Module
5

Broadcast Communication Networks

Lesson 2

Medium Access Control (MAC) Techniques

Specific Instructional Objectives

At the end of this lesson, the student will be able to:

- Explain the goals and requirements of Medium Access Control (MAC) techniques
- Identify the key issues related to MAC techniques.
- Give an outline of possible MAC techniques.
- Distinguish between Centralized and Distributed MAC techniques.
- Classify various contention based techniques such as ALHOA, CSMA, CSMA/CD and CSMA/CA
- Compare performance of contention based techniques
- Explain round robin based MAC techniques.
    - Polling
    - Token passing

5.2.1 Introduction

A network of computers based on multi-access medium requires a protocol for effective sharing of the media. As only one node can send or transmit signal at a time using the broadcast mode, the main problem here is how different nodes get control of the medium to send data, that is *"who goes next?"*. The protocols used for this purpose are known as *Medium Access Control (MAC) techniques*. The key issues involved here are - *Where* and *How* the control is exercised.

'Where' refers to whether the control is exercised in a *centralised* or *distributed* manner. In a centralised system a master node grants access of the medium to other nodes. A centralized scheme has a number of advantages as mentioned below:

- Greater control to provide features like priority, overrides, and guaranteed bandwidth.
- Simpler logic at each node.
- Easy coordination.

Although this approach is easier to implement, it is vulnerable to the failure of the master node and reduces efficiency. On the other hand, in a distributed approach all the nodes collectively perform a medium access control function and dynamically decide which node to be granted access. This approach is more reliable than the former one.

'How' refers to in what manner the control is exercised. It is constrained by the topology and trade off between cost-performance and complexity. Various approaches for medium access control are shown in Fig. 5.2.1. The MAC techniques can be broadly divided into four categories; *Contention-based*, *Round-Robin*, *Reservation-based* and. *Channelization-based*. Under these four broad categories there are specific techniques, as shown in Fig. 5.2.1. In this lesson we shall concentrate of the MACs of the first two categories, which have been used in the legacy LANs of the IEEE standard. The CSMA/CA, a collision-free protocol used in wireless LAN, will be presented in Lesson 5.5. Channalization-based MACs, which are used in cellular telephone networks, will be

covered in Lesson 5.6. And the reservation-based MACs, which are used in satellite networks, will be discussed in Lesson 5.7.

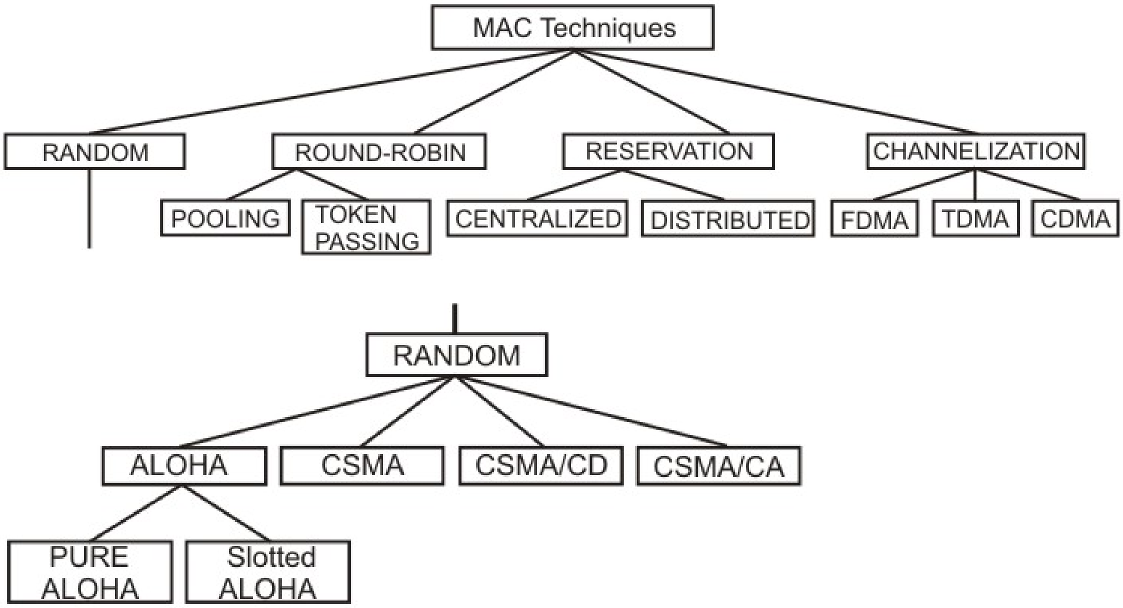


Figure 5.2.1 Possible MAC techniques

5.2.2 Goals of MACs

Medium Access Control techniques are designed with the following goals in mind.

