Data Security

→ It is the protection of data from unauthorized users.

→ Only the authorized users are allowed to access the data.

→ Most of the users are allowed to access a part of the database. i.e, the data that is related to them or related to their department

→ Mostly, the DBA or Head of department can access all the data in the database

→ Some users may be permitted only to retrieve data, whereas others are allowed to retrieve as well as to update data.

→ The database access is controlled by the DBA

→ He/She creates the accounts of users & gives rights to access the database.

→ Users or group of users are given usernames protected by passwords.

Scanned with CamScanner

→ The user enters his/her account number (or user name) & password to access the data from the database.

→ For ex; If you have an account in the "Yahoo.com", then you have to give your correct username & password to access your account or e-mail.

→ Similarly, when you insert your ATM card into the Automated Teller Machine (ATM), the machine reads your ID number printed on the card & then asks you to enter your pincode (or password). In this way, you can access your account.

Data Integrity

→ Data Integrity means that the data contained in the database is both correct & consistent. For this purpose, the data stored in the database must satisfy certain types of constraints (rules).

→ For ex, a balance for any account must not be less than zero. Such constraints are enforced in the system by adding appropriate

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE INTERNATIONAL SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL | The Sage Foundation

Scanned with CamScanner

code in application programs. But, when new constraints are added, such as balance should not be less than Rs 500 application programs need to be changed. But it is not an easy task to change programs whenever required.

→ Data in a database must be correct & consistent.

→ So, data stored in the database must satisfy certain types of constraints (rules).

→ DBMS provides different ways to implement such types of constraints (rules)

→ This improves data integrity in a database.

P.T.O.

Scanned with CamScanner

Comparison B/w Security & Integrity

Data Security	Data Integrity
1) Data security defines the prevention of data corruption through the use of controlled access mechanisms.	1) It defines the quality of data, which guarantees the data is complete & ~~dat~~ has a whole structure
2) It deals with the protection of data	2) It deals with the validity of data
3) It is making sure only the people who should have access to the data are the only ones who can access the data	3) It is making sure the data is correct & not corrupt.
4) It refers to making sure that data is accessed by its intended users, thus ensuring the privacy & protection of data.	4) It refers to the structure of the data & how it matches the schema of the database.
5) Authentication/Authorization,	5) Backing up, designing

M/s Agrawal Construction Co. | SIRT Sagar Group of Institutions | SAGE School | SAGE University | SAGE Hospital | Agrawal | Sage Foundation

Scanned with CamScanner

Data Security	Data Integrity
encryptions & masking are some of the popular means of data security.	a suitable user interface & error detection/correction in data are some of the means to preserve integrity.

Error Detecting Codes

Whenever a message is transmitted, it may get scrambled by noise & data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. Ex- Parity check.

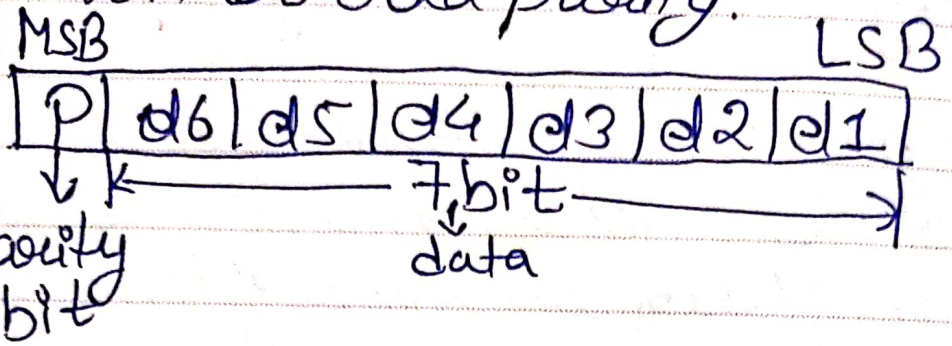
Parity Checking

It is the simplest technique for detecting & correcting errors. The MSB of an 8-bit word is used as the parity bit & the remaining 7 bit are used as data or message bits. The parity of 8-bits transmitted word can be either

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | SAGE HOSPITAL | AGRAWAL | Sage Foundation

Scanned with CamScanner

Even or odd parity.



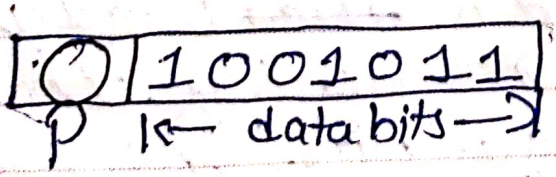
i) Even parity :- Even parity means the number of 1's in the given word including the parity bit should be even (2, 4, 6...)

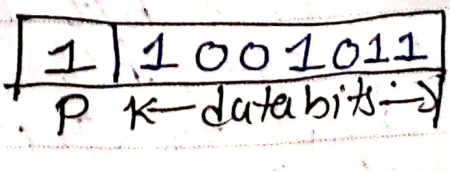
ii) Odd parity :- Odd parity means the number of 1's in the given word including the parity bit should be odd (1, 3, 5...)

☆ Use of parity bit

The parity bit can be set 0 & 1 depending on the type of the parity required.

→ For even parity, the bit is set to 1 or 0 such that the nos. of 1's bits in the entire word is ~~odd~~ even.

