2/9/24

ASSIGNMENT 3

Unit-3 Data Link Layer

Q.1 Explain ARP with diagram.

—↳ Address Resolution Protocol (ARP) is a network protocol used to map a known IP address to a MAC (Media Access Control) address within a local network. ARP is fundamental to network communication because while IP addresses are used for routing across networks, MAC addresses are required for communication within the same network segment (eg: LAN).

—↳ The working of ARP :-

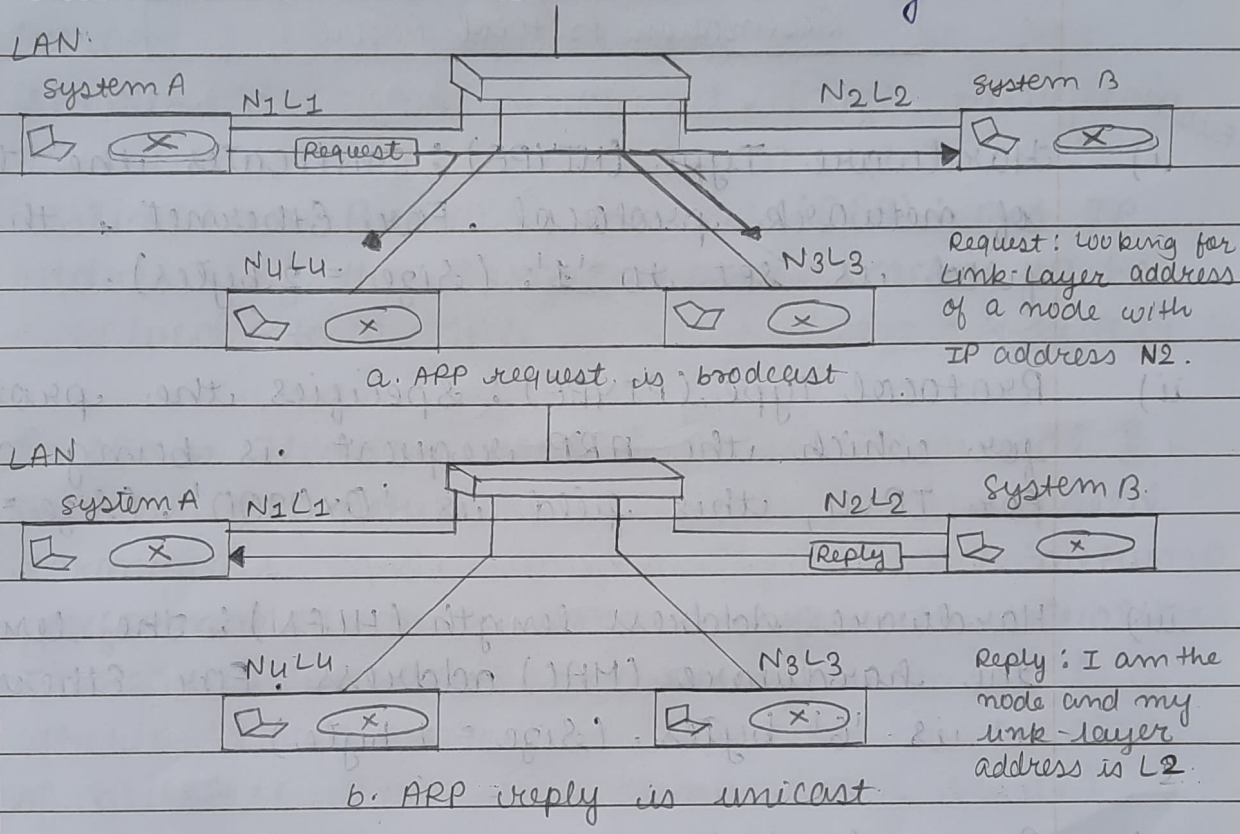
i) ARP Request : When Host A wants to communicate with Host B on the same network, it knows Host B's IP address but needs the MAC address. Host A broadcasts an ARP request packets to all devices on the local network. This ARP packet contains :-
a) Source IP and MAC address (Host A)
b) Destination IP address (Host B)

ii) ARP Reply : When Host B receives the request and sees that its IP address matches the destination IP address, it responds with an ARP reply packet, containing its own IP and MAC addresses.

iii) Caching : Host A stores the IP-to-MAC

mapping in its ARP cache to minimize future ARP requests. (Time limited).

iii) Communication : Host A uses the MAC address to communicate directly with Host B.



Q.2 Discuss ARP Packet Format ?

