CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assessment Test 2– Feb 2024

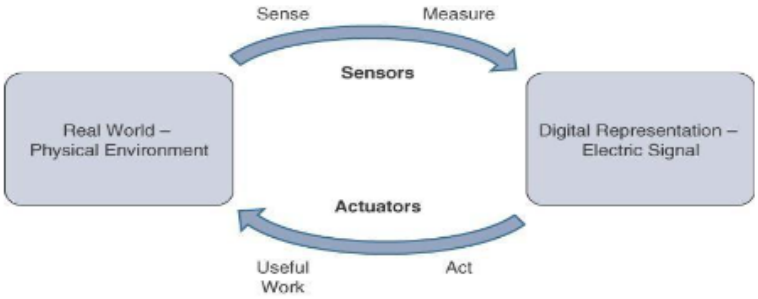
Sub:	Internet of Things					Sub Code:	**22MCA32**	Branch:	MCA
Date:	15\02\2024	Duration:	90 min's	Max Marks:	50	Sem	III		

Q1. Define sensors and actuators; explain how actuators and sensors interact with physical world with the neat diagram. Classify actuators based on energy type.

A sensor measures some physical quantity and converts that measurement reading into a digital representation.

Sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).

Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force,



and so on.

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

Q2. List and explain different type of sensors with an example.

A sensor measures some physical quantity and converts that measurement reading into a digital representation.

Sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Q3. Define smart object and explain the characteristics, Also provide the definition for SANET? Explain the advantages and disadvantages of it.

Smart Objects

Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way. A *smart object*, is a device that has, at a minimum, the following four defining characteristics

- **Processing Unit:** A smart object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensor(s), coordinating control signals to any actuators, and controlling a variety of functions on the smart object, including the communication and power systems.
- **Sensor(s) and /or actuator(s):** A smart object is capable of interacting with the physical world through sensors and actuators. A smart object does not need to contain

  both sensors and actuators. In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.
- **Communication Device:** The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network). Communication devices for smart objects can be either wired or wireless.
- **Power Source:** Smart objects have components that need to be powered. Interestingly, the most significant power consumption usually comes from the communication unit of a smart object.

Sensor Networks:

- A sensor/actuator network (SANET), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment.
- The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner.
- SANETs offer highly coordinated sensing and actuation capabilities.
- Smart homes are a type of SANET that display this coordination between distributed sensors and actuators.
- For example, smart homes can have temperature sensors that are strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators. When a sensor detects a specified temperature, this can trigger an actuator to take action and heat or cool the home as needed.

The following are some advantages and disadvantages that a wireless-based solution offers:

Advantages:

- Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
- Simpler scaling to a large number of nodes
- Lower implementation costs
- Easier long-term maintenance
- Effortless introduction of new sensor/actuator nodes
- Better equipped to handle dynamic/rapid topology changes

Disadvantages:

- Potentially less secure (for example, hijacked access points)
- Typically, lower transmission speeds
- Greater level of impact/influence by environment

Q4. List and explain any 15 sensors present in smart phones with its purpose

.

