Medium access control sublayer(CO2)

Topic objective

- Understand the Medium access sub layer of data link layer
- Understand the Functions of MAC
- Find out Channel allocation problem and
- Various multiple access protocols

Medium access control sublayer(CO2)

- It is responsible for flow control and multiplexing for transmission medium.

- The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems.

- The data link layer is divided into two sublayers −
  - The logical link control (LLC) sublayer
  - The medium access control (MAC) sublayer

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC

- MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device.
- It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.
- This layer determines who goes next on a multi-access channel
- MAC protocols are mechanisms that allow users to access a common medium or channel.
- Aloha, slotted Aloha, and Carrier Sense Multiple Access protocols are used
- This layer is important in LAN's
- Channel allocation problem
  - Static channel
  - Dynamic channel allocation

Static channel Allocation(CO5)

- For fixed channel and traffic from N users
- Divide up bandwidth using FDM, TDM, CDMA, etc. − FDM and TDM
- problematic with large no. of senders or bursty traffic
- This static allocation performs poorly for bursty traffic
  - Most data transmissions are inherently bursty
  - Allocation to any given user will sometimes go unused = wasteful

Dynamic channel Allocation(CO5)

- Dynamic allocation gives the channel to a user when they need it.
- Potentially N times as efficient for N users.

Various schemes

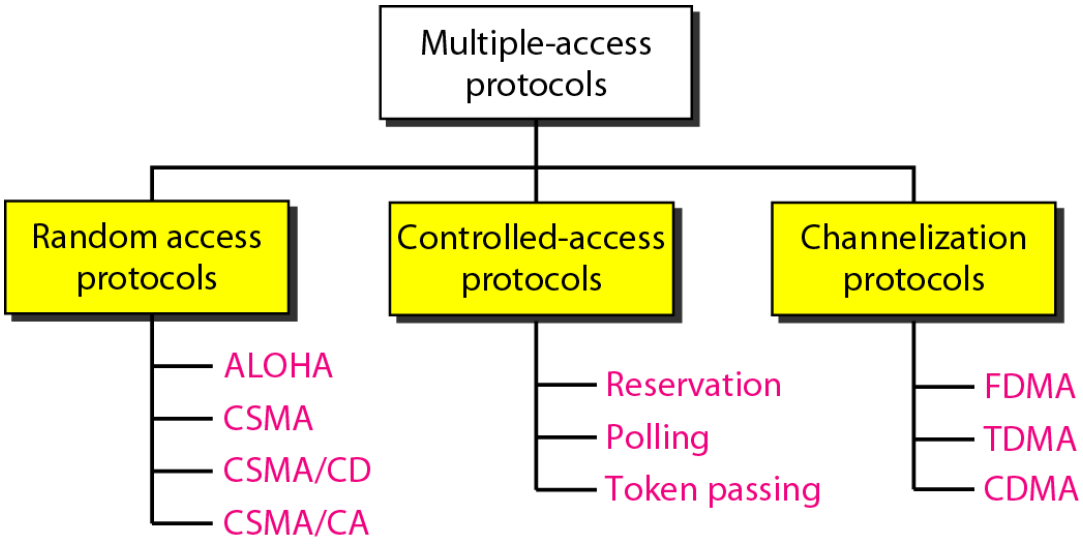
• Independent traffic analysis	Often not a good model, but permits
• Single channel	No external way to coordinate senders
• Observable collisions	Needed for reliability; mechanisms vary
(2+ sending simultaneously)	
• Continuous or	Slotting (time divided up into discrete
slotted time	intervals) may improve
performance	
• Carrier sense available	Can improve performance if
no carrier sense	

Multiple Access Protocols(CO2)

- Two basic strategies for channel acquisition in a broadcast network:

1. Contention (e.g., Aloha, CSMA) – preferable for low load because of its low delay characteristics

2. Collision Free Protocols – preferable at high load

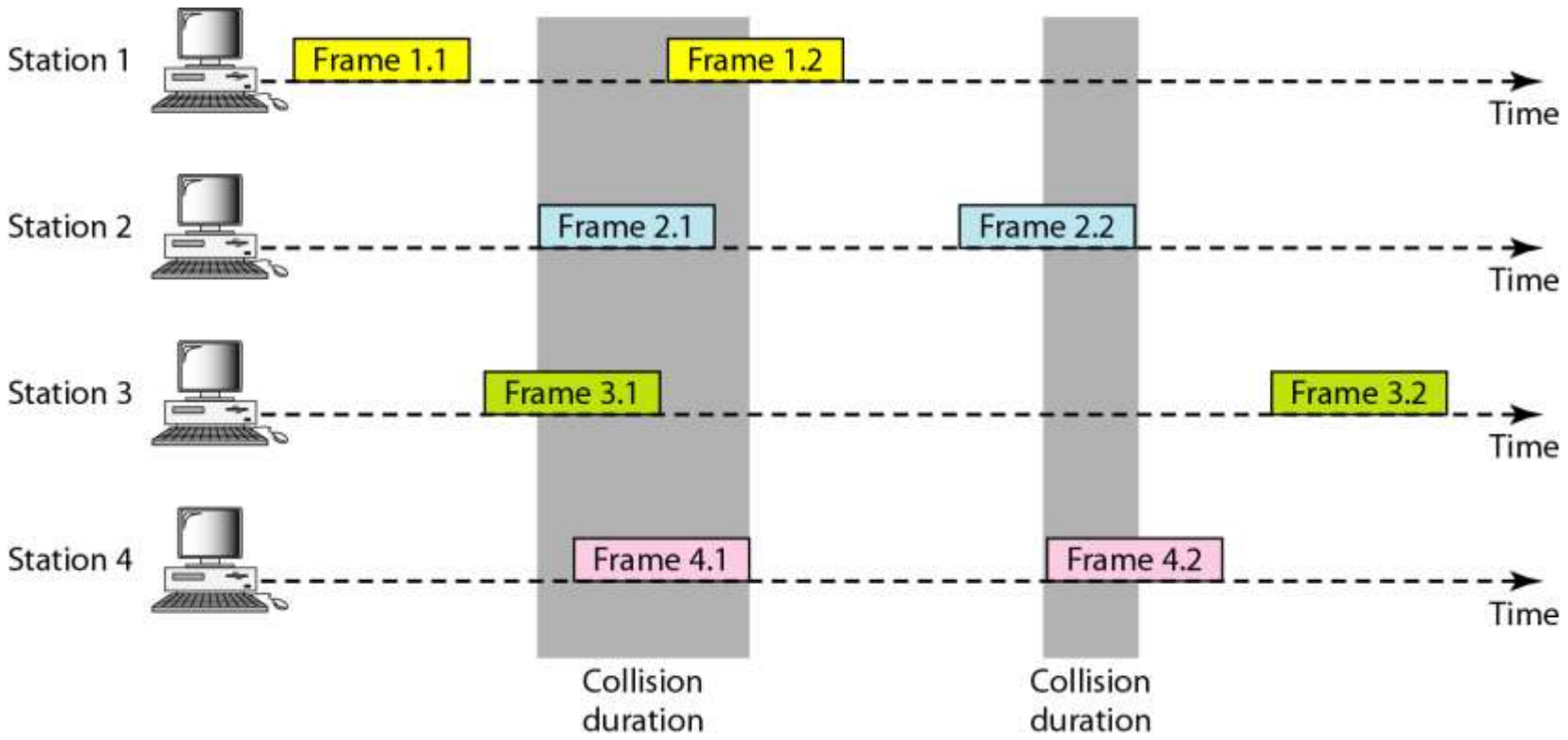


Random access protocols

- 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.

