Smart Objects: The “Things” in IoT

Module 2

- Sensors are fundamental building blocks of IoT networks
- Sensors are the foundational elements found in smart objects—the “things” in the Internet of Things

- Smart objects are **any physical objects** that contain **embedded technology to sense and/or interact with their environment in a meaningful way by being interconnected and enabling communication among themselves or an external agent.**

SENSORS, ACTUATORS, AND SMART OBJECTS

- **A sensor**: It senses
- More specifically, ***a sensor measures some physical quantity and converts that measurement reading into a digital representation.***
- ***That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans***
- Sensors are not limited to human-like sensory data.
- They are able to provide an extremely wide spectrum of rich and diverse measurement data with far greater precision than human senses

Categories

- **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).**

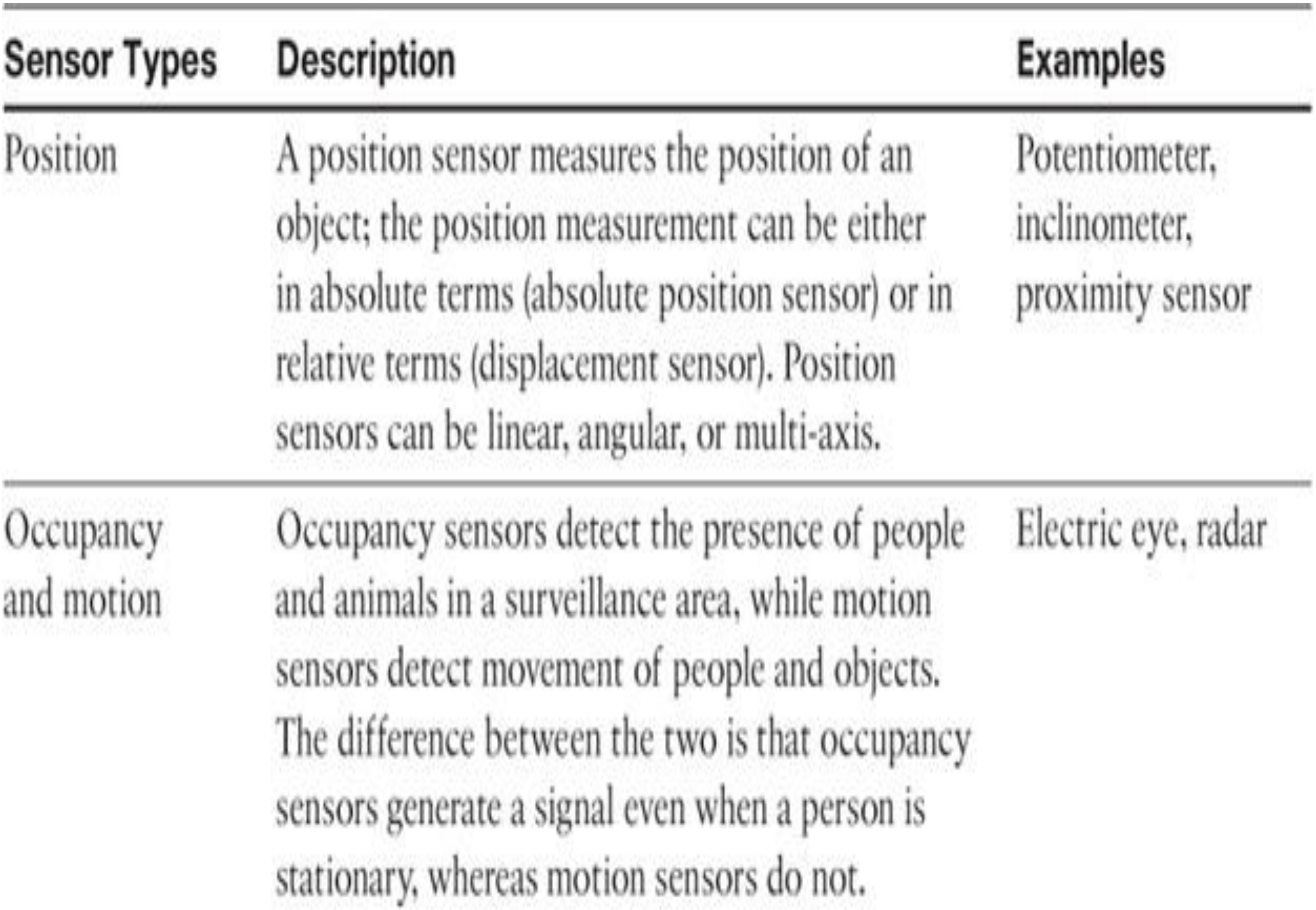
- **Area of application:**
- Sensors can be categorized based on the **specific industry** or **vertical** where they are being used.

- **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*).

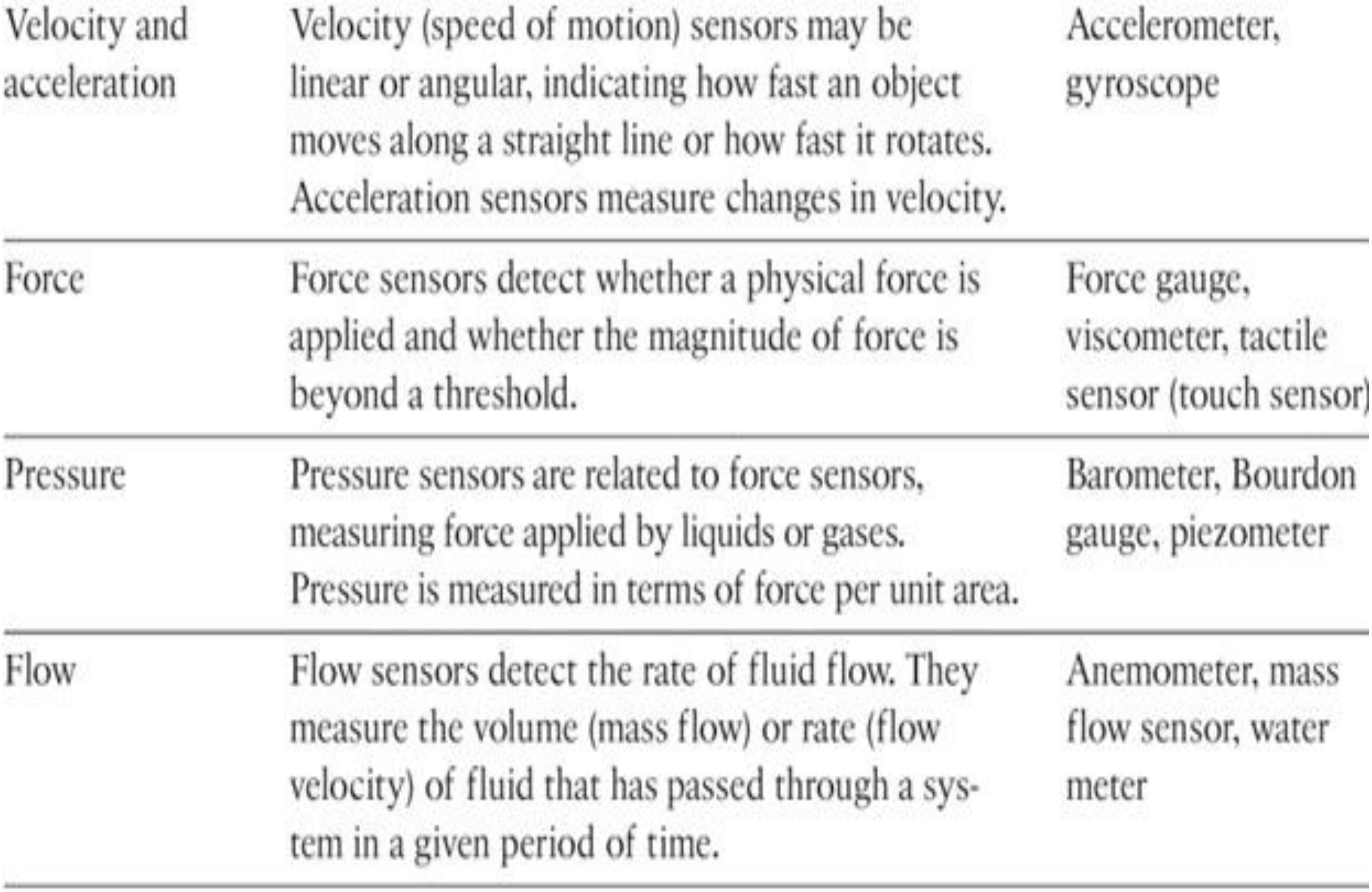
- **What sensors measure:**
- Sensors can be categorized **based on their applications** or **what physical variables they measure.**