→ An ARP Packet is encapsulated within an Ethernet frame when transmitted over a local network. The ARP packet has a fixed format, which includes several fields that carry the necessary information for IP-to-MAC address resolution.

→ The ARP Packet structure :-

0	8	16	31
Hardware Type		Protocol Type	
Hardware Length	Protocol Length	Operation Request: 1, Reply: 2	
Source Hardware Address			
Source Protocol Address			
Destination Hardware Address (empty in request)			
Destination Protocol Address			

Fields:-

i) Hardware Type (HTYPE): Indicates the type of network protocol. For Ethernet, this field is set to '1'. (Size = 2 bytes).

ii) Protocol Type (PTYPE): Specifies the protocol for which the ARP request is being made. For IPV4, this field is '0x0800'. (Size = 2 bytes).

iii) Hardware Address length (HLEN): The length of the hardware (MAC) address. For Ethernet, it is '6' bytes. (Size = 1 byte)

iv) Protocol Address length (PLEN): The length of the protocol (IP) address. For IPV4, it is '4' bytes. (Size = 1 byte).

v) Operation (OPER): Indicates type of ARP operation.
a) 1 for ARP request
b) 2 for ARP reply (Size = 2 bytes).

vi) Source Hardware Address (SHA): The MAC address of the sender. For an ARP request, this is the address of host making the request. (Size = 6 bytes).

(vii) Source Protocal Address (SPA): The IP address of the host sending the request. (size = 4 bytes)

(viii) Destination Hardware Address (DHA): The MAC address of the target. This field is empty (zeroed out) in the request because the sender does not know it. (size = 6 bytes).

(ix) Destination Protocol Address (DPA): The IP address of the target, which needs to be resolved to a MAC address. (size = 4 bytes)

Q.3 — 4 Explain Hidden and Exposed terminal

In wireless networks, hidden and exposed terminals can significantly impact network performance. These terms refer to situations where devices cannot directly hear each other's transmissions due to the nature of wireless communication (over Wi-Fi).

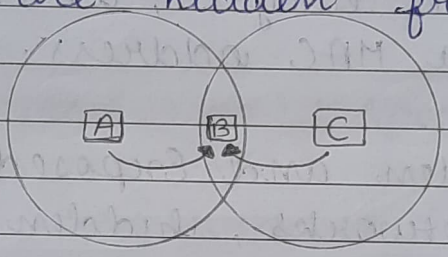
1. Hidden Terminal Problem.

Occurs when two devices (A and C) are out of each other's range but both are within range of a common device (B). A and C cannot detect each other and may send data to B simultaneously, causing collisions.

It happens when devices cannot hear each other but transmit to the same destination. So collisions occur at the

receiving device. The solution is to use protocols like {RTS/CTS (Request to Send/ Clear to Send). {A sends an RTS to B, B responds with CTS, allowing A to transmit while C waits).

eg: a) Device A is sending data to Device B.
b) Device C, which cannot hear A, also sends data to B.
c) ~~B ser~~ This results in collision at B since A and C are "hidden" from each other.



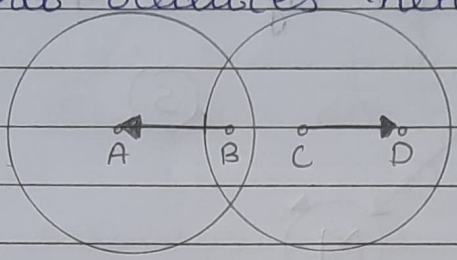
2. Exposed Terminal Problem.

Occurs when a device is prevented from sending data ~~to~~ because it mistakenly thinks its transmission will cause a collision with another device transmitting to a different device.

It happens when devices can hear each other but transmit to different destinations. So it creates unnecessary delay in transmission due to false collision detection. The solution is to use protols like RTS/CTS to reduce false collision assumption.

eg: a) Device C wants to send data to Device D
b) Device B is transmitting to Device A.

c) C senses (hear) B's transmission to A and falsely assumes it cannot transmit, though B's transmission to D would not be interefered by B's. This leads to unnecessary delays and reduces network throughput



Q.4 Explain Bluetooth Architecture in detail.

