Module-2

Smart Objects: The "Things" in IOT

Sensors, Actuators and Smart Objects

In this section we learn the capabilities, characteristics and functionality of sensors and actuators. These foundational elements together to form smart objects, which are connected to form the sensor and actuator networks that make most IOT use case possible.

- **Sensors:-**

A sensor does exactly as its name indicates: It senses. A sensor measures some physical quantity and converts that measurement reading into a digital representation. That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or human.

- Sensors are not limited to human-like sensory data. In fact, they are able to provide an extremely wide spectrum of rich and diverse measurement data with sensor

- There are a number of ways to group and cluster sensors into different categories, including the following:

* **Active or Passive:** Sensors can be categorized based on whether they produce an energy output and typically require an external power supply — Active / or whether they simply receive energy and typically require no external supply — Passive.

* **Invasive or Non-invasive:** Sensors can be categorized based on whether they sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).

* Contact or No-contact: Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
* Absolute or Relative: Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).
* Area of application: Sensors can be categorized based on the specific industry or vertical where they are being used
* How Sensors measure: Sensors can be categorized based on the physical mechanism used to measure sensory input
* What Sensors measure: Sensors can be categorized based on their applications or what physical variables they measure

Actuators:

Actuators are natural completements to Sensors. The following figure demonstrates the symmetry and complementary nature of these two types of devices.

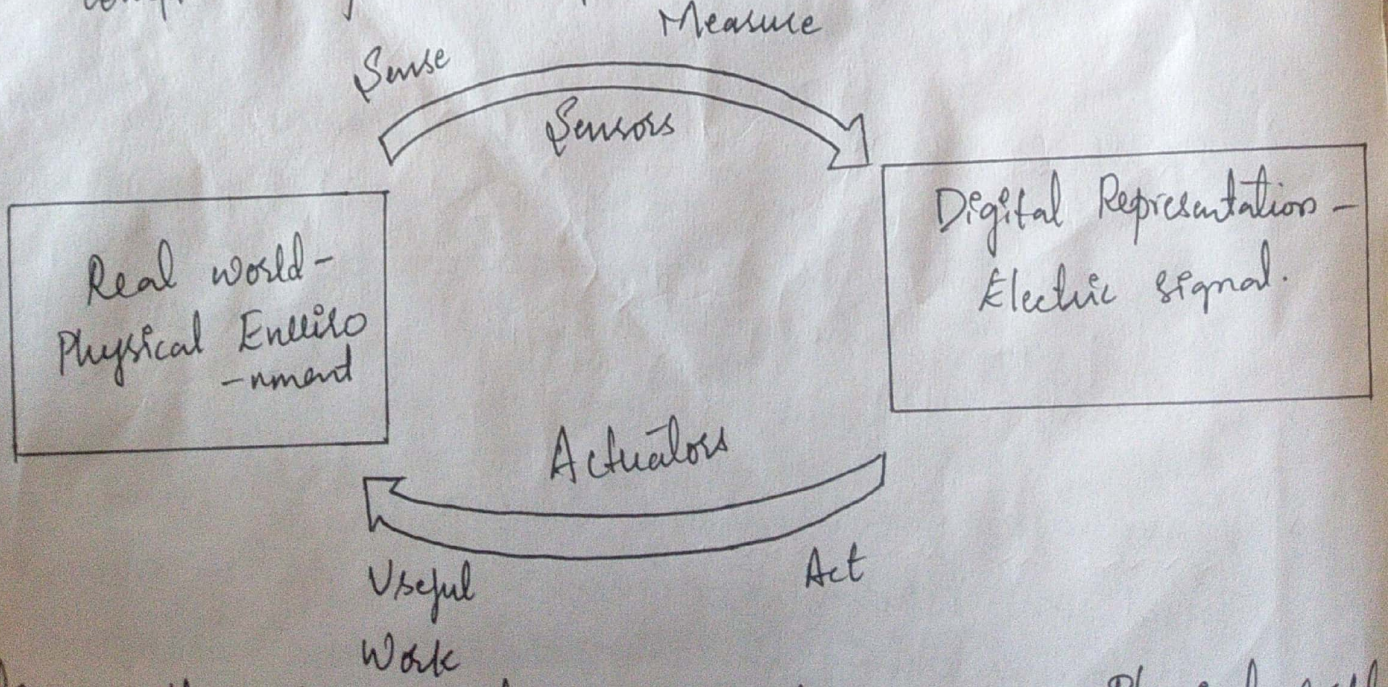
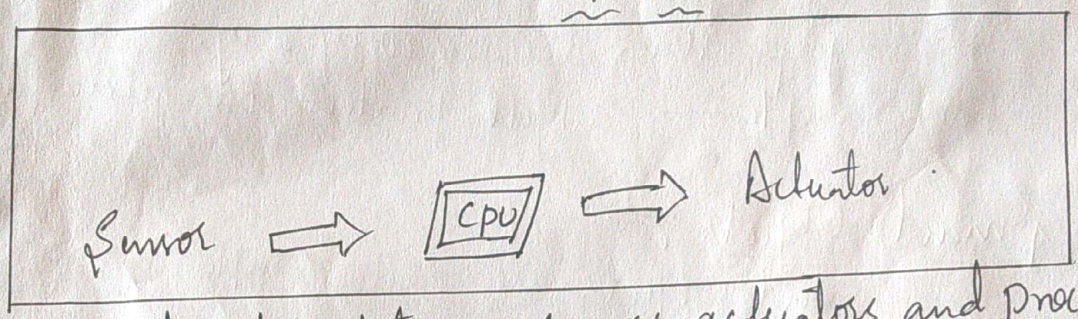


Figure: How Sensors and Actuators Interact with the Physical World.