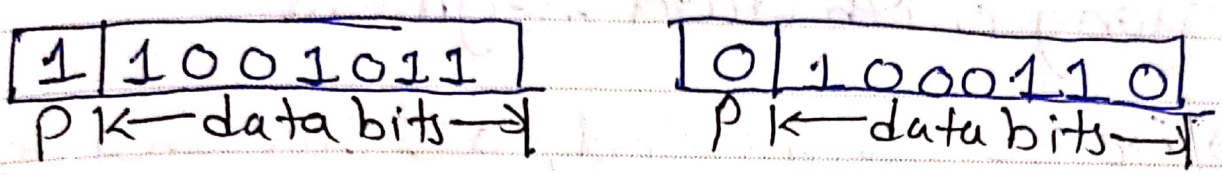




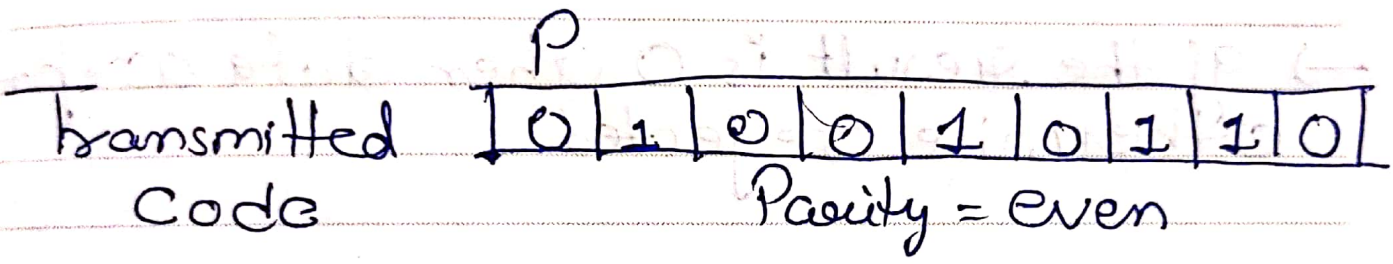
M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE INTERNATIONAL SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL | Sage Foundation

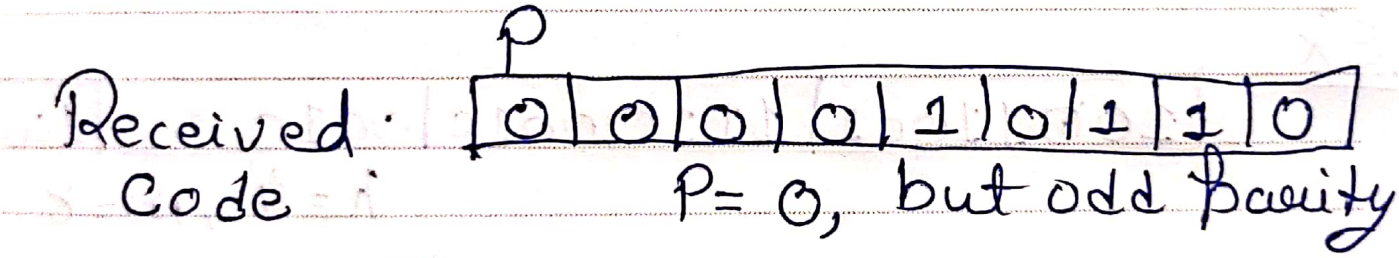
Scanned with CamScanner

→ For odd parity, the bit is set to 1 or 0 such that the nos. of '1' bits in the entire word is odd.



How Does Error Detection take Place

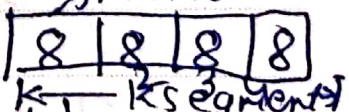




Decision → Incorrect Word.

2) Check Sum Error Detection

→ In this scheme, the data is divided into k segment, each of n bits.



→ In the sender end, the segment are added using 1's complement arithmetic to get the sum. The sum is complemented

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POWER PVT. LTD. | Sage Foundation

Scanned with CamScanner

to get the Checksum

→ Now Checksum Segment is sent along with data segment

→ At receiver's end, all receiver segment are added using 1's complement arithmetic to get the sum. The sum is complemented

→ If the result is 0 then data accepted otherwise rejected.

Ex

10011001	11100010	00100100	10000100

K=4, m=8

Sol^n Sender

1→ 10011001
2→ 11100010
(1) 01111011
+ 1
01111100
3→ 00100100
10100000
4→ 10000100
(1) 00100100
+ 1
00100101 ⇒ Sum
11011010 ⇒ ~~Complement~~ Checksum

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | MY SAGE HOSPITAL | AGRAWAL | Sage Foundation

Scanned with CamScanner

Receiver

1→ 10011001
2→ 11100010
(1) 01111011
↳ 1
01111100
3→ 00100100
10100000
4→ 10000100
(1) 00100100
↳ 1
00100101
11011010 → Checksum
11111111
⇒ 00000000 → Data is Accepted

Diagram

Words will be added to the previous word
↓ total sum
1's

Data | Checksum → Sent → Receiver: Data | Checksum

Sender

Receiver: Calculate checksum by adding checksum
↓ Compare by complementing
If all 0's then no error. Accepted.

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL

Scanned with CamScanner

Ex

10110011	10101011	01011010	11010101

Sol^n Sender

1→ 10110011
2→ 10101011
(1) 01011110
1
01011111
3→ 01011010
10111001
4→ 11010101
(1) 10001110
1
10001111 ⇒ Sum
01110000 ⇒ Checksum

Receiver

1→ 10110011
2→ 10101011
(1) 01011110
1
01011111
3→ 01011010
10111001
4→ 11010101
(1) 10001110
1
10001111
01110000
11111111
Checksum 00000000

Accept data.

M/s Agrawal Construction Co. | SIRT Sagar Group of Institutions | SAGE School | SAGE University Indore • Bhopal | My SAGE Hospital | Agrawal Power Pipes Ltd. | Sage Foundation

Scanned with CamScanner

3) Cyclic Redundancy Check

→ It is a method of detecting accidental changes / errors in the communication channel.

→ CRC uses Generator Polynomial which is available on both Sender & Receiver side.

→ An example generator polynomial is of the form like x^3+x+1. This generator polynomial represents key 1011. OR Another ex is x^2+1 that represents key 101.

n → Number of bits in data to be sent from Sender side.

k → Number of bits in the key obtained from generator polynomial.