Ans Bluetooth is a wireless technology standard, designed for short range communication between devices Typically within 10 meters. The usual data rate is 1Mbps with a 2.4 GHz bandwidth. The Bluetooth architecture is defined by 2 types of networks :-

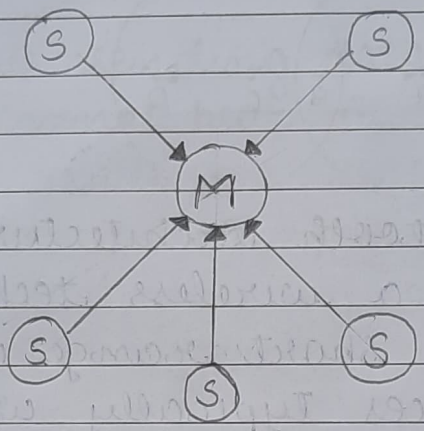
1. Piconet

A small network formed by a master device and one or more slave devices.

The Master Device, controls the network and coordinates communication. Only one master is allowed per piconet. The Slave Device, up-to 7 active devices can communicate with the master. Additional devices can be in a parked state (inactive but synchronized).

The master communicates with each

slave on a time-division duplex (TDD), meaning slaves do not directly communicate with each other. All devices in a piconet share the same frequency-hopping sequence defined by the master.

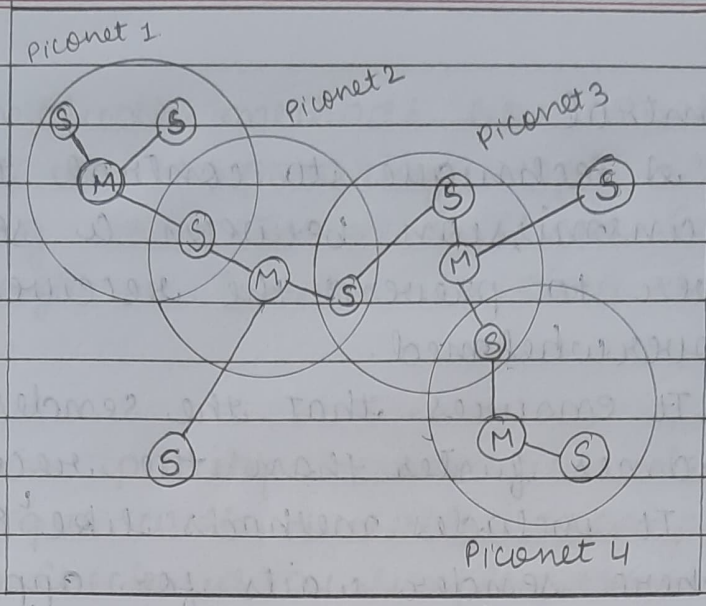


2. Scatternet

A Network formed by connecting multiple piconets, where a device (known as a bridge) belongs to two or more piconets.

* Bridge Device, that is part of more than one piconet and allows communication between them. It can act as a master in one piconet and as a slave in another. A scatternet can have multiple overlapping piconets, allowing more devices to be connected beyond the limitations of a single piconet.

Allows devices in different piconets to communicate with each other. Provides greater ~~the~~ coverage and device ~~cont~~ connectivity than a single piconet.



Q.5 Explain Scatternet with diagram.

—↳ Same answer as in Question - 4

Q.6 Discuss different services provided by data link layer.

—↳ The Data Link Layer (layer 2) in the OSI model is responsible for providing ~~effectivite~~ effective and reliable communication between devices on a network.

i) Framing.

The process of dividing the data stream into manageable units called frames.

Adds a header and trailer to each frame, which contains control information such as source / destination addresses. It helps to detect the start and end of each frame, ensuring that the ~~it~~ data is correctly interpreted by the receiver.

ii) Flow Control

A Technique to control the rate of data transmission between a sender and a receiver to prevent the receiver from being overwhelmed.

It ensures that the sender does not send frames faster than the receiver can process. It includes methods like 'Stop-and-wait', where sender waits for approval after each frame & 'sliding window', where it allows multiple frames to be sent before requiring an approval.

iii) Error Control

A service that ensures the reliable delivery of data by detecting and correcting errors.

It detects transmission errors using parity checks, checksums or CRC. It includes methods like 'ARQ (Automatic Repeat reQuest)', where it retransmits frames if errors are detected & 'FEC (Forward Error Correction)', where it corrects errors at the receiver without retransmission.

iv) Congestion Control

A service to prevent network congestion by controlling the amount of data entering by network.

It reduces congestion and packet loss.

It include methods like 'Backpressure', where it temporarily stops data transmission during congestion & 'Choke Packets', where it informs sender to slow down transmission.

Q.7 Explain parity check error detection technique with suitable example.

