CHAPTER 4

Modern Communication Technology

Objectives...

- To study wireless sensor network, its architecture and topologies.
- To learn about bluetooth, wi-fi and RFID protocols.
- To understand basics of Arduino platform and data acquisition system using Arduino.
- To learn the definition, characteristics, challenges and applications of IoT.

4.1 INTRODUCTION

- The rapid advancement of wireless and embedded technologies has led to the development of interconnected systems capable of sensing, communication and intelligent decision-making. This chapter provides an overview of Wireless Sensor Networks (WSNs) and their fundamental components such as sensing, actuation, network architecture and various topologies. It also introduces the types of nodes, co-ordinator, router and end device, that enable efficient data communication and network management.
- Further, the chapter discusses commonly used wireless communication protocols like Bluetooth, Wi-Fi and RFID, which form the backbone of short and medium-range wireless connectivity. The section on Data Acquisition highlights the basics of the Arduino platform, its pin configuration and its role in I/O control and data collection from sensors.
- Finally, the concept of the Internet of Things (IoT), a network of interconnected devices capable of exchanging data intelligently are discussed. It covers its definition, characteristics, challenges and real-world applications, providing learners with a foundational understanding of modern smart systems that integrate sensing, computation and communication for automation and innovation.

4.2 WIRELESS SENSOR NETWORK

- In a Wireless Sensor Network (WSN), sensing and actuation are two fundamental functions that enable monitoring and control of physical environments.

1. **Sensing:**
   - The process of collecting data from the surrounding environment using sensors.

   - Sensors convert physical quantities such as temperature, pressure, humidity, light, motion or vibration into electrical signals.
   - This sensed data is then processed and transmitted wirelessly to a base station or sink node for analysis.
   - Example: A temperature sensor measuring ambient temperature in a greenhouse.
2. **Actuation:**
   - The process of performing an action based on the sensed data or received control command.
   - Actuators convert electrical signals into physical actions, such as moving a motor, opening a valve, or turning on a fan.
   - Actuation provides a control response to the environment, forming a closed-loop system with sensors.
   - Example: If the sensed temperature exceeds a threshold, an actuator can automatically turn on a cooling system.

4.3 WSN ARCHITECTURE

- A Wireless Sensor Network (WSN) consists of a large number of spatially distributed sensor nodes that monitor physical or environmental conditions such as temperature, pressure, humidity or motion and transmit the collected data to a central location for processing and analysis.
- The basic block diagram of a WSN is shown in below Fig. 4.1.

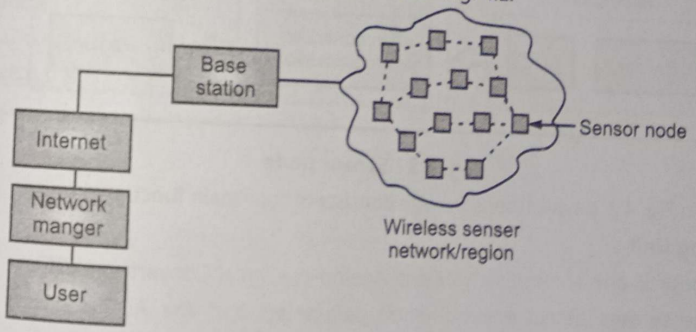

Fig. 4.1 : Basic block diagram of WSN

- As shown in Fig. 4.1, WSN architecture is generally divided into following main components:

1. **Sensor Nodes:** These are small, low-power devices equipped with sensors, processors, memory and communication modules. Their main function is to sense data from the environment and transmit it to other nodes or the base station.
2. **Base Station (BS) / Sink node:** The sink or base station acts as a central hub that collects data from various sensor nodes. It often connects the WSN to external networks like the internet or a cloud server for further processing.

3. **Gateway / Co-ordinator:** Gateway basically connects the sensor network with other communication networks. It manages network control, data aggregation and routing between the WSN and the outside world.
4. **Network Manager:** Responsible for network configuration, monitoring and maintenance. It ensures efficient routing, energy management and data synchronization among nodes.
5. **User (User Interface):** This allows end users to access and visualize the sensed data, perform analysis and control actuators remotely.

Sensor Node :

- A sensor node (also known as a mote) is the fundamental building block of a Wireless Sensor Network (WSN). It is a small, intelligent electronic device capable of sensing, processing and communicating data wirelessly. These nodes work collaboratively to monitor physical or environmental conditions such as temperature, pressure, light, sound, motion, or humidity and transmit the collected data to a base station or sink node for analysis.
- A sensor node in WSN consists of four basic components as shown in Fig. 4.2.

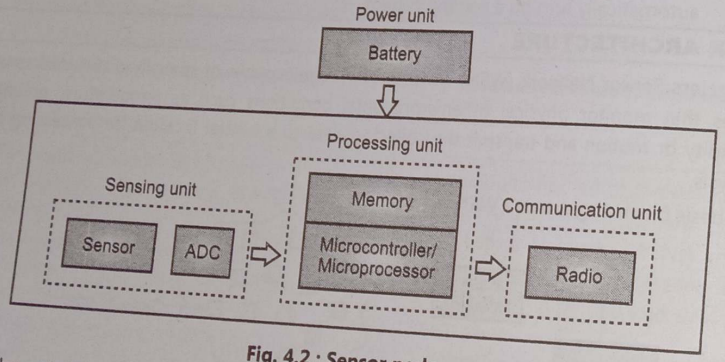

Fig. 4.2 : Sensor node

- As shown in Fig. 4.2, a typical sensor node consists of four main functional units:

(a) Sensing Unit :

- Contains one or more sensors and Analog-to-Digital Converters (ADC).
- The sensors detect environmental parameters and the ADC converts the analog signals into digital form for processing.
- Example: Temperature, humidity, gas, vibration, or light sensors.

(b) Processing Unit :

- The "brain" of the node, usually a microcontroller or microprocessor (like Atmega, ARM, or MSP430).
- Performs local computations such as data compression, aggregation and decision-making.
- Stores program code and data in memory (RAM/Flash).

(c) Communication Unit :

- Comprises a transceiver (Transmitter + Receiver) that enables wireless communication using standards like IEEE 802.15.4, Bluetooth, or Wi-Fi.
- Responsible for data transmission, reception and co-ordination with neighboring nodes.

(d) Power Unit :

- Supplies energy to all components, usually through batteries or energy harvesting sources (solar, vibration).
- Efficient power management is crucial since WSN nodes often operate in remote or inaccessible areas.

Working :

- The sensor unit senses the environmental parameter and converts it into an electrical signal.
- The ADC converts analog data received from sensor into digital data and thus digitizes this signal.
- The processing unit processes or filters the data.
- The transceiver sends the processed data to the next node or sink node.
- The power unit continuously supplies energy for the operation.

Characteristics of a Good Sensor Node :

- Low power consumption.
- Small size and lightweight.
- Scalability (can be part of a large network).
- Self-organization capability.
- Reliable and robust communication.

4.3.1 Structure of WSN Architecture

- The WSN architecture is shown in Fig. 4.3.

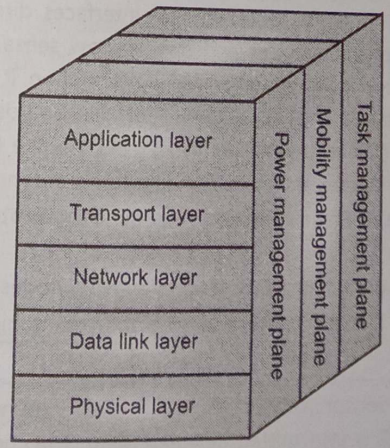

Fig. 4.3 : WSN architecture

- As shown in Fig. 4.3, WSN follows a layered communication structure similar to the OSI (Open System Interconnection) reference model, but it is optimized for low-power, distributed and data-centric communication. Each layer in the architecture performs a specific function as follows :

1. **Physical Layer :** The physical layer is responsible for the transmission and reception of raw data bits over the wireless medium. It defines how data is physically modulated and transmitted through radio waves, infrared or optical signals. It is responsible for signal modulation and demodulation, data encoding and decoding, frequency selection and channel assignment, managing energy consumption during transmission and establishing physical connectivity among sensor nodes.
2. **Data Link Layer (MAC Layer) :** The data link layer ensures reliable and energy-efficient data transfer between neighboring nodes. It manages access to the wireless communication medium and handles error detection and correction. It prevents data collision between nodes. It organizes data into frames for transmission and minimizes retransmissions.
3. **Network Layer :** This layer is responsible for routing data from sensor nodes to the base station efficiently. Since WSNs are energy-constrained, the routing algorithm must minimize power usage, balance the load and tolerate node failures. It selects optimal paths for data packets and manages dynamic network topology. It handle data aggregation (Combining similar data to reduce redundancy) and reroutes data if nodes fail or paths break.
4. **Transport Layer :** The transport layer provides end-to-end reliability and congestion control. It ensures that the sensed data reaches the base station correctly even in the presence of packet loss or network congestion. It ensures packets are received successfully. It regulates data traffic to prevent overload and retransmits lost or corrupted packets.
5. **Application Layer :** This is the top layer that interfaces directly with the end user. It provides application-specific services and defines how sensed data is represented and processed. It converts raw data into meaningful information. It tracks node health, energy and performance and displays sensor data through dashboards or IoT platforms.
6. **Management Planes (Cross-Layer Functions) :** Besides the five core layers, WSNs also include cross-layer management planes that operate across multiple layers:
   - Power Management Plane: Controls energy consumption and extends network lifetime.
   - Mobility Management Plane: Keeps track of moving nodes and adjusts routes.
   - Task Management Plane: Schedules sensing and communication tasks for efficiency.

4.4 WSN TOPOLOGIES

- A topology in a Wireless Sensor Network defines the arrangement and interconnection of sensor nodes and how data is transmitted between them. The choice of topology affects the network's performance, power consumption, scalability and fault tolerance.