- Note that this is by no means an exhaustive list, and there are many other classification and taxonomic schemes for sensors, including those based on material, cost, design, and other factors

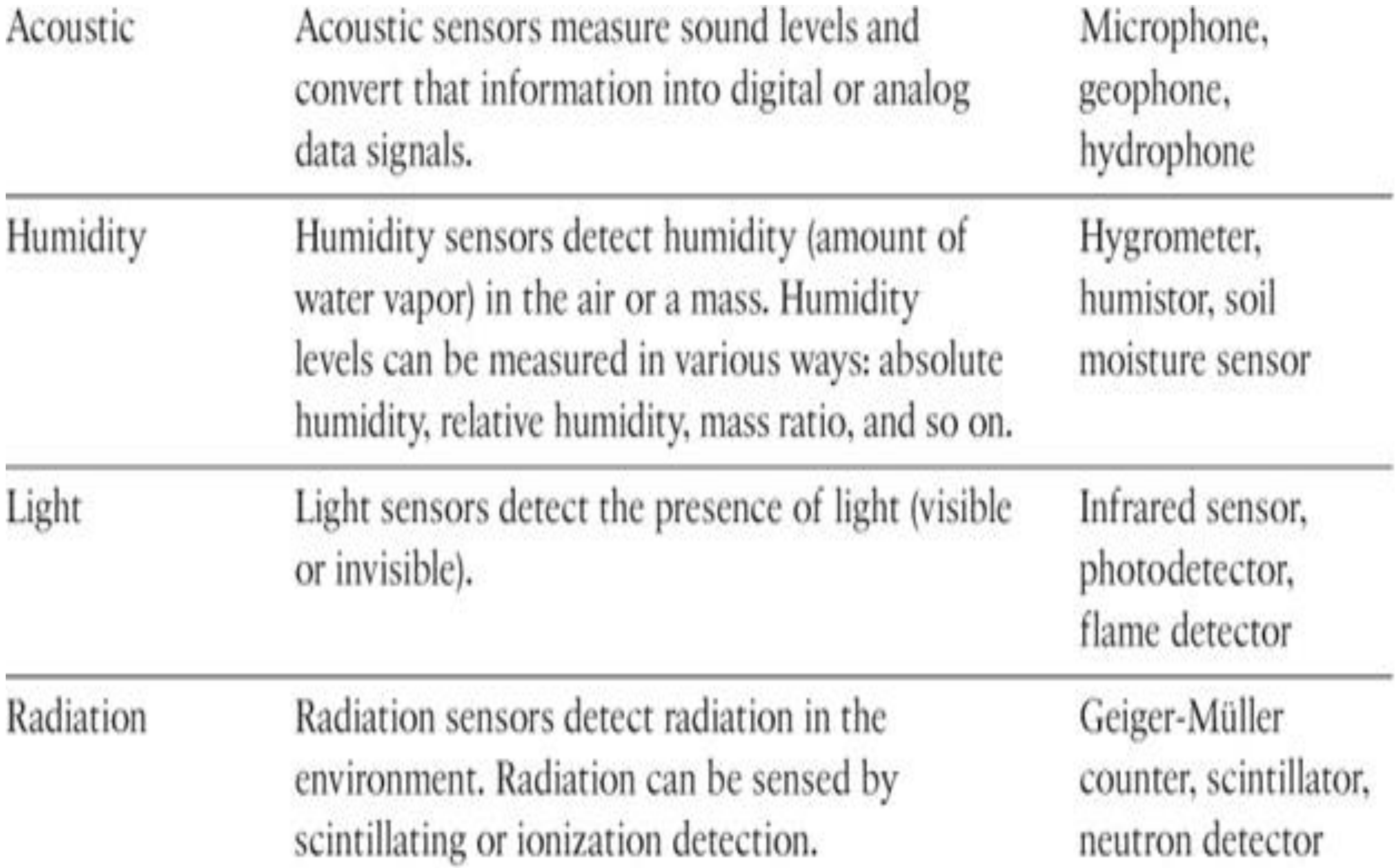
Categorization based on what physical phenomenon a sensor is measuring



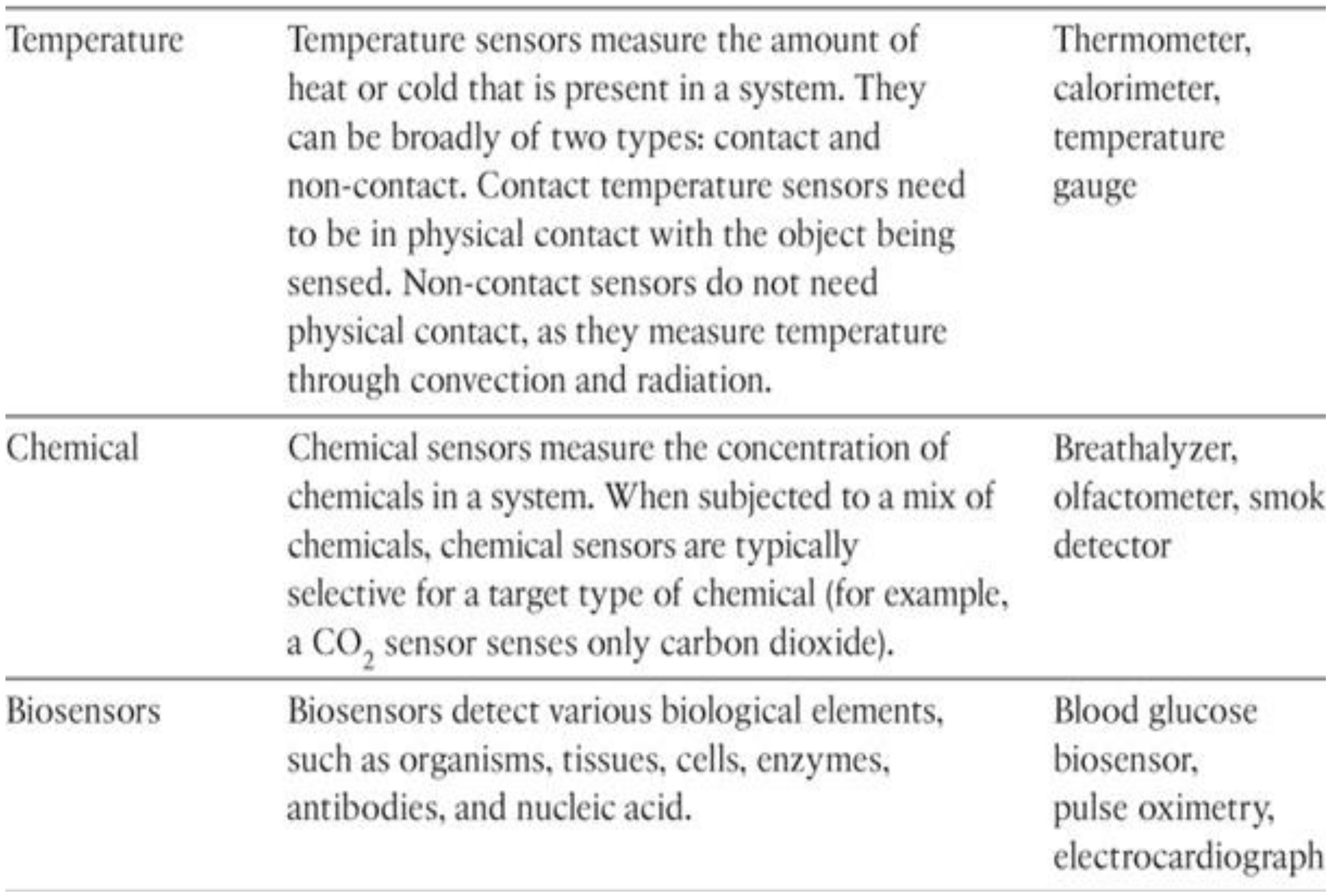
Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar



Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter



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
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
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, smok detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

Precision agriculture (smart farming)

- which uses a variety of technical advances to improve the efficiency, sustainability, and profitability of traditional farming practices.
- This includes the *use of GPS and satellite aerial imagery for determining field viability; robots for high-precision planting, harvesting, irrigation, and so on; a*nd *real-time analytics and artificial intelligence to predict optimal crop yield, weather impacts, and soil quality*.
- Among the most significant impacts of precision agriculture are those dealing with **sensor measurement of a variety of soil characteristics**. *These include real- time measurement of soil quality, pH levels, salinity, toxicity levels, moisture levels for irrigation planning, nutrient levels for fertilization planning, and so on*.
- All this detailed sensor data can be analyzed to provide highly valuable and actionable insight to boost productivity and crop yield.