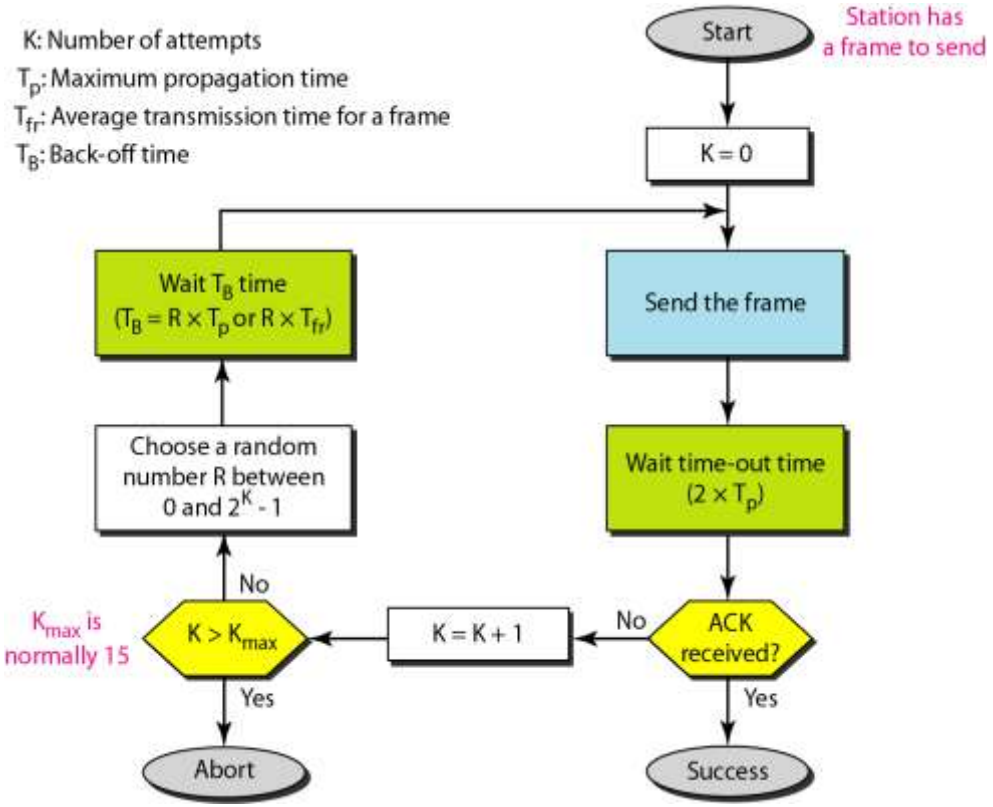
Pure Aloha

Frames are transmitted at completely arbitrary times



Procedure for pure Aloha

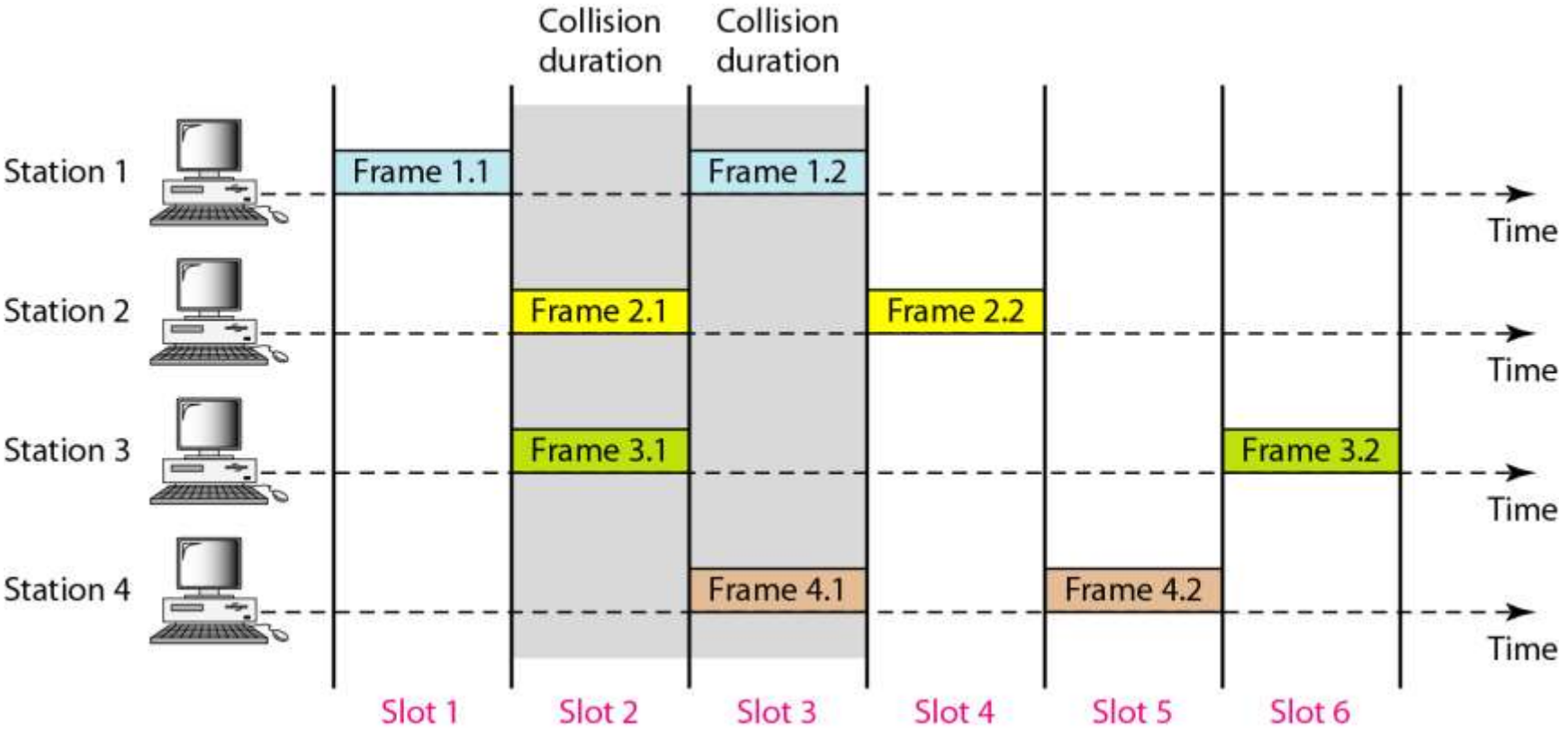
- The throughput for pure ALOHA is $S = G \times e^{-2G}$.
- The maximum throughput
- $S_{max} = 0.184$ when G= (1/2).



Slotted Aloha

- Time in uniform slot equal to frame transmission time
- Need central clock for synchronisation
- Transmission begins at slot boundary
- The throughput for slotted ALOHA is
  $S = G \times e^{-G}$.
- The maximum throughput
  $S_{max} = 0.368$ when G = 1.

Slotted Aloha



CSMA(CO2)

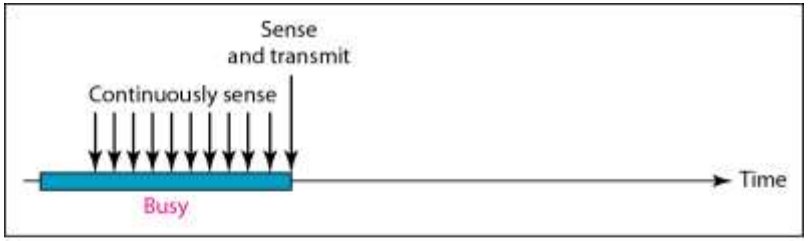
- Carrier Sense Multiple Access (CSMA)

improves on ALOHA by sensing the channel

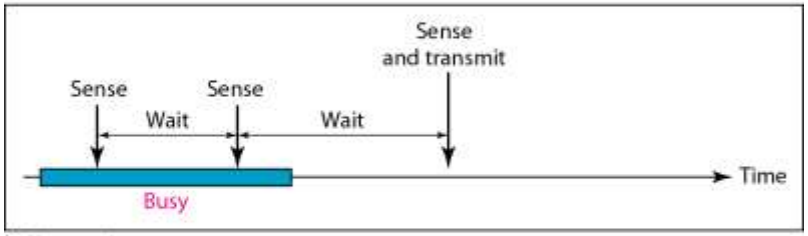
- Variations (within CSMA) on what to do

if the channel is busy:

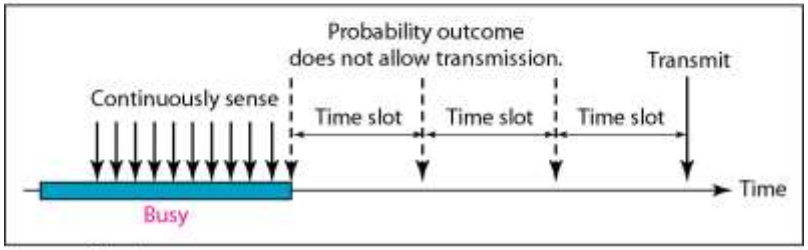
1. 1-persistent
2. Non persistent
3. P-persistent



