CONTENTS

LEARNING OBJECTIVES

After studying this chapter, you will be able to:

1- Define what a wireless sensor network (WSN) is and list its main components.

2- Distinguish between different types of wireless ad hoc and sensor networks (MANET, VANET, WSN, WBAN, etc.).

3- Describe the typical hardware and software architecture of a sensor node.

4- Explain how communication works in WSNs, including topologies and the three-tier model (node-to-node, nodes-to-sink, sink-to-cloud).

5- Identify key constraints (energy, processing, memory) and how they affect design.

6- List common applications of WSNs, especially in medical and environmental fields.

1 INTRODUCTION

Wireless Sensor Networks (WSNs) are everywhere around us. They consist of many small, battery-powered devices called sensor nodes that work together to monitor the physical world. These nodes measure things like temperature, sound, motion, or air quality and send the data wirelessly to a central point where it can be analyzed and used.

What makes WSNs special is that they are self-organizing. You can drop hundreds of nodes in a field, a forest, or a building, and they will automatically form a network without any wires or human help. This flexibility allows us to monitor places that were previously hard to reach or too expensive to wire.

We will explore the different types of wireless ad hoc and sensor networks, look inside a sensor node, understand how they communicate, and see real-world applications—from healthcare to smart cities. By the end, you will have a solid foundation for designing or working with these powerful systems.

2 TYPES OF WIRELESS AD HOC & SENSOR NETWORKS

2.1 IMPORTANT DEFINITIONS

Ad Hoc Network: A wireless network formed spontaneously without pre-existing infrastructure (no base stations, access points, or central controllers). Nodes self-organize to establish communication; the topology may change dynamically due to mobility or failures.

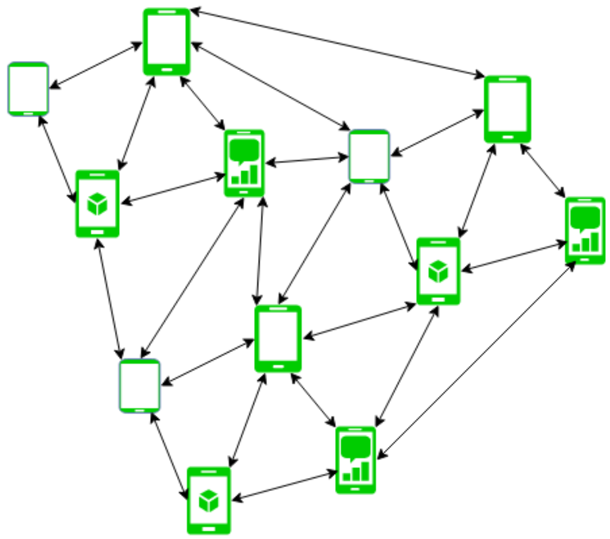

Figure 1: Ad hoc Networks

Multi-Hop Communication: A method where data packets traverse multiple intermediate nodes (hops) to reach the destination. It extends coverage beyond the direct radio range and reduces transmit power per node. Multi-hop is commonly used in ad hoc networks but can also appear in infrastructure networks (e.g., wireless mesh backhaul).

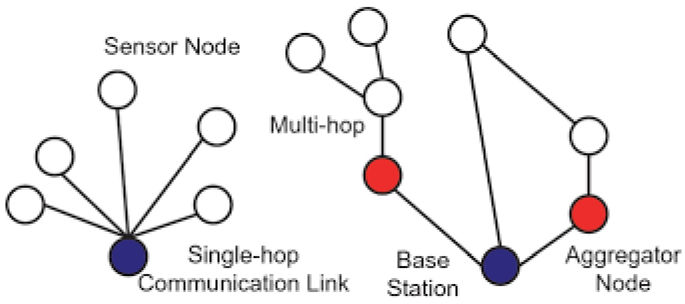

Figure 2: Single and multi-hop networks

Infrastructure Network: A network that relies on fixed, pre-deployed infrastructure such as access points, base stations, or switches (e.g., Wi-Fi with routers, cellular networks). Ad hoc networks operate without such infrastructure.

Self-Organizing: The ability of nodes to automatically discover neighbors, establish routes, and reconfigure the network without manual intervention.

Below are the main types, each with its full name and a description.

2.2 WSN – WIRELESS SENSOR NETWORK

A network of spatially distributed, low-power sensor nodes that monitor physical or environmental conditions (e.g., temperature, pressure, motion). Data is forwarded wirelessly, often via multi-hop, to a sink (gateway). Nodes are typically static, energy-constrained, and self-organizing.

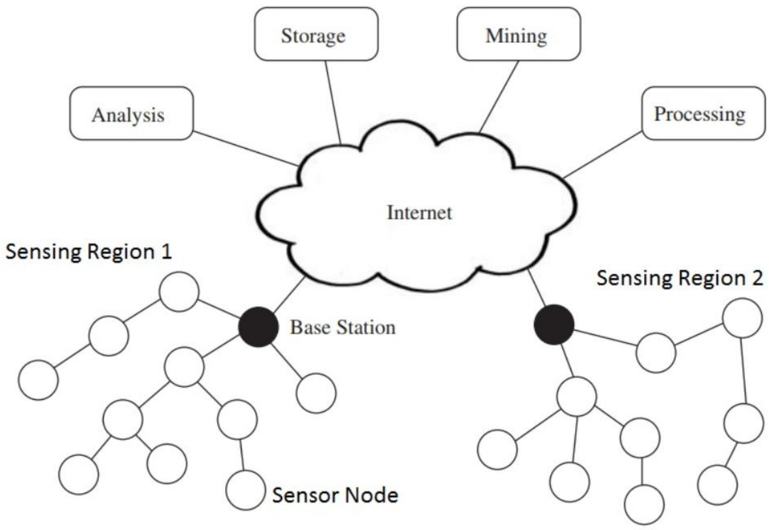

Figure 3: Typical Wireless Sensor Networks.

2.3 MANET – MOBILE AD HOC NETWORK

A self-configuring network of mobile devices (laptops, smartphones, tablets) that communicate without fixed infrastructure. Nodes act as both hosts and routers; the topology changes frequently due to node mobility.

A real-world example of a MANET (Mobile Ad Hoc Network):

- **Military battlefield communication**, where soldiers, vehicles, and drones form a decentralized network on-the-fly to exchange data without relying on fixed infrastructure.