IoT Use Case: Area of precision agriculture (smart farming)

- biodegradable, passive microsensors to measure soil and crop and conditions

.

- These sensors, developed at North Dakota State University (NDSU), can be planted directly in the soil and left in the ground to biodegrade without any harm to soil quality.

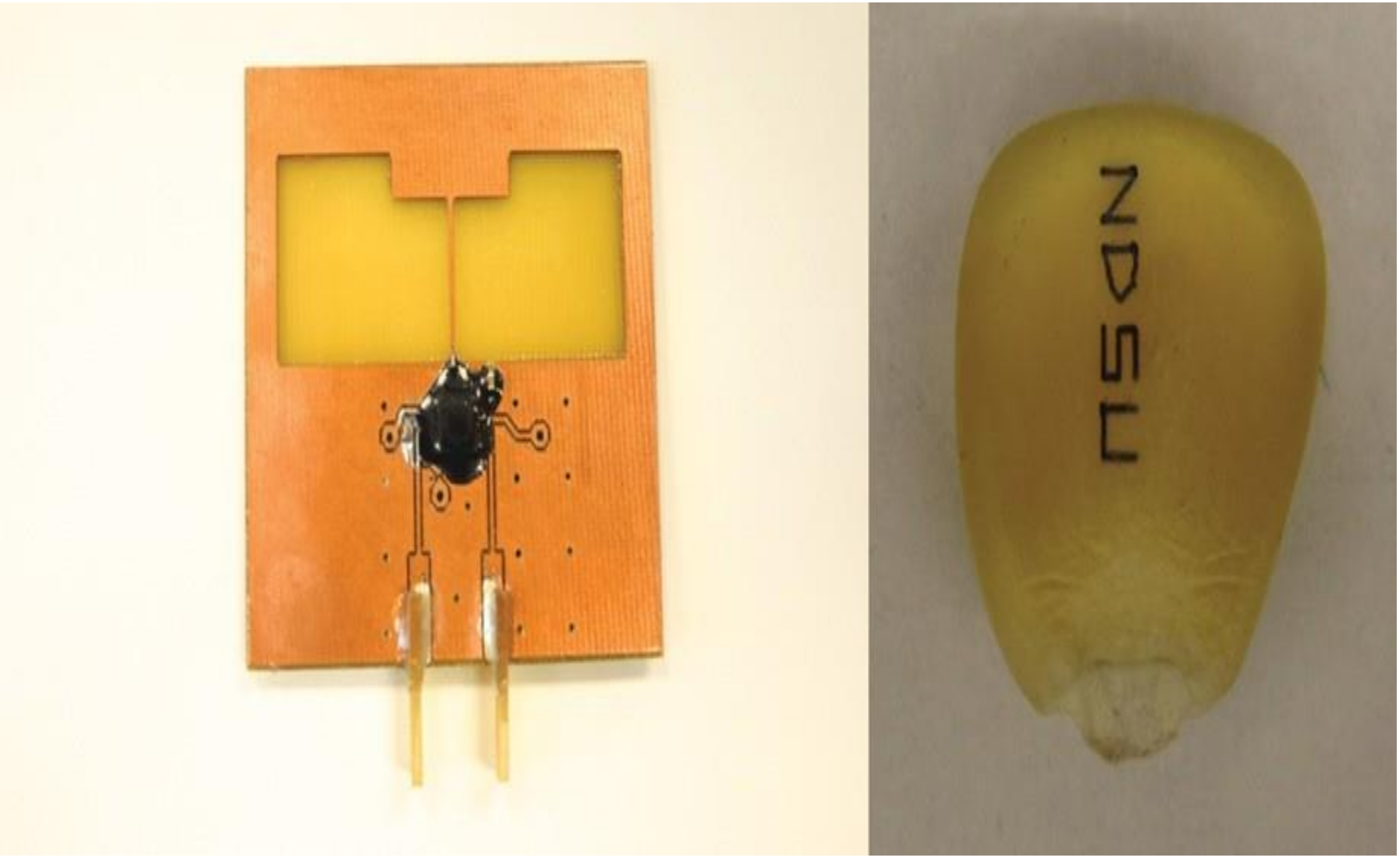
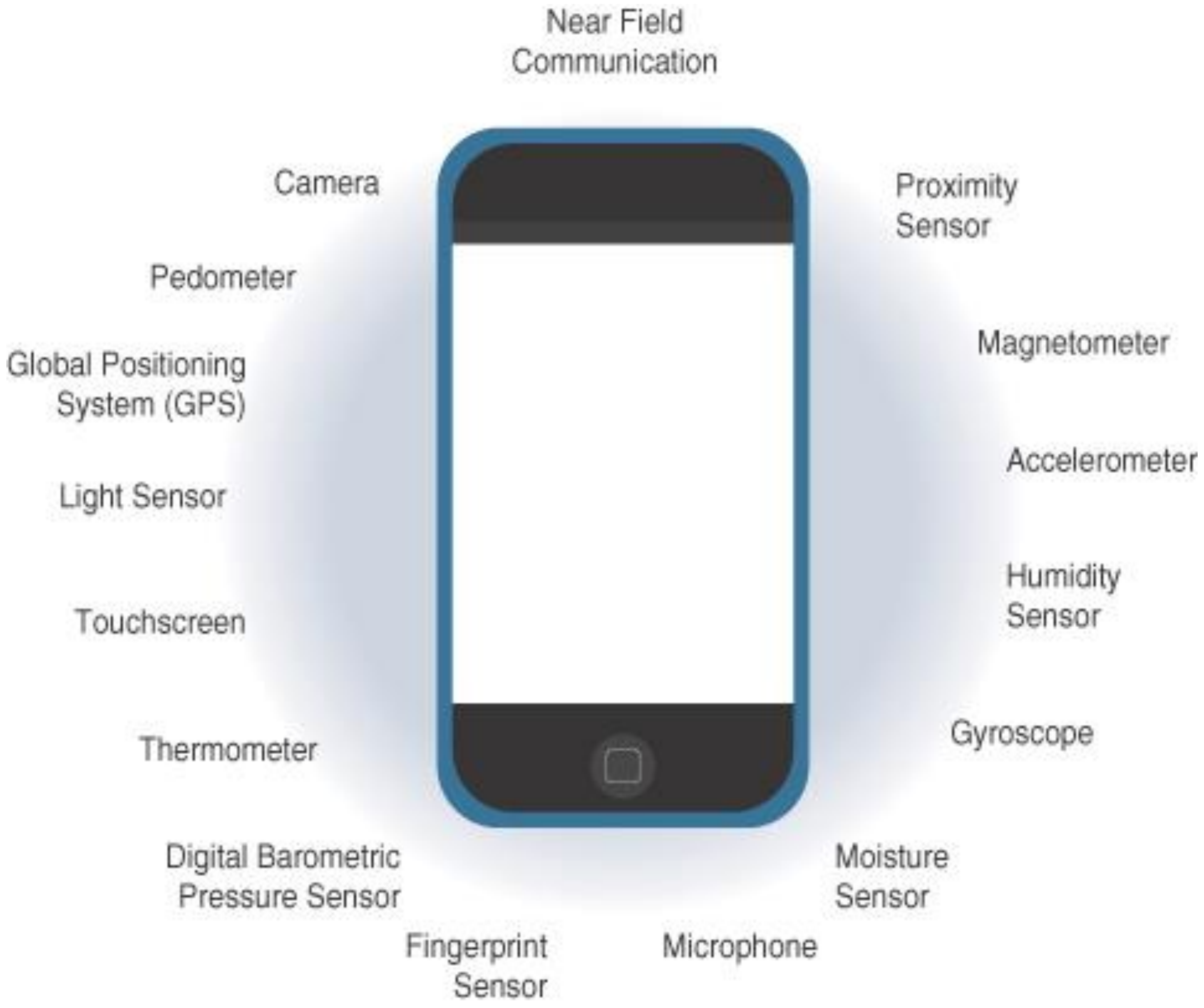


Figure 3-1 *Biodegradable Sensors Developed by NDSU for Smart Farming*

Sensors in a Smart Phone



Near Field Communication

Proximity Sensor

Magnetometer

Accelerometer

Humidity Sensor

Gyroscope

Moisture Sensor

Microphone

Fingerprint Sensor

Digital Barometric Pressure Sensor

Thermometer

Touchscreen

Light Sensor

Global Positioning System (GPS)