The major types of WSN topologies are:

1. **Star Topology :**
   - In this topology, all sensor nodes are directly connected to a central node (often called the *co-ordinator* or *base station*). Communication occurs only between the end nodes and the central node, not between the end nodes themselves.
   - The star topology is shown in Fig. 4.4.
   - Each sensor node sends data directly to the base station, which processes or forwards it to other networks.

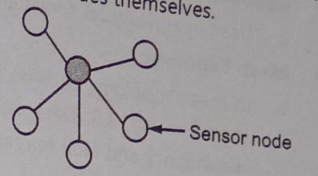

Fig. 4.4 : Star topology

Advantages :
   - Simple to design and implement.
   - Easy to manage and control.
   - Failure of one node does not affect others.

Disadvantages :
   - If the central node fails, the entire network collapses.
   - Limited range, nodes must be within direct communication distance of the base station.

Applications :
   - Used in small-scale monitoring systems such as home automation or indoor environmental monitoring.

2. **Tree Topology (Clustered or Hierarchical Topology) :**
   - This topology is an extension of the star topology, where multiple star networks are connected in a hierarchical manner as shown in Fig. 4.5. Each cluster has a cluster head that communicates with a higher-level node or the base station.

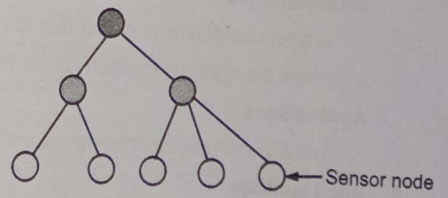

Fig. 4.5 : Tree topology

   - Sensor nodes send data to their cluster head; the cluster head aggregates and forwards the data to the sink or upper cluster head.

Advantages:
   - Scalable and suitable for large networks.
   - Reduces energy consumption through data aggregation.
   - Easier management through clustering.

Disadvantages:

- Failure of a cluster head affects all nodes within that cluster.
- Complex to configure and maintain.

Applications:

- Used in agricultural, forest and industrial area monitoring systems.

3. **Mesh Topology :**
   - In mesh topology, each node can communicate with multiple neighboring nodes as shown in Fig. 4.6. Data can take multiple paths to reach the sink node, enabling redundancy and fault tolerance.

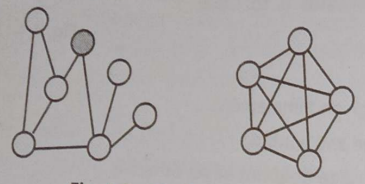

Fig. 4.6 : Mesh topology

- Nodes co-operate to relay data from one node to another using multi-hop routing until it reaches the base station.

Advantages :

- Highly reliable and fault-tolerant.
- Self-healing, if one path fails, data is rerouted automatically.
- Supports large coverage area.

Disadvantages :

- Higher complexity and cost due to multiple communication links.
- More energy consumption for routing and processing.

Applications :

- Used in military, environmental and smart city applications where reliability is critical.

4. **Bus Topology :**
   - In bus topology, all nodes are connected to a single communication line (bus) used for data transmission between nodes and the base station as shown in Fig. 4.7. Data travels along this bus from one node to the next.

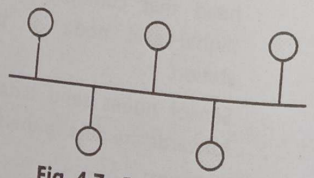

Fig. 4.7 : Bus topology

- All nodes share a common communication medium. Each node listens to the bus and transmits when the channel is free. Data packets contain destination addresses.

Advantages:

- Simple and low-cost setup.
- Easy to add new nodes.
- Efficient for small networks.

Disadvantages:

- Single point of failure (bus failure).
- Limited scalability.
- Communication collisions may occur.

Applications:

- Small-scale laboratory sensor setups.
- Industrial process monitoring.

5. **Ring Topology :**
   - In a Ring Topology, all the sensor nodes are connected in a circular manner, forming a closed loop as shown in Fig. 4.8. Each node has exactly two neighboring nodes, one on its left and one on its right and data travels around the ring in one or both directions until it reaches the destination.

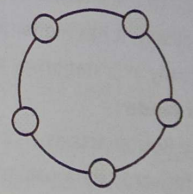

Fig. 4.8 : Ring topology

   - Each node in the ring receives data from its previous neighbor and passes it to the next node. Data flows sequentially through the network. The sink node (or base station) may be connected to any node in the ring to collect data. Some implementations allow bi-directional flow for fault tolerance.

Advantages:

- Simple and organized communication structure.
- Equal access for all nodes to the network medium.
- Reduced data collision, as data moves in an orderly way.
- Easy to install for small, circular sensor layouts.

Disadvantages:

- Single node failure can disrupt the entire communication loop.
- Data transmission delay increases with more nodes (since data travels through each).
- Difficult to reconfigure or add/remove nodes once set up.
- Less efficient for dynamic or large-scale WSNs.

Applications:

- Small or medium industrial monitoring systems arranged in circular setups.
- Pipeline or perimeter monitoring systems.
- Environmental monitoring around circular areas (e.g., volcano craters, water tanks).

4.4 TYPES OF NODES

- In a Wireless Sensor Network, nodes are classified based on their roles and functionalities in the network. The three main types of nodes are Co-ordinator, Router and End Device. Each has a specific function in data collection, processing and communication within the network.

1. **Co-ordinator Node :**
   - The Co-ordinator is the central or main controlling node in a WSN.
   - It is responsible for network formation, management and control.
   - The co-ordinator initializes the network, assigns addresses to other nodes and maintains information about the overall network topology.
   - It creates and maintains the network and stores routing and node information.
   - It manages synchronization between nodes and acts as a gateway to external networks (e.g., to the internet or base station).
   - Typically, it has higher processing power, energy supply and storage capacity.
   - Usually, it is stationary and always active.
2. **Router Node :**
   - The Router acts as an intermediate node between the co-ordinator and end devices.
   - It forwards data packets from one node to another, extending the coverage area of the network.
   - It performs routing of data between nodes and maintains information about neighboring nodes.
   - It helps in network reliability and fault tolerance by providing multiple data paths and assists in load balancing within the network.
   - It can communicate with both the co-ordinator and end devices.
   - It requires more power than end devices.
   - This node may be fixed or mobile, depending on the application.
3. **End Device (Sensor Node) :**
   - The End Device is a simple, low-power sensor node that collects environmental data (e.g., temperature, humidity, pressure).
   - It senses and transmits data to the router or co-ordinator but does not route data from other nodes.
   - It performs data sensing, processing and transmission.
   - It operates mostly in sleep mode to save energy.
   - It sends data periodically or when triggered by an event.
   - It has limited processing and communication capabilities.
   - Low energy consumption and cost-effective.
   - It communicates with only one parent node (router or co-ordinator).

Table 4.1 : Comparison of nodes

Node Type	Main Role	Power Usage	Routing Capability	Communication With	Example
Co-ordinator	Network creation, management	High	Yes	Routers and End Devices	Base station
Router	Data forwarding, routing	Medium	Yes	Co-ordinator and End Devices	Relay node
End Device	Data sensing and transmission	Low	No	Router or Co-ordinator	Temperature sensor

4.5 WIRELESS COMMUNICATION PROTOCOLS

- To communicate successfully, some guidelines must be established between the sender and the receiver. That is specific rules and procedures must be agreed upon at the transmitting and receiving ends of the communication system. These rules and procedures are called as Protocols.
- Wireless communication protocols define the rules and standards that enable electronic devices to communicate without physical connections.
- Protocols ensure reliable data transmission, synchronization and security between devices.
- Three commonly used wireless communication protocols are Bluetooth, Wi-Fi and RFID.

4.5.1 Bluetooth

- Bluetooth was invented in 1994 by Ericsson company. Bluetooth wireless technology was named after a Danish Viking and King, Harald Blatand; his last name means "Bluetooth" in English.
- Bluetooth is a short-range wireless communication technology designed for connecting electronic devices such as smartphones, laptops and headsets.
- It consumes less power and is used to communicate between mobile phones, computers and other network devices.
- It supports frequency band of 2.45 GHz and can transfer data bits upto 721 KBps (Bits per second)
- Typically, its range is up to 10 m (Class 2 devices) and up to 100 m (Class 1).
- Data rates are up to 3 Mbps (Bluetooth 2.0 + EDR) and higher in later versions (Bluetooth 5.0 > 50 Mbps).
- The architecture of Bluetooth networks is based on the concepts of Piconet and Scatternet, which define how devices connect, communicate and share data in an organized manner.

Advantages of Bluetooth :

- It eliminates the need for physical cables between devices, providing freedom of movement and reducing clutter.
- Bluetooth devices consume minimal power, making them suitable for battery-operated devices such as wireless earphones, smartwatches and sensors.

- The components and modules required for Bluetooth are inexpensive, leading to low overall implementation costs.
- Bluetooth pairing is simple and often automatic. Devices can detect each other and connect quickly within range without complex configuration.
- Bluetooth is a global standard, ensuring compatibility across a wide range of devices (smartphones, laptops, speakers, IoT devices, etc.).
- Once paired, devices can reconnect automatically when in range.
- It supports security features like authentication, encryption and authorization to protect data.
- Through Piconet and Scatternet structures, Bluetooth can connect several devices simultaneously (1 master + up to 7 active slaves per piconet).
- Capable of handling both voice and data communications, useful in applications like hands-free calling and file transfers.
- It operates in the license-free 2.4 GHz ISM band, making it accessible worldwide without regulatory issues.
- New versions of Bluetooth (e.g., Bluetooth 5.x) remain compatible with older versions, ensuring long-term device usability.