a. 1-persistent

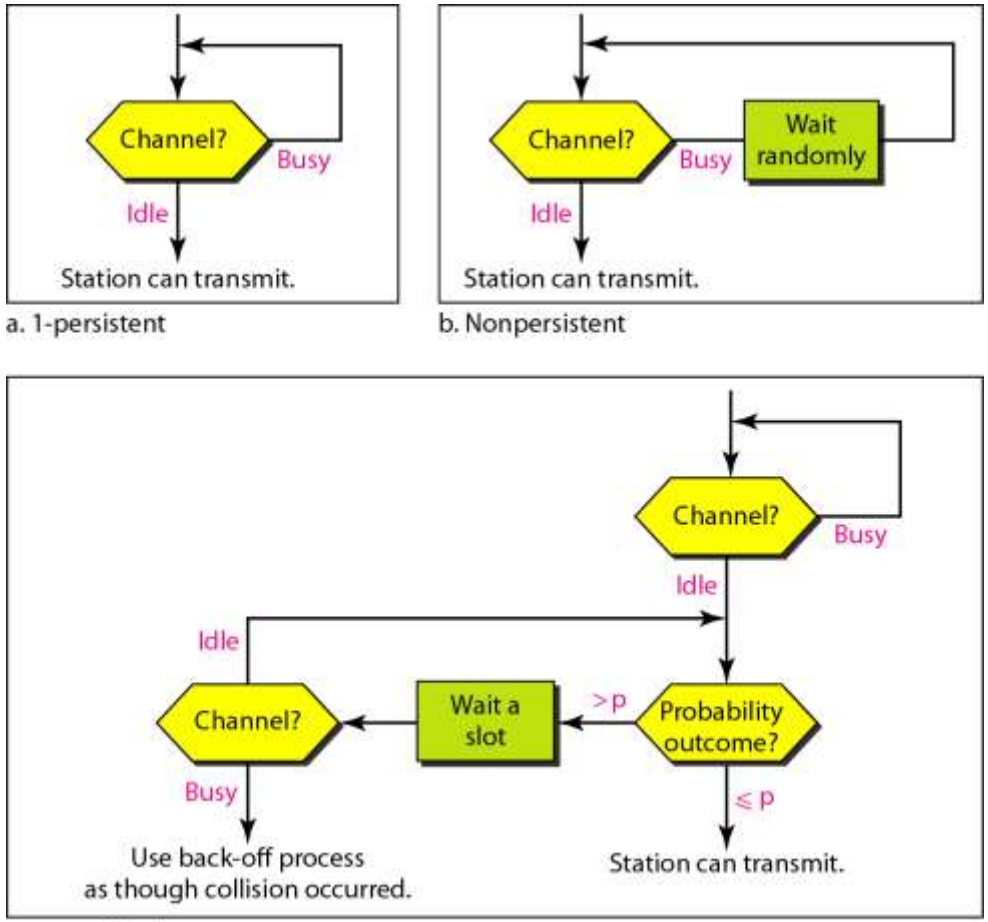


b. Nonpersistent



c. p-persistent

CSMA

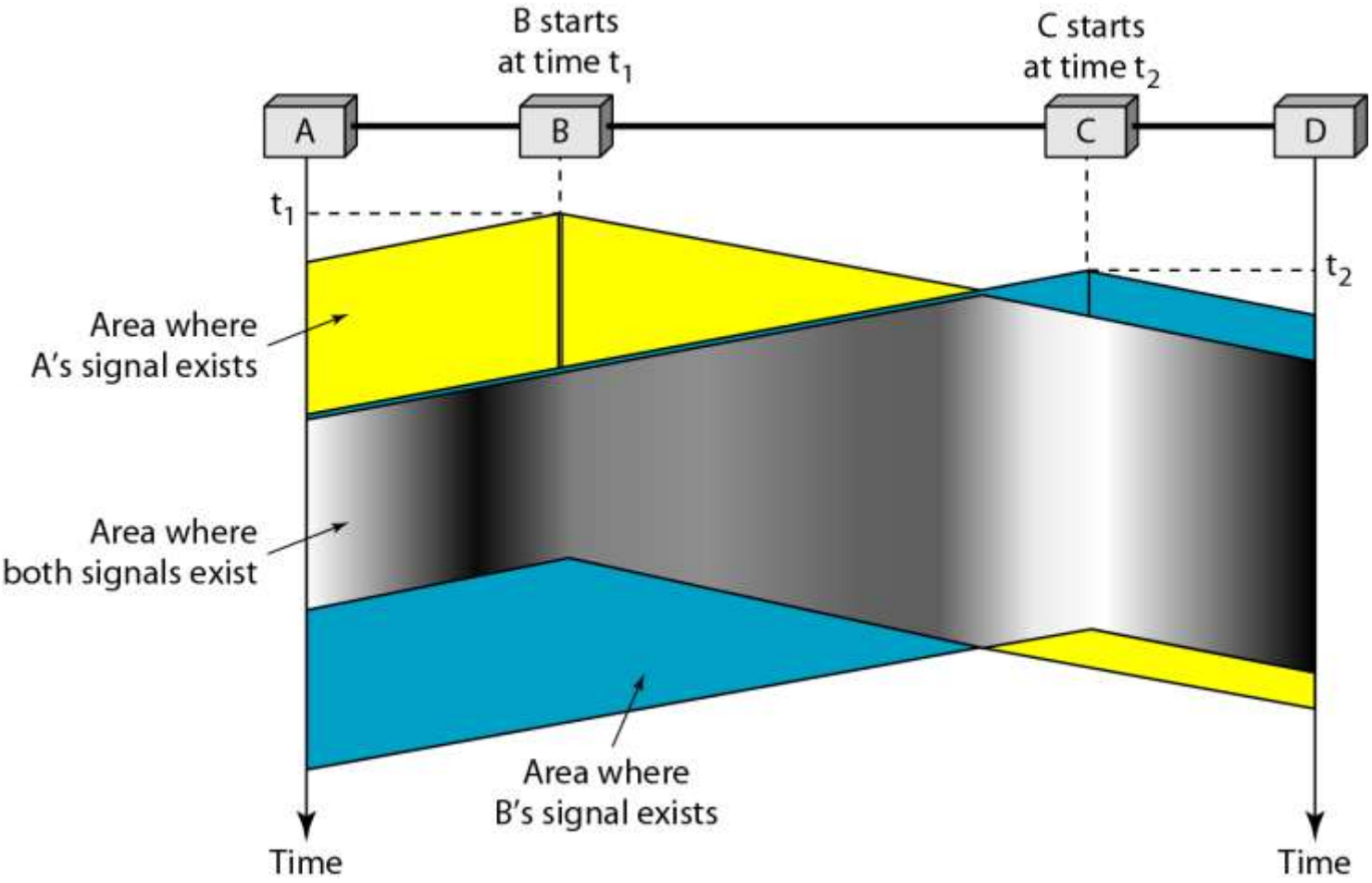


a. 1-persistent

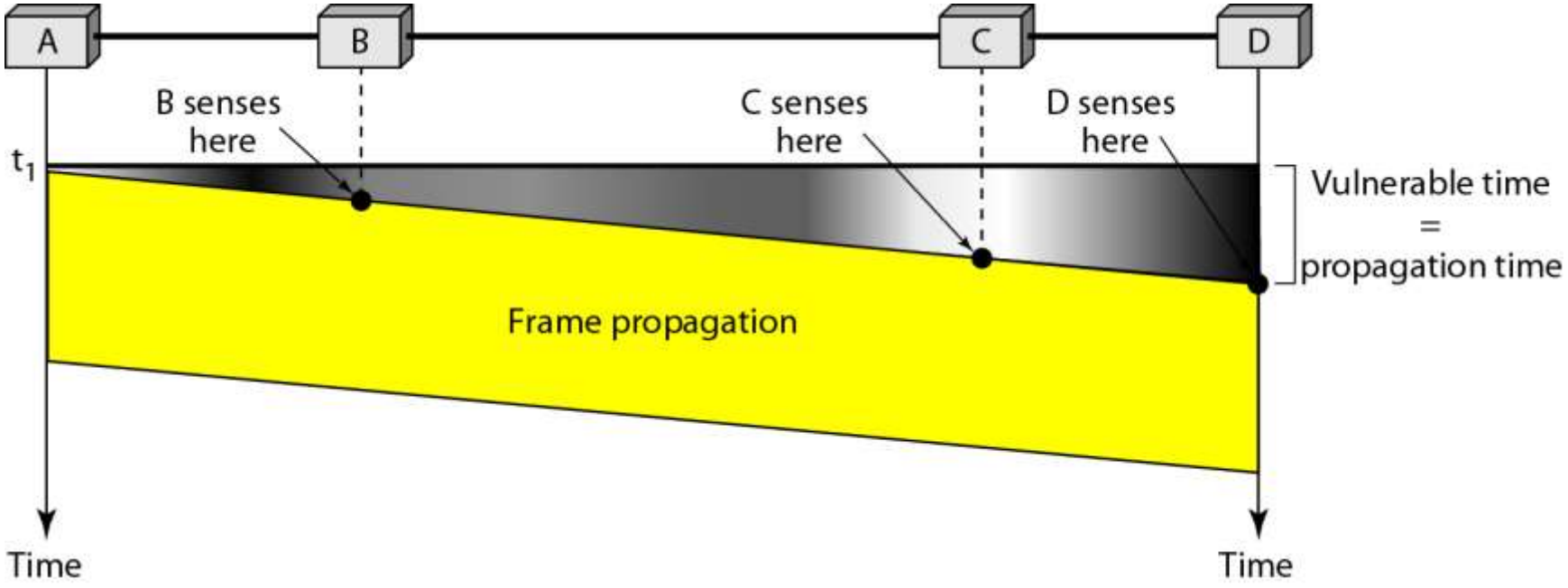
b. Nonpersistent

c. p-persistent

CSMA


B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where A's signal exists
Area where both signals exist
Area where B's signal exists
Time
Time

Vulnerable time in CSMA



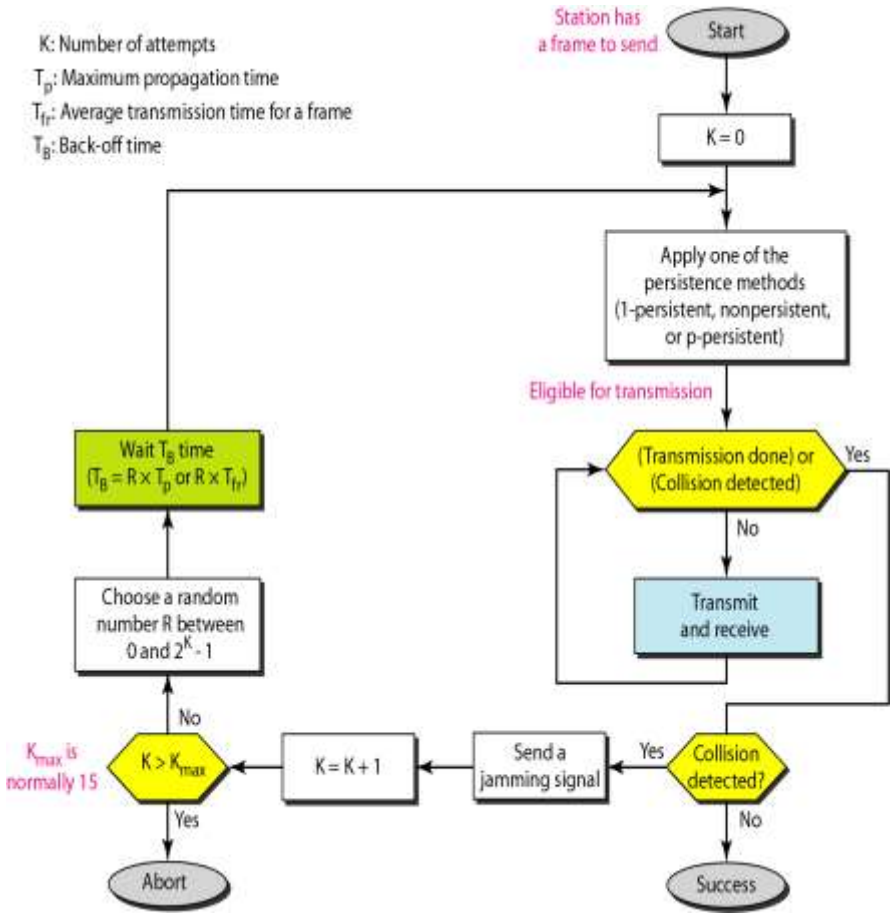
CSMA/CD

Step 1: Check if the sender is ready for transmitting data packets.

Step 2: Check if the transmission link is idle?

Step 3: Transmit the data & check for collisions.

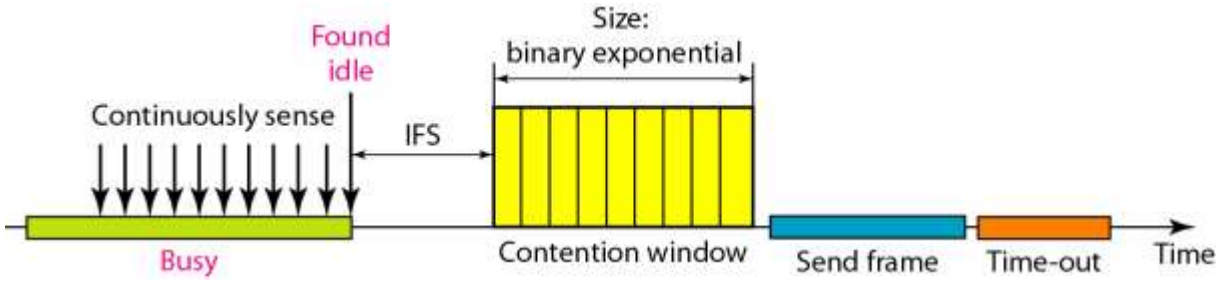
Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

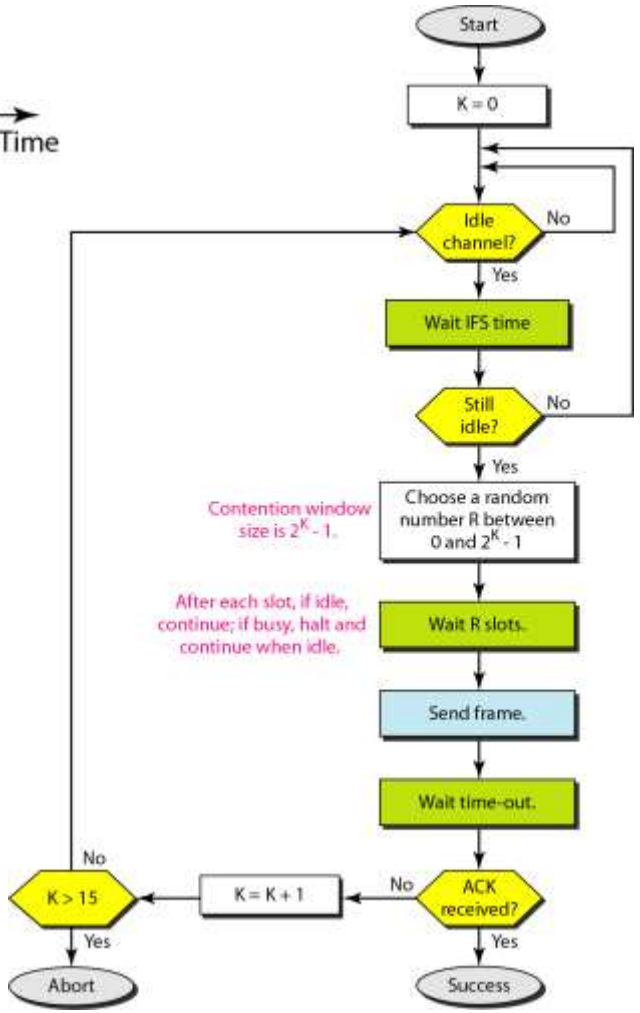


CSMA/CA

- Three type of strategies:
- **InterFrame Space (IFS) –** When a station finds the channel busy, it waits for a period of time called IFS time. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
- **Contention Window –** It is the amount of time divided into slots.A station which is ready to send frames chooses random number of slots as **wait time**.
- **Acknowledgements –** The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

CSMA/CA


Found idle
Size: binary exponential
Continuously sense
IFS
Busy
Contention window
Send frame
Time-out
Time


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.
No
ACK received?
No
K = K + 1
K > 15
Yes
Abort
Yes
Success

Controlled access

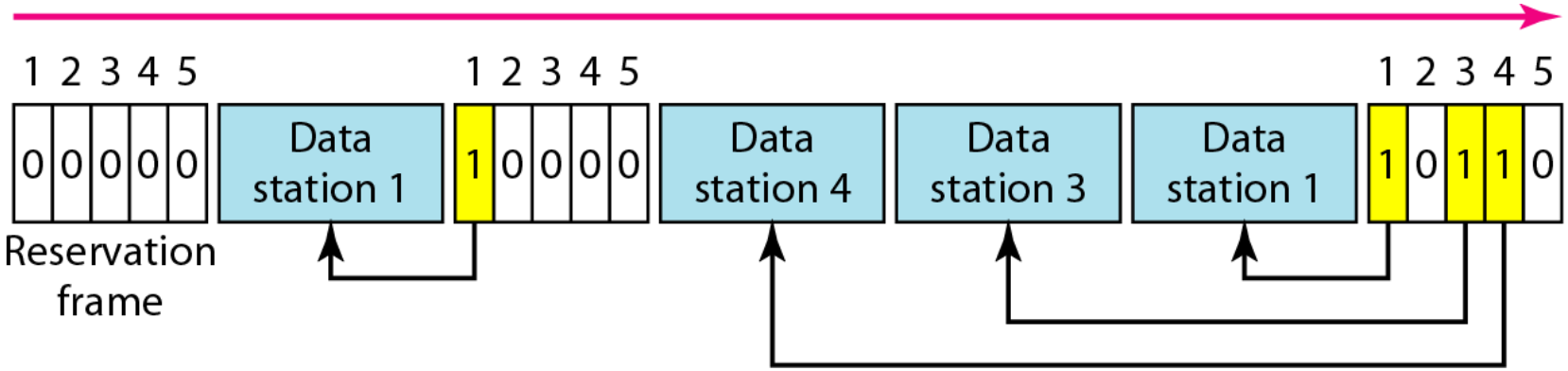
- the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.
- Methods
  - Reservation
  - Polling
  - Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  - Reservation interval of fixed time length
  - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.

