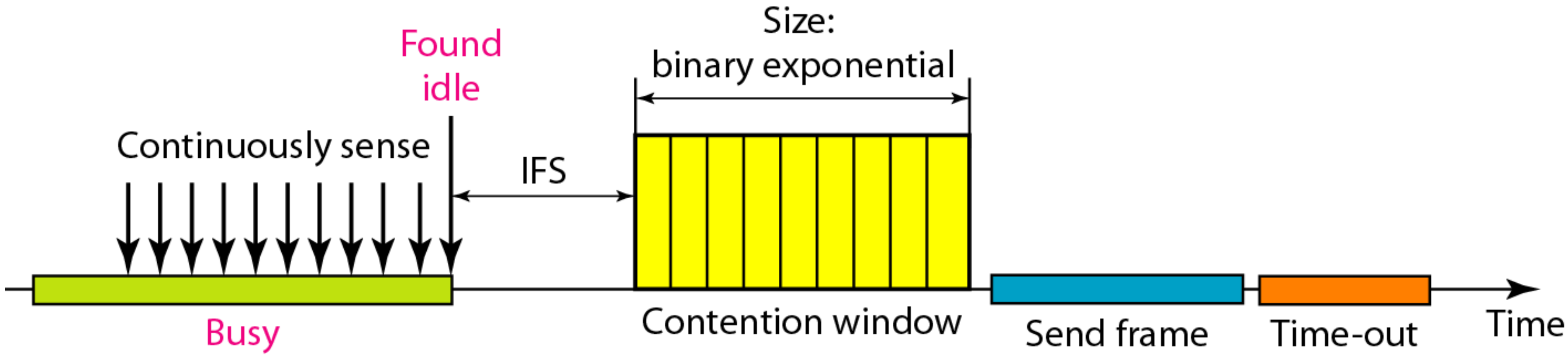
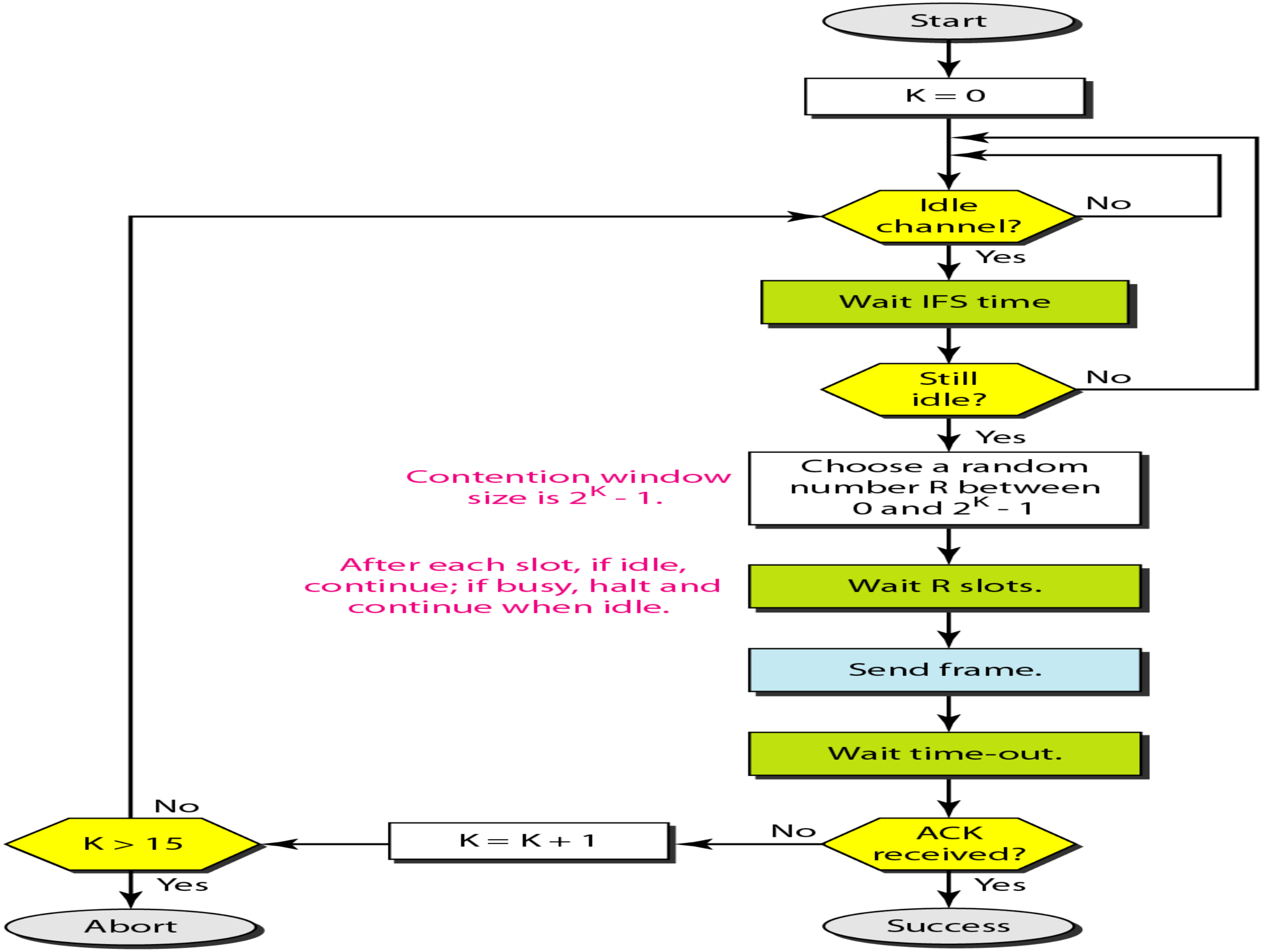


Figure: Flow diagram for CSMA/CA



Note

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

Note

In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.


ANY QUERIES