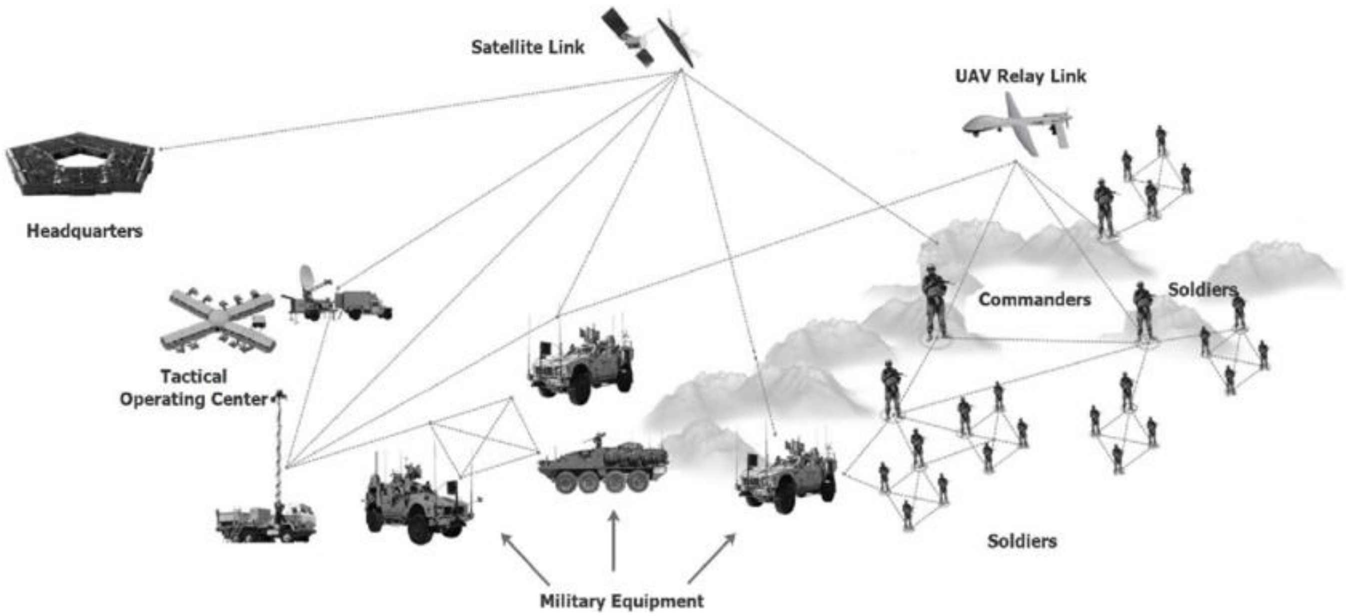

Figure 4: MANET for military applications.

- **Disaster Management/Emergency Services:** Following a earthquake or flood, search-and-rescue teams establish instant, spontaneous communication networks (MANET) between vehicles, handheld units, and UAVs (drones) when conventional cellular infrastructure has failed

2.4 VANET – VEHICULAR AD HOC NETWORK

A specialized MANET for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. It enables safety applications, traffic efficiency, and infotainment. Characterized by high mobility, predictable movement (roads), and often assisted by roadside units.

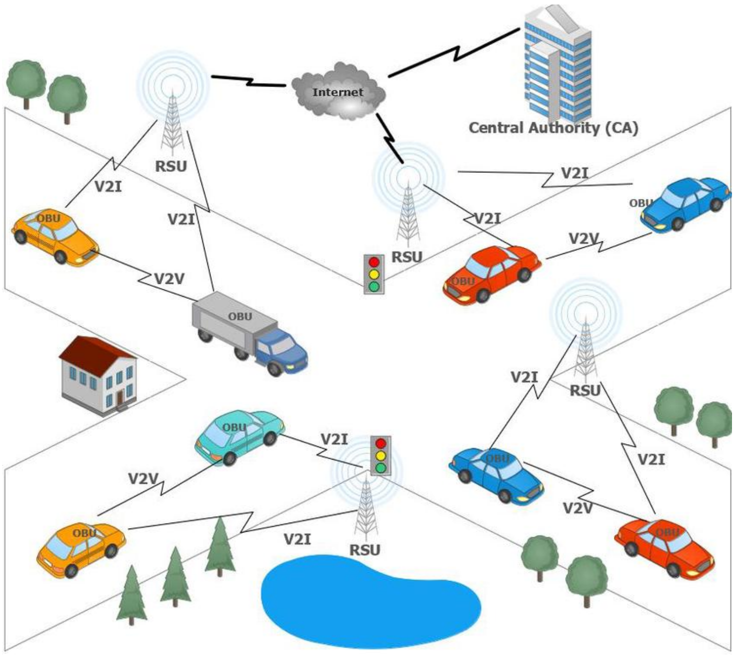

Figure 5: Vehicular Ad Hoc Network.

2.4.1 COMPONENTS OF VANET

- **On-Board Units (OBU):** Devices inside vehicles that process data and communicate.
- **Roadside Units (RSU):** Static infrastructure nodes placed along roads to extend network range.

2.4.2 PRIMARY VANET APPLICATIONS

1. **Safety-Oriented Applications:** Aim to reduce accidents and fatalities. Examples include collision alerts, blind-spot warnings, emergency electronic brake lights, and hazard warnings.
2. **Traffic Management (Efficiency):** Optimize traffic flow, reduce congestion, and provide real-time updates on road conditions.
3. **Comfort & Infotainment:** Provide internet access, electronic toll collection, parking management, and Peer-to-Peer (P2P) data sharing for passengers.

2.5 FANET – FLYING AD HOC NETWORK

An ad hoc network composed of unmanned aerial vehicles (UAVs or drones). Nodes communicate wirelessly in three-dimensional space with intermittent connectivity; used in surveillance, search and rescue, agriculture, and drone swarms.