Reservation

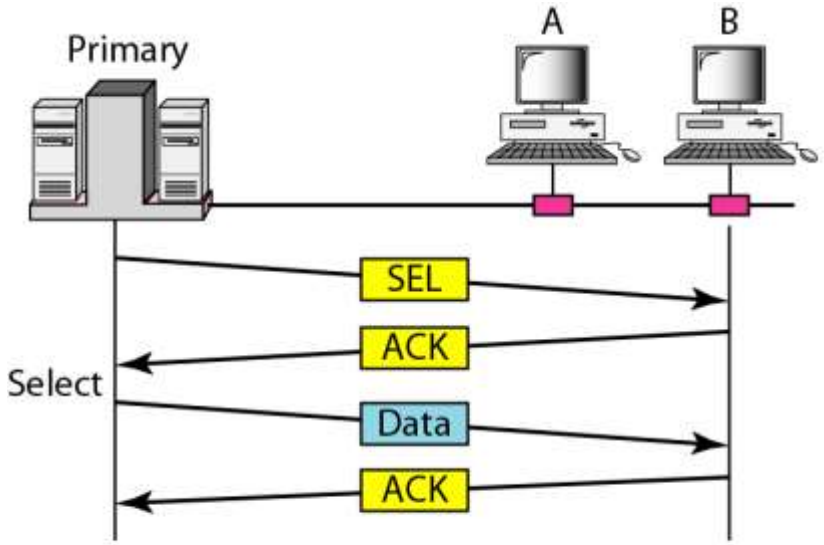
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

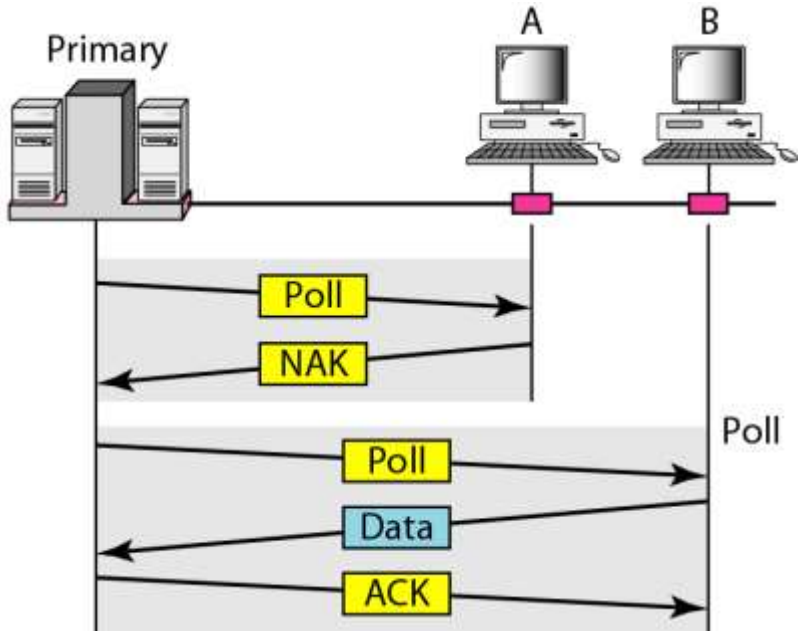


Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message but the addressed one responds to it and sends data, if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

Polling


Primary
A
B
SEL
ACK
Select
Data
ACK


Primary
A
B
Poll
NAK
Poll
Poll
Data
ACK

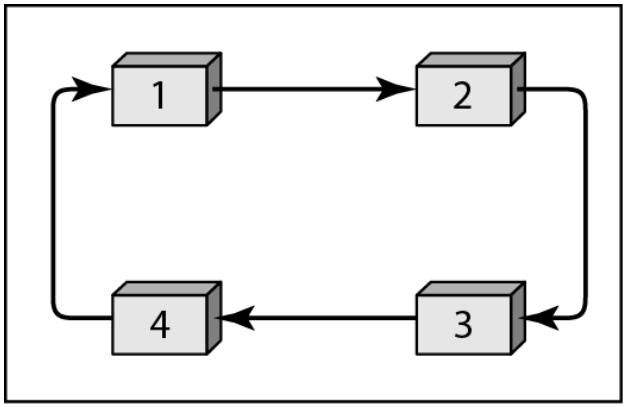
Token passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.

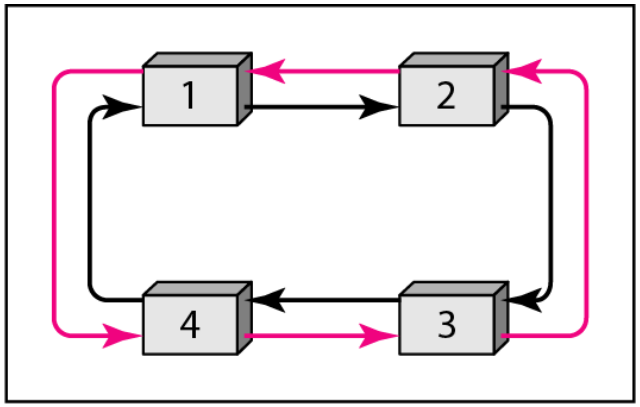
Token passing

- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbors and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.

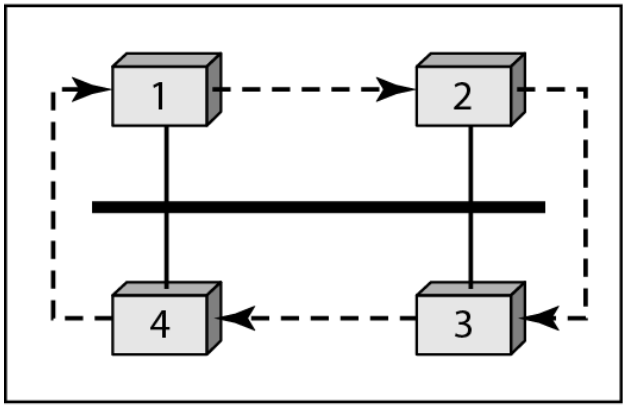
Token ring



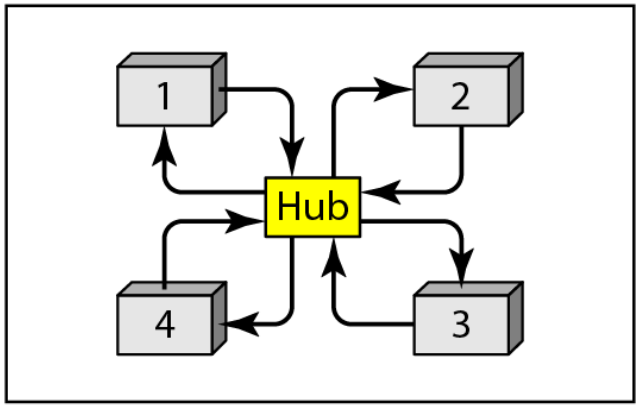
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

Protocols(CO3)

Topic objective

- Understand the protocols used in Data link layer
- Understand the Noisy and noiseless channels
- Implement the error detection and error correction

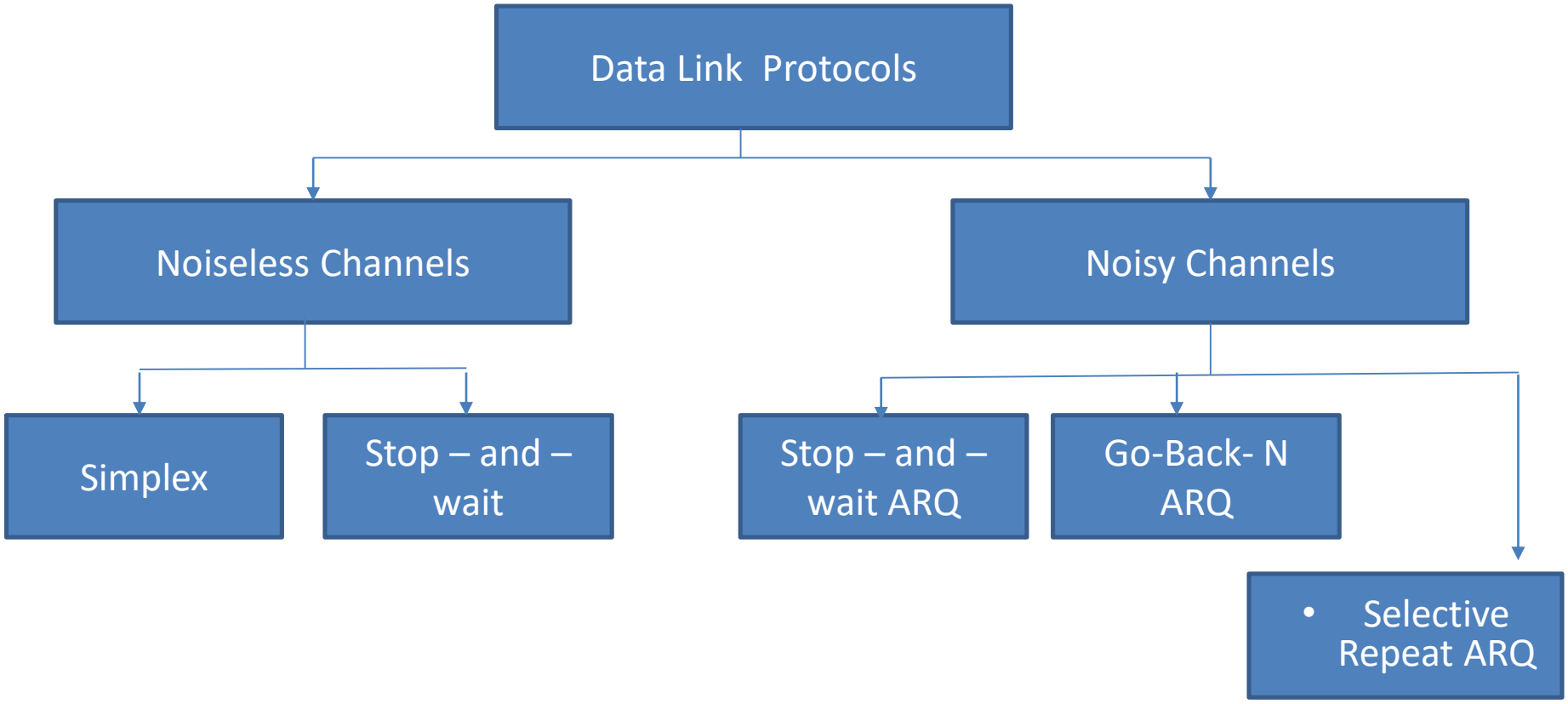
Recap of previous topic

- MAC gives access to multiple channels
- Channel is allocated based on static or dynamic
- Multiple Access protocols are used to allocate channels

Protocols(CO3)

- Protocols in the data link layer are designed so that this layer can perform its basic functions:
- Framing - process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes
- error control - transmission errors and retransmission of corrupted and lost frames
- flow control - regulates speed of delivery and so that a fast sender does not drown a slow receiver.