Disadvantages of Bluetooth :

- Bluetooth typically operates within 10 meters (Class 2 devices), though some high-power devices (Class 1) can reach up to 100 meters, still much less than Wi-Fi or cellular ranges.
- Compared to Wi-Fi or wired connections, Bluetooth offers lower bandwidth (Approximately 1-3 Mbps for Bluetooth 2.0 and up to 50 Mbps for Bluetooth 5), making it unsuitable for high-speed applications.
- Since bluetooth operates in the 2.4 GHz ISM band, it may face interference from other wireless technologies such as Wi-Fi, microwave ovens, or cordless phones.
- Although encryption is used, Bluetooth connections can still be vulnerable to hacking, eavesdropping, or unauthorized access if not properly secured.
- Continuous Bluetooth operation (especially with older versions) can lead to faster battery depletion in mobile devices.
- A single piconet can have only one master and up to seven active slaves, restricting scalability.
- It is not suitable for long-distance communication or large-area networks like cellular or Wi-Fi systems.
- In applications like gaming or real-time video, Bluetooth may introduce noticeable delay (latency) between input and output.

Bluetooth Piconet :

- A Piconet is the basic unit of Bluetooth networking, formed when two or more Bluetooth devices are connected in an adhoc manner within a common radio range.
- The term "Piconet" comes from 'pico' meaning "small", thus, it represents a small wireless network.

- In a Piconet, one device acts as the Master and up to seven active devices act as Slaves as shown in Fig. 4.9.
- The Master device controls the communication, timing and frequency hopping pattern.
- Slave devices synchronize to the master's clock and frequency hopping sequence.
- Additional devices can remain in a parked or standby mode, ready to join when needed.

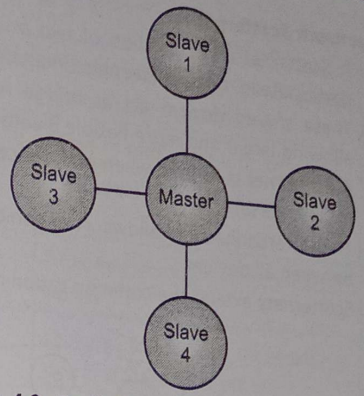

Fig. 4.9 : Typical bluetooth piconet with one master and four slaves (Star topology)

Working of a Piconet :

- When two Bluetooth devices discover each other, one becomes the Master and the other(s) become Slaves.
- Slaves synchronize their clocks and frequency hopping sequences with the Master.
- The Master controls all communication using Time Division Multiplexing (TDM).
- Each Slave is assigned a specific time slot for data exchange.
- No direct communication occurs between Slaves , all data passes through the Master.
- When communication ends, devices can leave the Piconet and either become Masters of new Piconets or remain idle.

Advantages of Piconet :

- Simple and low-power communication setup.
- Flexible, can connect different types of Bluetooth devices (phones, speakers, laptops, sensors).
- Supports both voice and data transmission.
- Dynamic, devices can easily join or leave the network.

The description of Piconet in summarised form is given in below table.

Table 4.2

Parameter	Description
Maximum Active Devices	8 (1 Master + 7 Slaves)
Communication Range	Typically 10 m (can extend up to 100 m)
Topology Type	Star topology
Frequency Band	2.4 GHz ISM Band
Access Technique	Time Division Duplex (TDD) and Frequency Hopping Spread Spectrum (FHSS)

Bluetooth Scatternet :

- A Scatternet is a collection of two or more interconnected Piconets where certain devices participate in multiple Piconets simultaneously as shown in Fig. 4.10.
- These shared devices act as bridge nodes, enabling data transfer between Piconets and allowing larger and more flexible Bluetooth networks.
- A Scatternet is formed when one device acts as a Slave in one Piconet and Master in another (or vice versa).
- This interconnection allows communication across multiple Piconets without direct links between all devices.
- Scatternets extend the communication range and increase network capacity.

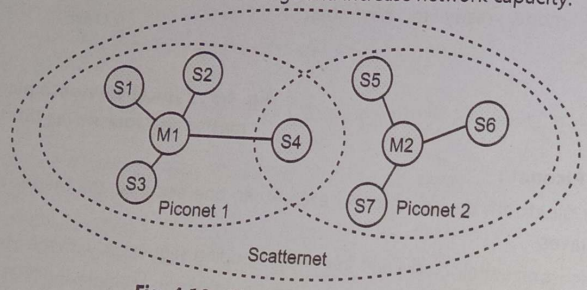

Fig. 4.10 : Bluetooth scatternet

Working of a Scatternet :

- Two or more Piconets form independently.
- A device common to both networks (bridge device) connects them.
- Each Piconet maintains its timing and frequency hopping pattern independently.
- The bridge device switches between the two time slots of different Piconets.
- Data transfer between devices in different Piconets occurs via the bridge node.
- The bridge handles synchronization and avoids interference between networks.

Advantages of Scatternet :

- Supports large-scale Bluetooth networks by linking multiple Piconets.
- Increases coverage area and number of devices that can communicate.
- Enhances network flexibility and data sharing across multiple devices.
- Enables multi-hop communication, improving range and efficiency.

The description of Scatternet in summarised form is given in below table.

Table 4.3

Parameter	Description
Number of Devices	More than 8 (multiple Piconets combined)
Network Type	Multi-hop, mesh-like structure
Role Switching	Devices can act as Master in one and Slave in another Piconet
Communication Control	Each Master controls its own Piconet

Comparison between Piconet and Scatternet :

Feature	Piconet	Scatternet
Definition	Basic Bluetooth network with 1 Master and up to 7 Slaves	Combination of multiple Piconets through common devices
Topology	Star topology	Mesh or multi-hop topology
Number of Devices	Maximum 8 active	More than 8 (multiple Piconets)
Communication Range	Limited (10-100 m)	Extended through interconnected nodes
Device Roles	Fixed (1 Master, others Slaves)	Dynamic (device can be Master in one and Slave in another)
Data Sharing	Within one Piconet	Across multiple Piconets
Complexity	Simple	More complex synchronization and scheduling

Applications:

- Wireless audio devices (headphones, speakers).
- File transfer between mobile devices.
- Internet of Things (IoT) smart gadgets.

4.5.2 Wi-Fi (Wireless Fidelity)

- Wi-Fi is a high-speed wireless networking technology based on the IEEE 802.11 family of standards.
- It provides broadband access by connecting devices such as computers, smartphones and IoT devices to a wireless router or access point.
- It uses frequency bands of 2.4 GHz and 5 GHz, with 6 GHz for Wi-Fi 6E.
- Data rate ranges from 11 Mbps (802.11b) to multi-Gbps (Wi-Fi 6 and 7).
- Coverage range is typically 30-100 m indoors.
- It supports multiple users and high-data applications like video streaming and VoIP.

Types of Wi-Fi Connections :

(a) Based on IEEE Standards :

- Wi-Fi is a wireless networking technology based on the IEEE 802.11 family of standards, enabling devices to communicate over local area networks (LANs) without physical cables.
- Wi-Fi connections can be categorized based on network modes, frequency bands and IEEE standards used.
- Each type determines the speed, range and application of the wireless connection.
- Wi-Fi has evolved through various generations, each defined by an IEEE 802.11 standard.

Table 4.4 : Major types of Wi-Fi

Wi-Fi Standard	Frequency Band	Maximum Data Rate	Approx. Range	Remarks / Features
802.11a	5 GHz	54 Mbps	35 m indoors	High speed, less interference, short range
802.11b	2.4 GHz	11 Mbps	38 m indoors	Longer range, more interference
802.11g	2.4 GHz	54 Mbps	38 m indoors	Backward compatible with 802.11b
802.11n (Wi-Fi 4)	2.4 & 5 GHz	600 Mbps	70 m indoors	MIMO technology introduced
802.11ac (Wi-Fi 5)	5 GHz	1.3 Gbps	35 m indoors	Uses MU-MIMO, high data rate
802.11ax (Wi-Fi 6)	2.4 & 5 GHz	9.6 Gbps	70 m indoors	High efficiency, better coverage in crowded areas
802.11be (Wi-Fi 7)	2.4, 5 & 6 GHz	Up to 46 Gbps	100 m indoors	Next-gen with multi-link operation and wider channels

(b) Wi-Fi Based on Operating Modes :

- Wi-Fi networks can also be classified based on how devices are connected and communicate.

(i) Infrastructure Mode :

- This is the most common mode used in homes, offices and public hotspots.
- Devices (clients) connect to a central Access Point (AP) such as a Wi-Fi router.
- The AP manages communication between all connected devices and the Internet.
- It is reliable and easy to manage.
- It enables connection to wired networks and the Internet.
- Examples are, Laptop, smartphone and printer connected via a Wi-Fi router.

(ii) Ad-Hoc Mode (Peer-to-Peer Mode) :

- In Ad-Hoc mode, devices communicate directly with each other without an access point.
- They form a temporary wireless network between two or more devices.
- Examples are, file transfer between two laptops or mobile phones directly via Wi-Fi.
- For this mode, no router or infrastructure required.
- It is quick and has simple setup.
- It has limited range, no Internet access through this network and less security.

(iii) Mesh Mode :

- In this mode, multiple Wi-Fi nodes (routers) work together to form a mesh network.
- Each node acts as both a transmitter and receiver, forwarding data to other nodes until it reaches its destination.

- If one node fails, data is rerouted through another path, improving network reliability and coverage.
- It is used in Smart homes, campus networks and city-wide Wi-Fi.
- It has large coverage area, self-healing network.
- It is ideal for IoT and smart environments.

(iv) Hotspot / Infrastructure BSS (Basic Service Set) :

- A Wi-Fi hotspot provides Internet access to the public through an Access Point.
- It is common in cafes, airports and hotels.
- It operates in Infrastructure mode, where the Access Point connects users to the Internet via a service provider.

