Chapter 12

course	Computer Networks
Zohaib	rookie
Status	Not started
Resource	☐

Notes

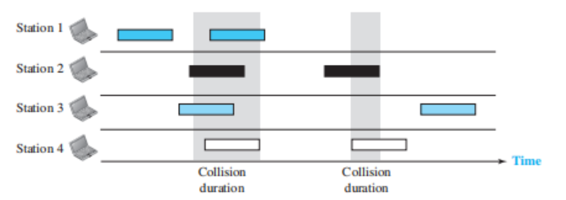
Summary of Random Access Methods in ALOHA

Random access methods allow stations to share a communication channel without a central controller. This chapter focuses on ALOHA, a foundational protocol for random access.

Key Points

- **Random access vs. Scheduled access:** Random access allows stations to transmit whenever they have data, unlike scheduled access where stations transmit at predefined times.
- **Collision:** When multiple stations transmit simultaneously, their data packets collide and become corrupted.
- **ALOHA:** The first random access protocol, developed for wireless LANs.
- **Pure ALOHA:** A simple but inefficient protocol. Stations transmit whenever they have data, leading to collisions.
    - **Vulnerable time:** The time period where a transmission from another station can collide with the current transmission (2 * frame transmission time).
    - **Throughput:** The percentage of successful transmissions. Pure ALOHA has a maximum throughput of 18.4%, achieved when the system generates on average half a frame during a frame transmission time.

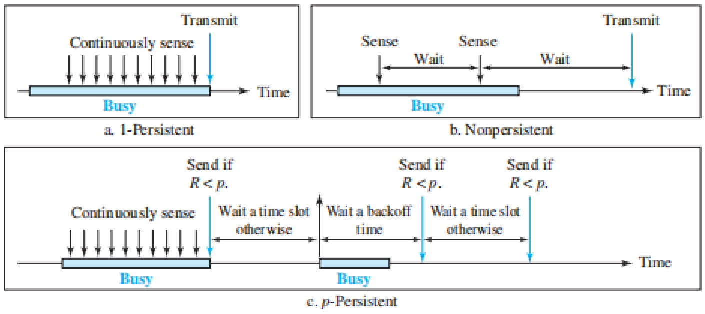
Figure 12.2 *Frames in a pure ALOHA network*

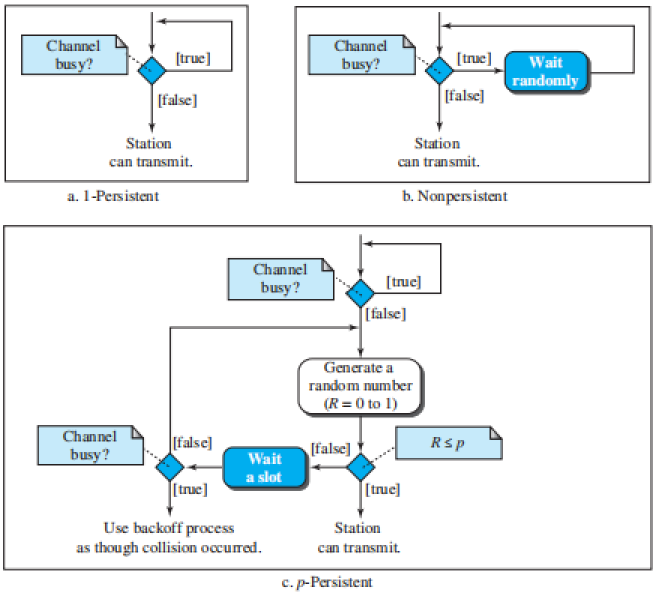


- **Slotted ALOHA:** An improvement over pure ALOHA that reduces collisions.
    - **Time slots:** The channel is divided into fixed-size time slots. Stations can transmit only at the beginning of a slot.
    - **Reduced vulnerable time:** The vulnerable time is reduced to the frame transmission time.

- **Throughput:** Slotted ALOHA offers a maximum throughput of 36.8%, achieved when the system generates on average one frame during a frame transmission time.