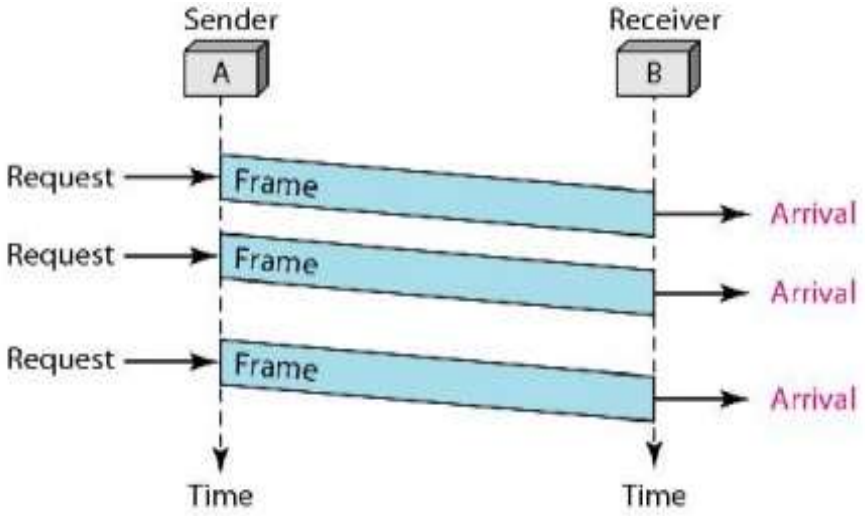
Protocols


Data Link Protocols
Noiseless Channels
Noisy Channels
Simplex
Stop – and – wait
Stop – and – wait ARQ
Go-Back- N ARQ
Selective Repeat ARQ

For Noiseless channels

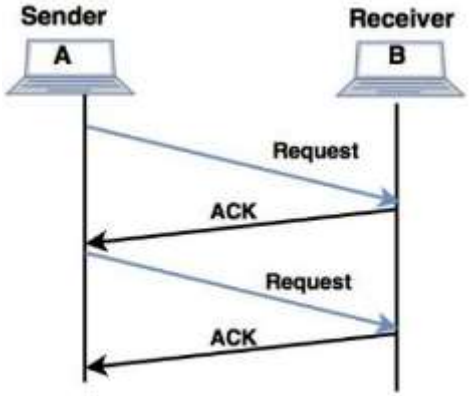
Simplex Protocol

- unidirectional data transmission over an ideal channel
- It has distinct procedures for sender and receiver.
- The sender simply sends all its data available onto the channel as soon as they are available its buffer.
- The receiver is assumed to process all incoming data instantly.



For Noiseless channels

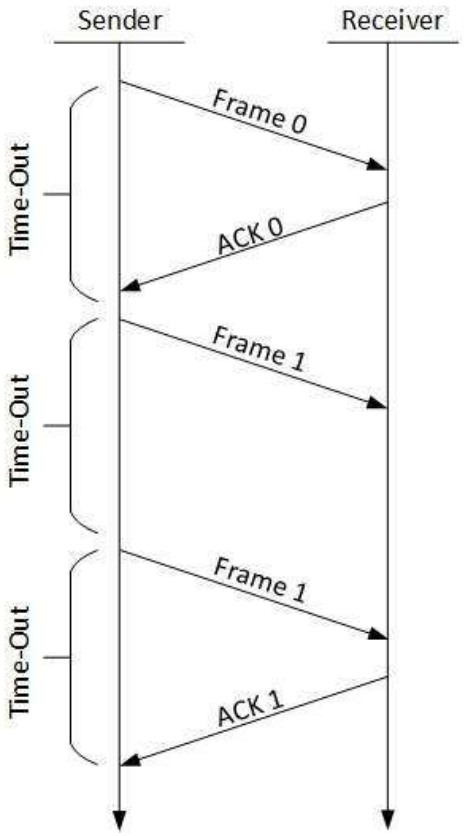
- **Stop – and – Wait Protocol**
- unidirectional data transmission without any error control facilities
- flow control so that a fast sender does not drown a slow receiver.
- The receiver has a finite buffer size with finite processing speed.
- The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.



Stop and Wait

For Noisy Channels

- **Stop – and – Wait ARQ (**Automatic Repeat Request)
- with added error control mechanisms
- The sender keeps a copy of the sent frame.
- It then waits for a finite time to receive a positive acknowledgement from receiver.
- If the timer expires or a negative acknowledgement is received, the frame is retransmitted.
- If a positive acknowledgement is received then the next frame is sent.

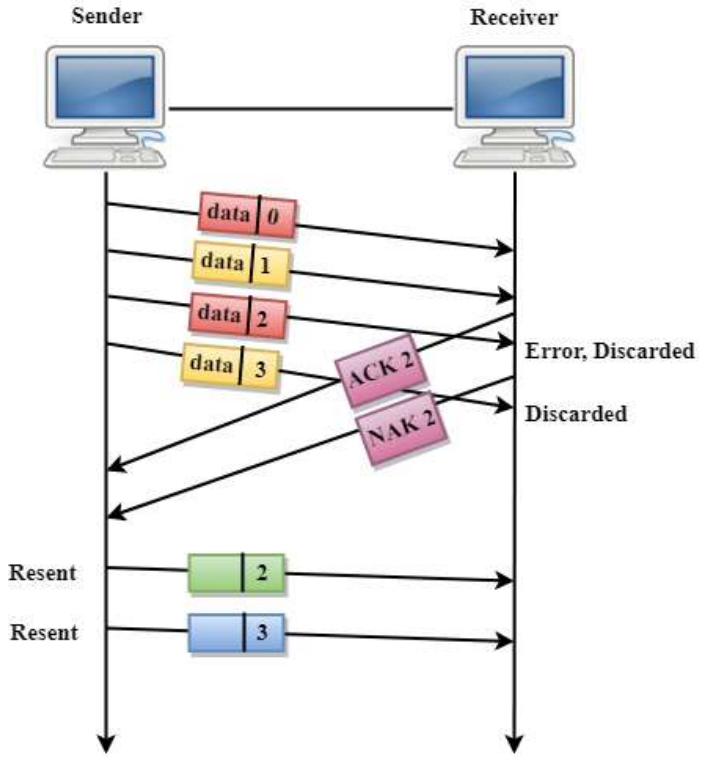


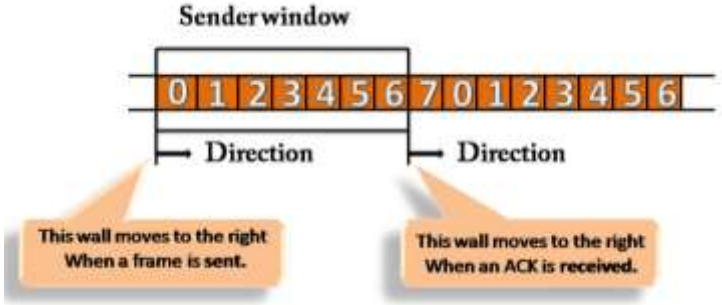
For Noisy Channels

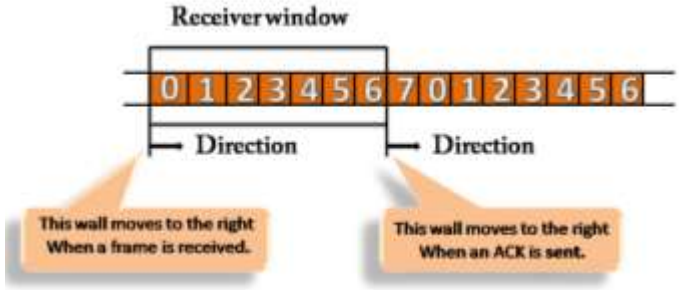
- **Go – Back – N ARQ**
- sending multiple frames before receiving the acknowledgement for the first frame.
- It uses the concept of sliding window, and so is also called sliding window protocol.
- The frames are sequentially numbered and a finite number of frames are sent.
- If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.
- Reason for retransmission
  - Damaged frame
  - Lost data frame
  - Lost Acknowledgement

For Noisy Channels

Go – Back – N ARQ





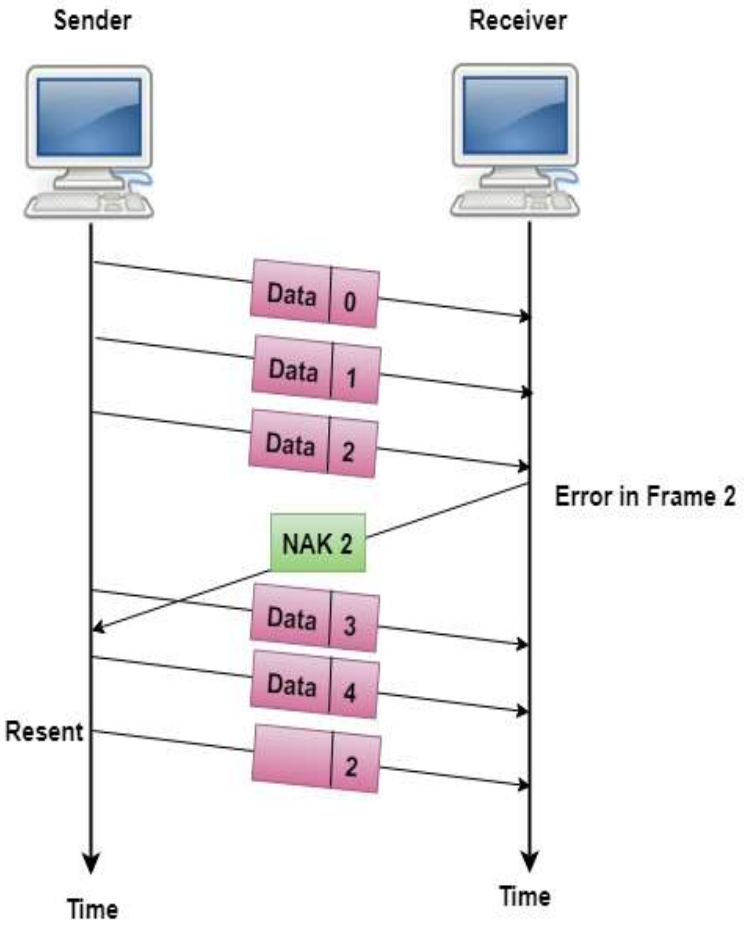


For Noisy Channels

- Piggy backing Technique
  - there is a need for transmitting data in both directions between 2 computers.
  - A full duplex circuit is required for the operation.
  - the data frames and ACK (control) frames in the reverse direction have to be interleaved.
  - An efficient method is to absorb the ACK frame into the header of the data frame going in the same direction. This technique is known as *piggybacking.*
  - When a data frame arrives at an IMP (receiver or station), instead of immediately sending a separate ACK frame, the IMP restrains itself and waits until the host passes it the next message.
  - The acknowledgement is then attached to the outgoing data frame using the ACK field in the frame header.