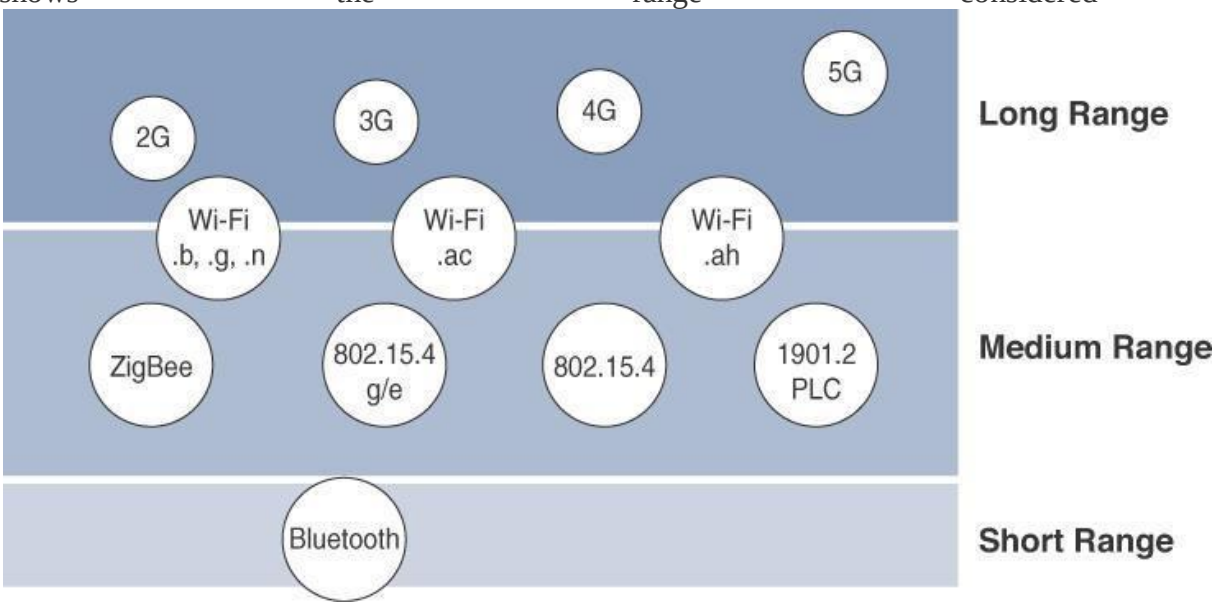
Explain any 15 from the following

Figure 3-2 *Sensors in a Smart Phone*

Q5) Explain the communication criteria's for connecting smart objects in detail

The characteristics and attributes considered when selecting and dealing with connecting smart objects are

1. **Range:** It defines how far does the signal need to be propagated? That is, what will be the area of coverage for a selected wireless technology? The below figure 2.4 shows the range considered



- **Short Range:**
  - The classical wired example is a serial cable.
  - Wireless short-range technologies are often considered as an alternative to a serial cable, supporting tens of meters of maximum distance between two devices.
  - Examples of short-range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC).

    - These short-range communication methods are found in only a minority of IoT installations.
- **Medium Range:**
    - In the range of tens to hundreds of meters, many specifications and implementations are available.
    - The maximum distance is generally less than 1 mile between two devices.
- **Long Range**:
    - Distances greater than 1 mile between two devices require long-range technologies. Wireless examples are cellular (2G, 3G, 4G) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies.
    - LPWA communications have the ability to communicate over a large area without consuming much power.
    - These technologies are therefore ideal for battery-powered IoT sensors.
    - Found mainly in industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications are classified as long range but are not really considered IoT access technologies.

Frequency Bands:

- Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).
- These groups define the regulations and transmission requirements for various frequency bands.
- For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
- Focusing on IoT access technologies, the frequency bands leveraged by wireless communications are split between licensed and unlicensed bands.
- Licensed spectrum is generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.
- The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands.
- These frequencies are used in many communications technologies for short-range devices (SRDs).
- Unlicensed means that no guarantees or protections are offered in the ISM bands for device communications.

Power Consumption:

- Battery-powered nodes bring much more flexibility to IoT devices.
- These nodes are often classified by the required lifetimes of their batteries.
- A powered node has a direct connection to a power source, and communications are usually not limited by power consumption criteria.
- IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes.
- This has led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA).

Topology

- Among the access technologies available for connecting IoT devices, three main topology schemes are dominant: star, mesh, and peer-to-peer.
- For long-range and short-range technologies, a star topology is prevalent, as seen with cellular, LPWA, and Bluetooth networks.
- Star topologies utilize a single central base station or controller to allow communications with endpoints.

- For medium-range technologies, a star, peer-to-peer, or mesh topology is common.
- Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other.
- Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.

Constrained Devices:

Constrained nodes have limited resources that impact their networking feature set and capabilities.

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

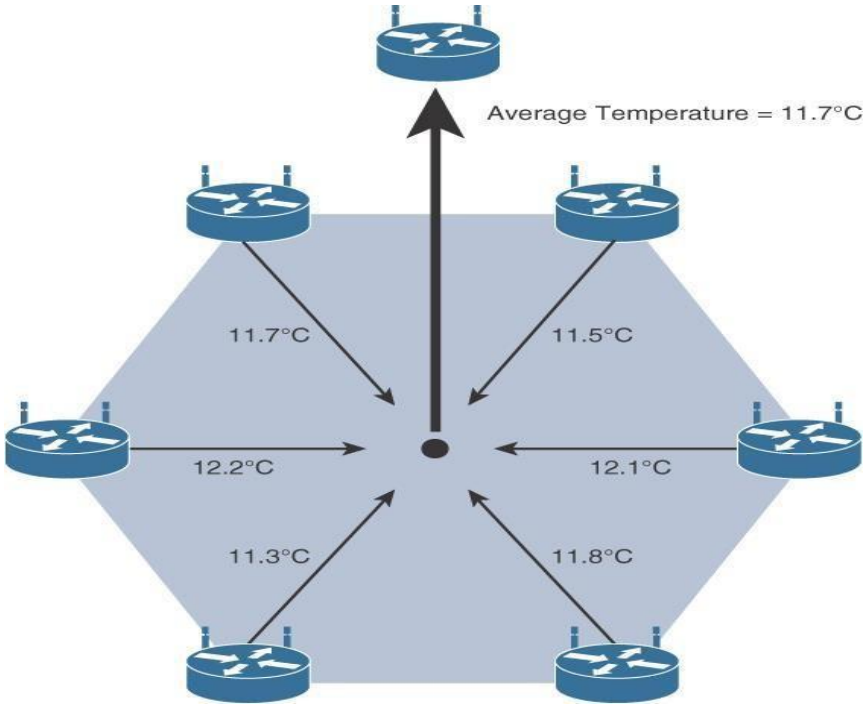
Q6) List out the limitations of the smart objects in WSNs and explain the data aggregation in WSN with a neat diagram.