In conclusion, ALOHA provides a basic understanding of random access methods. However, its low efficiency limitations led to the development of more sophisticated protocols like CSMA/CD and CSMA/CA.





CSMA/CD vs CSMA/CA: A Quick Study Guide

Carrier Sense Multiple Access (CSMA)

CSMA is a protocol used in shared media networks to avoid collisions between data packets from different stations. It works by having stations listen to the medium before transmitting.

- **Collision:** When multiple stations transmit simultaneously, their data packets collide and become corrupted.

Types of CSMA

- **Pure ALOHA:** A simple but inefficient protocol. Stations transmit whenever they have data, leading to high collision rates.
- **Slotted ALOHA:** An improvement over pure ALOHA that reduces collisions. The channel is divided into fixed-size time slots. Stations can transmit only at the beginning of a slot.

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

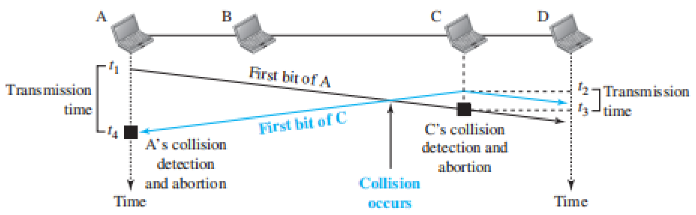
- Improves on CSMA by adding collision detection.
- Stations listen before transmitting and continue listening while transmitting.
- If a collision is detected, both stations stop transmitting and retransmit after a random delay.
- Requires a minimum frame size to ensure collision detection before the entire frame is sent.
- Commonly used in wired Ethernet networks (e.g., 10Mbps Ethernet).

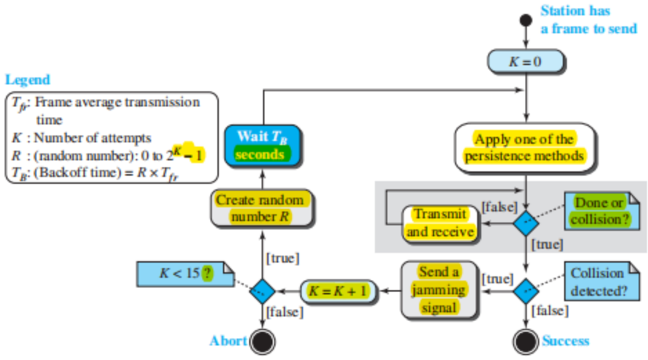
Advantages:

- Simpler implementation compared to CSMA/CA
- Higher throughput compared to pure ALOHA

Disadvantages:

- Increased collisions in heavy traffic conditions
- No mechanism to prevent collisions entirely
-





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

- Designed for wireless networks to avoid collisions before they occur.
- Uses three key strategies:
  - **Interframe Space (IFS):** Stations wait a short period after finding the channel idle to account for ongoing transmissions from distant stations.
  - **Contention Window:** Stations choose a random slot within a contention window to transmit, reducing the chance of multiple stations transmitting at the same time.
  - **Acknowledgments (ACKs):** Sending station receives an ACK from the receiving station to confirm successful reception, reducing wasted transmissions due to collisions.

- Uses control frames (RTS/CTS) for handshaking to further reduce collisions.

Advantages:

- Significantly reduces collisions compared to CSMA/CD
- More efficient in wireless networks

Disadvantages:

- More complex implementation compared to CSMA/CD
- Potential overhead due to control frames

In summary:

- CSMA/CD is simpler and more efficient for wired networks with moderate traffic.
- CSMA/CA is more complex but offers better collision avoidance for wireless networks.

