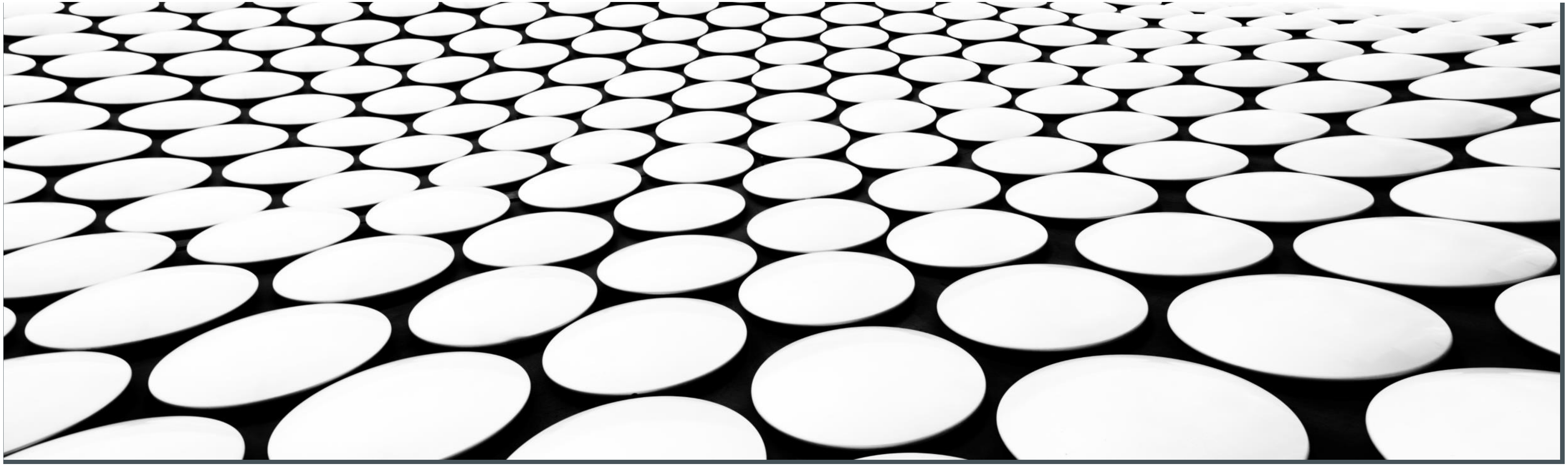
COMPUTER NETWORKS

DATA LINK LAYER

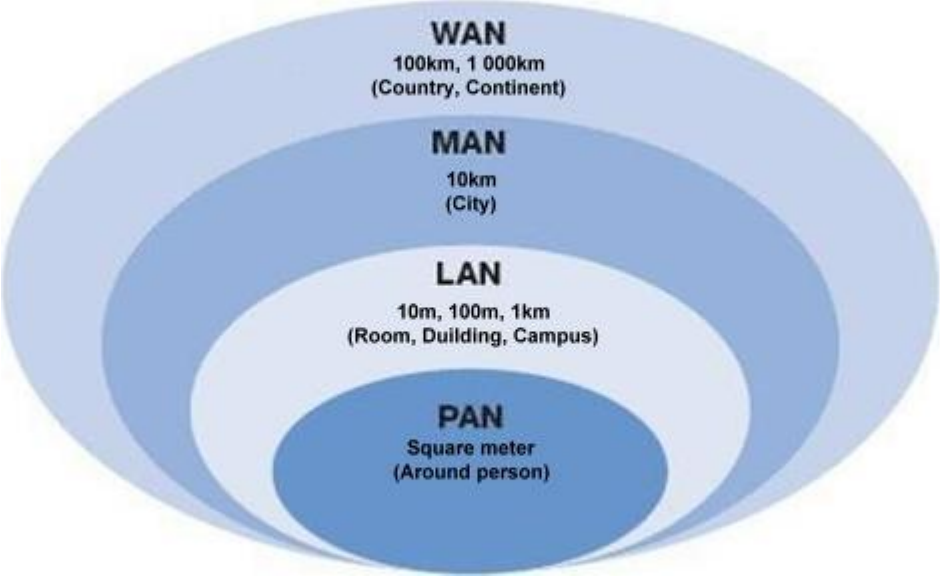
HEMANT GHAYVAT, (hemant.ghayvat@lnu.se)



TODAY

- Hop to hop
- Flow control
- Error control
- Access control
- Physical address (MAC)
- Framing (+header +trailer)

BY SIZE

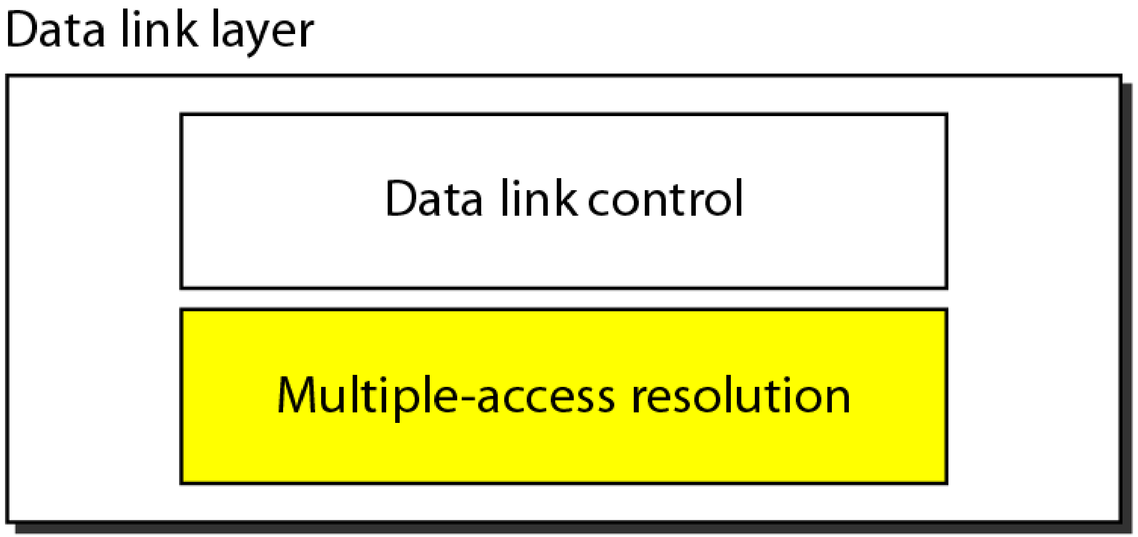


Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

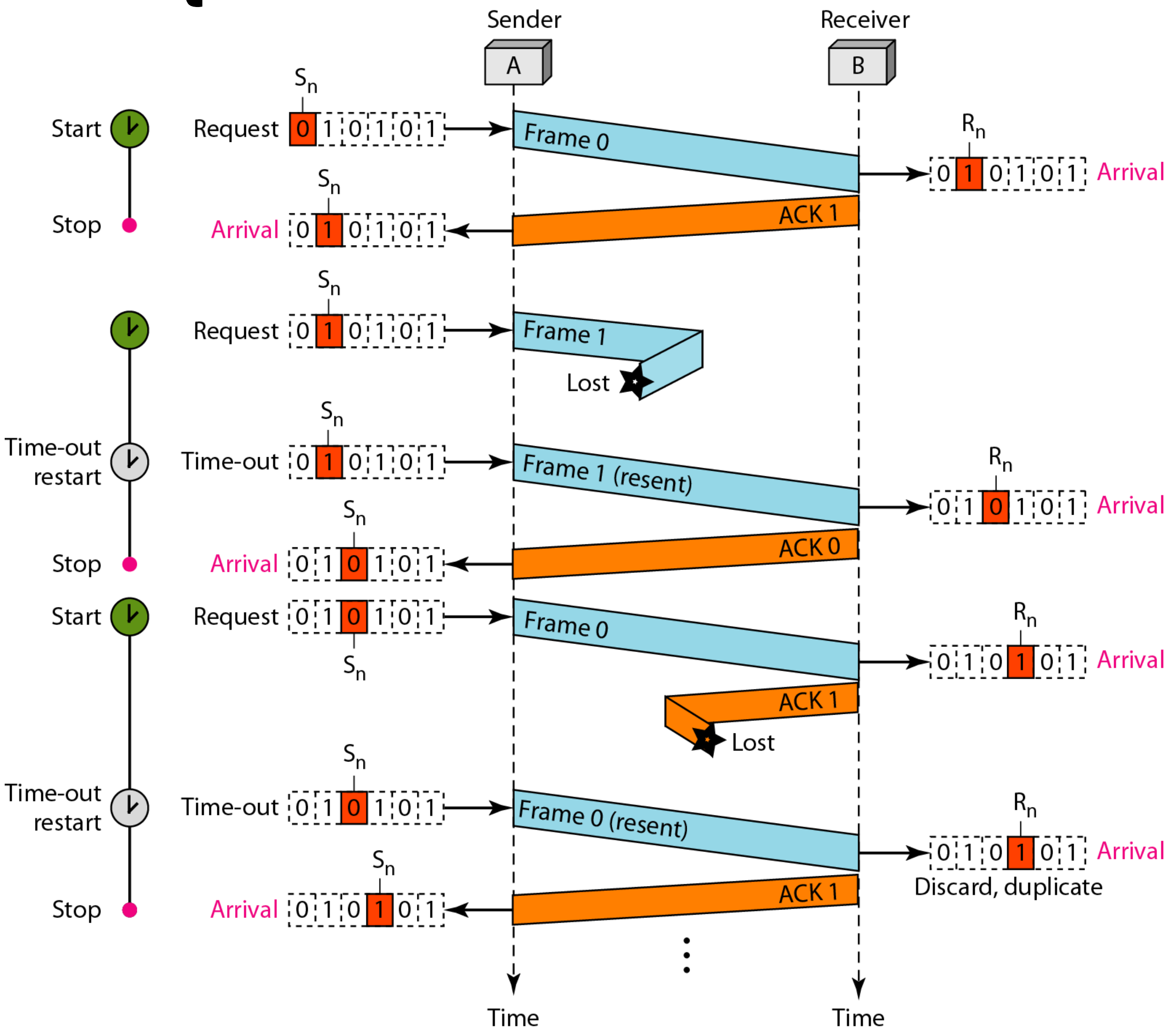
LAN TOPOLOGIES

- Bus
- Ring
- Star

DATA LINK LAYER DIVIDED INTO TWO FUNCTIONALITY-ORIENTED SUBLAYERS



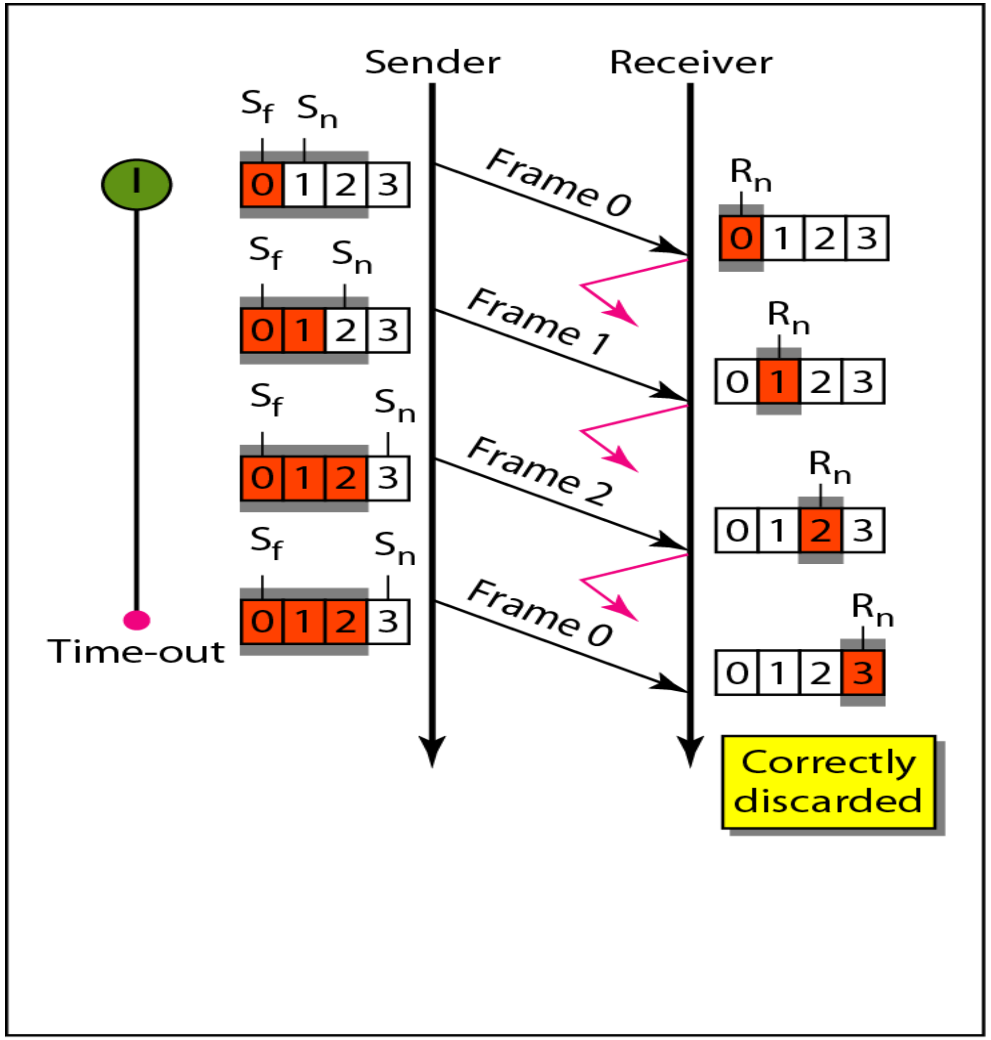
Stop-and-Wait ARQ Protocol



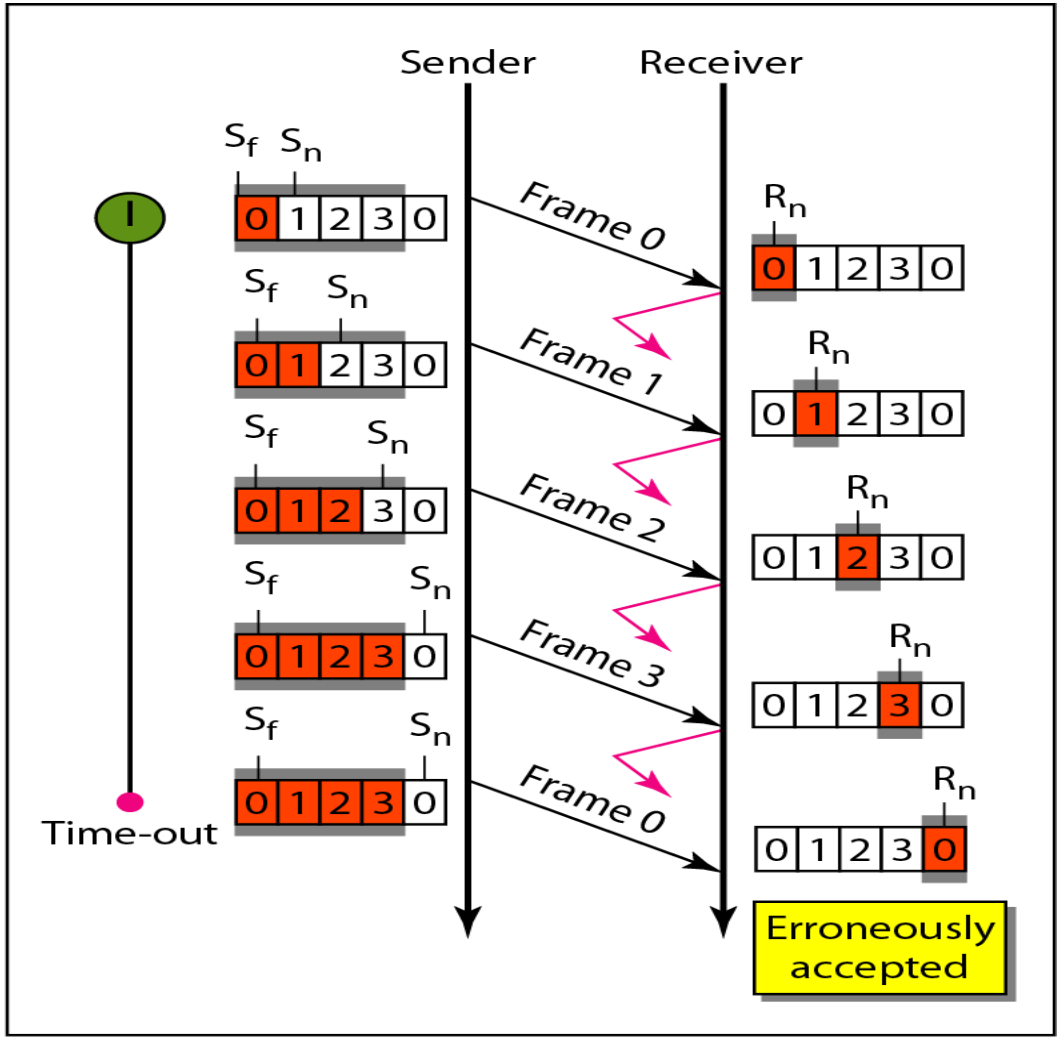
Stop-and-Wait ARQ is a special case of Go-Back-N ARQ in which the size of the send window is 1

In Go-Back-N ARQ, the size of the send window must be less than 2^m *Or* (2^m -1), the size of the receiver window is always 1. m is the number of bits to represent the sequence number