Pedometer

Camera

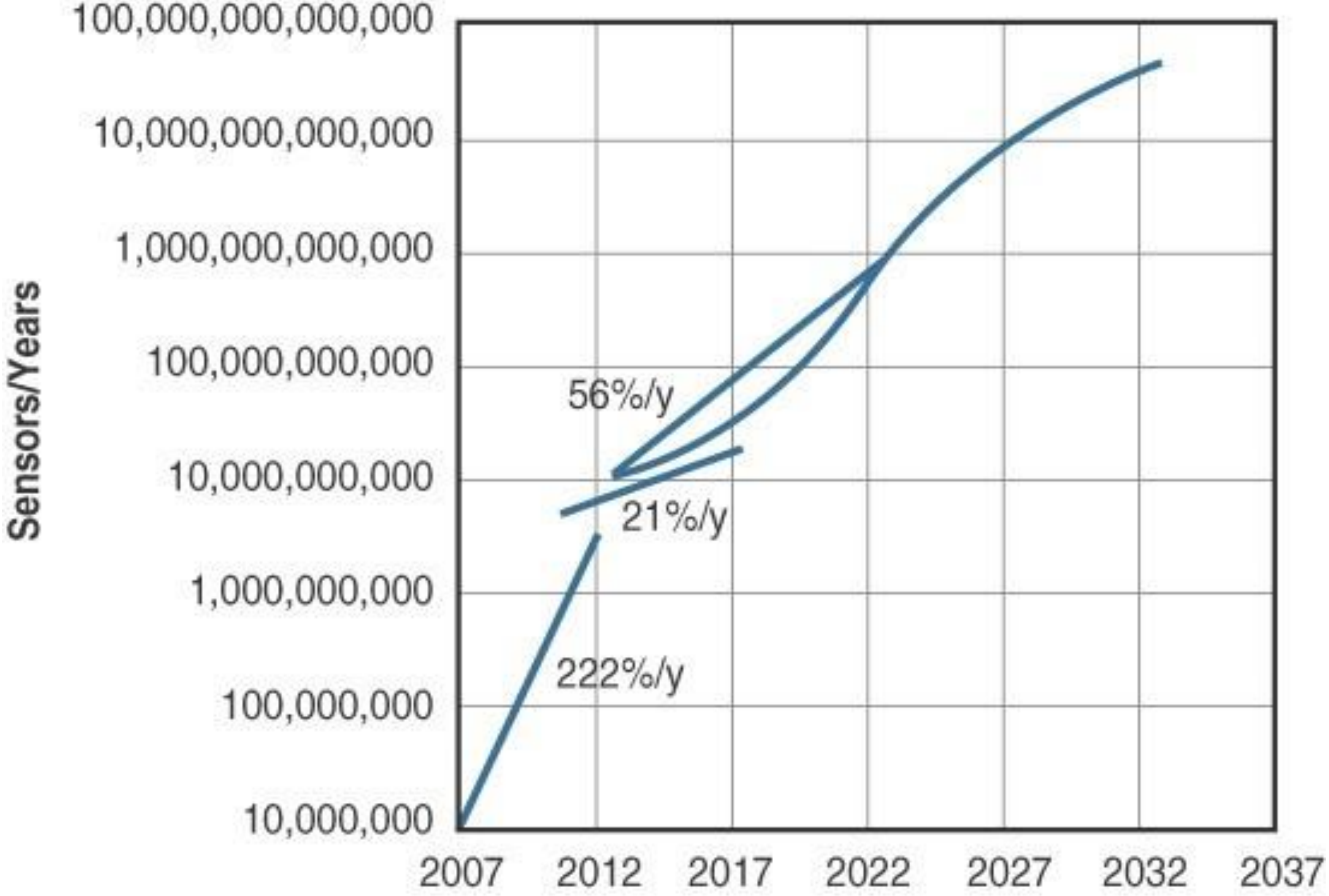
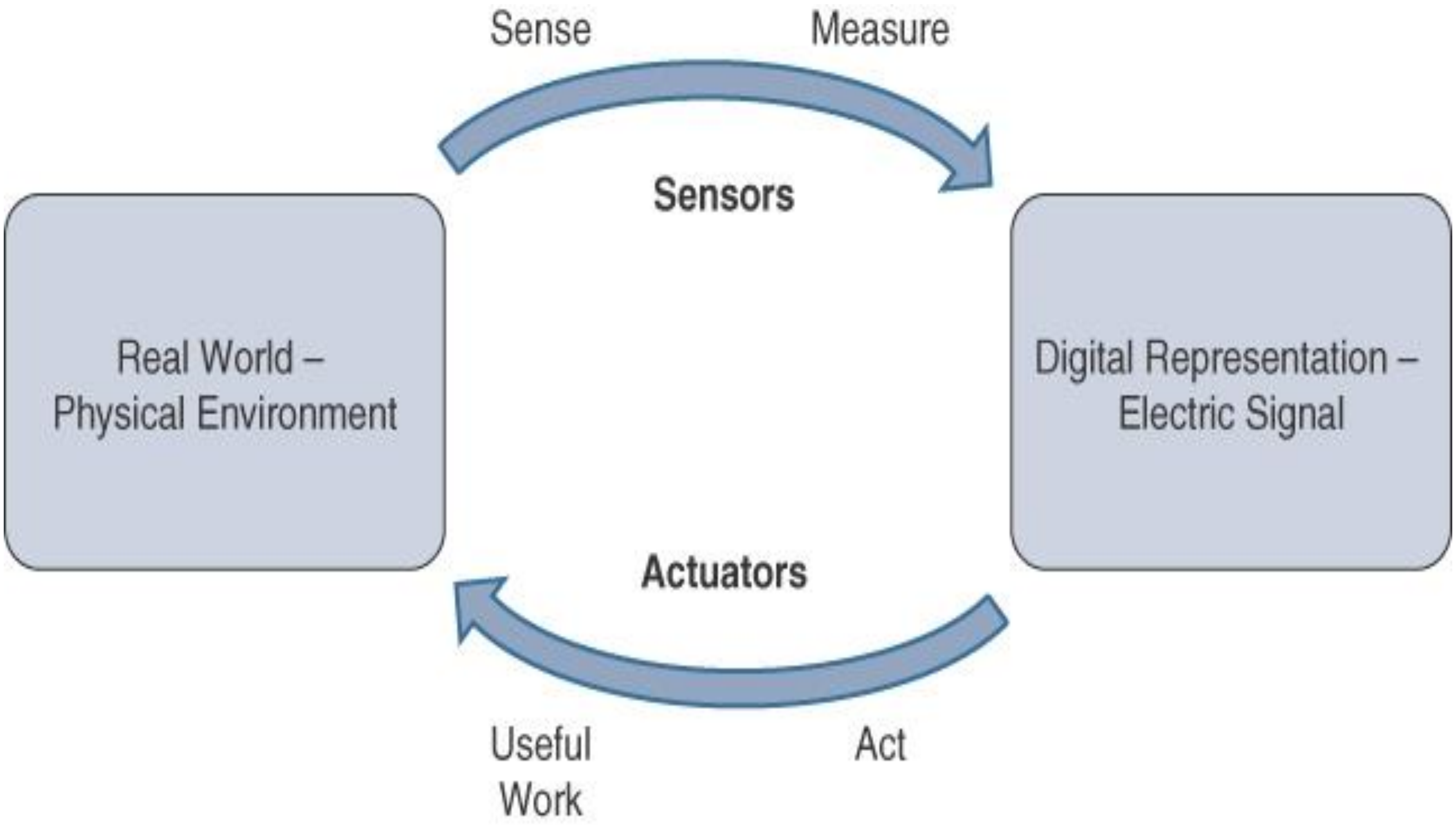


Figure 3-3 *Growth and Predictions in the Number of Sensors*

Actuators

- Actuators are natural complements to sensors
- Sensors are designed to sense and measure practically any measurable variable in the physical world.
- They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).
- **Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.**
- ***Sensors provide the information, actuators provide the action***



