UNIT 2

Smart Objects: The Things in IOT

Smart objects: The "Things" in IoT, Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access, Technologies, IoT platforms, Programming with Arduino, Programming with Raspberry Pi and Node MCU

Sensors, Actuators and Smart objects

What is a sensor?

Sensor is a device which is able to detect changes in an environment and respond to environment.

Sensor converts physical attribute to electrical signal which is then converted to digital or analog signal which then sent to another device for transformation into useful data that can be consumed by intelligent devices or humans. example: light sensors, thermostat sensor, pressure sensors etc..

There are a number of ways to group and cluster sensors into different categosies include 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 power supply (passive).

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

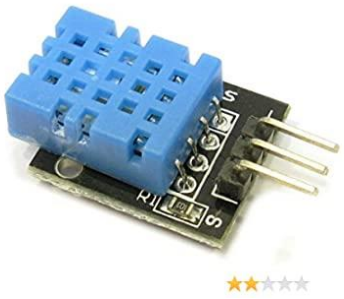
Contact or no-contact: Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).

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).

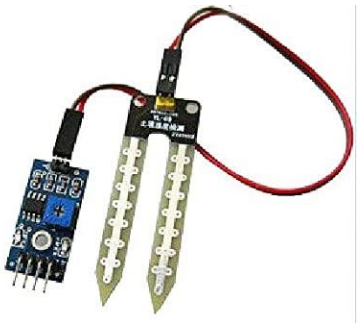
Area of application: Sensors can be categorized based on the specific industry or vertical where they are being used.

How sensors measure: Sensors can be categorized based on the physical mechanism used to measure sensory input (for example,thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photoelastic).

What sensors measure: Sensors can be categorized based on their applications or what physical variables they measure.



Temperature and humidity sensor



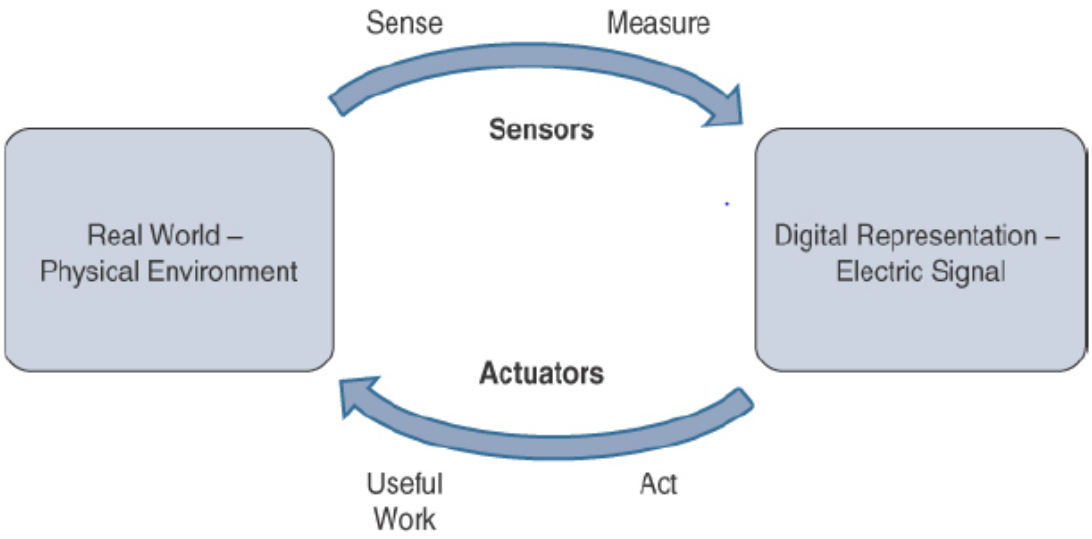
Soil Moisture Sensor

Difference between sensor and actuator?

Sensor convert physical attribute to electrical signal like it sense temperature by measuring heat and converts into electrical signal.

Where an **actuator** converts electrical signal into physical action by keeping some temperature value as threshold, if temperature value goes beyond threshold then motor should on, here motor becomes actuator.

They are devices which transform an input signal (mainly an electrical signal) into some form of motion.



Actuators are classified based on

Type of motion

Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).

Power

Actuators can be classified based on their power output (for example, high power, low power, micro power)

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.

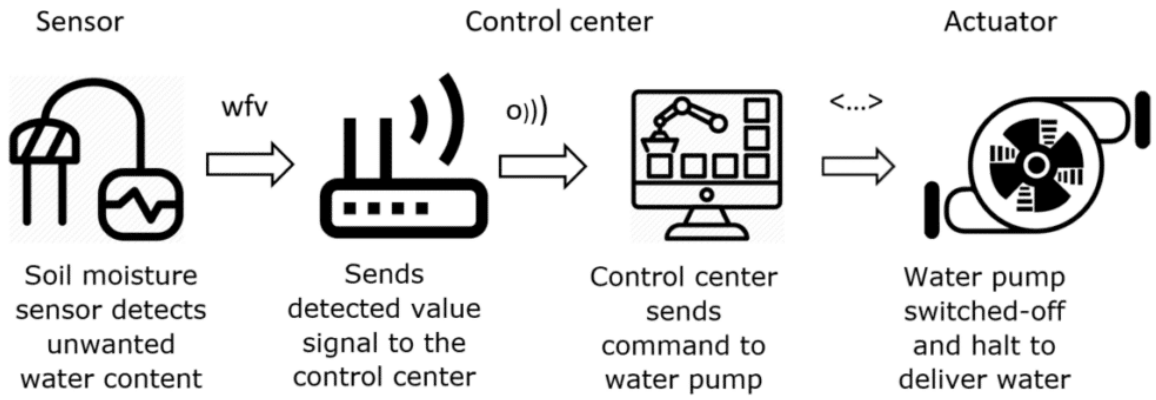
Type of energy

Actuators can be classified based on their energy type.

Below table shows classification of actuators base on energy

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

While sensors give the data, actuators give the activity. The most fascinating use cases for IoT are those where sensors and actuators cooperate in an insightful, key, and correlative style. This incredible mix can be utilized to take care of ordinary issues by just lifting the information that sensors give to noteworthy understanding that can be acted on by work-delivering actuators.



Example:

Soil moisture sensor detects moisture content in soil and sensor to microcontroller which is control center where threshold value is set. If soil moisture value is above the threshold value then automatically water pump should on .

Here water pump is **Actuator**

MEMS-Micro-Electro-Mechanical system

- MEMS are micro machines can integrate and combine electric and mechanical elements such as machines.
- **It is a technology used to do small integrated devices or systems that is a combination of mechanical and electrical components**.
- One of the keys to this technology is **a microfabrication technique that is similar to what is used for microelectronic integrated circuits.**
- This approach allows mass production at very low costs. The combination of tiny size, low cost, and the ability to produce makes MEMS an attractive option for a huge number of IoT applications.
- Smart phones also use MEMS technologies for things like accelerometers and gyroscopes. In fact, automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers.
- Size can vary from a few micrometres to millimetres.
- MEMS uses batch processing technologies.
- Sensors sucha as MEMS accelerators,MEMS pressure sensors,tilt sensor and other types of sensors
- Actuators such as MEMS switches ,micro pumps, micro-levels and micro-grippers.

Smart objects:

- A smart object is an object that enhances the interaction with not only people but also with other smart objects.
- Also known as smart connected products or smart connected things (SCoT), they are products, assets and other things embedded with processors, sensors, software and connectivity that allow data to be exchanged between the product and its environment, manufacturer, operator/user, and other products and systems.(wiki)
- Connectivity also enables some capabilities of the product to exist outside the physical device, in what is known as the product cloud.
- The data collected from these products can be then analyzed to inform decision-making, enable operational efficiencies and continuously improve the performance of the product.

Smart Objects: A Definition

Historically, the definition of a smart object has been a bit nebulous because of the different interpretations of the term by varying sources.

To add to the overall confusion, the term smart object, despite some semantic differences, is often used interchangeably with terms such **as smart sensor, smart device, IoT device, intelligent device, thing, smart thing, intelligent node, intelligent thing, ubiquitous thing, and intelligent product.**

A smart object is a device that should have following characteristics:

1.Processing unit:

A smart object must have processing unit for getting data, processing and analysing 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.

The most common is a microcontroller because of its small form factor, flexibility, programming simplicity, ubiquity, low power consumption, and low cost.

2.Sensors and actuators:

A smart object is capable of interacting with the physical world through sensors and actuators. Depending on application one or more sensors and actuators are used.