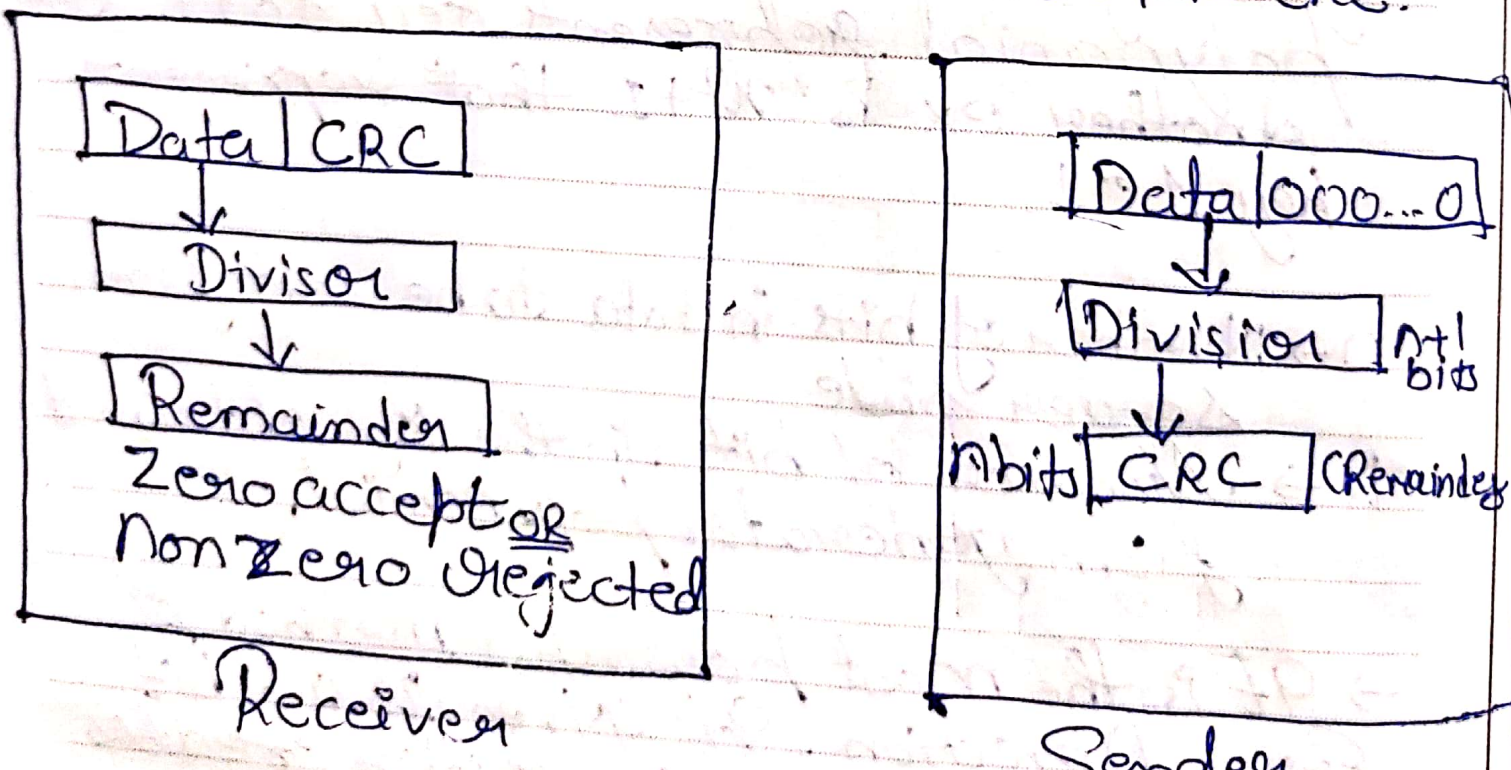
→ It is the most powerful method of Error Detection. It gives as a k bit message. & the transmitter creates an (n-k) bit sequence called frame Check sequence.

Scanned with CamScanner

→ The outcoming frame, including n bits, is precisely divisible by some fixed number.

→ Modul 2 Arithmetic is used in this binary addition with no carries, just like the XOR operation.

→ Redundancy means duplicay. The redundancy bits used by CRC are changed by splitting the data unit by a fixed divisor. The remainder is CRC.