We all know that the sensors convert their measurable (analog) into electrical signals or digital representation that can be consumed by an intelligent agent (device/human).

On the other hand, Actuators receive some type of control signal (electrical / digital) that triggers a physical effect, usually some type of motion, force and so on.....

figure :- Comparison of sensor and Actuator functionality with human.



This interaction between sensors, actuators and processors and the similar functionality in biological systems is the basis for various technical fields, including robotics and biometrics.

Like sensors, actuators also vary greatly in function, size, design and so on. Some common ways include the following:-

* Type of motion :- Actuators can be classified based on the type of motion they produce (eg- linear, rotary, etc).
* Power :- Actuators can be classified based on their power output (eg- high power, low power etc).
* Binary or Continuous :- Actuators can be classified based on the number of stable-state outputs.
* Area of application : Actuators can be classified based on the specific industry or vertical where they are used.
* Type of energy : Actuators can be classified based on their energy type.

* Micro-Electro-Mechanical System (MEMS) :—

The most interesting advances in sensors and actuators are how they are deployed. MEMS are referred as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuator on small scale.

- The combination of tiny size, low costs, and the ability to mass produce makes MEMS an attractive option for a huge number of IOT applications.
- MEMS devices have already been widely used in a variety of different applications and can be found in very familiar devices every day. for example — inkjet printers use micro pump MEMS.

* Smart Objects :—

Smart objects are quite simple, the building blocks of IOT.

Consider, if a sensor is a standalone device that simply measures the humidity of the soil, it is interesting and useful, but it is not revolutionary.

If that same sensor is connected as part of an intelligent network that is able to co-ordinate intelligently with actuators to trigger irrigation systems as needed based on those sensor readings, we have something far and powerfull.

- Smart objects : A Definition

Often used terms such as "smart sensor, smart device, IOT device, intelligent device, thing, smart thing, intelligent node, intelligent thing, Ubiquitous thing, and intelligent product", are one at the same and have similar meaning, hence we provide that smart object - a device that has minimum, the following four defining characteristics :—

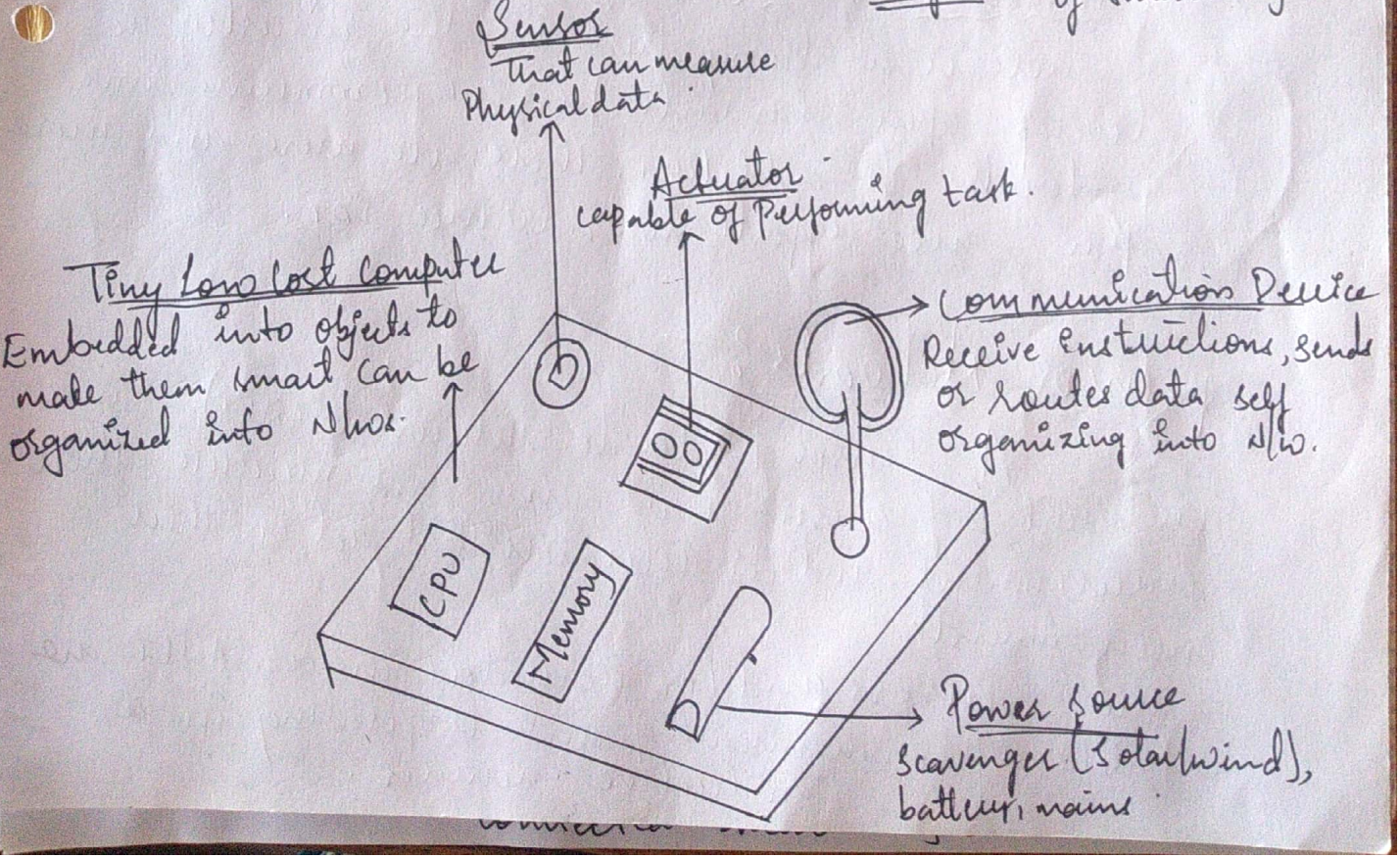
→ Processing Unit :- A smart object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensor(s), coordinating control signals to any actuators and controlling a variety of functions on the smart object, including the communication and power system.

