MODULE 2 INTERNET OF THINGS

Reference Textbook: 1. **Fundamentals: Networking Technologies, Protocols, and Use Cases for the "Internet of Things" by** David Hanes and Jerome Henry, 1st Edition, 2008, Pearson Education.

- Sensors, Actuators and Smart Objects,
- Physical phenomenon of sensors,
- Micro-Electro-Mechanical Systems (MEMS)
- IP as the IoT Network Layer
- Connecting Smart Objects,
- Communications Criteria,
- IoT AccessTechnologies-LoRaWAN

Module – 2

Smart Objects: The “Smart Objects: The “Things” in IoT ings” in IoT

- The capabilities, properties, and functionality of sensors and actuators are described in this section.
- It explains in detail how the economic and technological conditions are finally favorable for the Internet of Things is going to take off.
- A sensor detects something. A sensor, in further detail, measures a physical amount and turns the reading into a digital representation.
- That digital representation is often transmitted to another device for transformation into valuable data that intelligent devices or humans can consume.
- Sensors give people superhuman sensory capacities.
- Sensors may be simply integrated into any physical object that is connected to the Internet.

Different Categories of Sensors

1. Active or passive
2. Invasive or non-invasive
3. Contact or no-contact
4. Absolute or relative
5. Area of application
6. How sensors measure
7. What sensors measure:

1. Active or Passive

   Sensors are classified as active or passive, depending on whether they produce energy and require an external power supply (active) or merely receive energy and do not require an external power supply (passive) (passive)

2. Invasive or non-invasive

   Sensors are classified according to whether they are part of a system or not.

   It is either intrusive to the environment it is measuring or external to it (non-invasive).

3. Contact or No-contact:

Sensors are classified according to whether or not they require physical interaction.

(Contact) or (non-contact) with the thing they're measuring (no-contact).

4. Relative or Absolute

Sensors are classified according to whether they measure on an absolute scale (absolute) or a difference from a fixed or changeable reference value (relative).

5. Application field:

Sensors are classified according to the industry or vertical in which they are used being put to use

6. What sensors are used for:

The physical mechanism employed to measure sensory input (thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photoelastic, and so on) can be used to categorize sensors.

7. Sensors that measure:

Sensors are classified according to their uses or the physical characteristics they measure.

Based on Physical phenomenon of sensors

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope

Based on Physical phenomenon of sensors Continued..

Sensor Types	Description	Examples
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Based on Physical phenomenon of sensors Continued..

Sensor Types	Description	Examples
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector

Based on Physical phenomenon of sensors Continued..

Sensor Types	Description	Examples
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge

Based on Physical phenomenon of sensors Continued..

Sensor Types	Description	Examples
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

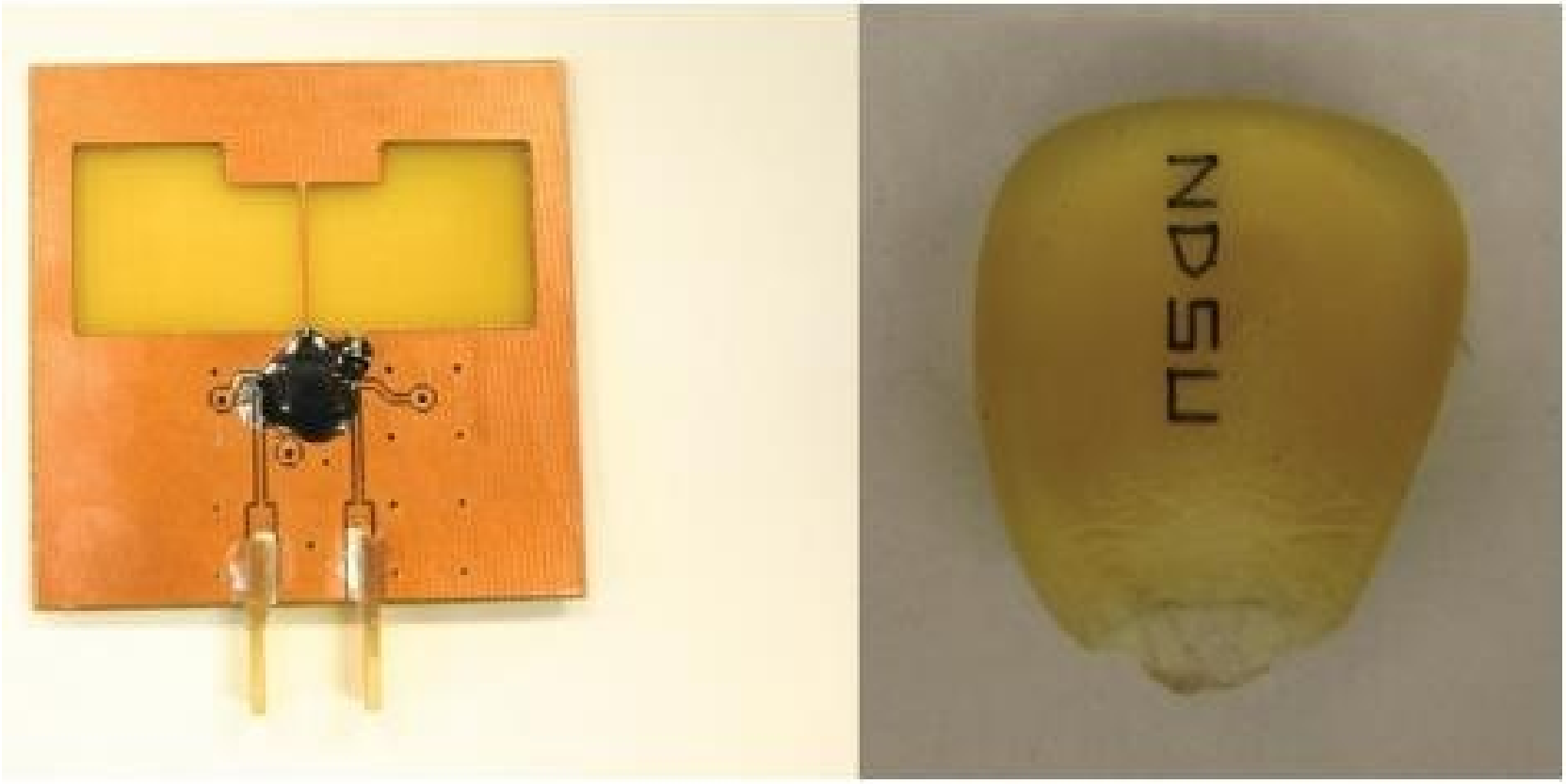
Sensors:

- Sensors exist in a variety of shapes and sizes, and they can detect a wide range of physical variables.
- Precision agriculture (also known as smart farming) is a fascinating use case that highlights the capabilities of sensors and IoT.
- Precision agriculture combines a range of technological developments to increase the efficiency, sustainability, and profitability of traditional farming operations.
- This involves using GPS and satellite aerial images to determine field viability; robots for high-precision planting, harvesting, irrigation, and other tasks; and real-time analytics and artificial intelligence to anticipate optimal crop output, weather impacts, and soil quality, among other things.

Sensors Continued..

- Sensor measurements of a range of soil parameters are the most significant benefits of precision agriculture.
- Real-time measurements of soil quality, pH, salinity, toxicity, moisture levels for irrigation planning, and nutrient levels for fertilization planning are among them.
- All of this precise sensor data may be examined to provide highly valuable and actionable knowledge into how to increase agricultural output and productivity.
- Figure depicts biodegradable, passive micro sensors used to monitor soil, crop, and environmental conditions.
- These sensors, which were created at North Dakota State University (NDSU), can be planted directly in the soil and permitted to biodegrade without causing any harm to the environment.

Biodegradable Sensors- NDSU



Biodegradable Sensors Developed by NDSU for Smart Farming

Sensors Continued..

- The Internet of Things (IoT) and, by extension, networked sensors have been often mentioned as one of a handful of emerging breakthrough technologies that will transform the global economy and determine the future.
- The incredible number of sensors is attributable in great part to their reduced size, form factor, and lower cost.
- These factors make it economically and technically feasible to increase the density of sensors in all kinds of devices.
- Mobile phones are the most major accelerator for sensor deployments.
- Every year, more than a billion smart phones are sold, with each one including well over a dozen sensors.

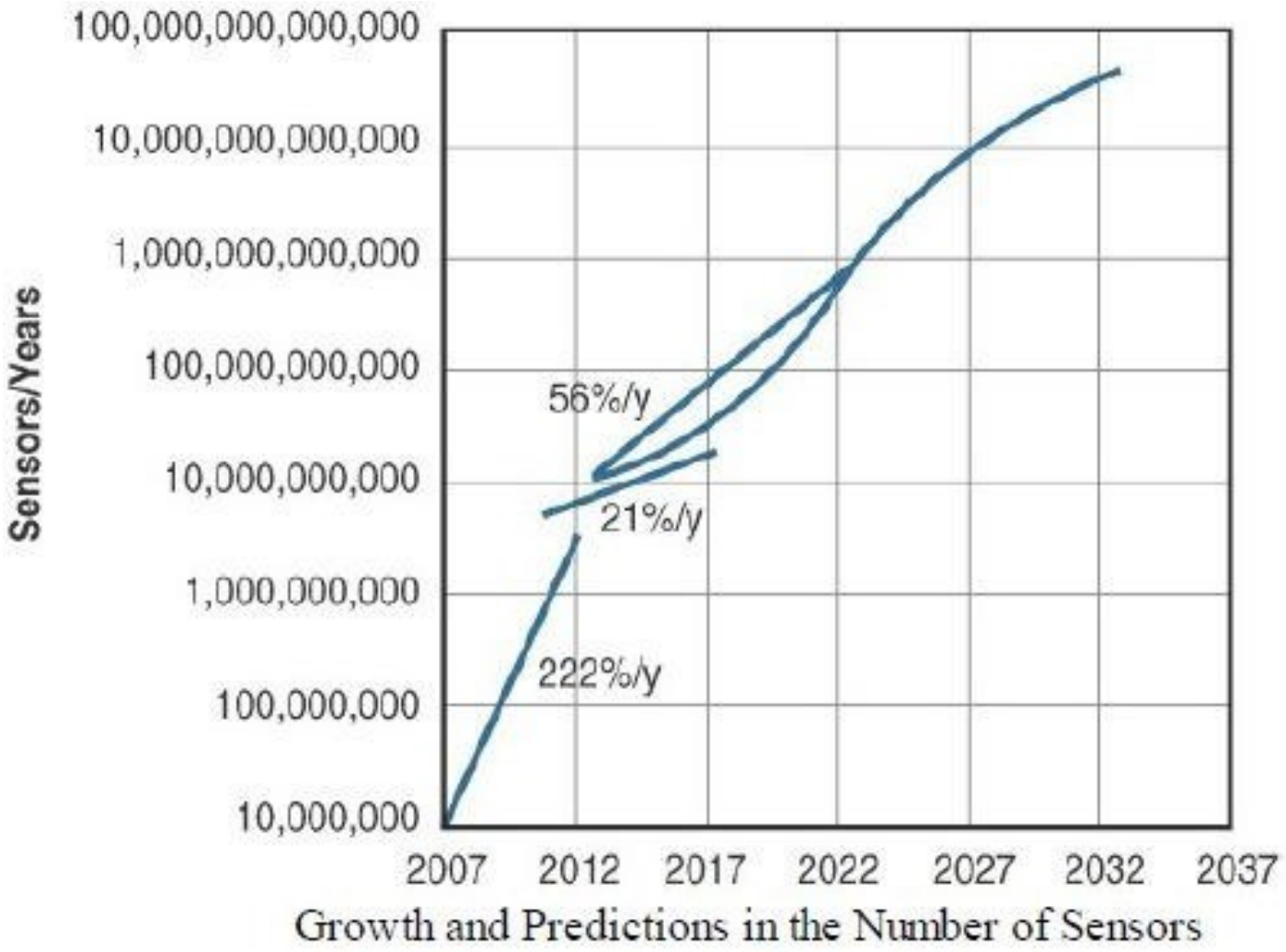
Sensors in Smart Phone

Sensors in a Smart Phone

Sensors Continued..

