ITMC412 PAN
شبكات المنطقة الشخصية

MAC Technologies
L3

By: Dr. Abdussalam Nuri Baryun
abaryun.teaching@gmail.com

Mobile Computing Department, Faculty of Information Technology, University of Tripoli

This Course Focus on

- ALOHA
- CSMA
- CSMA/CA
- Controlled Access
- TDMA

This presentation includes the CSMA and controlled access techniques.

Improve the MAC protocol

- Receiving acknowledgement for all transmissions.
- Reduce Collisions between senders, by reducing vulnerability period.
- Limit transmission start time to the beginning of discrete time slices (Slots).
- Listen before talking to avoid having a collision with an ongoing packet transmission.

Carrier Sense Multiple Access (CSMA)

- Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- CSMA is a probabilistic Media Access Control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared physical medium, such as an electrical bus, or a band of electromagnetic spectrum.
  - "Carrier Sense" describes the fact that a transmitter listens for carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the node waits for the transmission in progress to finish before initiating its own transmission.
  - "Multiple Access" describes the fact that multiple nodes send and receive on the medium. Transmissions by one node are generally received by all other nodes using the medium.

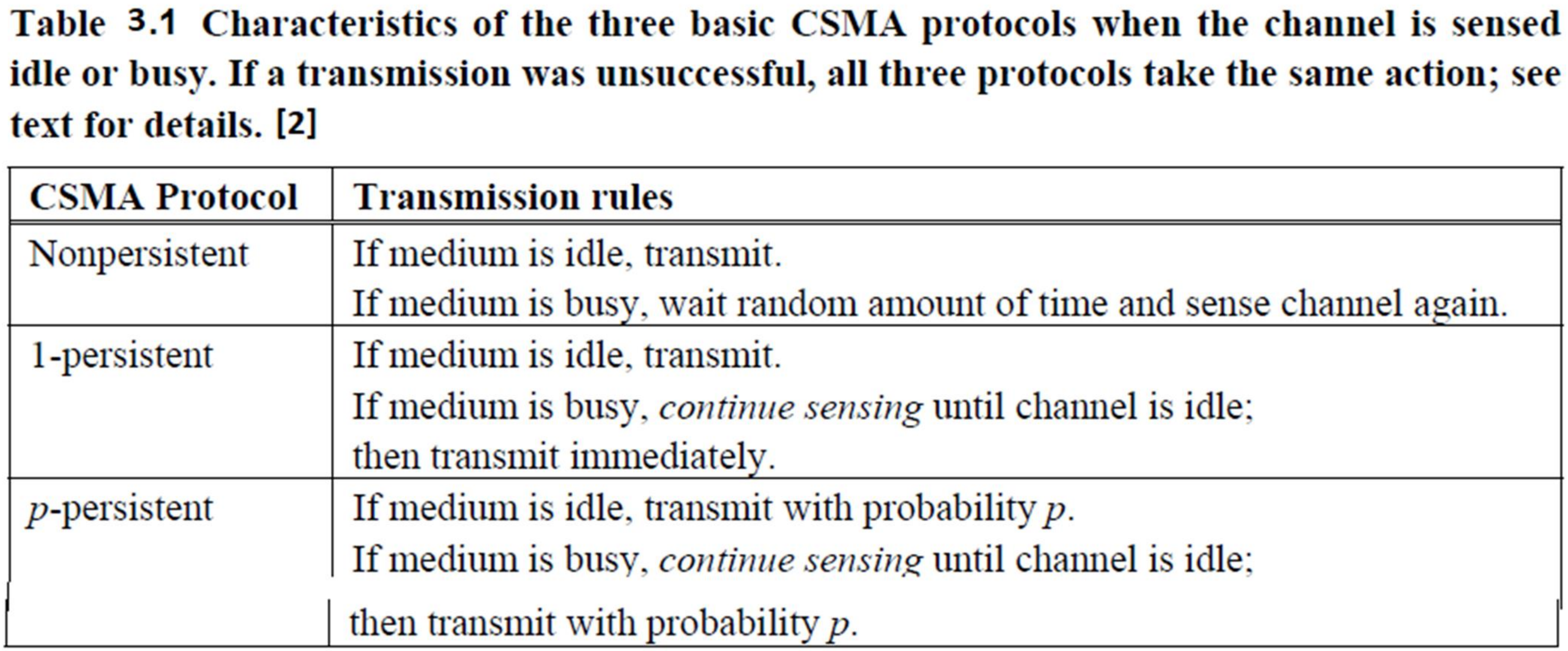


Table 3.1 Characteristics of the three basic CSMA protocols when the channel is sensed idle or busy. If a transmission was unsuccessful, all three protocols take the same action; see text for details. [2]

CSMA Protocol	Transmission rules
Nonpersistent	If medium is idle, transmit. If medium is busy, wait random amount of time and sense channel again.
1-persistent	If medium is idle, transmit. If medium is busy, *continue sensing* until channel is idle; then transmit immediately.
p-persistent	If medium is idle, transmit with probability *p*. If medium is busy, *continue sensing* until channel is idle; then transmit with probability *p*.

- the performance of CSMA degrades with increasing β and also degrades with increasing transmission rate and with decreasing packet size.

Comparison

- The efficiency of CSMA is better than that of ALOHA because of the CSMA's shorter vulnerable period: The stations will not initiate transmission if they sense a transmission already in progress.
- Notice that non-persistent CSMA is less greedy than 1-persistent CSMA in the sense that, upon observing a busy channel, it does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- Instead, non-persistent CSMA waits a random period of time and then repeats the procedure. Consequently, this protocol leads to better channel utilization but longer delays than 1-persistent CSMA.

Frame Propagation and Sensing

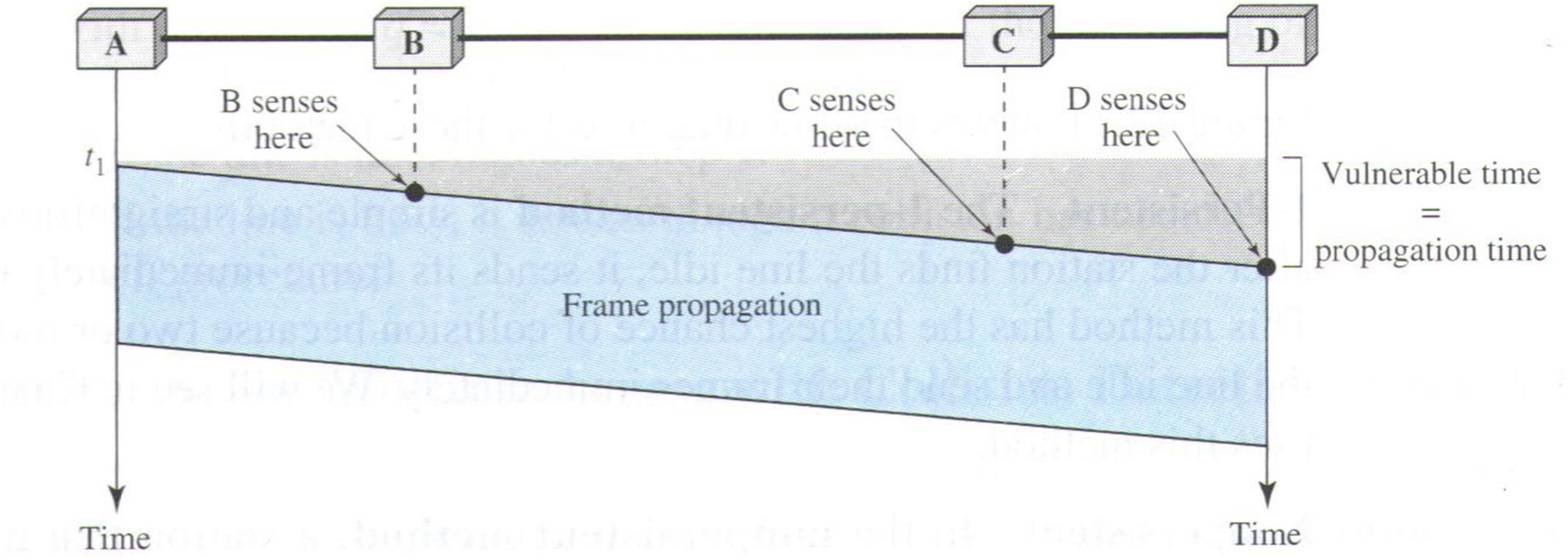


Fig (3.1) *Vulnerable time in CSMA*

Propagation Constant β

$$\beta = \frac{t_{prop}}{t_{xmit}} = \frac{t_{prop} \cdot R}{L}$$

L is the frame/packet size in bits

R is transmission rate in bit per second

t_{xmit} is the frame/packet transmission time

t_{prop} is the frame/packet propagation time

For a 1 Kbytes packet and a transmission speed of R =1 Mbps, the transmission time is $t_{xmit} = (8 \times 1000 \text{ bits}) / (1 \times 10^6 \text{ b/s}) = 8$ ms.