3.Communication device:

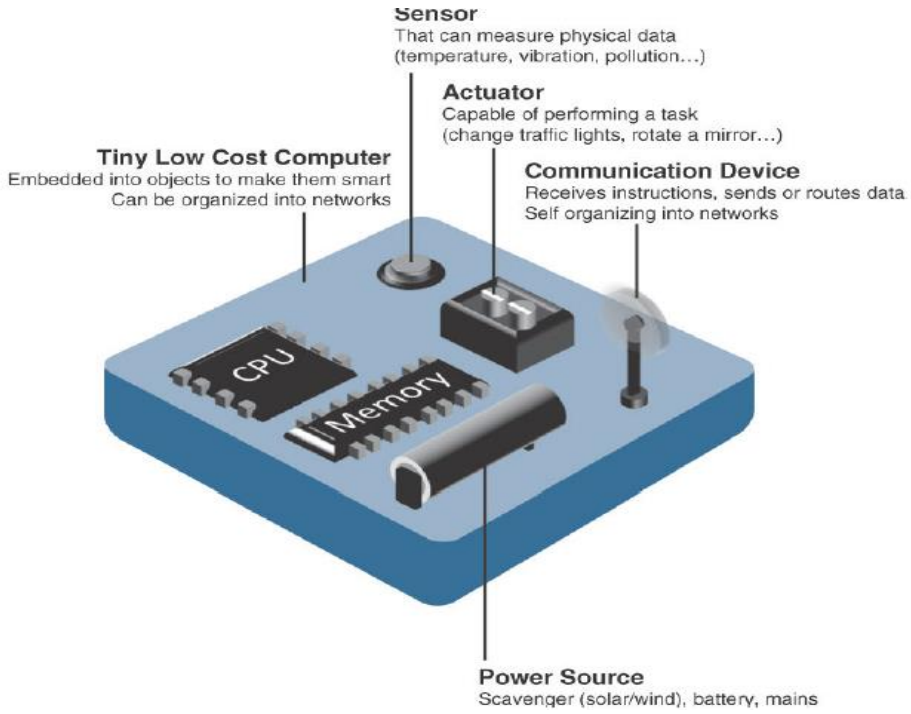
To talk with one smart object to another smart objects and to connect to network communication device is required . Connection between the devices can be either wired or wireless. Overwhelmingly, in IoT networks smart objects are wirelessly interconnected for a number of reasons, including cost, limited infrastructure availability, and ease of deployment. There are myriad different communication protocols for smart objects

4.Power source:

Power source is one of the most significant part . As with the other three smart object building blocks, the power requirements also vary greatly from application to application.

since power for smart objects are limited in power which needs to be run for long time and are not easily accessible.

This combination, especially when the smart object relies on battery power, implies that power efficiency, judicious power management, sleep modes, ultra-low power consumption hardware, and so on are critical design elements.



Characteristics of a smart object

Trends in smart objects:

Following are trends impacting Smart object

Size is decreasing: Some smart objects are very small .this reduced size makes smart objects easier to embed in day to day objects.

Power consumption is decreasing: Many sensors consume less power that can be battery powered. Some battery-powered sensors last 10 or more years without battery replacement.

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

Communication capabilities are improving: It's no big surprise that wireless speeds are continually increasing, but they are also increasing

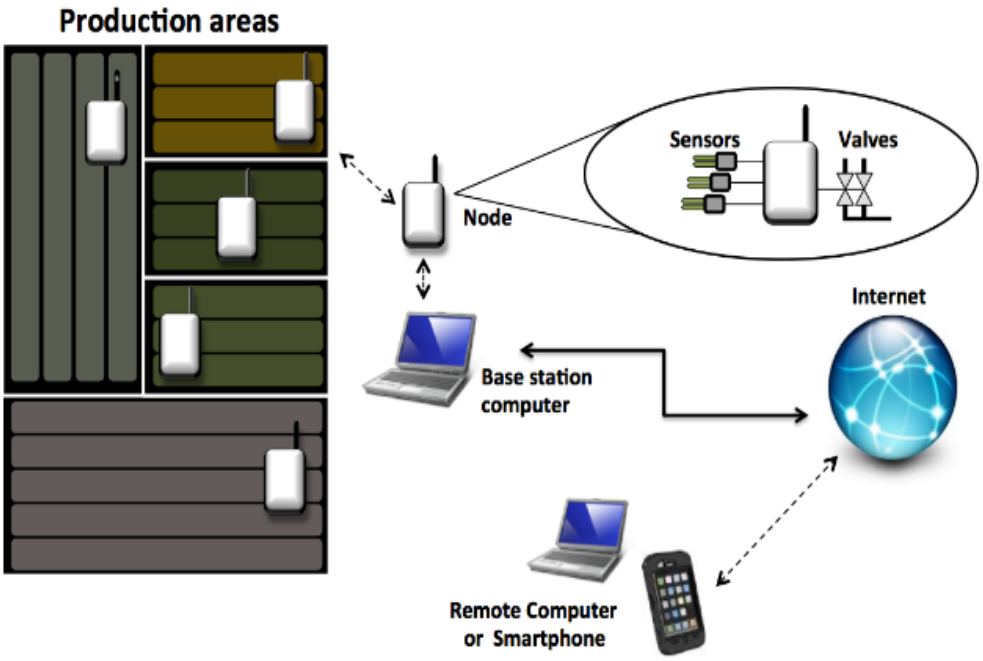
in range.

Communication is being increasingly standardized: There is a strong push in the industry to develop open standards for IoT communication protocols.

Sensor Networks:

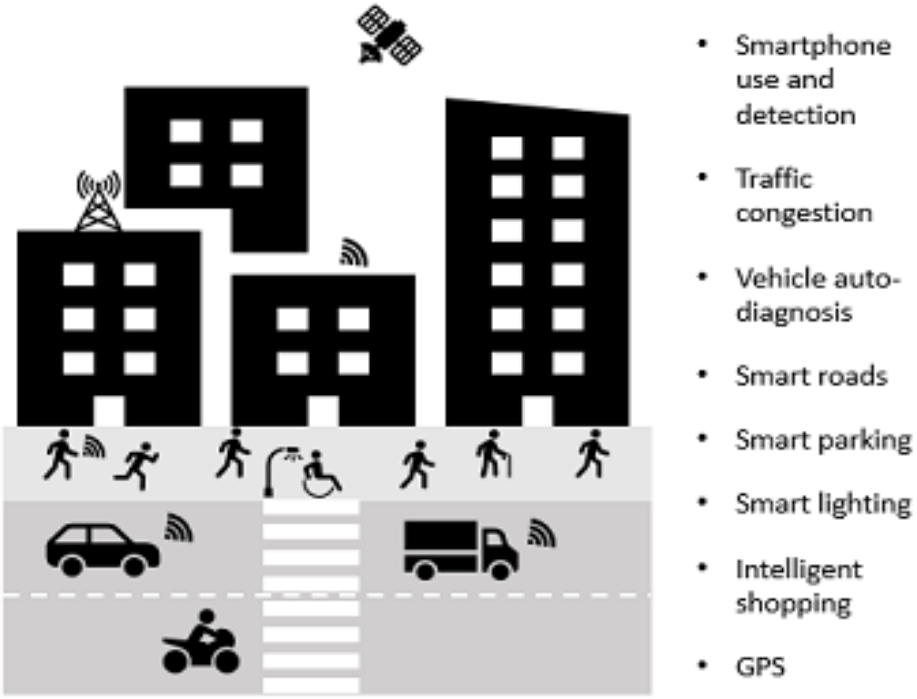
What is a Sensor networks?

- 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.
- While such networks can theoretically be connected in a 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.

- Today sensors are everywhere. We take these for granted, but sensors are in our phones, workplaces, vehicles, and the environment.
- A sensor network comprises a group of small, powered devices, and a wireless or wired networked infrastructure. They record conditions in any number of environments including industrial facilities, farms, and hospitals. The sensor network connects to the internet or computer networks to transfer data for analysis and use.
- Sensor network nodes cooperatively sense and control the environment. They enable interaction between persons or computers and the surrounding environment.



Advantages:

- Greater deployment flexibility.
- Simpler scaling to a larger number of nodes.
- Lower implementation costs
- Easier long-term maintenance.

- Effortless long-term maintenance

Disadvantages:

- Less secure
- Less transmission speed

Wired vs wireless Sensor network

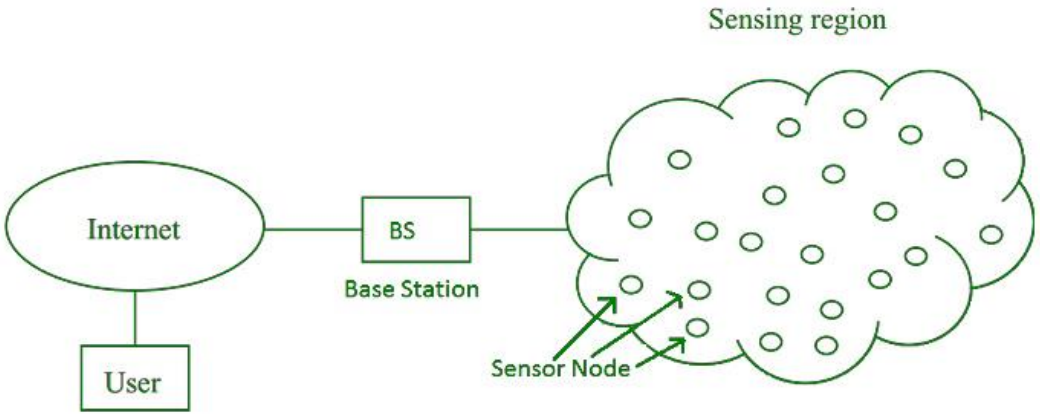
Sensor network can be wired or wireless. wired network use ethernet cables to connect sensors.

Wireless sensor network use technologies such as
Bluetooth, cellualar, wifi or near field communication to connect sensors.