-> Parity Check is a simple error detection technique used to detect errors in transmitted data. It involves adding a parity bit to a data set, which helps determine whether the data has been transmitted correctly or if an error occurred during transmission.

Here, a dataword of K bits is transformed into a codeword of n bits where, $n = K + 1$. The additional bit, is calculated to ensure an Even or Odd number of 1's.

-> The Parity Check works in

i) Sender's side

* Before sending the data, it calculates the no. of 1s in the data.
* Adds a parity bit (even or odd) to ensure the total no. of 1s meets the desired parity

ii) Receiver side

- Counts the no. of 1s in the received data (including the parity bit).
- Verifies if the parity matches; if not, an error is detected.

It is very simple to implement and requires minimal hardware but it can only detect single-bit errors and it is not suitable for high-reliability applications.

eg: even parity

Dataword = 1011	
Sent codeword : 10111	Sent : 10111
received codeword : 10101	received : 00110
Result : Error detected. SINGLE BIT ERROR	Result : NO Error detected TWO BIT ERROR but the data is wrongly accepted (limitation)

Q.8 Discuss pure-ALOHA and slotted-ALOHA and describe which one is better.

—ᵛ ALOHA is a simple communication protocol used in wireless networks to control data transmission and avoid collisions when multiple devices attempt to transmit data simultaneously. There are two versions :-

1. Pure ALOHA.

A Protocol where devices transmit data whenever they have data to send.

The device transmits data at any

time, after that it waits for approval from the receiver. If a collision occurs (two devices transmitting at the same time), the data is retransmitted after a random time delay.

It has a maximum throughput of 18.4% (1/2e), meaning only about 18.4% of the time is used effectively for data transmission due to collisions. (rest is wasted).

2. Slotted ALOHA

A Protocol where time is divided into discrete slots and devices can only transmit at the beginning of each time slot.

Time is divided into equal-sized slots, so each device must wait for the beginning of the next time slot to send a packet, after that it waits for approval from the receiver. It reduces the chances of collisions since transmission only occur at slot boundaries.

It has a maximum throughput of 36.8% (1/e) because it reduces the vulnerable period for collisions by half.

-4 Slotted ALOHA is generally better because it offers higher throughout and lower collision probability by synchronizing transmissions. However, it requires time to synchronization among devices, which add complexity.

Features	Pure ALOHA	Slotted ALOHA
Transmission Time	Any Time.	At the beginning of a time slot.
Collision probability	Higher (twice the vulnerable period)	lower (reduced by half)
Throughput	up to 18.4% (1/2e)	up to 36.8% (1/e)
Synchronization	Not required	Required (devices need to be synchronized).

Q.9 Explain CRC with suitable example.

-4 Cyclic Redundacy check (CRC) is an error detection technique used to detect changes or errors in transmitted data. CRC is more reliable than methods like parity checks because it can detect multiple errors in a data frame. It is widely used in network communications, storage devices and file formats.

-4 The Process of CRC :-

i) Polynomical Representation

Data is represented as a predetermined polynomial known as the 'Generator Polynomial' which is used to divide the

data polynomial (G(x))

ii) Encoding

Append a no. of zeroes to the end of the data equivalent to the degree of G(x). Using XOR, perform binary polynomial division on the modified data with the g(x). The remainder left is CRC checksum, which is then appended to the original data to form codeword CRC.

iii) Transmission

The codeword i.e. original data + CRC checksum, is transmitted

iv) Decoding

The Receiver performs the same division on the received codeword. If remainder is zero, the data is considered error-free. If not, an error is detected.

eg: Here, $G(x) = x^3 + x + 1$

Data = 1101 (4 bits)

Now, Append 3 zeroes to data ∵ of G(x)

∴ Data = 1101000

Remainder = 001

CRC codeword = 1101001

```
        1011 | 1101000
               1011
               -----
               01100
                1011
                ----
                01110
                 1011
                 ----
                 0101
                  1011
                  ----
                  0001
```

* Now, divide again with CRC codeword, the remainder will be zero that means there is no error, data is correct.

Q.10 Explain CSMA technique with its different methods.

—↓ Carrier Sense Multiple Access (CSMA) is a network protocol used to avoid collisions in networks that share a common communication channel (like Ethernet). In CSMA, a device first 'listens' to the channel to check if its free before transmitting data. If the channel is busy, the device waits for it to become free.

i) 1-Persistent CSMA.

A Protcol where a device continuously senses the channel and transmits immediately with a probability of 1 when the channel is free.