(v) Wi-Fi Direct :

- It enables device-to-device communication similar to Bluetooth, but with higher speed.
- Devices connect directly without an AP, using Wi-Fi Protected Setup (WPS) or PIN authentication.
- Example are, wireless printing or media sharing between smartphones and smart TVs.

(vi) Enterprise Mode :

- It is used in corporate and institutional networks.
- Employs 802.1X authentication (via RADIUS server) for secure login and encryption.
- It provides better control, monitoring and access management than home networks.

(c) Wi-Fi based on Frequency Bands :

- Wi-Fi operates in three major frequency bands:

1. **2.4 GHz Band :**
   - Greater range but prone to interference.
   - Used by Wi-Fi 4 (802.11n) and earlier versions.
   - Suitable for low-speed and long-range applications.
2. **5 GHz Band :**
   - Higher data rate, less interference, but shorter range.
   - Used by Wi-Fi 5 and Wi-Fi 6.
3. **6 GHz Band (Wi-Fi 6E / Wi-Fi 7) :**
   - Newest band with higher bandwidth and reduced congestion.
   - Ideal for streaming, gaming and VR applications.

(d) Wi-Fi Based on Networks Coverage Area :

Table 4.5 : Types of Wi-Fi based on network coverage area

Type	Full Form	Coverage Area	Use Case
WLAN	Wireless Local Area Network	Within a building (up to 100 m)	Homes, offices
WMAN	Wireless Metropolitan Area Network	Up to 50 km	City-wide Wi-Fi
WWAN	Wireless Wide Area Network	Nationwide	Cellular Internet, hotspots
WPAN	Wireless Personal Area Network	Few meters	Bluetooth, Wi-Fi Direct

4.5.3 Radio Frequency Identification (RFID)

- Radio Frequency Identification (RFID) is a technology used for wireless identification and tracking of objects using radio waves.
- RF controllers have been well known for many years. They offer transmission rate upto 115 K bit/s (wireless extension of serial interface) and operate on many different ISM bands (depending on national regulations e.g. 27, 315, 418, 426, 433, 868, 915 MHz).
- The first RFID emerged during the 1980. In the beginning, these very cheap tags were used for asset tracking only. As soon as a product with RFID tag passed a reader, the product was registered. Now-a-days, RFIDs are available in dozens of different styles with different properties.
- RFIDs can respond to a radio signal and transmit their tag. They can store additional data, employ collision avoidance schemes and comprise smart card capabilities with simple processing power.
- RFID system comprises three main components:
  1. Reader (Interrogator) – Transmits radio signals.
  2. Tag (Transponder) – Stores data and responds to the reader.
  3. Antenna – Facilitates signal exchange between reader and tag.
- RFID operates across different frequency ranges —
  - Low Frequency (LF): 125–134 KHz
  - High Frequency (HF): 13.56 MHz
  - Ultra-High Frequency (UHF): 860–960 MHz

Types of RFID :

- RFID (Radio Frequency Identification) systems can be classified based on several criteria such as power source, frequency of operation and communication mechanism.

(A) Types Based on Power Source of Tag :

- The most common classification is based on the power source of the tag, which determines the range, cost and application area.

1. **Passive RFID System :**
   - The passive tag does not contain any internal power supply.
   - It receives energy from the RF field emitted by the RFID reader.
   - The induced current powers the microchip in the tag, which modulates the backscattered signal to send data back to the reader.
   - Its operating frequency is , LF (125-134 KHz), HF (13.56 MHz), or UHF (860–960 MHz).
   - It has limited storage (typically a few kilobytes).
   - Its lifespan is practically unlimited (no battery to replace).

   Advantages:
   - Inexpensive and lightweight.
   - Maintenance-free (no battery).
   - Long life and suitable for harsh environments.

   Disadvantages:
   - Short read range (a few centimeters to a few meters).
   - Requires strong reader signal for activation.
   - Limited data storage and read speed.

   Applications:
   - Access control systems.
   - Library book tracking.
   - Retail inventory management.
   - Smart cards (metro cards, ID badges).
2. **Active RFID System :**
   - An active RFID tag has an internal battery that powers both the microchip and the transmitter.
   - The tag actively emits radio signals, which can be detected by a reader over long distances.
   - Its operating frequency is usually UHF (433 MHz or 2.45 GHz).
   - It has memory larger than passive tags, it can store detailed data.
   - It has limited lifespan (battery lasts 3-5 years depending on use).

   Advantages:
   - Long reading range (up to 100 meters or more).
   - Can monitor environmental parameters (temperature, motion).
   - Fast and reliable communication.

Disadvantages:

- Higher cost due to battery and electronics.
- Larger size and limited battery life.
- Not suitable for small items or disposable use.

Applications:

- Vehicle tracking and toll collection (e.g., FASTag).
- Real-time location systems (RTLS).
- Cargo and container tracking in logistics.
- Military asset tracking.

3. **Semi-Passive (Battery-Assisted Passive) RFID System :**
   - A semi-passive tag contains a small battery that powers only the tag's microchip (not the transmitter).
   - It uses backscatter to communicate with the reader, similar to a passive tag.
   - The battery helps improve sensitivity and reliability of communication.
   - Its operating frequency is usually UHF.
   - Battery used to activate chip and sensors.
   - It has range longer than passive but shorter than active.

Advantages:

- Moderate cost compared to active tags.
- Better performance and reliability than passive tags.
- Can include sensors for temperature, humidity etc.

Disadvantages:

- Battery limits life expectancy.
- Slightly larger and more expensive than passive tags.

Applications:

- Environmental monitoring.
- Asset tracking in warehouses.
- Supply chain management for perishable goods.

Comparison between Types of RFID :

Feature	Passive RFID	Semi-Passive RFID	Active RFID
Power Source	None (Reader-powered)	Battery (Chip only)	Battery (Chip + Transmitter)
Range	Up to 10 m	Up to 30 m	Up to 100 m
Data Storage	Limited	Moderate	High
Cost	Low	Medium	High
Maintenance	None	Battery replacement	Battery replacement
Applications	Retail, access control	Cold chain, environment monitoring	Vehicle and asset tracking

[B] Classification Based on Frequency Range :

- RFID systems also differ depending on the operating frequency band, which affects read range, data rate and interference characteristics as shown in below Table 4.6.

Table 4.6

Frequency Band	Range	Read Distance	Typical Applications
Low Frequency (LF) (30-300 KHz, typically 125 KHz)	Short	< 10 cm	Animal tracking, access control
High Frequency (HF) (13.56 MHz)	Medium	< 1 m	Library systems, contactless cards
Ultra-High Frequency (UHF) (860-960 MHz)	Long	1-12 m	Logistics, inventory, vehicle tracking
Microwave (SHF) (2.45 GHz, 5.8 GHz)	Very long	> 10 m	Active RFID, toll collection

[C] Classification Based on Communication Mechanism :

- RFID systems can also be categorized based on how the tag communicates with the reader as shown in below Table 4.7.

Table 4.7

Type	Description	Example
Full Duplex (FDX)	Tag and reader communicate simultaneously	LF animal identification tags.
Half Duplex (HDX)	Reader and tag communicate alternately	UHF passive systems.
Sequential (SEQ)	Tags respond in sequence to avoid collision	Multi-tag environments.

Block Diagram of RFID :

- An RFID system mainly consists of three components, RFID Tag (Transponder), RFID Reader (Interrogator) and Antenna as shown in Fig. 4.11.

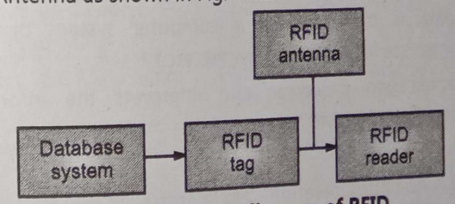

Fig. 4.11 : Block diagram of RFID

Main Components of RFID :

(a) RFID Tag (Transponder) :

- The tag is attached to the object to be identified.
- It consists of a microchip that stores data (such as an ID number or product information) and an antenna for communication.
- Depending on its power source, the tag may be passive, active, or semi-passive.

(b) RFID Reader (Interrogator) :

- The reader emits radio frequency signals through its antenna to detect nearby tags.
- It also receives the response signals from the tags and converts them into digital data.
- The reader is connected to a host computer or network for data processing and management.

(c) Antenna :

- The antenna establishes the communication link between the tag and the reader.
- It transmits RF waves to power the tag (in case of passive tags) and receives the backscattered signal containing information from the tag.

Working :

- The operation of an RFID system is as follows:
  - The RFID reader continuously transmits electromagnetic waves using its antenna.
  - When a passive RFID tag enters this field, the RF energy induces an electric current in the tag's antenna coil through electromagnetic induction.
  - This energy powers the microchip embedded in the tag.
  - In active tags, this step is not required as the tag has its own battery.
  - Once activated, the tag sends data back to the reader using backscatter modulation (in passive tags) or active radio transmission (in active tags).
  - The tag's microchip modulates the reflected signal to include its stored identification data.
  - The reader receives the backscattered or transmitted signal through its antenna.
  - The reader's receiver section demodulates and decodes the data embedded in the signal.
  - The information typically contains the Unique Identification Number (UID) and other stored details.
  - The decoded data is then sent to a computer system or database through a communication interface (USB, Wi-Fi, Ethernet, etc.).
  - The software application processes and interprets the information for tracking, verification, or inventory purposes.

Advantages of RFID :

1. Non-contact and Automatic Operation – No line-of-sight required.
2. High Speed and Efficiency – Can read hundreds of tags simultaneously.
3. Rewritable Memory – Data can be updated or modified.
4. Durable and Long-Lasting – Tags can withstand harsh environments.
5. Enhanced Security – Can use encryption and authentication features.
6. Improved Inventory Accuracy – Real-time tracking and visibility of assets.
7. Wide Range of Applications – From retail and logistics to healthcare and defense.