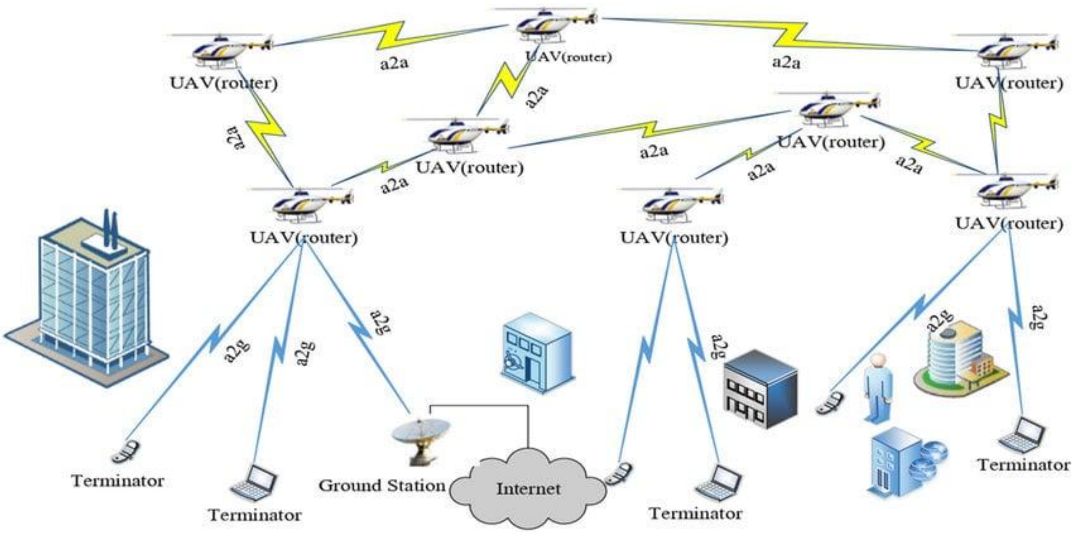

Figure 6: Flying Ad Hoc Network.

2.5.1 APPLICATIONS OF FANETS

FANETs are used in various civilian, commercial, and military applications

- **Search and Rescue (SAR):** Drones can quickly scan vast, inaccessible areas, locate victims using thermal cameras, and establish communication links when ground networks are damaged.
- **Disaster Management:** Used for monitoring forest fires, floods, or earthquakes, providing real-time data to ground controllers.
- **Smart Agriculture & Forestry:** UAVs monitor crop health, mapping areas for expansion, and perform precision spraying.

- **Military & Border Patrol:** Swarms of drones can be used for surveillance, reconnaissance, and protecting borders.
- **Traffic Monitoring & Management:** Drones monitor traffic in real-time, detect accidents, and assist in managing traffic flow, especially in urban areas.
- **Environmental Monitoring:** Sensors equipped on UAVs measure pollution levels, track wildlife, or monitor climate change.
- **Communication Relay:** Acting as aerial base stations to provide connectivity to IoT devices or to extend the range of ground-based communication networks (5G/6G)

2.6 WMN – WIRELESS MESH NETWORK

A multi-hop network where dedicated mesh routers form a resilient wireless backbone. Clients connect to these routers; the network self-heals by rerouting around failures. May include gateways to the Internet. Often infrastructure-oriented but can be self-forming.

2.7 WBAN – WIRELESS BODY AREA NETWORK

A network of sensors placed on, in, or around the human body, typically communicating with a central hub (e.g., smartphone). Used for healthcare monitoring, with strict requirements for reliability, low power, and data privacy.

2.7.1 APPLICATIONS OF WBAN

- **Medical/Health Monitoring:** Remote health monitoring for chronic diseases (cardiovascular, asthma), computer-assisted rehabilitation, and early detection of medical conditions.
- **Non-Medical:** Real-time streaming of biometrics, gaming, secure authentication using biometric patterns, and tracking physical activity

- **Military/Defense:** Monitoring the health and vital signs of soldiers to enhance security, according to.

2.8 UWSN – UNDERWATER WIRELESS SENSOR NETWORK

A network of sensor nodes deployed underwater (oceans, rivers, lakes) that primarily use **acoustic communication**, as radio waves attenuate rapidly in water. **Optical communication** is possible only in very clear, short-range conditions (e.g., harbors or controlled environments) and is rarely used in most underwater deployments due to high attenuation from turbidity, scattering, and alignment requirements. UWSNs are characterized by high latency, low bandwidth, node mobility due to currents, and significant energy constraints.

2.9 IOT NETWORK – INTERNET OF THINGS NETWORK

A broad term encompassing interconnected devices (sensors, actuators, appliances) that communicate over IP or non-IP networks, often integrating with cloud services. Can use various topologies (star, mesh, cellular) and protocols (MQTT, CoAP, LoRa). May include ad hoc elements but often relies on infrastructure.

2.10 LPWAN – LOW-POWER WIDE-AREA NETWORK

A class of wireless technology designed for long-range communication (kilometers) with low power consumption. Most LPWAN technologies (e.g., LoRaWAN, NB-IoT, Sigfox) use a **star-of-stars topology** where devices communicate directly to gateways, not in an ad-hoc mesh. However, some LPWAN variants (such as MIOTY and certain implementations of LoRa with mesh extensions) support mesh or repeater capabilities to extend coverage. In general, LPWANs are optimized for low power and wide area, with star topology being the predominant architecture.

3 INTRODUCTION TO WIRELESS SENSOR NETWORKS

3.1 DEFINITION OF WSN

A **Wireless Sensor Network (WSN)** is a self-organizing system of spatially distributed, autonomous devices called **sensor nodes**. These nodes work as a team to monitor physical or environmental conditions—such as temperature, sound, vibration, pressure, or pollutants—and wirelessly relay that data to a central **sink or base station** for processing.

Core Capabilities:

- **Infrastructure-less & Self-Configuring:** They don't need pre-existing wires or setups; nodes find each other and build the network automatically.
- **Bi-directional Communication:** The network doesn't just "listen" (collect data); it can also "talk" back, allowing the central station to control or trigger specific sensor activities.
- **Collaborative Intelligence:** Instead of working alone, these independent sensors share the workload to pass data across the network efficiently.