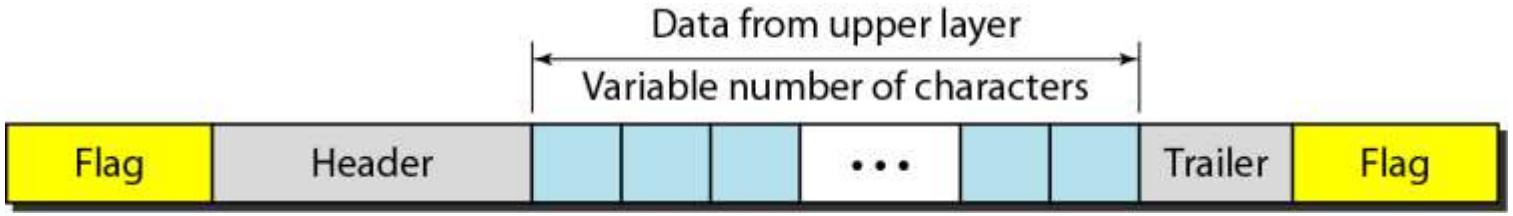
For Noisy Channels

- **Selective Repeat ARQ**
- sending multiple frames before receiving the acknowledgement for the first frame.
- only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.



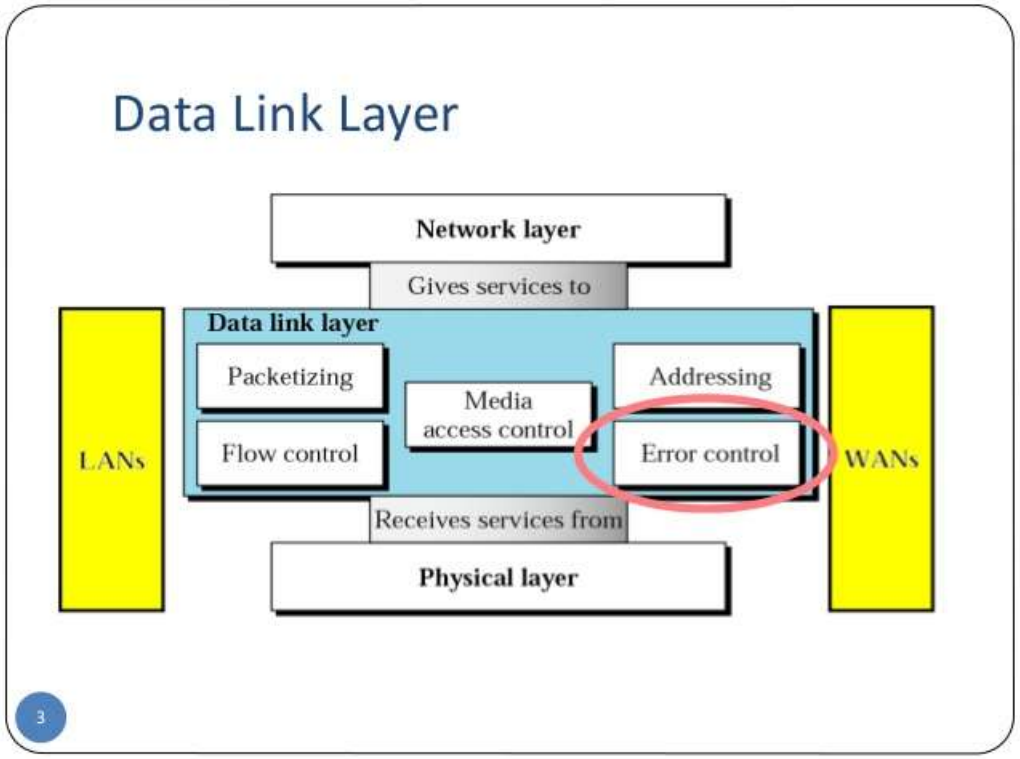
Data Link Layer(CO5)

- *The data link layer needs to pack bits into frames, so that each frame is distinguishable from another.*



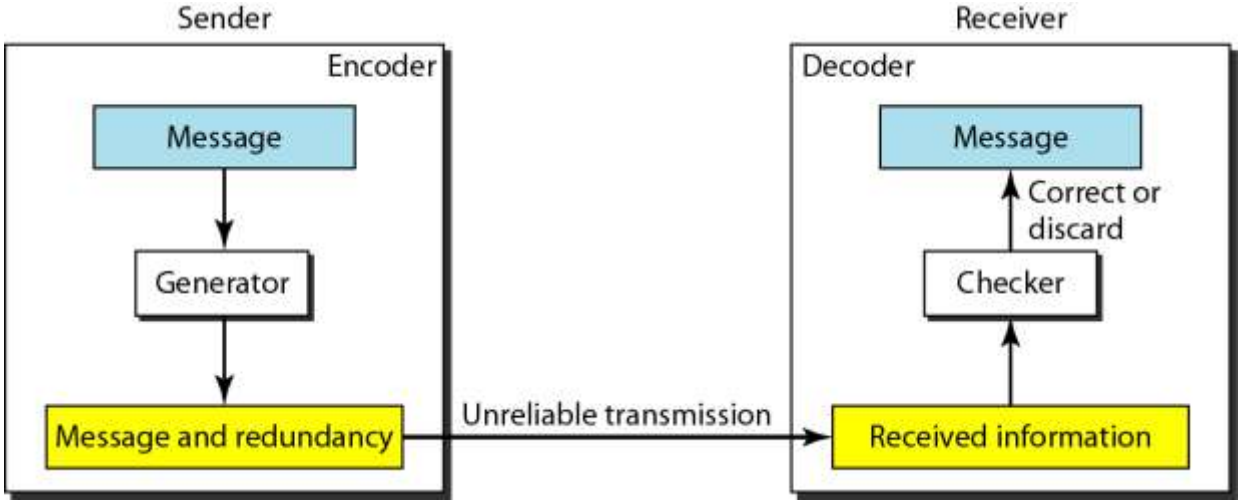
- The three main functions of the **data link layer** are
  - to deal with transmission errors,
  - regulate the flow of **data**, and
  - provide a well-defined interface to the network **layer**
- **Design issues -Error Control**
  - Dealing with transmission errors.
  - Sending acknowledgement frames in reliable connections.
  - Retransmitting lost frames.
  - Identifying duplicate frames and deleting them.
  - Controlling access to shared channels in case of broadcasting.

Error Control



Error detection and correction

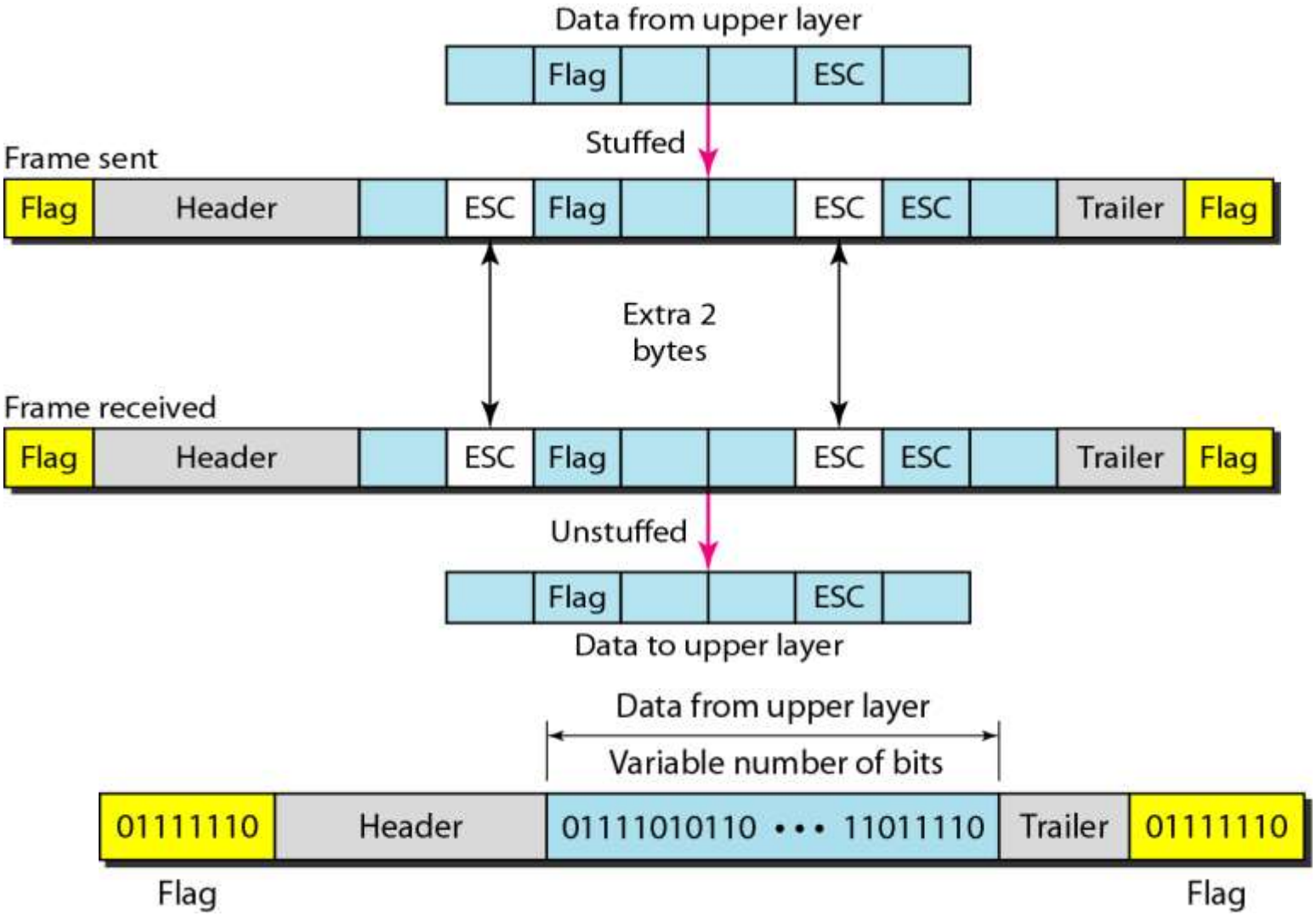
- Data can be corrupted during transmission
- Types of error
  - Bit error
  - Burst error
- To detect or correct errors, we need to send extra (redundant) bits with data.