- **Initialisation**: The technique enables network stations, upon power-up, to enter the state required for operation.
- **Fairness**: The technique should treat each station fairly in terms of the time it is made to wait until it gains entry to the network, access time and the time it is allowed to spend for transmission.
- **Priority**: In managing access and communications time, the technique should be able to give priority to some stations over other stations to facilitate different type of services needed.
- **Limitations to one station**: The techniques should allow transmission by one station at a time.
- **Receipt**: The technique should ensure that message packets are actually received (no lost packets) and delivered only once (no duplicate packets), and are received in the proper order.
- **Error Limitation**: The method should be capable of encompassing an appropriate error detection scheme.
- **Recovery**: If two packets collide (are present on the network at the same time), or if notice of a collision appears, the method should be able to recover, i.e. be able to halt all the transmissions and select one station to retransmit.

- **Reconfigurability**: The technique should enable a network to accommodate the addition or deletion of a station with no more than a noise transient from which the network station can recover.
- **Compatibility**: The technique should accommodate equipment from all vendors who build to its specification.
- **Reliability**: The technique should enable a network to confine operating inspite of a failure of one or several stations.

5.2.3 Round Robin Techniques

In Round Robin techniques, each and every node is given the chance to send or transmit by rotation. When a node gets its turn to send, it may either decline to send, if it has no data or may send if it has got data to send. After getting the opportunity to send, it must relinquish its turn after some maximum period of time. The right to send then passes to the next node based on a predetermined logical sequence. The right to send may be controlled in a centralised or distributed manner. *Polling* is an example of centralised control and *token passing* is an example of distributed control as discussed below.

5.2.3.1 Polling

The mechanism of polling is similar to the roll-call performed in a classroom. Just like the teacher, a controller sends a message to each node in turn. The message contains the address of the node being selected for granting access. Although all nodes receive the message, only the addressed node responds and then it sends data, if any. If there is no data, usually a *"poll reject"* message is sent back. In this way, each node is interrogated in a round-robin fashion, one after the other, for granting access to the medium. The first node is again polled when the controller finishes with the remaining codes.

The polling scheme has the flexibility of either giving equal access to all the nodes, or some nodes may be given higher priority than others. In other words, priority of access can be easily implemented.

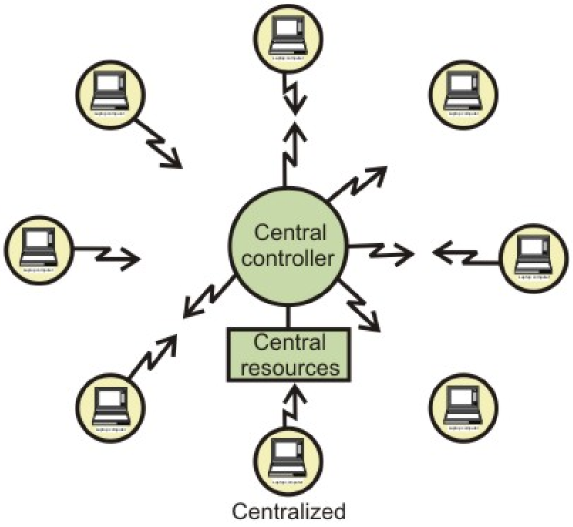


Figure 5.2.2 Polling using a central controller

Polling can be done using a central controller, which may use a frequency band to send outbound messages as shown in Fig. 5.2.2. Other stations share a different frequency to send inbound messages. The technique is called frequency-division duplex approach (FDD). Main drawbacks of the polling scheme are high overhead of the polling messages and high dependence on the reliability of the controller.

Polling can also be accomplished without a central controller. Here, all stations receive signals from other stations as shown in Fig. 5.2.3. Stations develop a polling order list, using some protocol.

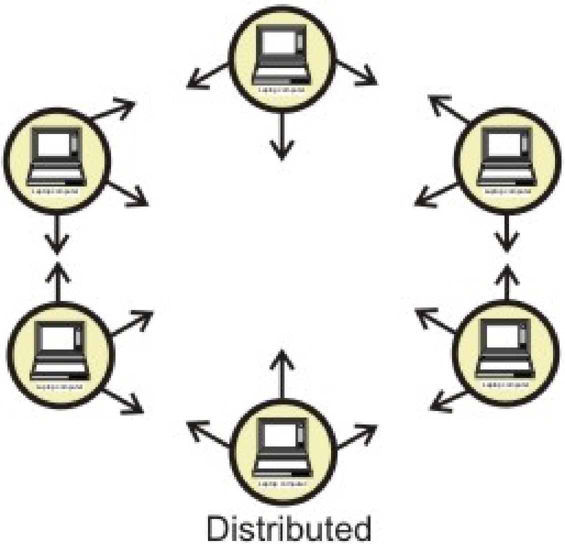


Figure 5.2.2 Polling in a distributed manner

5.2.3.2 Token Passing

In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a *token*. A *token* is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node. Token passing can be used with both broadcast (token bus) and sequentially connected (token ring) type of networks with some variation in the details as considered in the next lesson.

In case of token ring, token is passed from a node to the physically adjacent node. On the other hand, in the token bus, token is passed with the help of the address of the nodes, which form a logical ring. In either case a node currently holding the token has the ‘right to transmit’. When it has got data to send, it removes the token and transmits the data and then forwards the token to the next logical or physical node in the ring. If a node currently holding the token has no data to send, it simply forwards the token to the next node. The token passing scheme is efficient compared to the polling technique, but it relies on the correct and reliable operation of all the nodes. There exists a number of potential problems, such as *lost token*, *duplicate token*, *and insertion of a node*, *removal of a node,* which must be tackled for correct and reliable operation of this scheme.