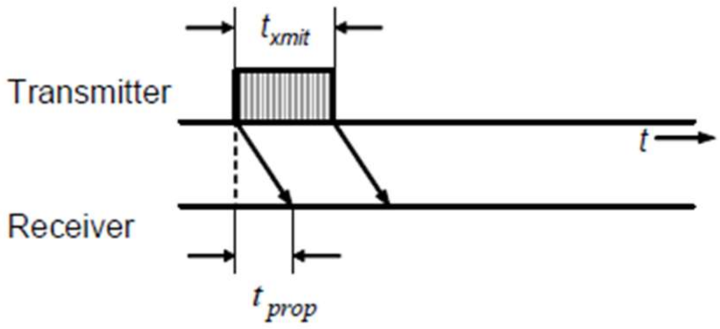


Fig (3.2)

in PAN usually $\beta << 1$

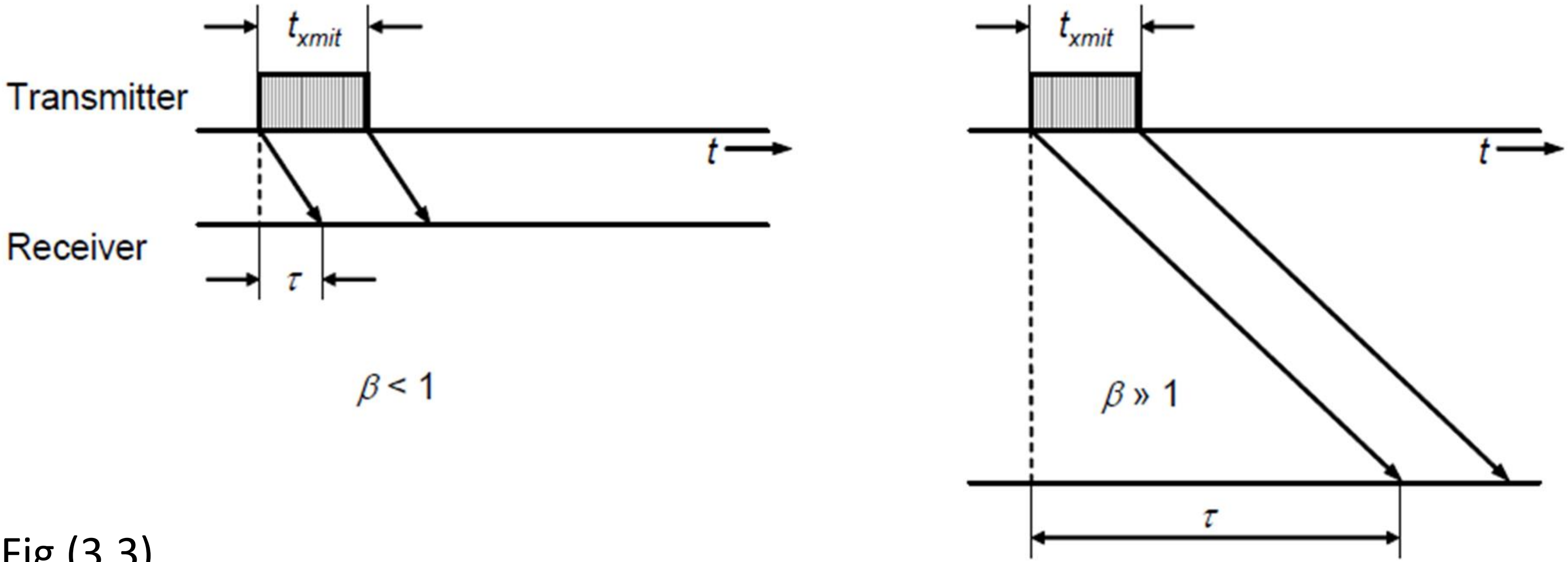
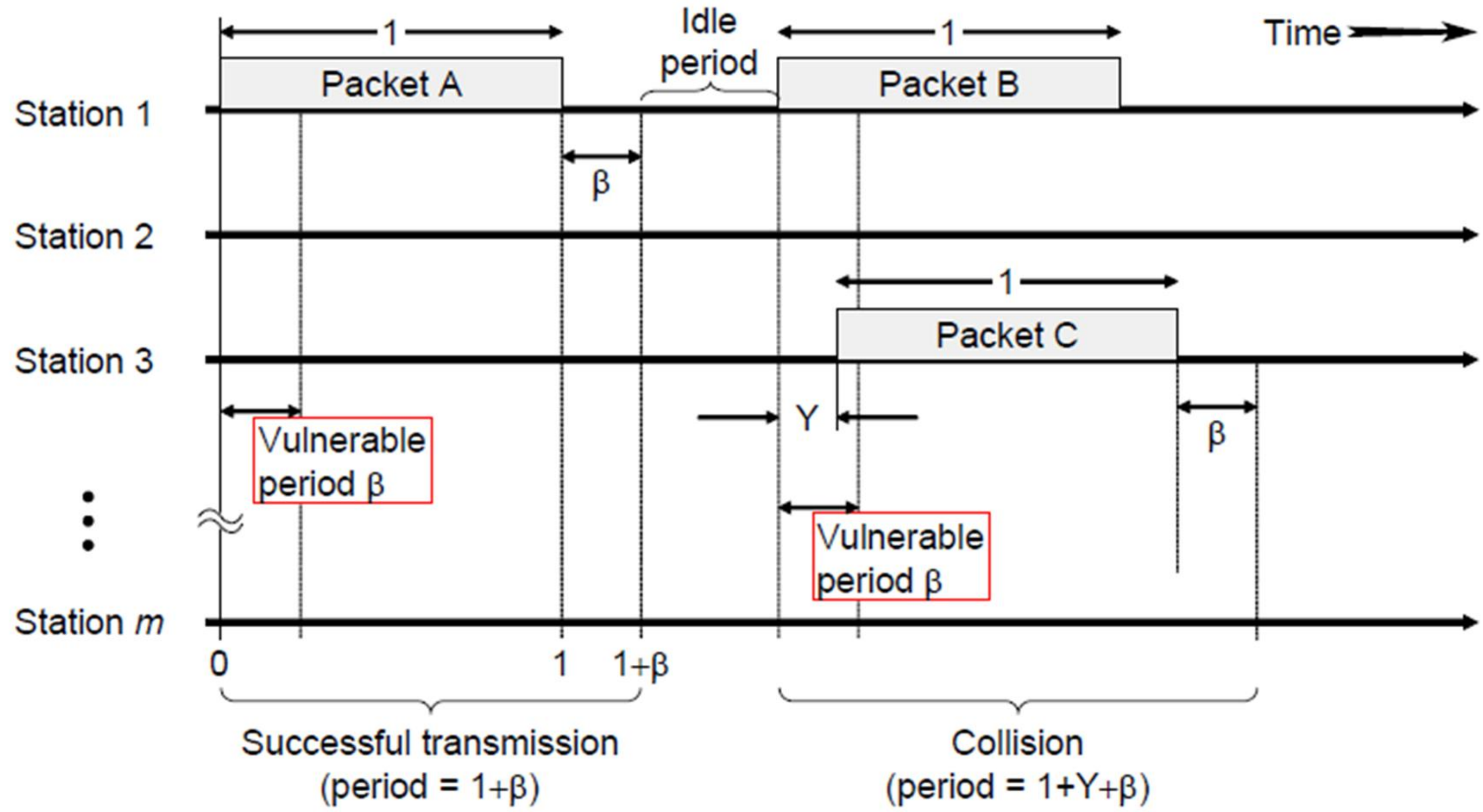


Fig (3.3)

Propagation constant β for different ratios of propagation and transmission times. τ combines both propagation and detection delay.