→ 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.

figure : Characteristics of smart object



→ Trends in Smart Objects:-

The following are some broad generalizations and trends impacting IOT:

→ Size is decreasing:- Some smart objects are so small they are even not visible to the naked eyes. This reduced size makes smart objects easier to embed in everyday objects.

→ Power consumption decreasing:- The different hardware components of smart object continually consume less power. This is true for sensors which are completely passive.

→ Processing Power is increasing:- Processors are continually getting more powerful and smaller. This is the key advancement for smart objects, as they become increasingly complex and connected.

→ Communication capabilities are improving:- It is not big surprise that wireless speeds are continually increasing, but they are also increasing in range.

→ Communication is being increasingly standardized:- There is a strong push in the industry to develop open standards for IOT communications protocols. In addition, there are more and more open source efforts to advance IOT.

Sensor Networks:-

A sensor / actuator network (SANET) - 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 b/w distributed sensors and actuators.
- while some networks can theoretically be connected in wired or wireless fashion, the fact that SANETs are typically found in the "real world" means that they need an extreme level of deployment flexibility.

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

→ Advantages :-

* Greater deployment flexibility
* 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 :-

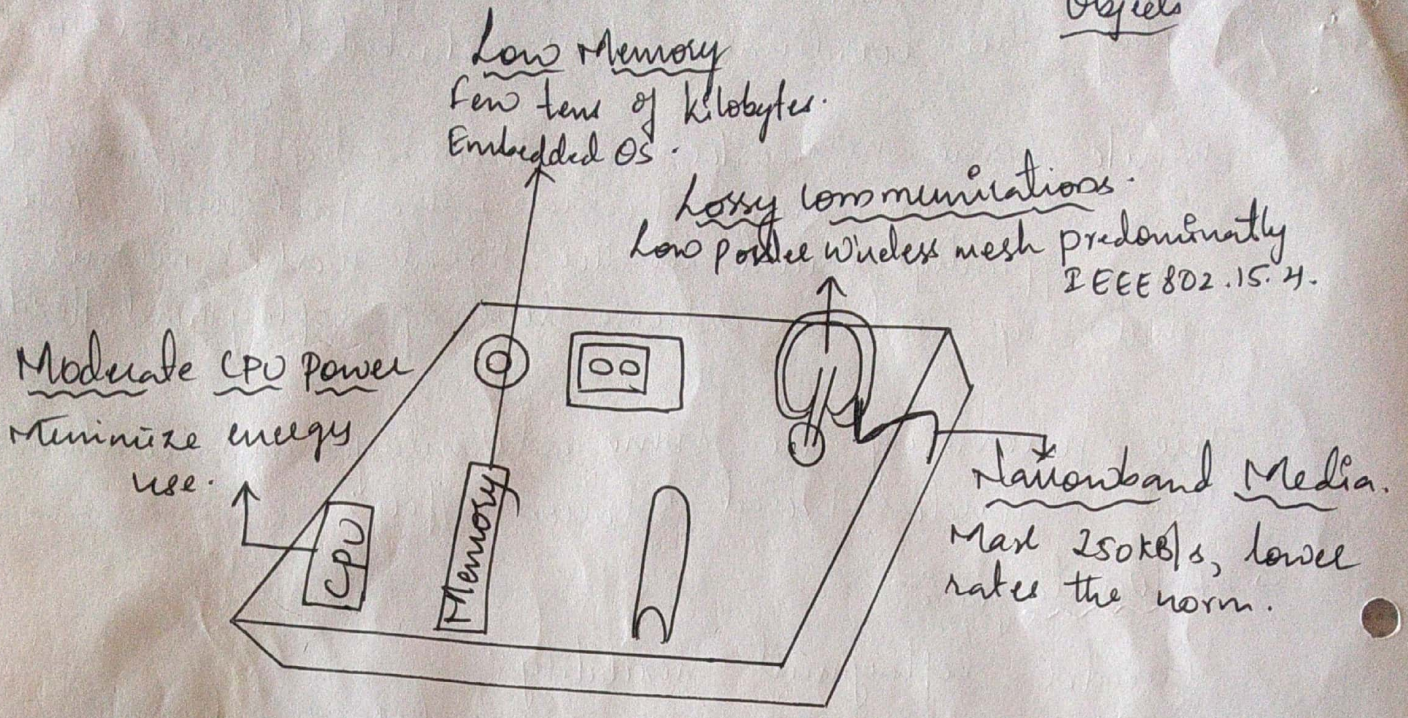
* Potentially less secure
* Typically lower transmission speeds
* Greater level of impact/influence by environment.