Window size for Go-Back-N ARQ

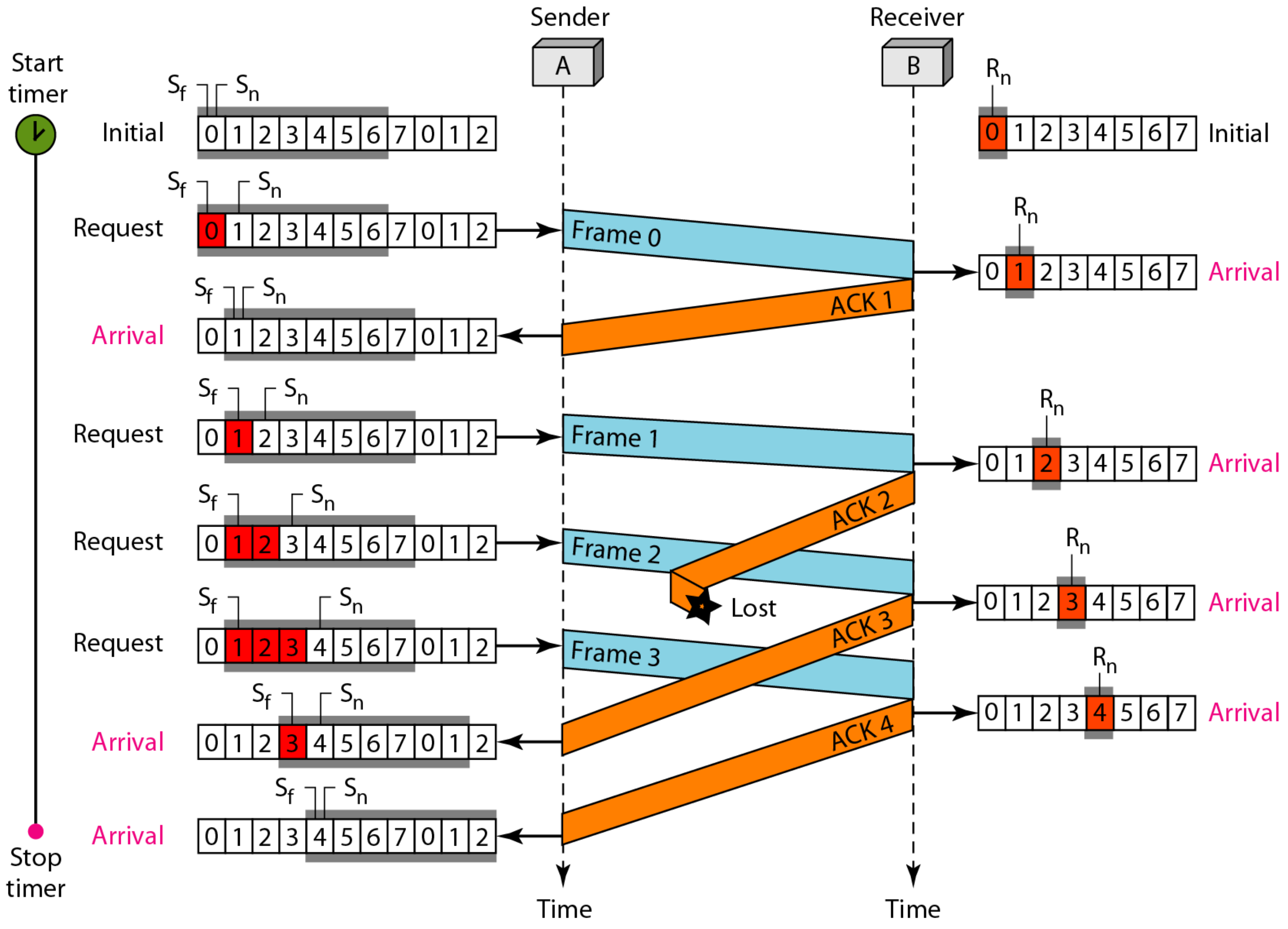


a. Window size $< 2^m$

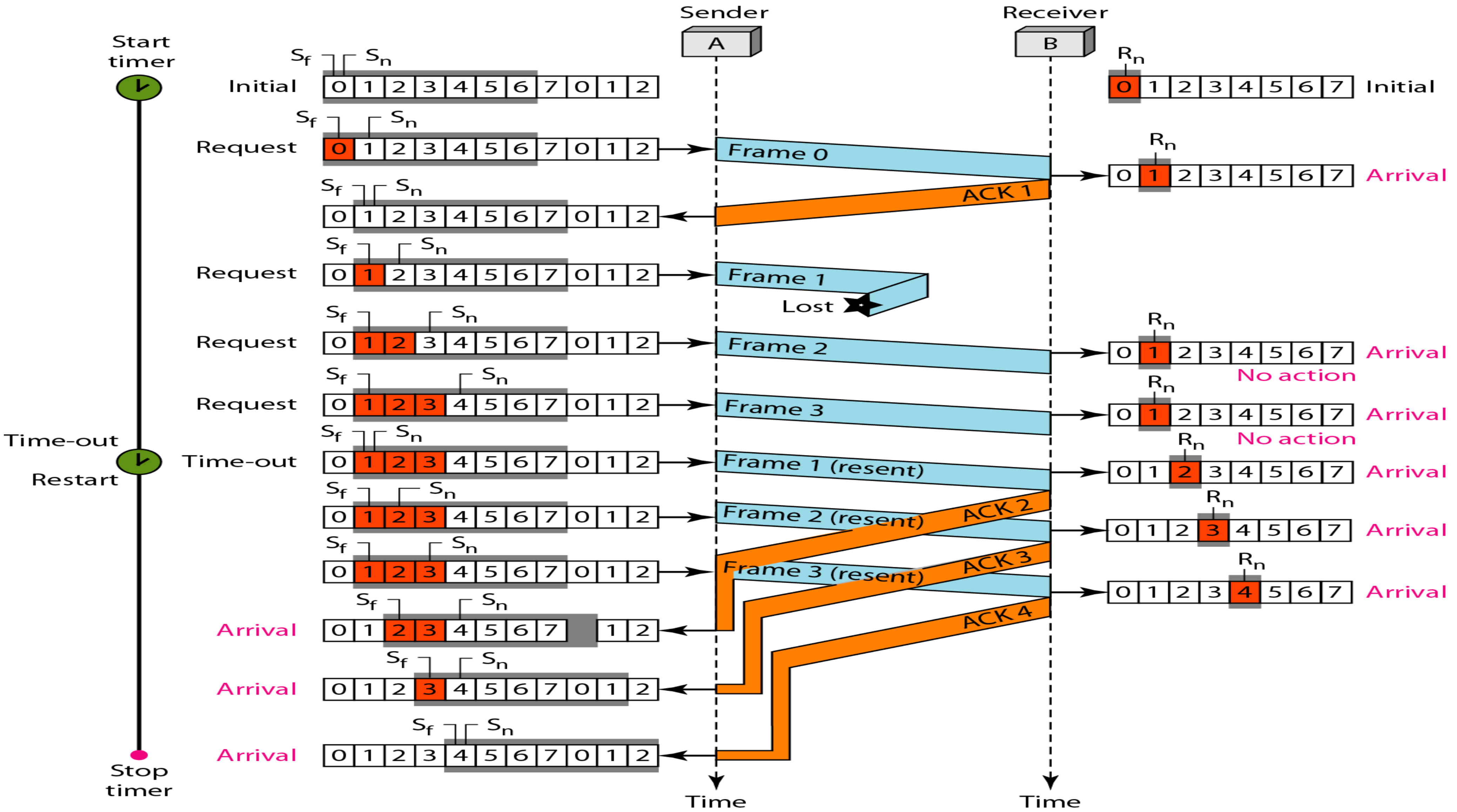


b. Window size $= 2^m$

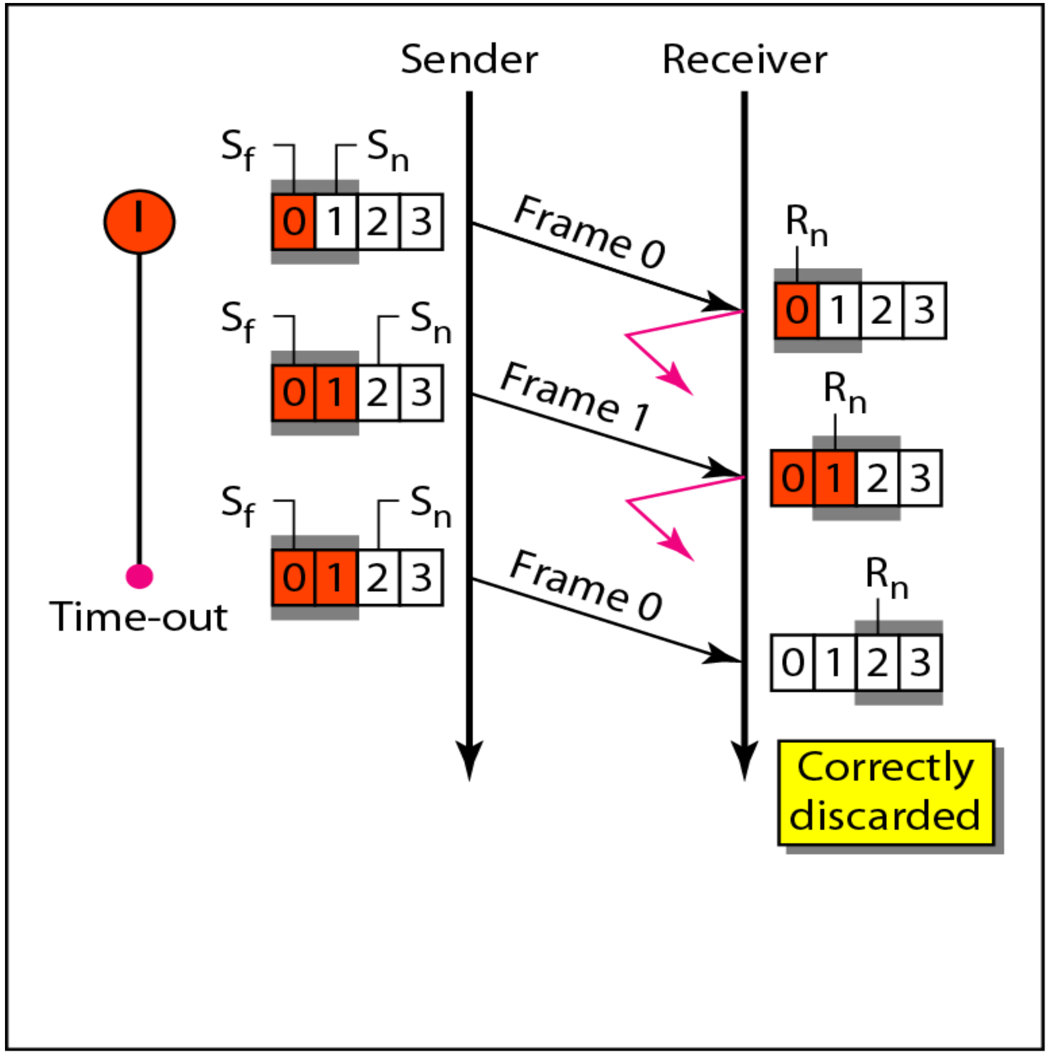
Cumulative acknowledgments can help if acknowledgments are delayed or lost



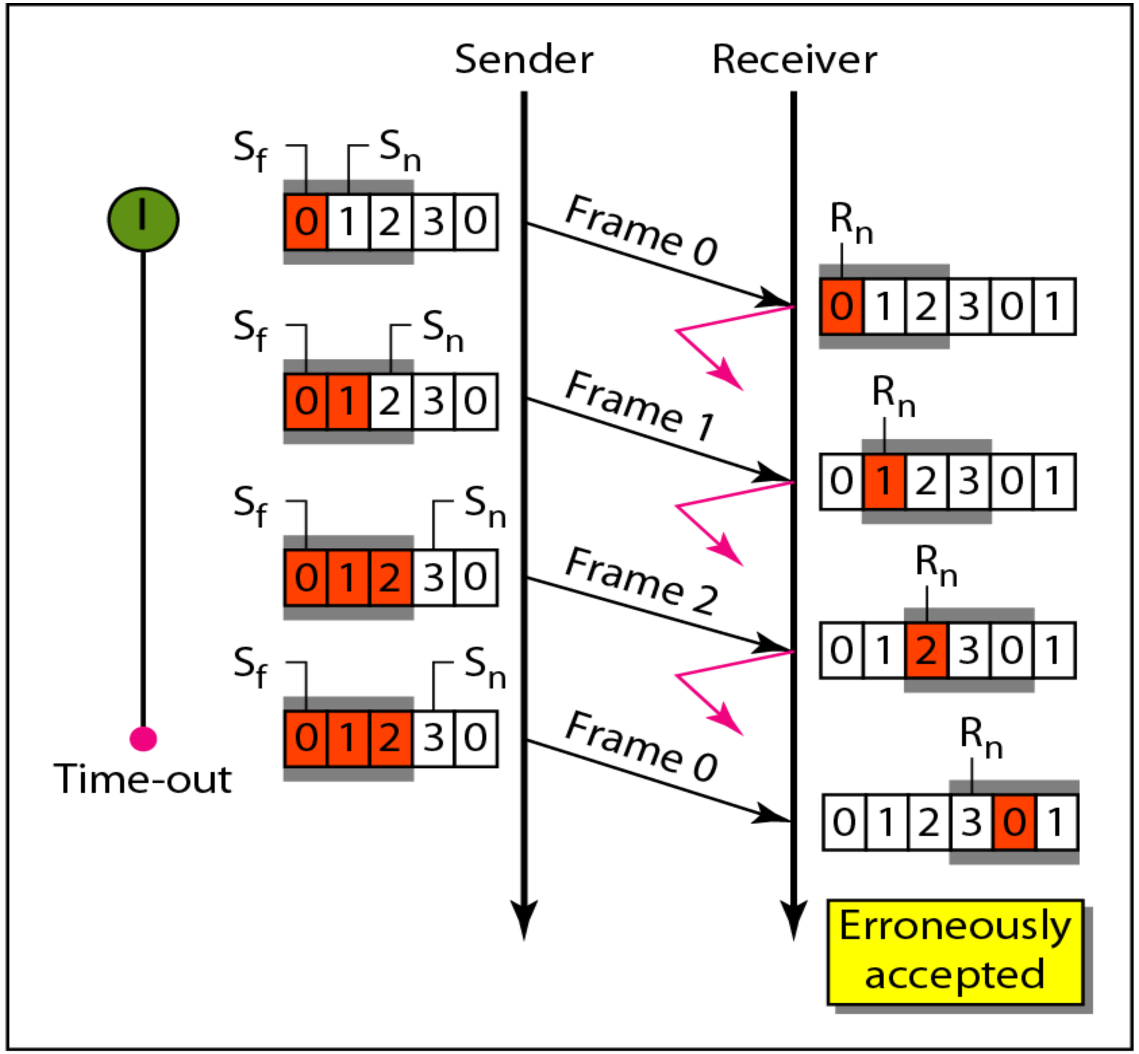
Out of order frames case in Go back-N ARQ



In Selective Repeat ARQ, the size of the sender and receiver window must be at most 2^{m-1}.

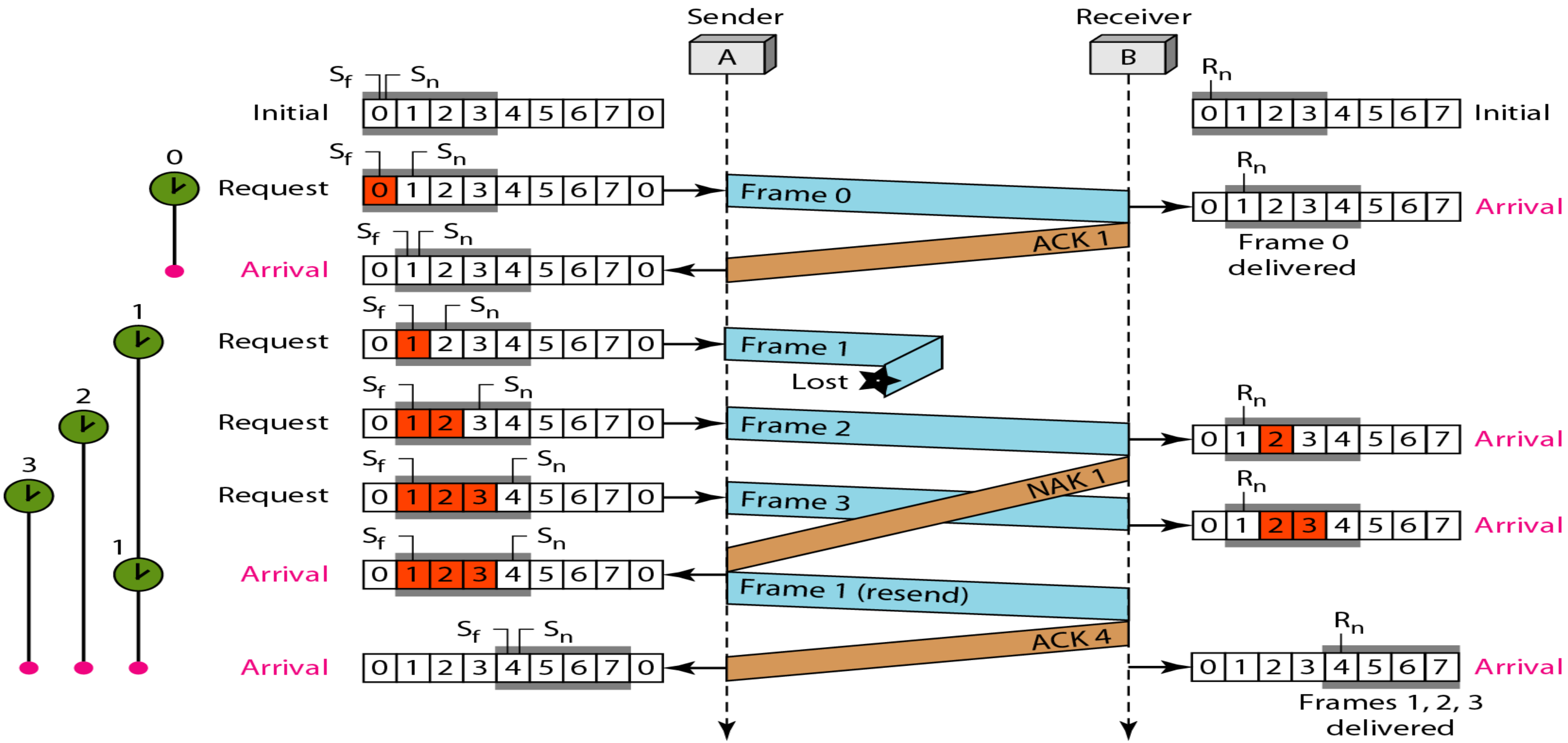


a. Window size = 2^{m-1}

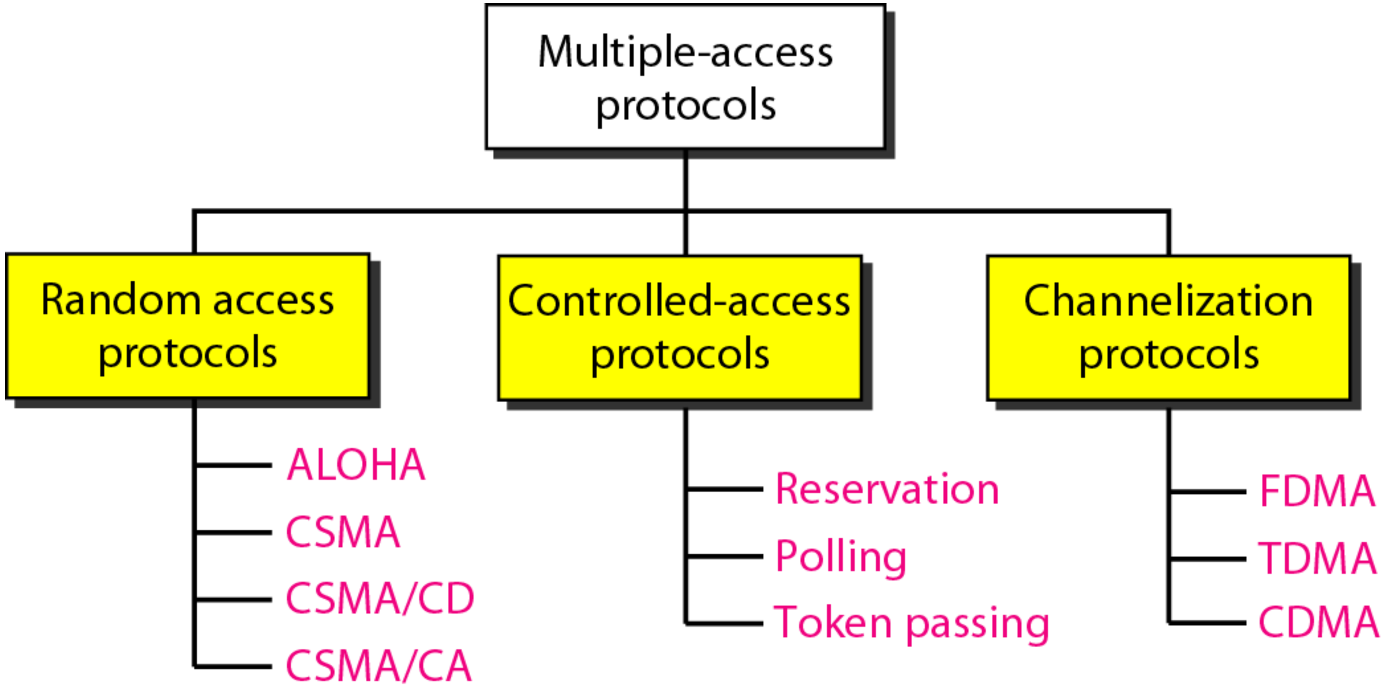


b. Window size > 2^{m-1}

Out of order frame in case of Selective Repeat ARQ



TAXONOMY OF MULTIPLE-ACCESS PROTOCOLS



Multiple-access protocols

- Random access protocols
  - ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- Controlled-access protocols
  - Reservation
  - Polling
  - Token passing
- Channelization protocols
  - FDMA
  - TDMA
  - CDMA