Wireless Sensor Networks (WSNs)

Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as *motes*. The following are some of the most significant limitations of the smart objects in WSNs:

- Limited processing power
- Limited memory
- Lossy communication
- Limited transmission speeds
- Limited power

These limitations greatly influence how WSNs are designed, deployed, and utilized. Figure 2.3 below shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.



These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSNs with very large numbers of deployed smart objects. Wirelessly connected smart objects generally have one of the following two communication patterns:

- **Event-driven:** Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.
- **Periodic:** Transmission of sensory information occurs only at periodic intervals.

Q7) Explain sensor networks in detail

Sensor Networks:

- A sensor/actuator network (SANET), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment.
- The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner.
- SANETs offer highly coordinated sensing and actuation capabilities.
- Smart homes are a type of SANET that display this coordination between distributed sensors and actuators.
- For example, smart homes can have temperature sensors that are strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators. When a sensor detects a specified temperature, this can trigger an actuator to take action and heat or cool the home as needed.

The following are some advantages and disadvantages that a wireless-based solution offers:

Advantages:

- Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
- Simpler scaling to a large number of nodes
- Lower implementation costs
- Easier long-term maintenance
- Effortless introduction of new sensor/actuator nodes
- Better equipped to handle dynamic/rapid topology changes

Disadvantages:

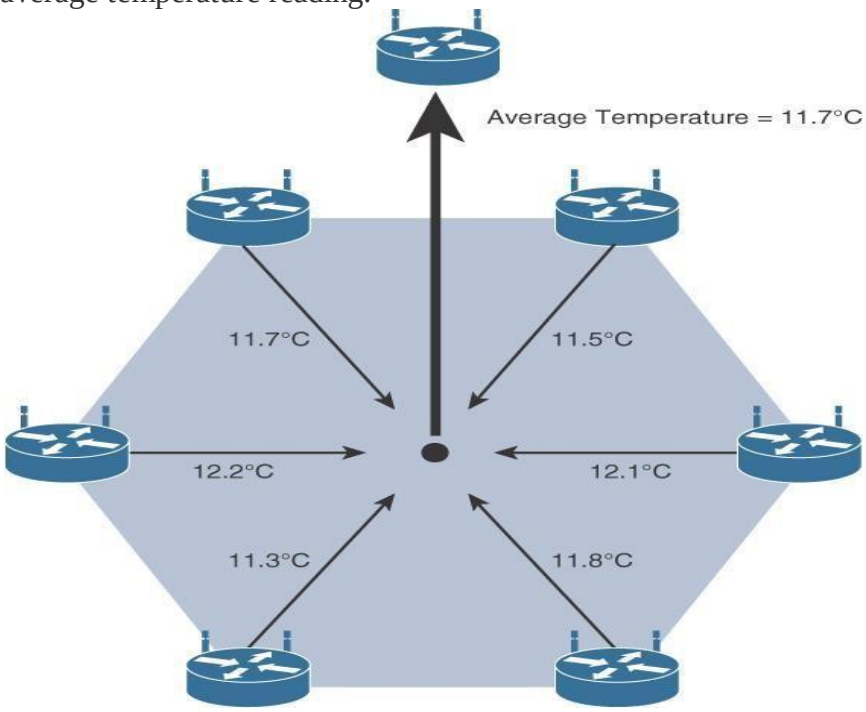
- Potentially less secure (for example, hijacked access points)
- Typically, lower transmission speeds
- Greater level of impact/influence by environment

Wireless Sensor Networks (WSNs)

Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as *motes*. The following are some of the most significant limitations of the smart objects in WSNs:

- Limited processing power
- Limited memory
- Lossy communication
- Limited transmission speeds
- Limited power

These limitations greatly influence how WSNs are designed, deployed, and utilized. Figure 2.3 below shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.