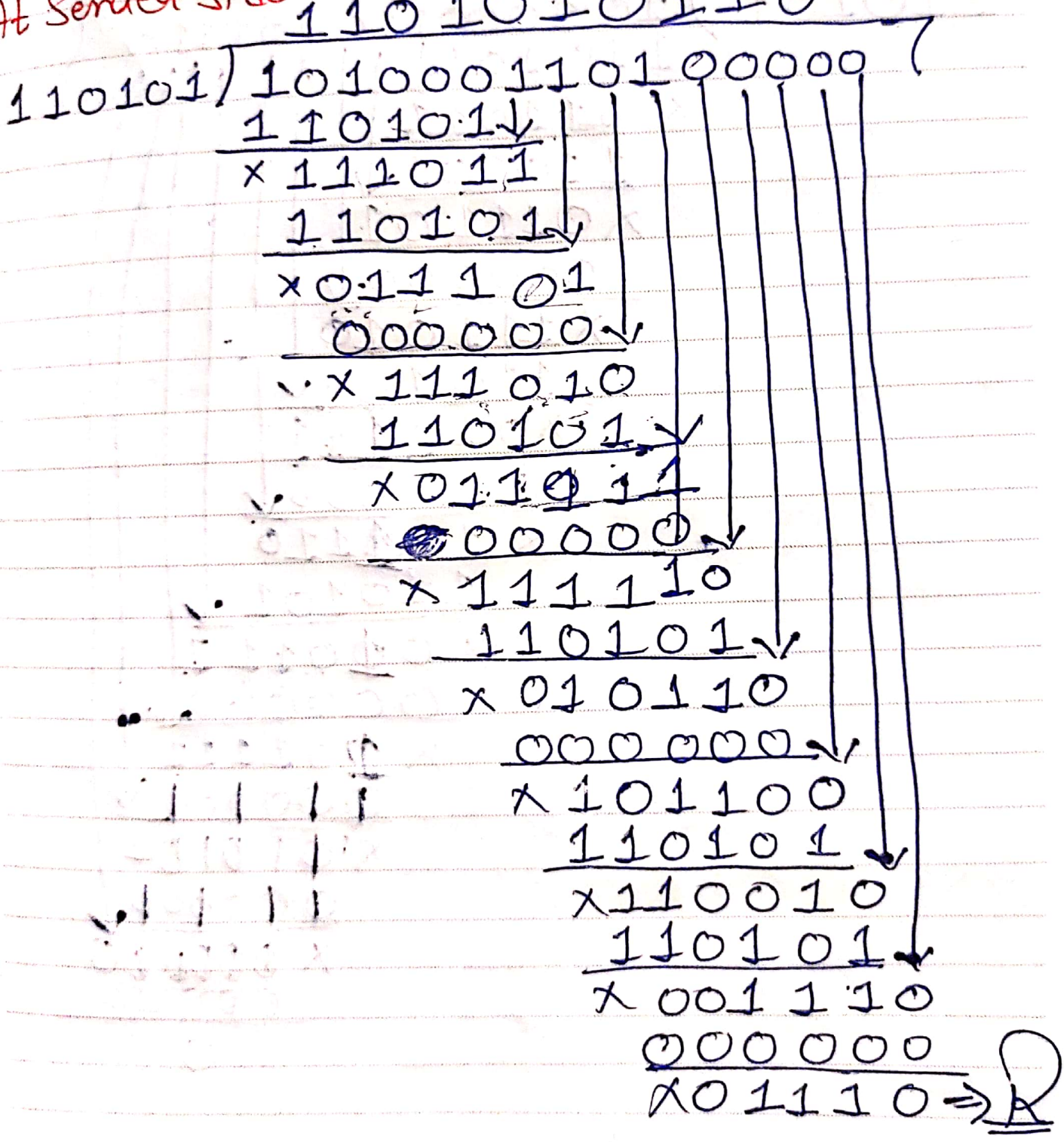


M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE

Scanned with CamScanner

d 1010001101 ⇒ Message
110101 ⇒ Predetermined bits

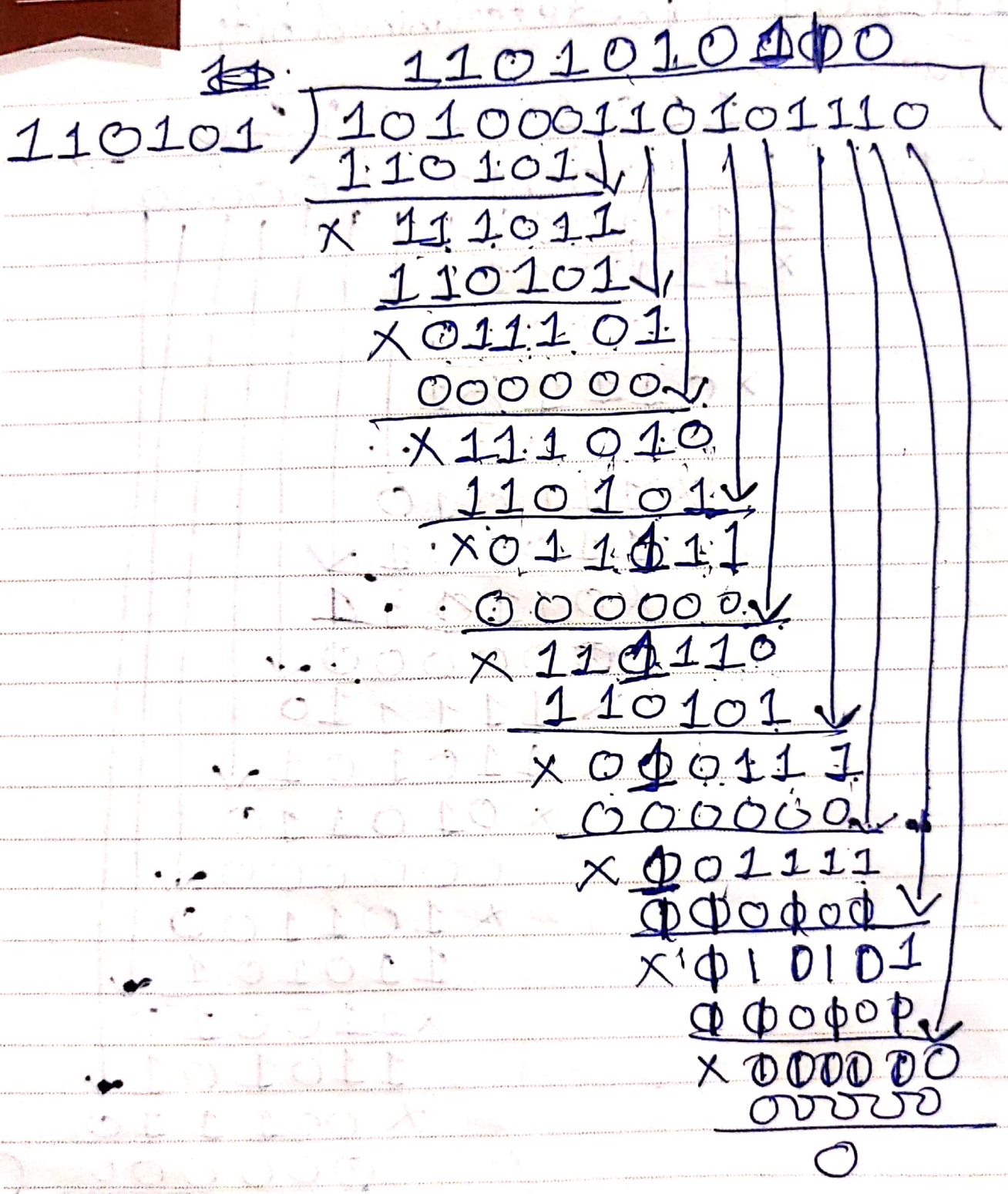
i) At Sender Side



M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | MY SAGE HOSPITAL | AGRAWAL | The Sage Foundation