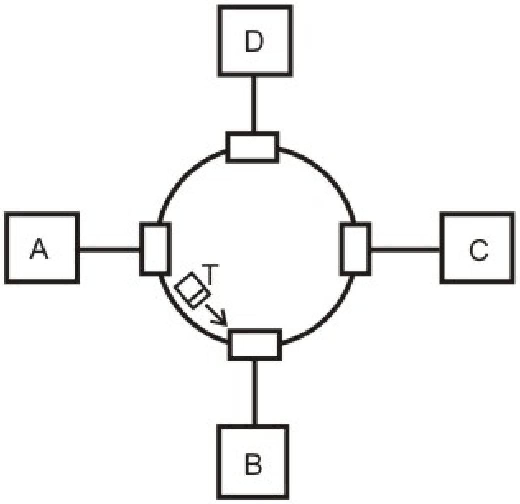


Figure 5.2.3 A token ring network

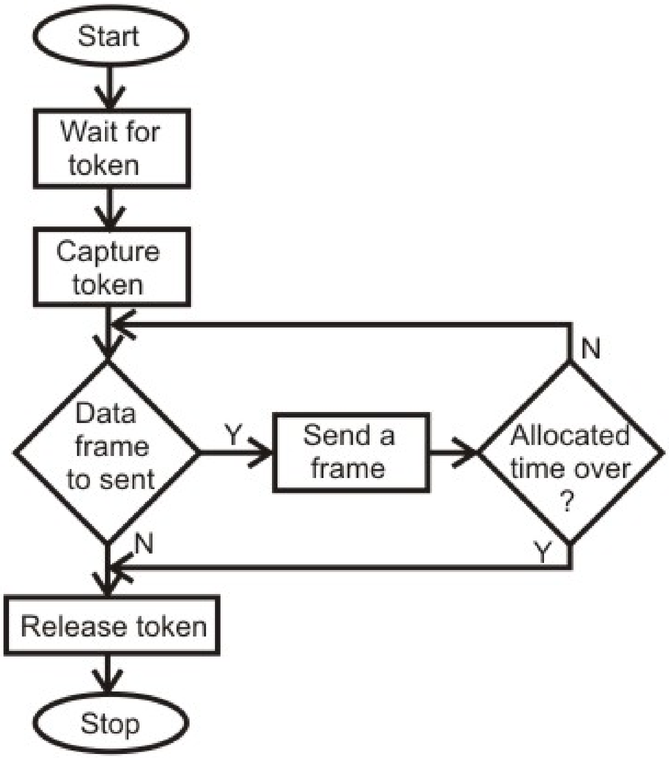


Figure 5.2.4 Token passing mechanism

Performance: Performance of a token ring network can be represented by two parameters; *throughput*, which is a measure of the successful traffic, and *delay*, which is a measure of time between when a packet is ready and when it is delivered. A station starts sending a packet at $t = t_0$, completes transmission at $t = t_0 + a$, receives the tail at $t_0 + 1 + a$. So, the average time (delay) required to send a token to the next station = a/N. and throughput, $S = 1/(1 + a/N)$ for a<1 and $S = 1/a(1 + 1/N)$ for a>1.

5.2.4 Contention-based Approaches

Round-Robin techniques work efficiently when majority of the stations have data to send most of the time. But, in situations where only a few nodes have data to send for brief periods of time, Round-Robin techniques are unsuitable. Contention techniques are suitable for bursty nature of traffic. In contention techniques, there is no centralised control and when a node has data to send, it contends for gaining control of the medium. The principle advantage of contention techniques is their simplicity. They can be easily implemented in each node. The techniques work efficiently under light to moderate load, but performance rapidly falls under heavy load.

5.2.4.1 ALOHA

The ALOHA scheme was invented by Abramson in 1970 for a packet radio network connecting remote stations to a central computer and various data terminals at the campus of the university of Hawaii. A simplified situation is shown in Fig. 5.2.5. Users are allowed random access of the central computer through a common radio frequency band f_1 and the computer centre broadcasts all received signals on a different frequency band f_2. This enables the users to monitor packet collisions, if any. The protocol followed by the users is simplest; whenever a node has a packet to sent, it simply does so. The scheme, known as *Pure ALOHA*, is truly a *free-for-all* scheme. Of course, frames will suffer collision and colliding frames will be destroyed. By monitoring the signal sent by the central computer, after the maximum round-trip propagation time, an user comes to know whether the packet sent by him has suffered a collision or not.