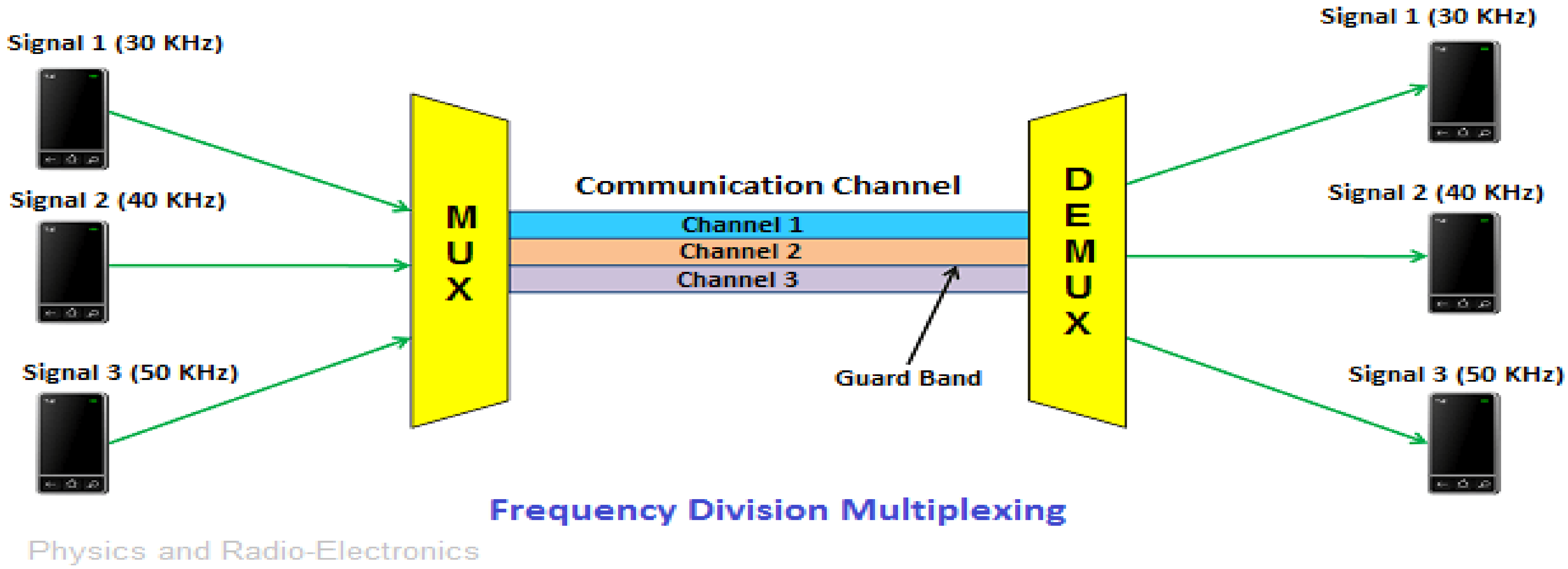
CHANNELIZATION

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. In this section, we discuss three channelization protocols.

Topics discussed in this section:

Frequency-Division Multiple Access (FDMA)
Time-Division Multiple Access (TDMA)
Code-Division Multiple Access (CDMA)

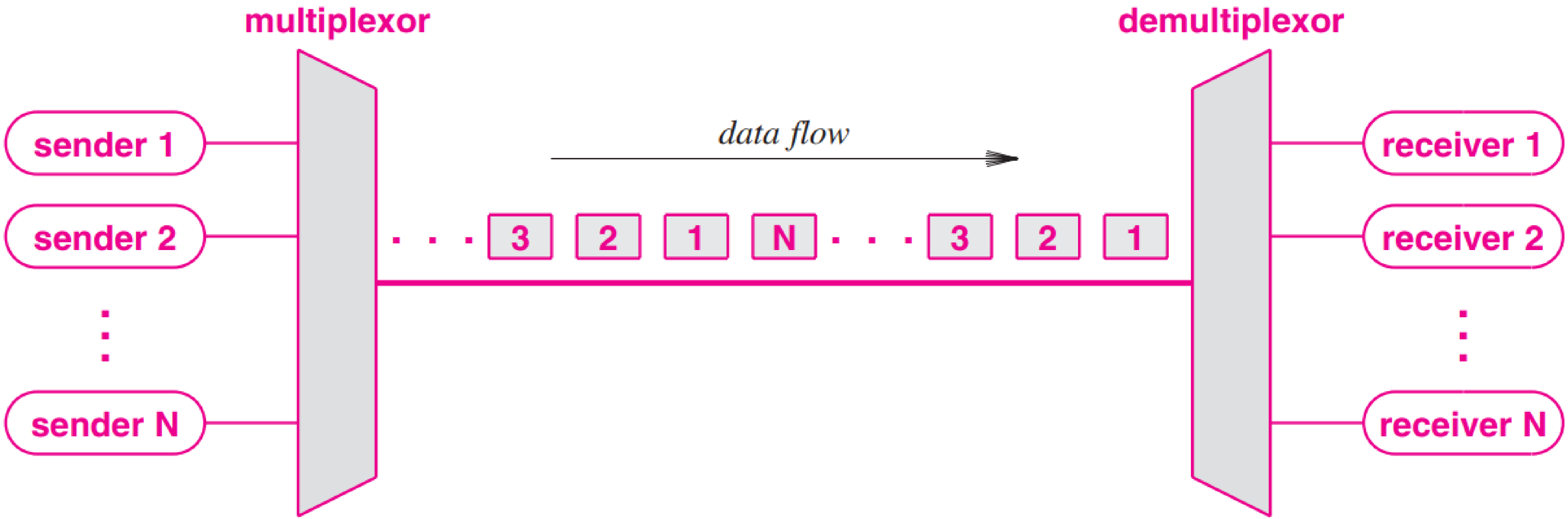
Frequency-Division Multiple Access (FDMA)



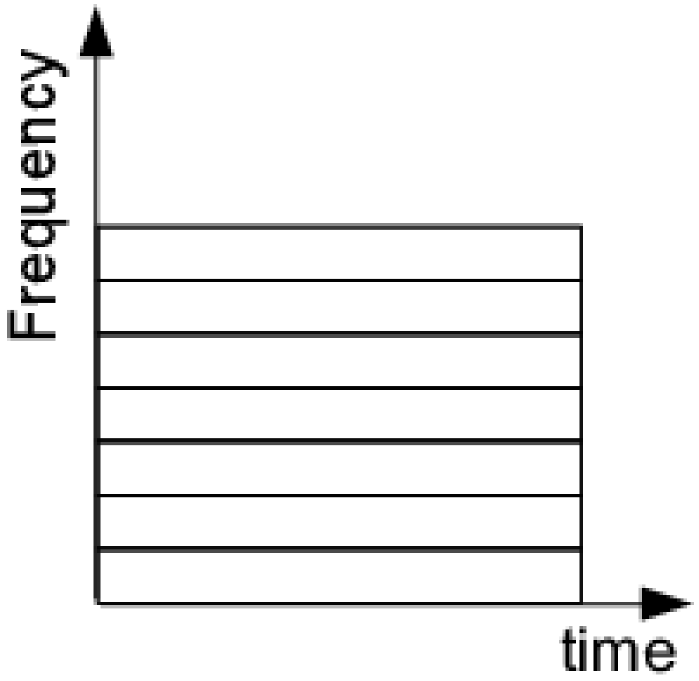
Because carrier waves on separate frequencies do not interfere, frequency division multiplexing provides each sender and receiver pair with a private communication channel.

TDMA

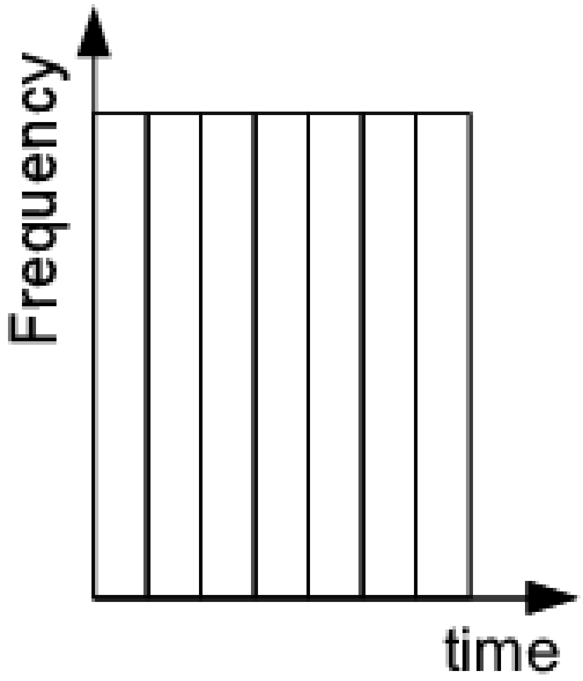
- Instead of splitting the original RF channel in to two or more RF sub-channels, it is instead split into timeslots. The transmitted RF frequency is identical in each slot, but each slot is still capable of carrying a separate conversation.
- TDMA is utilized by Digital-Advanced Mobile Phone System (D-AMPS) and Global System for Mobile communications (GSM). However, each of these systems implements TDMA in a somewhat different and incompatible way.


multiplexor
demultiplexor
data flow
sender 1
sender 2
sender N
receiver 1
receiver 2
receiver N
3
2
1
N
3
2
1

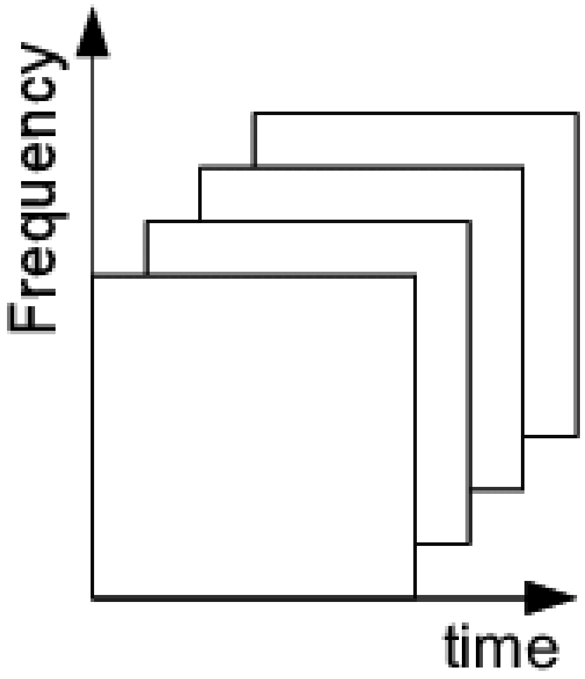
FDMA TDMA AND CDMA



FDMA



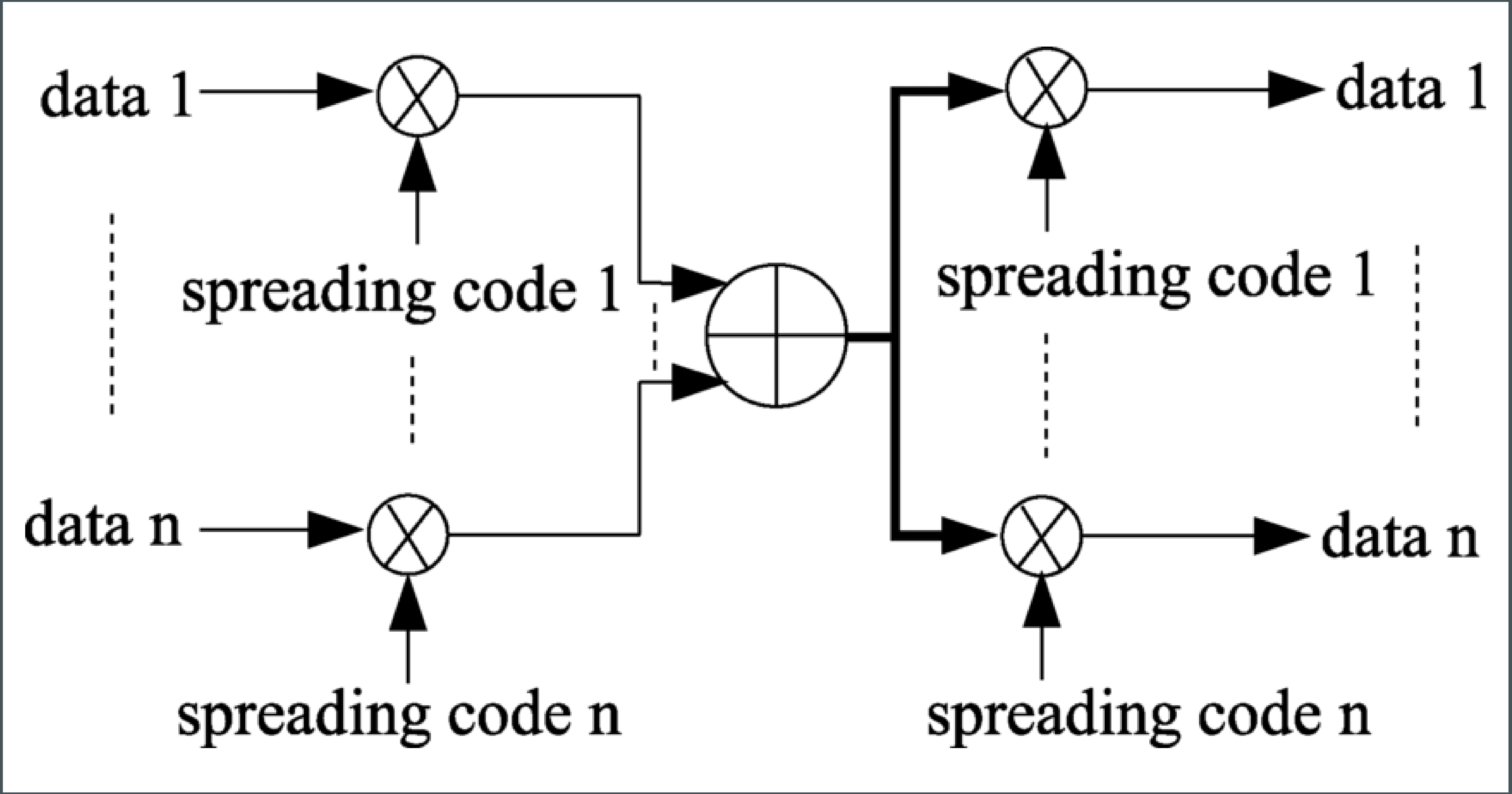
TDMA



CDMA

CDMA

- Multiple signals in the same frequency band and in the same time slot.
- Each signal uses a different code (i.e., a spread spectrum code)
- Originally Spread Spectrum technology for a military use.
  - More secure against an eavesdropping
  - More resilient against a noise
- The receiver, must know:
  - Spread spectrum code
  - The time the code was generated ➔ Need to be synchronized
    - Currently use GPS (Global Positioning System)


data 1
spreading code 1
data n
spreading code n
data 1
spreading code 1
data n
spreading code n

RANDOM ACCESS

In random access or contention methods, no station is superior to another station and none is assigned the control over another. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether to send.