* Wireless Sensor Network (WSNs) :-

Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as motes.

The fact that there is no infrastructure to consider with WSNs is surely a powerful advantage for flexible deployments, but there are a variety of design constraints to consider with these wirelessly connected smart objects.

Figure:- Design constraints for wireless Smart Objects.



Power consumption is critical
Energy efficiency is Paramount
Battery Powered devices must last years.

The following are some of the most significant limitations of 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.

CHAPTER-2 : Connecting Smart Objects

Communications Criteria :-

In the world of connecting "things", a large number of wired and wireless access technologies are available or under development.

Wireless communication is prevalent in the world of smart object connectivity, mainly because it eases deployment and allows smart objects to be mobile, changing location without losing connectivity.

Range :- The following are the categories of ranges :-

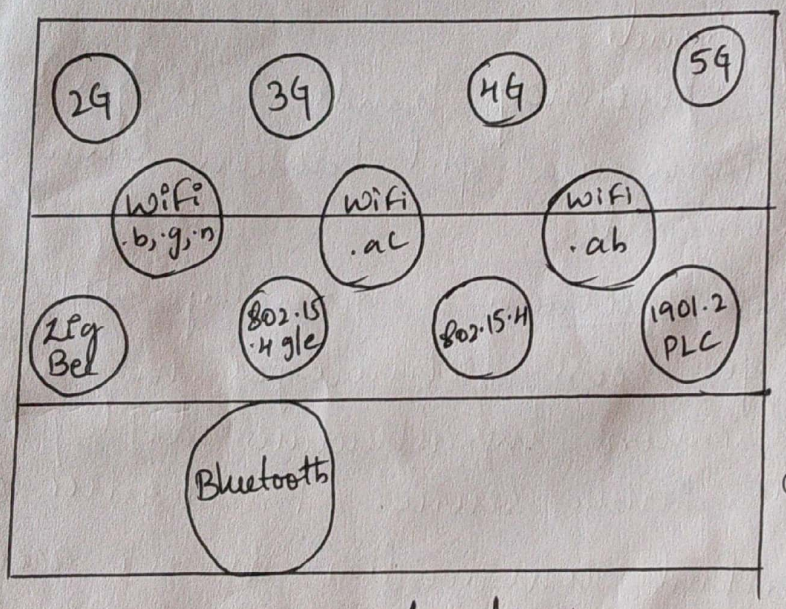


Figure : Wireless Access Landscape.

→ **Short range :-** 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 - Short range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7

→ **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, although RF technologies do not have real maximum distances defined.
Example - medium range wireless technologies include IEEE 802.11 wifi, IEEE 802.15.4 etc.

→ Long range :- Distance greater than 1 mile between two devices require long-range technologies wireless examples are cellular (2G, 3G, 4G 80 km) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-power wide-Area (LPWA) technologies.

* Frequency Bands :-

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 communication infrastructures deployed by services providers, public services, broadcasters and utilities.

- An important consideration for IoT access Infrastructure that needs to utilize licensed spectrum is that users must subscribe to services when connecting their IoT devices.

Examples of Licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.

Unlicensed band — Means that no guarantees or protections are offered in the RSM bands for device communications. For IoT access, these are the most well-known RSM bands:

- 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
- IEEE 802.15.1 Bluetooth
- IEEE 802.15.4 WPAN.

→ Unlicensed band/spectrum is usually simpler to deploy than licensed because it does not require a service provider.

- The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies.

→ Power Consumption :— A powered node has a direct connection to a power source, and communications are usually not limited by power consumption criteria.

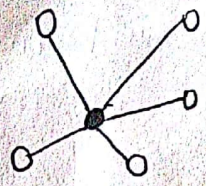
- Battery-powered nodes bring much more flexibility to IoT devices. These nodes are often classified by the required lifetimes of their batteries.

- IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes.