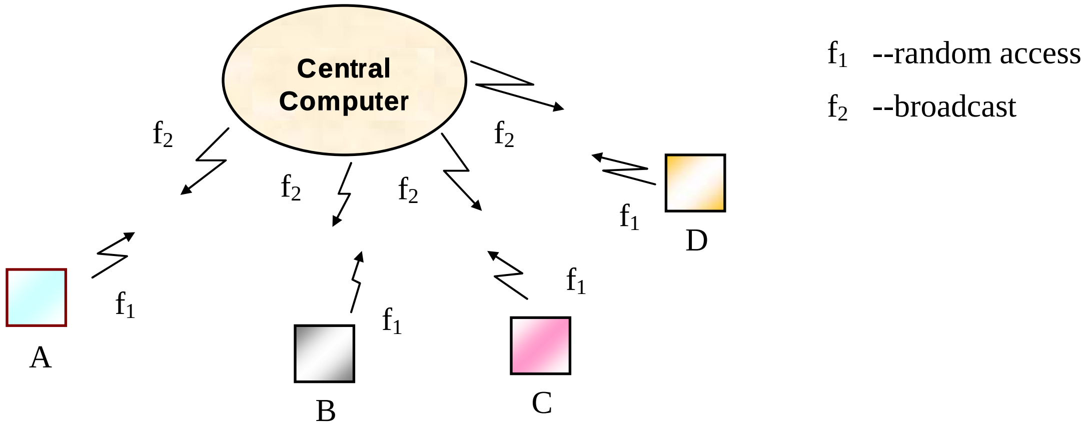


Figure 5.2.5 Simplified ALOHA scheme for a packet radio system

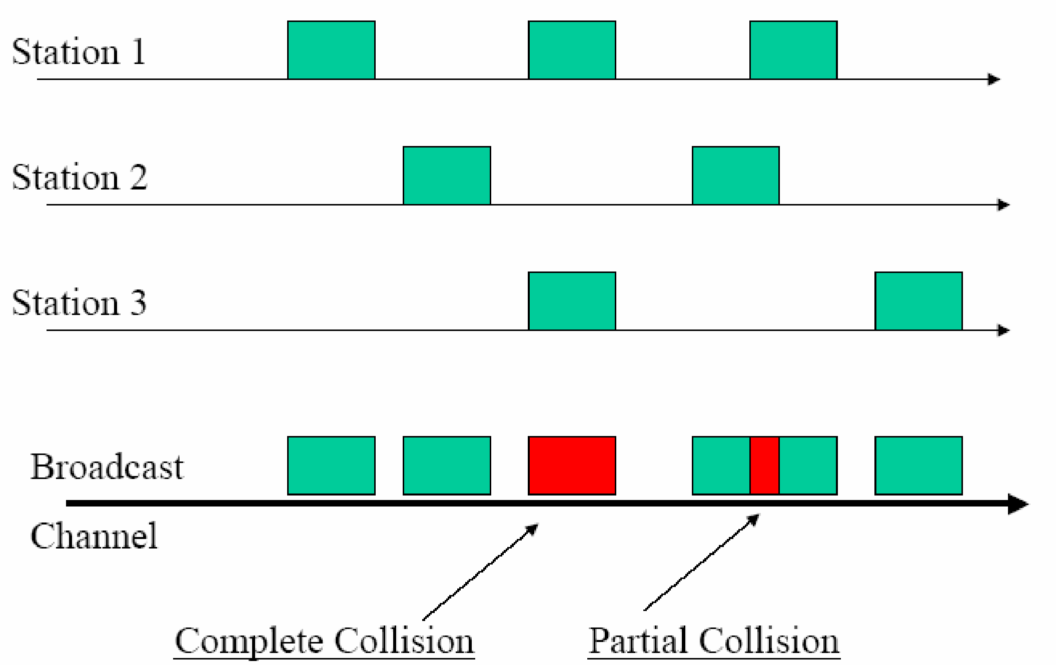


Figure 5.2.6 Collision in Pure ALOHA

It may be noted that if all packets have a fixed duration of τ (shown as F in Figure 5.2.7), then a given packet A will suffer collision if another user starts to transmit at any time from τ before to until τ after the start of the packet A as shown in Fig. 5.2.6. This gives a vulnerable period of 2τ. Based on this assumption, the channel utilization can be computed. The channel utilization, expressed as throughput S, in terms of the offered load G is given by $S=Ge^{-2G}$.