- There are smart homes with hundreds of sensors, intelligent vehicles with 100 or more sensors, connected cities with thousands upon thousands of connected sensors, and so on.
- The graph depicts the dramatic year-over-year increase in sensor numbers over the last few years and some bold projections for sensor numbers in the next years.
- According to the sensor industry, this sum will surpass a trillion dollars in the next several years.
- Many major companies in the sensor business have formed industry consortia, such as the TSensors Summits (www.tsensorssummit.org), to develop a strategy and roadmap for a trillion-dollar sensor economy.
- The trillion-sensor economy will function in this way.

Sensors- Growth Prediction

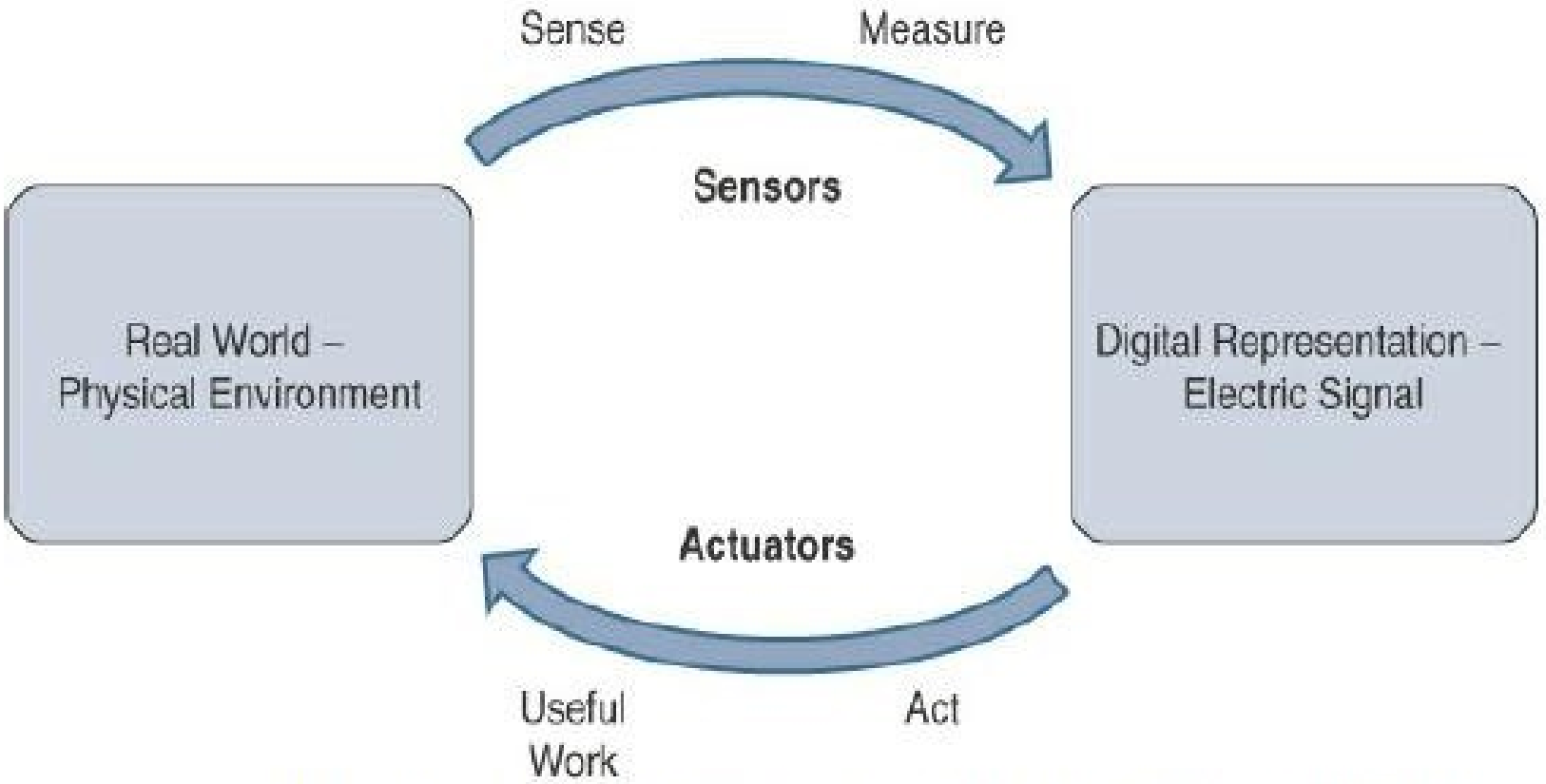


Growth and Predictions in the Number of Sensors

Actuators:

- Sensors and actuators are natural partners.
- The symmetry and complementary nature of these two types of devices can be seen in the diagram.
- Sensors are built to detect and quantify almost every observable variable in the physical world.
- They convert their measurements (which are usually analogue) into electric signals or digital representations that an intelligent entity can understand (a device or a human).
- Actuators receive a control signal (often an electric signal or a digital command) that causes a physical effect, such as motion, force, and so on.

Sensors and Actuators

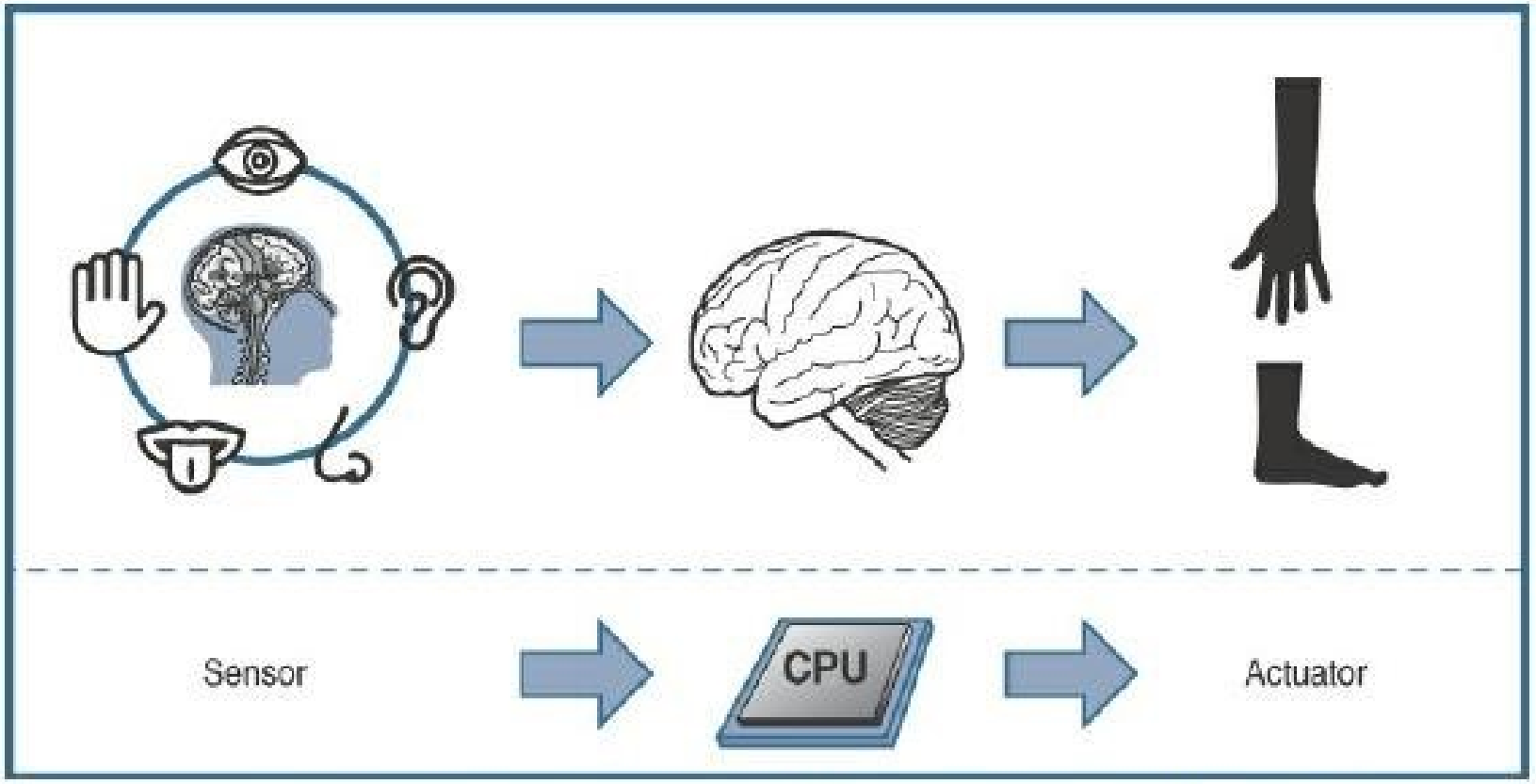


How Sensors and Actuators Interact with the Physical World

Sensors and Actuators Continued..

- IoT sensors are devices that detect and measure the physical world and (usually) transmit their findings as electrical signals to a microprocessor or microcontroller for further processing.
- In turn, a processor can send an electric signal to an actuator, which converts the signal into some form of movement (linear, rotational, and so on) or useful labour that affects or changes the physical world.
- The interplay of sensors, actuators, and processors, as well as biological systems' equivalent functioning, provides the foundation for a variety of technical domains, including robotics and biometrics.

Comparison of Sensors and Actuators



Comparison of Sensor and Actuator Functionality with Humans

Classification of Actuators

1. **Type of motion**
2. **Power**
3. **Binary or continuous**
4. **Area of application**
5. **Type of energy**

Classification of Actuators Continued..

- Actuators are categorized according to the sort of motion they produce (linear, rotational, one/two/three-axes, for example).
- Actuators are categorized according to their power output (for example, high power, low power, micro power)
- Actuators are classed as binary or continuous based on the number of stable-state outputs.
- Actuators are classed according to the industry or vertical in which they are employed.
- Actuators can be categorized based on the sort of energy they use.

Classification of Actuators Based 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

Actuator Classification by Energy Type

Actuators Continued..

- The information is provided by sensors, and the action is provided by actuators.
- The most intriguing IoT use cases are those in which sensors and actuators collaborate intelligently.
- Smart sensors that measure a range of soil, temperature, and plant variables, for example, can be linked to electrically or pneumatically controlled valve actuators that control water, pesticides, fertilizers, herbicides, and other chemicals.
- To deliver a highly optimized and bespoke environment-specific solution, intelligently triggering a high-precision actuator based on well-defined sensor readings of temperature, pH, soil/air humidity, nutrient levels, and so on is genuinely smart.