1
Packet A
Idle period
1
Packet B
Time
Station 1
β
Station 2
1
Packet C
Station 3
Y
β
Vulnerable period β
Vulnerable period β
Station *m*
0
1
1+β
Successful transmission (period = 1+β)
Collision (period = 1+Y+β)

Fig (3.4)

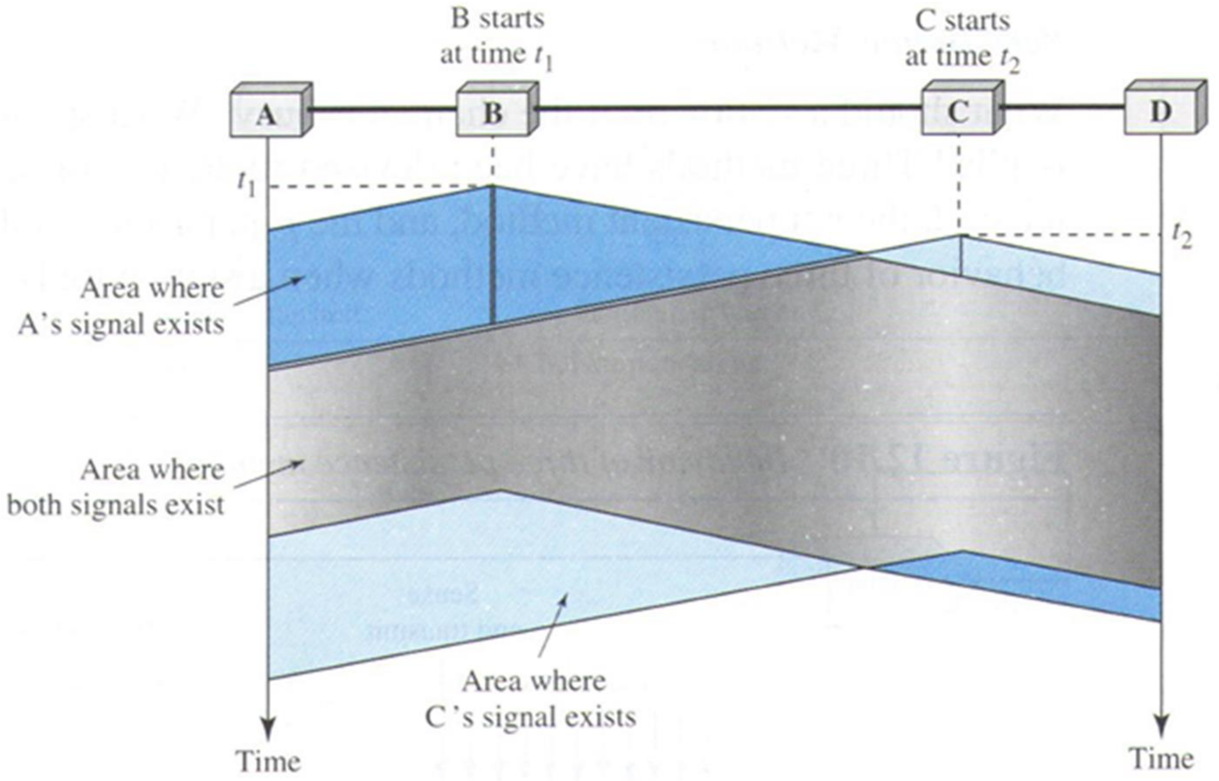


Fig (3.5) *model of the collision in CSMA*

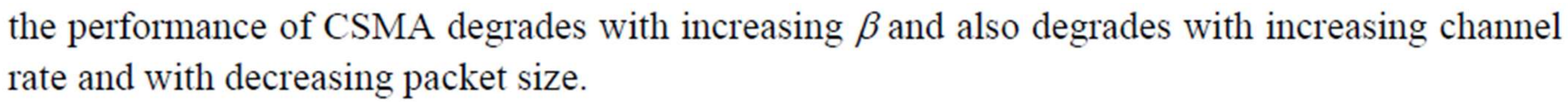
At time t_1, station B senses the medium and finds it idle, so it sends a frame. At time t_2 ($t_2 > t_1$), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.

Collision Avoidance in Wireless Networks

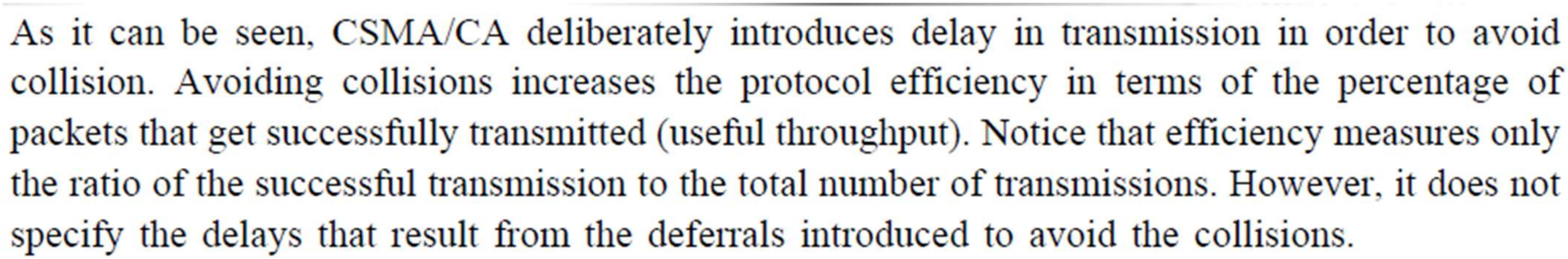
In wireless LANs it is not practical to do collision detection because of two main reasons:

1. Implementing a collision detection mechanism would require the implementation of a full duplex radio, capable of transmitting and receiving at once. Unlike wired LANs, where a transmitter can simultaneously monitor the medium for a collision, in many wireless LANs the transmitter's power overwhelms a collocated receiver. The dynamic range of the signals on the medium is very large.
2. In a wireless environment we cannot assume that all stations hear each other, which is the basic assumption of the collision detection scheme. Again, due to the propagation loss we have the following problem. The fact that the transmitting station senses the medium free

CSMA Performance [2]



the performance of CSMA degrades with increasing β and also degrades with increasing channel rate and with decreasing packet size.



As it can be seen, CSMA/CA deliberately introduces delay in transmission in order to avoid collision. Avoiding collisions increases the protocol efficiency in terms of the percentage of packets that get successfully transmitted (useful throughput). Notice that efficiency measures only the ratio of the successful transmission to the total number of transmissions. However, it does not specify the delays that result from the deferrals introduced to avoid the collisions.