It provides High Efficiency when the network is not heavily loaded. But it has higher collision probability when multiple devices wait for the channel to be free.

ii) Non-Persistent CSMA.

A Protcol where a device senses the channel; if busy, it waits for a random time before sensing the channel again.

It provides lower collision probability because it reduces the chance of multiple devices transmitting simultaneously. But it has lower efficiency and higher time due to random back-off periods.

iii) p-Persistent CSMA.

A protocol mainly used in slotted channels where a device senses the channel and if free, transmits with a probability 'p'. If the device decides not to transmit (with probability '1-p'), it waits for next time slot.

It offers balance between High efficiency and reduced collisions. However, it requires channel synchronization and works best in slotted systems.

iv) CSMA/CD (Collision Detection)

A Method used in wired networks (like Ethernet) where a device senses the channel and transmits if it's free. While transmitting, it continuously monitors for collisions.

If a collision is detected, the device stops transmitting and sends a jam signal to notify other devices of the collision. The device waits for a random time before reattempting to transmit.

It is efficient in detecting collisions quickly, reducing network congestion. But it is not suitable for wireless because it is difficult to detect collisions due to "hidden terminal problem".

v) CSMA/CA (Collision Avoidance)

A Method used in wireless networks (like

(Wi-Fi) where devices attempt to avoid collisions rather than to detect them.

Devices use techniques like RTS and CTS before transmitting data. A device sends an RTS signal; if it receives a CTS reply, it means the channel is free for transmission.

It reduces collisions and is more ~~reliable~~ suitable for wireless networks. But it has higher overhead due to the RTS/CTS handshake mechanism.

Q.11 Discuss ARP protocol with suitable example.

—ᵛ Same answer as in Question-1 (pg:54)

Q.12 Given the data word "101001111" and the divisor "10111", show the generation of cyclic redundancy check codeword at the sender site.

—ᵛ To generate a CRC, we use polynomial division.

Given,

> Data word = 101001111

> Divisor (1+x) = 10111

∴ Degree = 4

∴ so append 4 zeroes to data word

⇒ Data word = 101001111 0000

codeword.

```
10111 | 101001111 0000
        10111↓↓↓
        00011111
          10111↓
          01000 1
           10111↓
           00110 00
            10111↓
            01110
             10111
             01001 0
              10111
              00101
               10111
               00010
                10111
                00101
```

∴ Remainder = 0101 ; so add this to the data word to generate codeword.

→ The codeword at sender site will be, '10100111110101'.

Q.13 Explain CSMA/CD technique.

→ Same answer as in Question - 10 (pg : 69)

Q.14 Discuss types of data transmission errors. Describe the difference between error detection and error correction.

→ Data Transmission Error occur when data being sent over a network or stored in a system becomes corrupted or altered. These errors can arise from various sources, including noise, signal degradation and hardware faults.

1. Single-Bit Error

An Error where only one bit ~~is~~ in the transmitted data is altered (flipped from 0 to 1 or 1 to 0).

usually caused by ~~a~~ minor noise or interference in the communication channel. Also, it is easier to detect and correct using simple error techniques like parity checks.

For example, in a byte '10011010', a

single-bit error might change it to '10011110'.

2. Burst Error.

An Error where two or more consecutive bits in the data stream are altered.

Typically caused by prolonged interference or noise affecting multiple bits in sequence. Due to this, it is more challenging to detect and correct because multiple bits are affected. Advanced techniques like CRC or FEC are often required.

Error Detection	Error Correction
Identifying the presence of errors in transmitted data.	Identifying and correcting errors in transmitted data.
To check if data has been altered during transmission	To reconstruct the original data by correcting errors.
Requires less processing and is faster	Requires more processing and may introduce transmission delay.
Data is usually.	Errors are corrected

retransmitted if an error is detected	on the fly without the need for retransmission
Techniques used are parity checks, CRC, checksums.	Techniques used are Hamming code, Reed-Solomon, convolutional codes

Q.15 Given the data word "1001000" and the divisor "1011", show the generation of cyclic redundancy check codeword at the sender site.

→ To generate a CRC codeword with given data, we use 'polynomial division'.

Given,
Dataword = 1001000
G(x) = 1011 (degree = 3)
so, add 3 zeroes to dataword

⇒ Dataword = 1001000000

```
1011 | 1001000000
       1011
       -----
        00100 0
          1011
          ----
          00110 0
            1011
            ----
            01110
             1011
             ----
             01010
              1011
              ----
              0001
```

∴ remainder = 001

⇒ So, the codeword at the sender side is, '1001000001'.