Wireless Sensor Network(WSN)

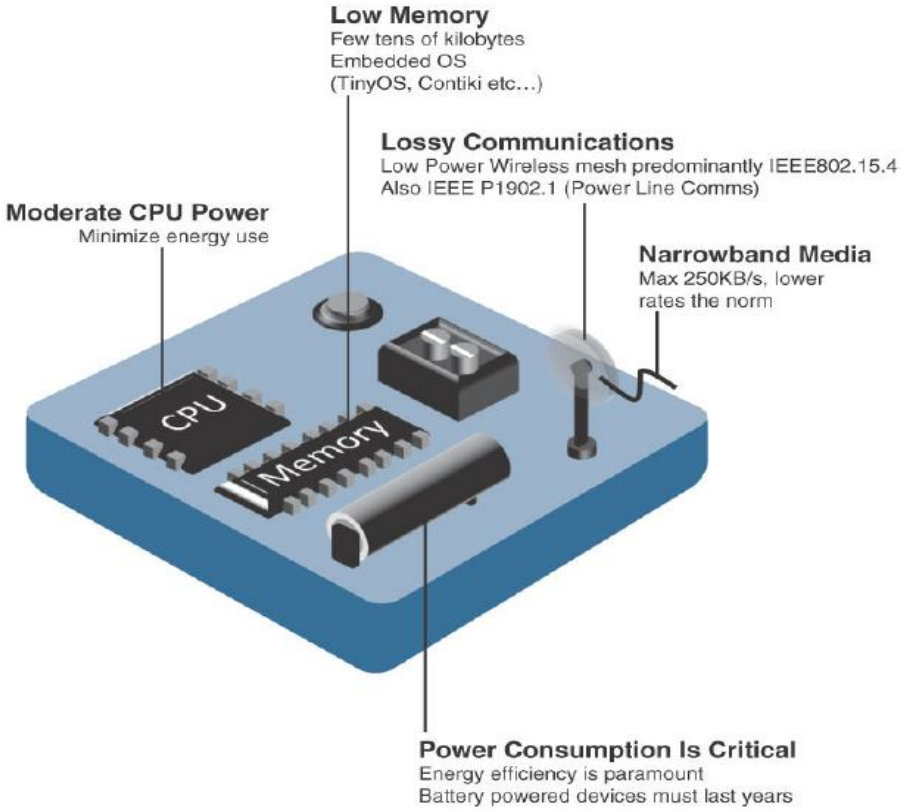
With the rapid development of sensors and wireless technologies, WSNs have become a key technology of the IoT .

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.(wiki)



As name suggests connecting smart objects wirelessly which are referred to as **motes.**

WSNs are easier to deploy and maintain and offer better flexibility of devices. WSNs don't need the physical network infrastructure to be modified.



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

Smart objects with limited processing, memory, power, and so on are often referred to as constrained nodes.

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.

Communication Protocols for Wireless Sensor Networks

- Since advancement in IOT technology in many areas the number of sensors deployed is increasing day by day and WSNs are becoming heterogenous with more interactions.
- WSNs must communication may vary from one type sensor to multiple type of sensors.
- Here challenge occurs since communication must happen in heterogeneous environment.
- The protocols governing the communication for WSNs must deal with the inherent defining characteristics of WSNs and the constrained devices within them

- Any communication protocol must be able to scale to a large number of nodes.
- When selecting a communication protocol, you must carefully take into account the requirements of the specific application and consider any trade-offs the communication protocol offers between power consumption, maximum transmission speed, range, tolerance for packet loss, topology optimization, security, and so on.
- Wireless sensor networks interact with their environment. Sensors often produce large amounts of sensing and measurement data that needs to be processed. This data can be processed locally by the nodes of a WSN or across zero or more hierarchical levels in IoT networks.
- Communication protocols need to facilitate routing and message handling for this data flow between sensor nodes as well as from sensor nodes to optional gateways, edge compute, or centralized cloud compute. IoT communication protocols for WSNs thus straddle the entire protocol stack. Ultimately, they are used to provide a platform for a variety of IoT smart services

Connecting Smart objects:

All of us used internet for browsing the web,reading and sending email, listening to music. But familiarity with the Internet is very much on a gradient. Using the Internet daily is a first step in understanding it; developing software or Things that speak to the Internet is another; and developing or debugging the software that runs the Internet itself is yet another.

After getting to know about smart objects which consists of sensors, actuators, microcontrollers after setting up ,the next step is to connecting the smart object. There are different protocols to connect them.

Communication criteria

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

The characteristics and attributes to consider when selecting and dealing with connecting smart objects.

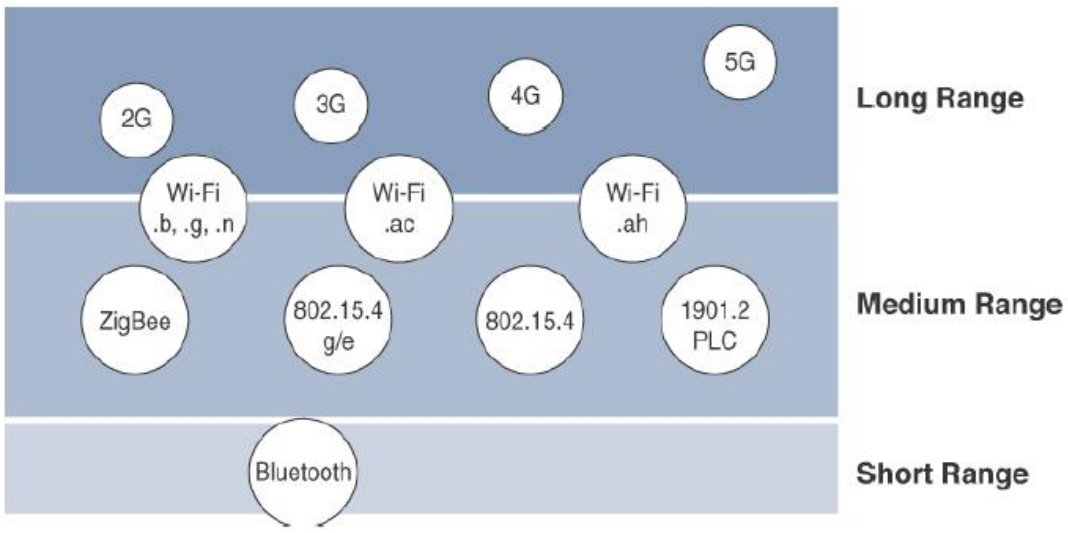
Range:

One of the important criteria to be considered

How far smart object signal need to be propagated?

How much are area wireless technology is going to cover?

Should indoor versus outdoor deployments be differentiated?



The above figure shows categorization of technologies like:

Short range:

In case of wired example is a serial cable.

In case of wireless,technology that supports maximum of ten meter between two devices. example: Bluetooth and visible light communication.

Medium range:

Most of the IOT devices use this technology .the range is from ten to hundred meters, Maximum range is generally less than 1 mile between two devices. Examples of medium-range wireless technologies include IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN. Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC) may also be classified as medium range, depending on their physical media characteristics.

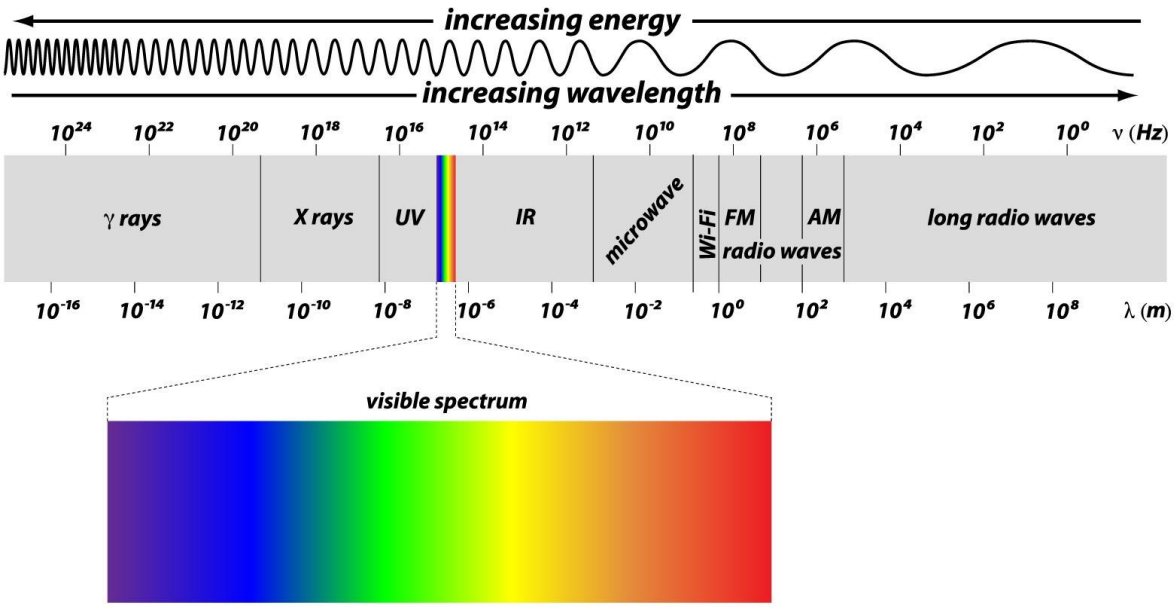
Long range:

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.

Frequency Bands

Most IoT systems link networks of sensors via **radio waves**, which transmit data from one place to another.

Radio waves, which are primarily used in communication technologies, are a type of electromagnetic radiation (a form of energy); they make up a small part of what is called the **electromagnetic (EM) spectrum,** which is divided up into sections called **frequency bands.**



A frequency band is an interval in the frequency domain, delimited by a lower frequency and an upper frequency. The term may refer to a radio band or an interval of some other spectrum**.**

Radio waves are measured by wavelength or frequency, with wavelength being the distance between two identical points in a waveform signal, and frequency referring to the number of waves that passes a given point per second. The sweet spot for most modern data communication is between 300 megahertz (MHz) and 6 gigahertz (GHz) frequency.

Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC), to allocate the spectrum so it's used effectively.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.**

For certain users lincesed radio spectrum will be issued by the FCC to certain user like for television and radio broadcaster.

Alternatively, organizations can still use the airwaves to transmit communications without getting permission from the FCC, but they must transmit within those parts of the spectrum that are designated for **unlicensed users**. The amount of spectrum that is available for public and unlicensed use is very small—only a few bands. Both the size of the area and the lack of exclusivity mean there's greater potential for interference from other users located nearby.