Basic CSMA with hidden node

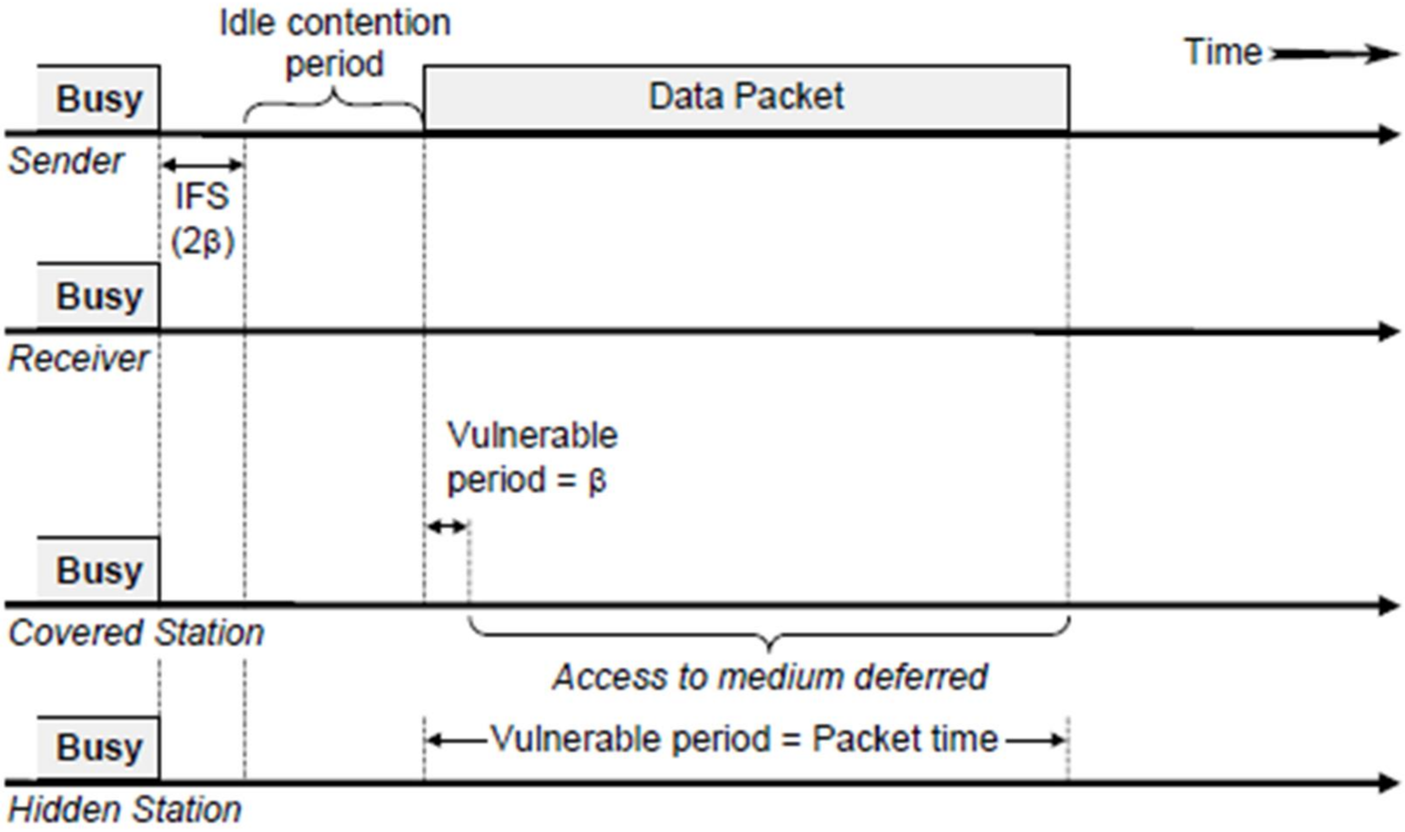


Fig (3.6) The vulnerability period for the network is higher when has hidden terminals

Collisions are avoided by

- Interframe space (IFS) , when channel is ideal the sender does not send immidiatly but waits for IFS time. IFS can be used to define priority.
- Contention Window, a station is ready to send but uses a random number of slots as its wait time. In this window a station has to sense channel after each slot.
- Acknowledgement,

CSMA/CA

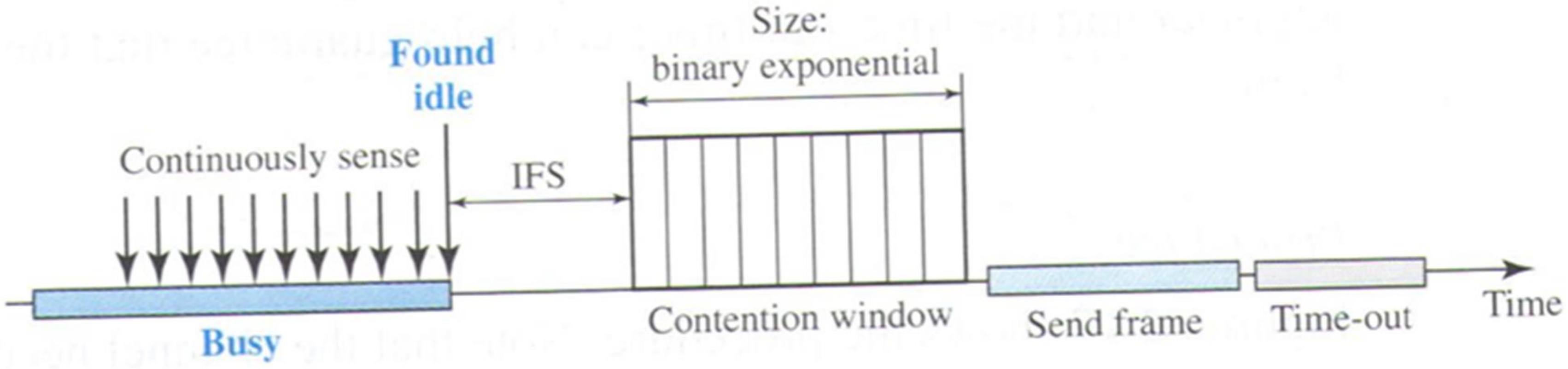


Fig (3.7) **Timing in CSMA–CA** **Ref [1]**

- IFS: Inter-Frame Slot
- CW: Contention Window

CSMA/CA flow diagram

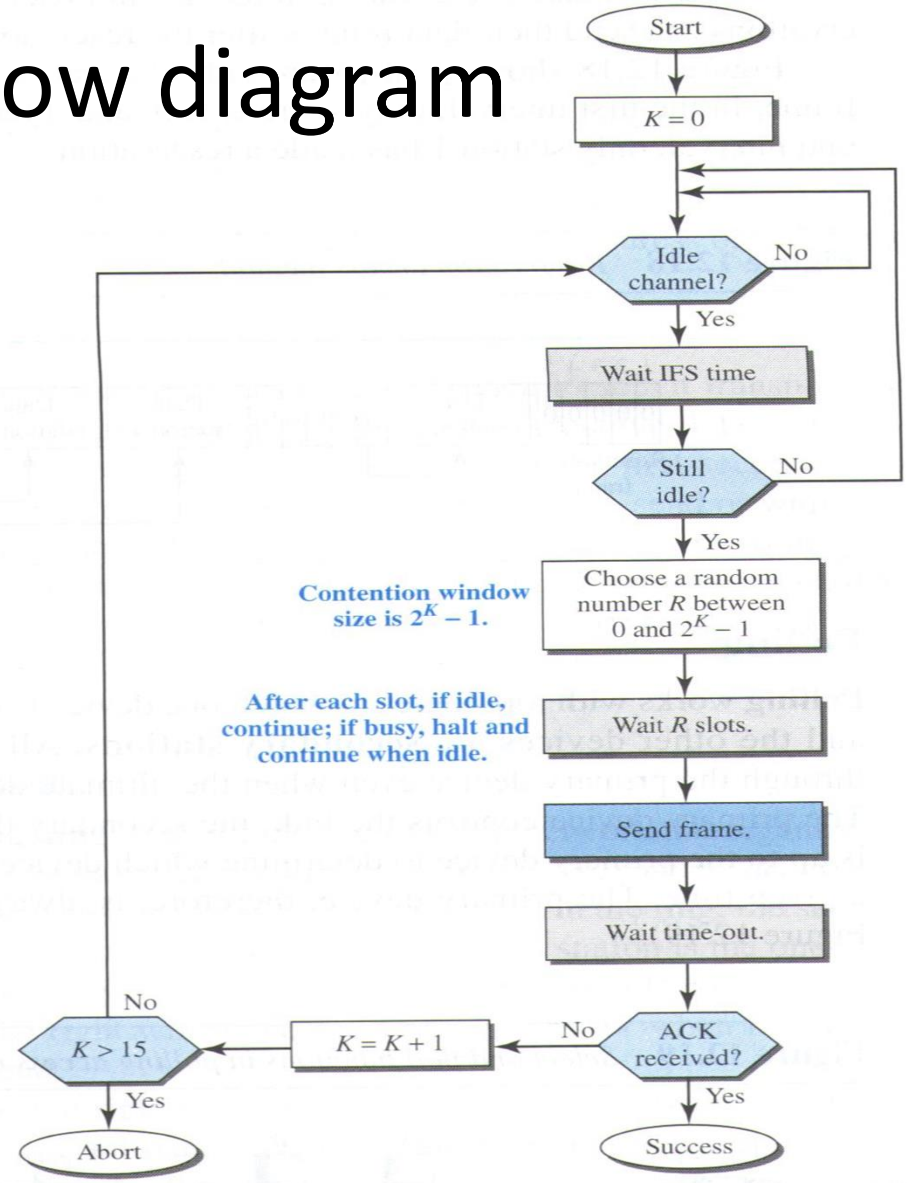

Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is $2^K - 1$.
Choose a random number R between 0 and $2^K - 1$
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
ACK received?
No
Yes
K = K + 1
K > 15
No
Yes
Abort
Success

Fig (3.8) *Flow diagram for CSMA/CA* **Ref [1]**

IEEE802.11 CSMA/CA

- Avoids collision by sending a short message: Ready to send (RTS) RTS contains destination. address and duration of message. Tells everyone to backoff for the duration.
- Destination sends: Clear to send (CTS)
- Can not detect collision ⇒ Each packet is acked.
- MAC level retransmission if not acked.