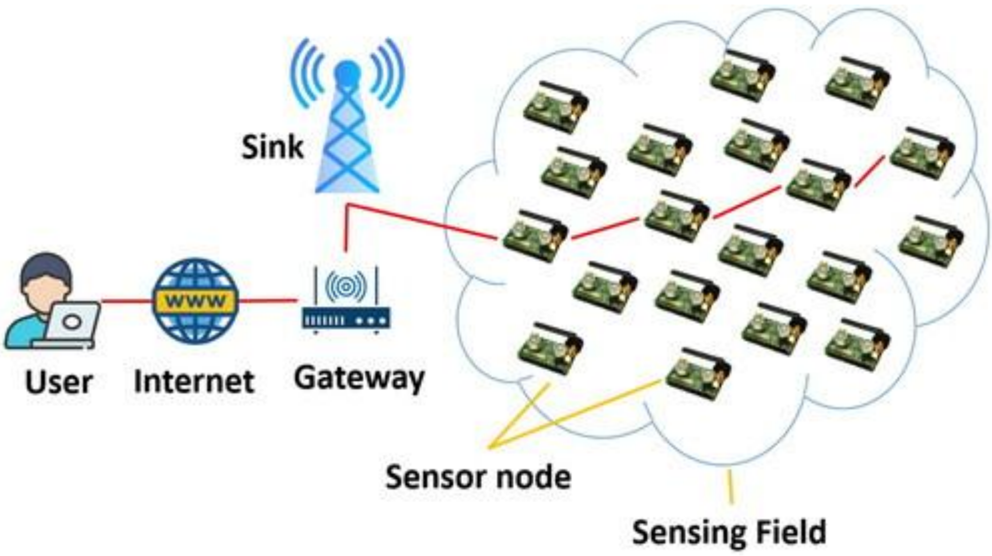

Figure 7: Wireless Sensor Networks.

4 COMPONENTS OF WIRELESS SENSOR NETWORKS

4.1 SENSOR NODES

The general architecture and the major components of a wireless sensor device (node) are illustrated in Figure 3.1. A wireless sensor device is generally composed of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. Moreover, additional components can also be integrated into the sensor node depending on the application. These components as shown by the dashed boxes in Figure 3.1 include: a location finding system, a power generator, and a mobilizer. Next, each component is described in detail:

- **Sensing unit:** The sensing unit is the main component of a wireless sensor node that distinguishes it from any other embedded system with communication capabilities. The sensing unit may generally include several sensor units, which provide information gathering capabilities from the physical world. Each sensor unit is responsible for gathering information of a certain type, such as temperature, humidity, or light, and is usually composed of two subunits: a sensor and an analog-to-digital converter (ADC). The analog signals produced by the sensor based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit.

- **Processing unit:** The processing unit is the main controller of the wireless sensor node, through which every other component is managed. The processing unit may consist of an on-board memory or may be associated with a small storage unit integrated into the embedded board. The processing unit manages the procedures that enable the sensor node to perform sensing operations, run associated algorithms, and collaborate with the other nodes through wireless communication.

- **Transceiver unit:** Communication between any two wireless sensor nodes is performed by the transceiver units. A transceiver unit implements the necessary procedures to convert bits to be transmitted into radio frequency (RF) waves and recover them at the other end. Essentially, the WSN is connected to the network through this unit.

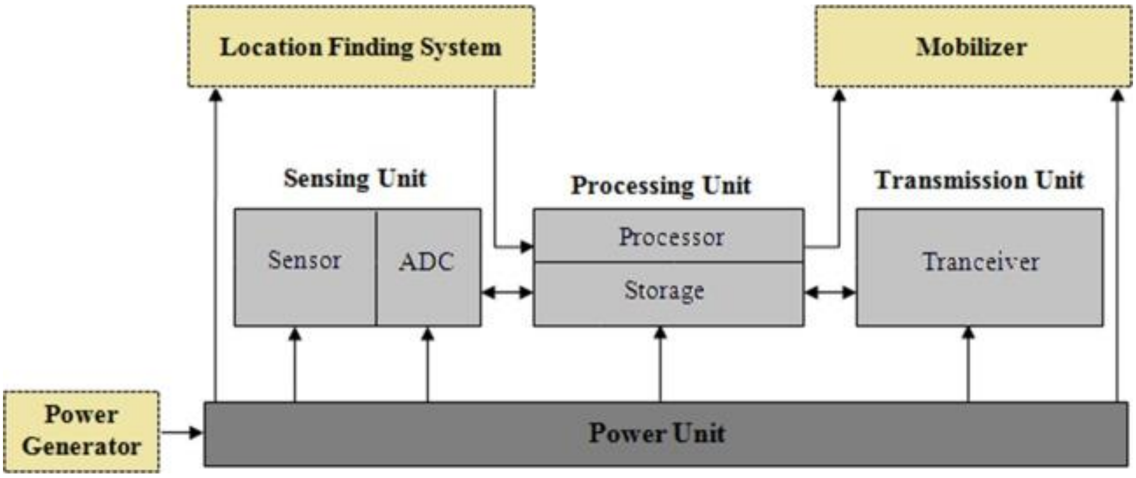

Figure 8: Block diagram of sensor node.

- **Power unit:** One of the most important components of a wireless sensor node is the power unit. Usually, battery power is used, but other energy sources are also possible. Each component in the wireless sensor node is powered through the power unit and the limited capacity of this unit requires energy-efficient operation for the tasks performed by each component.

- **Location finding system:** Most of the sensor network applications, sensing tasks, and routing techniques need knowledge of the physical location of a node. Thus, it is common for a sensor node to be equipped with a location finding system. This system may consist of a GPS module for a high-end sensor node or may be a software module that implements the localization algorithms that provide location information through distributed calculations.

- **Mobilizer:** A mobilizer may sometimes be needed to move sensor nodes when it is necessary to carry out the assigned tasks. Mobility support requires extensive energy resources and should be provided efficiently. The mobilizer can also operate in close interaction with the sensing unit and the processor to control the movements of the sensor node.

- **Power generator:** While battery power is mostly used in sensor nodes, an additional power generator can be used for applications where longer network lifetime is essential. For outdoor applications, solar cells are used to generate power. Similarly, energy scavenging techniques for thermal, kinetic, and vibration energy can also be used.

Sensor nodes have three main functions in the network:

- To collect information from sensors
- To transmit sensor data through the network to the main location
- To relay sensor data from other sensor nodes through the network to the main location

4.2 SINK / BASE STATION

A **sink node** (also called a **base station** or **gateway**) is a special node in a Wireless Sensor Network (WSN) that serves as the central collection point for data generated by all sensor nodes. It acts as the bridge between the wireless sensor network and the external world (e.g., the Internet, a cloud platform, or a local server).