Micro-Electro-Mechanical Systems (MEMS):

- How sensors and actuators are packaged and deployed is one of the most fascinating breakthroughs in sensor and actuator technology.
- Micro-electro-mechanical systems (MEMS), also known as micro-machines, are devices that can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very tiny size (millimetre or less).
- A microfabrication approach comparable to that used in microelectronic integrated circuits is one of the essential components of this technology.This method enables for low-cost mass production.

Micro-Electro-Mechanical Systems (MEMS) Continued..

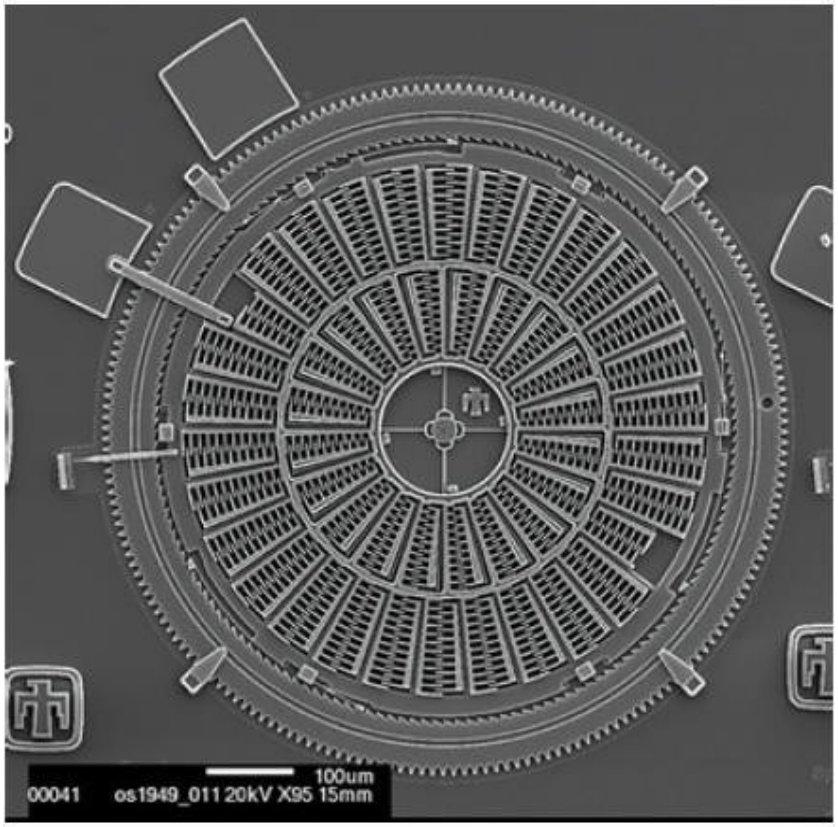
- MEMS are an appealing alternative for a wide range of IoT applications due to its small size, low cost, and ability to mass produce.
- MEMS devices are already widely employed in a number of applications and can be found in many commonplace household items.
- Micro pump MEMS are used in inkjet printers, for example.
- MEMS technology is also used in smart phones for accelerometers and gyroscopes.
- With airbag accelerometers, automobiles were among the first to commercially introduce MEMS to the mass market.

Micro-Electro-Mechanical Systems (MEMS) Continued..

Sandia National Laboratory created the torsional ratcheting actuator (TRA) MEMS as a low-voltage alternative to a micro-engine.

This MEMS is only a few hundred micrometres across, therefore the amount of detail apparent in the figure requires a scanning electron microscope.

Micro-scale sensors and actuators can be easily embedded in common objects, which is a distinguishing feature of the Internet of Things.



Smart Objects

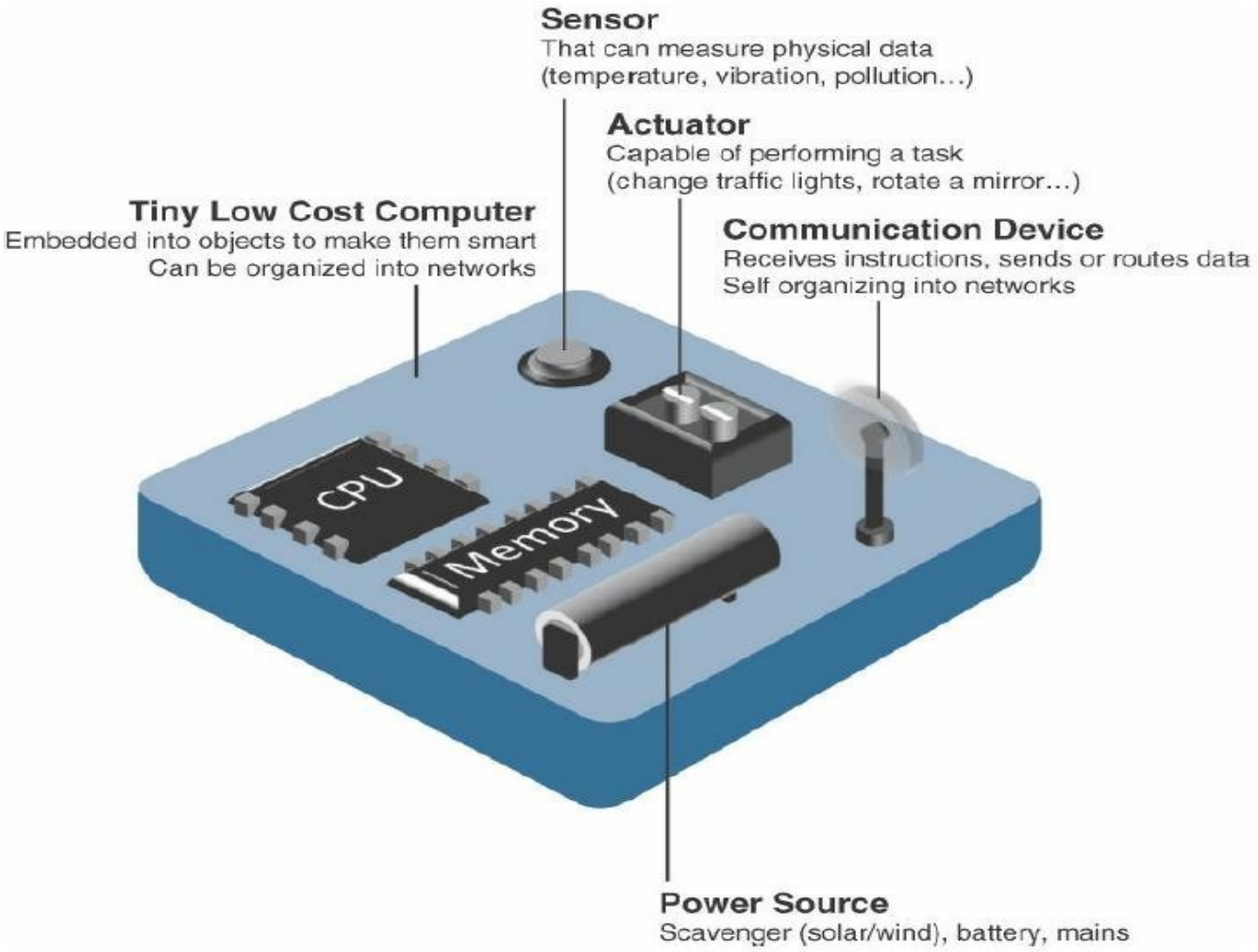
- The IoT's building blocks are smart objects.
- They turn ordinary objects into a network of sentient objects that can learn from and interact meaningfully with their surroundings.
- We have something significantly more powerful if soil sensors are connected as part of an intelligent network that can intelligently coordinate with actuators to trigger watering systems as needed depending on sensor readings.
- The coordinated sensor/actuator set communicates with an intelligent backend to determine crop yield potential and is intelligently integrated with additional sensor/actuator sets to further coordinate fertilization, pest management, and so on.

Smart Objects Continued..

- The phrases smart object, smart sensor, smart device, IoT device, intelligent device, thing, smart thing, intelligent node, intelligent thing, ubiquitous item, and intelligent product are frequently used interchangeably.
- Definition:A smart object is a device that possesses at least four of the following characteristics:

1. Processing unit
2. Communication device
3. Sensor(s) and/or actuator(s)
4. Power source

Characteristics of a Smart Object



Trends in Smart Objects:

IoT Impact on generalization:

1. Size is decreasing
2. Power consumption is decreasing
3. Processing power is increasing
4. Communication capabilities are improving
5. Communication is being increasingly standardized

Sensor Networks:

- A sensor/actuator network (SANET) is a collection of sensors that sense and measure their surroundings, as well as actuators that act on them.
- A SANET's sensors and/or actuators are capable of productive communication and collaboration.
- Because the sensors and actuators in SANETs are diverse, heterogeneous, and resource-constrained, effective and well-coordinated communication and cooperation is a significant problem.

Sensor Networks Continued..

- SANETs are capable of highly coordinated sensing and actuation.
- The coordination between dispersed sensors and actuators is demonstrated in smart houses, which are a sort of SANET.
- Temperature sensors, for example, can be strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators in smart houses.
- When a sensor detects a certain temperature, an actuator can be triggered to heat or cool the home as needed.