Using frames for access control

- To reduce collisions within WPAN.

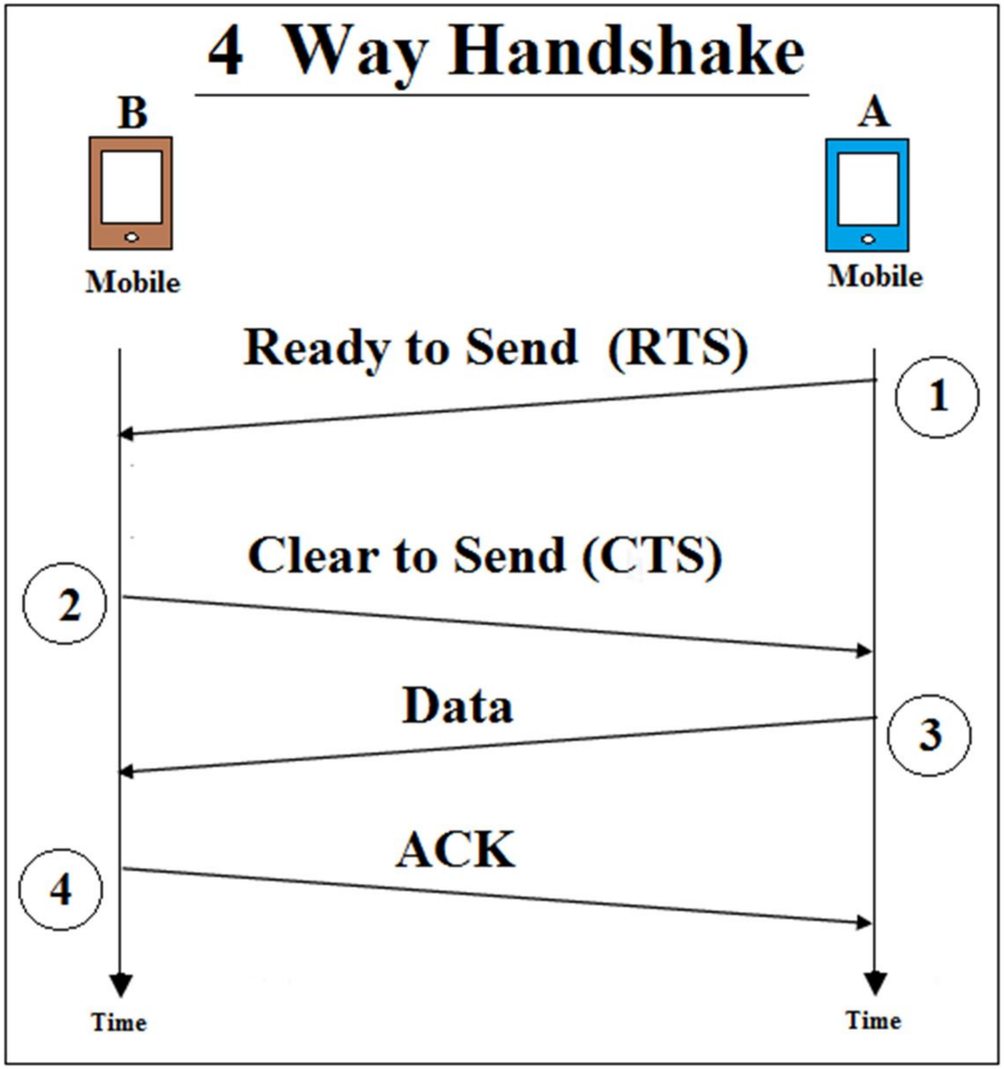


Fig (3.9)