Sense

Measure

Sensors

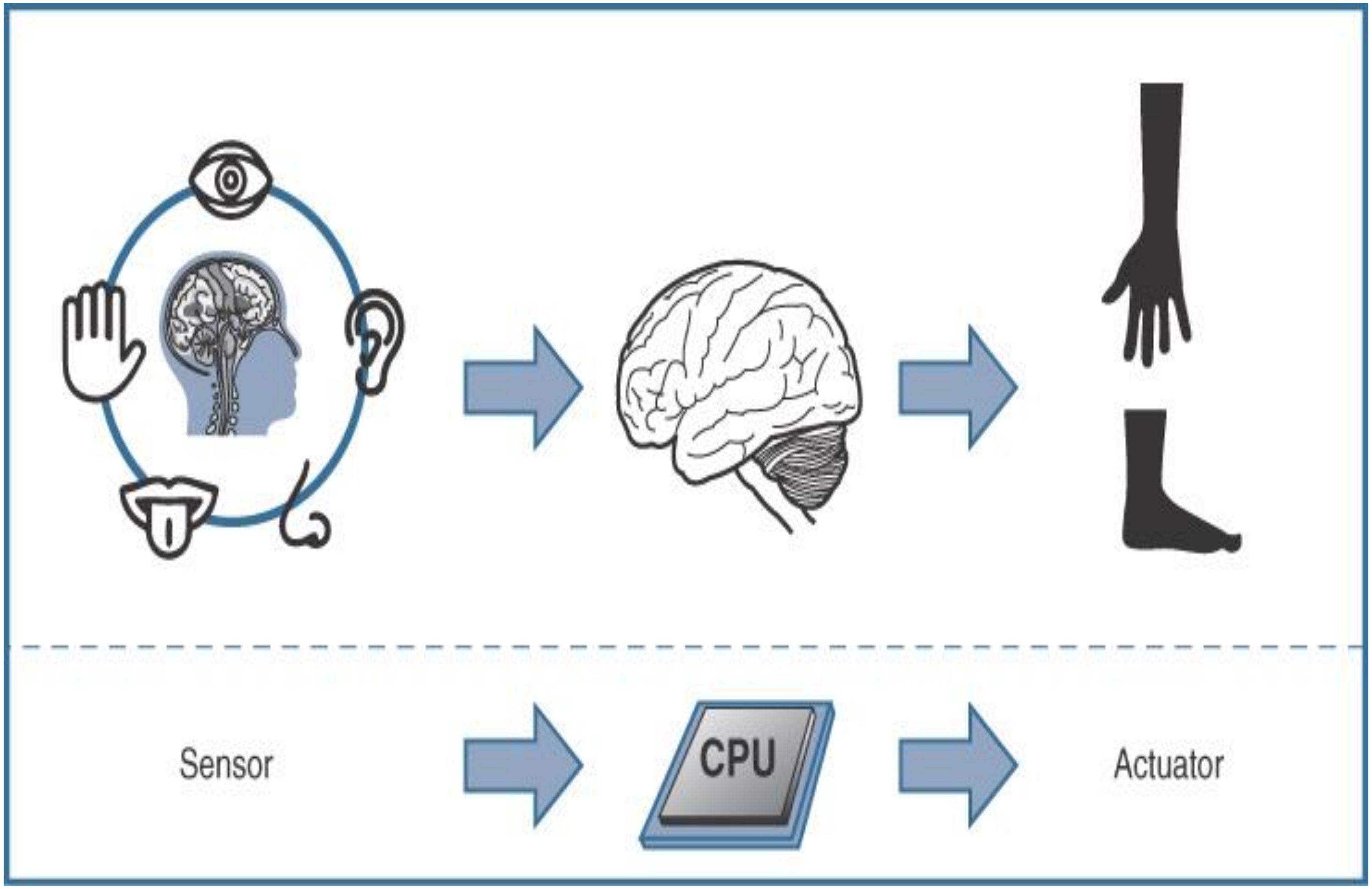
Real World –
Physical Environment

Digital Representation –
Electric Signal

Actuators

Useful
Work

Act



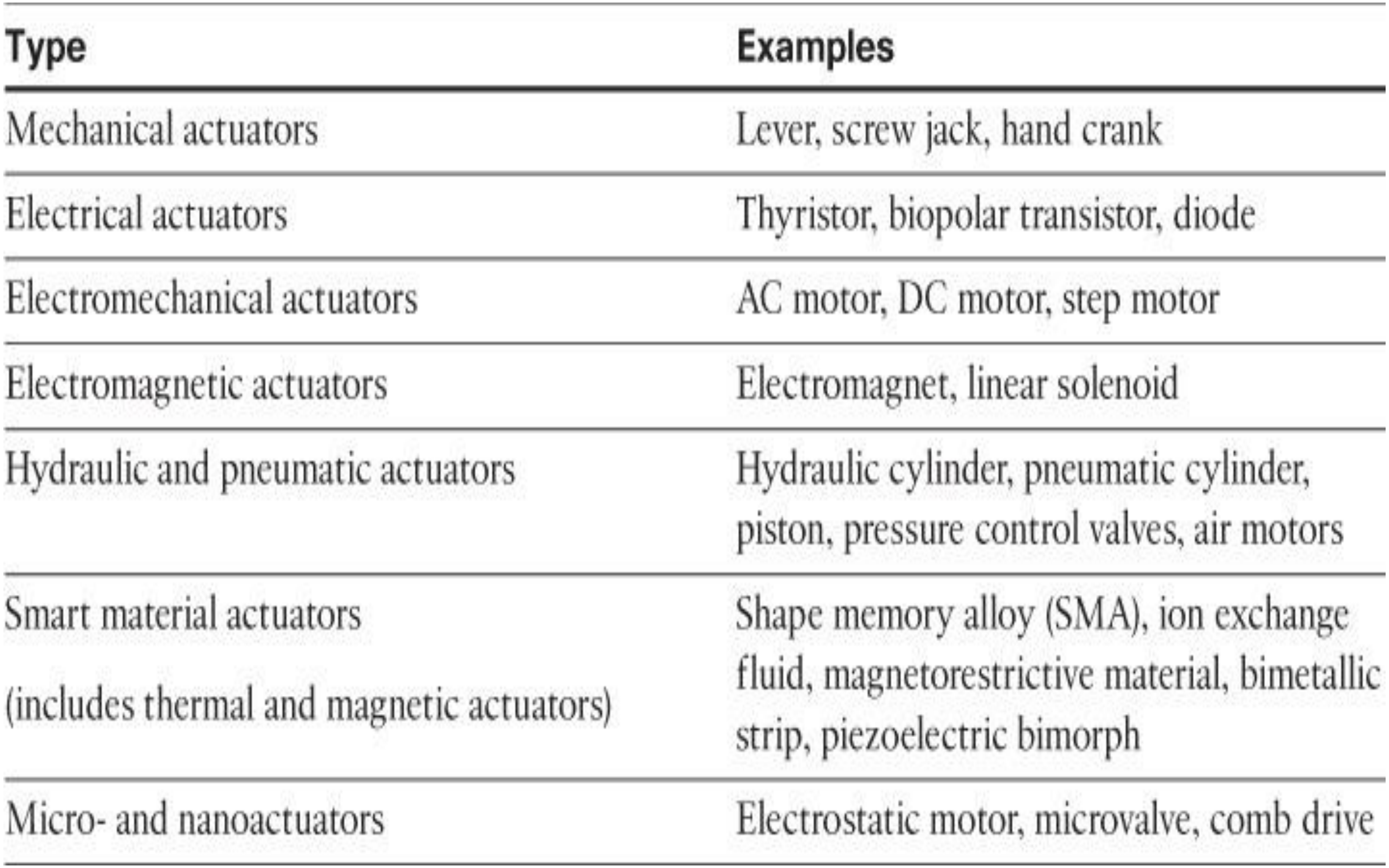
Sensor

CPU

Actuator

- Actuators also vary greatly in function, size, design, and so on.
- Some common ways that they can be classified include the following:
- **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.

Classification based on energy type



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

Micro-Electro-Mechanical Systems (MEMS)

- Interesting advances in sensor and actuator technologies is in **how they are packaged and deployed**.

- Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can i*ntegrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale.*

- 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 mass produce makes MEMS an attractive option for a huge number of IoT applications.
- MEMS devices have already been widely used in a **variety of different applications** and can be found in very familiar everyday devices.
- For example**,** ***inkjet printers*** *use micropump MEMS.*
- **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.