Scanned with CamScanner

At Receiver Side



M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | MY SAGE HOSPITAL | AGRAWAL | Sage Foundation

Scanned with CamScanner

Error Correction

Hamming Code:-

It is a set of error-correction codes that can be used to detect & correct the errors, that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

⇒ Redundant bits:-

These are extra binary bits that are generated & added to the information-carrying bits of data transfer to ensure that no bits were lost during data transfer

The number of redundant bits can be calculated using the formula:-

$$2^r \geq m + r + 1$$

where, r = redundant bit, m = data bit

Ex→ Suppose the ~~dat~~ nos. of data bits is 7. then the number of redundant bits can be calculated using:-

$$2^4 \geq 7 + 4 + 1$$

Thus, the number of redundant bits = 4

M/s Agrawal Construction Co. | SIRT Sagar Group of Institutions | SAGE School | SAGE University Indore • Bhopal | My SAGE Hospital | Agrawal | Sage Foundation

Scanned with CamScanner

⇒ Parity bits

A parity bit is a bit appended to a data of bits to ensure that the total number of 1's in the data is even or odd. Parity bits are used for error detection. There are two types of parity bits:-

1) Even Parity bit:-
In this case, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.

2) Odd Parity bits:- In this case, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bits value is 0.

Scanned with CamScanner

Flow Control In DLL

Flow Control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

Protocals

- For Noiseless Channel
  - Simplest
  - Stop & Wait
- For Noisy Channel
  - Stop & Wait (ARQ)
  - Sliding Window
    - Go-back-N
    - Selective Repeat

⇒ Protocal = Framing + Flow Control + Error Control

* Framing ⇒ Message from source to destination by giving sender & destination address (fixed & variable size)

⇒ Protocols are implemented in software by using programming language.

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE INTERNATIONAL SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POLYTECHNIC | The Sage Foundation

Scanned with CamScanner

⇒ All protocols are unidirectional i.e. from sender to receiver.

⇒ Special frames like Acknowledgement & NAK (Negative Acknowledgment) can flow in opposite direction for flow & error control purpose.

⇒ The flow control methods will help in ensuring that the data doesn't get lost. The flow control method will check that the senders & send the data only at a rate that the receiver can receive & process

1) STOP AND WAIT Protocal (ARQ → Automatic Repeat Request)

→ In this sender will transmit one frame at a time to the receiver.

→ The sender will stop & wait for the acknowledgment from the receiver.

→ When the sender gets the acknowledgement it will send the next data packet to the receiver & wait for the disclosure again

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE INTERNATIONAL SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POWER PVT. LTD. | Sage Foundation

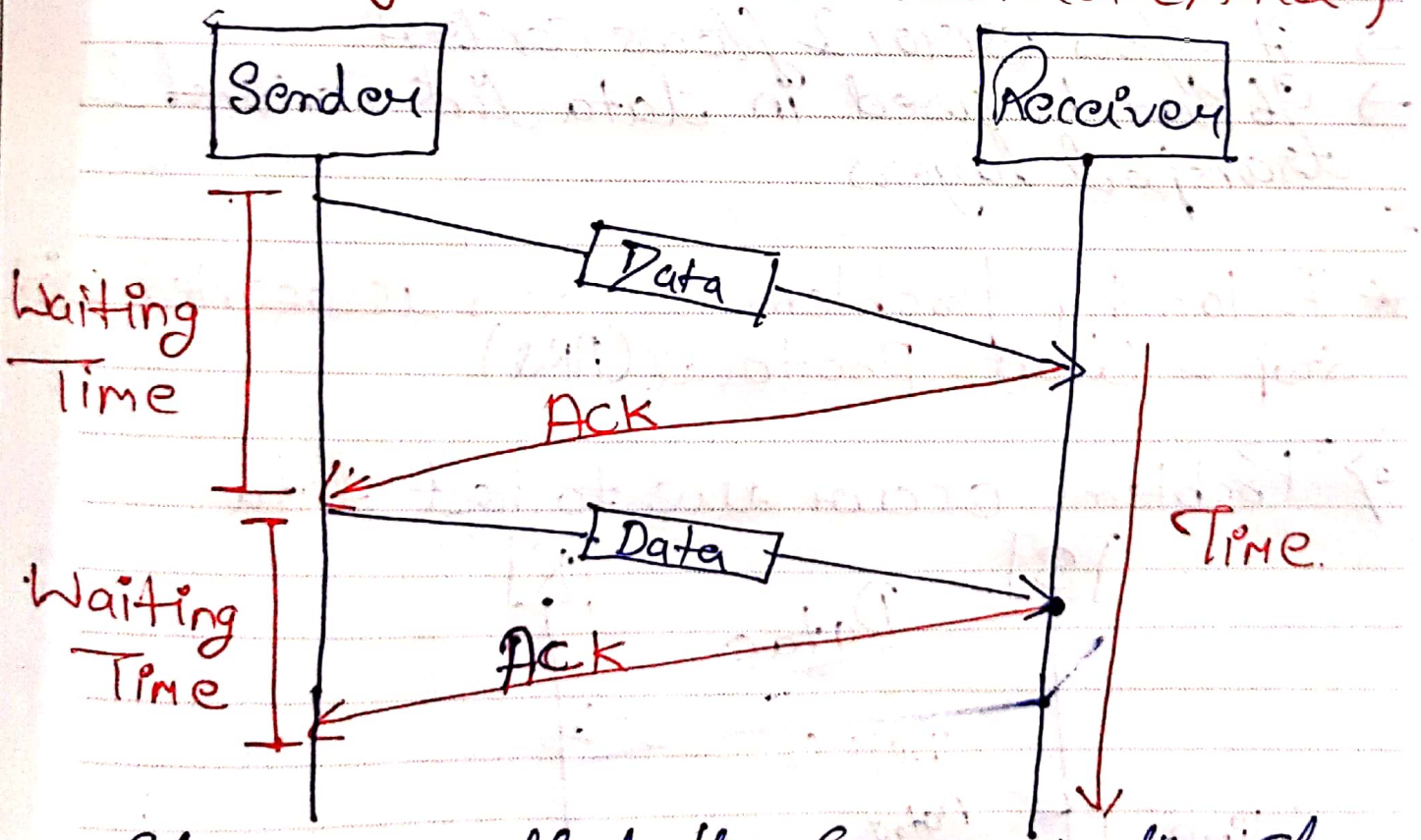
Scanned with CamScanner

& this process will continue as long as the sender has the data to send.