CSMA/CA IEEE802.11

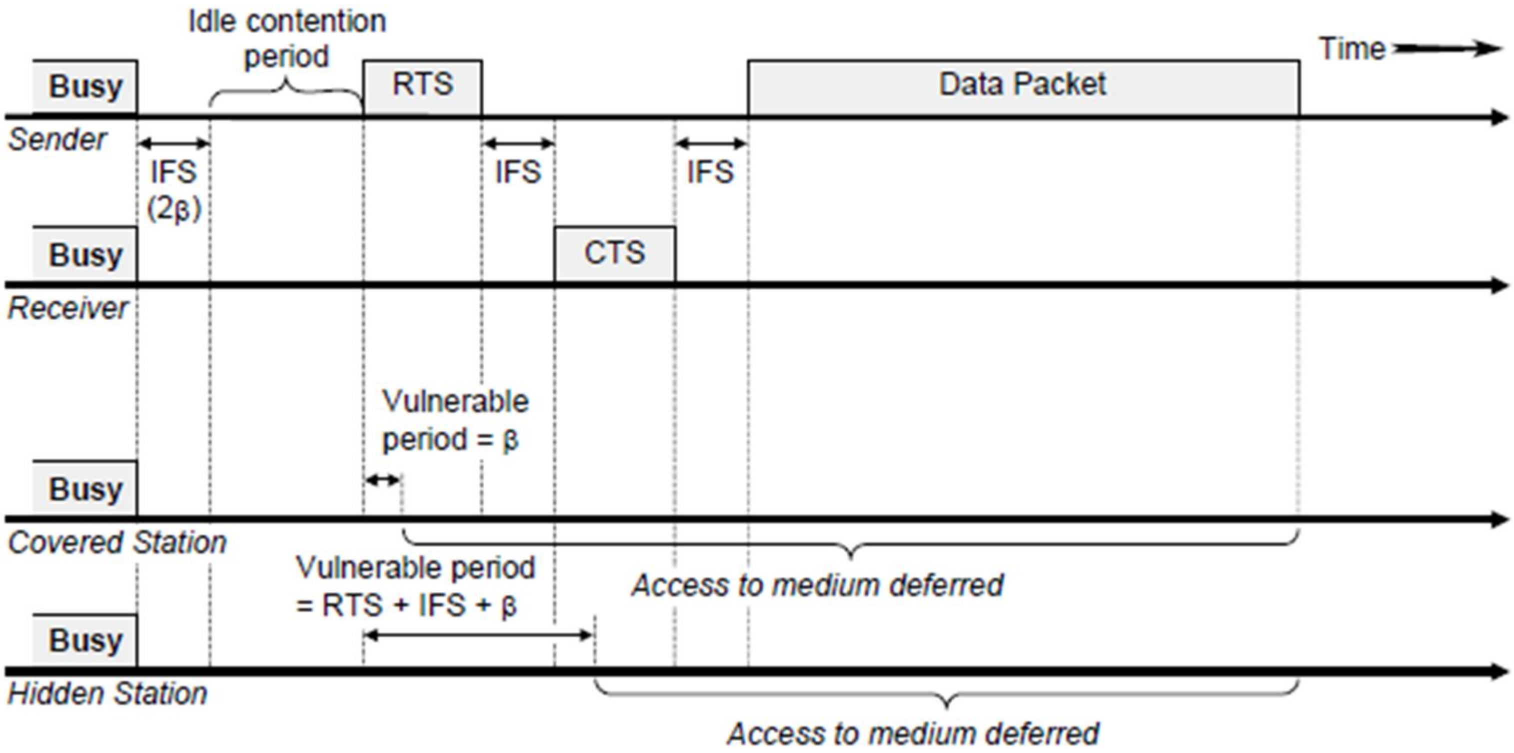


Fig (3.10) The vulnerability period for CSMA/CA can be reduced using RTS and CTS

CSMA/CA flowchart **with control frames** **Ref [1]**

CSMA/CA with RTS/CTS

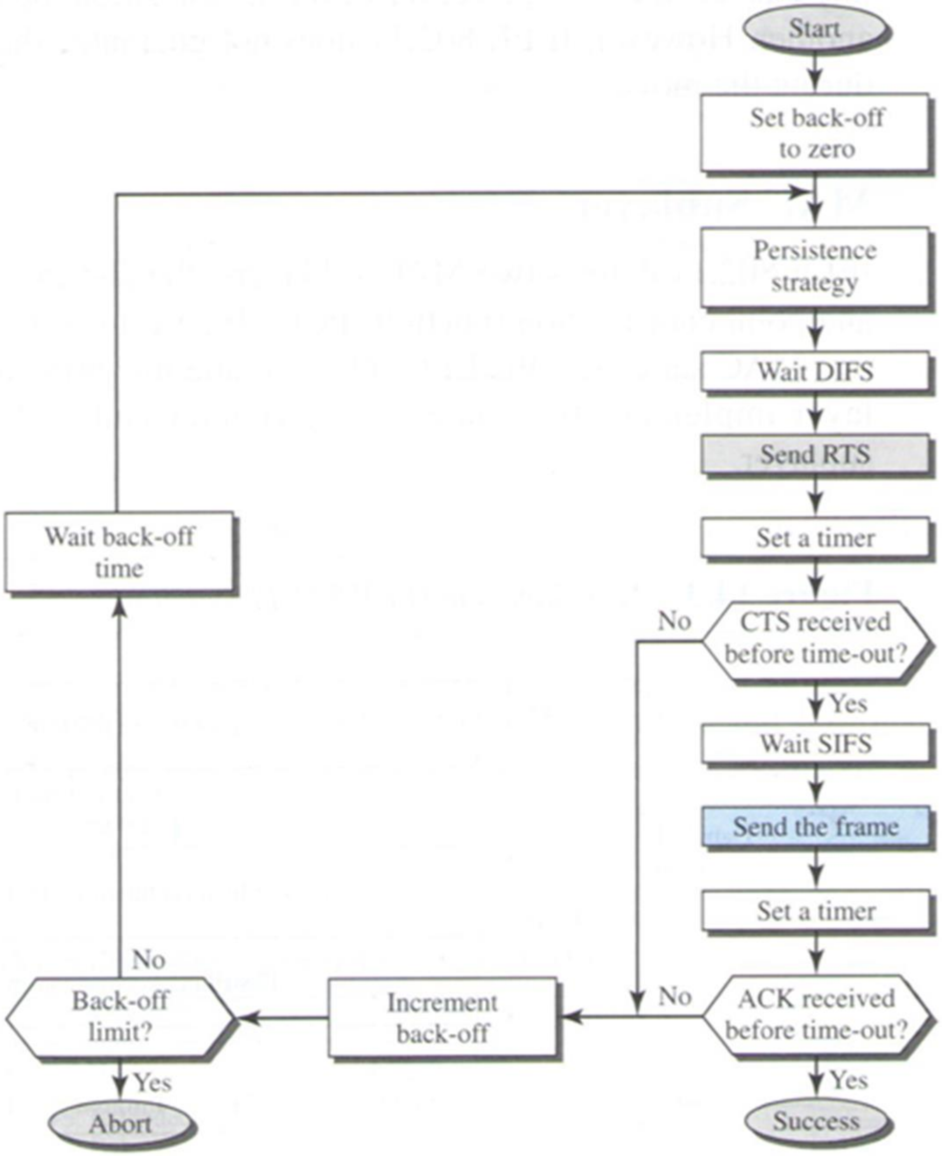
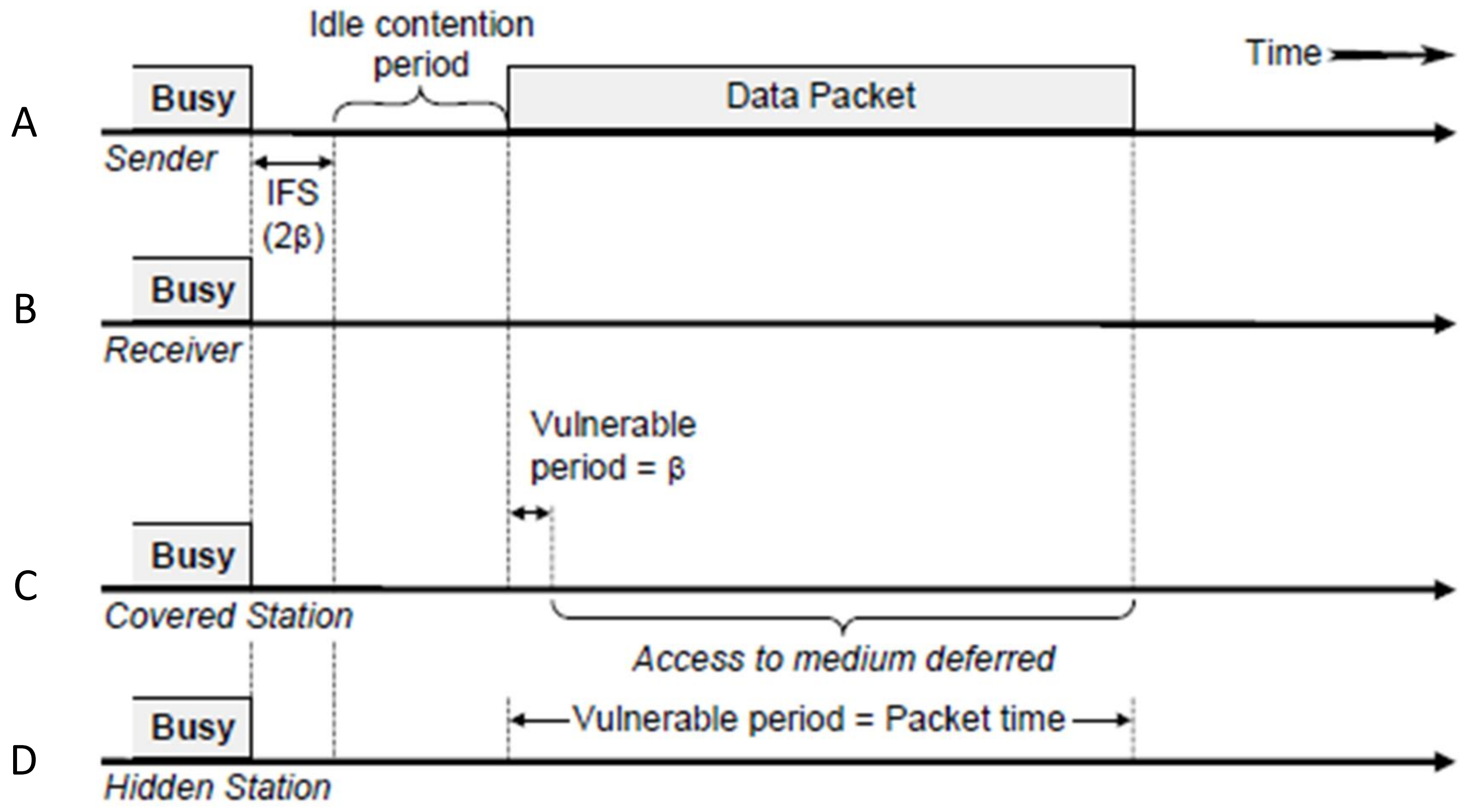


Fig (3.11)