Key Functions of a Sink Node

- **Data Aggregation:** Collects data from sensor nodes, often via multi-hop routing, and may perform fusion or compression to reduce redundancy.

- **Gateway Role:** Translates between the WSN's communication protocols (e.g., Zigbee, LoRa) and backhaul networks (Ethernet, Wi-Fi, cellular, satellite).
- **Command and Control:** Sends configuration commands, queries, or over-the-air updates to the sensor nodes.
- **Temporal Storage:** May buffer data temporarily before forwarding it to a backend system.

4.2.1 TYPES OF SINK NODES.

- **Fixed sink:** Stationary, placed at a predetermined location.
- **Mobile sink:** Moves through the network (e.g., drone, vehicle) to collect data, reducing multi-hop overhead.
- **Multiple sinks:** Used for fault tolerance, load balancing, or covering large geographic areas.

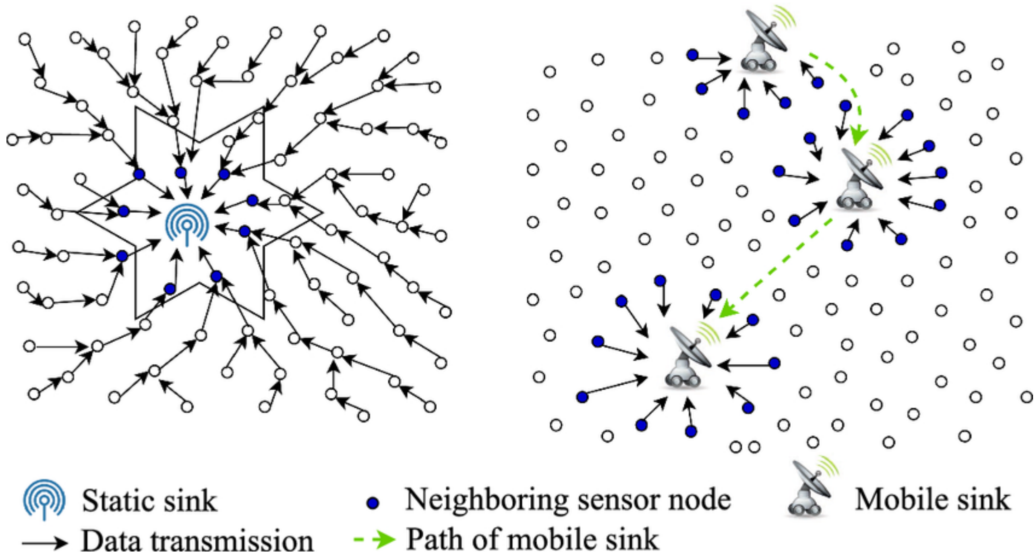

Figure 9: Fixed vs Mobile Sink nodes.

Feature	Sensor Node	Sink Node
Role	Collect data from environment	Collect data from all nodes
Power	Battery-powered (limited)	High power / mains supply
Processing	Low	High
Memory	Small	Large

Function	Sense and send data	Aggregate and control network

4.3 COMMUNICATION INFRASTRUCTURE

A WSN consists of spatially distributed sensor nodes that collaborate to monitor the physical world. Communication is the backbone: it enables data to flow from where it is sensed to where it is processed and acted upon.

Communications in Wireless Sensor Networks (WSNs) form the backbone of distributed sensing systems, enabling tiny, battery-powered nodes to collect, process, and transmit environmental data to a central sink or base station. Due to resource constraints (power, memory, computing) and wireless medium limitations (attenuation, interference), WSN communications prioritize energy efficiency over high data rates.

4.3.1 WSN NETWORK TOPOLOGIES

Wireless Sensor Networks (WSNs) can be organized into different network topologies based on their application and network type. Here are the most common types:

- **Bus Topology**: In a bus topology, multiple nodes share a single communication line. Data travels along this line from node to node. While simple, wireless bus topologies are **rare in modern WSNs** because a single break can isolate the entire network. They are occasionally used in **niche linear deployments** (e.g., sensors along a pipeline, conveyor belt, or tunnel) where wired backbones or deterministic routing are acceptable. In most cases, tree or mesh topologies are preferred for reliability and scalability.

- **Star Topology**: have a central node, called the master node, which connects directly to multiple other nodes. Data flows from the master node to the connected nodes. This topology is efficient for centralized control.

- **Tree Topology**: arrange nodes in a hierarchical structure resembling a tree. Data is transmitted from one node to another along the branches of the tree structure. It's useful for expanding coverage in hierarchical deployments.

- **Mesh Topology**: feature nodes interconnected with one another, forming a mesh-like structure. Data can travel through multiple paths from one node to another until it reaches its destination. This topology offers robust coverage and redundancy.