Disadvantages of RFID :

1. High Initial Cost – Tags and readers are costlier than barcodes.
2. Signal Interference – Metal surfaces and liquids can cause signal distortion.
3. Privacy Concerns – Tags can be read without user consent.
4. Reader Collisions – Multiple readers can interfere with each other.
5. Limited Standardization – Compatibility issues between manufacturers.
6. Power Requirement (for active tags) – Batteries need replacement or maintenance.

Applications of RFID :

1. Supply Chain Management: Tracking goods and shipments in real-time.
2. Retail Industry: Inventory management and theft prevention.
3. Access Control: Employee ID cards and secure entry systems.
4. Transportation: Electronic toll collection (e.g., FASTag).
5. Healthcare: Tracking medical equipment, patients and pharmaceuticals.
6. Libraries: Book tracking and automated checkout.
7. Livestock and Agriculture: Animal identification and health monitoring.
8. Aviation: Baggage and cargo tracking.
9. Smart Cards and Payments: Contactless credit cards and metro passes.

Comparison of Bluetooth, Wi-Fi and RFID :

Feature	Bluetooth	Wi-Fi	RFID
Range	10-100 m	30-100 m	Up to several meters
Frequency Band	2.4 GHz	2.4 GHz / 5 GHz / 6 GHz	LF / HF / UHF
Data Rate	Up to 50 Mbps	Up to 10 Gbps	Low (KHz - MHz)
Main Function	Device-to-device communication	Internet and local networking	Object identification and tracking
Typical Applications	Audio, IoT, file sharing	Internet access, streaming	Logistics, access control

4.6 DATA ACQUISITION - BASICS OF ARDUINO

- Arduino is an open source electronics platform, which consists of hardware and software.
- Arduino is simple and accessible to all the users. With the help of Arduino, different types of projects and applications can be constructed.
- Software used for Arduino is easy, flexible. It can run on Mac, Windows and Linux.
- Various sensors such as light sensor, temperature sensor etc. can be connected to Arduino and also it can provide output which can activate motor or LED.
- With the help of set of instructions, Arduino can be programmed as per the need of an application.

- Basically, Arduino is an easy tool for fast prototyping for the students without a background of programming and Electronics.
- Arduino can be used for the applications based on IoT, wearable, 3D printing and for development of embedded systems.
- All Arduino boards are totally open-source, works independently. Software used for it is also open source.

Features of Arduino:

- Arduino boards are inexpensive compared with other microcontroller platforms. Arduino software that is Integrated Development Environment (IDE) is easy to use and flexible.
- Most of the microcontroller systems work with Windows. Arduino software (IDE) runs on windows, Macintosh OSX and on Linux operating system.
- Arduino software is an open source tool that means user/experienced programmers can upgrade it. User can add AVR-C code directly into Arduino programs.
- The Arduino boards are published under a Creative Common license, so experienced programmers/designers can expand it, can make their own version of module, extend it and improve it.
- Arduino boards can read analog/digital input signals from various sensors and provide output based on a particular program.
- Ardunio does not require any programmer to program it. With the help of USB cable, program can be loaded into Arduino.
- Arduino IDE uses a simplified version of C++ which is easy to learn.
- Arduino provides a standard form factor which can break the functions of microcontroller into accessible packages.

4.6.1 Arduino Uno Board Pin Configuration

- Arduino Uno is the most popular board in the Arduino family. Majority of the components of all the Arduino boards are same.
- Arduino Uno board is based on 8-bit ATmega328p microcontroller.
- It consists of other components such as crystal oscillator, serial communication, voltage regulator etc. to support the microcontroller.
- Arduino Uno has 14 digital input/output pins out of which 6 pins can be used as PWM outputs, 6 analog input pins, USB connection. It also has a power barrel jack, an ICSP header and reset button on the board.
- Fig. 4.12 shows the Arduino Uno board.

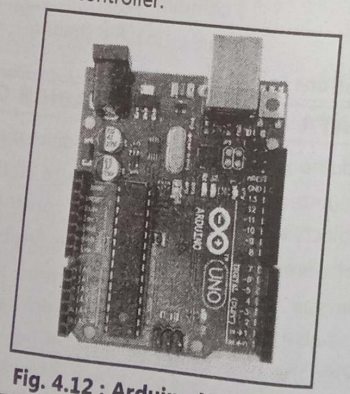

Fig. 4.12 : Arduino Uno board

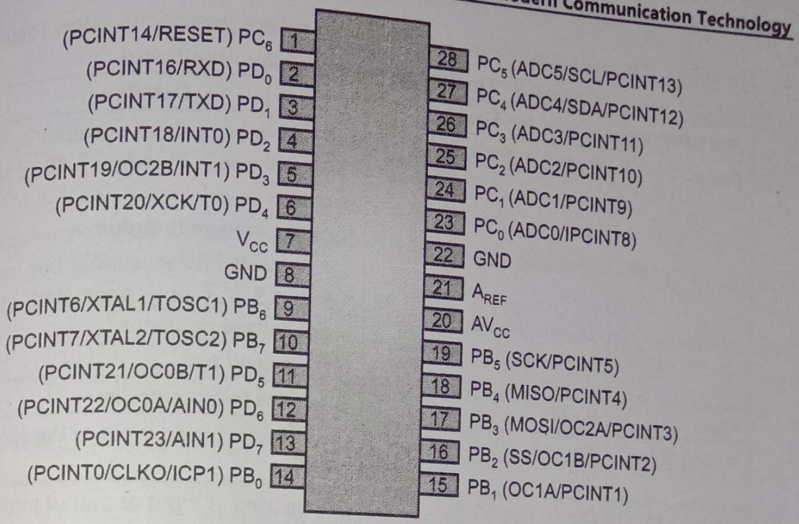

Fig. 4.13 : Pin configuration of Arduino Uno

Table 4.8

	Arduino Function		Arduino Function
Pin 1	Reset	Pin 15	Digital pin 9 (PWM)
Pin 2	Digital pin 0 (RX)	Pin 16	Digital pin 10 (PWM)
Pin 3	Digital pin 1 (TX)	Pin 17	Digital pin 11 (PWM)
Pin 4	Digital pin 2	Pin 18	Digital pin 12
Pin 5	Digital pin 3 (PWM)	Pin 19	Digital pin 13
Pin 6	Digital pin 4	Pin 20	V_{cc}
Pin 7	V_{cc}	Pin 21	Analog reference
Pin 8	GND	Pin 22	GND
Pin 9	Crystal	Pin 23	Analog input 0
Pin 10	Crystal	Pin 24	Analog input 1
Pin 11	Digital pin 5 (PWM)	Pin 25	Analog input 2
Pin 12	Digital pin 6 (PWM)	Pin 26	Analog input 3
Pin 13	Digital pin 7	Pin 27	Analog input 4
Pin 14	Digital pin 8	Pin 28	Analog input 5

- The details of the pins available on Arduino Uno board are given in the below Table 4.9.

Table 4.9 : Pin description of Arduino Uno board

Pin Category	Pin Name	Details
Power	V_{in}, 3.3 V, 5 V, GND	Arduino board can be powered by using the USB cable through USB port of computer. V_{in}: Input voltage to Arduino. 5 V: Regulated power supply 3.3 V: 3.3 V supply generated by on-board voltage regulator. GND: ground pins.
Reset	Reset	Resets the microcontroller.
Analog Pins	A0 - A5	Can provide analog input in the range of 0-5 V.
Input/Output Pins	Digital Pins 0 - 13	Can be used as input or output pins.
Serial	0(R_x), 1(T_x)	Used to receive and transmit TTL serial data.
External Interrupts	2, 3	To trigger an interrupt.
PWM	3, 5, 6, 9, 11	Provides 8-bit PWM output.
SPI	10 (SS), 11 (MOSI), 12 (MISO) and 13 (SCK)	Used for SPI communication.
Inbuilt LED	13	To turn ON the inbuilt LED.
TWI	A4 (SDA), A5 (SCA)	Used for TWI communication.
AREF	AREF	To provide reference voltage for input voltage.

4.6.3 I/O Control and Data Acquisition using Arduino

- Any devices or peripheral can be connected to Arduino through analog and digital pins. The analog signal can have any number of values. It is continuously changing signal.
- Digital signal can have only two values either high or low.
- Arduino has in-built ADC (Analog to Digital Converter). The ADC has 10-bit resolution and it can return integers from 0 to 1023. Sensors which have analog output can be connected to Arduino. The ADC converts the analog signal into digital signal. The function analogRead(pin) is used to obtain the value of analog signal. Here pin is the pin number where analog input is connected. This function converts the analog voltage on the specified analog input pin and returns a digital value from 0 to 1023 relative to the reference value. The default reference voltage is 5 V for Arduino boards which are operating on 5 V.

- Arduino does not have built-in DAC (Digital to Analog Converter). However, Arduino can use pulse width modulation (PWM) and obtain digital signal. The function used to output PWM signal is analogWrite(pin,value). Here pin is the pin number used for the PWM output and value is a number proportional to duty cycle of the signal. When value = 0, the signal is always OFF, when value = 255 the signal is always ON.
- The PWM function is available on the pins 3, 5, 6, 9, 10 and 11 on most of Arduino boards.
- The frequency of the PWM signal is approximately 490 Hz. Arduino Uno board uses pin 5, 6 and have 980 Hz frequency.
- To map the analog input, values ranges from 0 to 1023 to a PWM output signal which ranges from 0 to 255, map (value, from Low, from High, to Low, to High) function is used. This function has five parameters, one is the variable which has analog value and other are 0,1023,0 and 255 respectively.
- Brightness of LED can be controlled using this technique with the help of potentiometer.
- In Arduino, analog pins are used as an input pins where input devices such as sensors can be connected and digital pins are used as output pins where output devices such as LED, buzzer can be connected.
- Before using a digital pin, it has to be set in input/output mode using pinMode() command.
- Digital pin can also be used in input mode.