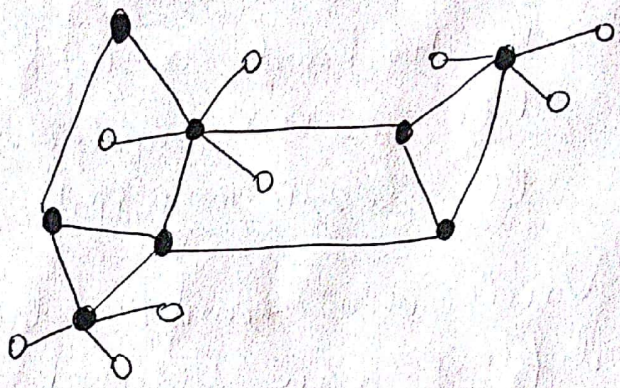
- Topology :— The access technologies available for connecting IoT devices, three main topology schemes are dominant : Star, mesh and peer-to-peer.

Figure : Star, Peer-to-peer and Mesh Topologies

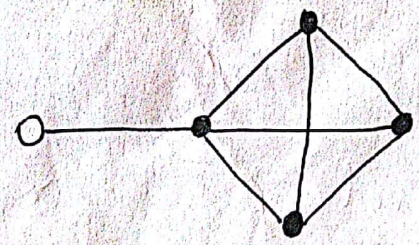
Star Topology



Mesh Topology



Peer-to-peer Topol



- Full function Device
- Reduced function Device

- 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.
- A mesh topology helps cope with low transmit power, searching to each a greater

A Mesh topology requires the implementation of a Layer 2 forwarding protocol known as mesh-over on each intermediate node.

Constrained Devices :-

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

→ Classes of constrained Nodes, as Defined by RFC 7228.

Class	Definition
– Class 0	This class of nodes is severely constrained, with less than 10KB of memory and less than 100 KB of flash processing and storage capability. 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 of class 1 are still low than expected for a complete IP stack implementation. 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 50KB of memory and 250 KB of flash, so they can be fully integrated in IP networks. A smart power meter is an example of class 2 node.

IOT Access Technologies :—

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.

- IEEE 802.15.4 is commonly found in the following types of deployments : i) Home and building automation ii) Automotive networks iii) Industrial wireless sensor networks iv) Interactive toys and remote controls.

→ **Standardization and Alliance :—**

IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area network (WPAN).

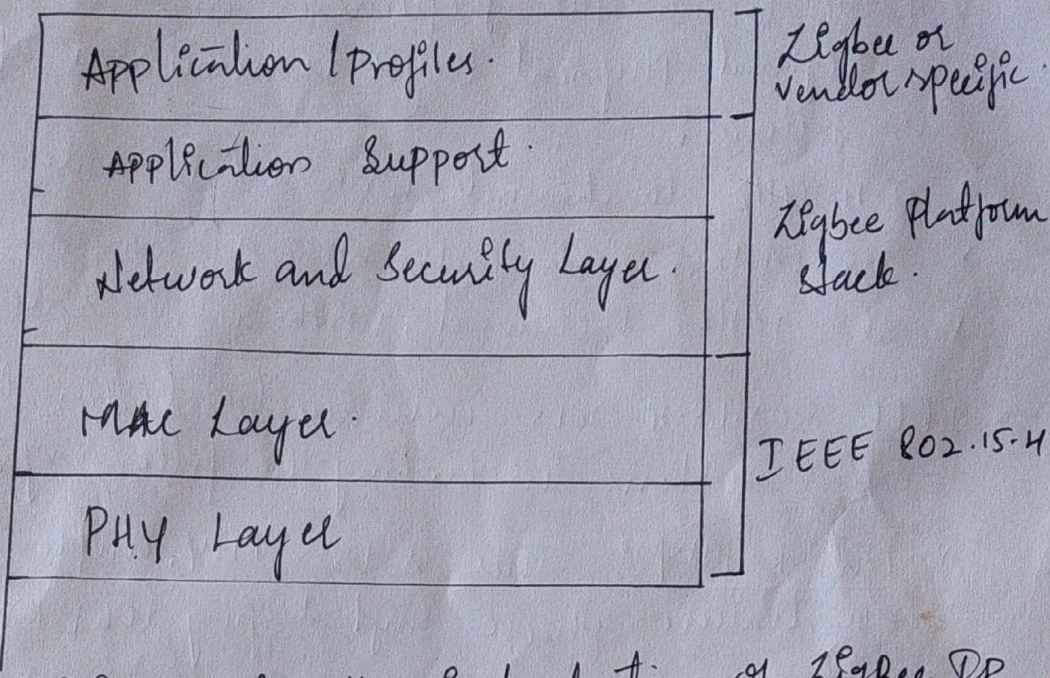
- There are some protocol stacks utilizing IEEE 802.15.4, are — ZigBee, 6LOWPAN, ZigBee IP, ISA100.11a, WirelessHART, Thread

ZigBee :— The basic idea of ZigBee-style networks in the late 1990s, ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs. The main Area where ZigBee is the most well-known include automation for commercial, retail and home applications and smart energy.