Sensor Networks - Advantages

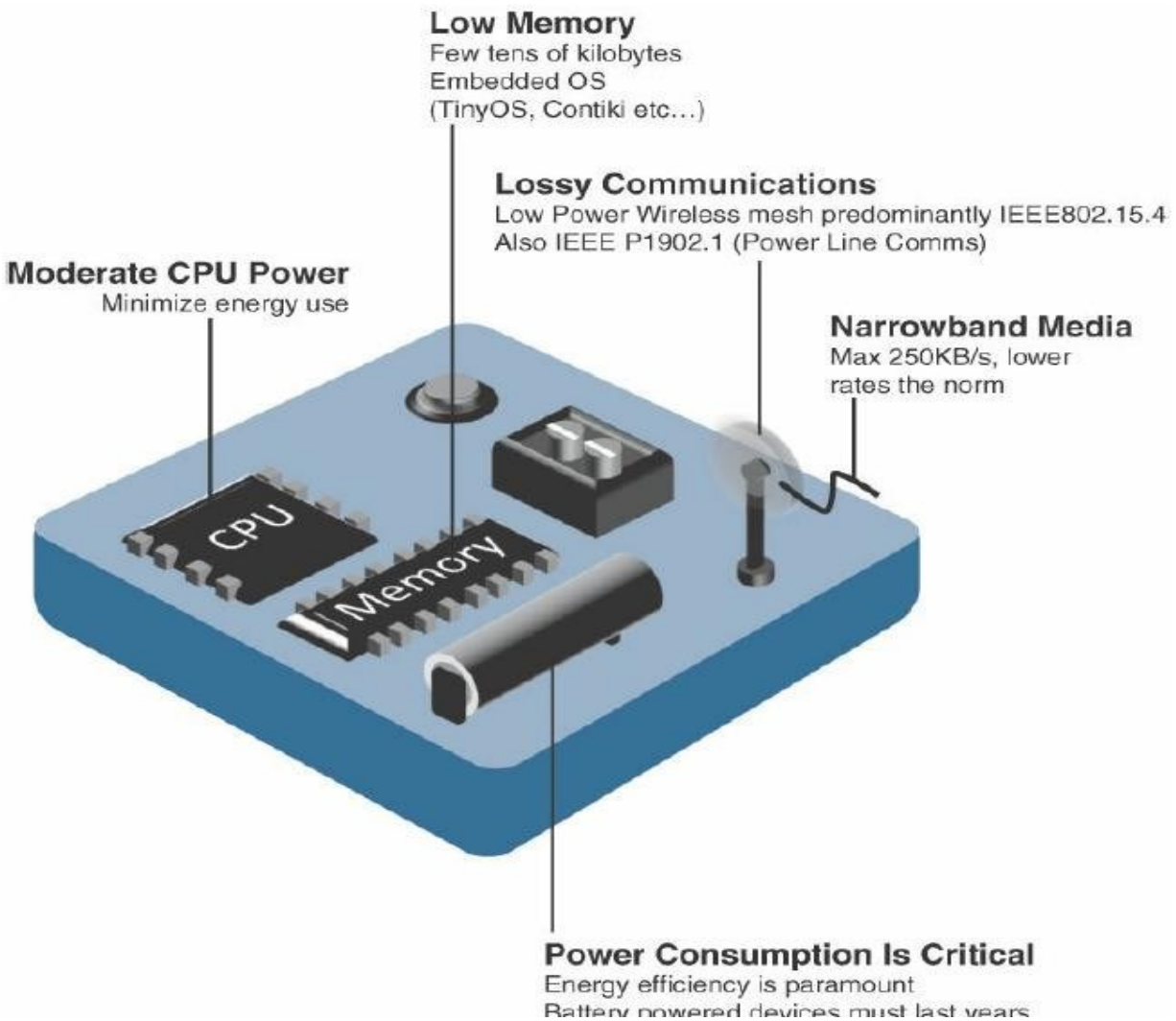
- More flexibility in deployment (especially in extreme environments or hard-to-reach places)Scalability to a large number of nodes is more straightforward.
- Reduced costs of implementation
- Long-term upkeep is less difficult.
- New sensor/actuator nodes can be added without difficulty.
- More capable of dealing with dynamic situations.

Wireless Sensor Networks (WSNs):

- Wireless sensor networks are made up of motes, which are wirelessly connected smart objects.
- Some of the most major smart object constraints in WSNs are as follows:

1. Processing power is limited.
2. Memory problems
3. Communication breakdown
4. Transmission speeds are restricted.

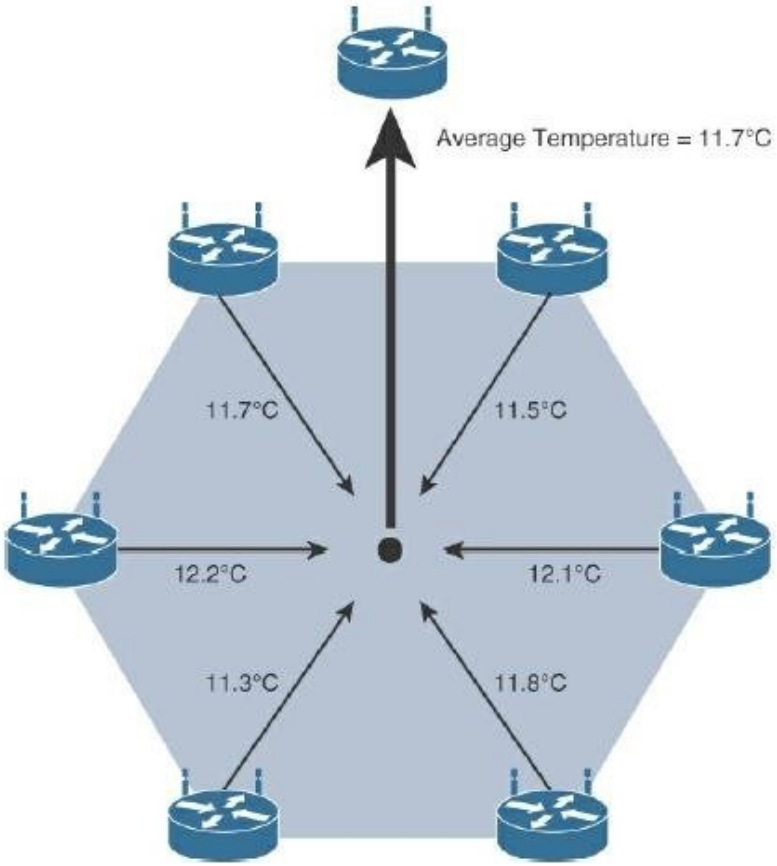
Design Constraints for Wireless Smart objects



Data Aggregation in Wireless Sensor Networks Smart Objects

In WSNs with a large number of deployed smart objects, data aggregation techniques are useful for decreasing overall traffic (and energy).

Fog and mist computing are key IoT architectural aspects for delivering the scalability and performance required by so many IoT use cases by aggregating data at the network edges.



Wireless Sensor Networks (WSNs)Continued..

- The following two communication patterns are common among wirelessly connected smart objects:

1. Event-driven:Sensory data is only transmitted when a smart object detects a certain event or reaches a predetermined threshold.
2. Periodic:Sensory information is only transmitted at regular intervals.

Wireless Sensor Networks (WSNs)Continued..

- “Communications Criteria” specifies the features and attributes that should be taken into account while selecting and dealing with connected smart objects.
- Depending on the criteria used to assess them, the various technologies for connecting sensors can vary substantially.
- 1. Range
- 2. Frequency Bands
- 3. Electricity Consumption
- 4. Organizational structure
- 5. Devices with Restrictions
- 6.Constrained-Node Networks are a type of network that has a limited number of nodes.

Wireless Sensor Networks (WSNs)Continued..

1. **Range:** How far does the signal have to travel to reach its destination?

- What will the coverage area be for a certain wireless technology?
- Should there be a distinction between inside and outdoor deployments?

A. Short range: A serial cable is a classic wired example.

- Wireless short-range solutions, which can enable tens of metres of maximum distance between two devices, are frequently regarded as a replacement to serial cables.
- IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications are two examples of short-range wireless technologies (VLC).

Wireless Sensor Networks (WSNs)Continued..

B. **Mid-range:**

This is the most common type of IoT access technology.

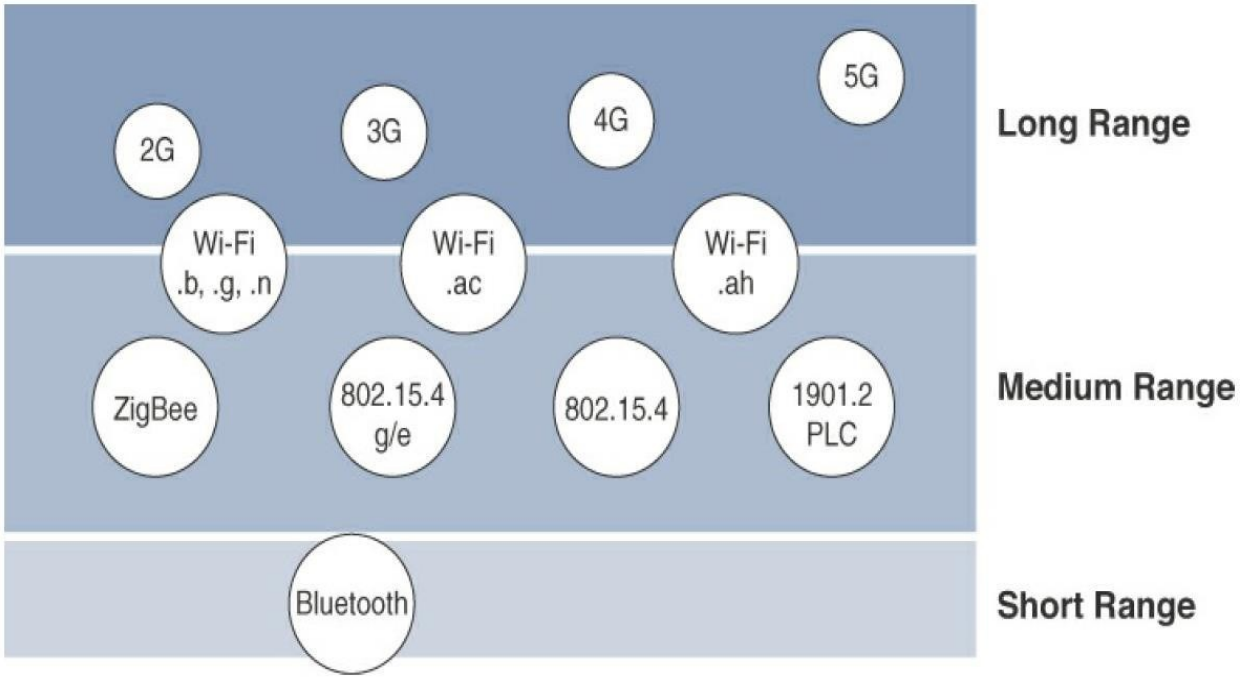
Many specifications and implementations are available in the tens to hund reds of metres range.

Although RF technologies do not have genuine maximum distances establi shed, the maximum distance between two devices is normally less than on e mile, as long as the radio signal is delivered and received within the bou ndaries of the applicable specification.

C.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.

Communications Criteria:



Wireless Access Landscape

2. Frequency Bands:

- Countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission, govern radio spectrum (FCC).
- These organizations set the rules and specifications for particular frequency bands.
- Radio, television, military, and other sorts of telecommunications, for example, are allotted portions of the spectrum.
- The frequency at which a signal is transmitted has a direct impact on how it propagates and its practical maximum range.
- Some communications in the ISM bands take place at sub-GHz frequencies.
- Protocols like IEEE 802.15.4, 802.15.4g, and 802.11ah, as well as LPWA (Low-Power Wide-Area) technologies like LoRa and Sigfox, utilise sub-GHz frequencies.T
- he sub-GHz frequency bands allow for longer distances between devices in both indoor and outdoor installations.

3. Consumption of energy

- A battery life of 2 to 3 years is an option for devices that are regularly maintained.
- Low power consumption and connectivity for battery-powered nodes must be addressed by IoT wireless access solutions.
- As a result, a new wireless environment called as Low-Power Wide-Area has emerged (LPWA)Just about any wireless technology can be powered by batteries.
- In practise, however, no operational deployment will be feasible if hundreds of batteries must be replaced every month.