Difference between Digital and Analog Pins of Arduino :

- Arduino Uno has 14 digital input/output pins, out of which, 6 pins can be used as PWM outputs and 6 analog input pins.
- The function digitalRead() works on all pins on Arduino Uno board. digitalRead() will round the received analog value.
- digitalWrite() allows digital parameter such as 0 or 1.
- analogRead() is used only for analog pins. It can accept value between 0 and 1023.
- The analog pins read the values from the input devices such as sensors and give a range of voltages between 0 and 5 which can be measured with the help of multimeter.
- Analog pins send pulses of 0 V and 5 V to get an output which is similar to analog that is PWM. PWM is like a pseudo-analog signal.
- To have response as 0 or 1 digitalRead() is used and to read sensor analogRead() is used.
- analogWrite() can be used for all analog pins and all digital PWM pins. The value between 0 and 255 can be used.
- Analog read is very slow; however it is very accurate and precise.
- Analog pins take input in the form of analog signal and return values between 0 and 1023. Arduino Uno has in-built 10-bit ADC which does this conversion.
- ADC of Arduino Uno works in 3 stages - Sampling, Quantization and Digitization.

- The summary of the analog, digital and PWM pins is given in below Table 4.10.

Table 4.10

Pin Type	Quantity	Function
Digital I/O Pins	14 (0-13)	Used for digital input or output (HIGH/LOW)
Analog Input Pins	6 (A0-A5)	Used to read analog voltage values (0-5V)
PWM Pins	6 (3, 5, 6, 9, 10, 11)	Generate analog-like signals using Pulse Width Modulation

4.6.3.1 I/O Control using Arduino

Digital Input Control:

- It is used to read the state of devices such as push buttons, IR sensors, or switches. Each digital pin can detect two states: HIGH (1) → 5V and LOW (0) → 0V

Example Code: Reading a Button Input

```
int buttonPin = 2;
int buttonState = 0;

void setup() {
  pinMode(buttonPin, INPUT);          // Set pin 2 as input
  Serial.begin(9600);
}

void loop() {
  buttonState = digitalRead(buttonPin);      // Read input
  Serial.println(buttonState);
  delay(100);
}
```

Digital Output Control :

- It is used to control external devices such as LEDs, buzzers, or relays. By writing a HIGH or LOW signal to a pin, Arduino can turn a device ON or OFF.

Example Code: Controlling an LED

```
int ledPin = 13;

void setup() {
  pinMode(ledPin, OUTPUT);          // Set pin 13 as output
}
```



```
void loop() {
  digitalWrite(ledPin, HIGH);          // LED ON
  delay(1000);
  digitalWrite(ledPin, LOW);           // LED OFF
  delay(1000);
}
```

Analog Output (PWM) Control :

- Arduino cannot produce true analog voltage output, but it can simulate analog behavior using Pulse Width Modulation (PWM).
- PWM changes the duty cycle of a square wave to vary the average voltage supplied to devices such as motors or LEDs.

Example Code: Adjusting LED Brightness

```
int ledPin = 9;
int brightness = 0;

void setup() {
  pinMode(ledPin, OUTPUT);
}

void loop() {
  for (brightness = 0; brightness <= 255; brightness++) {
    analogWrite(ledPin, brightness);
    delay(10);
  }
}
```

4.6.3.2 Data Acquisition using Arduino

- Data Acquisition (DAQ) involves measuring physical quantities like temperature, light intensity, or distance using sensors, converting them into electrical signals and then reading them using the Arduino's Analog-to-Digital Converter (ADC).

(a) Analog Input Reading :

- The Arduino Uno has a 10-bit ADC, which converts analog signals (0-5V) into digital values ranging from 0 to 1023.
- Each analog pin (A0-A5) can be used to acquire analog signals from sensors.

Example Code: Reading from a Temperature Sensor (LM35)

```
int sensorPin = A0;
float temperature;
```

```
void setup() {
  Serial.begin(9600);
}

void loop() {
 int sensorValue = analogRead(sensorPin);                  // Read analog voltage
 temperature = (sensorValue * 5.0 * 100.0) / 1023.0;       // Convert to °C
 Serial.print("Temperature: ");
 Serial.print(temperature);
 Serial.println(" °C");
 delay(1000);
}
```

Examples : Arduino program is always run on IDE (Integrated Development Environment).

Steps to Run the Program on Arduino are as follows:

1. Take Arduino Uno board.
2. Install Arduino programmer (IDE).
3. Install USB drivers.
4. Connect Arduino board to the computer through USB cable.
5. Set the board type and the serial port in the Arduino IDE.
6. Open example program, upload it and observe output.

- New program can be written and can be pasted in IDE.
- The program consists of five parts; header describing the sketch, declaration of variables, initial conditions if any, main code. Arduino program is called as sketch. All sketches must include the setup and loop functions.

Example 1- LED Blinking

LED can be made ON/OFF continuously. The code to blink LED is given below:

```
void setup()
{
// initialize digital pin LED_BUILTIN as an output.
pinMode(LED_BUILTIN, OUTPUT);
}
// the loop function runs over and over again forever

void loop()
```



```
{
digitalWrite(LED_BUILTIN, HIGH);
// turn the LED on (HIGH is the voltage level)
delay(1000);
digitalWrite(LED_BUILTIN, LOW);                    // wait for a second
// turn the LED off by making the voltage LOW
delay(1000);
}                                                  // wait for a second
```

After running this program, LED will turn ON and OFF with delay of 1 msec.

Example 2- Push Button Interfacing

The push button connects two points in a circuit when it is pressed.

Any device connected to it will be turned ON/OFF using this switch.

Below example will turn ON the LED when the push button is pressed.

At pin 13 of Arduino, LED is connected and at pin 7 push button is connected.

The code to make LED ON/OFF using push button is given below:

```
intledPin =13;                    // LED is connected to pin 13
intledPin =7;                     // Pushbutton is connected to pin 7
intval =0;                        // variable to read input status
void setup()
{
pinMode(ledpin, OUTPUT);          // Declare LED as OUTPUT
pinMode(ledpin, INPUT);           // Declare Pushbutton as INPUT
}

Void loop()
{
Val =digitalRead(ledPin);         // read input value
If(val== HIGH)                    //check if input is High (push button released)

{
Val =digitalWrite(ledPin, LOW);   // turn LED off.
}
else
```

```
{
digitalWrite(ledpin, High);          //turn LED ON
}
}
```

After running the program, when push button is pressed, LED will turn ON and when it is released, LED will turn OFF.

4.7 INTRODUCTION TO IOT

- In the decade of years 1990 to 2000 Internet connectivity began to proliferate in enterprise and consumer markets, but was still limited in its use because of the low performance of the network interconnectivity.
- From year 2000, Internet connectivity goes superior for many applications.
- Today many options are available to get internet connectivity not only in office, home but at in pocket with smartphone, laptop, etc.
- Everyone is aware of use of internet with connectivity for world wide web browsing and lot of information is available for many enterprise, industrial and consumer products, government services, educational services and many more.
- Now, the concept of Internet of Things (IoT), which is an interconnected network of machines and applications is used in daily routine of everyone's life.
- IoT is a network between objects other than computer machine. Here objects means, the things that are used in our daily life like Tube light, Fridge, Air conditioner, Automotive car, Microwave oven, Smart TV and many more.
- In simple language, the network controlling functions of these things related with their interdependence automatically is nothing but IoT. It does not have any dependency on internet connectivity that are using for browsing.
- Some practical examples of IoT are Smart refrigerators, which not only inform you about the consumed items or empty bottles in the fridge but also order them online before they runs out.
- The automotive companies like Ford, Tesla has already stepped into the world where Car would also be the part of IoT. Tesla car is really a big achievement in this field. Imagine that, a car automatically opens the garage door before you arrive at home and you can remotely control the temperature, lights, charging of the car. The car can upgrade itself automatically by downloading and installing the latest firmware and software. It has 18 sensors to automate the things and it can fix a service schedule at the car service station by itself.
- A very popular device, the Smart Phones, are the most common example of IoT. The Smart Phone is one of the first few "Things" in the 'Internet of Things', because through various APP we can have remote controls on smart TV, Air conditioner, LCD projector, Wi-Fi digital sound system etc.

4.7.1 Definition of IoT

- The Internet of Things (IoT) refers to a network of interconnected physical devices, such as sensors, home appliances, vehicles, machines and other embedded systems that are equipped with electronics, software, sensors and connectivity features enabling them to collect, exchange and act on data over the Internet without requiring direct human intervention.
- In simple terms, IoT connects the physical world with the digital world, allowing devices to sense, communicate and respond intelligently to their environment.

Evolution of IoT :

- Kevin Ashton is an innovator and consumer sensor expert who coined the phrase "the Internet of Things" to describe the network connecting objects in the physical world to the Internet.
- Kevin Ashton is accredited for using the term "Internet of Things" for the first time during a presentation in 1999.
- He believes the "things" aspect of the way we interact and live within the physical world that surrounds us needs serious reconsideration, due to advances in computing, Internet and data generation rate by smart devices.
- Year wise evolution of IoT can be stated in brief as below.
  - In 1997, "The Internet of Things" is the seventh in the series of ITU Internet Reports originally launched in 1997 under the title "Challenges to the Network".
  - In 1999, Auto-ID Center founded in MIT.
  - In 2003, EPC Global founded in MIT.
  - In 2005, important technologies of the Internet of Things was proposed in WSIS conference.
  - In 2008, First international conference of Internet of Things : The IoT 2008, was held at Zurich.
  - As of 2013, the vision of the Internet of Things has evolved due to a convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanical systems (MEMS).
  - Here after the traditional fields of embedded systems, wireless sensor networks, control systems, automation including home and building automation and others all contribute to enabling the Internet of Things (IoT).
  - Now a day's IoT network give more value to the need for everywhere, anywhere and autonomous networks of objects of which identification and service integration have an important predictable role.
  - Advantages of IoT are improved communication between the devices, automation and various controls made possible, it saves time and off course money.
  - There are some disadvantages also, like complexity of systems, privacy and secrecy of transmission of data, compatibility of software and hardware for servicing of systems.