Figure 12.15 *Flow diagram of CSMA/CA*

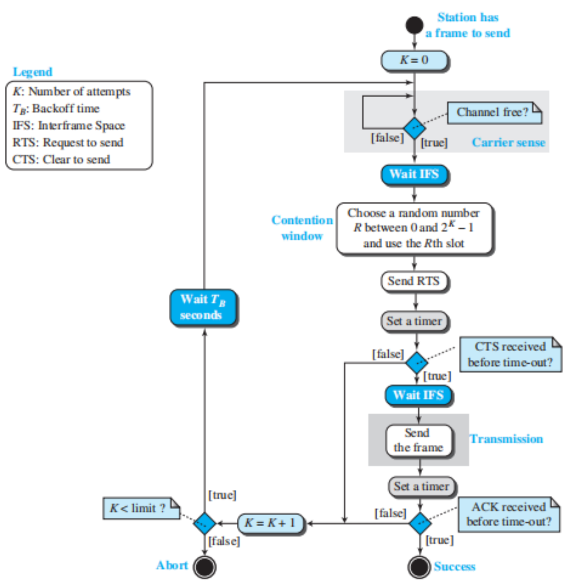
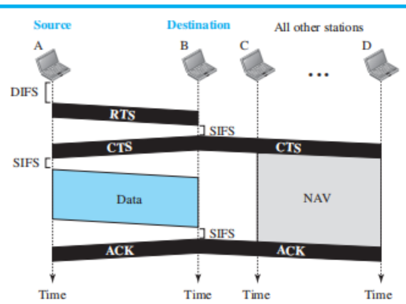


Figure 12.17 *CSMA/CA and NAV*



Controlled Access Methods in MAC

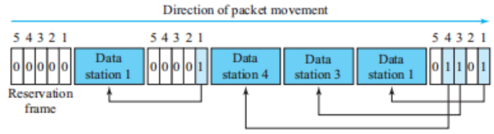
Controlled access methods ensure only one device transmits data at a time on a shared medium, preventing collisions. Here's a breakdown of three main techniques:

1. Reservation

- Stations reserve a time slot before transmitting data.

- A reservation frame precedes data frames, specifying which stations have reserved slots.
- Suitable for predictable traffic patterns.

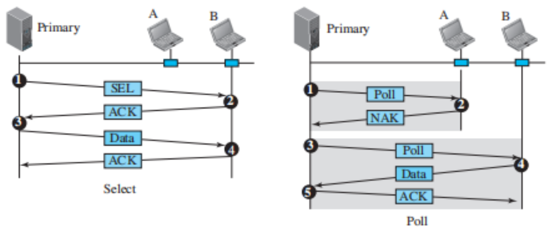
Figure 12.18 *Reservation access method*



2. Polling

- A designated primary station controls the channel.
- The primary station polls secondary stations to see if they have data to transmit.
- Simple but inefficient for many devices or unpredictable traffic.

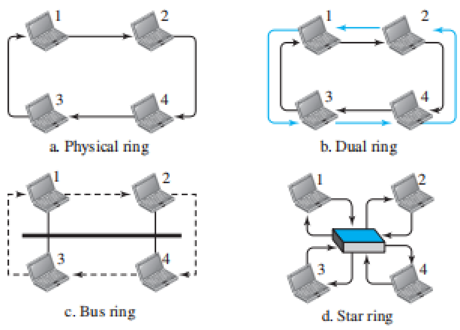
Figure 12.19 *Select and poll functions in polling-access method*



3. Token Passing

- Stations are logically arranged in a ring.
- A special token circulates through the ring, granting transmission rights to the holding station.
- The station with the token can transmit data and then passes the token to its successor.
- Ensures fairness and avoids collisions but adds overhead for token management.