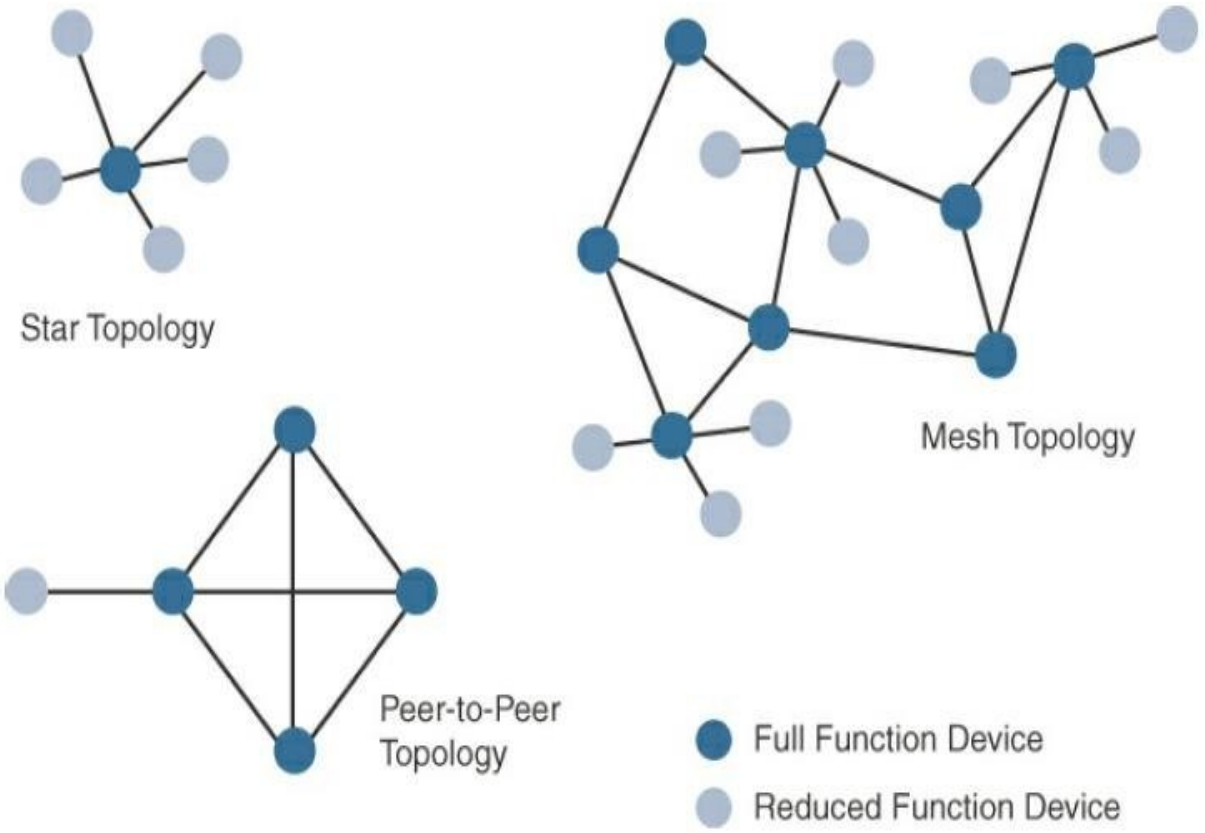
Network Topologies

Three basic topology schemes dominate among the access methods available for connecting IoT devices: star, mesh, and peer-to-peer.

A star topology is common in long-range and short-range technologies, such as cellular, LPWA, and Bluetooth networks.

To communicate with endpoints, star topologies use a single central base station or controller.

Network Topologies Continued..



Star, Peer-to-Peer, and Mesh Topologies

5. Constrained Devices:

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.

Classes of Constrained Nodes, as Defined by RFC 7228

IoT Access Technologies:

1. Standardization and alliances: The standards bodies that maintain the protocols for a technology Layer
2. Physical The required frequencies and wired or wireless techniques
3. MAC layer: Considerations at the Media Access Control (MAC) layer, which connects the physical and data link control layers.
4. Topology: The technology's supported topologies
5. Security: Aspects of technology security Competitive technologies:

IoT Access Technologies Continued..

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.

IoT Access Technologies Continued..

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.

ZigBee Alliances

- The initial ZigBee specification was introduced in 2004, shortly after the IE EE 802.15.4 specification was released the year before. It was based on th e idea of ZigBee-style networks in the late 1990s.

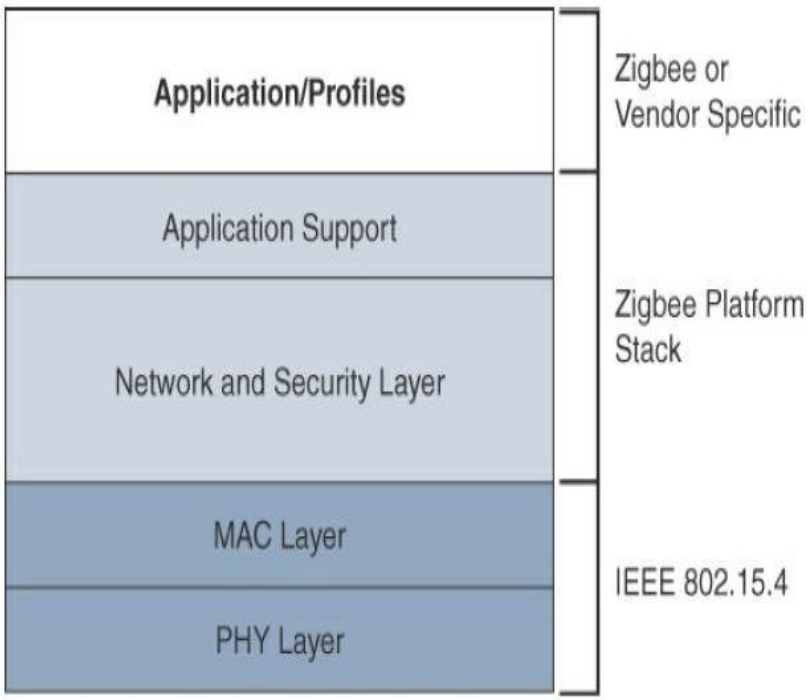
  The ZigBee Alliance now has over 400 members, representing a significant increase in industry support.

  •

  The Zigbee Alliance, is an industry body dedicated to certifying vendor co mpatibility and advancing and growing ZigBee as an IoT solution for interc onnecting smart items.
- ZigBee can control lighting, thermostats, and security systems in the home.
- ZigBee Smart Energy connects a number of interoperable items, such as smart meters, to monitor and regulate the use and delivery of utilities like electricity and water.
- The utility provider controls these ZigBee items, which can help coordinate use between homes and businesses, as well as the utility provider itself, for more efficient operations.

ZigBee Alliances Continued..

- The IEEE 802.15.4 protocol is still supported by ZigBee IP, but the IP and TCP/UDP protocols, as well as other open standards, are now supported at the network and transport layers.
- The ZigBee-specific layers are now found only at the top of the protocol stack for the applications.
- The open standards resulting from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL, were incorporated into ZigBee IP.



High-Level ZigBee Protocol Stack

LoRaWAN: Low-Power Wide-Area Network

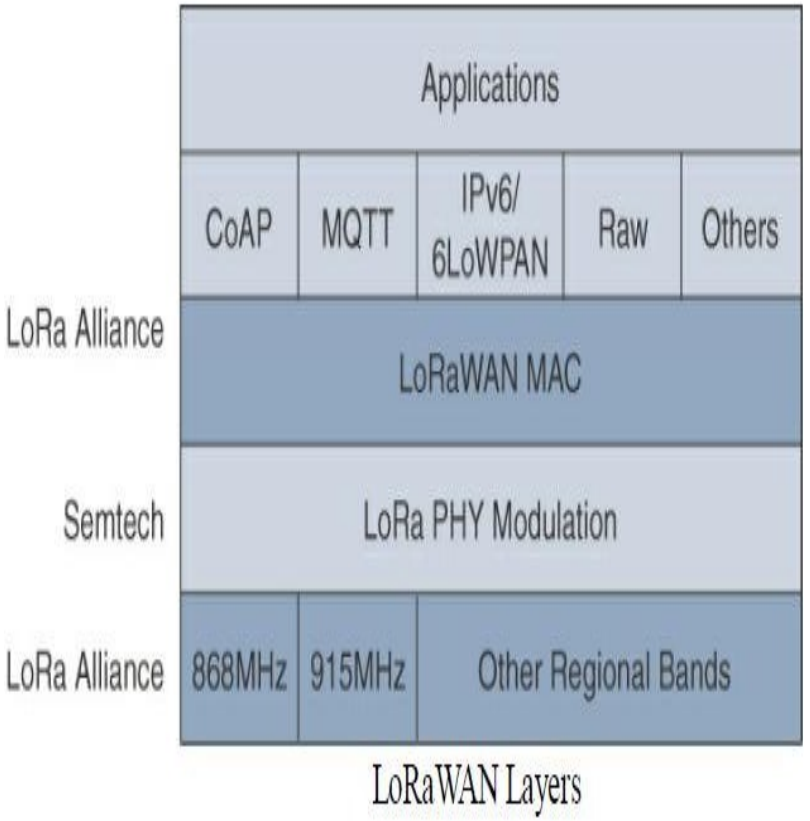
- LoRaWAN:Low-Power Wide-Area Wireless is a new collection of wireless technologies (LPWA).
- LPWA technologies, which are particularly well suited for long-range and battery-powered endpoints, open up new business prospects for both service providers and businesses seeking IoT solutions.
- Standardization and Alliances: Initially, LoRa was a physical layer, or Layer 1, modulation created by Cycleo, a French firm.
- Cycleo was later purchased by Semtech.
- With the formation of the LoRa Alliance, the technology moved fro m Layer 1 to a broader scope, optimised for long-range, two-way communications and low battery consumption.

LoRaWAN Continued..

- Multiple chipset suppliers provide Semtech LoRa as a Layer 1 PHY modulation technology, resulting in standardisation and alliances.
- The LoRa Alliance uses the word LoRaWAN to denote to its architecture and specifications that describe end-to-end LoRaWAN communications and protocols, as opposed to the physical layer modulation known as LoRa.
- The LoRaWAN layers are depicted in the following diagram at a high level.Semtech is in charge of the PHY layer in this diagram, whereas the LoRa Alliance is in charge of the MAC layer.

LoRaWAN Standardization and Alliances:

- The Semtech LoRa modulation is based on chirp spread spectrum modulation, which sacrifices a lower data rate for higher receiver sensitivity in order to greatly extend communication distance.
- It also allows demodulation below the noise floor, provides robustness against noise and interference, and regulates the occupation of a single channel by different spreading factors.
- This allows LoRa devices to receive data on many channels at the same time.
- The key unlicensed sub-GHz frequency bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz are described in the LoRaWAN 1.0.2 regional specifications.



LoRaWAN Layers

Competitive Technologies

Characteristic	LoRaWAN	Sigfox	Ingenu Onramp
Frequency bands	433 MHz, 868 MHz, 902–928 MHz	433 MHz, 868 MHz, 902–928 MHz	2.4 GHz
Modulation	Chirp spread spectrum	Ultra-narrowband	DSSS
Topology	Star of stars	Star	Star; tree supported with an RPMA extender
Data rate	250 bps–50 kbps (868 MHz) 980 bps–21.9 kbps (915 MHz)	100 bps (868 MHz) 600 bps (915 MHz)	6 kbps
Adaptive data rate	Yes	No	No
Payload	59–230 bytes (868 MHz) 19–250 bytes (915 MHz)	12 bytes	6 bytes–10 KB
Two-way communications	Yes	Partial	Yes

LoRaWAN Conclusions

- The LoRaWAN wireless technology was created for low-power wide-area networks (LPWANs), which are crucial for deploying many new devices on IoT networks.
- LoRaWAN focuses on the architecture, the MAC layer, and a unified, single standard for smooth interoperability, while LoRa refers to the PHY layer.
- The LoRa Alliance, an industry association, is in charge of LoRaWAN.