Focusing on IoT access technologies, the frequency bands leveraged by wireless communications are split between **licensed and unlicensed bands.**

With the exception of cellular devices, almost all IoT devices operate in the unlicensed spectrum currently.

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.

An important consideration for IoT access infrastructures that wish to utilize licensed spectrum is that users must subscribe to services when connecting their IoT devices

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).

Improvements have been made in handling the complexity that is inherent when deploying large numbers of devices in the licensed spectrum. Thanks to the development of IoT platforms, such as the Cisco Jasper Control Center, automating the provisioning, deployment, and management of large numbers of devices has become much easier. Examples of licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.

Unlicensed means that no guarantees or protections are offered in the ISM bands for device communications. For IoT access, these are the most wellknown

ISM 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

(More details refer page number 169).

Power consumption

Power consumption is another important criteria to consider.

There can two type of power source given to IOT nodes.

1.Powered nodes(external power source)

2.Battery-powered nodes.

Communication are 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. This has led to the evolution of a new wireless environment known as Low-Power Wide-Area(LPWA). Obviously, it is possible to run just about any wireless technology on batteries.

Topology

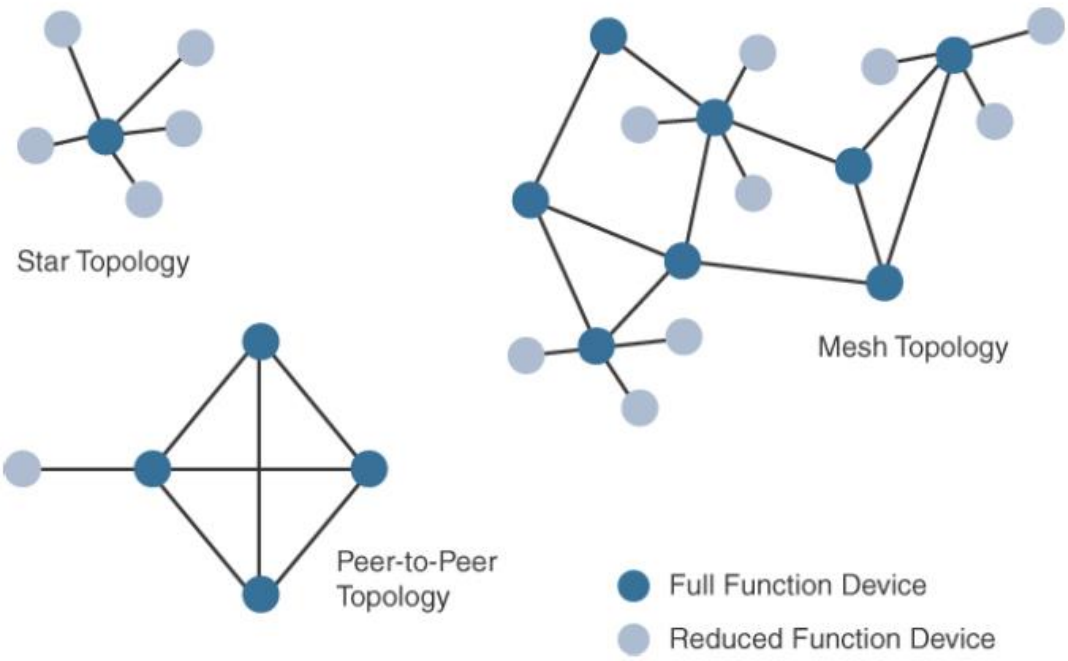
For connecting IOT devices three main topology schemes are dominant:

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, as shown in Figure Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other. Obviously, peer-to-peer topologies rely on multiple full-function devices. Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.



For example, indoor Wi-Fi deployments are mostly a set of nodes forming a star topology around their access points (APs). Meanwhile, outdoor Wi-Fi may consist of a mesh topology for the backbone of APs, with nodes connecting to the APs in a star topology.

A mesh topology helps cope with low transmit power, searching to reach a greater overall distance, and coverage by having
intermediate nodes relaying traffic for other nodes.

Constrained Devices

Small devices with limited CPU, memory, and power resources, so called "constrained devices" (often used as sensors/actuators, smart objects, or smart devices) can form a network, becoming "constrained nodes" in that network.

The Internet Engineering Task Force (IETF) acknowledges in RFC 7228 that different categories of IoT devices are deployed. While categorizing the

class of IoT nodes is a perilous exercise, with computing, memory, storage, power, and networking continuously evolving and improving, RFC 7228 gives some definitions of constrained nodes.

Constrained nodes have limited resources that impact their networking feature set and capabilities. Therefore, some classes of IoT nodes do not implement an IP stack. According to RFC 7228, constrained nodes can be broken down into the classes defined in Table

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.

Constrained-Node Networks

A constrained network is composed of a significant portion of constrained nodes. Mostly, these constrained node networks are deployed in the edge network of an IoT system.

Constrained-node networks are often referred to as low-power and lossy networks (LLNs). Low-power in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes

A constrained network exhibits below characteristics:

Low bit-rate/throughput

High packet loss and high variability of packet loss

Highly asymmetric link characteristics

Lack of advanced network services like multi-cast

Data Rate and Throughput

Bandwidth is defined as the potential of the data that is to be transferred in a specific period of time. Maximum amount of data that can be transferred per second(bps), Mega bits per second(Mbps) or Giga bits per second(Gbps).

What is Data rate?

Data rate is defined as the amount of data transmitted during a specified time period over a network. The speed at which data is transferred from one device to another.

What is Throughput?

It is the amount of data is transmitted during a specified time period via network, interface or channel.

In IOT access technologies data rate range from 100 bps with protocols Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac.

Technologies like cellular and wifi which are not designed particularly for IOT but helps when IOT devices need high bandwidth requirements.

Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints

The IoT access technologies developed for constrained nodes are optimized for low power consumption, but they are also limited in terms of data rate, which depends on the selected frequency band, and throughput.

Today this sort of expertise is helpful for LPWA networks, which are designed with a certain number of messages per day or per endpoint rather than just having a pure bandwidth usage limit in place.

Latency and Determinism

Another important consideration is latency for iot application.

What is latency?

In a network, latency measures the time it takes **for some data to get to its destination across the network.** It is usually measured as a round trip delay - the time taken for information to get to its destination and back again.

On constrained networks, latency may range from a few milliseconds to seconds, and applications and protocol stacks must cope with these wide ranging values.

Overhead and payload

What is Payload?

When data is sent over the Internet, each unit transmitted includes both **header information and the actual data** being sent.

The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications. In addition, you should be aware of any requirements for IP. The minimum IPv6 MTU size is expected to be 1280 bytes. Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs.

For technologies that fall under the LLN definition but are able to transport IP, such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization is important.

Most LPWA technologies offer small payload sizes. These small payload sizes are defined to cope with the low data rate and time over the air or duty cycle requirements of IoT nodes and sensors

IoT Access Technologies

IOT Access Technologies Provides an in-depth look at some of the technologies that are considered when connecting smart objects. Currently, the number of technologies connecting smart objects is quite extensive, but you should expect consolidation, with certain protocols eventually winning out over others in the various IoT market segments.

What is a protocol?

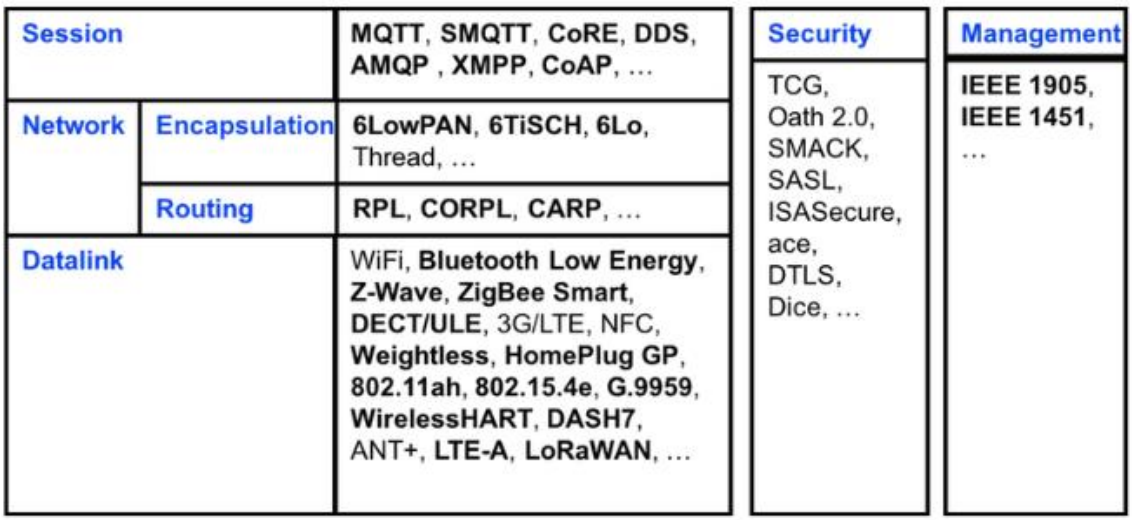
A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted ,what commands are used to send and receive data and how data transfers are confirmed.

IOT protocols is very important part in the IOT.IOT protocol enable it to exchange data in a structured and meaningful way. IOT involves sensors , devices, gateways, server and user application ,IOT protocols is a language used to communicate between devices.

Without IOT protocol only hardware connection does not make sense that is without exchange of data.