→ While sending the data from the sender to the receiver, the data flow needs to be controlled.

→ If the sender is transmitting the data at a higher rate then the receiver can receive & process it, the data will get lost.

* Working of Stop & Wait Protocol (ARQ)



⇒ It assumes that the communication channel is noisy & Errors may get introduced in the data during the transmission. It is a modified version & improved version of Stop & Wait Protocol

M/s Agrawal Construction Co. | SIRT Sagar Group of Institutions | SAGE International School | SAGE University Indore • Bhopal | My SAGE Hospital | Agrawal Power Pvt. Ltd. | The Sage Foundation

Scanned with CamScanner

Advantage

→ Its accuracy, As the next frame is transmitted only when the first frame is acknowledged. So there is no chance of the frame being lost.

Disadvantage

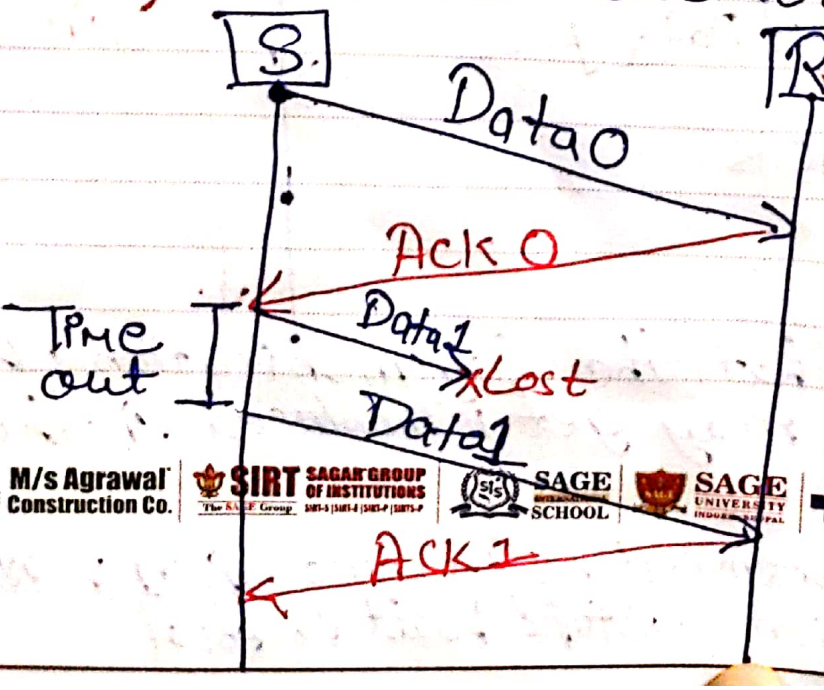
→ It is inefficient, its make the transmission process slow.

Features :-

→ It is used in Connection-oriented communicat
→ It offers error & flow control
→ It can be used in data link ~~control~~ & transport layers

* Following problem occurs associated with Stop & Wait protocal (ARQ)