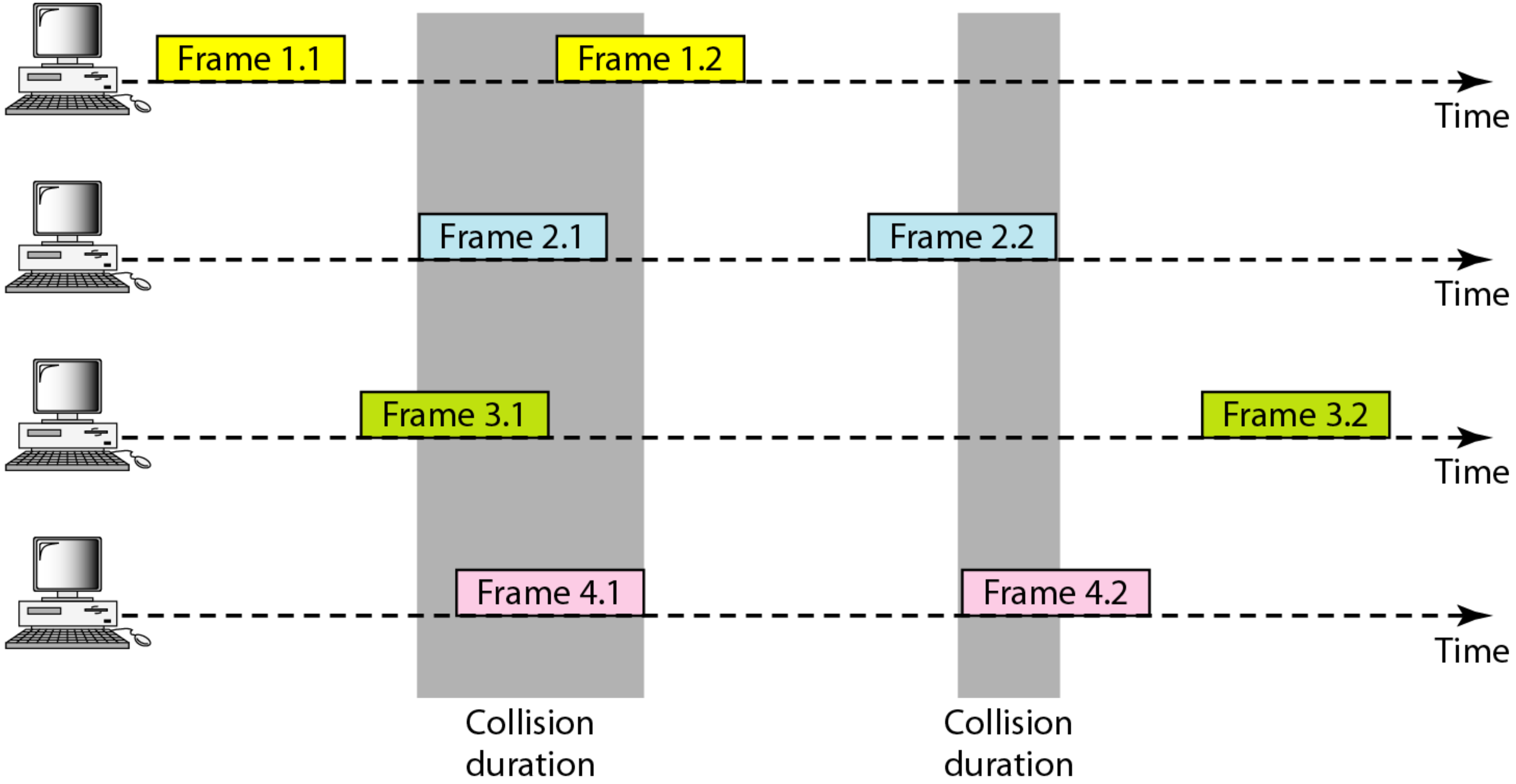
Topics discussed in this section:

ALOHA (Pure and Slotted)
Carrier Sense Multiple Access
Carrier Sense Multiple Access with Collision Detection
Carrier Sense Multiple Access with Collision Avoidance

ALOHA (ADDITIVE LINKS ON-LINE HAWAII AREA) PROTOCOL

- If there is a collision,
  - the sender waits a random amount of time and sends it again.
- The waiting time must be random. Otherwise, the same packets will collide again.

Frames in a pure ALOHA network



SLOTTED ALOHA

- » Slotted ALOHA divides the time into slots equal to packet transmission time.
- A node transmits at the beginning of the next slot.
- If collision, wait for a future slot and decreases the risk of collisions
- Synchronous, that is time is divided into slots
- Slot size is equal to the transmission time of a packet
- When you are ready, transmit at the start of the time slot.
- Doubles the efficiency of Aloha (38% throughput)
- But requires synchronization!

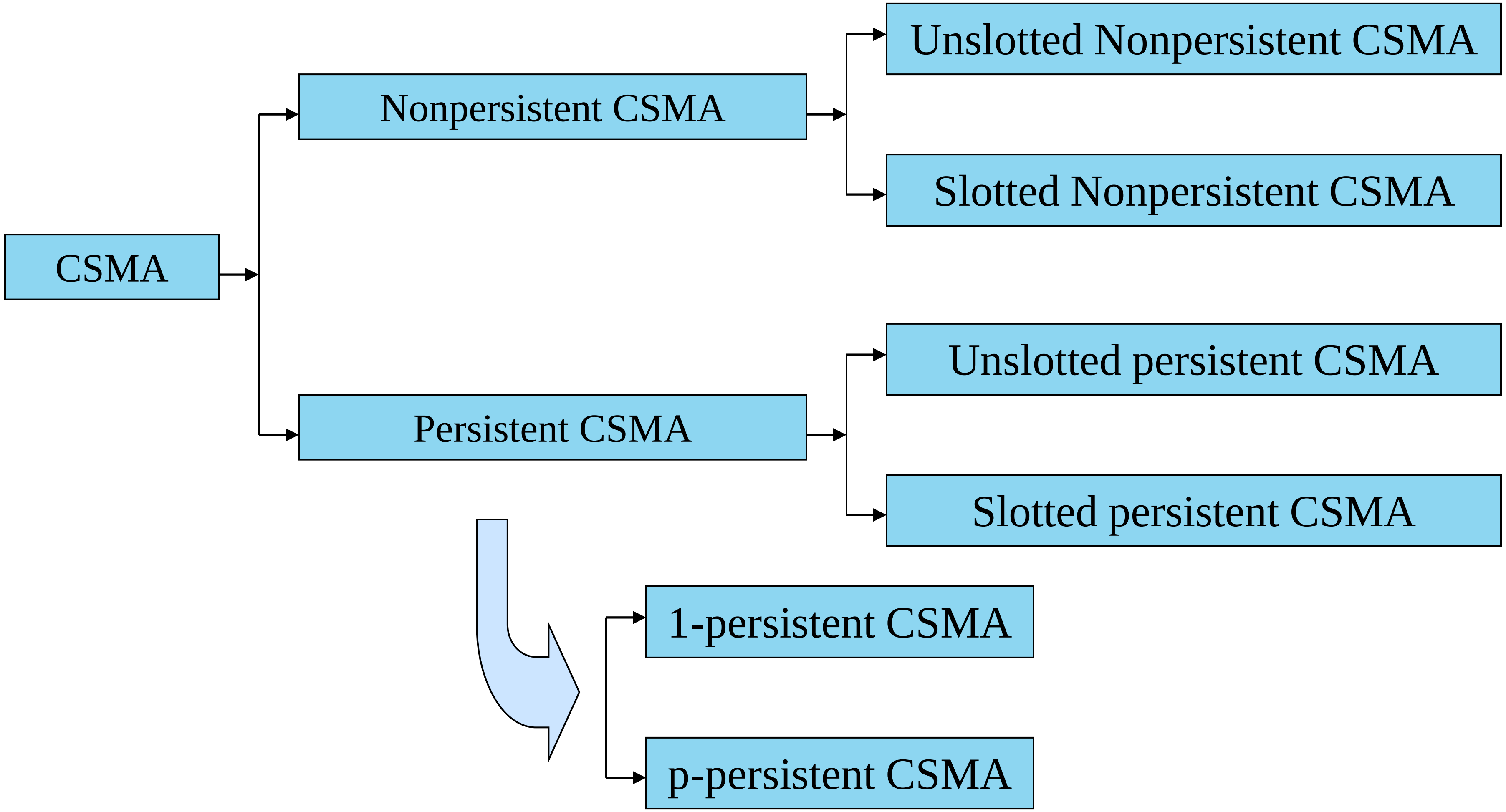
CSMA (CARRIER SENSE MULTIPLE ACCESS)

✓ Max throughput achievable by slotted ALOHA is 0.368.

CSMA gives improved throughput compared to Aloha protocols.

Listens to the channel before transmitting a packet (avoid avoidable collisions).

KINDS OF CSMA



NONPERSISTENT/X-PERSISTENT CSMA PROTOCOLS

- Nonpersistent CSMA Protocol:

Step 1: If the medium is idle, transmit immediately

Step 2: If the medium is busy, wait a random amount of time (waste of BW or collision) and repeat **Step 1**

  - Random backoff reduces probability of collisions
  - Waste idle time if the backoff time is too long

- 1-persistent CSMA Protocol:

Step 1: If the medium is idle, transmit immediately

Step 2: If the medium is busy, continue to listen until medium becomes idle, and then transmit immediately

  - There will always be a collision if two nodes want to retransmit

    (usually you stop transmission attempts after few tries)

NONPERSISTENT/X-PERSISTENT CSMA PROTOCOLS

- p-persistent CSMA Protocol:

Step 1: If the medium is idle, transmit with probability p, and delay for worst case propagation delay for one packet with probability (1-p)

Step 2: If the medium is busy, continue to listen until medium becomes idle, then go to **Step 1**

Step 3: If transmission is delayed by one time slot, continue with **Step 1**

  - A good tradeoff between nonpersistent and 1-persistent CSMA

CSMA/CD (CSMA WITH COLLISION DETECTION)

- In CSMA, if 2 terminals begin sending packet at the same time, each will transmit its complete packet (although collision is taking place).

- Wasting medium for an entire packet time.

- CSMA/CD

  Step 1: If the medium is idle, transmit

  Step 2: If the medium is busy, continue to listen until the channel is idle then transmit

  Step 3: If a collision is detected during transmission, cease transmitting

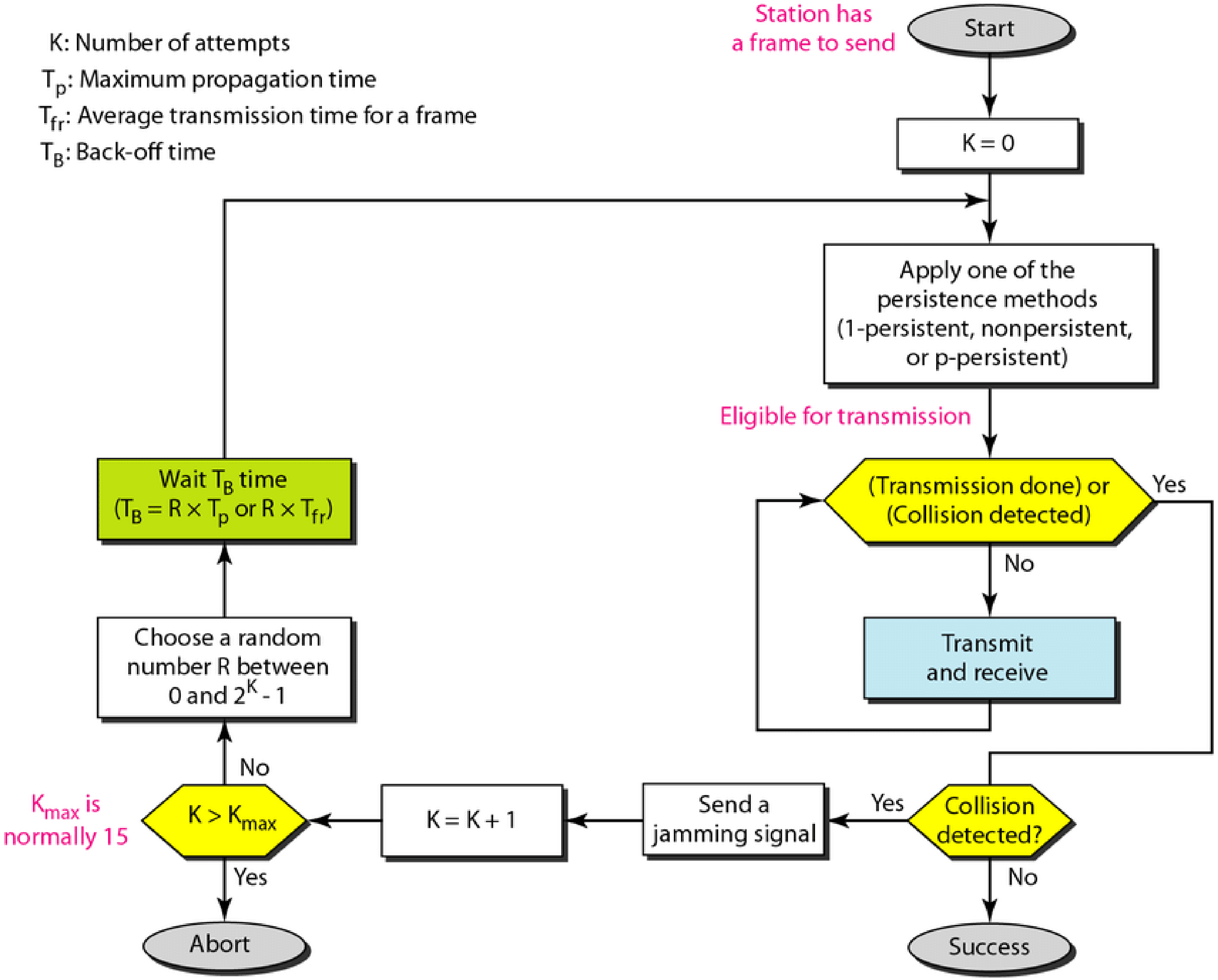
  Step 4: Wait a random amount of time and repeats the same algorithm

K: Number of attempts

T_p: Maximum propagation time

T_{fr}: Average transmission time for a frame

T_B: Back-off time



Station has a frame to send

Start

K = 0

Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)

Eligible for transmission

(Transmission done) or (Collision detected)

Yes

No

Transmit and receive

Collision detected?

Yes

No

Success

Send a jamming signal

K = K + 1

$K > K_{max}$

K_{max} is normally 15

Yes

Abort

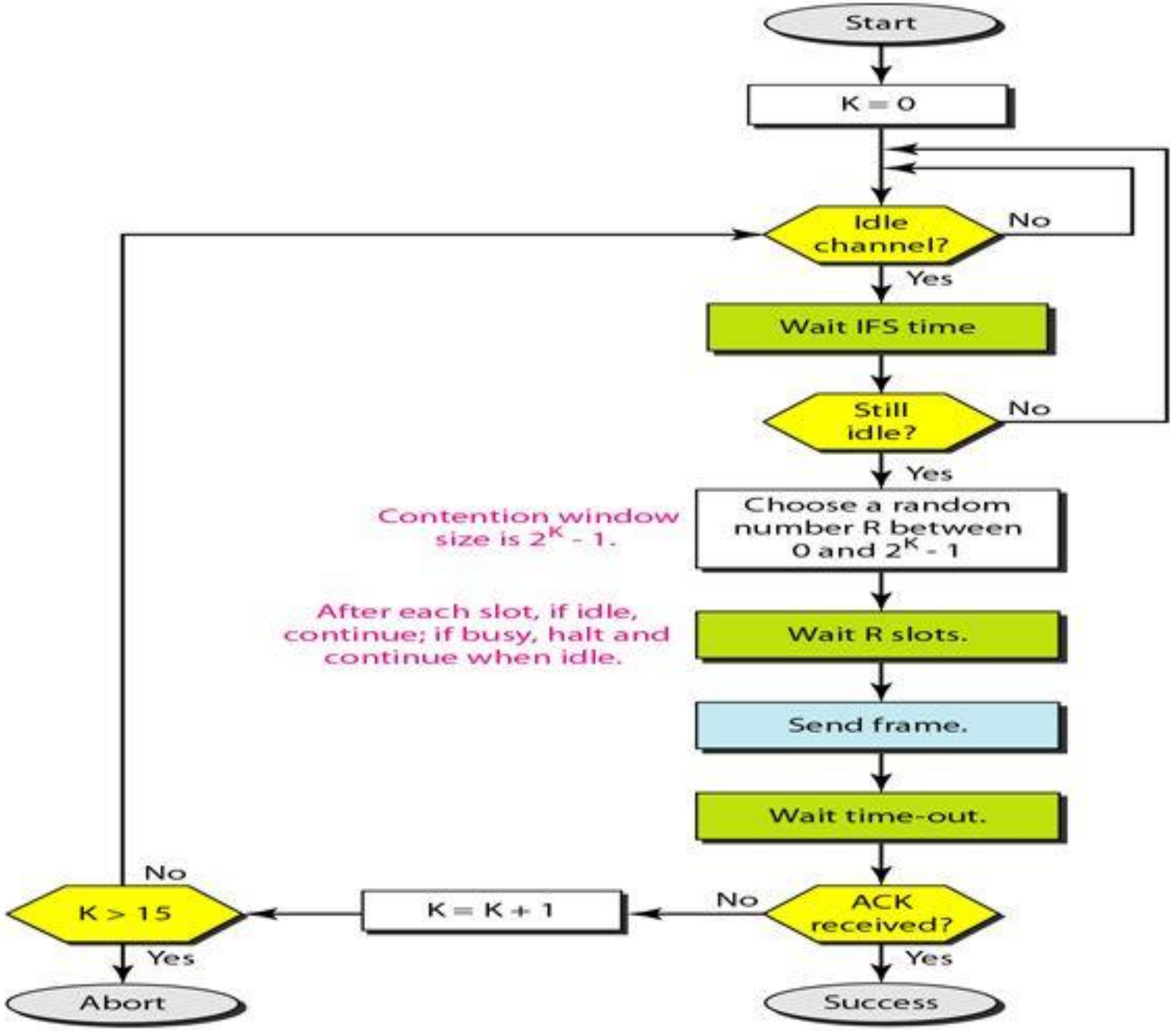
No

Choose a random number R between 0 and $2^K - 1$

Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)

CSMA/CA (CSMA WITH COLLISION AVOIDANCE)

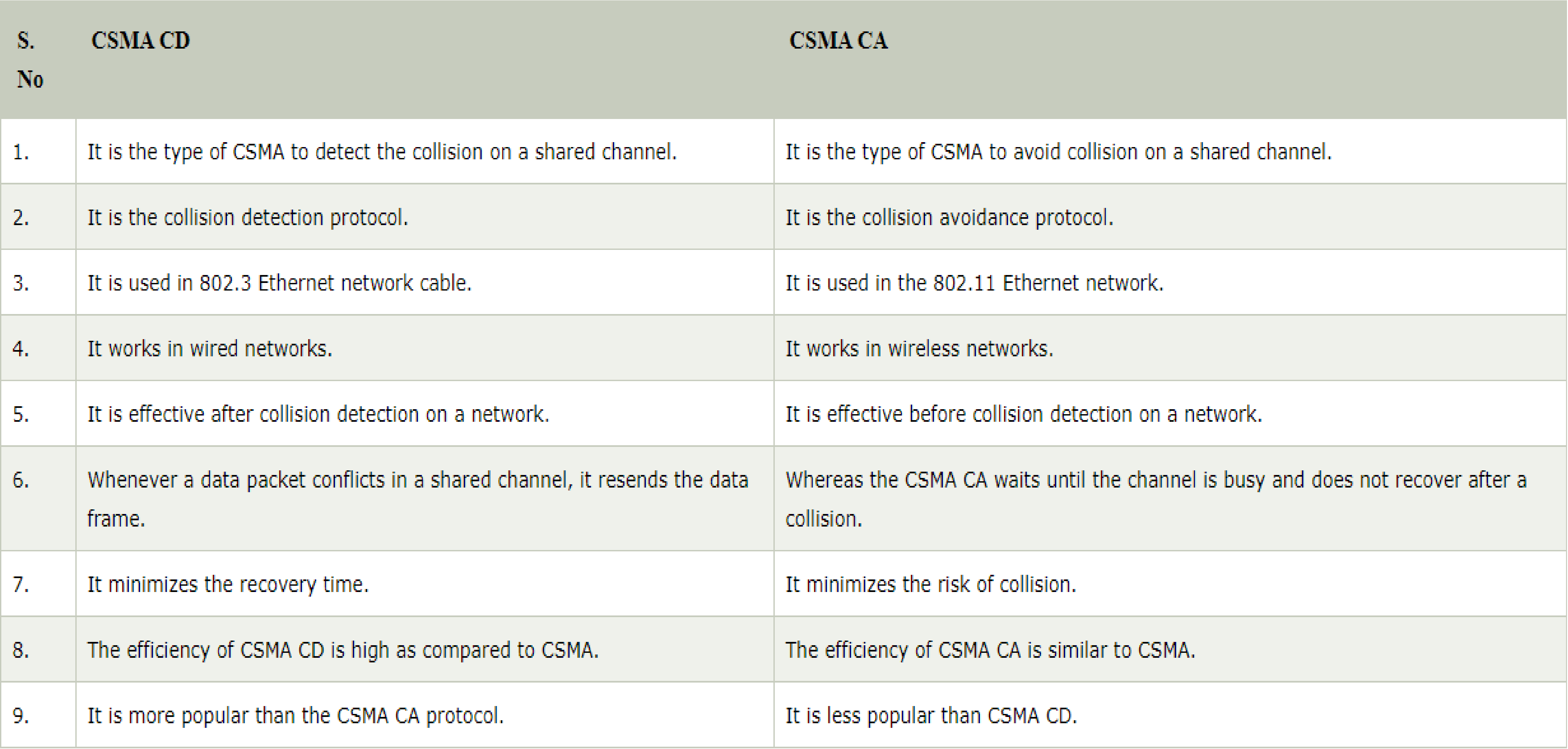
- All terminals listen to the same medium as CSMA/CD.
- Terminal ready to transmit senses the medium.
- If medium is busy it waits until the end of current transmission.
- It again waits for an additional predetermined time period DIFS (Distributed inter frame Space).
- Then picks up a random number of slots (the initial value of backoff counter) within a contention window to wait before transmitting its frame.
- If there are transmissions by other terminals during this time period (backoff time), the terminal freezes its counter.
- It resumes count down after other terminals finish transmission + DIFS. The terminal can start its transmission when the counter reaches to zero.