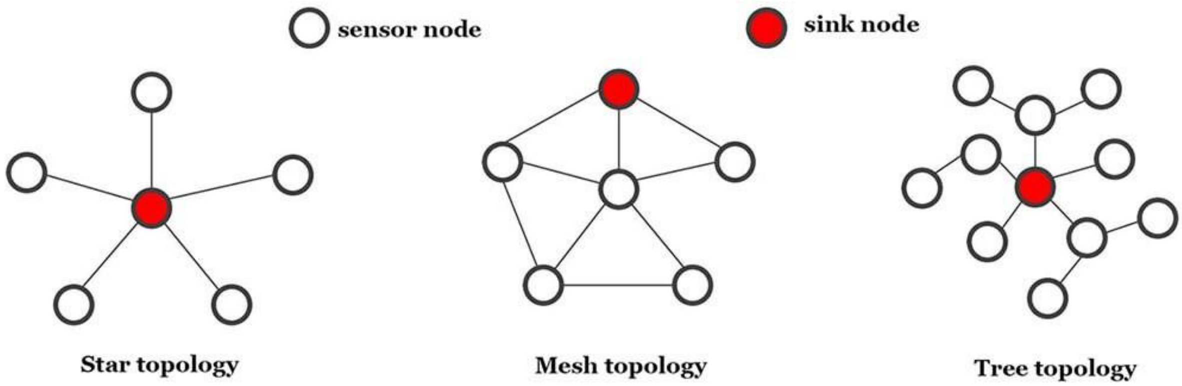

Figure 10: WSN Network Topologies

Application	Suitable WSN Topology(s)	Remarks
Smart Agriculture (soil moisture, weather, irrigation)	**Cluster-tree**, **Mesh**, **Star**, **Bus** (for linear layouts like drip irrigation lines)	Bus can be used when sensors are placed along a single line (e.g., pipeline monitoring).
Environmental Monitoring (forest fire, air quality, wildlife)	**Mesh**, **Tree**, **Hybrid**, **Bus** (for trail or riverbank deployments)	Linear deployments (e.g., along a river) may benefit from a bus or daisy-chain.
Industrial Automation (machine monitoring, predictive maintenance)	**Star**, **Mesh**, **Cluster-tree**, **Bus** (e.g., CAN bus, PROFIBUS, Foundation Fieldbus)	Wired bus topologies are common in factories; wireless bus is rare but possible with linear layouts.
Smart Home / Building Automation	**Star**, **Mesh**, **Tree**	Bus is not typical in wireless home automation due to complexity; wired systems (KNX, DALI) sometimes use bus.
Healthcare (wearable monitoring, fall detection)	**Star**, **Tree**	Bus is rarely used because devices are mobile and not arranged linearly.

Transportation / Smart Cities (traffic, parking, structural health)	**Mesh**, **Cluster-tree**, **Hybrid**, **Bus** (for tunnel or roadside linear networks)	Linear infrastructure (tunnels, bridges, roads) can be instrumented with bus-like multi-drop wired or wireless chains.
Military / Border Surveillance	**Mesh**, **Hierarchical**	Bus is generally avoided due to vulnerability; a single cut can break the network.
Supply Chain / Asset Tracking	**Star**, **Tree**, **Hybrid**	Bus is not common; tracking typically relies on star at checkpoints.
Disaster Management (earthquake, firefighter tracking)	**Mesh**, **Dynamic / Ad-hoc**	Bus lacks the resilience needed for disaster scenarios.
Smart Grid / Energy Management (AMI, line monitoring)	**Mesh**, **Tree**, **Cluster-tree**, **Bus** (for power line carrier communication)	Power line carrier (PLC) uses the electrical bus; wireless mesh is more common for AMI.

4.3.2 THREE-TIER COMMUNICATION ARCHITECTURE – DEFINITIONS, ROLES & TOPOLOGIES

4.3.2.1 Node to Node

- **Definition**: Communication between adjacent sensor nodes within the local network.
- **Role / Purpose**: Enables local cooperation (e.g., data fusion, synchronization), packet relaying toward the sink, and topology maintenance (neighbor discovery, link estimation, routing updates).
- **Topology**: Mesh (most common), Tree, Star (rare, usually for short range).

4.3.2.2 Nodes to Sink

- **Definition**: Multi-hop communication from multiple sensor nodes toward a central gateway (sink).

- **Role / Purpose**: Collects and aggregates data from the sensor field, forwards it through intermediate nodes to the sink, and provides reliability, congestion control, and in-network processing.
- **Topology**: Tree, Cluster-Tree, Mesh (with many-to-one routing), Star (if single hop).

4.3.2.3 Sink to Cloud

- **Definition**: Backhaul communication from the sink to external networks (Internet, cloud platforms, or control centers).
- **Role / Purpose**: Uploads sensor data for storage, analysis, and visualization; receives commands, configuration updates, and firmware from the cloud; bridges local WSN protocols with global IP networks.
- **Topology**: Star (point-to-point from sink to cloud), sometimes Bus (in wired backhaul), or Mesh (multiple gateways for redundancy).

4.3.3 COMPARISON TABLE – NODE TO NODE VS. NODES TO SINK VS. SINK TO CLOUD

Aspect	Node to Node	Nodes to Sink	Sink to Cloud
Communication Pattern	Peer-to-peer, any-to-any	Many-to-one (converged)	One-to-few (sink to cloud), bidirectional
Range	Short (meters)	Short to medium (multi-hop)	Long (kilometers via cellular, satellite, etc.)
Typical Protocols	IEEE 802.15.4, Zigbee, Thread, BLE, RPL, LOADng	RPL, CTP, 6LoWPAN, CoAP, MQTT-SN	MQTT, HTTPS, WebSocket, gRPC, cloud SDKs
Energy Constraints	Critical (battery-powered)	Moderate (nodes near sink may deplete faster)	Low (sink usually mains-powered)
Key Challenge	Interference, link asymmetry, duty-cycling	Funneling effect, congestion, reliability	Connectivity variability, security, cost
Topology	Mesh, Tree, Star	Tree, Cluster-Tree, Mesh (many-to-one)	Star, Bus, Mesh (redundant gateways)

Security Focus	Link-layer encryption, secure neighbor discovery	End-to-end authentication, secure routing	TLS/DTLS, device certificates, IAM policies

4.4 SOFTWARE

Software is a critical enabler in Wireless Sensor Networks, spanning from the embedded firmware on sensor nodes to cloud-based analytics platforms. The software stack varies significantly across the three main components: **Node**, **Sink**, and **Cloud**.

4.4.1 NODE SOFTWARE

Each sensor node has a small computer inside. The software on it is designed to save battery, talk to other nodes, and do its job. What it does:

- **Controls the hardware** – It turns sensors on/off, manages the battery, and puts the node to sleep when idle to save power.
- **Handles communication** – It uses simple, low-power wireless protocols (like Zigbee or LoRa) to send data to neighbors or directly to the sink.
- **Runs the application** – It reads sensor values, does basic processing (e.g., averaging), and sends the data toward the sink.

Examples of node software:

- **RIOT OS** – An operating system for small devices. It supports standard internet protocols (IPv6) and is easy to program.
- **Contiki** – A lightweight OS used a lot in research. It saves memory and includes a simulator for testing.
- **Zephyr RTOS** – A modern, secure OS that works with many wireless technologies (Bluetooth, LoRa, Thread).

4.4.2 SINK SOFTWARE

The sink (or gateway) is the central box that collects data from all sensor nodes and sends it to the internet. Its software acts as a translator and manager.

What it does:

- **Translates protocols** – It converts the wireless messages from nodes (e.g., CoAP, LoRa) into internet-friendly protocols (e.g., MQTT, HTTP) so cloud services can understand them.
- **Processes data locally** – It can combine, filter, or analyze data before sending it to the cloud, saving bandwidth.
- **Stores data temporarily** – If the internet goes down, it saves the data until the connection is restored.
- **Talks to the cloud** – It securely sends data to cloud platforms and receives commands for the network.