Figure 12.20 *Logical ring and physical topology in token-passing access method*



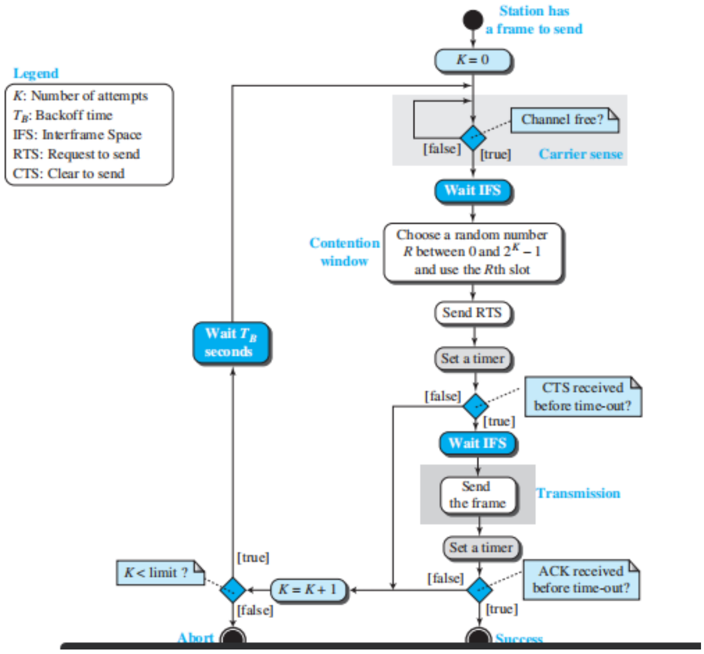
Comparison Table

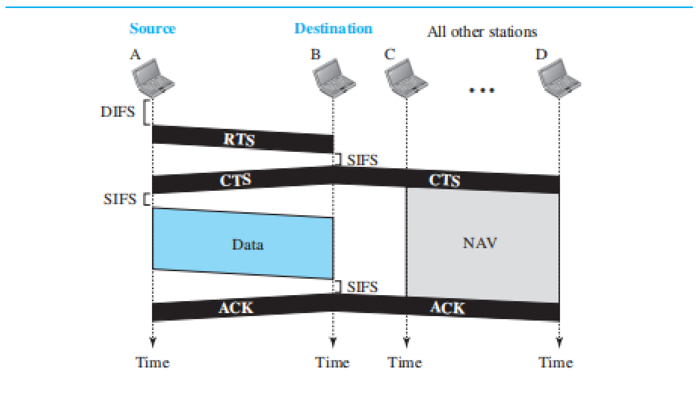
Feature	Reservation	Polling	Token Passing
Collision Risk	Low	Low	Low

Efficiency	Moderate	Low	Moderate
Scalability	Moderate	Low	Moderate
Complexity	Moderate	Low	High
Centralized Control	No	Yes	No

Additional Notes:

- Token passing can be implemented on various physical topologies (bus, star) creating logical rings.
- Controlled access methods offer better collision avoidance compared to CSMA/CD (Carrier Sense Multiple Access with Collision Detection) used in Ethernet.





Channelization in MAC

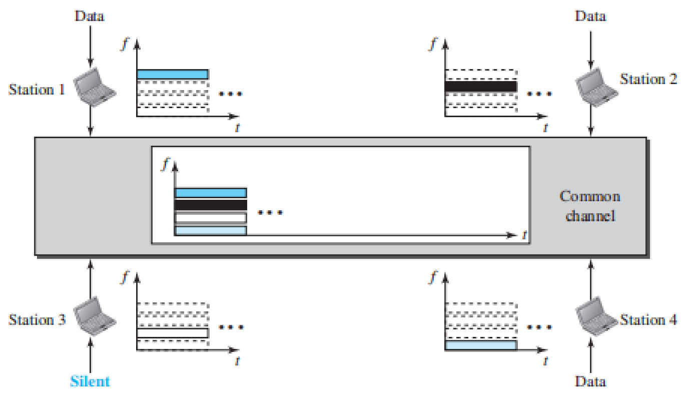
Channelization divides the available bandwidth of a communication link into smaller channels based on frequency (FDMA), time (TDMA), or code (CDMA). This allows multiple stations to share the medium without collisions.

1. Frequency-Division Multiple Access (FDMA)

- Divides bandwidth into frequency bands.
- Each station gets a designated band for exclusive use.

- Requires guard bands between bands to prevent interference.
- Suitable for predictable traffic patterns and applications requiring continuous data streams (e.g., cellular telephone systems).

Figure 12.21 *Frequency-division multiple access (FDMA)*

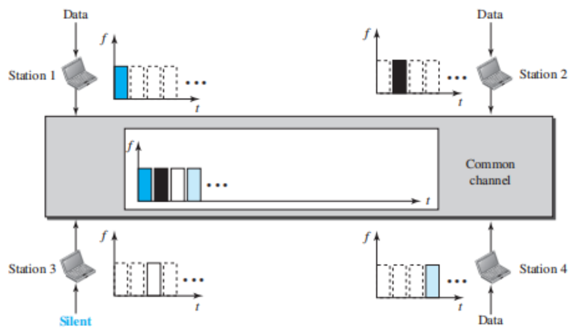


In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.