Contention window size is 2^K - 1.

After each slot, if idle, continue; if busy, halt and continue when idle.

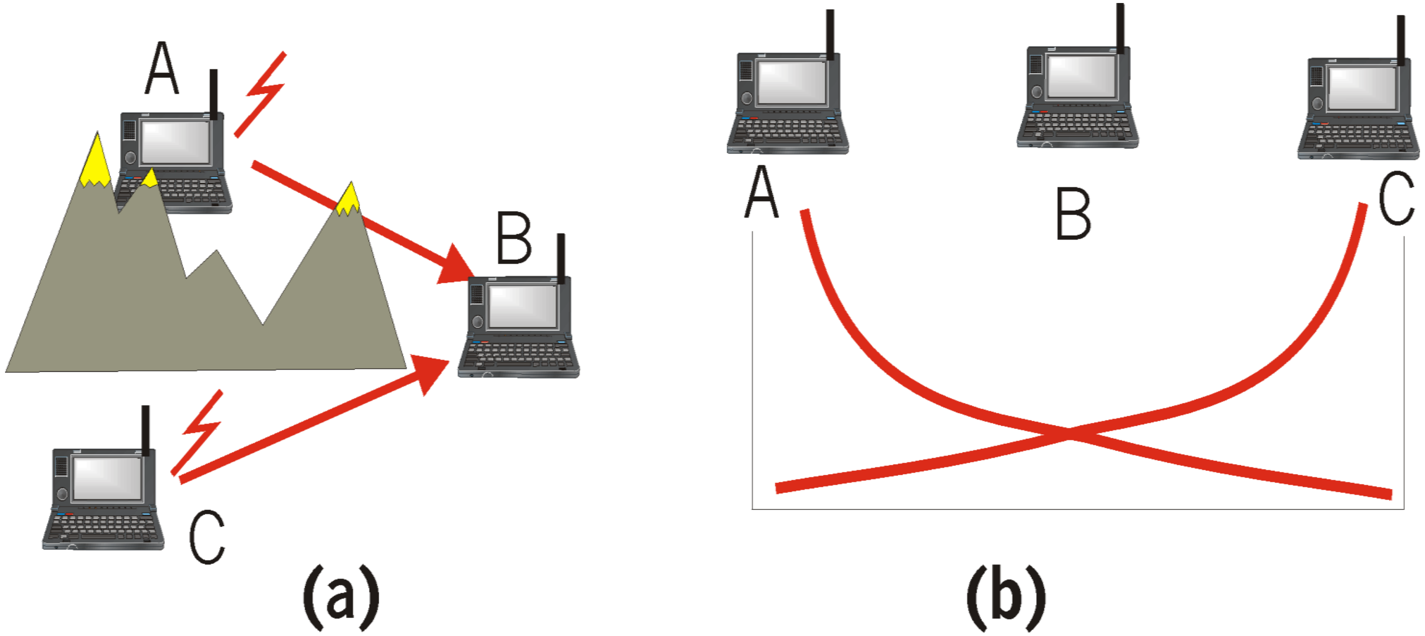
CSMA CD VS CSMA CA



S. No	CSMA CD	CSMA CA
1.	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
2.	It is the collision detection protocol.	It is the collision avoidance protocol.
3.	It is used in 802.3 Ethernet network cable.	It is used in the 802.11 Ethernet network.
4.	It works in wired networks.	It works in wireless networks.
5.	It is effective after collision detection on a network.	It is effective before collision detection on a network.
6.	Whenever a data packet conflicts in a shared channel, it resends the data frame.	Whereas the CSMA CA waits until the channel is busy and does not recover after a collision.
7.	It minimizes the recovery time.	It minimizes the risk of collision.
8.	The efficiency of CSMA CD is high as compared to CSMA.	The efficiency of CSMA CA is similar to CSMA.
9.	It is more popular than the CSMA CA protocol.	It is less popular than CSMA CD.

IEEE 802.11: MULTIPLE ACCESS

- Collision if 2 or more nodes transmit at same time
- CSMA makes sense:
  - get all the bandwidth if you're the only one transmitting
  - shouldn't cause a collision if you sense another transmission
- Collision detection doesn't work: hidden terminal problem



IEEE 802.11 MAC PROTOCOL: CSMA/CA

802.11 CSMA: sender

- if sense channel idle for Distributed coordination function (DCF) Inter-frame Space (DISF) sec.

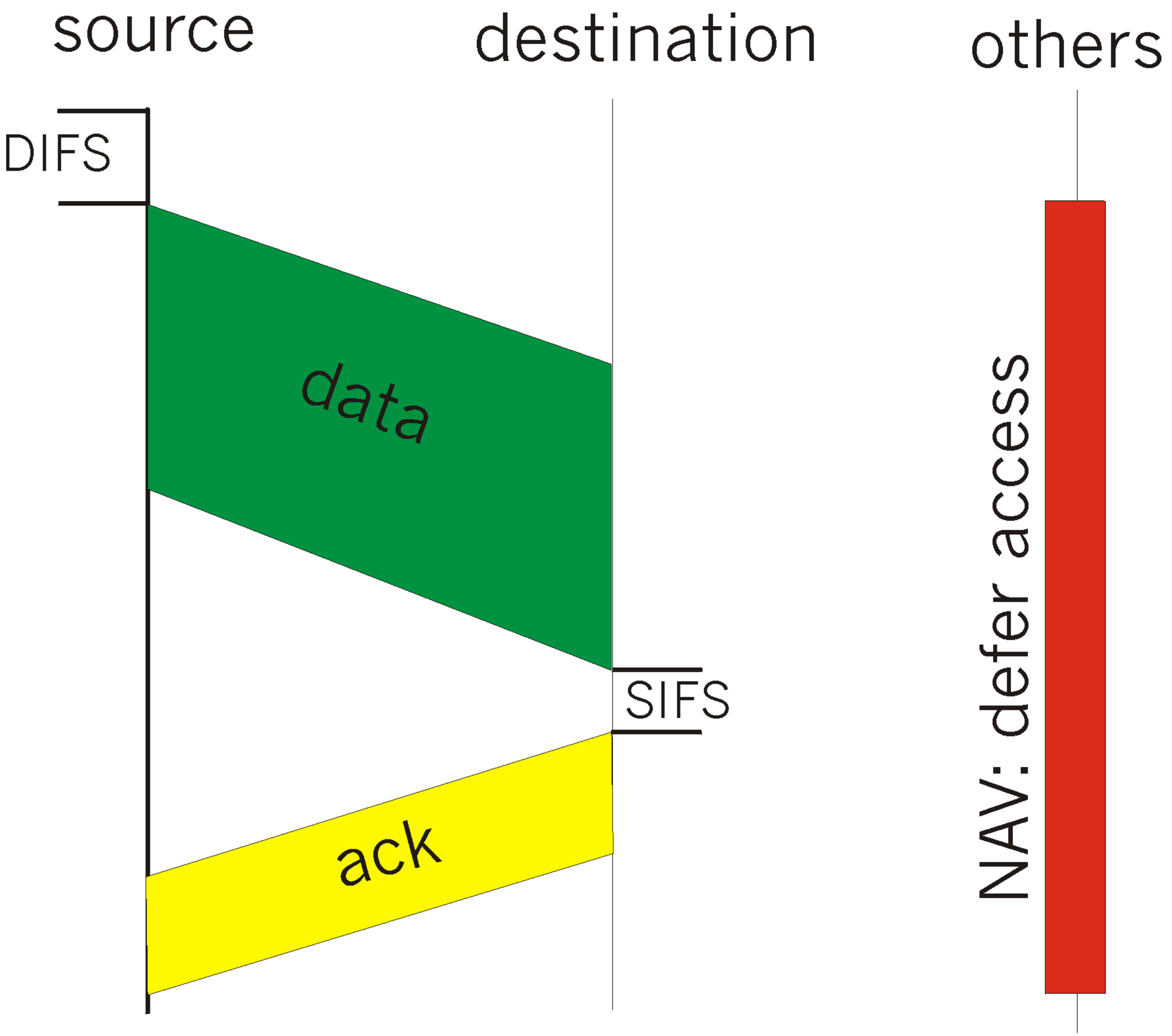
then transmit entire frame (no collision detection)

-if sense channel busy then binary backoff

802.11 CSMA receiver

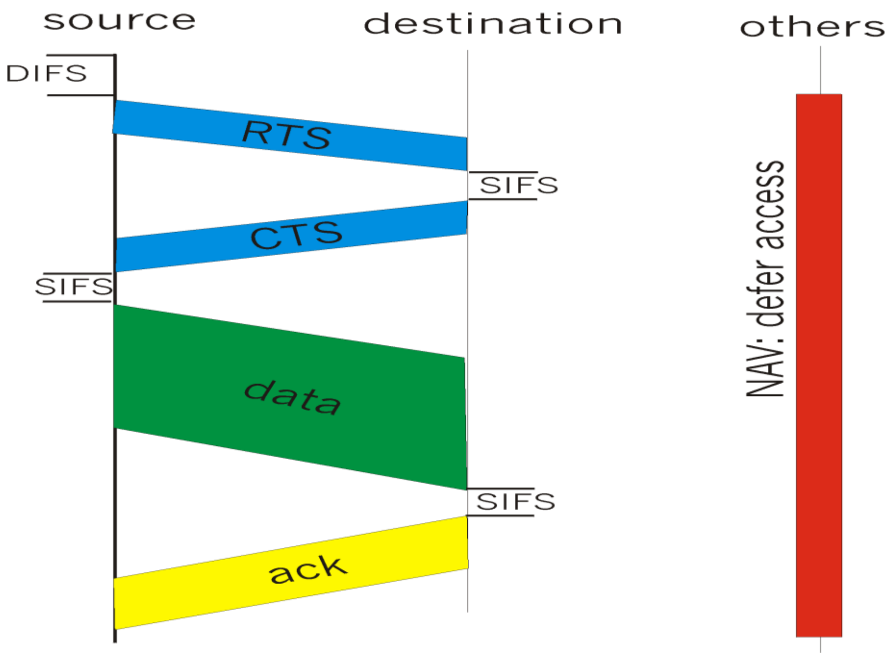
- if received OK

return ACK after Short Inter Frame Spacing (SIFS) sec (ACK is needed due to hidden terminal problem)



COLLISION AVOIDANCE: RTS-CTS EXCHANGE

- sender transmits short RTS (request to send) packet: indicates duration of transmission
- receiver replies with short CTS (clear to send) packet
  - notifying (possibly hidden) nodes
- hidden nodes will not transmit for specified duration: NAV



CONTROLLED ACCESS

In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations. We discuss three popular controlled-access methods.

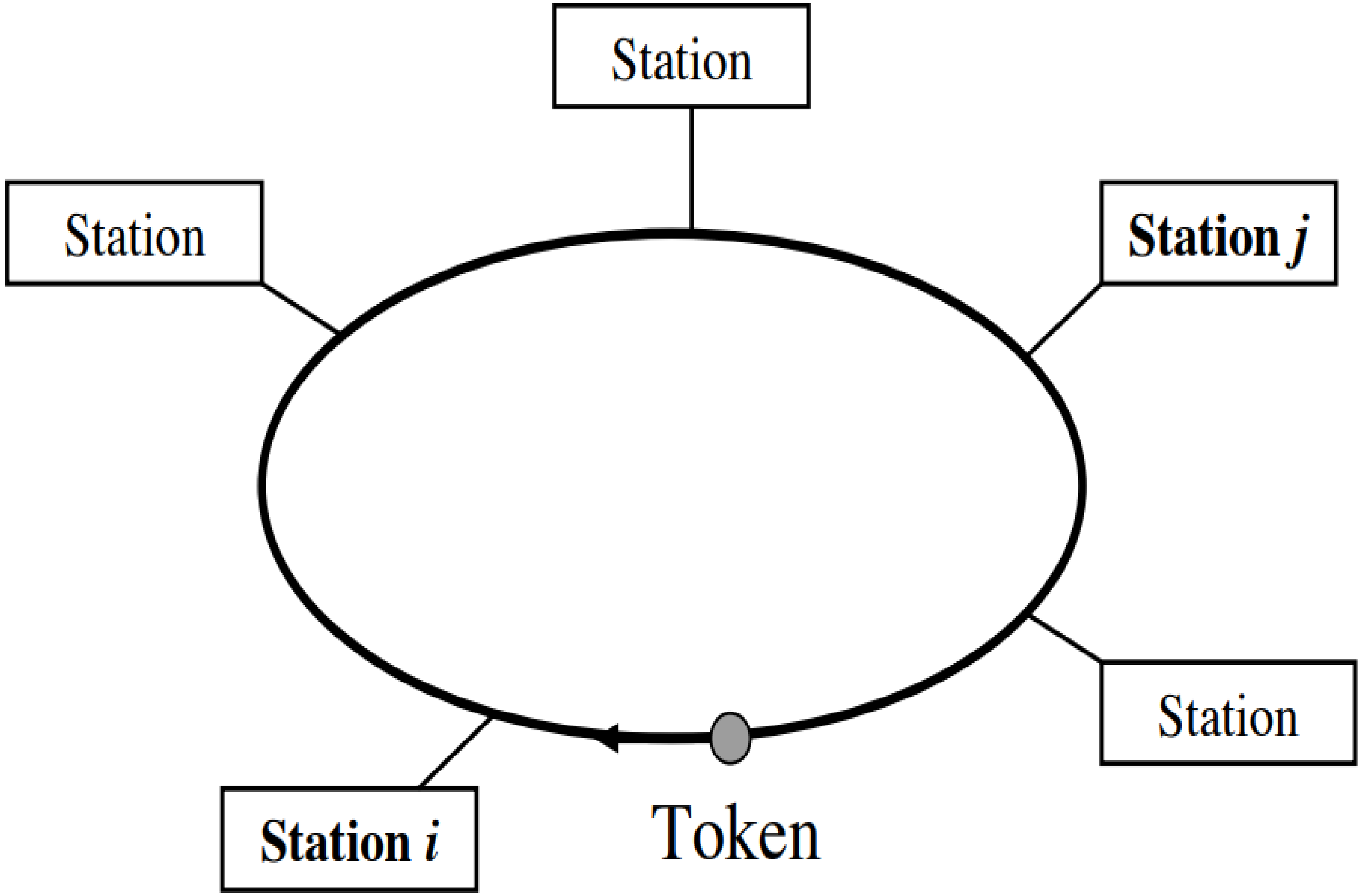
Topics discussed in this section:

Reservation
Polling
Token Passing

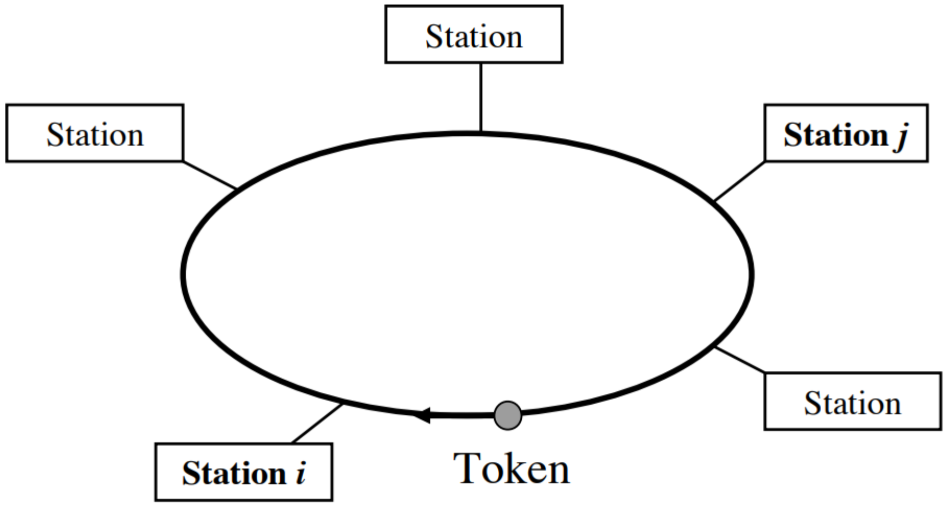
WAIT FOR YOUR TURN

Token-passing is a broadcast-based technology because all stations see every frame. The forwarding of both the token and data frames is performed by NICs in hardware.