The traditional ZigBee stack is illustrated in the above figure. ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers.

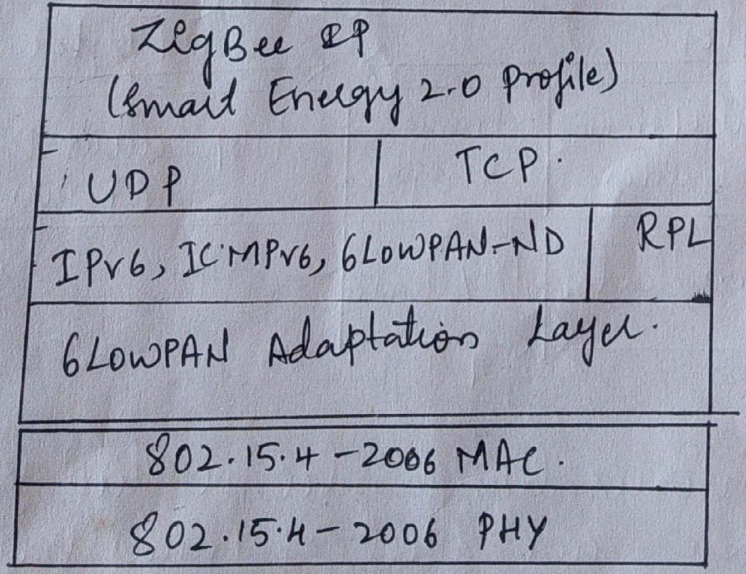
- ZigBee specifies the network and security layer and supporting layer that sit on top of the lower layers
- The ZigBee network and security layer provides mechanisms for network startup, configuration, routing and securing communications.

Figure :- High-Level ZigBee Protocol Stack.



→ ZigBee IP :- With the introduction of ZigBee IP, the support of IEEE 802.15.4 continues, but the IP and TCP/UDP protocols and various other open standards are now supported at the network and transport layers.

Figure :- ZigBee IP Protocol Stack.



ZigBee IP was created to embrace the open standards coming from the IETF's work on LLN's, such as IPv6, 6LOWPAN, and RPL.

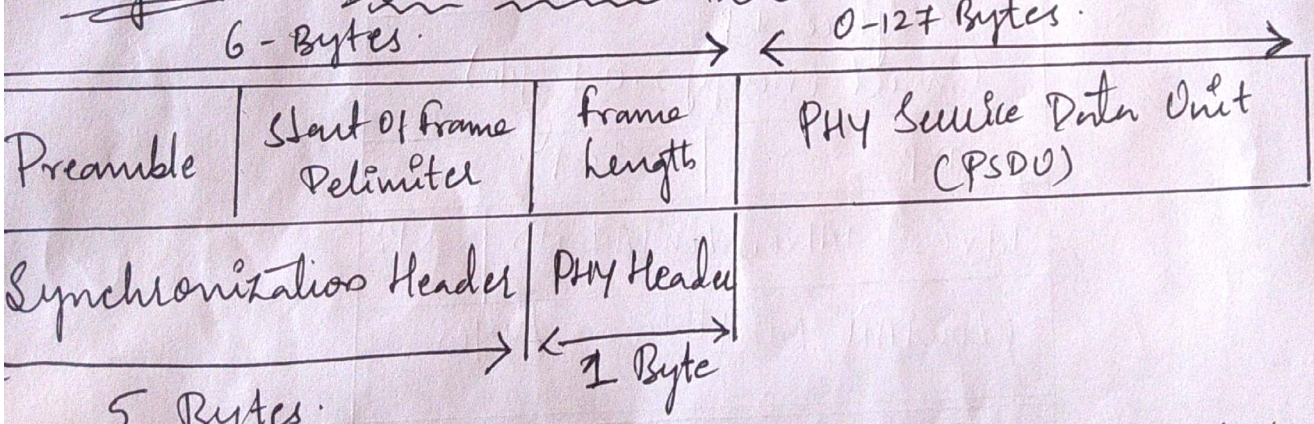
They Provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.

→ Physical 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 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 802.15.4-2015 introduced additional PHY communication options, including the following:
  * QPSK PHY: This is DSSS PHY, employing offset quadrature phase-shift keying (QPSK) modulation.
  * BPSK PHY: This is DSSS PHY, employing binary Phase-shift keying (BPSK) modulation.
  * ASK PHY: This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (OOK) and BPSK modulation.

Figure:- IEEE 802.15.4 PHY Format.



- The synchronization header for this frame is composed of Preamble and Start of Frame Delimiter fields.
- The Preamble field is a 32-bit 4-byte pattern that identifies the start of the frame and is used to synchronize the data transmission.
- The Start of Frame Delimiter field informs the receiver that frame contents start immediately after this byte.

MAC Layer :-

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.