These data aggregation techniques are helpful in reducing the amount of overall traffic (and energy) in WSNs with very large numbers of deployed smart objects. Wirelessly connected smart objects generally have one of the following two communication patterns:

- **Event-driven:** Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.
- **Periodic:** Transmission of sensory information occurs only at periodic intervals.

Q8) Write Explain any one IoT access technology in detail

IEEE 802.15.4:

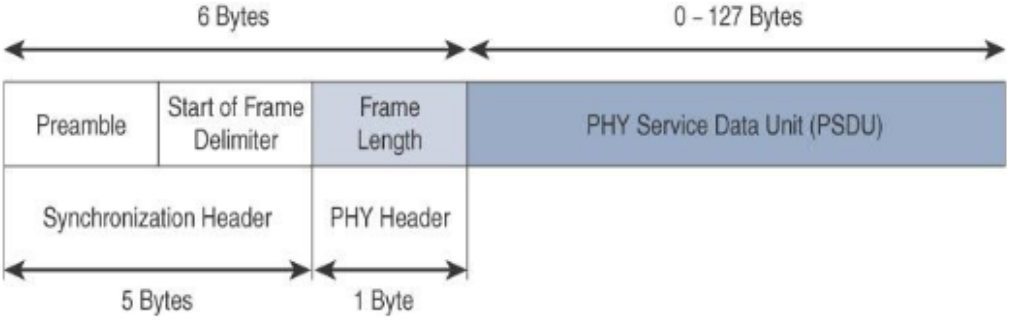
- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.
- This access technology enables easy installation using a compact protocol stack while remaining both simple and flexible.
- IEEE 802.15.4 is commonly found in the following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls
- Criticisms of IEEE 802.15.4 often focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading.
- Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique.

❖ Standardization and Alliances

- IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN).
- The IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks.
- These protocol stacks make use of 802.15.4 at the physical and link layer levels, but the upper layers are different.

❖ 802.15.4 Physical and MAC Layer:

- The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands.
- The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation.
- DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth.
- The original physical layer transmission options were as follows:
    - 2.4 GHz, 16 channels, with a data rate of 250 kbps
    - 915 MHz, 10 channels, with a data rate of 40 kbps
    - 868 MHz, 1 channel, with a data rate of 20 kbps
- IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following:
    - **OQPSK PHY:** This is DSSS PHY, employing offset quadrature phase-shift keying (OQPSK) modulation.
        - OQPSK is a modulation technique that uses four unique bit values that are signaled by phase changes.
        - An offset function that is present during phase shifts allows data to be transmitted more reliably.
    - **BPSK PHY:** This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation.
        - BPSK specifies two unique phase shifts as its data encoding scheme.
    - **ASK PHY:** This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation.
        - PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS.
        - ASK uses amplitude shifts instead of phase shifts to signal different bit values.



- The PHY Header portion of the PHY frame is shown in Figure 2.8 is simply a frame length value.
- It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY. The PSDU is the data field or payload.
- The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated.
- At this layer, the scheduling and routing of data frames are also coordinated.
- The 802.15.4 MAC layer performs the following tasks:
    - Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
    - PAN association and disassociation by a device
    - Device security
    - Reliable link communications between two peer MAC entities
    - The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of MAC frames are specified in 802.15.4:
    - Data frame: Handles all transfers of data
    - Beacon frame: Used in the transmission of beacons from a PAN coordinator
    - Acknowledgement frame: Confirms the successful reception of a frame
    - MAC command frame: Responsible for control communication between devices
- Each of these four 802.15.4 MAC frame types follows the frame format shown in Figure 2.9. In Figure 2.9, notice that the MAC frame is carried as the PHY payload.
- The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.