A common information set is provided about the IoT access technologies which are as listed below:

- Standardization and alliances: The standards bodies that maintain the protocols for a technology
- Physical layer: The wired or wireless methods and relevant frequencies
- MAC layer: Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control
- Topology: The topologies supported by the technology
- Security: Security aspects of the technology
- Competitive technologies: Other technologies that are similar and may be suitable alternatives to the given technology

Technologies for connecting smart objects

- **IEEE 802.15.4:** an older but foundational wireless protocol for connecting smart objects.
- **IEEE 802.15.4g and IEEE 802.15.4e:** improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
- **IEEE 1901.2a:** technology for connecting smart objects over power lines.
- **IEEE 802.11ah:** A technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
- **LoRaWAN: A** scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
- **NB-IoT and Other LTE Variations:** That are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

Communications Criteria

- **Range:** This section examines the importance of signal propagation and distance.
- **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies. Power Consumption: This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.
- **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.
- **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.
- **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.

IEEE 802.15.4

- Wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries
- Enables easy installation using a compact protocol stack
- Simple and flexible.
- Wide range of IoT use cases in both the consumer and business markets

IEEE 802.15.4 deployments:

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

Disadvantages

- The negatives around reliability and latency often have to do with the Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithms.
- CSMA/CA is an access method in which a device “listens” to make sure no other devices are transmitting before starting its own transmission. If another device is transmitting, a wait time (which is usually random) occurs before “listening” occurs again.
- Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique.
- Later variants of 802.15.4 from the IEEE start to address these issues.

S.No	Protocol	Description
1.	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
2.	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 enhancement to cope with the specific details of IEEE 802.15.4
3.	ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer , IPv6 network layer, RPL routing protocol. In addition, it offers improvement in IP security.
4.	ISA100.11a	This 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. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards
5.	Wireless HART	Wireless HART 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 2.4GHz frequency band.
6.	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.

ZIGBEE TECHNOLOGY

- Technological Standard Created for Control and Sensor Networks
- Based on the IEEE 802.15.4 Standard
- High level Communication
- Wireless Personal Area Networks (WPANs)
- Created by the ZigBee Alliance

History

- ZigBee-style networks began to be conceived in 1998 when many engineers realized that WiFi and Bluetooth would be unsuitable for many applications.

  In particular, many engineers saw a need for self-organizing ad-hoc digital radio networks.
- The IEEE 802.15.4 standard was completed in May 2003.
- The ZigBee specifications were ratified on 14 December 2004.
- The ZigBee Alliance announces the public availability of Specification 1.0 on 13 June 2005.

Layers of ZigBee network:

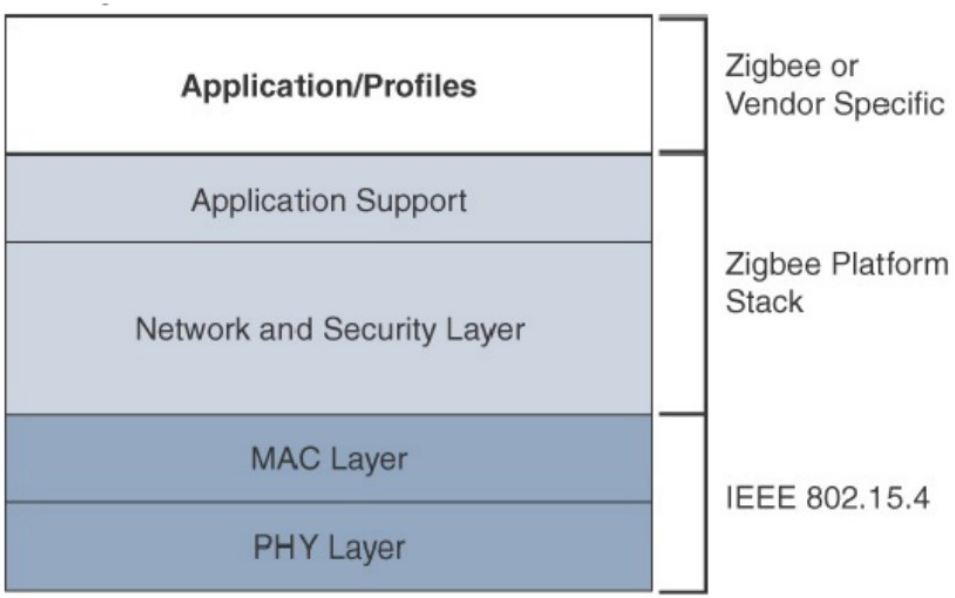
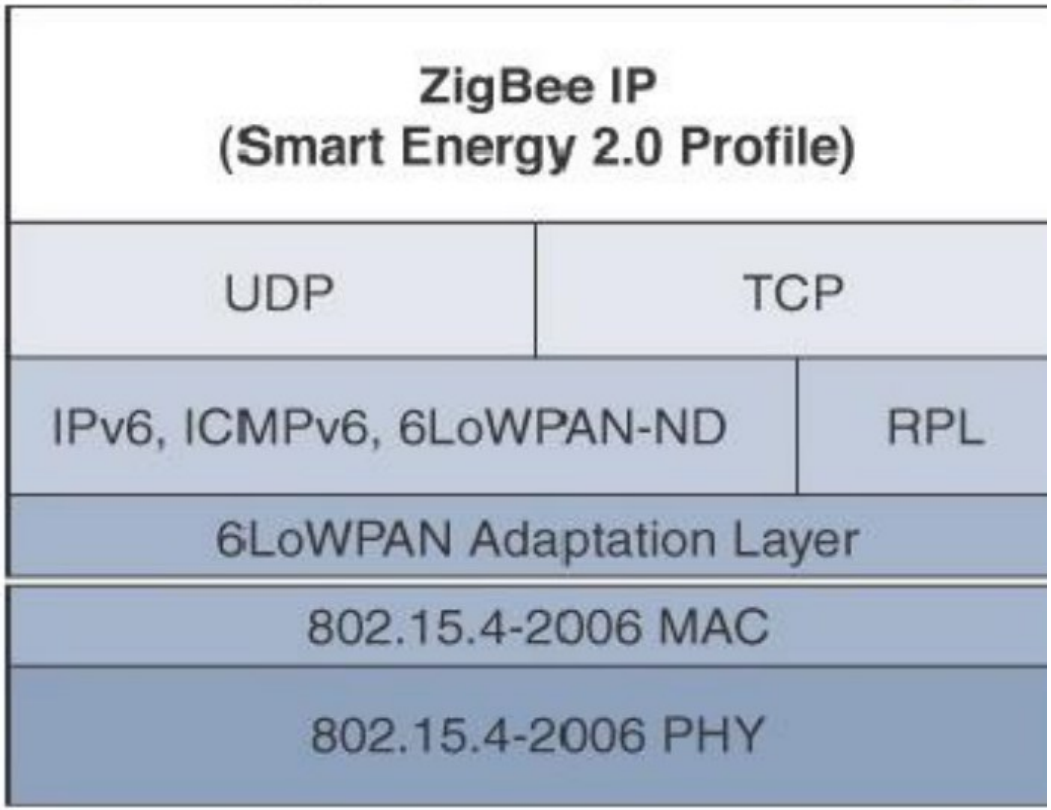


Figure 2.1 High Level ZigBee Protocol Stack

- The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications.
- This includes calculating routing paths in what is often a changing topology, discovering neighbors, and managing the routing tables as devices join for the first time.
- The network layer is also responsible for forming the appropriate topology, which is often a mesh but could be a star or tree as well.
- From a security perspective, 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.

- The application support layer 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. ZigBee is one of the most well-known protocols built on an IEEE 802.15.4 foundation. On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles.