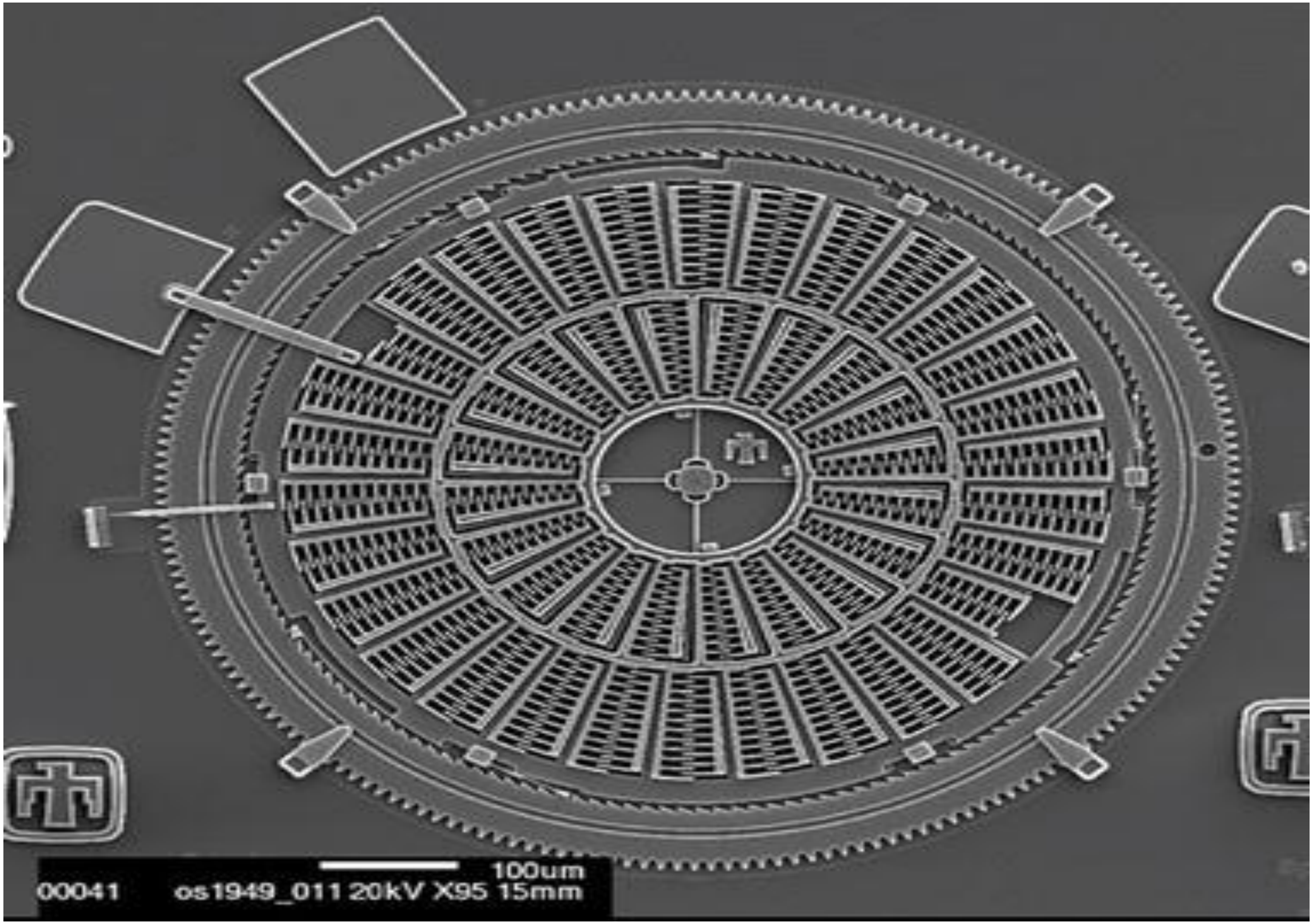


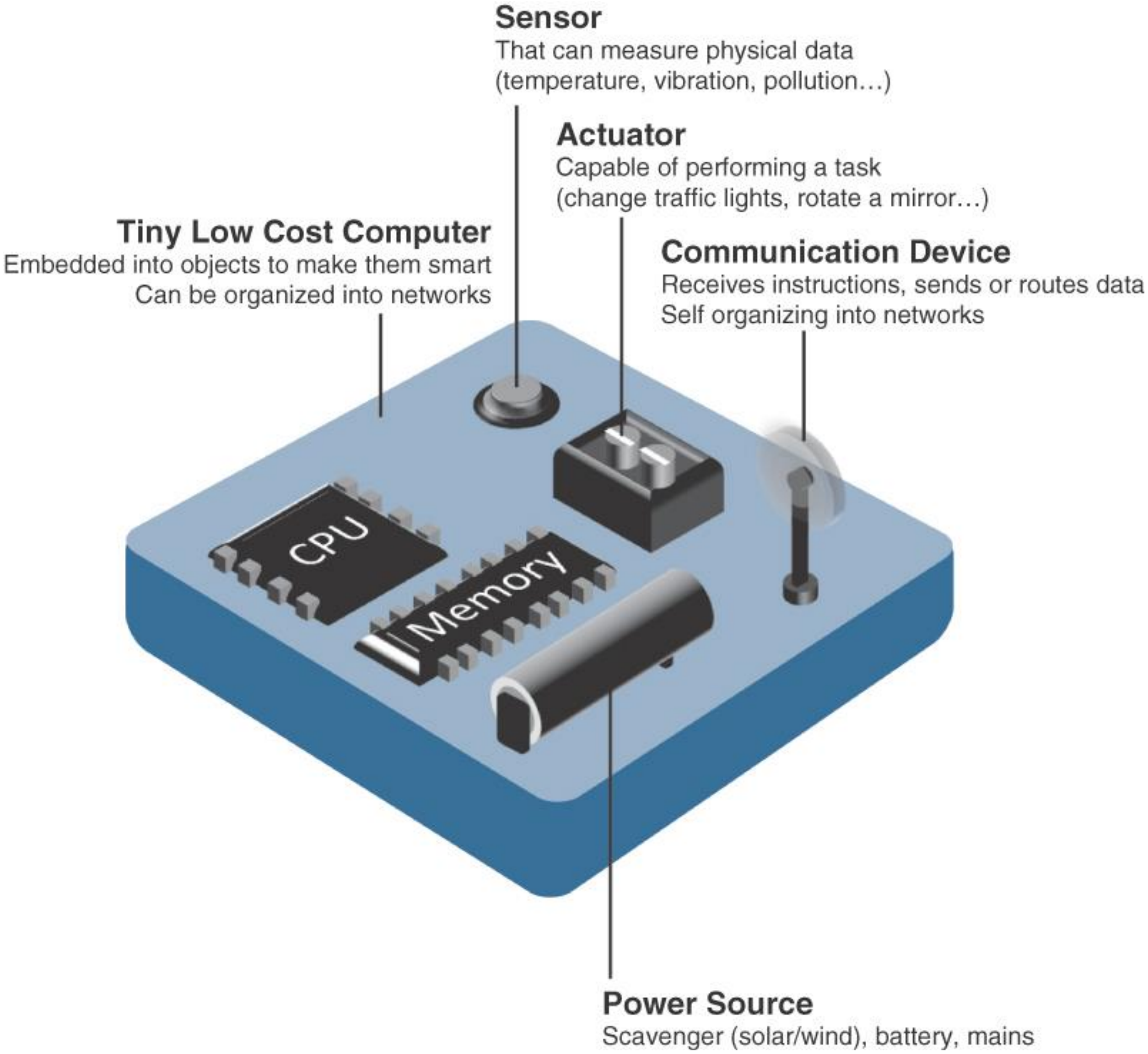
Figure 3-6 *Torsional Ratcheting Actuator (TRA) MEMS (Courtesy Sandia National Laboratories, SUMMiT™ Technologies, www.sandia.gov/mstc.)*

Smart Objects

- Smart objects are, quite simply, the building blocks of IoT.
- **They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way**
- The real power of smart objects in IoT comes from being networked together rather than being isolated as standalone objects

- If a sensor is a **standalone device** that simply measures the **humidity of the soil**, it is interesting and useful, but it isn't revolutionary
- If that **same sensor is connected as part of an intelligent network** that is **able to coordinate intelligently with actuators** to **trigger irrigation systems** as needed based on those **sensor readings**, we have something far more powerful
- Extending that even further, imagine that the **coordinated sensor/actuator set is intelligently interconnected with other sensor/actuator sets** to further coordinate ***fertilization, pest control, and so on—and even communicate with an intelligent backend to calculate crop yield potential***

- A *smart object*, is a device that has, at a minimum, the following four defining characteristics



Sensor
That can measure physical data
(temperature, vibration, pollution…)

Actuator
Capable of performing a task
(change traffic lights, rotate a mirror…)

Tiny Low Cost Computer
Embedded into objects to make them smart
Can be organized into networks

Communication Device
Receives instructions, sends or routes data
Self organizing into networks