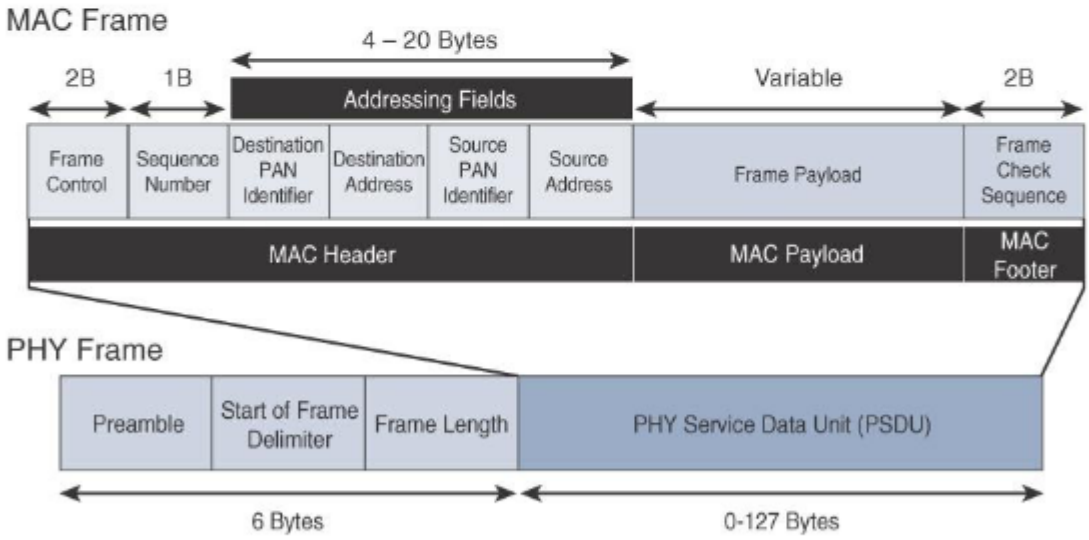


Figure 2.9 IEEE 802.15.4 MAC Format

- The MAC Header field is composed of the Frame Control, Sequence Number and the Addressing fields.
- The Frame Control field defines attributes such as frame type, addressing modes, and other control flags.
- The Sequence Number field indicates the sequence identifier for the frame.

❖ **Topology**

- IEEE 802.15.4–based networks can be built as star, peer-to-peer, or mesh topologies.
- Mesh networks tie together many nodes.
- This allows nodes that would be out of range if trying to communicate directly to leverage intermediary nodes to transfer communications.
- Every 802.15.4 PAN should be set up with a unique ID.
- All the nodes in the same 802.15.4 network should use the same PAN ID.
- Figure 2.10 shows an example of an 802.15.4 mesh network with a PAN ID of 1.

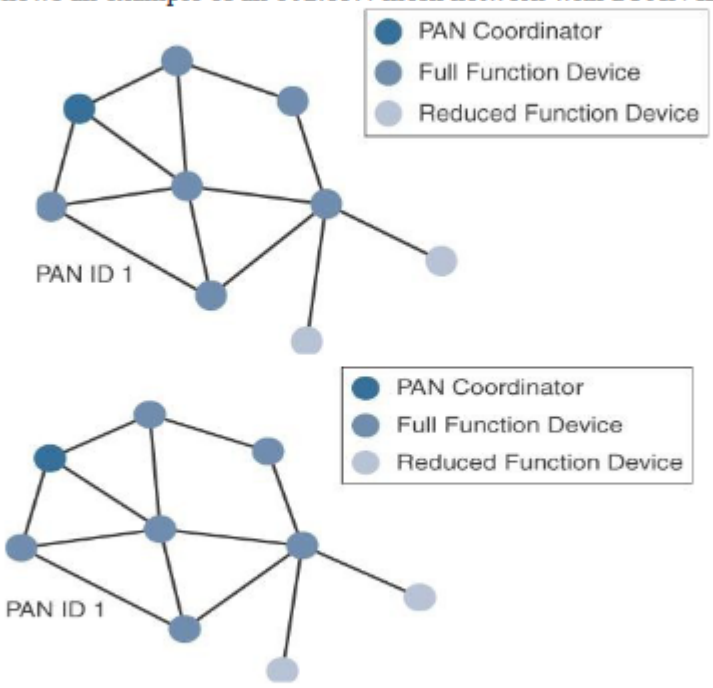


Figure 2.10: 802.15.4 Sample Mesh Network Topology

- FFD (full-function devices) acts as a PAN coordinator to deliver services that allow other devices to associate and form a cell or PAN.
- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

❖ **Security**

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data.
- In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent.
- This is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption.

- The figure 2.11 below shows the IEEE 802.15.4 frame format at a high level, with the Security Enabled bit set and the Auxiliary Security Header field present.