4.7.2 Characteristics of IoT

- The Internet of Things (IoT) has several defining characteristics that make it a powerful and transformative technology.
- These characteristics describe how IoT devices operate, communicate and add value to human life and industrial processes.

Characteristics of IoT :

- All IoT devices are interconnected through the Internet or other communication networks.
- It enables data sharing between devices, cloud platforms and applications.
- IoT devices have sensors that detect and measure physical parameters such as temperature, light, pressure, motion or humidity.
- These sensors convert real-world information into digital data for processing.
- IoT systems can analyze and act on data in real time.
- This enables immediate responses, such as triggering alarms or controlling machines automatically.
- IoT networks can easily expand by adding more devices without affecting overall performance.
- IoT systems use data analytics and AI to make intelligent decisions automatically.
- IoT devices from different manufacturers can communicate and work together using standard protocols and interfaces.
- As devices are connected to the Internet, data security and privacy are major considerations.
- Encryption, authentication and secure communication channels are essential.
- IoT devices are designed to consume minimal power for long-term operation, especially in remote or battery-powered applications.
- IoT allows users to monitor and control devices from anywhere using a smartphone or computer.
- IoT systems often use cloud computing to store and process large volumes of sensor data.
- The cloud enables advanced analytics and machine learning for better decision-making.

4.7.3 Challenges of IoT

- As the improvement in electronics field and internet connectivity there is large scope of business in IoT applications.
- With business in IoT applications there are certain challenges in developing any system or products by using IoT.
- These challenges can be of two types one may be in IoT system only and other in business kind of challenges.
- Development, production, implementation and successful servicing maintenance facilitate, competition for same parallel products in market are business kind of challenges in IoT applications.

- In point view of IoT itself there are challenges like Power or Energy, Efficient resource management, Things to cloud communication, Internet availability resources miniaturization, big data analytics, semantic technologies, Back up information, Virtualization, Privacy, Security, Heterogeneity, Dynamics, Scalability etc.
- Challenges are discussed below :

1. **Security and Privacy :**
   - One of the biggest challenges in IoT is security and privacy.
   - IoT devices collect and exchange sensitive data (like health, location, or financial information).
   - Without proper security measures, this data is vulnerable to hacking, unauthorized access and misuse.
   - Example: Smart home cameras being hacked to access live video streams.
2. **Interoperability and Standardization :**
   - IoT devices come from various manufacturers and often use different communication protocols.
   - Lack of common standards makes it difficult for devices to communicate with each other.
   - Example: A smart bulb from one brand may not work with a voice assistant from another brand.
3. **Data Management and Storage :**
   - IoT devices generate large amounts of data continuously.
   - Managing, processing and storing this big data requires powerful cloud infrastructure and analytics tools.
   - Inefficient data handling can lead to slow performance or loss of important information.
4. **Power Consumption :**
   - Many IoT devices are battery-operated and deployed in remote areas.
   - Ensuring long battery life and energy efficiency is a major concern.
   - Example: Environmental monitoring sensors in forests need to operate for months or years without battery replacement.
5. **Connectivity and Network Issues :**
   - IoT relies on stable Internet or wireless networks for communication.
   - In rural or remote regions, poor network coverage can cause data loss or delayed communication.
   - Example: Smart agriculture systems may fail to transmit sensor data due to poor signal strength.
6. **Cost of Implementation :**
   - The initial setup cost of IoT (devices, sensors, networks, cloud services) can be high.
   - This is a major barrier for small businesses and developing regions.
   - Example: Installing industrial IoT systems for predictive maintenance requires expensive sensors and software.

7. **Scalability :**
   - As the number of IoT devices increases, managing them becomes more complex.
   - The system must scale efficiently without performance degradation.
   - Example: A smart city with thousands of devices must handle massive real-time data traffic smoothly.
8. **Data Accuracy and Reliability :**
   - IoT systems depend on sensor data. Faulty or poorly calibrated sensors can lead to inaccurate or misleading data.
   - Example: A malfunctioning temperature sensor in a cold storage unit can spoil food if it sends wrong readings.
9. **Maintenance and Upgradation :**
   - IoT devices need regular software updates and maintenance to remain secure and functional.
   - Managing updates for thousands of devices across different locations is difficult.
10. **Ethical and Legal Issues :**
    - IoT data collection raises ethical questions about user consent and surveillance.
    - Governments and companies must follow data protection laws such as GDPR.
    - Example: Tracking wearable devices collecting personal health data without user awareness.

4.7.3 Applications of IoT

- Today IoT is used in Wearable, Smart Home Applications, Health Care, Smart Cities, Agriculture, Industrial Automation etc.
- Smart Cities where parking, lightning, water and waste management, fire smoke detection, buildings, citizens' safety services, physical city assets monitoring etc. are integrated through IoT.
- Smart Rural Communities and Smart Residential Communities are linked by IoT.
- Smart Tourist destinations are scheduled and operated through IoT.
- Other IoT applications are in Smart Port, Smart Airport and Smart Railway Stations.
- Smart Transportation where Co-operative Intelligent Transport Systems, Automotive Emergency Response systems are implemented through IoT.
- In transportation, IoT has role in Transportation Safety Services, Unmanned Aircraft Systems and Autonomous Driving etc.
- Smart Retail networks with the help of IoT are developed.
- In agriculture, Smart farming, Agriculture planning - cultivation, Livestock like poultry etc. are linked and monitored by IoT.
- As an industrial application, smart manufacturing with framework in the context of Industrial IoT is applied.

Wearable like smart bracelet, smart glasses, smart clothing, smart ring using IoT are used by us for E-health monitoring, security, safety etc.

Similarly IoT has applications in Smart Environmental Monitoring, monitoring and study of Global Processes of the Earth for disaster preparedness, Micro-Grids and Advanced Metering

Infrastructure, Connected Home Networks, Smart Education and many other smart applications.

Exercise

[A] Multiple Choice Questions:

[I] Choose the most correct alternative for each of the following and rewrite the sentence.

1. A Wireless Sensor Network (WSN) consists of a large number of ..... nodes.
   (a) Wired (b) Sensor
   (c) Mobile (d) Optical
2. The main function of sensing in WSN is to .....
   (a) Transmit data (b) Collect data from the environment
   (c) Store data (d) Route data
3. In a WSN, actuation refers to .....
   (a) Controlling the physical environment (b) Measuring voltage
   (c) Data transmission (d) Amplifying signals
4. The WSN architecture typically consists of .....layers.
   (a) Two (b) Three
   (c) Four (d) Five
5. Which of the following is not a topology used in WSN?
   (a) Star (b) Mesh
   (c) Tree (d) Ring
6. In a star topology, all nodes communicate through .....
   (a) Router (b) Co-ordinator
   (c) End device (d) Gateway
7. The Co-ordinator node in WSN is responsible for .....
   (a) Generating data (b) Managing the network and routing
   (c) Acting as a power supply (d) Only sensing data
8. The Router node in WSN .....
   (a) Directly interfaces with sensors (b) Forwards data between nodes
   (c) Acts as a storage unit (d) Controls actuation devices only
9. The End Device in WSN performs .....
   (a) Network management
   (b) Data sensing and communication with router
   (c) Routing decisions
   (d) System configuration
10. WSNs are widely used in .....
    (a) Gaming (b) Environmental monitoring
    (c) Cooking (d) Multimedia design
11. Bluetooth operates in the ..... frequency band.
    (a) 900 MHz (b) 2.4 GHz
    (c) 5 GHz (d) 10 GHz

12. A Bluetooth piconet can connect up to ..... active devices.
(a) 3 (b) 5
(c) 8 (d) 10

13. A Bluetooth scatternet is formed when .....
(a) A single master connects to one slave (b) Multiple piconets interconnect
(c) A device disconnects from the network (d) All devices go into sleep mode

14. Wi-Fi is based on the IEEE ..... standard.
(a) 802.11 (b) 802.15.4
(c) 802.16 (d) 802.20

15. Wi-Fi mainly operates in which frequency bands?
(a) 2.4 GHz and 5 GHz (b) 1 GHz and 3 GHz
(c) 900 MHz and 2 GHz (d) 10 GHz and 15 GHz

16. RFID stands for .....
(a) Radio Frequency Identification
(b) Remote Frequency Information Device
(c) Radio Frequency Intelligent Data
(d) Real Field Information Device

17. RFID uses ..... to transfer data.
(a) Visible light (b) Infrared rays
(c) Radio waves (d) Sound waves

18. Which of the following is a type of RFID tag?
(a) Active tag (b) Passive tag
(c) Semi-passive tag (d) All of the above

19. In active RFID, the tag is powered by .....
(a) External reader (b) Internal battery
(c) Magnetic field (d) Solar energy

20. RFID is mainly used for .....
(a) File compression (b) Object tracking and identification
(c) Power transmission (d) Audio communication

21. Arduino boards are based on ..... microcontrollers.
(a) PIC (b) AVR
(c) ARM (d) 8051

22. The analog input pins on Arduino are labeled as .....
(a) D0-D13 (b) A0-A5
(c) I0-I5 (d) P0-P5

23. The process of collecting data from sensors is called .....
(a) Actuation (b) Transmission
(c) Data acquisition (d) Coding

24. IoT stands for .....
(a) Internet over Transmission (b) Internet of Things
(c) Internal Operating Technology (d) Interlink of Terminals

25. The IoT is mainly based on ..... communication.
(a) Human-to-human (b) Machine-to-machine
(c) Human-to-machine (d) Manual data transfer