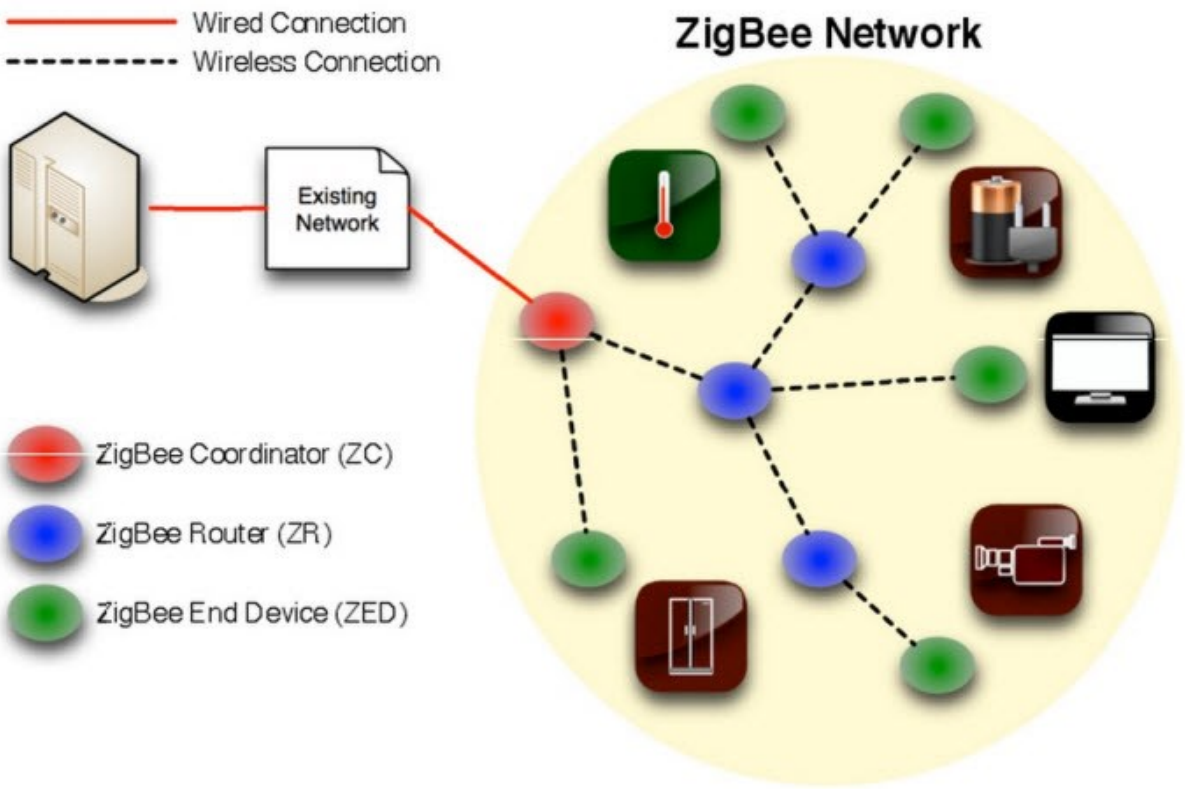


ZigBee IP protocol stack

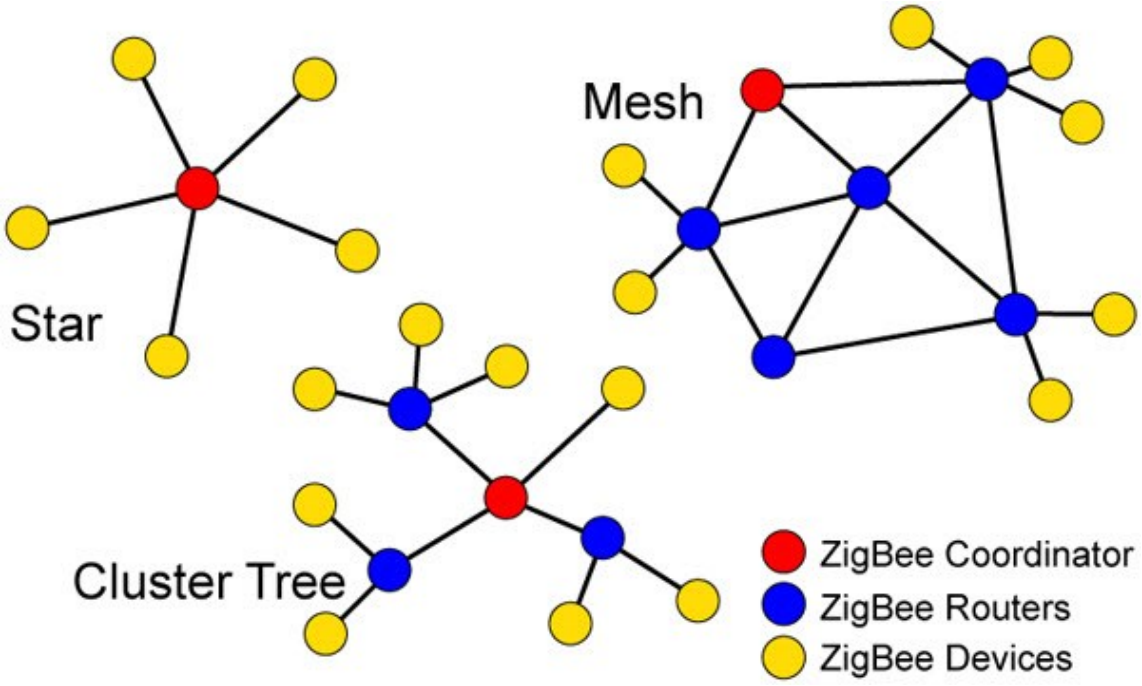
ZigBee IP/SE 2.0

- Follows IEEE STD 802.15.4 STD protocol
- Zigbee endpoint devices form WPAN of embedded sensors, actuators, appliance controllers or medical data s/y's – IoT Applications
- Zigbee Neighborhood Area N/w (NAN) is the version for Smart Grid. Ex Smart Metering.
- Features of Zigbee IP
  - Used for Low Power Short range WPAN
  - Device can function in 6 modes – end point, ZigBee device router, N/W coordinator, IP coordinator, IP router and IP Host
  - Supports RFD – Reduced function device - goes to sleep mode once its work is done
  - Supports IPv6 with 6LoWPAN
  - Self configuring, healing , dynamic pairing
  - Range – 10 – 200m, Data rates : 250kbps, low power operation
  - AES-CCM-128

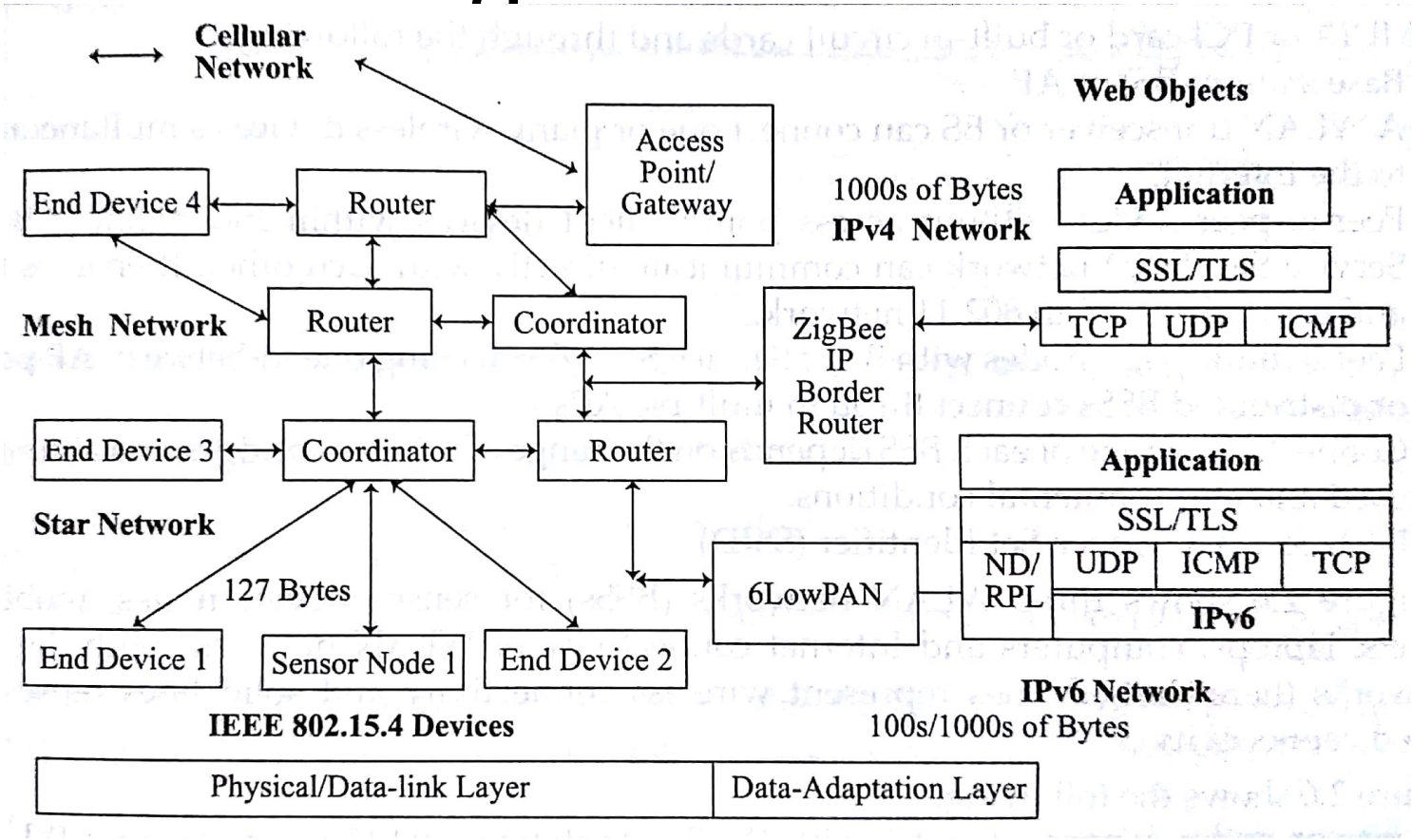
Zigbee


Wired Connection
Wireless Connection
Existing Network
ZigBee Network
ZigBee Coordinator (ZC)
ZigBee Router (ZR)
ZigBee End Device (ZED)

Zigbee Topologies



Zigbee - Modes



ZigBee IP/SE 2.0

- Features of Zigbee
- The router in star network connects to 6LoWPAN, which connects an IEEE 802.15.4 devices network to IPv6 n/w

Physical Layer

The original physical layer transmission options were as follows:

- 2.4 GHz, 16 channels, with a data rate of 250 kbps
- 915 MHz, 10 channels, with a data rate of 40 kbps
- 868 MHz, 1 channel, with a data rate of 20 kbps

IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following

- OQPSK PHY: This is DSSS PHY, employing offset quadrature phase-shift keying (OQPSK) modulation. OQPSK is a modulation technique that uses four unique bit values that are signaled by phase changes. An offset function that is present during phase shifts allows data to be transmitted more reliably.
- BPSK PHY: This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation. BPSK specifies two unique phase shifts as its data encoding scheme.
- ASK PHY: This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation. PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS. ASK uses amplitude shifts instead of phase shifts to signal different bit values

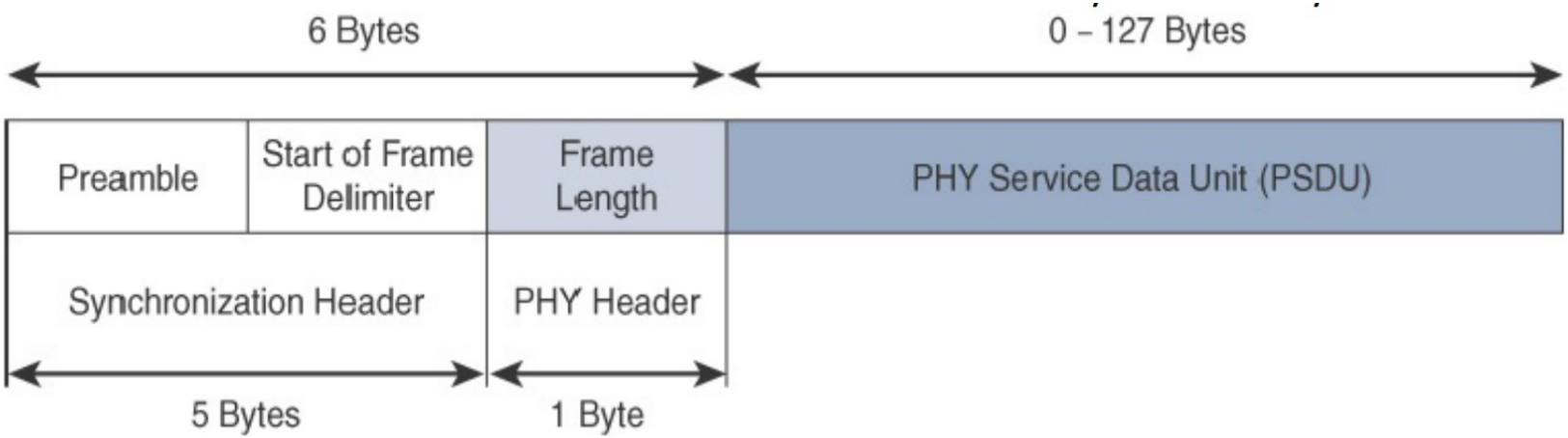


Figure 2.3 IEEE 802.15.4 PHY Format

MAC Layer

- The 802.15.4 MAC layer performs the following tasks:
  - Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
  - PAN association and disassociation by a device
  - Device security
  - Reliable link communications between two peer MAC entities

- The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of MAC frames are specified in 802.15.4:
  - Data frame: Handles all transfers of data
  - Beacon frame: Used in the transmission of beacons from a PAN coordinator
  - Acknowledgement frame: Confirms the successful reception of a frame
  - MAC command frame: Responsible for control communication between devices