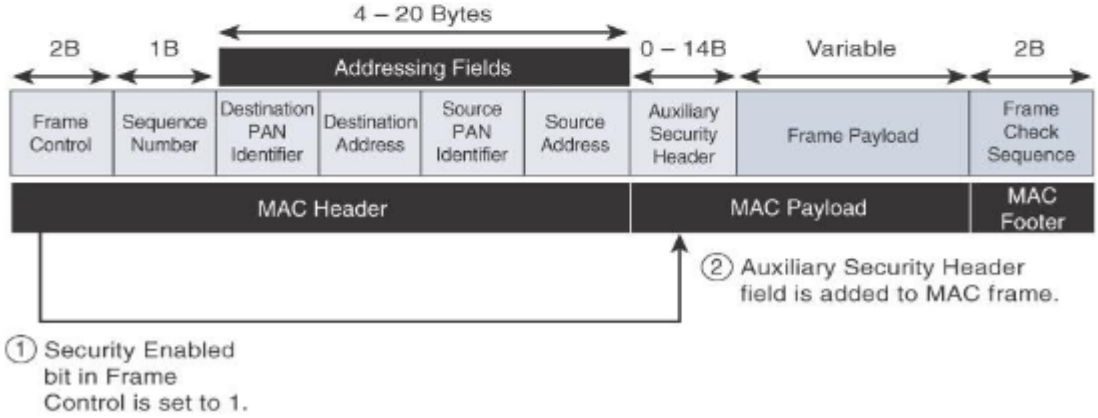


Figure 2.11:Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions

9) Write a program to implement intruder detection system using raspberry Pi

```
import RPi.GPIO as GPIO
import time

# Set GPIO mode
GPIO.setmode(GPIO.BOARD)

# Set up PIR sensor pin
PIR_PIN = 11
GPIO.setup(PIR_PIN, GPIO.IN)

# Function to detect motion
def motion_detected(channel):
    print("Intruder detected!")

# Add event listener to PIR sensor
GPIO.add_event_detect(PIR_PIN, GPIO.RISING, callback=motion_detected)

try:
    print("Intruder detection system running...")
    while True:
        time.sleep(1)
```

```
except KeyboardInterrupt:
    print("Stopping intruder detection system...")
    GPIO.cleanup()
```

Q10) Write a program to implement HVAC using any IoT board

```
import Adafruit_DHT
import RPi.GPIO as GPIO
import time

# Set GPIO mode
GPIO.setmode(GPIO.BOARD)

# Set up HVAC pins
HEATER_PIN = 11
COOLER_PIN = 12
FAN_PIN = 13
GPIO.setup(HEATER_PIN, GPIO.OUT)
GPIO.setup(COOLER_PIN, GPIO.OUT)
GPIO.setup(FAN_PIN, GPIO.OUT)

# Set up DHT11 sensor
DHT_SENSOR = Adafruit_DHT.DHT11
DHT_PIN = 4

# Function to read temperature and humidity
def read_temperature_humidity():
    humidity, temperature = Adafruit_DHT.read_retry(DHT_SENSOR, DHT_PIN)
    return humidity, temperature

# Function to control HVAC
def control_hvac(temperature, set_point):
    if temperature < set_point - 1:
        # Turn on heater
        GPIO.output(HEATER_PIN, GPIO.HIGH)
        GPIO.output(COOLER_PIN, GPIO.LOW)
        GPIO.output(FAN_PIN, GPIO.LOW)
        print("Heating...")
    elif temperature > set_point + 1:
        # Turn on cooler
        GPIO.output(COOLER_PIN, GPIO.HIGH)
        GPIO.output(HEATER_PIN, GPIO.LOW)
        GPIO.output(FAN_PIN, GPIO.LOW)
        print("Cooling...")
    else:
        # Turn off HVAC
        GPIO.output(HEATER_PIN, GPIO.LOW)
        GPIO.output(COOLER_PIN, GPIO.LOW)
        GPIO.output(FAN_PIN, GPIO.HIGH)
        print("Maintaining temperature...")

try:
    print("HVAC control system running...")
    while True:
        humidity, temperature = read_temperature_humidity()
        if humidity is not None and temperature is not None:
```

```
            print("Temperature: {:.1f}°C, Humidity: {:.1f}%".format(temperature, humidity))
            set_point = 25  # Change this to desired temperature set point
            control_hvac(temperature, set_point)
        else:
            print("Failed to retrieve data from DHT sensor")
        time.sleep(5)  # Wait for 5 seconds before reading temperature again

except KeyboardInterrupt:
    print("Stopping HVAC control system...")
    GPIO.cleanup()
```