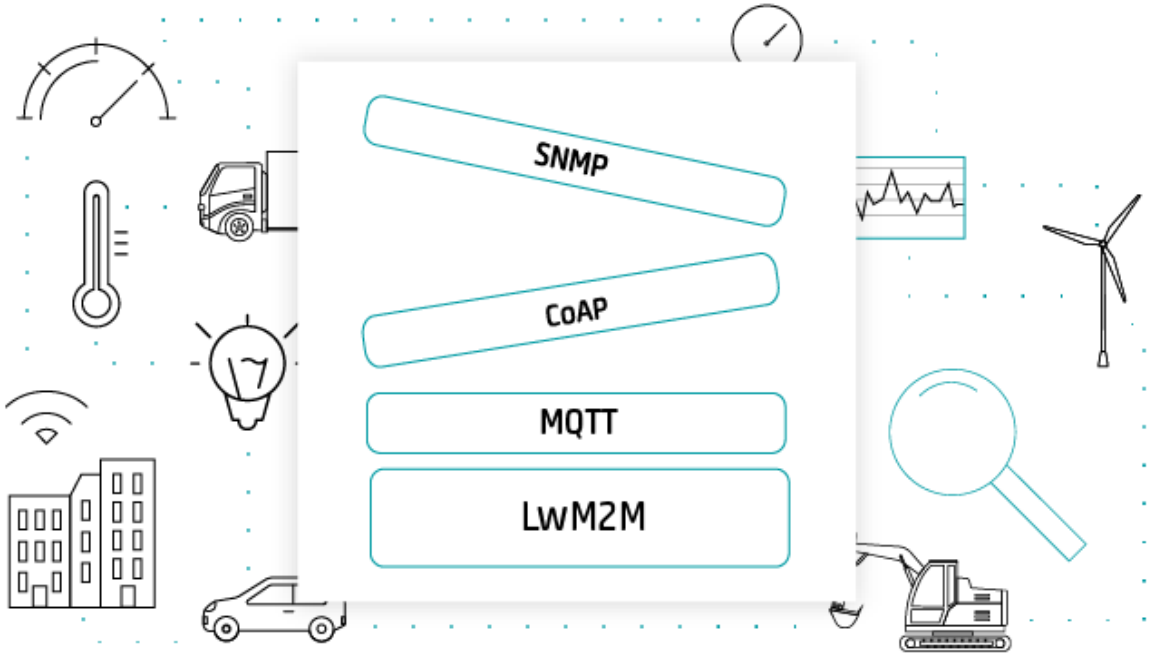
Often there is a need for multiple sensors to communicate and aggregate information before getting to the Internet. Specialized protocols have been designed for routing among sensors and are part of the routing layer. The session layer protocols enable messaging among various elements of the IoT communication subsystem.

Often there is a need for multiple sensors to communicate and aggregate information before getting to the Internet. Specialized protocols have been designed for routing among sensors and are part of the routing layer.



Protocols for IOT

Standardization and alliances: The standards bodies that maintain the protocols for a technology.



IEEE 802.15.4

IEEE 802.15.4 is the most commonly used IoT standard for MAC. It defines a frame format, headers including source and destination addresses, and how nodes can communicate with each other.

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:

- Home and building automation
- Automotive networks
- Industrial wireless sensor networks
- Interactive toys and remote controls

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).

This standard has evolved over the years and is a well-known solution for low complexity wireless devices with low data rates that need many months or even years of battery life.

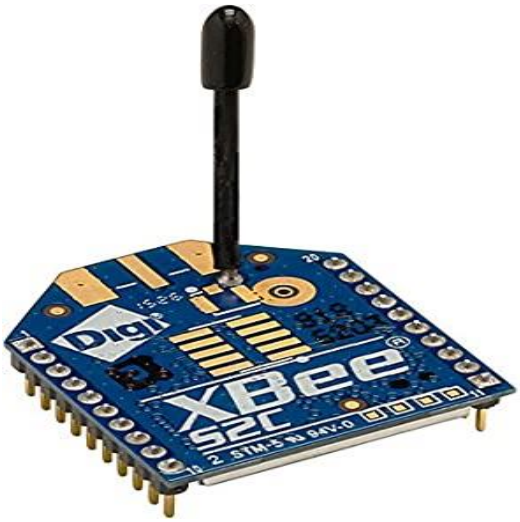
Some of the most well-known protocol stacks based on 802.15.4

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

Reference papers: https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf

Videos: https://www.youtube.com/watch?v=CfDEHd8nn2k

Zigbee



Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to **create personal area networks with small, low-power digital radios,** such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence**, Zigbee is a low-power, low data rate, and close proximity** (i.e., personal area) wireless ad hoc network.(wiki).

Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics.

Zigbee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones.

Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128 bit symmetric encryption keys.) Zigbee has a defined rate of 250 kbit/s, best suited for intermittent data transmissions from a sensor or input device.

ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs. Furthermore, products that are ZigBee compliant and certified by the ZigBee Alliance should interoperate even though different vendors may manufacture them.

The main areas where ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy. In the industrial and commercial automation space, ZigBee-based devices can handle various functions, from measuring temperature and humidity to tracking assets. For home automation, ZigBee can control lighting, thermostats, and security functions. ZigBee Smart Energy brings together a variety of interoperable products, such as smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water.

Frequency:2.4 Ghz

Distance:10m-100m

Battery life:7 years

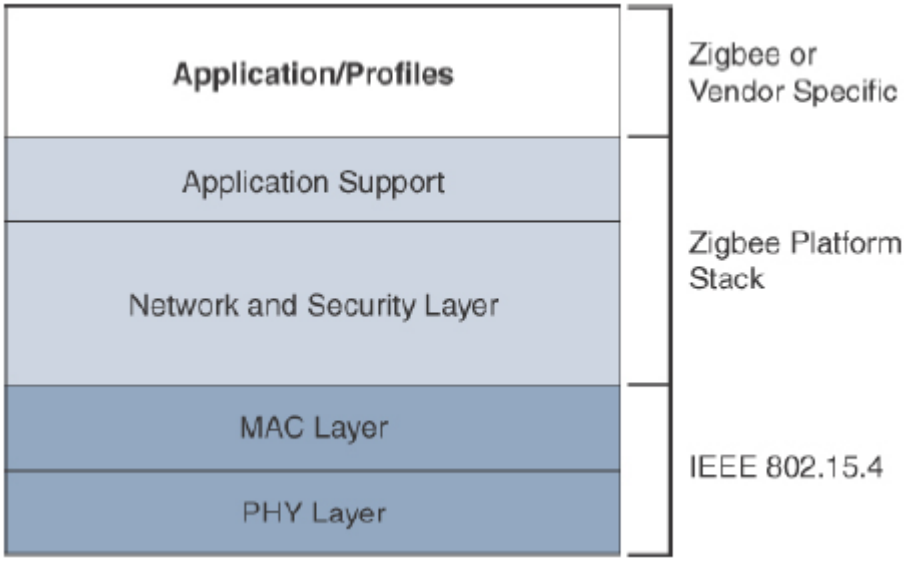
Working of Zigbee:

This technology uses digital radios to communicate from one device to another.

Zigbee consists of 3 kinds od devices:

- Zigbee Co-ordinator(ZC):this sets up the network ,and is aware of all the nodes within its network manages both the information about each node as well as the information that is being transmitted/received within the network Every ZigBee network must contain a network coordinator.
- Zigbee end device: An end device can be a smart thermostat, television, door, CCTV cameras, etc. There should be at least one coordinator in a network as it acts as a bridge and root for the entire network.
- ZigBee Router (ZR): In addition to running an application function, its is used to route the data from other devices and help it reach the destination.

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



High-level Zigbee Protocol stack

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
- 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

Network and security layer:

- The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications.
- ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.

Application layer:

- The application support layer in Figure interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher layer applications.
- ZigBee predefines many application profiles for certain industries, and vendors can optionally create their own custom ones at this layer.
  (more information refer page num 189)

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.

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 itsdata. Established by the US National Institute of Standards and Technology

in 2001,

IEEE 802.15.4g and 802.15.4e

The IEEE frequently makes amendments to the core 802.15.4 specification, before integrating them into the next revision of the core specification. When these amendments are made, a lowercase letter is appended.

Two such examples of this are **802.15.4e-2012 and 802.15.4g-2012**, both of which are especially relevant to the subject of IoT. Both of these amendments were integrated in IEEE 802.15.4-2015 but are often still referred to by their amendment names.

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. In addition to making general enhancements to the MAC layer, IEEE 802.15.4e also made improvements to better cope with certain application domains, such as factory and process automation and smart grid.

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. The focus of this specification is the

smart grid or, more specifically, smart utility network communication.

802.15.4g seeks to optimize large outdoor wireless mesh networks for field

area networks (FANs). New PHY definitions are introduced, as well as some

MAC modifications needed to support their implementation. This technology applies to IoT use cases such as the following:

- Distribution automation and industrial supervisory control and data
- acquisition (SCADA) environments for remote monitoring and control
- Public lighting
- Environmental wireless sensors in smart cities
- Electrical vehicle charging stations
- Smart parking meters
- Microgrids
- Renewable energy

Standardization and Alliances

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.

the additional capabilities and options provided by 802.15.4g-2012 and 802.15.4e-2012 led to additional difficulty in achieving the interoperability between devices and mixed vendors that users requested.

To guarantee interoperability, the **Wi-SUN Alliance was formed.**

This organization is not a standards body but is instead an industry alliance that defines communication profiles for smart utility and related networks.

These profiles are based on open standards, such as 802.15.4g-2012, 802.15.4e-2012, IPv6, 6LoWPAN, and UDP for the FAN profile.