Power Source
Scavenger (solar/wind), battery, mains

- **Processing unit:**
- Some type of processing unit for
- **Acquiring data,**
- **Processing and analyzing sensing information received by the sensor(s),**
- **Coordinating control signals to any actuators**, and
- **Controlling a variety of functions on the smart object,** including the communication and power systems
- The most common is a **microcontroller** because of its small form factor, flexibility, programming simplicity, ubiquity, low power consumption, and low cost

- **Sensor(s) and/or actuator(s):**
- A smart object is capable of interacting with the physical world through sensors and actuators
- **Communication device:**
- The communication unit is responsible for **connecting a smart object with other smart objects and the outside world (via the network).**
- Communication devices for smart objects can be either ***wired or wireless***

- **Power source:**
- Smart objects have ***components that need to be powered***.
- The most significant power consumption usually comes from the ***communication unit of a smart object***

Trends in Smart Objects

- Size is decreasing
- Power consumption is decreasing
- Processing power is increasing
- Communication capabilities are improving
- Communication is being increasingly standardized

SENSOR NETWORKS

- A sensor/actuator network **(SANET),** is a **network of sensors that sense and measure their environment and/or actuators that act on their environment**

- The sensors and/or actuators in a SANET are ***capable of communicating and cooperating***

- ***Effective and well-coordinated communication and cooperation*** is a **prominent challenge**, primarily because the sensors and actuators in SANETs are diverse, heterogeneous, and resource-constrained

- SANETs offer highly coordinated sensing and actuation capabilities.
- **Smart homes** are a type of SANET that ***display this coordination between distributed sensors and actuators***

- For example, smart homes can have **temperature sensors** that are strategically networked with **heating, ventilation, and air-conditioning (HVAC) actuators.**

- **When a sensor detects a specified temperature**, ***this can trigger an actuator to take action and heat or cool the home as needed.***

- Advantages and disadvantages that a **wireless-based solution offers:**

Advantages:

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

Disadvantages:

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

Wireless Sensor Networks (WSNs)

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

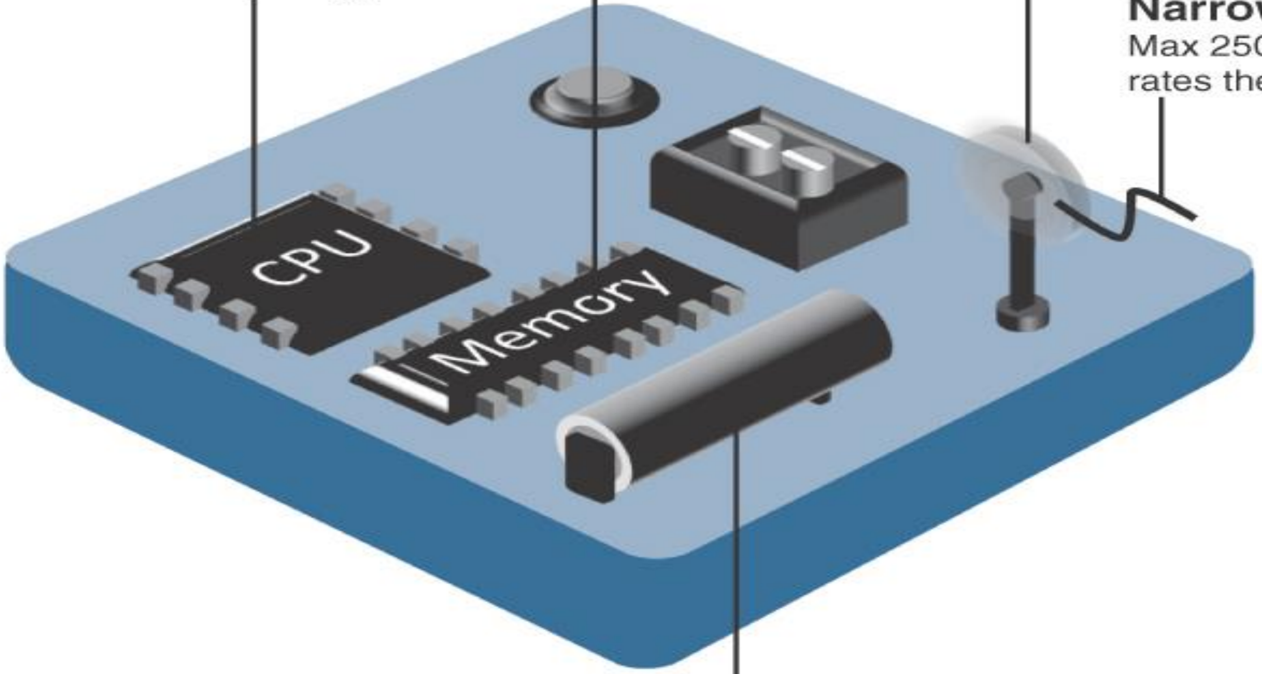
- The fact that there is no infrastructure to consider with WSNs is surely a powerful advantage for flexible deployments, but ***there are a variety of design constraints to consider with these wirelessly connected smart objects***

Low Memory
Few tens of kilobytes
Embedded OS
(TinyOS, Contiki etc…)

Lossy Communications
Low Power Wireless mesh predominantly IEEE802.15.4
Also IEEE P1902.1 (Power Line Comms)

Moderate CPU Power
Minimize energy use

Narrowband Media
Max 250KB/s, lower
rates the norm



Power Consumption Is Critical
Energy efficiency is paramount
Battery powered devices must last years

- 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

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

- These limitations greatly influence how WSNs are designed, deployed, and utilized.
- The fact that individual sensor nodes are typically so limited is a reason that they are often deployed in very large numbers.
- As the cost of sensor nodes continues to decline, the ability to deploy highly redundant sensors becomes increasingly feasible.
- Because many sensors are very inexpensive and correspondingly inaccurate, the ability to deploy smart objects redundantly allows for increased accuracy

- Such large numbers of sensors permit the introduction of **hierarchies of smart objects.**

- Such a hierarchy provides, among other organizational advantages, the ***ability to aggregate similar sensor readings from sensor nodes that are in close proximity to each other***

- . Figure 3-9 shows an example of such a data aggregation function in a WSN where ***temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.***

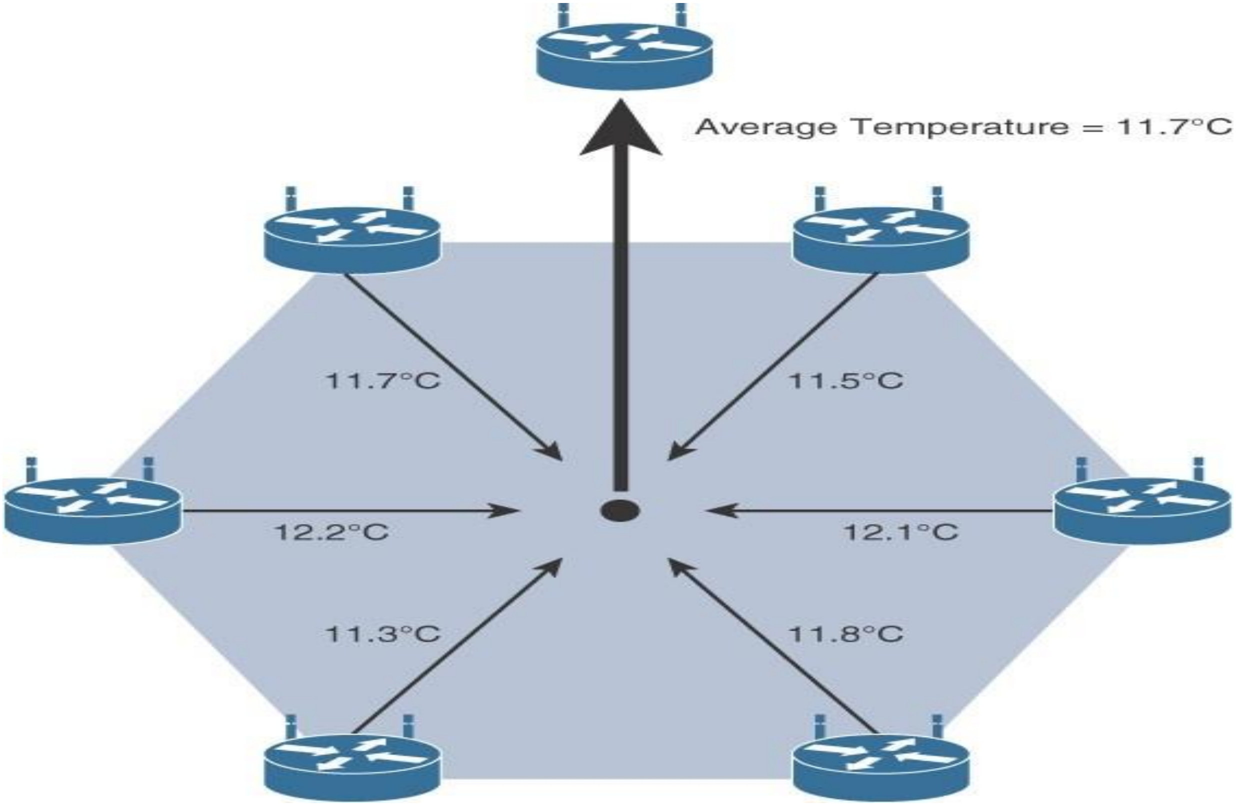


Figure 3-9 *Data Aggregation in Wireless Sensor Networks*

- These data aggregation techniques are ***helpful in reducing the amount of overall traffic (and energy) in WSNs*** with very large numbers of deployed smart objects.