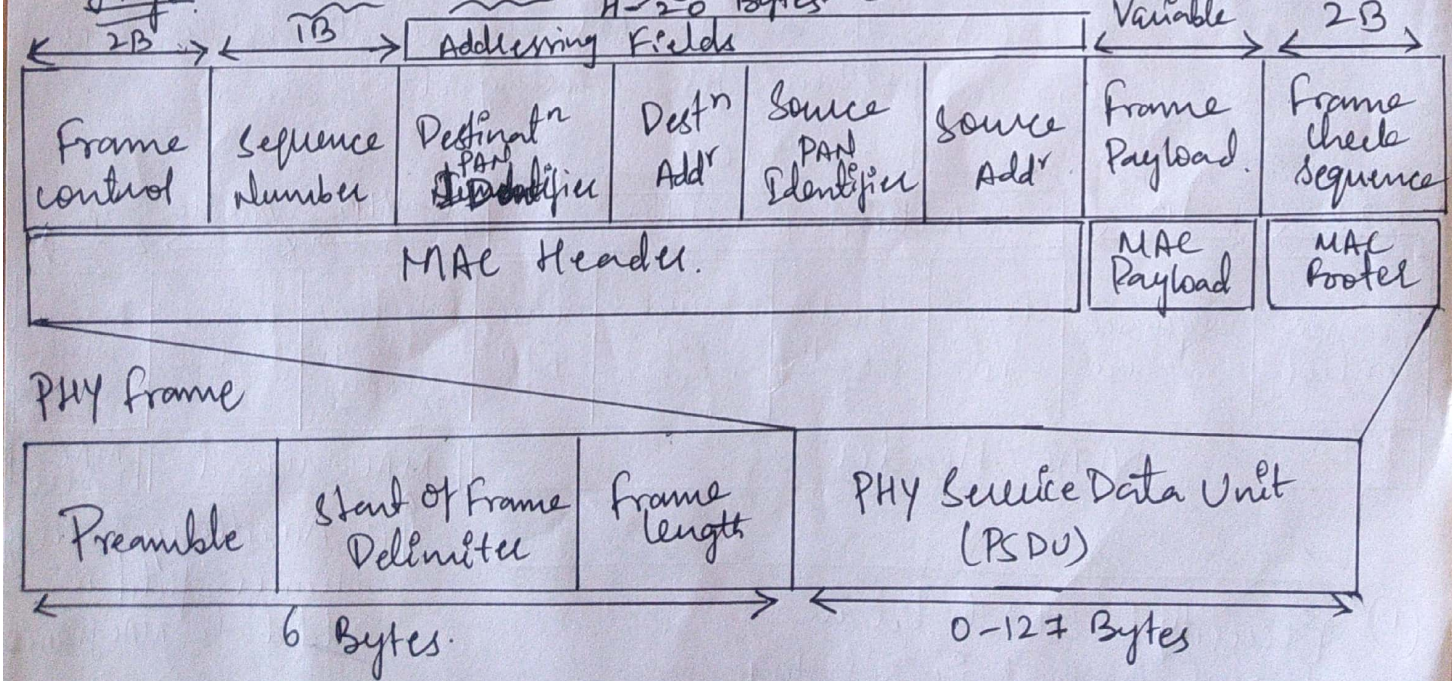
→ The 802.15.4 MAC layer performs the following tasks:

* Network beaconing for devices acting as coordinators
* PAN association and disassociation by a device
* Device security
* Reliable link communications between two peer MAC entities

→ The following are the four types of MAC frames specified in 802.15.4

* Data frame: Handles all transfers of data
* Beacon frame: Used in the transmission of beacon from a PAN coordinator.
* Acknowledgement frame: Confirms the successful reception of a frame.
* MAC command frame: Responsible for control communication between devices.

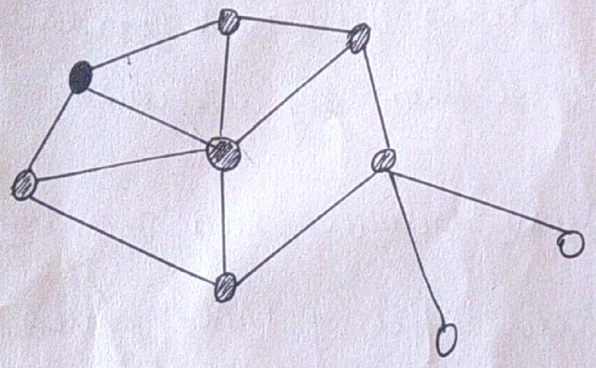
Figure: IEEE 802.15.4 MAC Format



Topology :-

IEEE 802.15.4 -based networks can be built as star, Peer-to-peer, or mesh topologies.

Figure :- 802.15.4 Sample Mesh Network topology.



- PAN coordinator
- Full function Device
- Reduced Function Device.

- Every 802.15.4 PAN should be set up with a unique ID. and all the nodes in the same 802.15.4 network should use the same PAN ID.
- The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology. This function can be done at Layer 2 and is known as mesh-under.

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.