Examples of sink software:

- **AWS Greengrass** – A piece of software that lets the sink run local computing and sync with Amazon's cloud when online.
- **Node-RED** – A visual tool that lets you draw flows to translate between different protocols and do simple logic without coding.
- **ChirpStack Gateway Bridge** – A service that forwards LoRa messages from a gateway to a LoRaWAN network server.

4.4.3 CLOUD SOFTWARE

The cloud is where data from many sensors is stored, analyzed, and viewed. Cloud software runs on big servers and provides services for managing devices and data.

What it does:

- **Collects data securely** – It identifies each sensor, checks that it is trusted, and receives its messages.
- **Stores and analyzes data** – It saves data in time-ordered databases and can run analytics (e.g., detect when a value is abnormal).
- **Manages devices** – It keeps track of which sensors are active, can update their software remotely, and stores their latest state.
- **Shows data to users** – It provides dashboards and graphs so people can see what's happening in real time.

Examples of cloud software:

- **AWS IoT Core** – Amazon's cloud service for connecting devices. It handles authentication, message routing, and device shadows.
- **Azure IoT Hub** – Microsoft's service for managing devices and sending data to Azure cloud tools.
- **Grafana** – A tool for creating dashboards that display sensor data from databases (like Prometheus or InfluxDB).

4.5 SUPPORTING ELEMENTS

- **Power Management** – Techniques to maximize network lifetime (duty cycling, energy-aware routing, energy harvesting).
- **Security** – Mechanisms to ensure confidentiality, integrity, and availability (encryption, authentication, intrusion detection).

- **Time Synchronization** – Maintaining a common time across nodes for coordinated sampling, TDMA scheduling, and data fusion.
- **Data Aggregation** – In-network processing to combine or summarize data, reducing transmissions and energy consumption.
- **Fault Tolerance** – Redundancy and self-healing mechanisms to maintain functionality despite node failures or link disruptions.
- **Quality of Service (QoS)** – Prioritization and resource reservation to meet requirements for latency, reliability, and bandwidth.
- **Mobility Management** – Handling node or sink movement, maintaining connectivity and routing in dynamic topologies.
- **Configuration and Management** – Tools and protocols for network deployment, parameter setting, firmware updates, and monitoring.
- **Middleware** – Software layers that abstract hardware and provide common services (e.g., publish-subscribe, database-like querying).

5 CHARACTERISTICS OF WIRELESS SENSOR NETWORK

Some basic characteristics of Wireless Sensor Networks are as follows:

- Power consumption constraints for nodes using energy harvesting or mainly batteries are used.
- Examples of suppliers are ReVibe Energy and Perpetuum
- Having the ability to deal with node failures (resilience)
- Having some mobility of nodes (for highly mobile nodes see Mobile Wireless Sensor Networks)

- Scalability to the large scale of deployment
- Ability to resist harsh environmental conditions
- Heterogeneity of nodes
- Homogeneity of nodes
- Easy to use
- Cross-layer optimization

5.1 ADVANTAGES

- **Low cost:** WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.
- **Wireless communication:** WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.
- **Energy efficiency:** WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.
- **Scalability:** WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.
- **Real-time monitoring:** WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

5.2 DISADVANTAGES

- **Limited range:** The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.
- **Limited processing power:** WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.
- **Data security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.
- **Interference:** Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.
- **Deployment challenges:** Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.
- while WSNs offer many benefits, they also have limitations and challenges that must be considered when deploying and using them in real-world applications.

6 TYPES OF WIRELESS SENSOR NETWORKS (WSN)

6.1 TERRESTRIAL WIRELESS SENSOR NETWORKS

- Used for efficient communication between base stations.

- Consist of thousands of nodes placed in an ad hoc (random) or structured (planned) manner.
- Nodes may use solar cells for energy efficiency.
- Focus on low energy use and optimal routing for efficiency.

Figure 11: TERRESTRIAL WIRELESS SENSOR NETWORKS

6.2 UNDERGROUND WIRELESS SENSOR NETWORKS

- Nodes are buried underground to monitor underground conditions.
- Require additional sink nodes above ground for data transmission.
- Face challenges like high installation and maintenance costs.
- Limited battery life and difficulty in recharging due to underground setup.

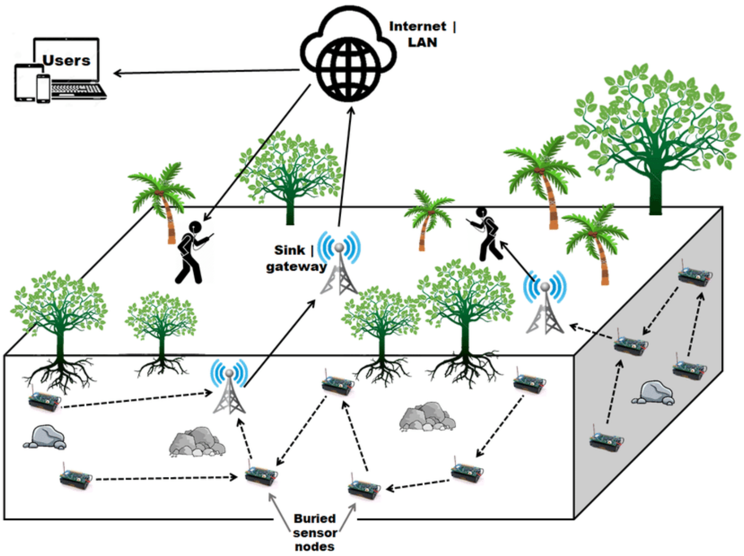

Figure 12: UNDERGROUND WIRELESS SENSOR NETWORKS

6.3 UNDERWATER WIRELESS SENSOR NETWORKS

- Deployed in water environments using sensor nodes and autonomous underwater vehicles.
- Face challenges like slow data transmission, bandwidth limitations, and signal attenuation.
- Nodes have restricted and non-rechargeable power sources.