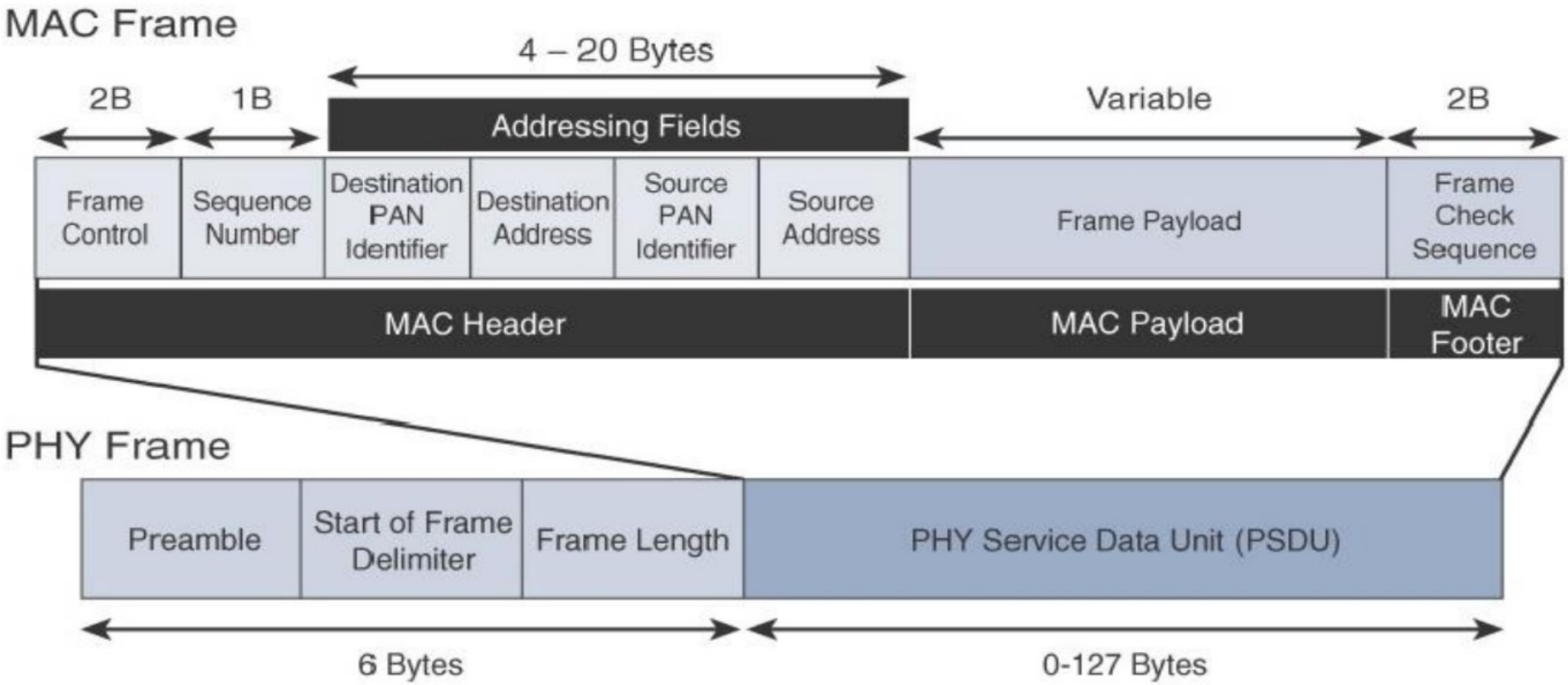


Figure 2.4 IEEE 802.15.4 MAC Format

IEEE 802.15.4g and 802.15.4e

- IEEE 802.15.4g-2012 is also an amendment to the IEEE 802.15.4-2011 standard
- 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 industrialsupervisory 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

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

Table 4-3 *Industry Alliances for Some Common IEEE Standards*

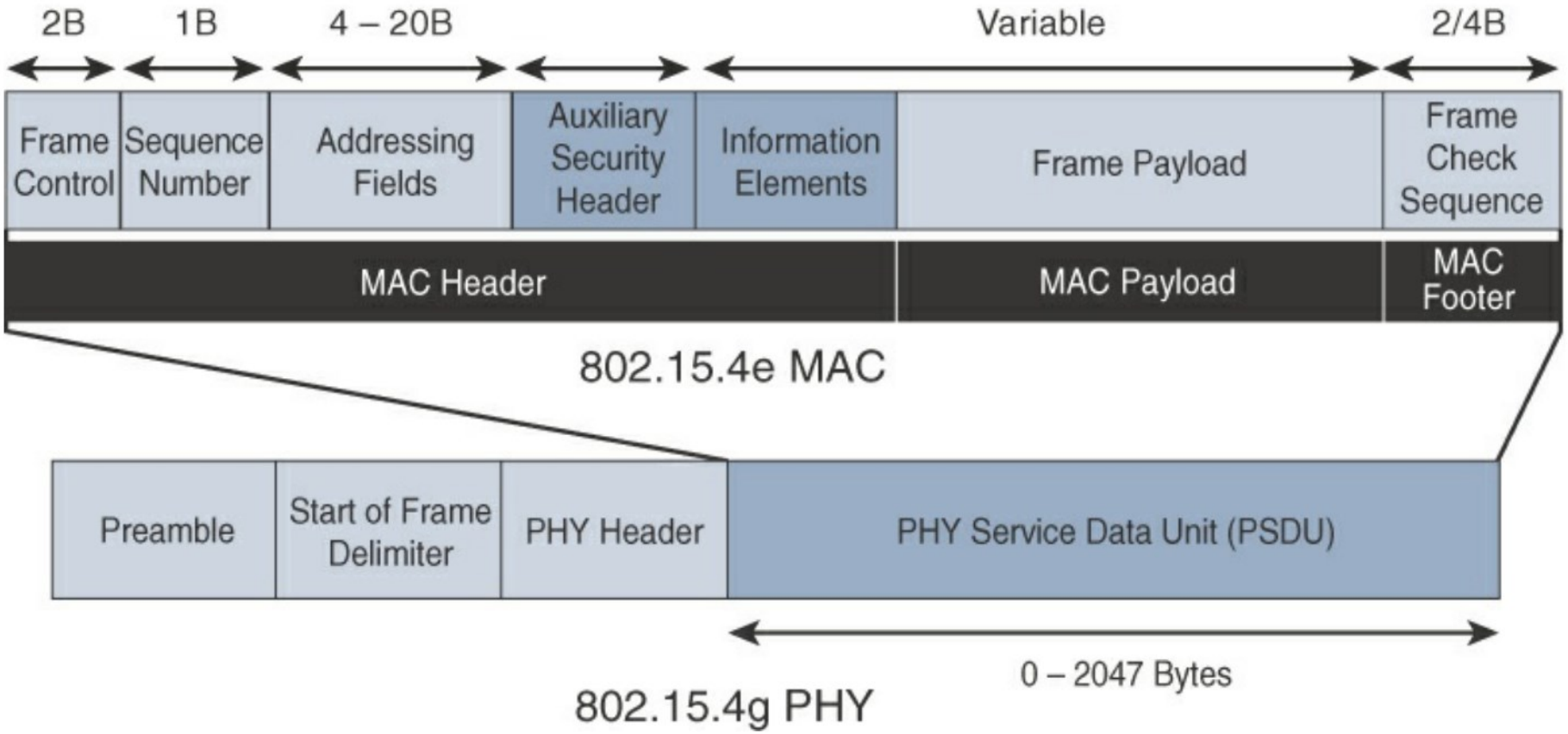
Physical Layer

- **Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK):** 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 cost-effective and easier to design

MAC Layer: enhancements to the MAC layer proposed by IEEE 802.15.4e-2012

- Time-Slotted Channel Hopping (TSCH)
- Information elements
  - allow for the exchange of information at the MAC layer in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).
  - Specified in a tag, length, value (TLV) format, the IE field allows frames to carry additional metadata to support MAC layer services.
- Enhanced beacons (EBs)
  - EBs extend the flexibility of IEEE 802.15.4 beacons to allow the construction of application-specific beacon content. This is accomplished by including relevant IEs in EB frames. Some IEs that may be found in EBs include network metrics, frequency hopping broadcast schedule, and PAN information version.

- 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. Beacon responses are then limited to what was requested in the EBR. For example, a device can query for a PAN that is allowing new devices to join or a PAN that supports a certain set of MAC/PHY capabilities.
- 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.


2B
1B
4 – 20B
Variable
2/4B
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security Header
Information Elements
Frame Payload
Frame Check Sequence
MAC Header
MAC Payload
MAC Footer
802.15.4e MAC
Preamble
Start of Frame Delimiter
PHY Header
PHY Service Data Unit (PSDU)
0 – 2047 Bytes
802.15.4g PHY

Topology

- Mesh
- 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. Considering the use cases addressed by this technology, powered nodes have been the primary targets of implementations. Support for batterypowered nodes with a long lifecycle requires optimized Layer 2 forwarding or Layer 3 routing protocol implementations. This provides an extra level of complexity but is necessary in order to cope with sleeping battery-powered nodes.

security

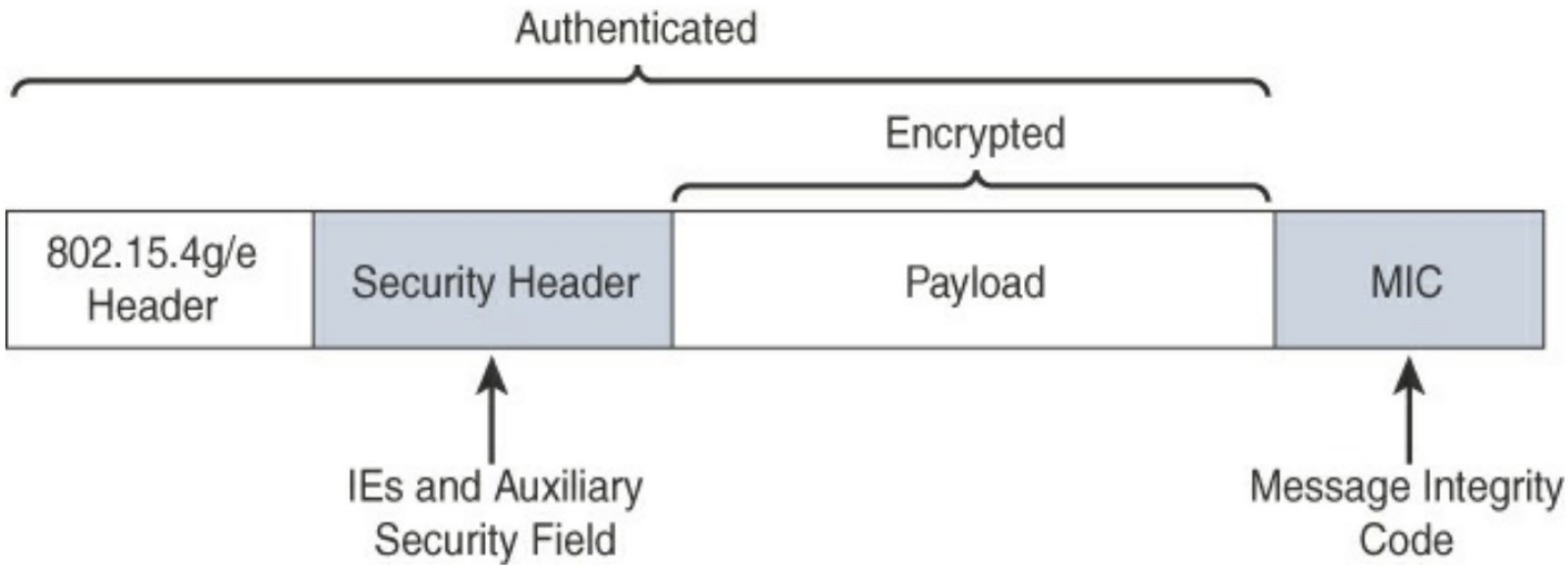


Figure 4-10 *IEEE 802.15.4g/e MAC Layer Security*