A token circulates among all stations. The token is a miniature, 3-byte frame (including start and end flags)

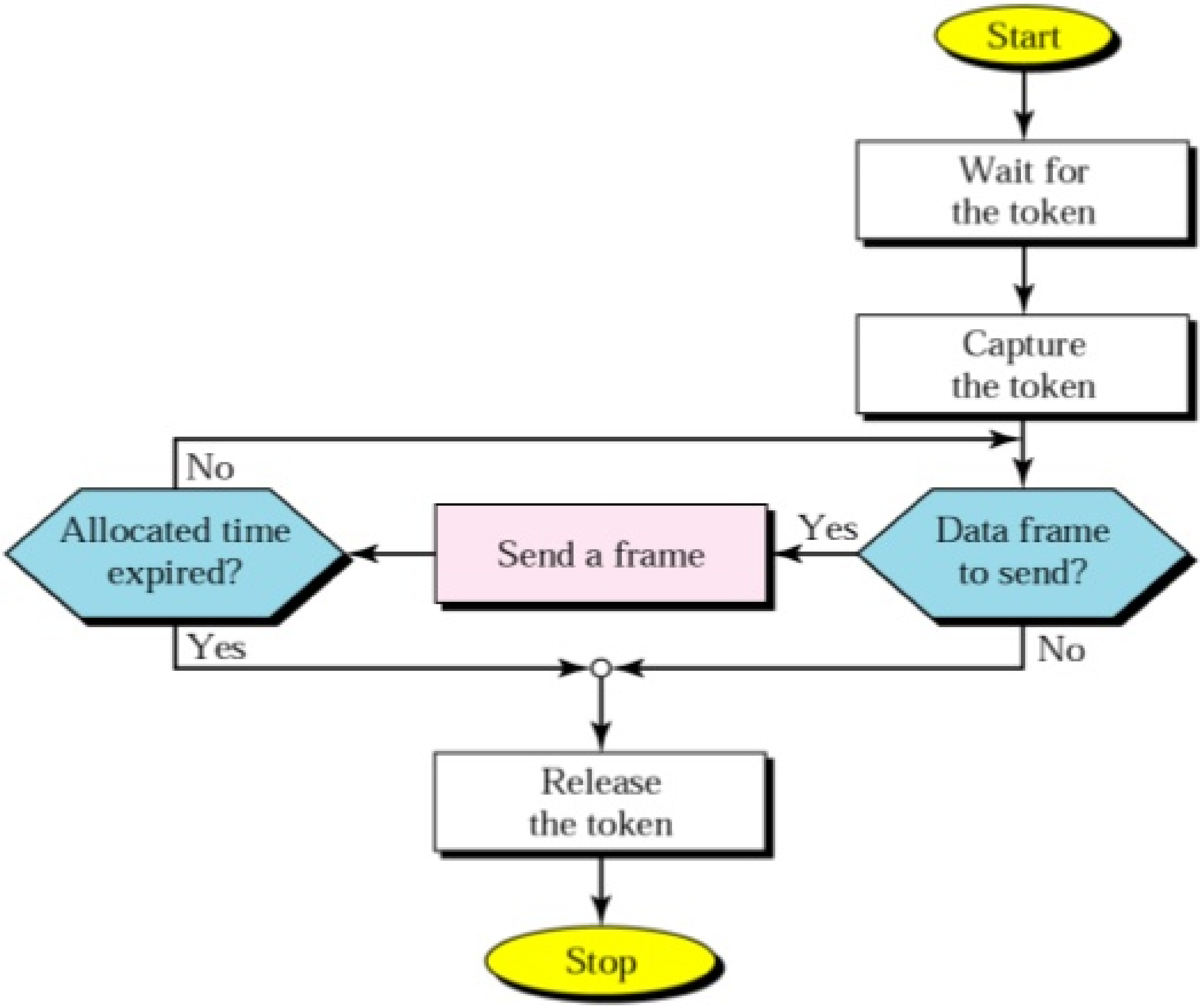


TOKEN-PASSING



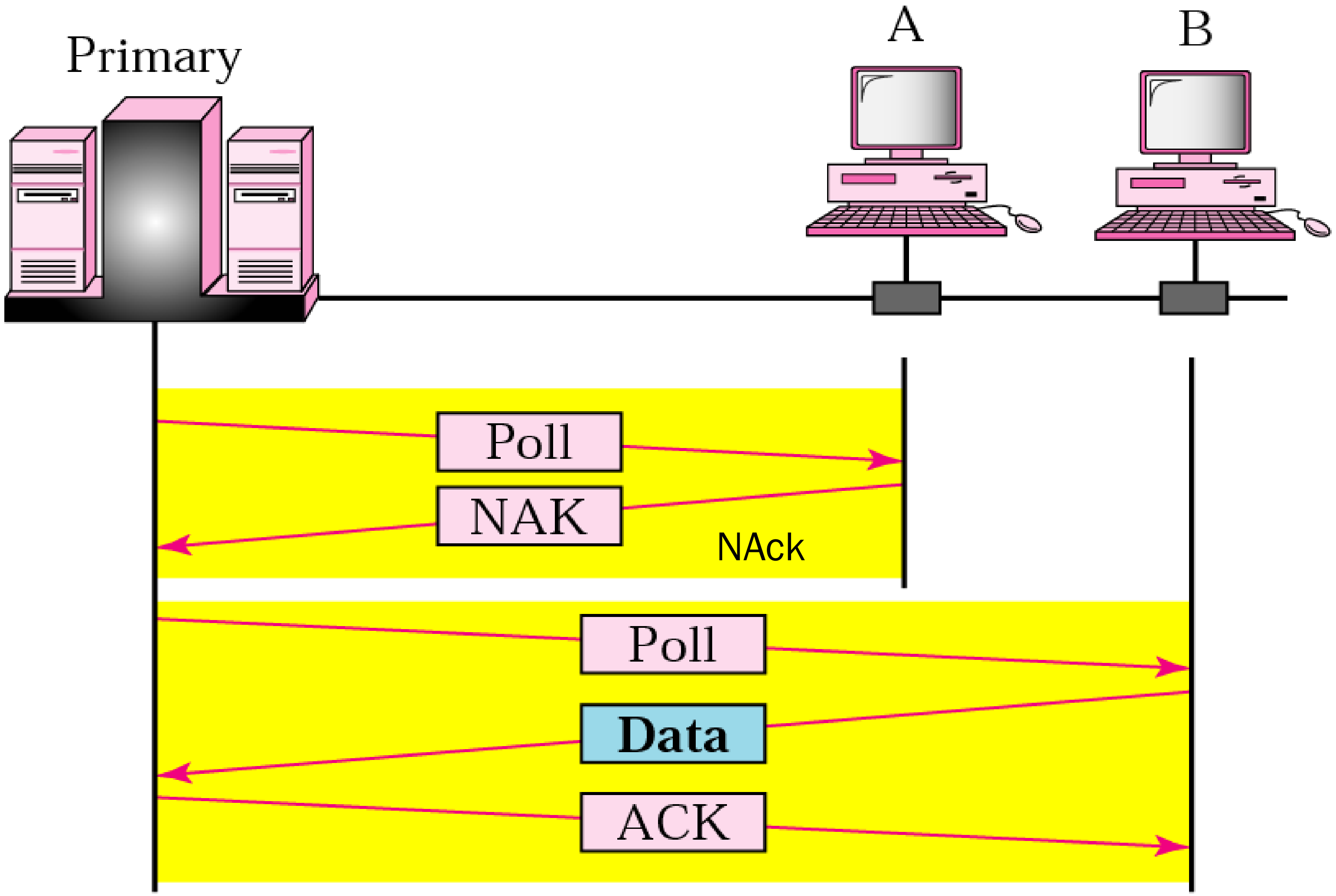
- When the token arrives, a station either seizes the token and sends a frame or passes the token to the next station. Assuming that station i has a frame f to send to station j.
- 1. Station i waits for the arrival of the token and seizes the token
- 2. Station i sends f to station i+1, which in turns passes f to station i+2
- 3. When frame f arrives at station j, station j picks up f and simultaneously forwards f to station j+1
- 4. Eventually, f returns to station i, which passes the token, rather than f, to station i+1 Computer Networks - Introduction / Data Link

Token Passing Flow Chart :



Polling

Whenever the primary station wants to receive the data, it asks the secondary stations present in its channel, this method is polling. In the first diagram, we see that primary station asks station A if it has any data ready for transmission, since A does not have any data queued for transmission it sends NAK (negative acknowledgement), and then it asks station B, since B has data ready for transmission, so it transmits the data and in return receives acknowledgement from primary station.



RESERVATION

- Whenever we travel from a train or an airplane, the first thing we do is to reserve our seats, similarly here a station must make a reservation first before transmitting any data-frames.
- This reservation timeline consists of two kinds of periods:

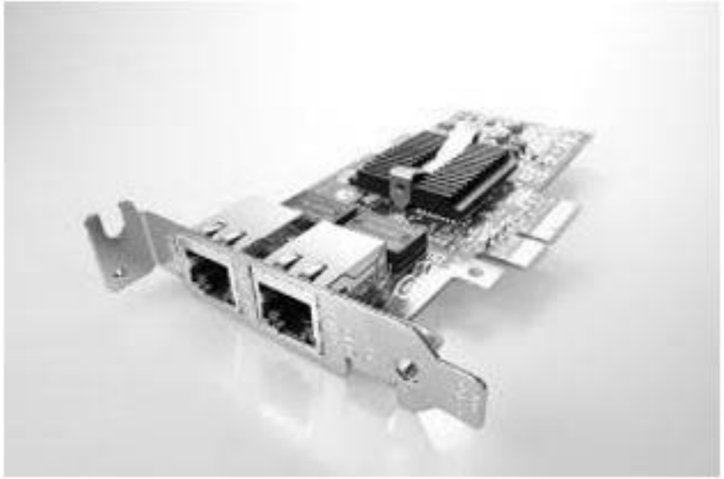
1. Reservation interval of a fixed time duration
2. Data transmission period of variable frames

ETHERNET »

- Ethernet is a family of computer networking technologies commonly used in LANs and MANs.
- » Ethernet was developed at Xerox PARC between 1973 and 1974. It was inspired by ALOHAnet.
- » It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3.

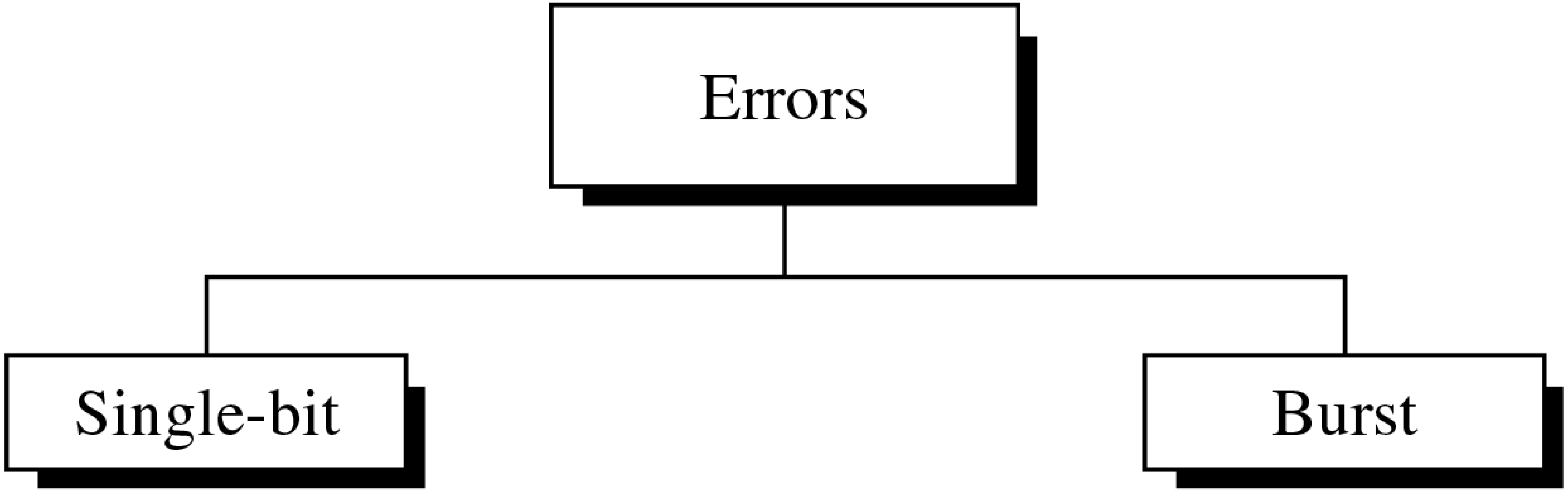
ETHERNET NIC

- Ethernet NIC card is a slot for a cable where we have to plug one end of the ethernet cable into the slots of the computer and another end of the cable is plugged into the modem, likewise, various devices are connected to make a communication set up between them.



- Wireless network NIC cards consist of a small antenna integrated onto the card, where the communication between various devices is set up wirelessly using the router and various network protocols. One such example of a wireless network NIC card is **fiber data digital interface** FDDI.

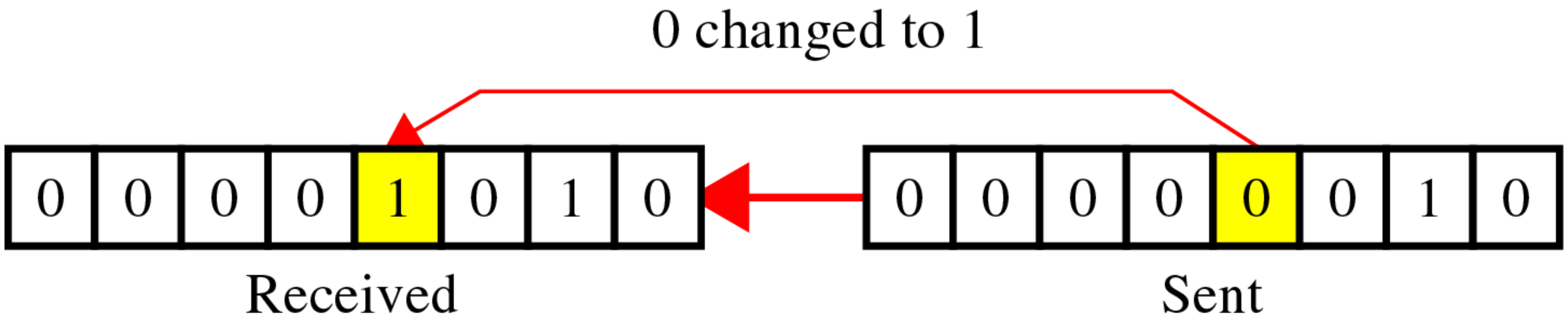
TYPE OF ERRORS



TYPE OF ERRORS(CONT'D)

- **Single-Bit Error**

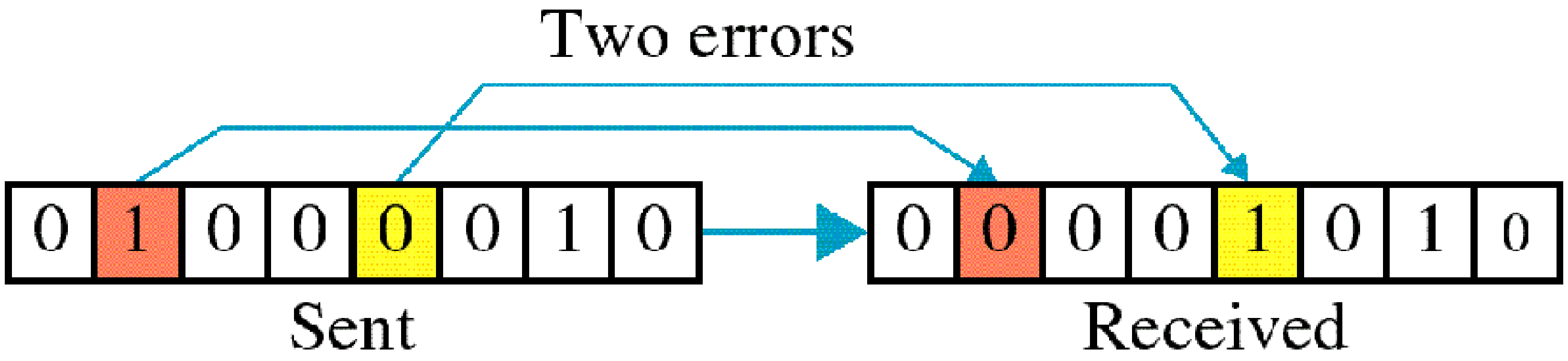
~ is when only one bit in the data unit has changed (ex : ASCII STX - ASCII LF)



TYPE OF ERRORS(CONT’D)

- Multiple-Bit Error

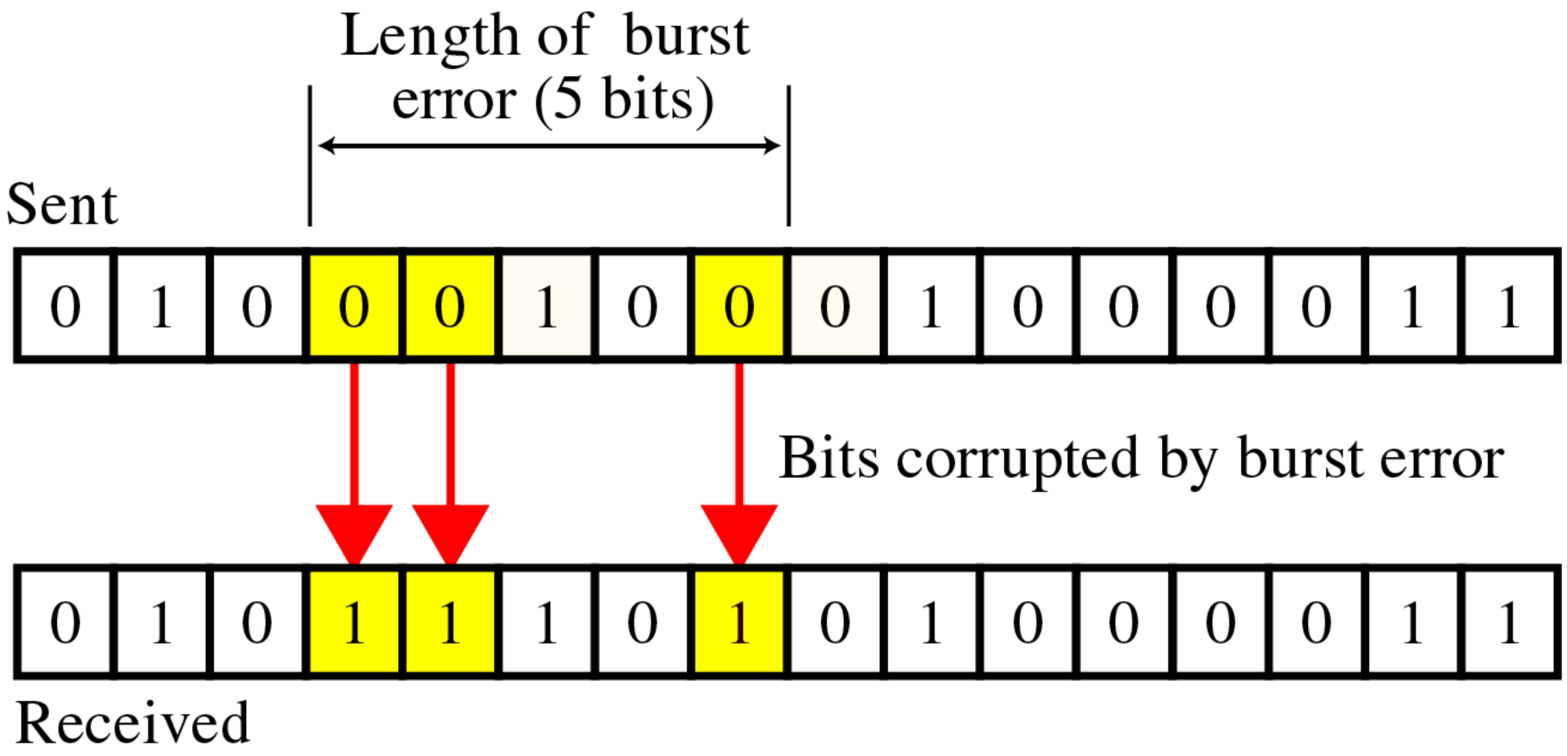
~ is when two or more nonconsecutive bits in the data unit have changed(ex : ASCII B - ASCII LF)