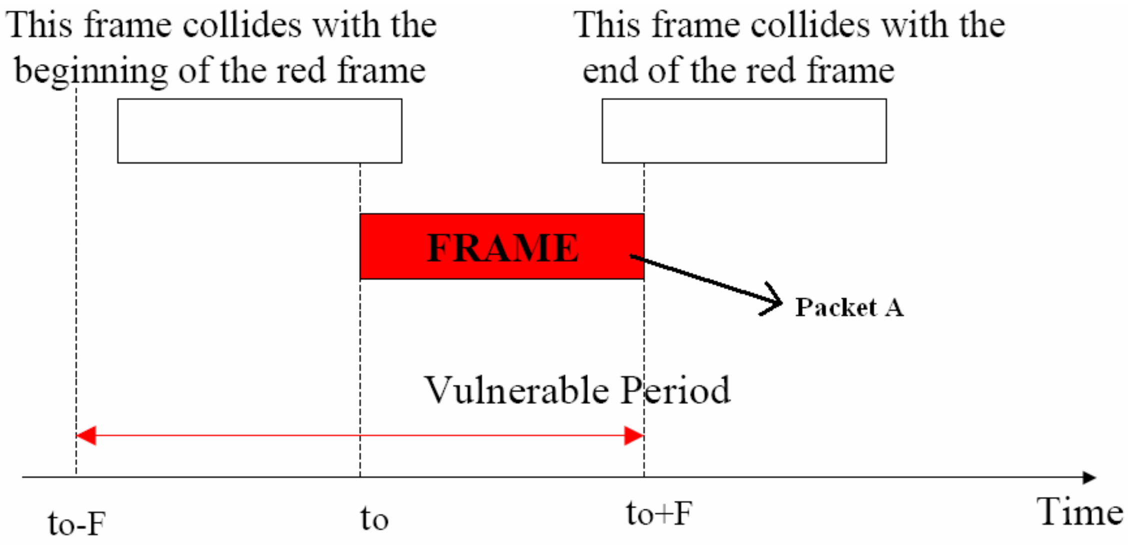

This frame collides with the beginning of the red frame
This frame collides with the end of the red frame
FRAME
Packet A
Vulnerable Period
to-F
to
to+F
Time

Figure 5.2.7 Vulnerable period in Pure ALOHA

Based on this, the best channel utilisation of 18% can be obtained at 50 percent of the offered load as shown in Fig. 5.2.8. At smaller offered load, channel capacity is underused and at higher offered load too many collisions occur reducing the throughput. The result is not encouraging, but for such a simple scheme high throughput was also not expected.

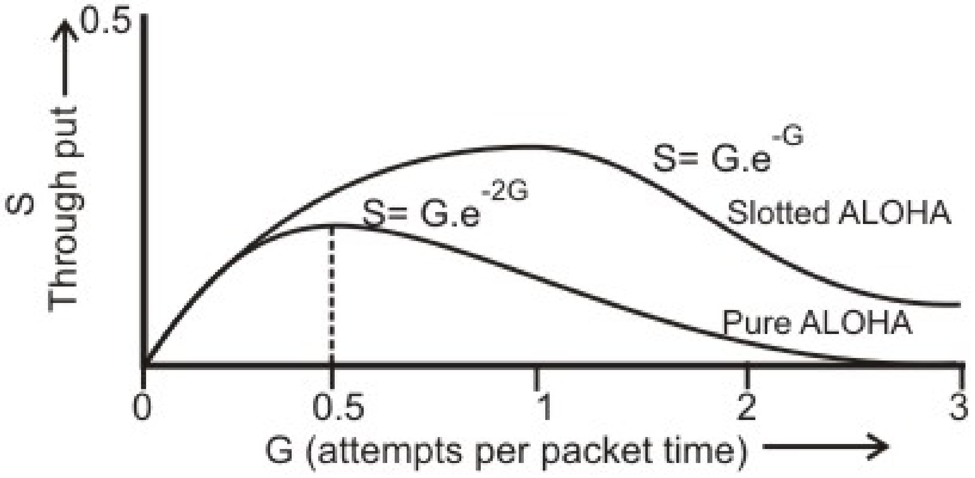


Figure 5.2.8 Throughput versus offered load for ALOHA protocol

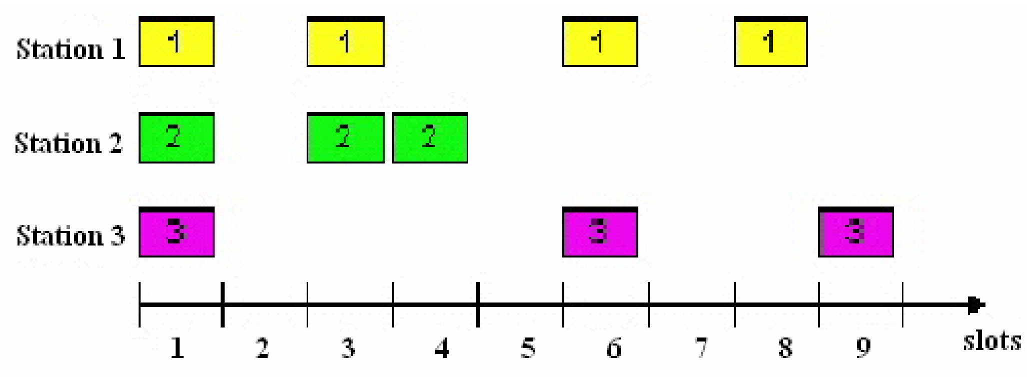


Figure 5.2.9 Slotted ALOHA: Single active node can continuously transmit at full rate of channel

Subsequently, in a new scheme, known as *Slotted ALOHA*, was suggested to improve upon the efficiency of pure ALOHA. In this scheme, the channel is divided into slots equal to τ and packet transmission can start only at the beginning of a slot as shown in Fig. 5.2.9. This reduces the vulnerable period from 2τ to τ and improves efficiency by reducing the probability of collision as shown in Fig. 5.2.10. This gives a maximum throughput of 37% at 100 percent of offered load, as shown in Figure 5.2.8.