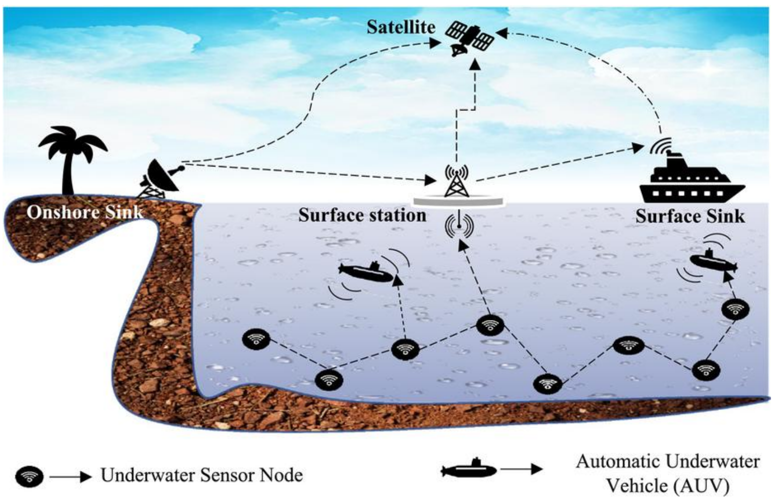

Figure 13: UNDERWATER WIRELESS SENSOR NETWORKS

6.4 MULTIMEDIA WIRELESS SENSOR NETWORKS

- Used to monitor multimedia events such as video, audio, and images.
- Nodes equipped with microphones and cameras for data capture.
- Challenges include high power consumption, large bandwidth requirements, and complex data processing.
- Designed for efficient wireless data compression and transmission.

6.5 MOBILE WIRELESS SENSOR NETWORKS (MWSNS)

- Composed of mobile sensor nodes capable of independent movement.
- Offer advantages like increased coverage area, energy efficiency, and channel capacity compared to static networks.
- Nodes can sense, compute, and communicate while moving in the environment.

7 CONSTRAINTS

Before detailing the constraints, it is important to recognize that each component in a Wireless Sensor Network operates under distinct limitations that shape system design. **Nodes** are severely resource-constrained, with energy being the most critical factor affecting lifetime and functionality. The **sink** acts as a gateway and faces challenges related to connectivity, security, and processing load. The **cloud** provides scalable back-end services but introduces latency, cost, and regulatory considerations. The following table summarizes the important constraints for each component, along with additional constraints that may apply depending on the deployment scenario.

Component	Important Constraints	Additional Constraints
Node	• **Energy** – Primary constraint; determines network lifetime. • **Processing Power** – Limited; restricts algorithm complexity. • **Memory** – Small RAM/flash limits program size and buffering. • **Communication Bandwidth** – Low data rates; multi-hop required.	• Radio range • Cost per node • Physical size / form factor • Hardware variability (sensors, MCU)
Sink	• **Connectivity Reliability** – Backhaul may be intermittent, expensive, or limited. • **Security** – Critical point; must authenticate nodes and protect credentials. • **Processing** – Must handle protocol translation, aggregation, and edge analytics. • **Storage** – Local buffering essential for cloud disconnections.	• Power source (mains vs. battery/solar) • Interoperability with multiple protocols • Environmental ruggedness
Cloud	• **Latency** – End-to-end delay may limit real-time applications. • **Bandwidth Cost** – Data egress and backhaul charges can be prohibitive. • **Security & Privacy** – Data must be encrypted; strict access controls required. • **Scalability** – Must handle large device counts and message volumes.	• Vendor lock-in • Dependency on internet connectivity • Data management (retention, archival) • Regulatory compliance (GDPR, data sovereignty)

8 MEDICAL APPLICATIONS

Application Area	Type of Node	Typical Topology	Type of Sink	Description / Examples
Remote Patient Monitoring	Wearable sensors (ECG patch, pulse oximeter, blood pressure cuff)	Star	Smartphone (hub) → Cloud / Physician portal	Continuous vitals sent to clinicians; e.g., Zio Patch, Masimo MightySat
In-Hospital Patient Tracking & Monitoring	Wearable tags, bed sensors, wireless vital sign monitors	Star / Mesh	Bedside gateway → Central nursing station / Asset management system	Real-time location of patients/equipment; fall detection; Philips IntelliVue

Elderly Care & Assisted Living	Wearable fall detector, ambient motion sensors, door contact sensors	Star	Home gateway → Cloud / Caregiver app	Alerts for falls, inactivity; e.g., Medical Guardian, Philips Lifeline
Chronic Disease Management	Continuous glucose monitor (CGM), insulin pump, spirometer	Star	Smartphone → Cloud / Clinical portal	Closed-loop insulin delivery; Dexcom G7, Freestyle Libre
Sleep Monitoring & Diagnostics	Wearable rings/headbands, under-mattress sensors	Star	Smartphone → Cloud / Sleep lab platform	At-home sleep apnea testing; WatchPAT, Oura ring
Rehabilitation & Motion Analysis	Inertial measurement units (IMUs), pressure-sensing insoles	Star / Mesh	Local gateway (PC/tablet) → Cloud / Therapist dashboard	Gait analysis, post-surgery recovery; used in stroke rehab
Emergency & Trauma Care	Body-worn sensors (ECG, SpO_2, temperature)	Star	Portable gateway (ambulance) → Hospital system	Real-time vitals to ER during transport; tactical casualty care
Drug Delivery Systems	Smart infusion pump, implantable drug dispenser	Star	Smartphone / Hospital network → Clinical monitoring	Remote-controlled drug delivery; smart insulin pumps
Infection Control & Contact Tracing	Wearable proximity sensors (RFID, BLE)	Mesh / Star	Facility-wide gateways → Central monitoring system	Hospital staff/patient contact logging; alerts for exposure
Mental Health Monitoring	Wearable (smartwatch, ring) with activity/HRV sensors	Star	Smartphone → Cloud / Research platform	Stress detection, sleep patterns; used in depression/anxiety studies

REFERENCES

- Communication Systems – Simon Haykin, 5th Edition, John Wiley & Sons, 2009.
- Modern Digital and Analog Communication Systems – B. P. Lathi and Zhi Ding, 4th Edition, Oxford University Press, 2009.

- Analog and Digital Communication Systems – Leon W. Couch II, 8th Edition, Pearson, 2013.
- Digital Communications – John G. Proakis and Masoud Salehi, 5th Edition, McGraw-Hill, 2007.