TYPE OF ERRORS(CONT'D)

- **Burst Error**

~ means that 2 or more consecutive bits in the data unit have changed



Length of burst error (5 bits)

Sent	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
Received	0	1	0	1	1	1	0	1	0	1	0	0	0	0	1	1

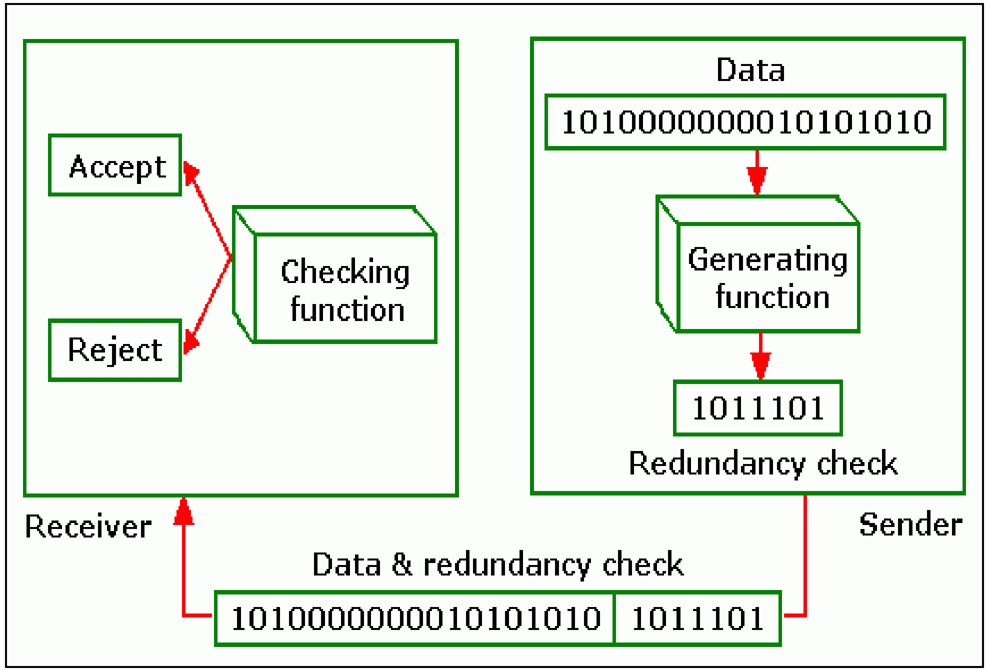
Bits corrupted by burst error

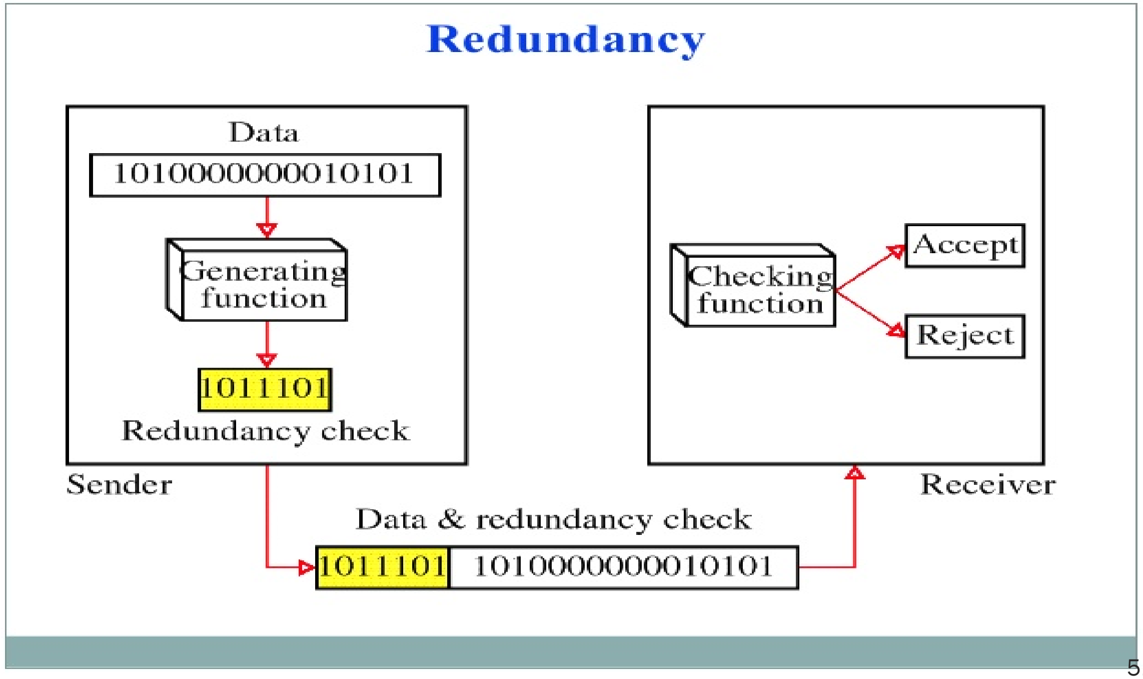
DETECTION

- Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination

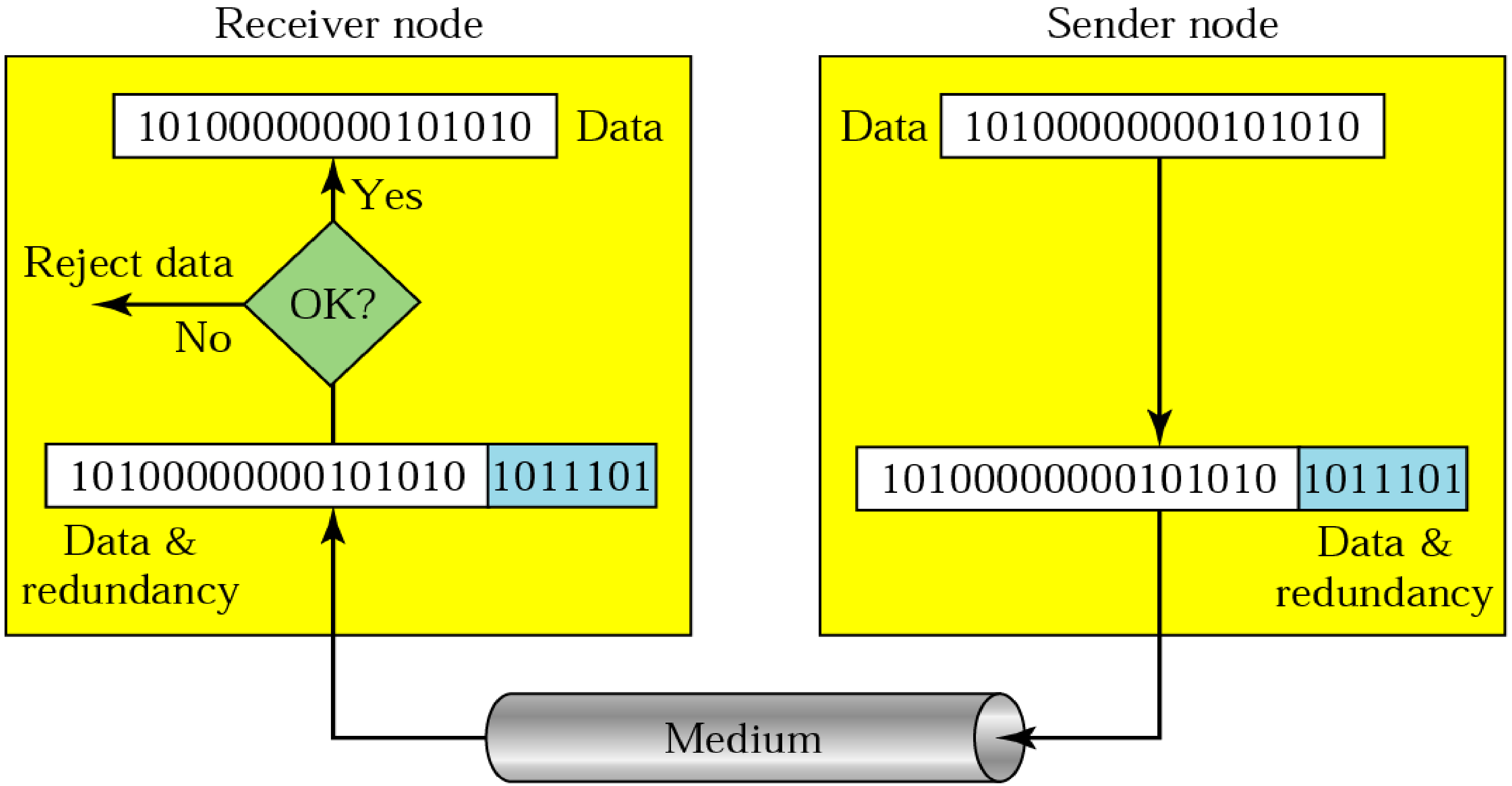
REDUNDANCY

To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver.



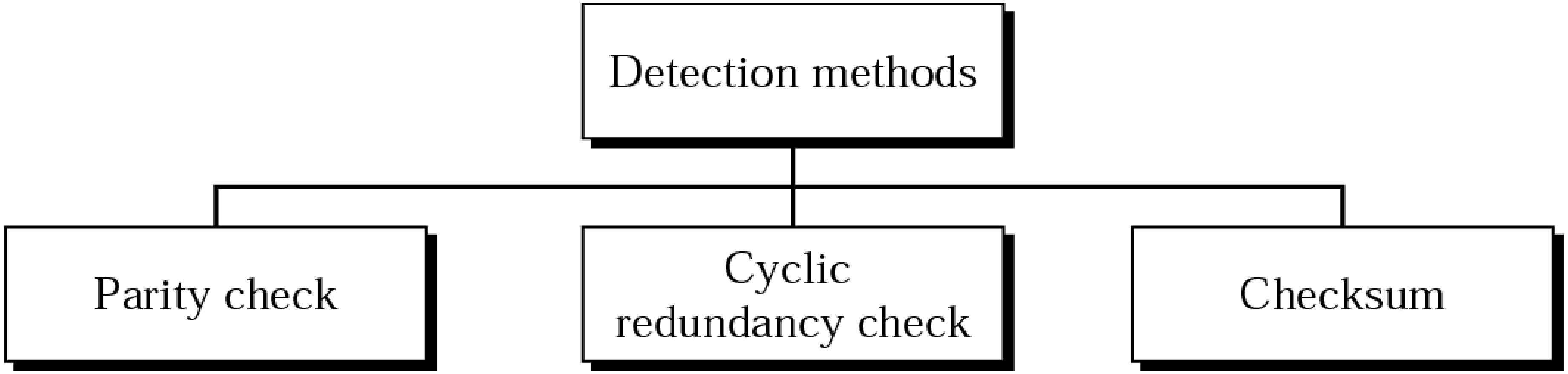


DETECTION(CONT’D)



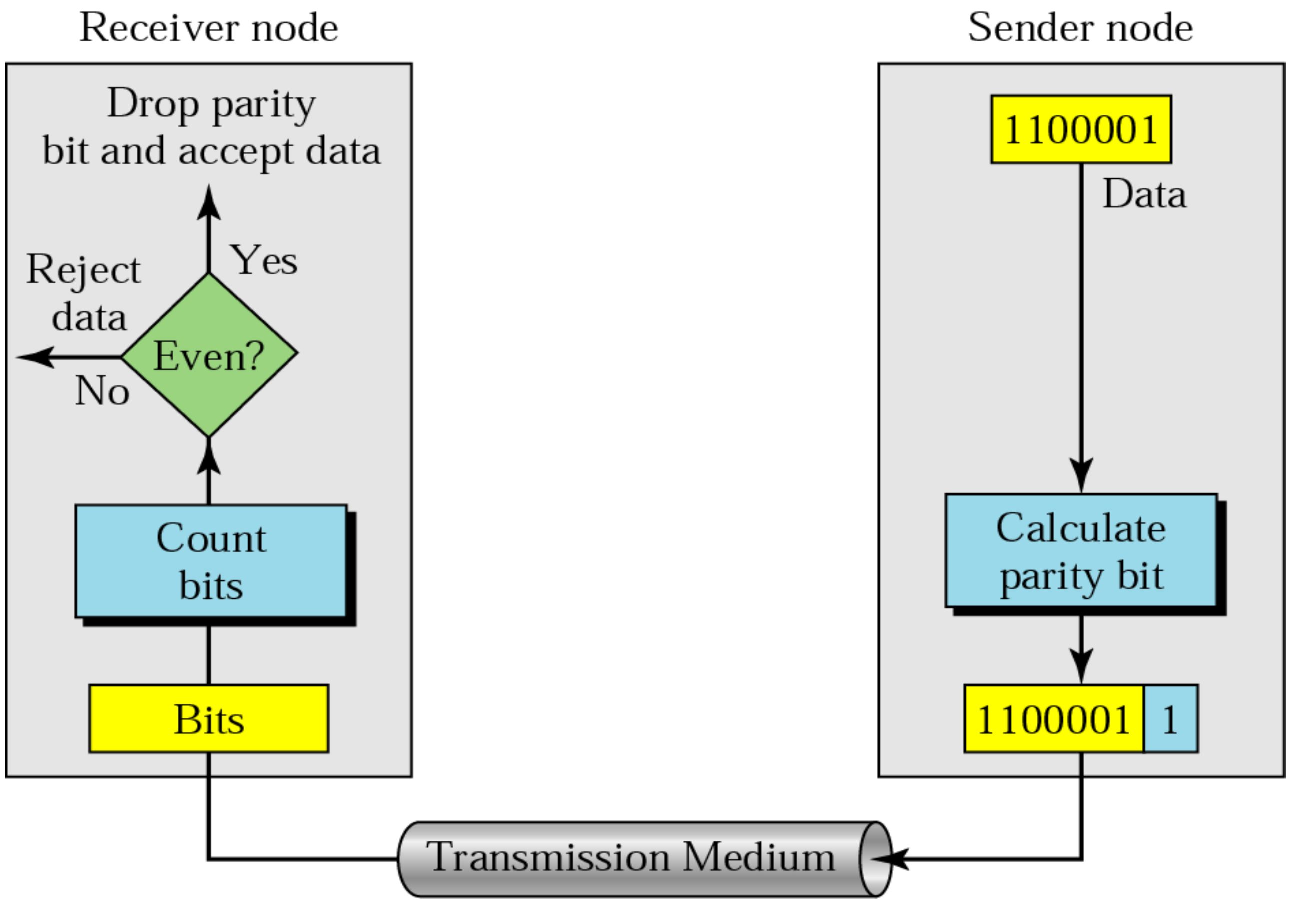
DETECTION(CONT’D)

- Detection methods



DETECTION(CONT'D)

- Parity Check
  - A parity bit is added to every data unit so that the total number of 1s(including the parity bit) becomes even for even-parity check or odd for odd-parity check
  - Simple parity check



DETECTION -EXAMPLES

Suppose the sender wants to send the word *world*. In ASCII the five characters are coded as

1110111 1101111 1110010 1101100 1100100

The following shows the actual bits sent

1110111**0** 1101111**0** 1110010**0** 1101100**0** 1100100**1**

DETECTION – EXAMPLES

Now suppose the word world in Example 1 is received by the receiver without being corrupted in transmission.

11101110 11011110 11100100 11011000 11001001

The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

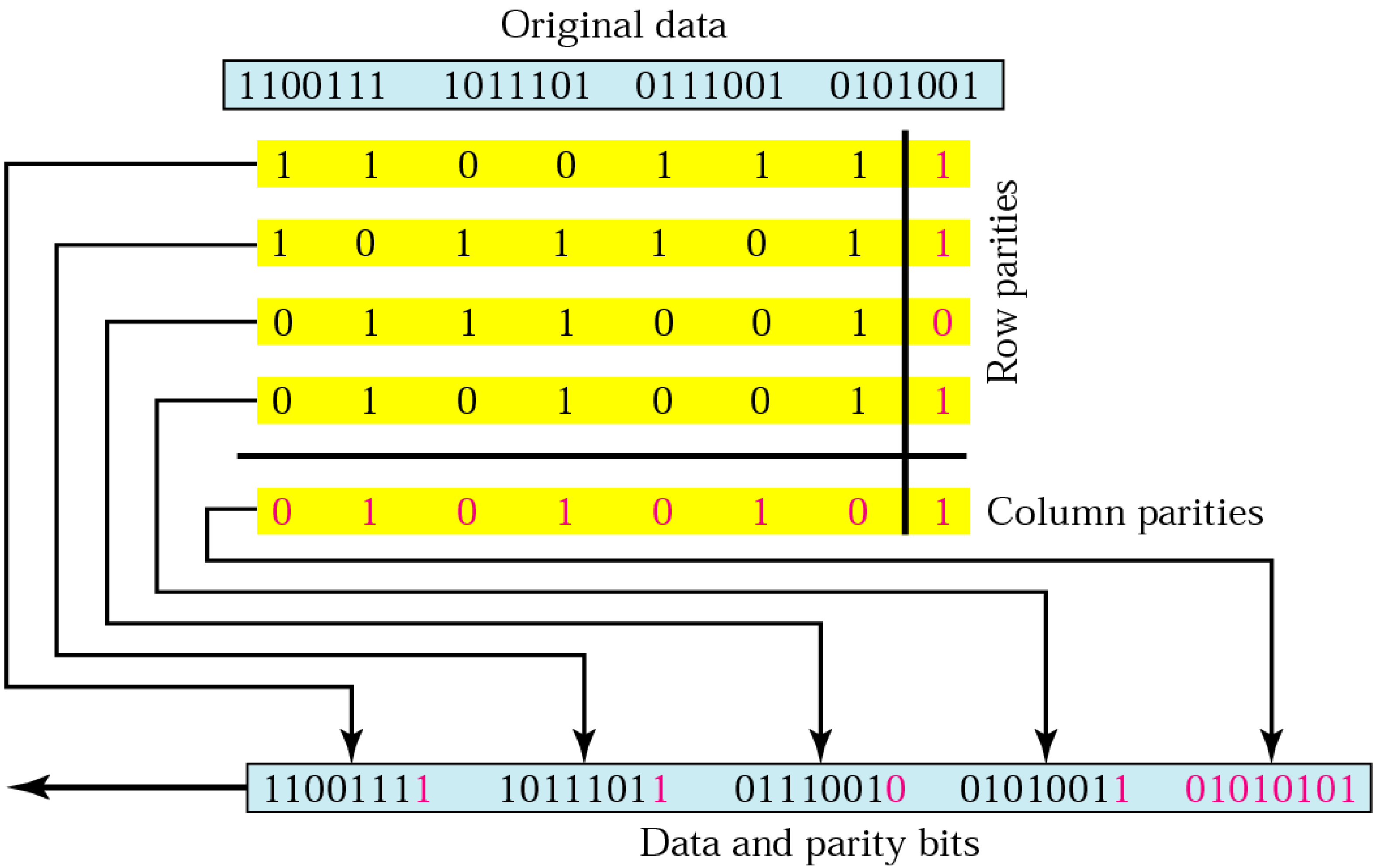
DETECTION – EXAMPLES

Now suppose the word world in Example 1 is corrupted during transmission.