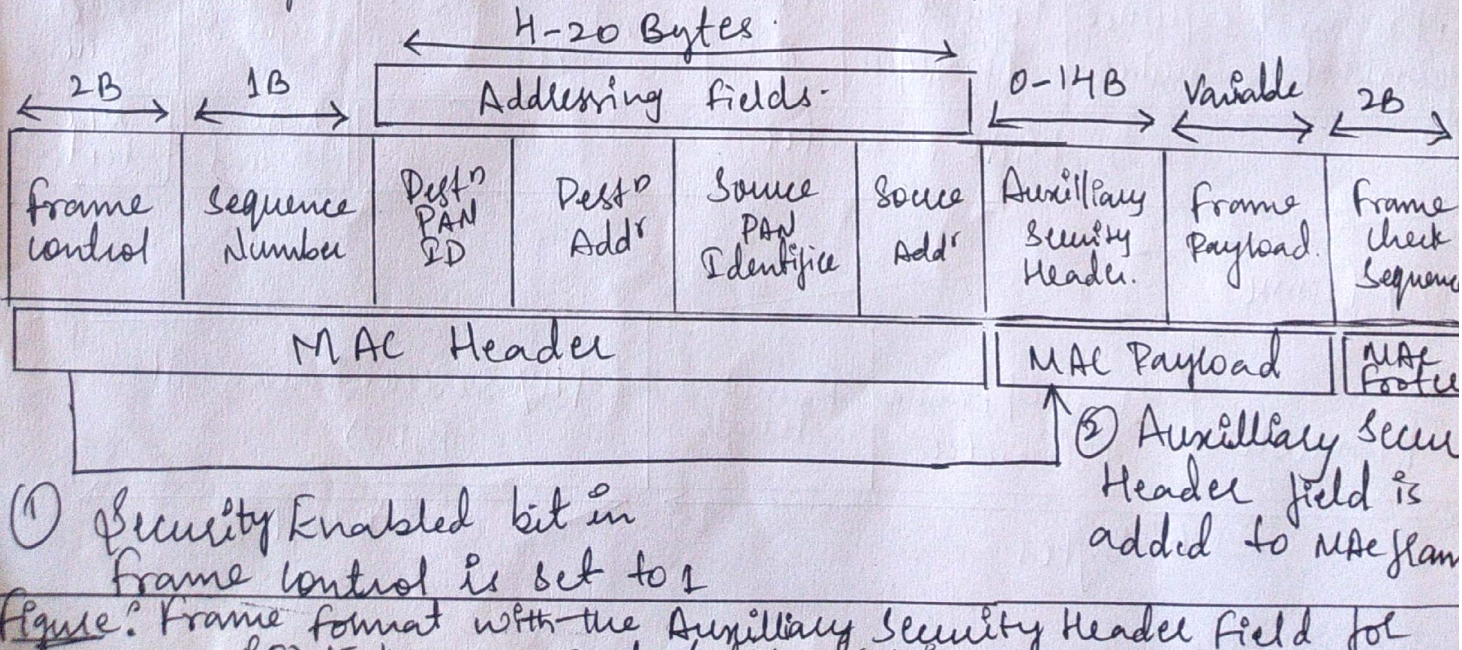


Figure: Frame format with the Auxiliary Security Header field for 802.15.4-2006 and later version.

Competitive Technologies :-

A competitive radio technology that is different in its PHY and MAC layers is DASH7. A DASH7 was originally based on the ISO18000-7 standard and positioned for industrial communications, whereas IEEE 802.15.4 is more generic.

- Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military forces for many years, mainly for logistics purposes.
- DASH7 is promoted by the DASH7 Alliance, which has evolved the protocol from its active RFID niche into a wireless sensor network technology that is aimed at the commercial market.

⇒ IEEE 802.15.4g and 802.15.4e :-

- The IEEE 802.15.4e amendment of 802.15.4-2011 expands the MAC layer feature set to remedy the disadvantages associated with 802.15.4, including MAC reliability, unbounded latency and multipath fading.
- The IEEE 802.15.4g-2012 is also an amendment to the IEEE 802.15.4-2011 standard, and just like 802.15.4e-2012, it has been fully integrated into the core IEEE 802.15.4-2015 specification.
- This technology applies to IOT use cases such as the following.
  - → Public lighting
  - → Environmental wireless sensors in smart cities
  - → Electrical vehicle charging stations
  - → Smart parking meters.
  - → Microgrids.

→ Standardization and Alliances :—

Because 802.15.4g-2012 and 802.15.4e-2012 are simply amendments to IEEE 802.15.4-2011, the same IEEE 802.15 Task Group 4 standards body authors, maintains and integrates them into the next release of the core specification.

→ Physical Layer :—

In IEEE 802.15.4g-2012, the original IEEE 802.15 maximum PSDU or Payload size of 127 bytes was increased for the SUN PHY to 2047 bytes.

— IEEE 802.15.4g compliant :

* Multi-Rate and Multi-Regional Frequency shift keying (MR-FSK)
* Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM)
* Multi-Rate and Multi-Regional Offset Quadrature Phase-shift keying (MR-OQPSK).

Head of the Dept.
Computer Science & Engineering
Basavakalyan Engineering College
BASAVAKALYAN