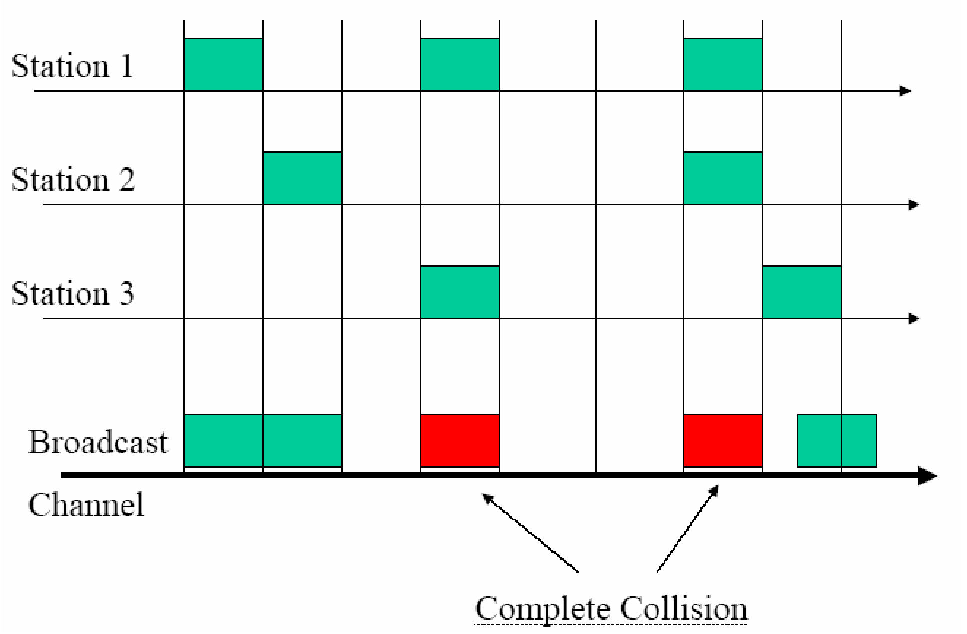


Figure 5.2.10 Collision in Slotted ALOHA

5.2.5 CSMA

The poor efficiency of the ALOHA scheme can be attributed to the fact that a node start transmission without paying any attention to what others are doing. In situations where propagation delay of the signal between two nodes is small compared to the transmission time of a packet, all other nodes will know very quickly when a node starts transmission. This observation is the basis of the *carrier-sense multiple-access* (CSMA) protocol. In this scheme, a node having data to transmit first listens to the medium to check whether another transmission is in progress or not. The node starts sending only when the channel is free, that is there is no carrier. That is why the scheme is also known as *listen-before-talk*. There are three variations of this basic scheme as outlined below.

(i) 1-persistent CSMA: In this case, a node having data to send, start sending, if the channel is sensed free. If the medium is busy, the node continues to monitor until the channel is idle. Then it starts sending data.

(ii) Non-persistent CSMA: If the channel is sensed free, the node starts sending the packet. Otherwise, the node waits for a random amount of time and then monitors the channel.

(iii) p-persistent CSMA: If the channel is free, a node starts sending the packet. Otherwise the node continues to monitor until the channel is free and then it sends with probability *p*.

The efficiency of CSMA scheme depends on the propagation delay, which is represented by a parameter a, as defined below:

$$a = \frac{\text{Propagation delay}}{\text{Packet transmission time.}}$$

The throughput of 1-persistent CSMA scheme is shown in Fig. 5.2.11 for different values of a. It may be noted that smaller the value of propagation delay, lower is the vulnerable period and higher is the efficiency.

5.2.6 CSMA/CD

CSMA/CD protocol can be considered as a refinement over the CSMA scheme. It has evolved to overcome one glaring inefficiency of CSMA. In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets. If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable. This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected. This refined scheme is known as *Carrier Sensed Multiple Access with Collision Detection* (CSMA/CD) or *Listen-While-Talk.*

On top of the CSMA, the following rules are added to convert it into CSMA/CD:

(i) If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.

(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.

The random delay ensures that the nodes, which were involved in the collision are not likely to have a collision at the time of retransmissions. To achieve stability in the back off scheme, a technique known as *binary exponential back off* is used. A node will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled. After 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error. A flowchart representing the binary exponential back off algorithm is given in Fig. 5.2.11.

Performance Comparisons: The throughput of the three contention based schemes with respect to the offered load is given in Fig 5.2.12. The figure shows that pure ALHOA gives a maximum throughput of only 18 percent and is suitable only for very low offered load. The slotted ALHOA gives a modest improvement over pure ALHOA with a maximum throughput of 36 percent. Non persistent CSMA gives a better throughput than 1-persistent CSMA because of smaller probability of collision for the retransmitted packets. The non-persistent CSMA/CD provides a high throughput and can tolerate a very heavy offered load. Figure 5.2.13 provides a plot of the offered load versus throughput for the value of a = 0.01.