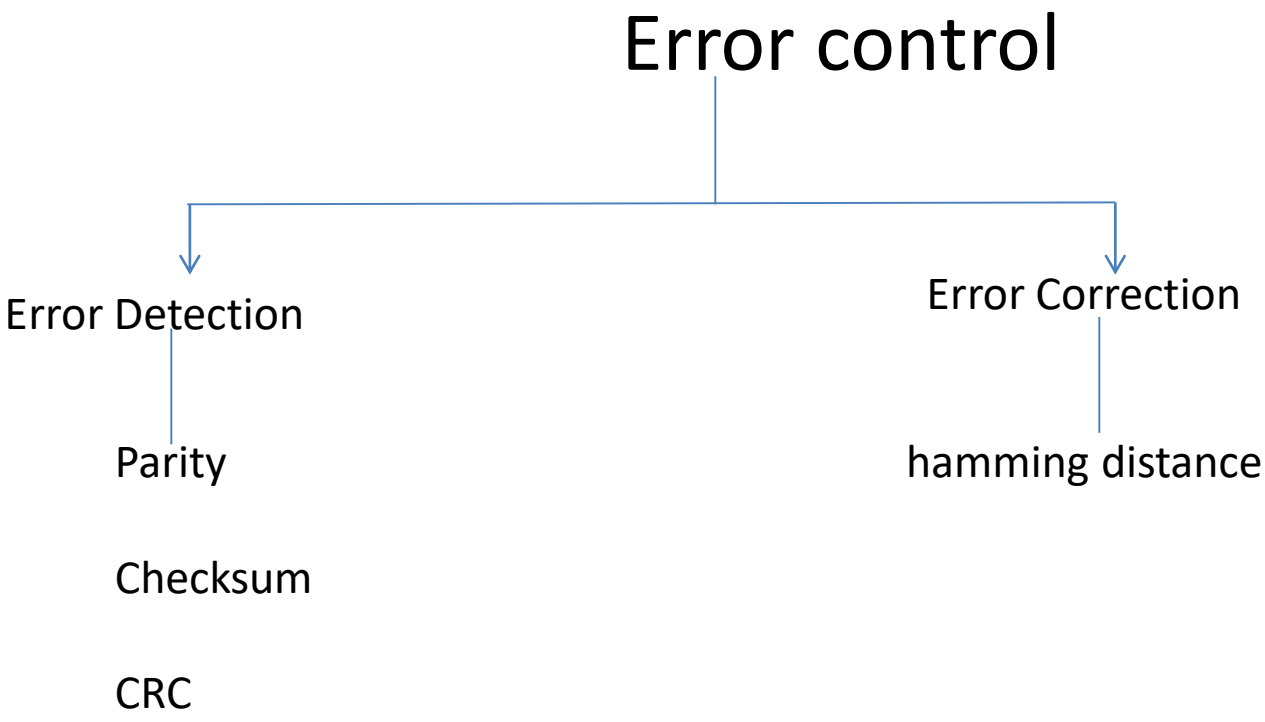
Error detection and correction

- An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected.
- Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.
- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data

Byte stuffing & bit stuffing(CO4)



Error Control



Error Detection(CO5)

- Parity checks
  - For a data of n size add a parity bit
    - Even parity
    - Odd parity

For example if a data to be send is 1110001

Then for even parity the bit will be 0

for odd parity the bit will be 1

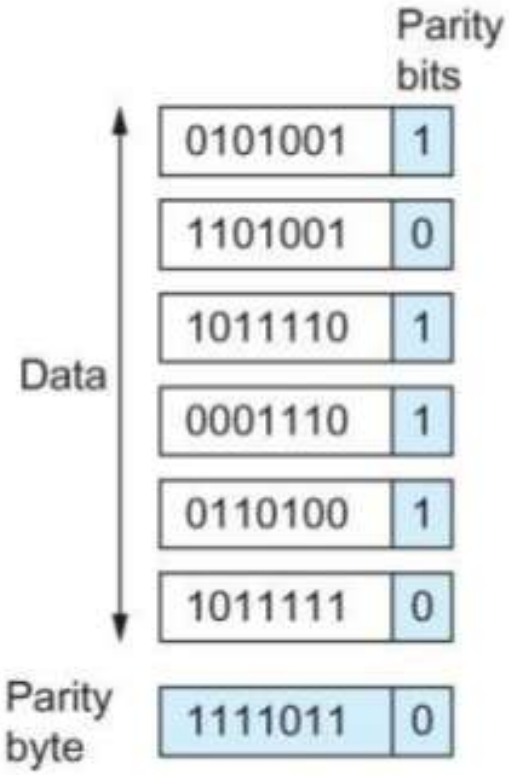
How many bit errors it can detect?

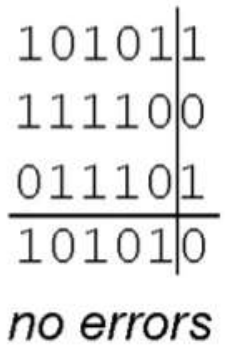
Suppose 10001110 is transmitted received as 10011110 ------- error detected

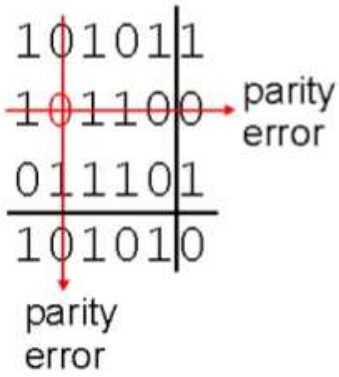
But if 10001110 is transmitted received as 10010110 --------no error detected

Error Detection

- Two dimensional parity checks

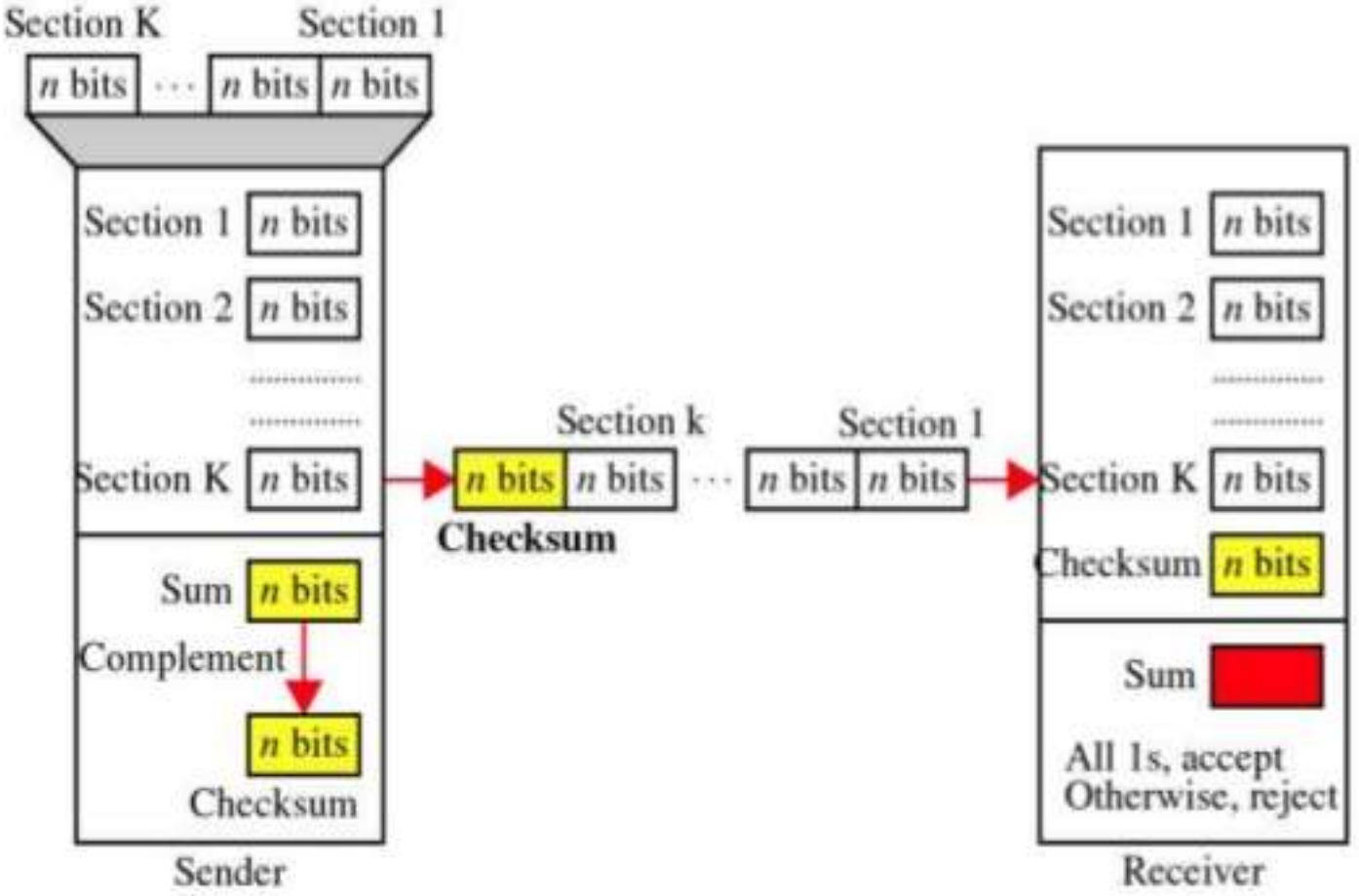






Error Detection

Checksum



Error Detection

Checksum

- When adding numbers in ones complement arithmetic, a carryout from the most significant bit needs to be added to the result (Wrapping).

Sender Side:

- The message is divided into 16-bit words.
- The value of the checksum word is set to 0.
- All words including the checksum are added using one's complement addition.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

Receiver Side:

- The message (including checksum) is divided into 16-bit words.
- All words are added using one's complement addition.
- The sum becomes the new checksum.
- If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

Error Detection

- Checksum

Frame Data: 01101101 10010011 01101101

n=8

Sender Side:

Calculating Checksum,

```
  01101101
  10010011
  01101101
  --------
  01101101  --------→1's Compliment--→ 10010010
  --------
```

Checksum = 10010001

So data transmitted over the link is: 01101101 10010011 01101101 **10010010**

Receiver Side: (without Error)

Received Data: 01101101 10010011 01101101 10010001

Calculating Sum,

```
  01101101
  10010011
  01101101
  10010010
  --------
  11111111   ----> All 1's So accepted (No error)
  --------
```

Receiver Side: (with Error)

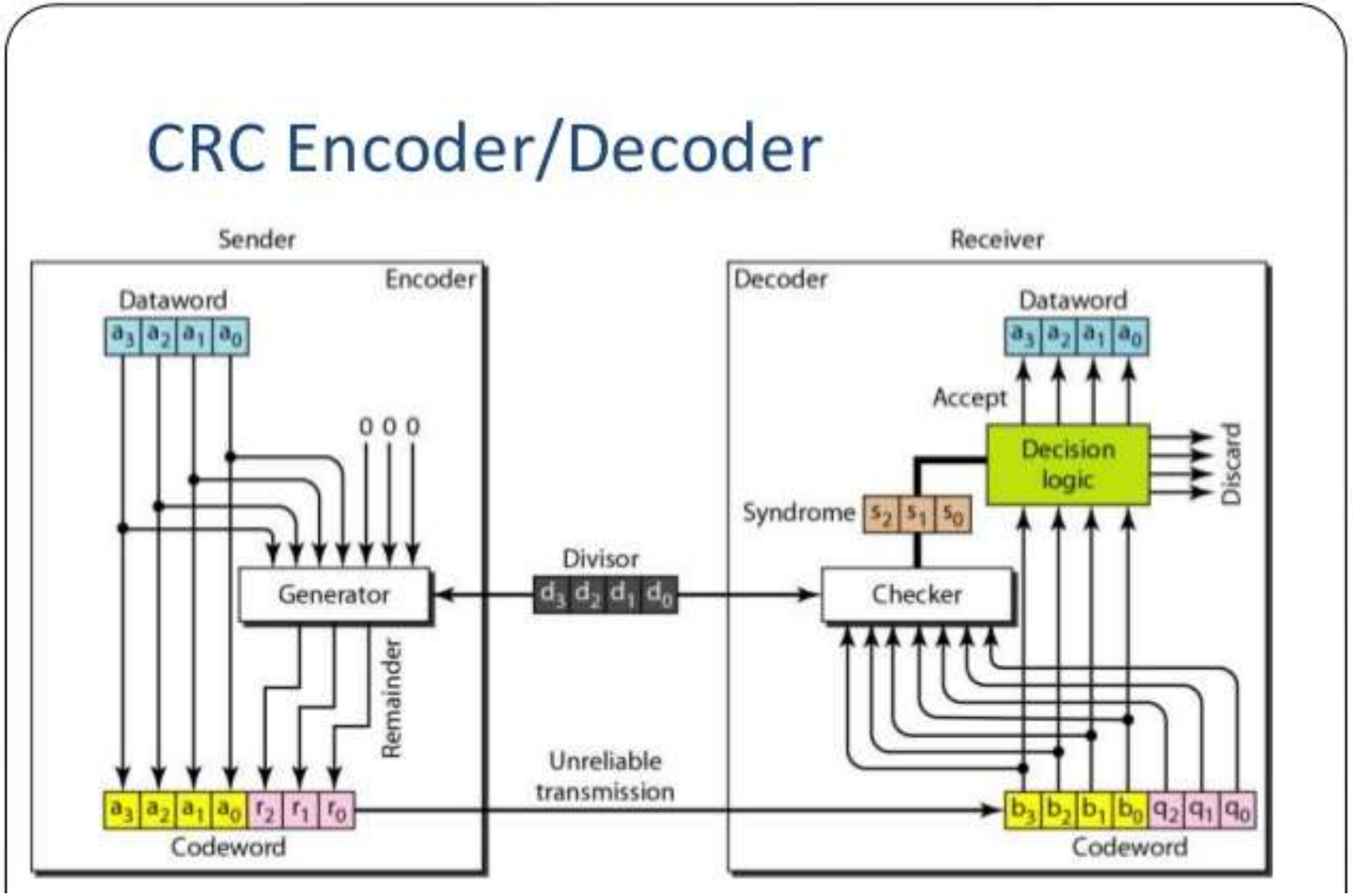
Received Data: 11101101 10010011 01101101

```
  11101101
  10010011
  01101101
  10010010
  --------
  01111111 ---> Not all 1's. So not accepted (Contains Error)
  --------
```