The Wi-SUN Alliance performs the same function as the Wi-Fi Alliance and WiMAX Forum.

Each of these organizations has an associated standards body as well as a commercial name, as shown in Table. For more

information on Wi-SUN, visit www.wi-sun.org

Table-Industry Alliances for some common IEEE standards

Commercial Name/Trademark	Industry Organization	Standards Body
Wi-Fi	Wi-Fi Alliance	IEEE 802.11 Wireless LAN
WiMAX	WiMAX Forum	IEEE 802.16 Wireless MAN
Wi-SUN	Wi-SUN Alliance	IEEE 802.15.4g Wireless SUN

Physical Layer

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

This provides a better match for the greater packet sizes found in many upper layer protocols.

The SUN PHY, as described in IEEE 802.15.4g-2012, supports multiple data rates in bands ranging from 169 MHz to 2.4 GHz. These bands are covered in the unlicensed ISM frequency spectrum specified by various countries and Regions.

Within these bands, data must be modulated onto the frequency using at least one of the following PHY mechanisms to be IEEE 802.15.4g compliant:

Multi-Rate and Multi-Regional Frequency Shift Keying (MRFSK):

Offers good transmit power efficiency due to the constant envelope of the transmit signal

Multi-Rate and Multi-Regional Orthogonal Frequency Division

Multiplexing (MR-OFDM): Provides higher data rates but may be too complex for low-cost and low-power devices.

Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift

Keying (MR-O-QPSK): Shares the same characteristics of the IEEE 802.15.4-2006 O-QPSK PHY, making multi-mode systems more costeffective

and easier to design.

MAC Layer: While the IEEE 802.15.4e-2012 amendment is not applicable to the PHY layer, it is pertinent to the MAC layer. This amendment enhances the MAC layer through various functions, which may be selectively enabled based on various implementations of the standard.

The following are some of the main enhancements to the MAC layer proposed by IEEE 802.15.4e-2012:

Time-Slotted Channel Hopping (TSCH): TSCH is an IEEE 802.15.4e-2012 MAC operation mode that works to guarantee media access and channel diversity. Channel hopping, also known as frequency hopping, utilizes different channels for transmission at different times.

- TSCH divides time into fixed time periods, or "time slots," which offer guaranteed bandwidth and predictable latency.
- In a time slot, one packet and its acknowledgement can be transmitted, increasing network capacity because multiple nodes can communicate in the same time slot, using different channels.
- A number of time slots are defined as a "slot frame," which is regularly repeated to provide"guaranteed access."
- The transmitter and receiver agree on the channels and the timing for switching between channels through the combination of a global time slot counter and a global channel hopping sequence list, as computed on each node to determine the channel of each time slot.

Information elements:

Information elements (IEs) allow for the exchange of information at the MAC layer in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).

Enhanced beacons (EBs):

EBs extend the flexibility of IEEE 802.15.4 beacons to allow the construction of application-specific beacon content.

Enhanced beacon requests (EBRs):

Like enhanced beacons, an enhanced beacon request (EBRs) also leverages IEs. The IEs in EBRs allow the sender to selectively specify the request of information.

Enhanced Acknowledgement: The Enhanced Acknowledgement frame allows for the integration of a frame counter for the frame being acknowledged. This feature helps protect against certain attacks that occur when Acknowledgement frames are spoofed.

Topology:

Deployments of IEEE 802.15.4g-2012 are mostly based on a mesh topology. This is because a mesh topology is typically the best choice for use cases in the industrial and smart cities areas where 802.15.4g-2012 is applied.

A mesh topology allows deployments to be done in urban or rural areas, expanding the distance between nodes that can relay the traffic of other

nodes.

Security

Both IEEE 802.15.4g and 802.15.4e inherit their security attributes from the IEEE 802.15.4-2006 specification. Therefore, encryption is provided by AES, with a 128-bit key.

IEEE 1901.2a

The IEEE Std 1901-2010 is a standard for high speed (up to 500 Mbit/s at the physical layer) **communication devices via electric power lines, often called broadband over power lines (BPL).**

The standard uses transmission frequencies below **100 MHz.** This standard is usable by all classes of BPL devices, including BPL devices used for the connection (<1500m to the premises) to Internet access services as well as BPL devices used within buildings for local area networks, smart energy applications, transportation platforms (vehicle), and other data distribution applications (<100m between devices)

While most of the constrained network technologies relate to wireless, IEEE 1901.2a-2013 is a wired technology that is an update to the original IEEE 1901.2 specification.

This is a standard for Narrowband Power Line Communication (NB-PLC). NB-PLC leverages a narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power. NB-PLC is often found in use cases such as the following:

Smart metering

Distribution automation

Public lighting

Electric vehicle charging stations

Microgrids

Renewable energy

All these use cases require a direct connection to the power grid. So it makes sense to transport IoT data across power grid connections that are already in place.

Standardization and Alliances

The first generations of NB-PLC implementations have generated a lot of interest from utilities in Europe but have often suffered from poor reliability, low throughput (in the range of a few hundred bits per second to a maximum of 2 kbps), lack of manageability, and poor interoperability.

This has led several organizations (including standards bodies and alliance consortiums) to develop their own specifications for new generations of NB-PLC technologies.

Most recent NB-PLC standards are based on orthogonal frequency-division multiplexing (OFDM). However, different standards from various vendors competing with one another have created a fragmented market.

OFDM encodes digital data on multiple carrier frequencies. This provides several parallel streams that suffer less from high frequency attenuation in copper wire and narrowband interference

Physical layer

NB-PLC is defined for frequency bands from 3 to 500 kHz. Much as with wireless sub-GHz frequency bands, regional regulations and definitions apply to NB-PLC.

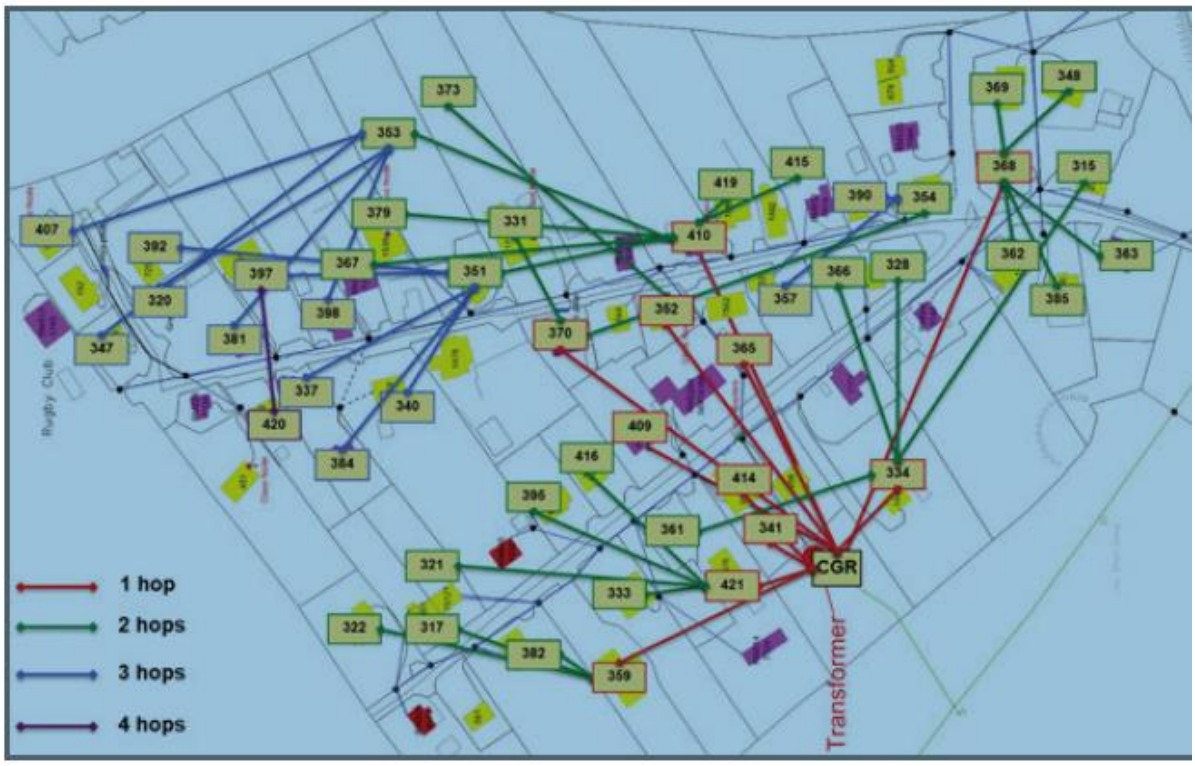
MAC Layer

The MAC frame format of IEEE 1901.2a is based on the IEEE 802.15.4 MAC frame but integrates the latest IEEE 802.15.4e-2012 amendment, which enables key features to be supported.

One of the key components brought from 802.15.4e to IEEE 1901.2a is information elements.

Topology

Use cases and deployment topologies for IEEE 1901.2a are tied to the physical power lines. As with wireless technologies, signal propagation is limited by factors such as noise, interference, distortion, and attenuation.These factors become more prevalent with distance, so most NB-PLC deployments use some sort of **mesh topology.**



IPV6 Mesh in NB-PLC

Security

IEEE 1901.2a security offers Encryption and authentication are performed using AES. In addition, IEEE 1901.2a aligns with 802.15.4g in its ability to support the IEEE 802.15.9 Key Management Protocol.