Vulnerability of Basic CSMA



Fig(3.12) CSMA with hidden terminal have large vulnerable period **Ref [2]**

CSMA/CA IEEE802.11

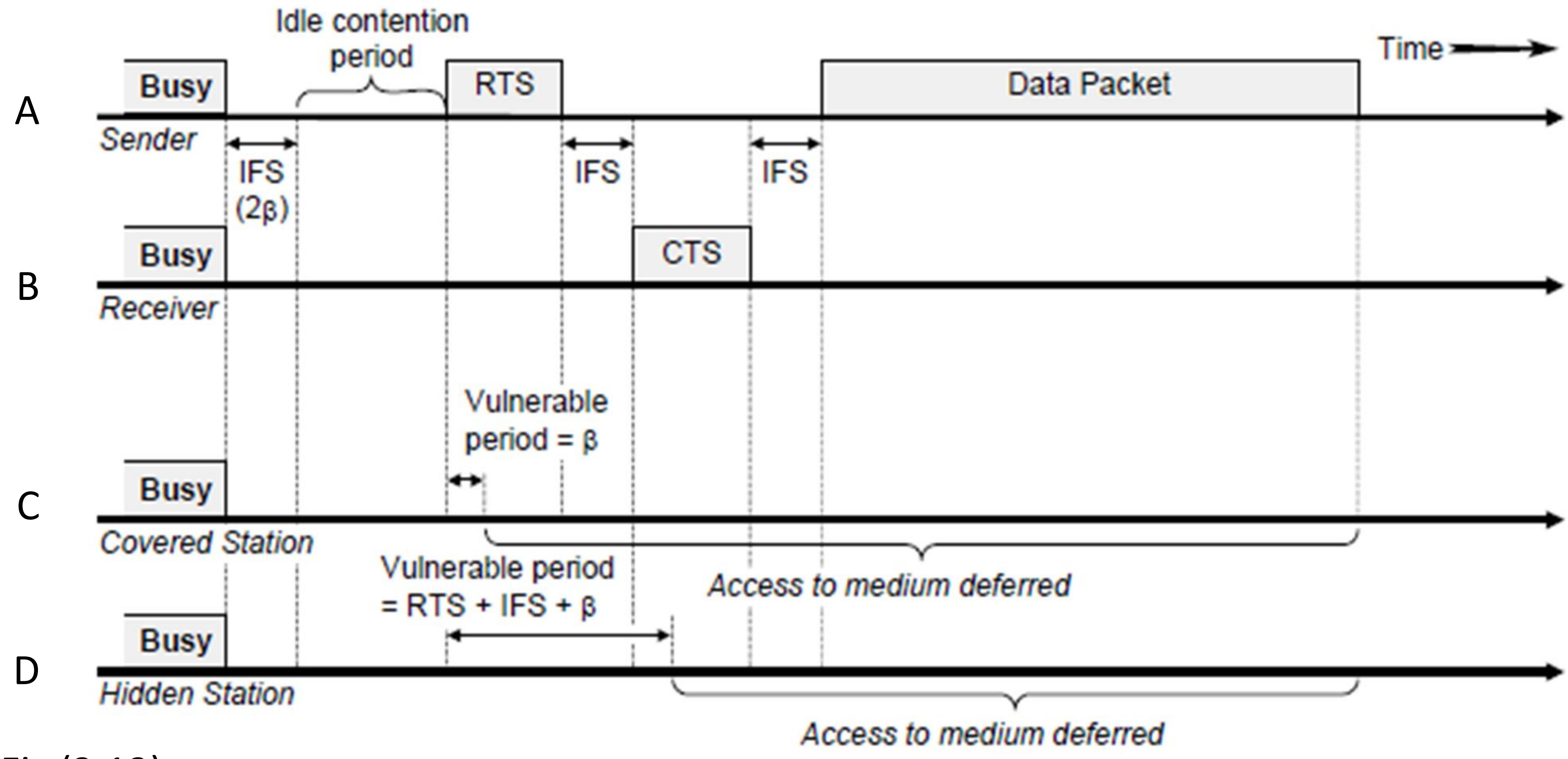
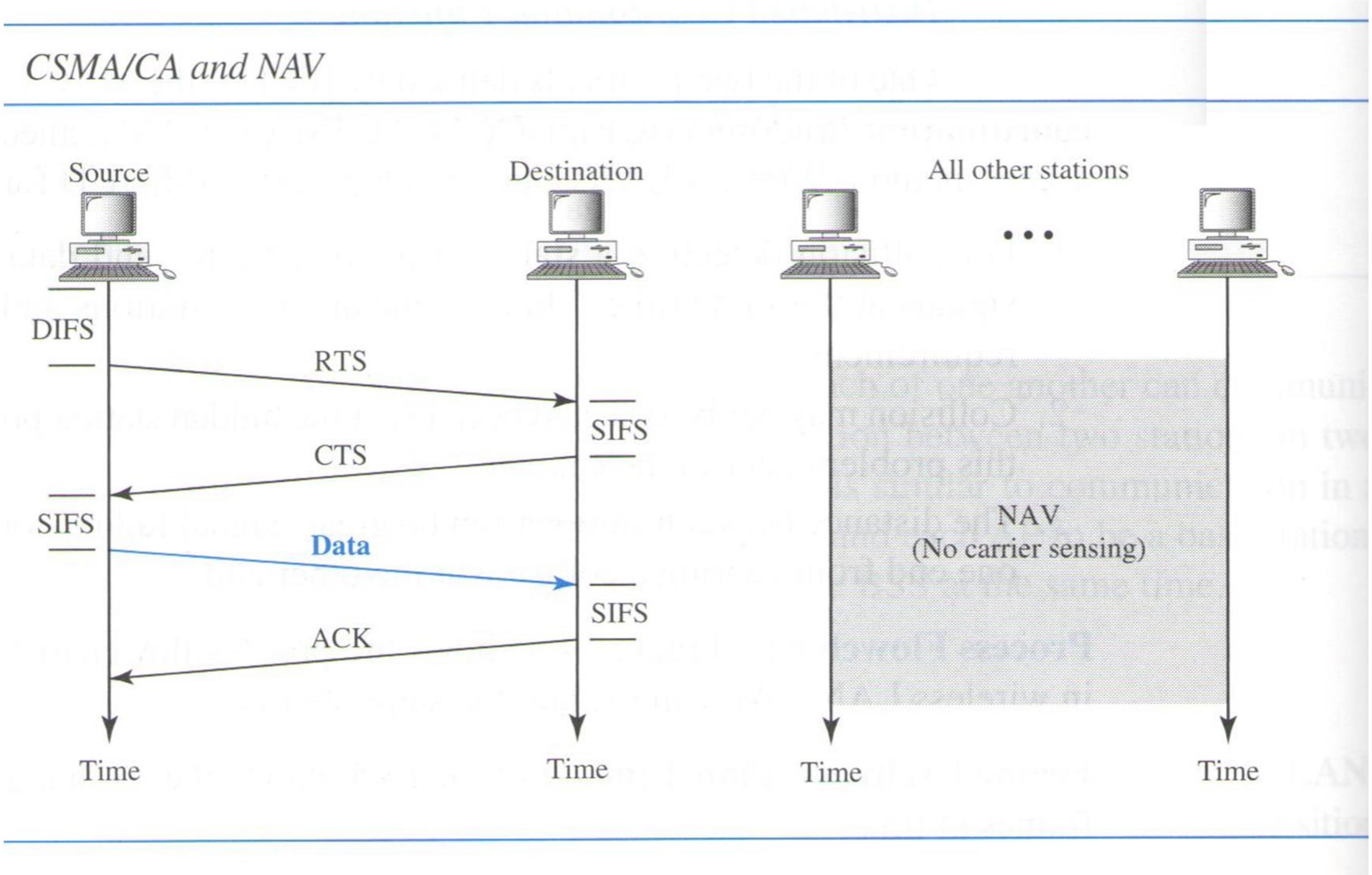


Fig (3.13)

- CSMA with RTS/CTS has reduced the vulnerable period at D. **Ref [2]**
- Collision may occur during RTS/CTS handshake.

Using Network Allocation Vector (NAV)



Fig(3.14) When other stations hears RTS or CTS they stop sensing for NAV time **Ref [1]**

Uses control frames with virtual channel sensing

- Node A is sending to B. The C hears A and holds for NAV.
- but D does not hear A. When B sends, D hears B and holds NAV.