Error Detection

- Cyclic Redundancy check (CRC)
  - Packet of data transmitted as a polynomial 1101 = x^3+x^2+1
  - At sender end - the polynomial is divided by the given generating polynomial
  - Remainder is attached to the end of the message
  - Quotient is discarded
  - Message is transmitted
  - Receiver divides the message with same polynomial
  - If remainder not equal to zero then error occurred
  - Else equal to zero then no error

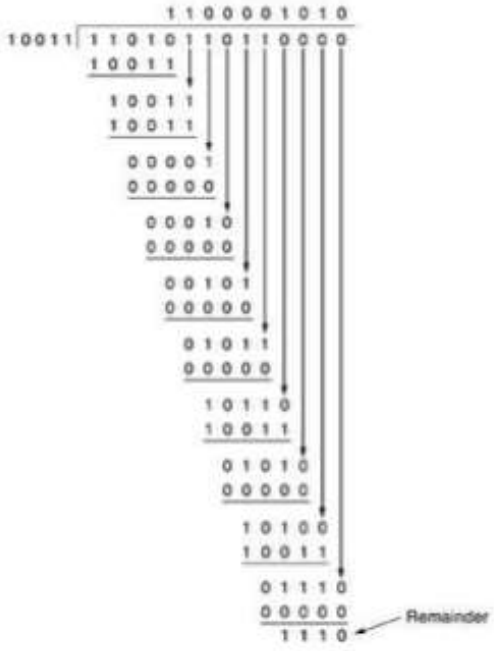
Error Detection



Error Detection

CRC - Example

Frame : 1101011011
Generator: 10011
Message after 4 zero bits are appended: 11010110110000



Frame – 1101011011

$G(x)=x^4+x+1$

Transmitted frame:

11010110110000 –

00000000001110

11010110111110

Transmitted frame: 11010110111110

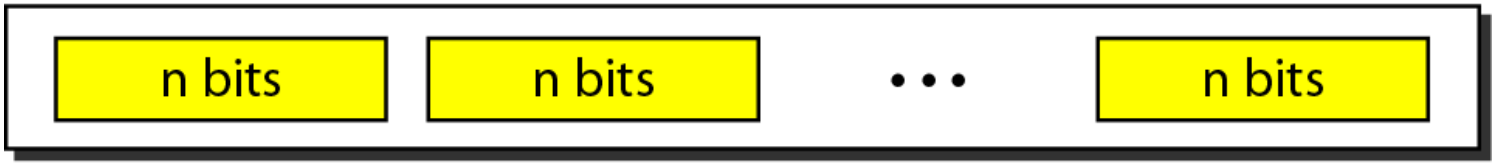
- K= 11010110110000
- N= 10011

- C = k+n-1 =14
- Remainder = 1110
- 11010110110000
- 1110
- Codeword =11010110111110
- N = 10011

Error Correction

- Block coding
  - *In block coding, we divide our message into blocks, each of k bits, called datawords.*
  - *We add r redundant bits to each block to make the length n = k + r.*
  - *The resulting n-bit blocks are called codewords.*

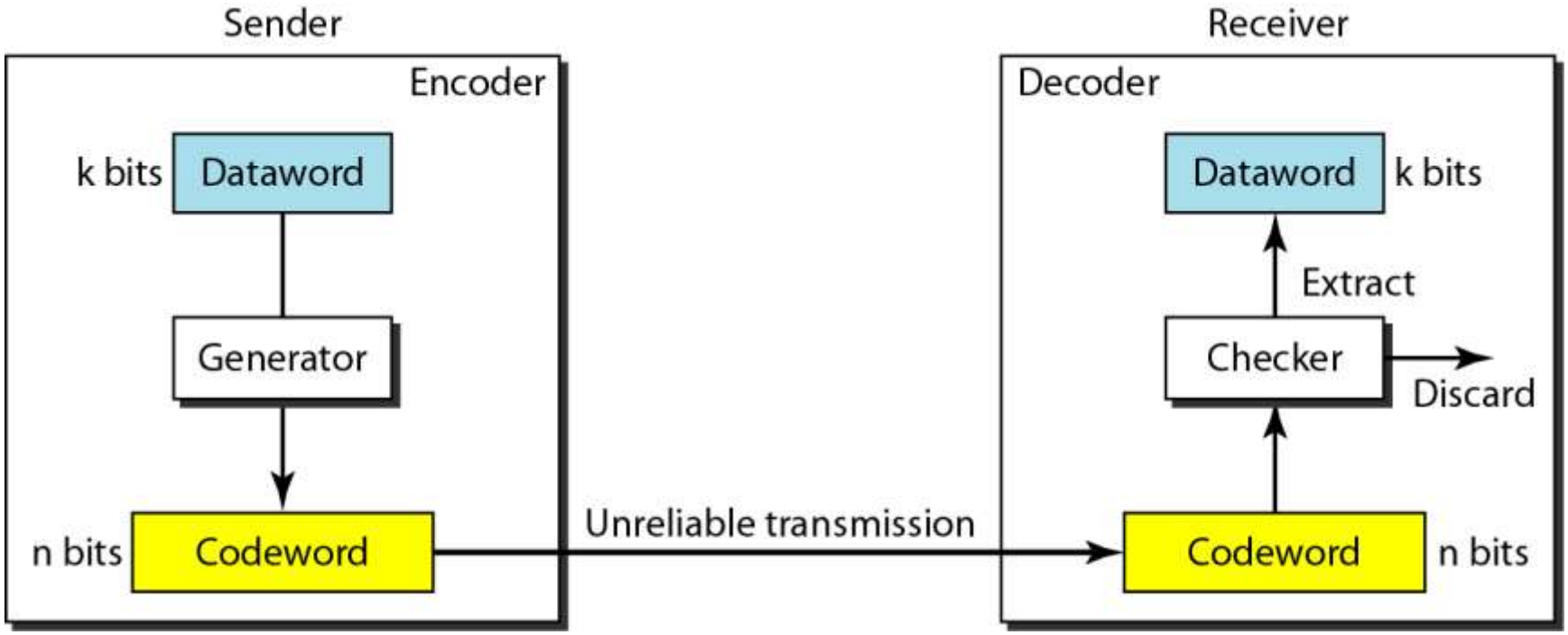
2^k Datawords, each of k bits



2^n Codewords, each of n bits (only 2^k of them are valid)

Error Correction

Block coding



Error Correction

- Hamming distance
  - The Hamming distance between two words is the number of differences between corresponding bits.
  - The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words.
  - To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = s + 1$.
  - To guarantee correction of up to *t* errors in all cases, the minimum Hamming distance in a block code must be $d_{min} = 2t + 1$.

Error Correction

Hamming distance

- The Hamming distance d(000,011) is 2
  000 XOR 011 is 011

Similarly for designing a code minimum hamming distance is used
Which is the smallest hamming distance between all possible pairs
Ex 1. For d(000,011)=2 d(000,101) =2 d(000,110) =2 d(011,101)=2
d(011,110) =2 d(101,110)=2

Ex. For d(00000,01011)= 3 d(00000,10101) =3 d(00000,11110)=4
Error detected =3
Error corrected =2

IEEE Standards(CO2)

Topic objective

- Understand the IEEE standards
- Various standard designed for IEEE

Recap of previous topic

- What are protocols?
- Protocols used for data link layer
- Implement error detection and correction code

IEEE Standards(CO2)

- In 1985 The Computer society started a project called Project 802
- Enable intercommunication among various devices
- Specify functions of physical layer and data link layer of LAN protocols
- Various IEEE 802 standards are as
- IEEE 802.1 High Level Interface
- IEEE 802.2 Logical Link Control(LLC)
- IEEE 802.3 Ethernet
- IEEE 802.4 Token Bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Networks
- IEEE 802.7 Broadband LANs
- IEEE 802.8 Fiber Optic LANS
- IEEE 802.9 Integrated Data and Voice Network
- IEEE 802.10 Security
- IEEE 802.11 Wireless Network

IEEE Standards

- 802.2 Logical Link Control
  - "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers).“
  - specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).
  - It is responsible for flow and error control.

IEEE Standards

- 802.3 Ethernet
  - standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
  - This standard encompasses both the MAC and Physical Layer standards.If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.
  - The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.
  - Commonly, Ethernet networks transmit data in packets, or small bits of information.
  - A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

IEEE Standards

- 802.4 Token Bus
  - Token bus standards as broadband computer networks
  - Logically, the stations are organized into a ring
  - When the logical ring is initialized, the highest numbered station may send the first frame. The token and frames of data are passed from one station to another following the numeric sequence of the station addresses.
  - The token does not follow the physical ordering of workstation attachment to the cable,there is no collision as only one station possesses a token at any given time.

IEEE Standards

- 802.5 Token Ring
  - designed to use the ring topology and utilizes a token to control the transmission of data on the network.
  - The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

IEEE Standard

- FDDI (Fiber Distributed Data Interface)
  - a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol
  - An FDDI network contains two token rings, one for possible backup in case the primary ring fails.

IEEE Standard

- The FDDI data frame format is:

PA	SD	FC	DA	SA	PDU	FCS	ED/FS
16 bits	8 bits	8 bits	48 bits	48 bits	up to 4478×8 bits	32 bits	16 bits

- Where
- **PA** is the preamble,
- **SD** is a start delimiter,
- **FC** is frame control,
- **DA** is the destination address, **SA** is the source address,
- **PDU** is the protocol data unit (or packet data unit),
- **FCS** is the frame check Sequence (or checksum), and
- **ED/FS** are the end delimiter and frame status.

IEEE Standards

- 802.11 Wireless Network Standards
  - collection of standards setup for wireless networking.
  - the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n.
  - Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.
  - 802.11a was one of the first wireless standards.
  - 802.11b standard was popular due to higher prices and lower range.
  - 802.11g is a standard operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment.
  - Wireless LANs primarily use CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance. It has a "listen before talk" method of minimizing collisions on the wireless network.
  - This results in less need for retransmitting data.