26. Which of the following is not a characteristic of IoT?
(a) Connectivity (b) Scalability
(c) Manual operation (d) Real-time data

27. The main challenge in IoT is .....
(a) Slow processing (b) Data security and privacy
(c) Simple hardware (d) Limited sensors

28. IoT devices are identified uniquely by .....
(a) Serial port (b) IP address
(c) MAC address only (d) GPS location

29. IoT has wide applications in .....
(a) Smart homes (b) Smart agriculture
(c) Smart cities (d) All of the above

30. In IoT, actuators are responsible for .....
(a) Storing data (b) Performing physical actions
(c) Collecting sensor data (d) Routing packets

Answers

1. (b)	2. (b)	3. (a)	4. (d)	5. (d)	6. (b)
7. (b)	8. (b)	9. (b)	10. (b)	11. (b)	12. (c)
13. (b)	14. (a)	15. (a)	16. (a)	17. (c)	18. (d)
19. (b)	20. (b)	21. (b)	22. (b)	23. (c)	24. (b)
25. (b)	26. (c)	27. (b)	28. (c)	29. (d)	30. (b)

[II] True or False :

1. A Wireless Sensor Network consists of interconnected sensor nodes that can collect and transmit data.
2. The function of actuation in WSN is to sense the environment.
3. The WSN architecture consists of physical, data link, network, transport and application layers.
4. In star topology, each node communicates directly with every other node.
5. The mesh topology provides high reliability and redundancy in communication.
6. In a WSN, the Co-ordinator node is responsible for collecting data from sensors.
7. Router nodes forward data between other nodes in the network.
8. End devices in WSN only sense or collect data from the environment.
9. WSNs are generally used for short-range communication only.
10. Environmental monitoring and smart agriculture are applications of WSN.
11. Bluetooth operates in the 5 GHz frequency band.
12. A Bluetooth piconet consists of one master and up to seven active slave devices.

13. A Bluetooth scatternet is formed by interconnecting multiple piconets.
14. Wi-Fi is based on IEEE 802.11 standard.
15. RFID stands for Radio Frequency Identification.
16. In RFID, data is transmitted using optical signals.
17. Passive RFID tags have an internal power source.
18. Active RFID tags can transmit data over longer distances than passive tags.
19. RFID is commonly used for inventory tracking and access control systems.
20. The analog input pins on Arduino are labeled as A0 to A5.
21. The digital pins on Arduino can be used for both input and output operations.
22. The function analogRead() is used to read digital data from a pin.
23. In Arduino, data acquisition refers to collecting data from sensors.
24. Data acquisition is the process of manually entering data into a computer.
25. Sensors and actuators are integral components of a data acquisition system.
26. In IoT, actuators are used for sensing environmental conditions.
27. IoT systems can face challenges related to data security and privacy.
28. IoT applications include smart homes, smart cities and healthcare systems.
29. IoT devices use the Internet to exchange data in real time.
30. Scalability and intelligence are key features of IoT networks.

Answers

1. True	2. False	3. True	4. False	5. True	6. False
7. True	8. True	9. False	10. True	11. False	12. True
13. True	14. True	15. True	16. False	17. False	18. True
19. True	20. True	21. True	22. False	23. True	24. False
25. True	26. False	27. True	28. True	29. True	30. True

[III] Fill In The Blanks :

1. The process of measuring environmental parameters such as temperature, humidity, or pressure is called .....
2. The process of performing a physical action in response to sensed data is called .....
3. The ..... of WSN is responsible for the transmission and reception of raw bitstreams over a physical medium.
4. The ..... provides the interface between the user and the network.
5. In a ....., all nodes communicate through a central co-ordinator.
6. In a ....., nodes are connected in a multi-hop manner for improved reliability.
7. The node that manages network formation and communication is known as the .....
8. The node that forwards data between devices and extends network range is called a .....
9. Bluetooth is a short-range wireless communication protocol that operates in the ..... ISM band.

10. A piconet in Bluetooth consists of one master device and up to ..... slave devices.
11. A network formed by interconnecting multiple piconets is called a .....
12. Wi-Fi operates based on the ..... standard.
13. ..... RFID tags have an internal battery to power the circuit.
14. Arduino is an ..... hardware and software platform used for building electronic projects.
15. Each IoT device is uniquely identified using an .....

Answers

1. Sensing	2. Actuation	3. physical layer
4. application layer	5. star topology	6. mesh topology
7. Co-ordinator	8. Router	9. 2.4 GHz
10. Seven	11. Scatternet	12. IEEE 802.11
13. Active	14. open-source	15. IP address

[B] Short Answer Questions :

1. What is a Wireless Sensor Network (WSN)?
2. Define sensing and actuation in WSN.
3. Mention the main components of a sensor node.
4. Explain the role of the physical layer in WSN.
5. What is the function of the data link layer in WSN architecture?
6. Describe the purpose of the network layer in WSN.
7. What is the application layer responsible for in WSN?
8. Differentiate between star and mesh topologies in WSN.
9. What is the advantage of using tree topology in a sensor network?
10. What is a bus topology in WSN?
11. List any three applications of WSN.
12. State the frequency band used by Bluetooth.
13. Define a piconet and scatternet in Bluetooth communication.
14. List any two advantages and disadvantages of Bluetooth.
15. Mention the commonly used frequency bands for Wi-Fi.
16. Write any two advantages of Wi-Fi networks.
17. Differentiate between active and passive RFID tags.
18. What are the main components of an RFID system?
19. What is the frequency range used by RFID systems?
20. Name the microcontroller used in the Arduino Uno board.
21. What are the key characteristics of IoT?
22. Mention any two major challenges faced in IoT implementation.
23. Give any two examples of IoT applications in daily life.
24. State any two advantages of using IoT in healthcare systems.

[C] Long Answer Questions :

1. Explain the concept of Wireless Sensor Networks (WSN). Describe their key components and applications.
2. Describe the WSN architecture in detail with a neat block diagram and explain the function of each layer.
3. What are the different WSN topologies? Explain each with advantages and limitations.
4. Define and differentiate between the Co-ordinator, Router and End Device nodes in a WSN.
5. Compare star, tree, mesh and bus topologies used in WSN
6. What is a piconet and scatternet in Bluetooth? Explain their formation and significance with diagrams.
7. Write the advantages and disadvantages of Bluetooth technology.
8. What is RFID technology? Explain its components and working with the help of a neat block diagram.
9. Compare active, passive and semi-passive RFID tags in terms of operation, power and applications.
10. Compare Bluetooth, Wi-Fi and RFID technologies in terms of range, frequency band and typical applications.
11. Explain how Arduino can be used for real-time data acquisition from sensors and control of actuators.
12. Explain analog and digital I/O pins of Ardinuo Uno.
13. Define IoT and explain its basic working principle with the help of a simple diagram.
14. List the key characteristics of IoT and explain how each contributes to its functionality.
15. What are the major challenges in IoT development and implementation? Explain any four in detail.
16. List the applications of IoT in healthcare, agriculture and smart cities.
17. Explain the concept of sensing and actuation in WSN with suitable examples.
18. Explain the working of a sensor node with a labeled block diagram and describe the function of each unit.
19. Differentiate between piconet and scatternet.
20. List advantages and disadvantages of Bluetooth technology.

Syllabus ...

1. Introduction to Communication System (6 Hours)

- **Introduction to Communication System:** Elements of digital communication system (block diagram and explanation).
- **Characteristics of Communication Channel:** Signal, Signal types, Signal bandwidth, Channel bandwidth, Signal to noise ratio, Noise figure, Data rate, Baud rate, Channel capacity, Shannon-Hartley theorem. (Definition only).
- **Signal encoding:** Types of signal encoding formats, M-ary coding (Concept level),
- **Error Handling Codes:** Necessity of error control codes, Types of error handling codes, Hamming code (Error detection and correction).
- **Modulation and Demodulation:** Definition of modulation and demodulation, Need of modulation, Classification of Modulation.

2. Digital Modulation, Multiplexing and Spread Spectrum Techniques (8 Hours)

- **Pulse Modulation:** Nyquist sampling theorem, PCM (Transmitter and receiver block diagram, Advantages, disadvantages and application), Concept of Delta modulation and Adaptive delta modulation.
- **Digital Modulation Techniques:** ASK, PSK (Concept, waveform and application), FSK, QPSK, (Transmitter end block diagram, working, waveforms, application), 4-QAM (Phaser Diagram, constellation diagram and application.)
- **Multiplexing Techniques:** Necessity of signal multiplexing, FDM, TDM, CDM, OFDM (Conceptual diagram and working).
- **Spread Spectrum Techniques:** Introduction to Spread Spectrum (SS), Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), Pseudo-random (PN) sequence.

3. Cellular and Satellite Communication (8 Hours)

- **Cellular Communication:** Cell and cellular telephony, Frequency reuse and hand-off, LTE, UMTS, 4G, 5G architecture network, Handovers in 5G, Future generation 6G.
- **Types of Antennas:** Working principle of dipole antenna and patch antenna.
- **Concept of Smart Antennas:** Importance and block diagram of MIMO, Concept of MU-MIMO and Massive MIMO.
- **Satellite Communication:** Segments, Orbits, Uplink and downlink (Block diagram and frequencies), and Applications.

4. Modern Communication Technology (8 Hours)

- **Wireless Sensor Network:** Sensing & Actuation (Concept only), WSN Architecture, WSN topologies, Types of nodes (Co-ordinator, Router and End Device).
- **Wireless Communication Protocols:** Bluetooth, Wi-Fi & RFID.
- **Data Acquisition**: Basic of Arduino platform (Pin diagram and significance of each pin), I/O control and data acquisition using Arduino.
- **Introduction of IoT:** Definition, Characteristics, Challenges and IoT applications.