2. Time-Division Multiple Access (TDMA)

- Divides bandwidth into time slots.
- Each station transmits data in its assigned time slot.
- Requires synchronization between stations to avoid collisions.
- Introduces overhead for guard times between slots to compensate for propagation delays.

Figure 12.22 *Time-division multiple access (TDMA)*



3. Code-Division Multiple Access (CDMA)

- All stations transmit data simultaneously on the entire bandwidth.
- Each station uses a unique code to differentiate its signal from others.
- Receivers use the same code to extract the desired signal.
- Requires complex coding and signal processing techniques.
- Offers higher capacity compared to FDMA/TDMA due to better bandwidth utilization.

Comparison Table

Feature	FDMA	TDMA	CDMA
Channel Division	Frequency	Time	Code
Access Method	Reservation-based	Controlled access	Carrier Sense
Efficiency	Moderate	Moderate	High
Scalability	Moderate	Moderate	Moderate
Complexity	Low	Moderate	High
Applications	Cellular phone, Radio, Satellite	Cellular phone, WLAN	Cellular phone, Bluetooth

---

1. Throughput for Pure ALOHA (S):

The formula S = (5 * G) / (3 * e^(2G)) calculates the throughput (S) for a given offered traffic (G). Here's how to use it:

- **G (Offered Traffic):** This represents the average number of transmissions attempted per frame time (T). It's a non-negative value.
- **S (Throughput):** This represents the number of successful transmissions per frame time. It will always be less than or equal to G (due to collisions).

Steps to solve:

1. Substitute the value of G in the formula.
2. Use a calculator to compute e^(2G) (e raised to the power of 2G).
3. Divide (5 * G) by the result obtained in step 2.

2. Maximum Throughput (Smax):

The formula Smax = 1 / (2e) = 0.184 tells you the theoretical maximum throughput (Smax) achievable in Pure ALOHA. It's a fixed value of approximately 18.4%.

Key Points:

- Throughput (S) calculated from formula 1 will always be less than or equal to Smax (0.184). This is because as the offered traffic (G) increases, collisions become more frequent, reducing successful transmissions.
- Pure ALOHA suffers from a trade-off between simplicity and efficiency. While it's easy to implement, its maximum throughput is quite low.

Example:

- Let's say G = 0.3 (offered traffic is 0.3 times the frame time).
- Using formula 1: S = (5 ∗ 0.3) / (3 * e^(2 ∗ 0.3)) ≈ 0.167.
- As expected, the throughput (0.167) is lower than the maximum throughput (0.184).

The information you provided "Pure ALOHA vulnerable time = 2 ∗ 3 Tfr" is actually correct. It describes the vulnerable time in Pure ALOHA, where Tfr represents the frame transmission time.

Here's a breakdown of the formula and why the vulnerable time is twice the frame transmission time:

- **Vulnerable Time:** This is the time period during which a collision can occur if another station transmits simultaneously.
- **Tfr (Frame Transmission Time):** This is the time it takes to transmit a complete frame on the channel.

Reasoning for 2 * Tfr:

1. **Collision Detection:** Pure ALOHA doesn't involve any carrier sensing before transmission. So, a station doesn't know if another station is already transmitting until its own transmission starts.
2. **Collision Window:** For a collision to occur, the beginning of another station's transmission must overlap with some part of your own transmission.
3. **Vulnerable Period:** Considering point 1, another station's transmission can potentially collide with yours as long as it starts anytime within a window of 2 * Tfr. This window includes:
    - **Tfr before your transmission:** If another station starts transmitting Tfr units before yours, the end of their transmission might overlap with the beginning of yours, causing a collision.
    - **Tfr during your transmission:** Even during your transmission, another station can initiate its transmission and collide with the remaining part of your frame.