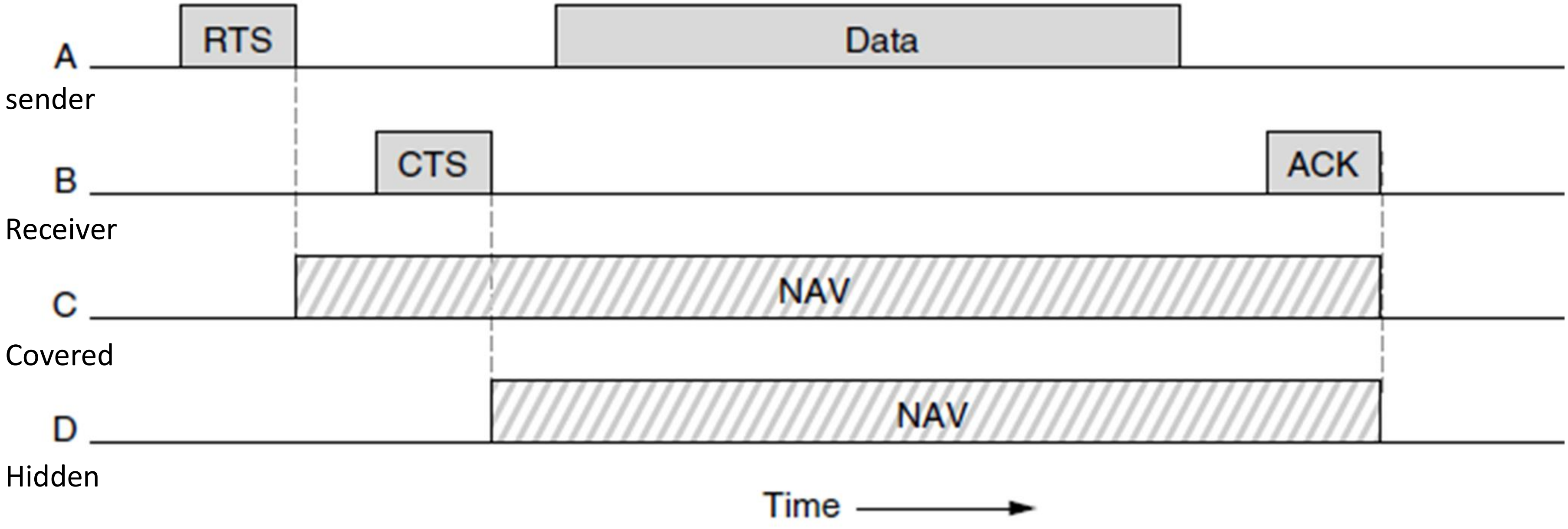


Fig (3.15) Virtual channel sensing using CSMA/CA. **Ref [3]**

Flow Control and Error Control

- The most important responsibilities of data link layer are flow control (FC) and error control (EC).
- **FC:** a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.
- **EC:** is error detection and correction process, can be based on automatic repeat request.

Controlled Access Techniques

- Reservation
- Polling
- Token Ring

Reservation Access

- If there are N stations in the system, there are exactly N reservation minislots in reservation frame. Each minislots belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservation can send their data frames after the reservation frame.
- The figure shows the situation with five stations and a five-minislots reservation frame. In the first interval, only station 1, 3, and 4 have made reservation. In the second interval, only station 1 has made a reservation.

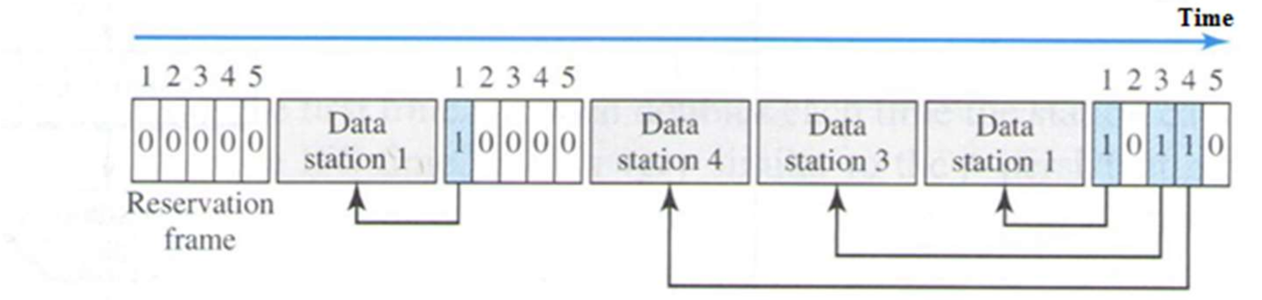


Fig (3.16) *Reservation access method* **Ref [1]**

Polling Access Technique

- Polling works with topologies in which one device is designated as primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.
- The primary device controls the link: the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore is always the initiator of a session.
- If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function. If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

Polling Access Technique

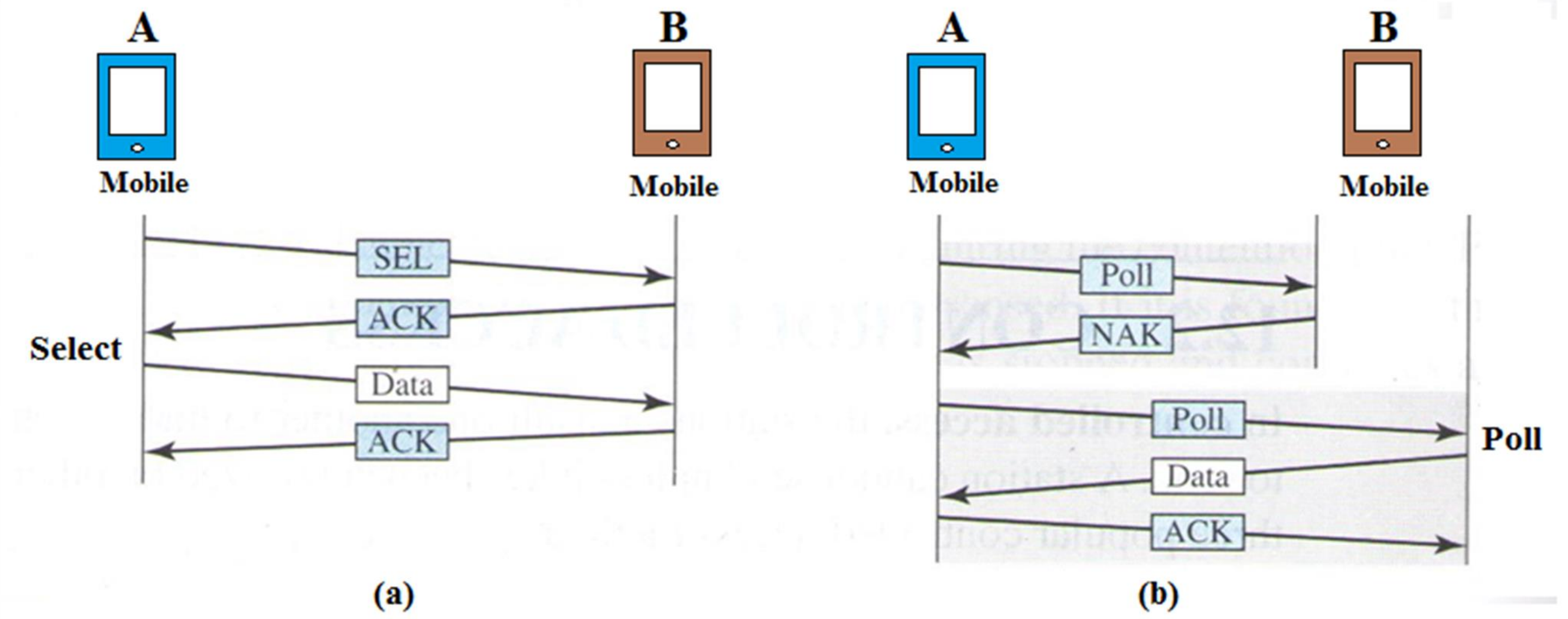


Fig (3.17) **Polling access method: a) Select Function b) Poll Function**

Select functions

- The Select function is used whenever the primary device has something to send. The primary device controls the link, and if the it is not sending nor receiving data it knows the link is available.

- If it has something to send, the primary device sends it. What it does know, is whether the target device is prepared to receive. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgement of the secondary's ready status. Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary.

Polling functions

- The poll function is used by the primary deice to solicit transmissions from the secondary devices. When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send. When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame)if it does.
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgement (ACK frame), verifying its receipt.

References

[1] Forouzan, B., Data Communications and Networking, 4ed.

[2] Marsic, I., Wireless Networks, Local and ad hoc networks, Rutger University.

[3] Tanenbaum, Computer Networks, 5ed.