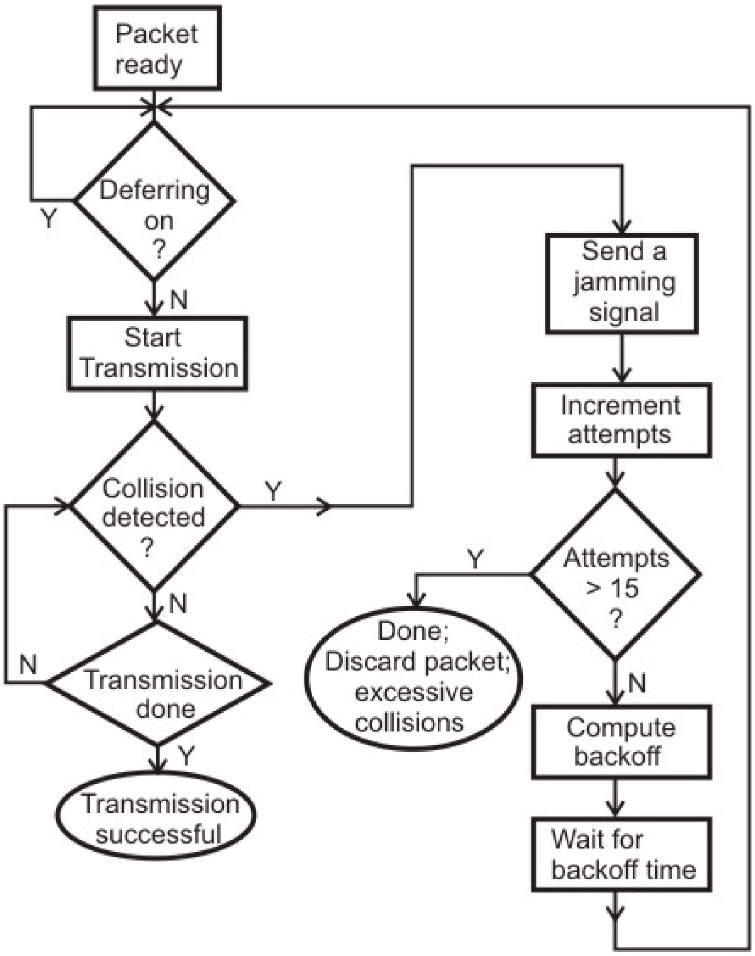
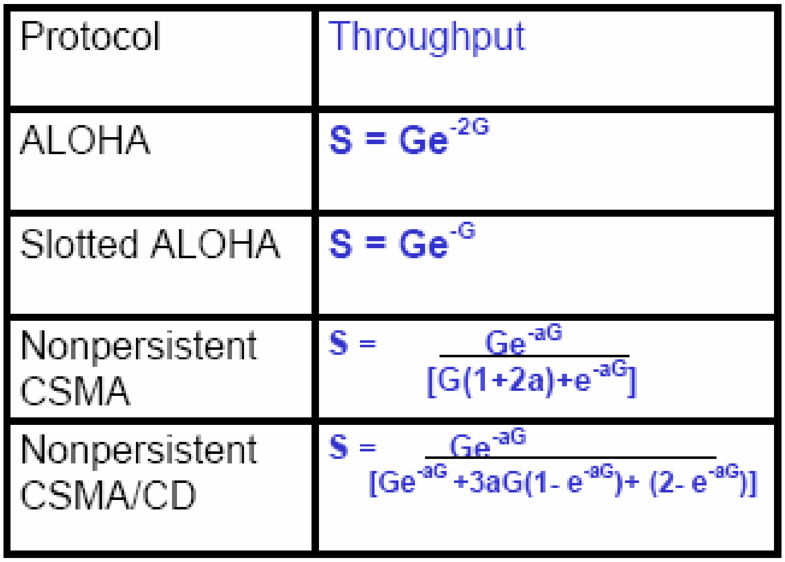


Figure 5.2.11 Binary exponential back off algorithm used in CSMA/CD



Protocol	Throughput
ALOHA	$S = Ge^{-2G}$
Slotted ALOHA	$S = Ge^{-G}$
Nonpersistent CSMA	$S = \frac{Ge^{-aG}}{[G(1+2a)+e^{-aG}]}$
Nonpersistent CSMA/CD	$S = \frac{Ge^{-aG}}{[Ge^{-aG} +3aG(1- e^{-aG})+ (2- e^{-aG})]}$