Q.16 write a short note on reservation and polling controlled ~~ac~~ access protocols.

-4 Controlled Access Protocols are used to control how multiple devices share a common communication channel, avoiding collisions and ensuring orderly data transmission. There are two common types of CAP :-

1. Reservation Protocol.

A Protocol where devices reserve a time slot in advance for transmission to avoid collisions.

The channel is divided into fixed time slots. A device that wants to transmit data ~~re~~ sends a request to reserve a slot. Then the network grants the reservation and the device can transmit data during its allocated ~~t~~ slot.

It is efficient for networks with predictable traffic patterns and reduces collisions due to the reserved slots. However, it can be less efficient with underutilized or has bursty traffic and requires overhead to manage reservations.

2. Polling Protocol.

A Protocol where a central controller (polling master) periodically checks each device to see if it has data to send.

Here, the polling master sends a poll message to each device in turn. If the polled device has data to send, it transmits, if not, the next device is polled. (like a round-robin fashion).

It is suitable for networks with a central controller or where devices cannot detect each other's transmissions, ensuring a fair chance for all devices to transmit. However, it is inefficient in large networks with many idle devices due to the overhead of polling and may cause delays due to its sequential manner.

Q.17 Explain error detection with any one technique.

→ Same answer as in Question - 9 (pg : 66)

Q.18 Given the data word polynomial is $x^8 + x^6 + x^3 + x^2 + x + 1$ and the divisor $x^4 + x^2 + x + 1$, show the generation of cyclic redundancy check codeword at the sender site.

→ To generate a CRC codeword with given data, we use polynomial division.

Given,

Data word Polynomial = $x^8 + x^6 + x^3 + x^2 + x + 1$

Polynomial $G(x) = x^4 + x^2 + x + 1$.

$$
\begin{array}{r|l}
 & x^4+x+1 \\
\hline
x^4+x^2+x+1 & x^8+x^6+x^3+x^2+x+1 \\
 & x^8+x^6+x^5+x^4 \\
\hline
 & x^5+x^4+x^3+x^2+x+1 \\
 & x^5+x^3+x^2+x \\
\hline
 & x^4+1 \\
 & x^4+x^2+x+1 \\
\hline
 & x^2+x
\end{array}
$$

$\therefore$ remainder = x^2+x

Now, add this 'remainder' to data word.

$\therefore (x^8+x^6+x^3+x^2+x+1) \oplus (x^2+x)$

$\therefore x^8+x^6+x^3+1$

Ans → So, the codeword at the sender site is '$x^8+x^6+x^3+1$'.

Q.19 Explain CDMA channelization protocol with suitable example.

–4 Code Division Multiple Access (CDMA) is a channelization protocol that allows multiple devices to transmit simultaneously over the same frequency band. This technique is widely used in wireless communication systems like 3G, 4G and 5G. It uses a technique called spread spectrum to spread data signal across a wider bandwidth, reducing interference and increasing security.

–4 Working of CDMA :-

(i) Each device is assigned a unique spreading code (a sequence of bits).

(ii) The data signal of each device is multiplied by its unique code, spreading the signal over a wider frequency range.

(iii) All devices transmit their spread signals simultaneously over the shared channel.

(iv) The receiver uses the same unique code of the transmitting device to decode the received signal. Then the receiver can extract the desired signal from the mixture of all signals.

eg:
$U_A = [1, -1, 1, -1]$ → Data Bit = 1
$U_B = [1, 1, -1, -1]$ → Data Bit = 0
$U_C = [1, -1, -1, 1]$ → Data Bit = 1

∴
$D_A = 1 \times [1, -1, 1, -1] = [1, -1, 1, -1]$
$D_B = -1 \times [1, -1, 1, -1] = [-1, -1, 1, 1]$
$D_C = 1 \times [1, -1, -1, 1] = [1, -1, -1, 1]$

Data bit 1 is represented by '+1' and 0 by '-1'.

$\therefore S = D_A + D_B + D_C$
$= [1-1+1, -1-1+1, 1+1-1, -1-1+1]$
$= [1, -3, 1, 1]$.

Received signal for A $= S \cdot U_A$
$= [1, -3, 1, 1] \cdot [1, -1, 1, -1]$
$= (1+3+1-1)$
$= 4$ (+ve).

∴ Bit for user A is 1. (∵ 4 (+ve))
∴ Bit for user B is 0. (∵ 4 (-ve))
∴ Bit for user C is 1 (∵ 4 (+ve)).