However, some differences exist. These differences are mostly tied to the PHY layer fragmentation capabilities of IEEE 1901.2a and include the following:

- The Security Enabled bit in the Frame Control field should be set in all MAC frames carrying segments of an encrypted frame.
- If data encryption is required, it should be done before packet segmentation. During packet encryption, the Segment Control field should not be included in the input to the encryption algorithm.
- On the receiver side, the data decryption is done after packet reassembly.
- When security is enabled, the MAC payload is composed of the ciphered payload and the message integrity code (MIC) authentication tag for non-segmented payloads. If the payload is segmented, the MIC is part of the last packet (segment) only. The MIC authentication is computed using only information from the MHR of the frame carrying the first segment.

IEEE 802.11ah

- Wi-Fi is certainly the most successfully deployed wireless technology.
- This standard is a key IoT wireless access technology, either for connecting endpoints such as fog computing nodes, high-data-rate sensors, and audio or video analytics devices or for deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments.

  Three main use cases are identified for IEEE 802.11ah:

Sensors and meters covering a smart grid: Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors

Backhaul aggregation of industrial sensors and meter data: Potentially connecting IEEE 802.15.4g subnetworks

Extended range Wi-Fi: For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough.

Standardization and Alliances

In July 2010, the IEEE 802.11 working group decided to work on an "industrial Wi-Fi" and created the IEEE 802.11ah group. The 802.11ah specification would operate in unlicensed sub-GHz frequency bands, similar to IEEE 802.15.4 and other LPWA technologies.

The industry organization that promotes Wi-Fi certifications and interoperability for 2.4 GHz and 5 GHz products is the Wi-Fi Alliance. The Wi-Fi Alliance is a similar body to the Wi-SUN Alliance. For more information on the Wi-Fi Alliance, see its webpage, at www.wi-fi.org.

Physical Layer

IEEE 802.11ah essentially provides an additional 802.11 physical layer operating in unlicensed sub-GHz bands.

For example, various countries and regions use the following bands for IEEE 802.11ah: 868–868.6 MHz for EMEAR, 902–928 MHz and associated subsets for North America and Asia- Pacific regions, and 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779– 787 MHz for China.

What is OFDM?

Orthogonal Frequency Division Multiplexing (OFDM) is a technique for transmitting large amounts of digital data over a radio wave The technology works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver.

Based on OFDM modulation, IEEE 802.11ah uses channels of 2, 4, 8, or 16 MHz (and also 1 MHz for low-bandwidth transmission). This is one-tenth of the IEEE 802.11ac channels, resulting in one-tenth of the corresponding data rates of IEEE 802.11ac.

The IEEE 802.11ac standard is a high-speed wireless LAN protocol at the 5 GHz band that is capable of speeds up to 1 Gbps.

MAC Layer

The IEEE 802.11ah MAC layer is optimized to support the new sub-GHz Wi-Fi PHY while providing low power consumption and the ability to support a larger number of endpoints.

Number of devices: Has been scaled up to 8192 per access point.

AC header: Has been shortened to allow more efficient communication.

Null data packet (NDP) support: Is extended to cover several control and management frames. Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided. This change makes the control frame exchanges efficient and less power consuming for the receiving stations.

Grouping and sectorization: Enables an AP to use sector antennas and also group stations (distributing a group ID). In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window.

Restricted access window (RAW): Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access to the wireless network. By providing more efficient access to the medium, additional power savings for battery powered devices can be achieved, and collisions are reduced.

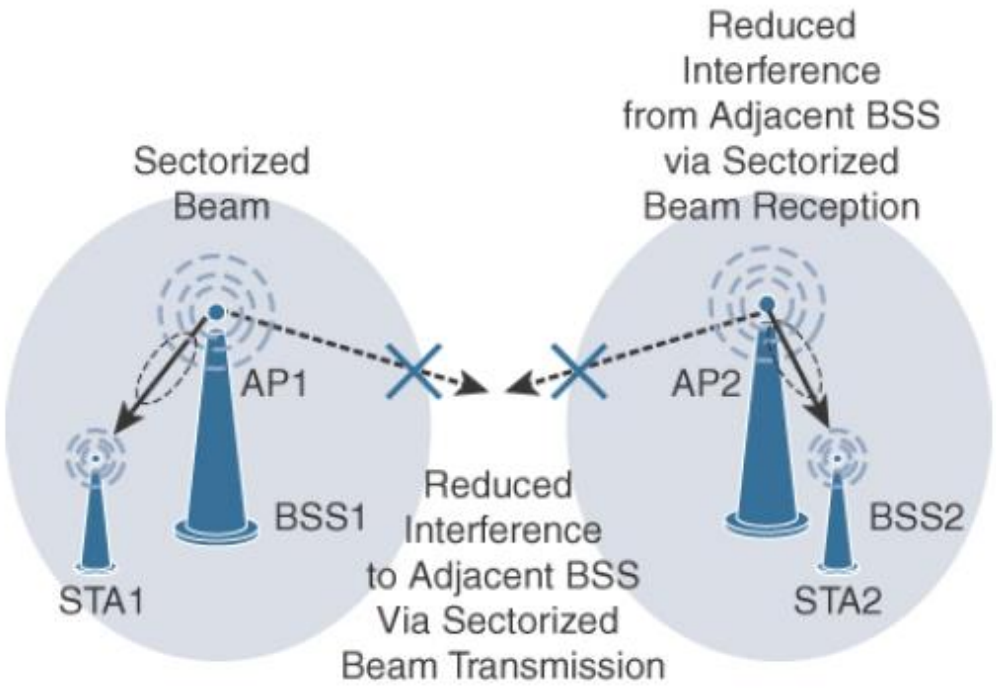
Target wake time (TWT): Reduces energy consumption by permitting an access point to define times when a device can access the network. This allows devices to enter a low-power state until their TWT time arrives. It also reduces the probability of collisions in large cells with many clients.

Speed frame exchange: Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP). This reduces contention on the medium, minimizes the number of frame exchanges to improve channel efficiency, and extends battery life by keeping awake times short.

Topology

- While IEEE 802.11ah is deployed as a star topology, it includes a simple hops relay operation to extend its range.
- This relay option is not capped, but the IEEE 802.11ah task group worked on the assumption of two hops.
- It allows one 802.11ah device to act as an intermediary and relay data to another. In some ways, this is similar to a mesh, and it is important to note that the clients and not the access point handle the relay function.
- This relay operation can be combined with a higher transmission rate or modulation and coding scheme (MCS). This means that a higher transmit rate is used by relay devices talking directly to the access point.

- Sectorization is a technique that involves partitioning the coverage area into several sectors to get reduced contention within a certain sector.
- This technique is useful for limiting collisions in cells that have many clients.
- This technique is also often necessary when the coverage area of 802.11ah access points is large, and interference from neighboring access points is problematic. Sectorization uses an antenna array and beam-forming techniques to partition the cell-coverage area.



Security

No additional security has been identified for IEEE 802.11ah compared to other IEEE 802.11 specifications. These protocols include IEEE 802.15.4, IEEE 802.15.4e, and IEEE 1901.2a, and the security information for them is also applicable to IEEE 802.11ah.

LoRaWAN

In recent years, a new set of wireless technologies known as Low-Power Wide-Area (LPWA) has received a lot of attention from the industry and press

- LoRaWAN is a protocol built on top of the LoRa technology was developed by the LoRa Association.
- LoRa is well adapted for long range and battery-powered end points.

To solve some portion of problems in IOT LPWAN is extensively used.

- LPWANs are explicitly focusing on circumstances where broadened inclusion is generally required, with minimal effort of arrangement, including gadgets that are delay tolerant, needn't bother with high data rates and desire low control utilization to organize. Specifically, seeing of a network or state in a faultless circumstance is where LPWANs fit.

LoRa Network Elements

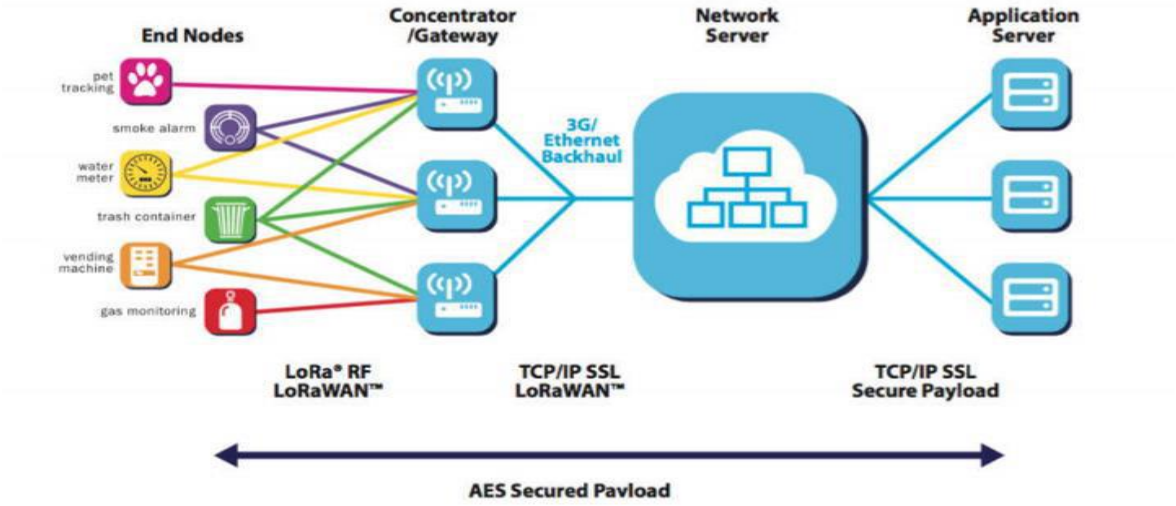
Star topology is used by LoRaWAN as it expands battery lifetime for appications that require long-range connectivity.