Figure 5.2.12 Comparison of the throughputs for the contention-based MACs

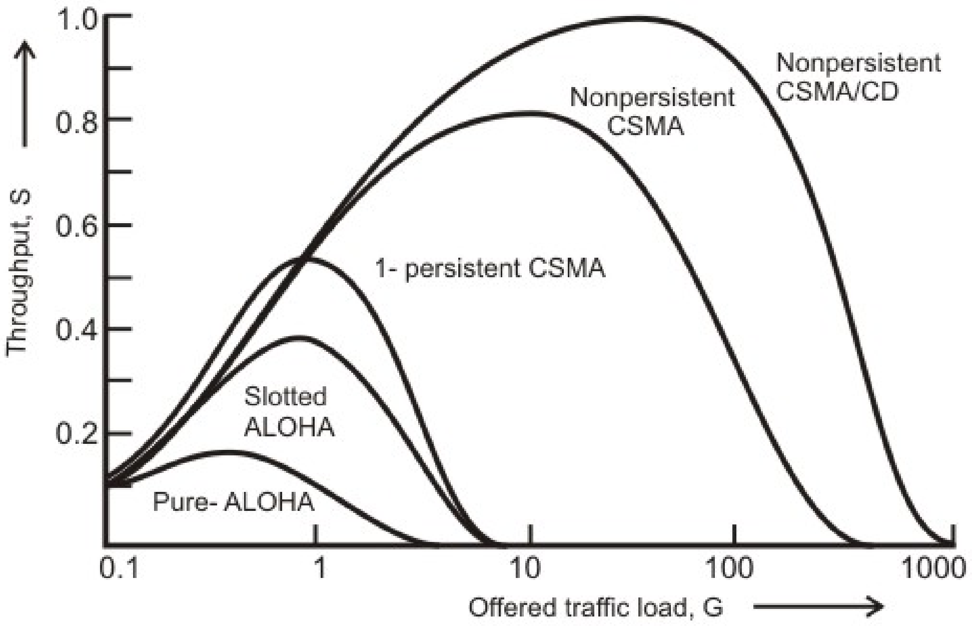


Figure 5.2.13 A plot of the offered load versus throughput for the value of a = 0.01

Performance Comparison between CSMA/CD and Token ring: It has been observed that smaller the mean packet length, the higher the maximum mean throughput rate for token passing compared to that of CSMA/CD. The token ring is also least sensitive to workload and propagation effects compared to CSMS/CD protocol. The CSMA/CD has the shortest delay under light load conditions, but is most sensitive to variations to load, particularly when the load is heavy. In CSMA/CD, the delay is not deterministic and a packet may be dropped after fifteen collisions based on binary exponential back off algorithm. As a consequence, CSMA/CD is not suitable for real-time traffic.

Fill In The Blanks:

1. The basic question which has to be answered by the medium-access control techniques is ***"How Goes ________"?***
2. In _______________ technique, each node gets a chance to access the medium by rotation.
3. The key issues involved in MAC protocol are - *Where* and ______ the control is exercised.
4. '**Where**' refers to whether the control is exercised in a _____________ or ______________ manner.
5. The _______________ techniques can be broadly categorized into three types; Round-Robin, Reservation and___________.
6. ______________ is an example of centralized control and ______________ is an example of distributed control

7. In Polling technique, if there is no data, usually a ______________ message is sent back.
8. In pure ALOHA, channel utilization, expressed as throughput S, in terms of the offered load G is given by _________
9. In slotted ALOHA, a maximum throughput of ________ percent at 100 percent of offered load can be achieved, while it is ______ percentage for pure ALOHA.
10. _________________ is abbreviated as CSMA/CD and is also known as __________.
11. To achieve stability in CSMA/CD back off scheme, a technique known as ______________ is used

Solutions:

1. Next
2. token passing
3. How
4. centralized, distributed
5. asynchronous, Contention
6. Polling, token passing
7. poll reject
8. $S=Ge^{-2G}$.
9. 37, 18
10. Carrier Sensed Multiple Access with Collision Detection, Listen-While-Talk .
11. binary exponential back off

Short Answer Questions:

Q-1. In what situations contention based MAC protocols are suitable?

Ans: Contention based MAC protocols are suitable for bursty nature of traffic under light to moderate load. These techniques are always decentralized, simple and easy to implement.

Q-2. What is vulnerable period? How it affects the performance in MAC protocols?

Ans: The total period of time when collision may occur for a packet is called vulnerable period. Let, all packets have a fixed duration λ. Then vulnerable period is 2λ in pure ALOHA scheme and λ in slotted ALOHA scheme. If vulnerable period is long, probability of the occurrence collision increases leading to reduction in throughput.

Q-3. How throughput is improved in slotted ALOHA over pure ALOHA?

Ans: In pure ALOHA vulnerable period is 2λ.
So, $S/G = e^{-2G}$ or throughput $S = G e^{-2G}$, where G is the total number of packets.
Maximum value of $G = 0.5$ or maximum throughput $S_{max} = 1/2e$.

In slotted ALOHA, vulnerable period is λ and $S/G = e^{-G}$ or throughput $S = G e^{-G}$. Here, maximum value of G is 1 and maximum throughput $S_{max} = 1/e$.

Q-4. What is the parameter 'a'? How does it affect the performance of the CSMA protocol?

Ans: The efficiency of CSMA scheme depends on propagation delay, which is represented by a parameter 'a' as defined below.

$$a = \frac{\text{propagation delay}}{\text{packet transmission time}}$$

Smaller the value of propagation delay, lower is the vulnerable period and higher is the efficiency. If propagation delay is zero, collision cannot occur in CSMA scheme. But in practice, there is some delay and depending on the value of 'a' collision occurs.

Q-5. How performance is improved in CSMA/CD protocol compared to CSMA protocol?

Ans: In CSMA scheme, a station monitors the channel before sending a packet. Whenever a collision is detected, it does not stop transmission leading to some wastage of time. On the other hand, in CSMA/CD scheme, whenever a station detects a collision, it sends a jamming signal by which other station comes to know that a collision occurs. As a result, wastage of time is reduced leading to improvement in performance.