1) Problems occur due to lost data

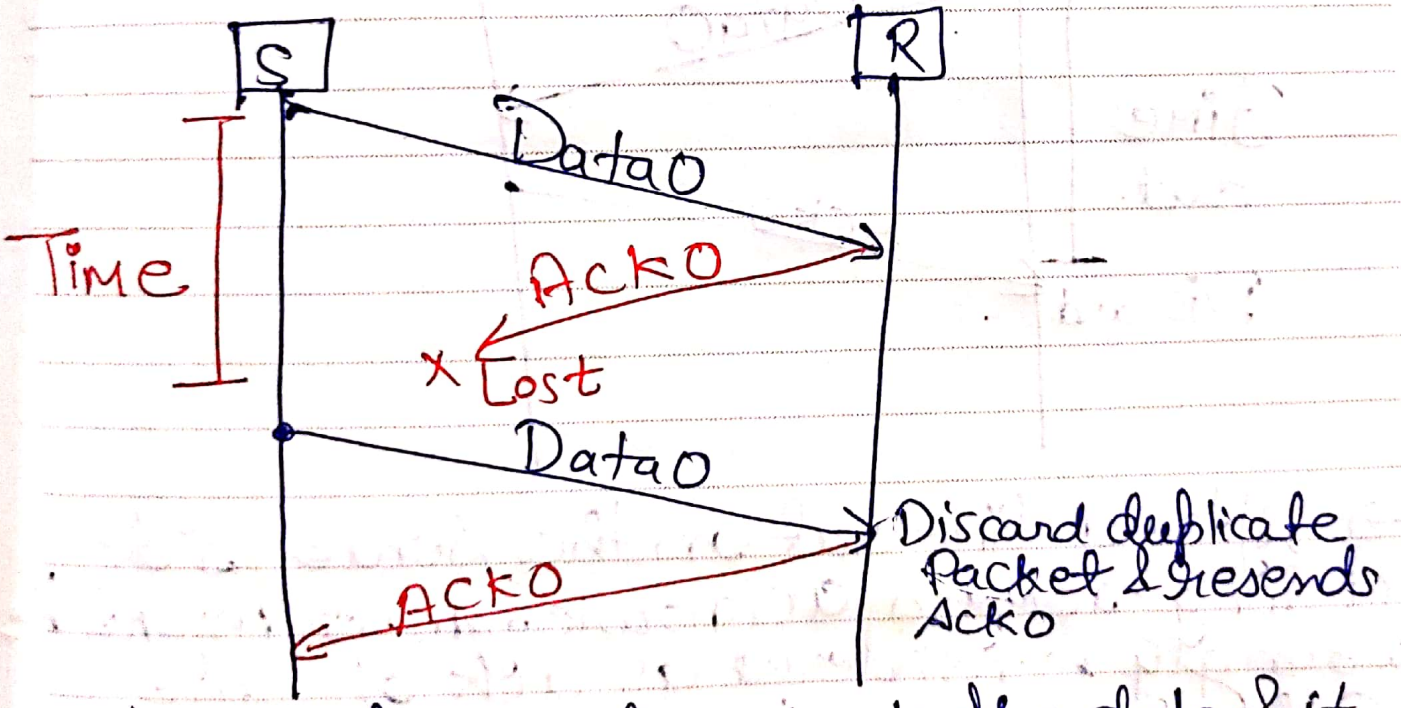


M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | MY SAGE HOSPITAL | AGRAWAL POWER | The Sage Foundation

Scanned with CamScanner

→ Suppose, the sender sends the data & the data is lost. The receiver is waiting for the data for a particular amount of time. Since, the data is not received by the receiver, so it does not send any acknowledgment. After timeout, the sender again send the same packet due to lost of data.

2) Problems occur due to lost of Acknowledgment



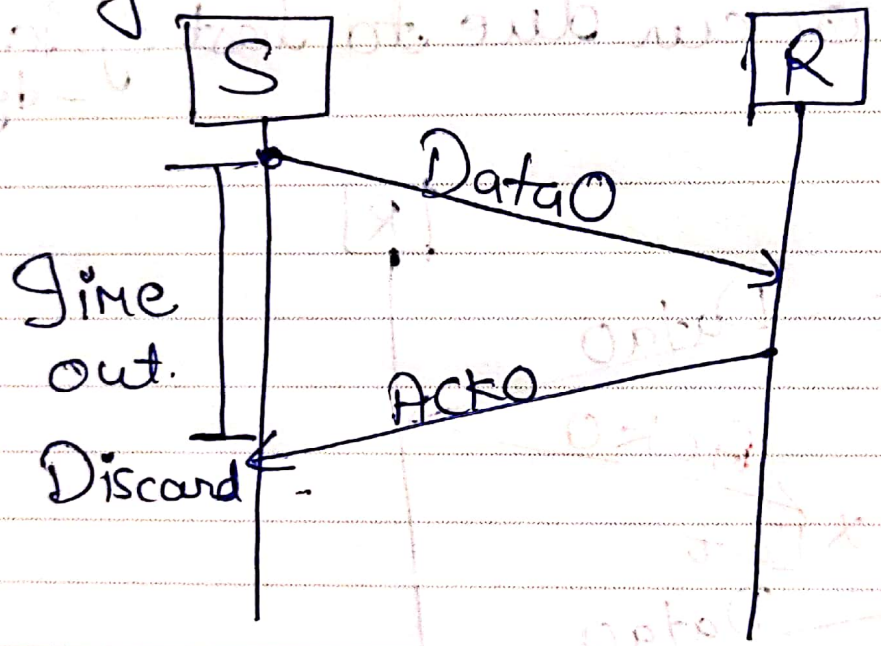
⇒ Suppose the sender sends the data & it has also received by the receiver. On receiving the packet, the ~~s~~receaver sends the acknowledgment. In this case, the ack. is lost.

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POWER PVT. LTD. | The Sage Foundation

Scanned with CamScanner

So there is no chance for the sender to receiver the acknowledgment. & also not send to new packet. After a particular time, Sender again send ~~data~~ same data, due to not received acknowledg-ment.

3) Problems occur due to delayed ackor delayed data

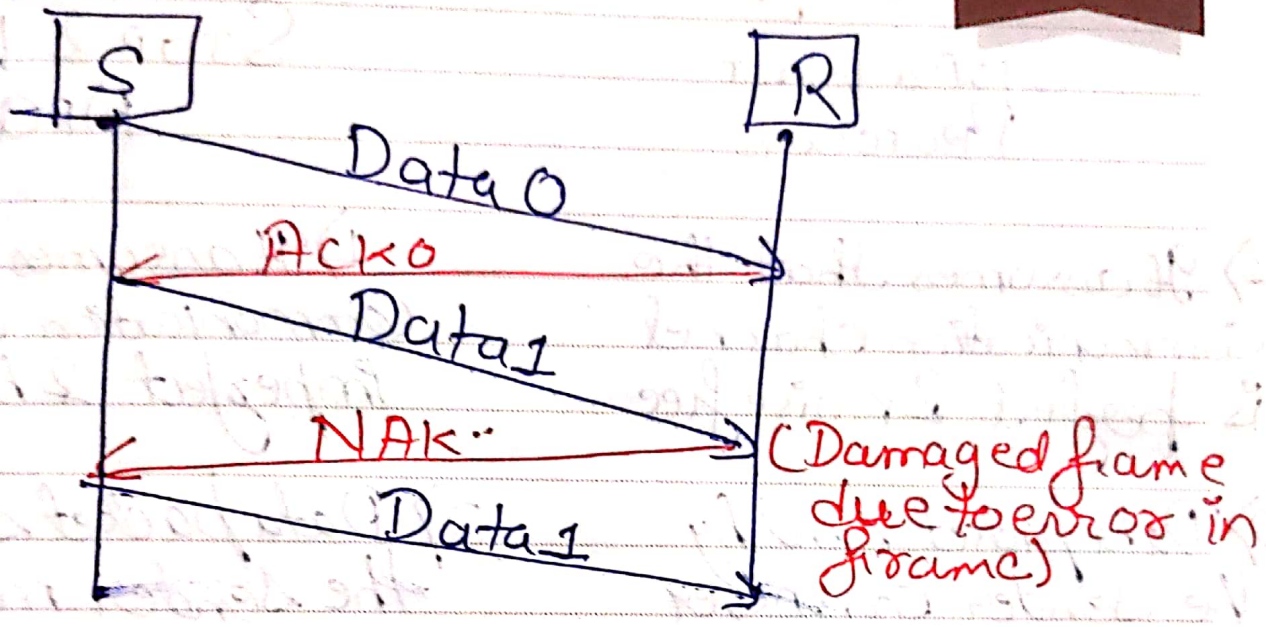


→ After a timeout on the Sender side, a long-delayed acknowledgment might be wrongly considered as ack of some other recent packet.