Figure explains the LoRa network which comprises of several components.The figure depicts the connection between end nodes and gateway,gateway and network server,network server and application server.

• **LoRa End Points/Nodes:** LoRa nodes are the applications or sensors where detection and control activity is carried out. These hubs are consistently placed at a remote place. Examples, tracking devices, sensors etc.

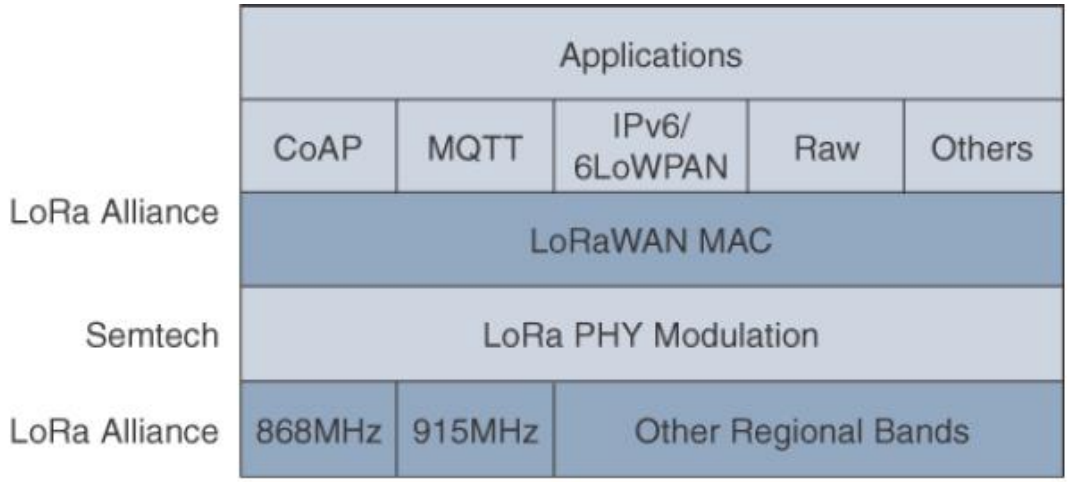
• **LoRa Gateways:** Not at all like cell correspondence where mobile phones are connected with the serving base stations to a particular portal, the LoRaWAN hubs are connected. Preferably, any data sent by the hub is first transmitted across all the portals and every door which gets a sign exchanges it to a cloud based framework server. Usually the network servers and gateways are connected via some terrestrial link (Wi-Fi, cellular, satellite, or ethernet).

•**Network Servers:** The network servers has all the intellect. The duplicate packets are filtered from various gateways, the security check is also done and the ACK's are sent to the gateways. At last if a packet was intended for a particular application server, the packet to the application server is sent by the network server. Making use of this type of network where all gateways can transmit same type of packets across the network server, the necessity of handover or hand-off is eliminated. It is helpful for applications which involve moving assets from one location to another namely asset tracking.



Standardization and Alliances

Initially, LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named Cycleo. Later, Cycleo was acquired by Semtech. Optimized for long-range, two-way communications and low power consumption, the technology evolved from Layer 1 to a broader scope through the creation of the LoRa Alliance.



Physical Layer

Semtech LoRa modulation is based on chirp spread spectrum modulation, which trades a lower data rate for receiver sensitivity to significantly increase the communication distance.

In addition, it allows demodulation below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.

MAC Layer

As mentioned previously, the MAC layer is defined in the LoRaWAN specification. This layer takes advantage of the LoRa physical layer and classifies LoRaWAN endpoints to optimize their battery life and ensure downstream communications to the LoRaWAN endpoints.

The LoRaWAN specification documents three classes of LoRaWAN devices:

Class A: This class is the default implementation. Optimized for battery-powered nodes, it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting. Two receive windows are available after each transmission.

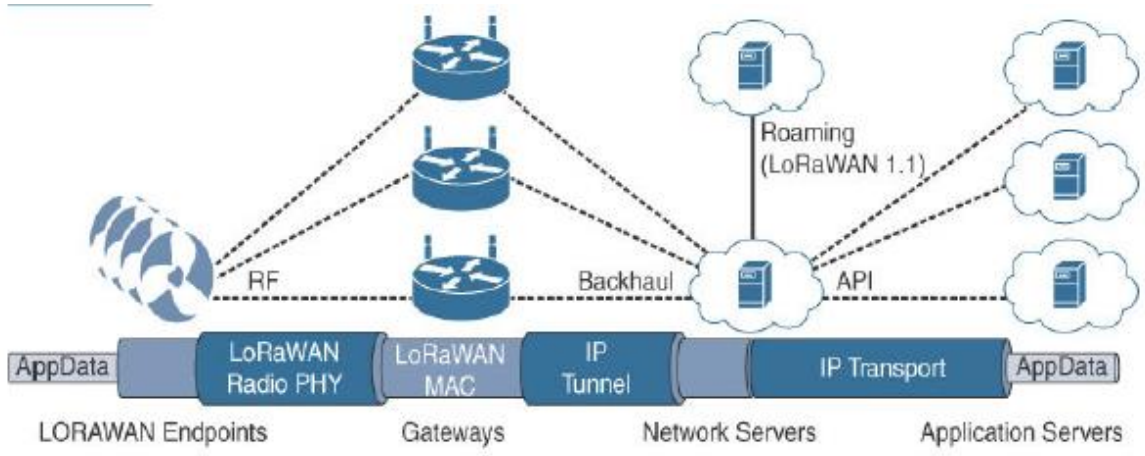
Class B: This class was designated "experimental" in LoRaWAN 1.0.1 until it can be better defined. A Class B node or endpoint should get additional receive

windows compared to Class A, but gateways must be synchronized through a beaconing process.

Class C: This class is particularly adapted for powered nodes. This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.

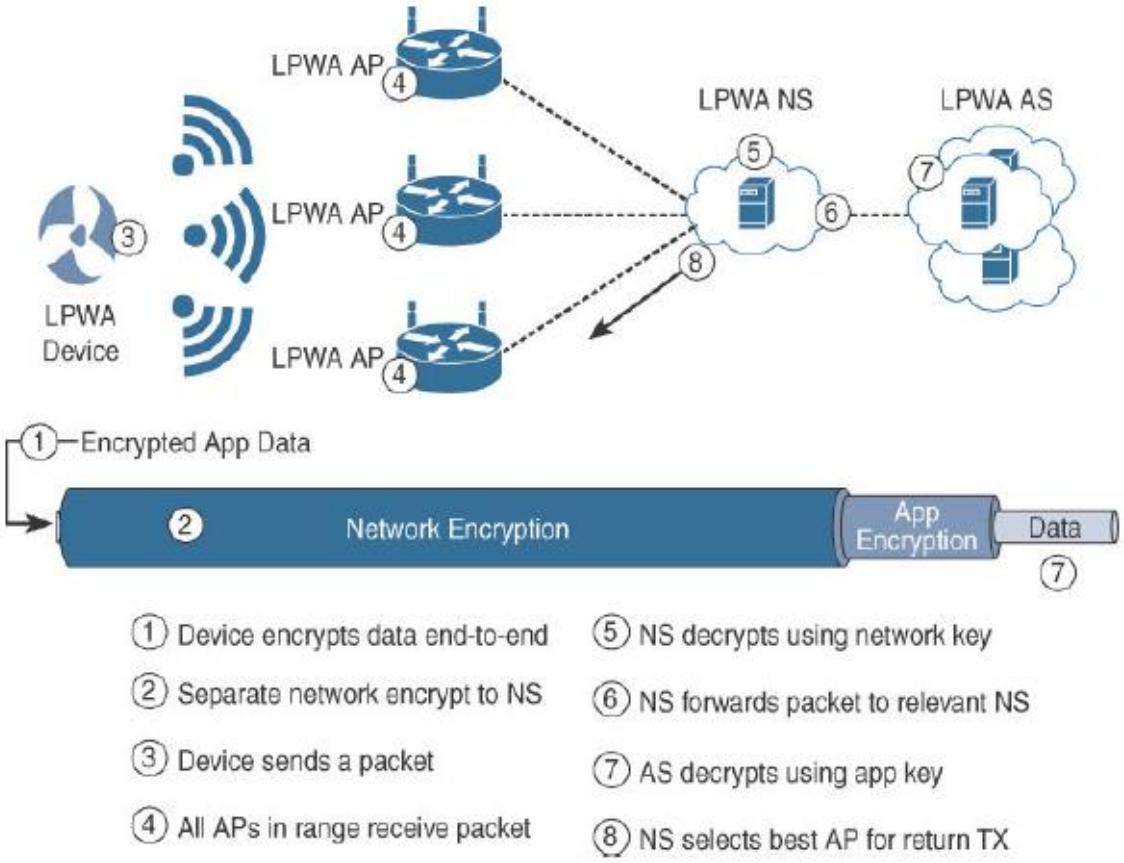
Topology

LoRaWAN topology is often described as a "star of stars" topology. As shown in Figure the infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server. Gateways connect to the backend network using standard IP connections, and endpoints communicate directly with one or more gateways.



Security

Security in a LoRaWAN deployment applies to different components of the architecture, as detailed in Figure LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.



- The first layer, called "network security" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server. Also, it protects LoRaWAN packets by performing encryption based on AES.
- Each endpoint implements a network session key (NwkSKey), used by both itself and the LoRaWAN network server. The NwkSKey ensures data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-only data message payloads.
- The second layer is an application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server.
- Furthermore, it computes and checks the application-level MIC, if included. This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access.

- Endpoints receive their AES-128 application key (AppKey) from the application owner. This key is most likely derived from an application specific root key exclusively known to and under the control of the application provider.