11111110 11011110 11101100 11011000 11001001

The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

TWO –DIMENSIONAL PARITY CHECK



Original data

1100111 1011101 0111001 0101001

1	1	0	0	1	1	1	1	Row parities
1	0	1	1	1	0	1	1	
0	1	1	1	0	0	1	0	
0	1	0	1	0	0	1	1	
0	1	0	1	0	1	0	1	Column parities

11001111 10111011 01110010 01010011 01010101

Data and parity bits

DETECTION - EXAMPLE

Suppose the following block is sent:

10101001 00111001 11011101 11100111 10101010

However, it is hit by a burst noise of length 8, and some bits are corrupted.

1010**0011** **1000**1001 11011101 11100111 10101010

When the receiver checks the parity bits, some of the bits do not follow the even-parity rule and the whole block is discarded.

10100011 10001001 11011101 11100111 **1**0**101**0**1**0

CHECKSUM

~ used by the higher layer protocols

~ is based on the concept of redundancy(VRC, LRC, CRC ....)

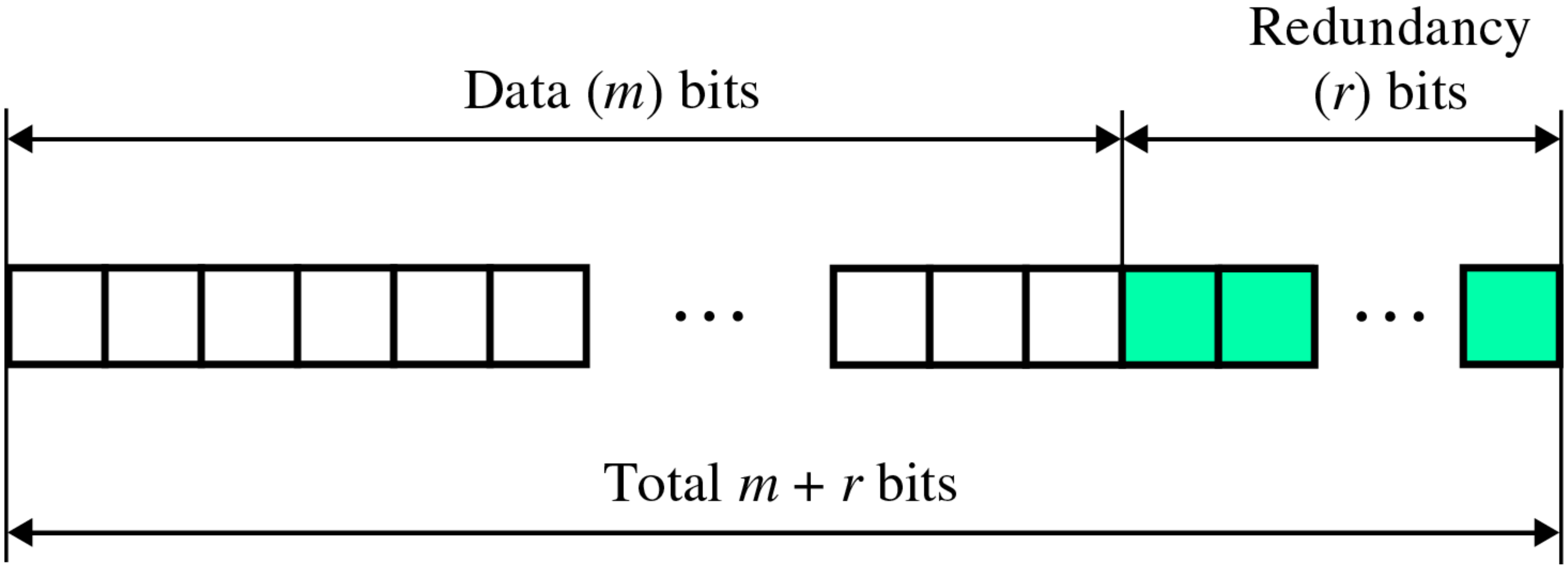
ERROR CORRECTION(CONT’D)

- Single-Bit Error Correction
  - parity bit
  - The secret of error correction is to locate the invalid bit or bits
  - For ASCII code, it needs a three-bit redundancy code(000-111)

ERROR CORRECTION(CONT'D)

- Redundancy Bits

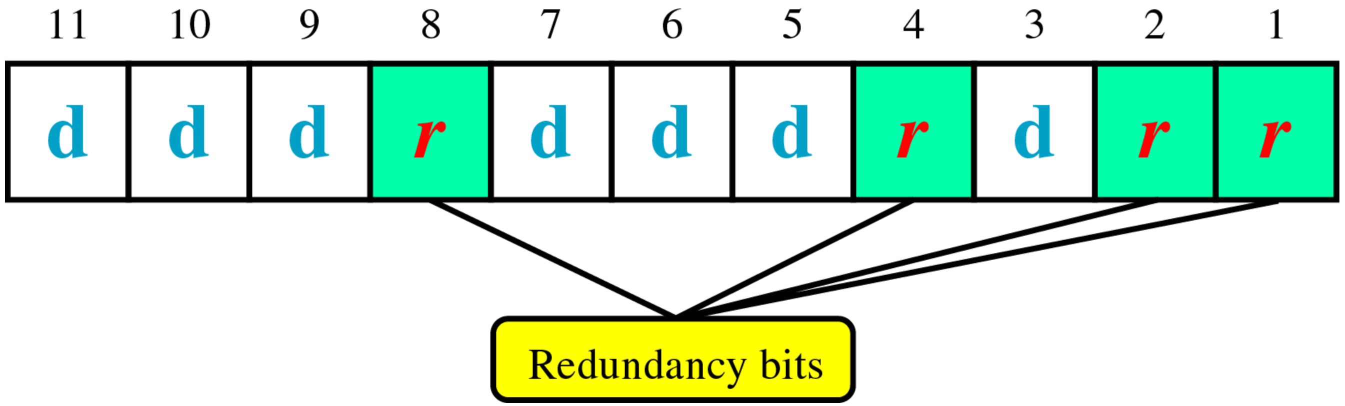
~ to calculate the number of redundancy bits (R) required to correct a given number of data bit (M)



HAMMING CODE

~ developed by R.W.Hamming

- positions of redundancy bits in Hamming code



11	10	9	8	7	6	5	4	3	2	1
d	d	d	*r*	d	d	d	*r*	d	*r*	*r*

Redundancy bits

HAMMING CODE

- each r bit is the VRC bit for one combination of data bits

r_1 = bits 1, 3, 5, 7, 9, 11

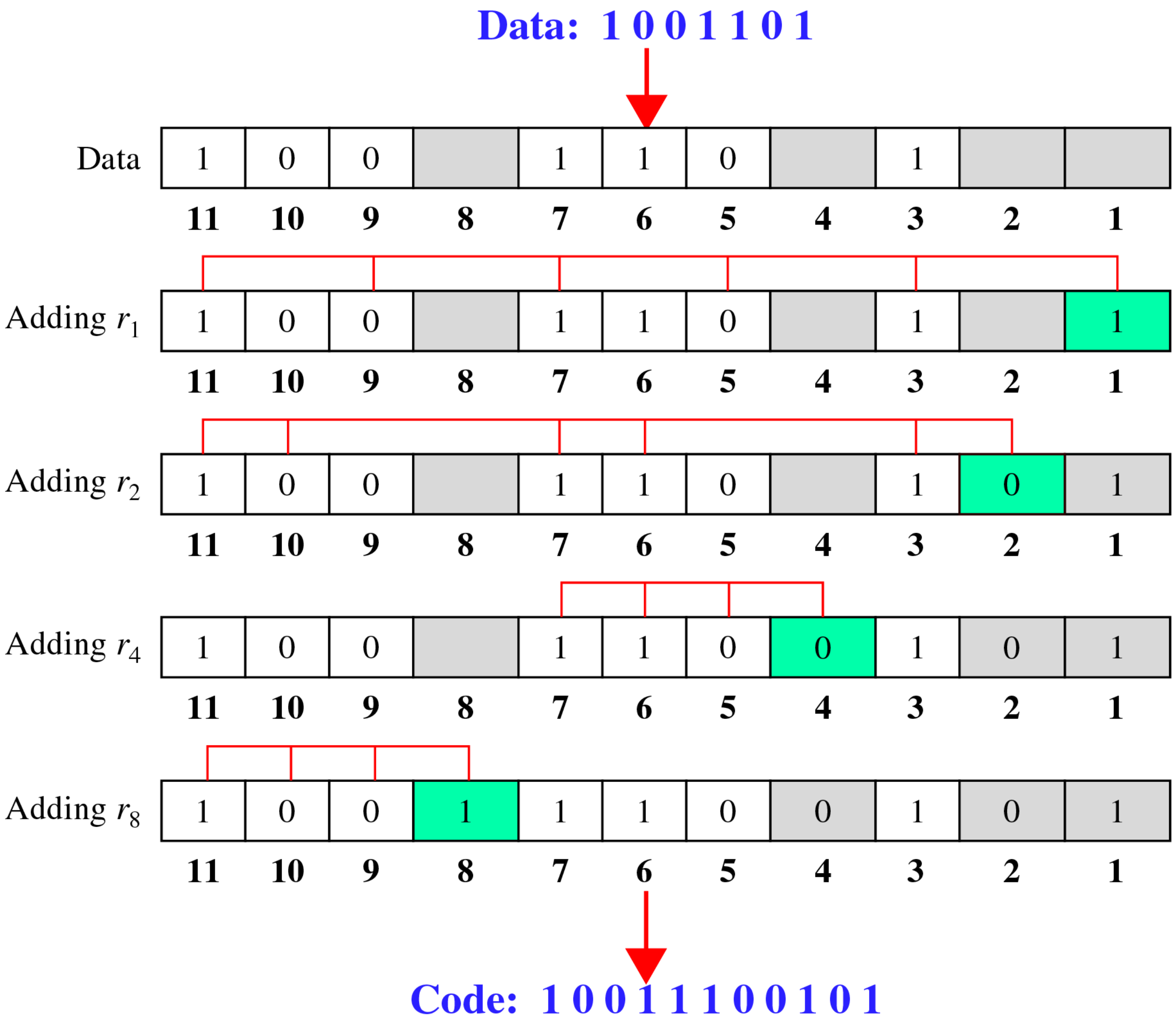
r_2 = bits 2, 3, 6, 7, 10, 11

r_4 = bits 4, 5, 6, 7

r_8 = bits 8, 9, 10, 11

HAMMING CODE (CONT'D)

- Calculating the r values



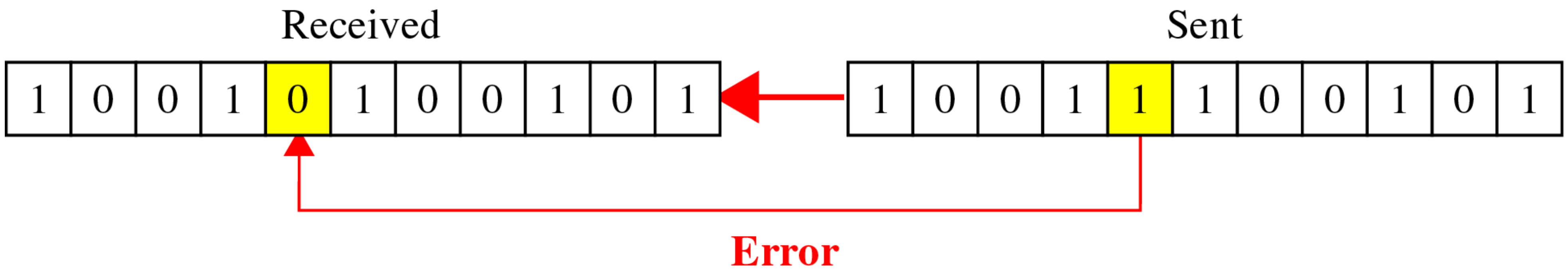
Data: 1 0 0 1 1 0 1

	11	10	9	8	7	6	5	4	3	2	1
Data	1	0	0		1	1	0		1		
Adding r_1	1	0	0		1	1	0		1		1
Adding r_2	1	0	0		1	1	0		1	0	1
Adding r_4	1	0	0		1	1	0	0	1	0	1
Adding r_8	1	0	0	1	1	1	0	0	1	0	1

Code: 1 0 0 1 1 1 0 0 1 0 1

HAMMING CODE (CONT'D)

- Error Detection and Correction



Received

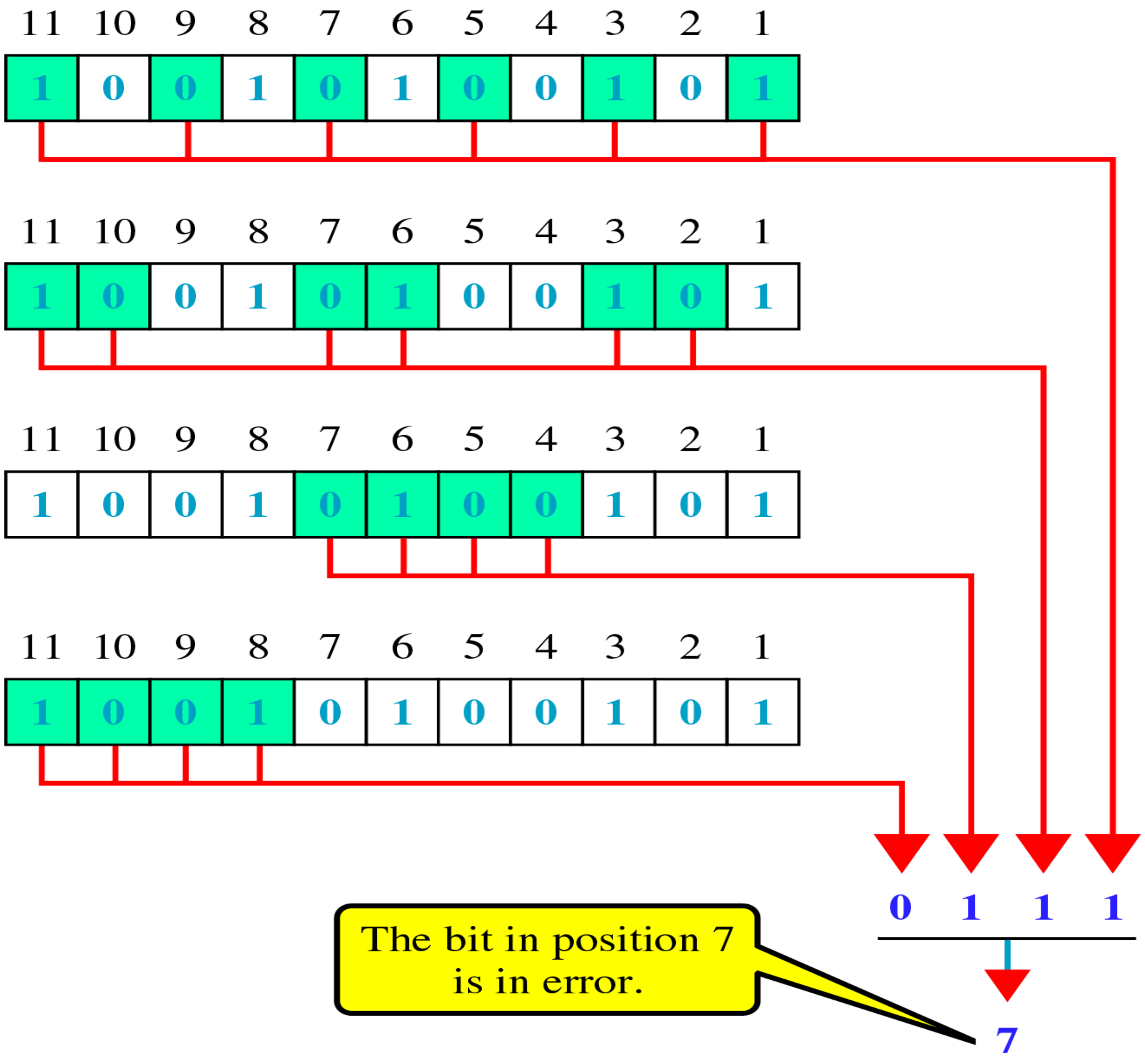
1 0 0 1 0 1 0 0 1 0 1

Sent

1 0 0 1 1 1 0 0 1 0 1

HAMMING CODE (CONT'D)

- Error detection using Hamming Code



11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	0	1	0	0	1	0	1

11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	0	1	0	0	1	0	1

11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	0	1	0	0	1	0	1

11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	0	1	0	0	1	0	1

The bit in position 7 is in error.

REFERENCES

- https://www.net.t-labs.tu-berlin.de/teaching/computer_networking
- https://techterms.in/
- https://github.com/HanochShi/Supplements-ComputerNetworking-ATopDownApproach-7th-ed
- https://www.youtube.com/channel/UCJQJ4GjTiq5lmn8czf8oo0Q
- http://www.whatis.com
- http://www.webopedia.com
- Understanding Data Communications & Networks, Shay (1999)
- http://www.daemon.org/ip.html

READING INSTRUCTIONS

- # Reading instructions
- Ch. 6-11