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POWER PVT. LTD. | Sage Foundation

Scanned with CamScanner

4) Problems occur due to damaged frame



→ If receives ~~a~~ receives a corrupted data from the sender, it sends a negative acknowledgment (NAK) to sender.

→ NAK requests the sender to send the data packet again

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY | MY SAGE HOSPITAL | AGRAWAL | Sage Foundation

Scanned with CamScanner

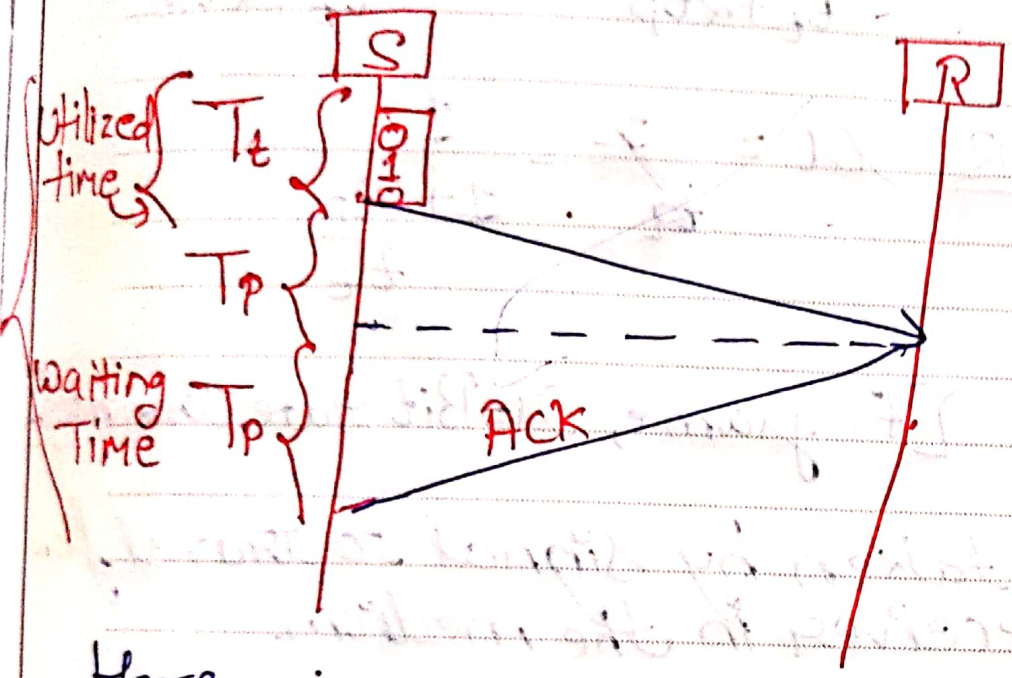
Difference B/w

STOP & WAIT PROTOCOL	STOP & WAIT ARQ
1) It assumes that the communication channel is perfect & noise free	1) It assumes that the communication channel is imperfect & busy
2) Data packet send by the sender can never get corrupt	2) Data packet send by the sender may get corrupt
3) There is no negative acknowledgments	3) ~~There~~ NAK is sent by the receiver if the data packet is found to be corrupt
4) There is no concept of time out timer	4) Sender starts the time out timer after sending the data packet
5) There is no concept of sequence number	5) Data packets & acks are numbered using sequence numbers

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | SAGE HOSPITAL | AGRAWAL POWER PVT. LTD. | Sage Foundation

Scanned with CamScanner

Numerical



Here,

→ Sender uses T_t time for transmiting the packet over the link

→ Then sender waits for $2 \times T_p$ time

→ After $2 \times T_p$ time, sender receives the acknowledgement for the sent frame from the receiver.

→ Then, Sender sends the next frame

→ This $2 \times T_p$ ~~time~~ waiting time is the actual cause of less efficiency.

*Formula:-

$$\text{Channel Utilization} = U$$

$$U = \frac{\text{Active time of Sender}}{\text{Total time of 1 cycle}}$$

M/s Agrawal Construction Co. | SIRT SAGAR GROUP OF INSTITUTIONS | SAGE SCHOOL | SAGE UNIVERSITY INDORE • BHOPAL | MY SAGE HOSPITAL | AGRAWAL POWER AND STEEL | The Sage Foundation

Scanned with CamScanner

i.e. $U = \frac{t_t}{t_t + 2t_p}$ % OR $\frac{t_t}{t_t + 2t_p} \times 100$

OR $U = \frac{1}{1 + \frac{2t_p}{t_t}}$

ii) $t_t = \frac{f}{R}$ [f = frame, R = Bit rate transmission

t_t is a time taken by signal to travel from sender to receiver in the medium.

iii) $t_p = \frac{d}{v}$ [d = distance, v = Signal propogation or speed

t_t is a time taken by a sender to transmit the data into the network Also referred as frame ~~preparad~~ preparation time.

Q Suppose that the stop & wait protocol is used on a link with a bit rate of 64 kb/s & 20 ms propagation delay. Assumes that the transmission delay for the acknowledgment & the processing time at nodes are negligible & the minimum frame size in bytes to achieve a link utilization of atleast 50% is

Scanned with CamScanner