- This data aggregation at ***the network edges is where fog and mist computing*** are critical IoT architectural elements needed to deliver the scale and performance required by so many IoT use cases

- **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.***

  - The decision of which of these communication schemes is used depends greatly on the specific application
  - ***For example: medical use cases***

- For example, in some **medical use cases,** ***sensors periodically send postoperative vitals, such as temperature or blood pressure readings***. In other medical use cases, ***the same blood pressure or temperature readings are triggered to be sent only when certain critically low or high readings are measured.***

Communication Protocols for Wireless Sensor Networks

- There are literally thousands of different types of sensors and actuators.
- WSNs are becoming increasingly heterogeneous, with more sophisticated interactions.

- **Any communication protocol must be able to scale to a large number of nodes.**

- Likewise, **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***

- They must also enable, as needed, the overlay **of autonomous techniques** (for example, self-organization, self-healing, self-configuration)

- 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***

- **standardization of communication protocols is a complicated task.**

- **While there isn’t a single protocol solution, there is beginning to be some clear market convergence around several key communication protocols.**

Connecting Smart Objects

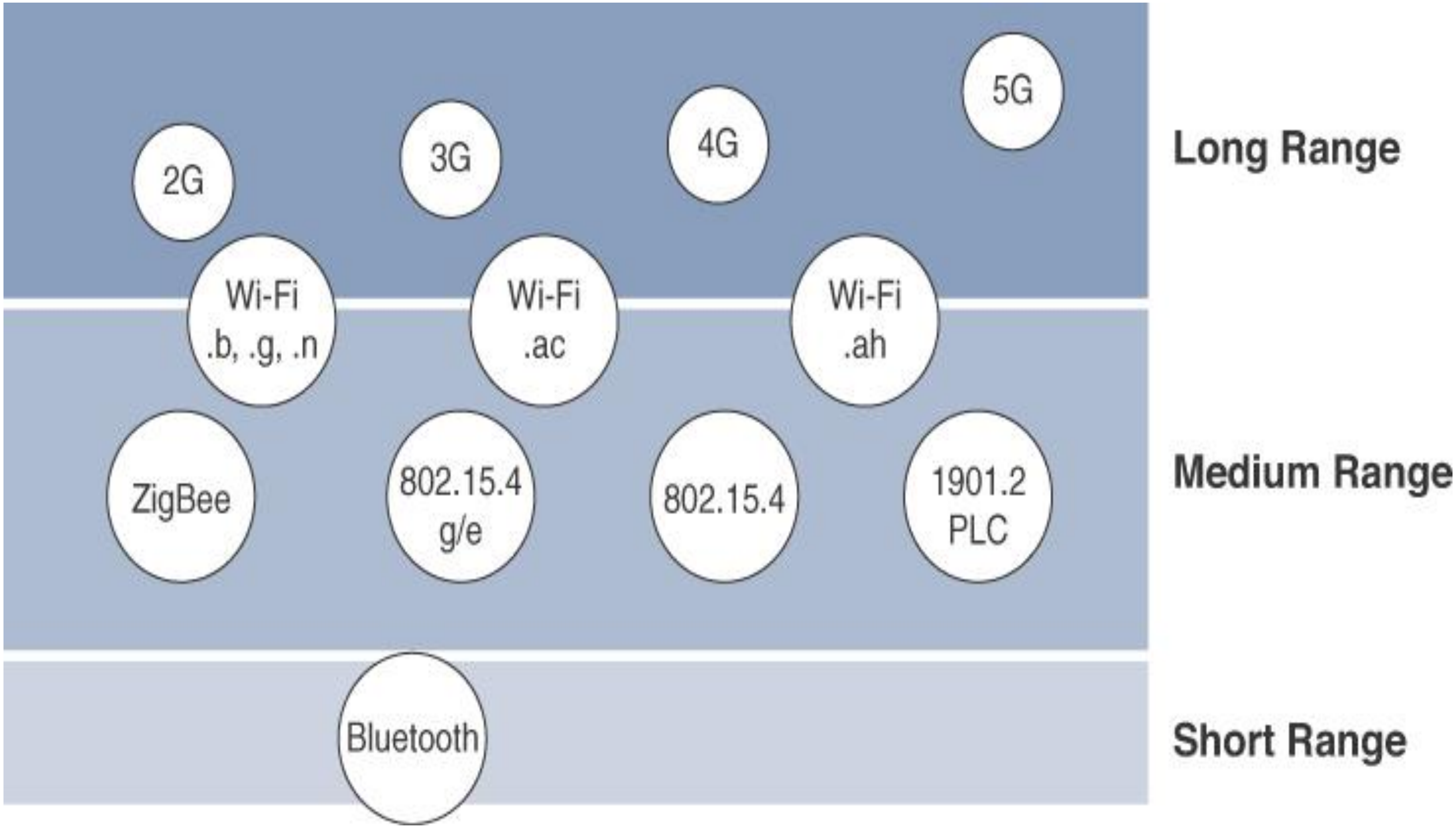
- IoT devices and sensors must be connected to the network for their data to be utilized.

- In addition to the wide range of sensors, actuators, and smart objects that make up IoT, there are also a number of different protocols used to connect them

COMMUNICATIONS CRITERIA

- *The characteristics and attributes you should consider when selecting and dealing with connecting smart objects*
- **Range**
- **Frequency Bands:**
- **Power Consumption:**
- **Topology**
- **Constrained Devices:**
- **Constrained-Node Networks:**

- **Range**
- How far does the signal need to be propagated?
- That is, what will be the area of coverage for a selected wireless technology?
- Should indoor versus outdoor deployments be differentiated?


5G
4G
3G
2G
Long Range
Wi-Fi .b, .g, .n
Wi-Fi .ac
Wi-Fi .ah
ZigBee
802.15.4 g/e
802.15.4
1901.2 PLC
Medium Range
Bluetooth
Short Range

- **Short range:**
- The classical wired example is a serial cable.

- Wireless short-range technologies are often considered as an alternative to a serial cable, supporting **tens of meters of** maximum distance between two devices.

- Examples of short-range wireless technologies are **IEEE 802.15.1 Bluetooth** and **IEEE 802.15.7 Visible Light Communications (VLC)**

- **Medium range:**
- This range is the ***main category*** of IoT access technologies.
- In the range of **tens to hundreds of meters,** many specifications and implementations are available.
- The **maximum distance** is generally ***less than 1 mile between two devices***
- 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)

- **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**
- **Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).**
- **These groups define the regulations and transmission requirements for various frequency bands**
- For example, **portions of the spectrum** are ***allocated to types of telecommunications such as radio, television, military, and so on.***

- Focusing on IoT access technologies, the frequency bands leveraged by **wireless communications are split between licensed and unlicensed bands.**
- ***Licensed spectrum is generally applicable to IoT long-range access technologies***
- In order to utilize licensed spectrum***, users must subscribe to services when connecting their IoT devices***
- In exchange for the subscription fee, the network operator can guarantee the exclusivity of the frequency usage over the target area and can therefore sell a better guarantee of service.

- The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands.
- These frequencies are used in many communications **technologies for short-range devices (SRDs).**
- ***Unlicensed means* that no guarantees or protections are offered in the ISM bands for device communications**
- **ISM bands for IoT access**
- 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
- IEEE 802.15.1 Bluetooth
- IEEE 802.15.4 WPAN

- Unlicensed spectrum is usually simpler to deploy than licensed because it does not require a service provider.
- However, it can suffer from more interference because other devices may be competing for the same frequency in a specific area
- The frequency of transmission directly impacts how a signal propagates and its practical maximum range.

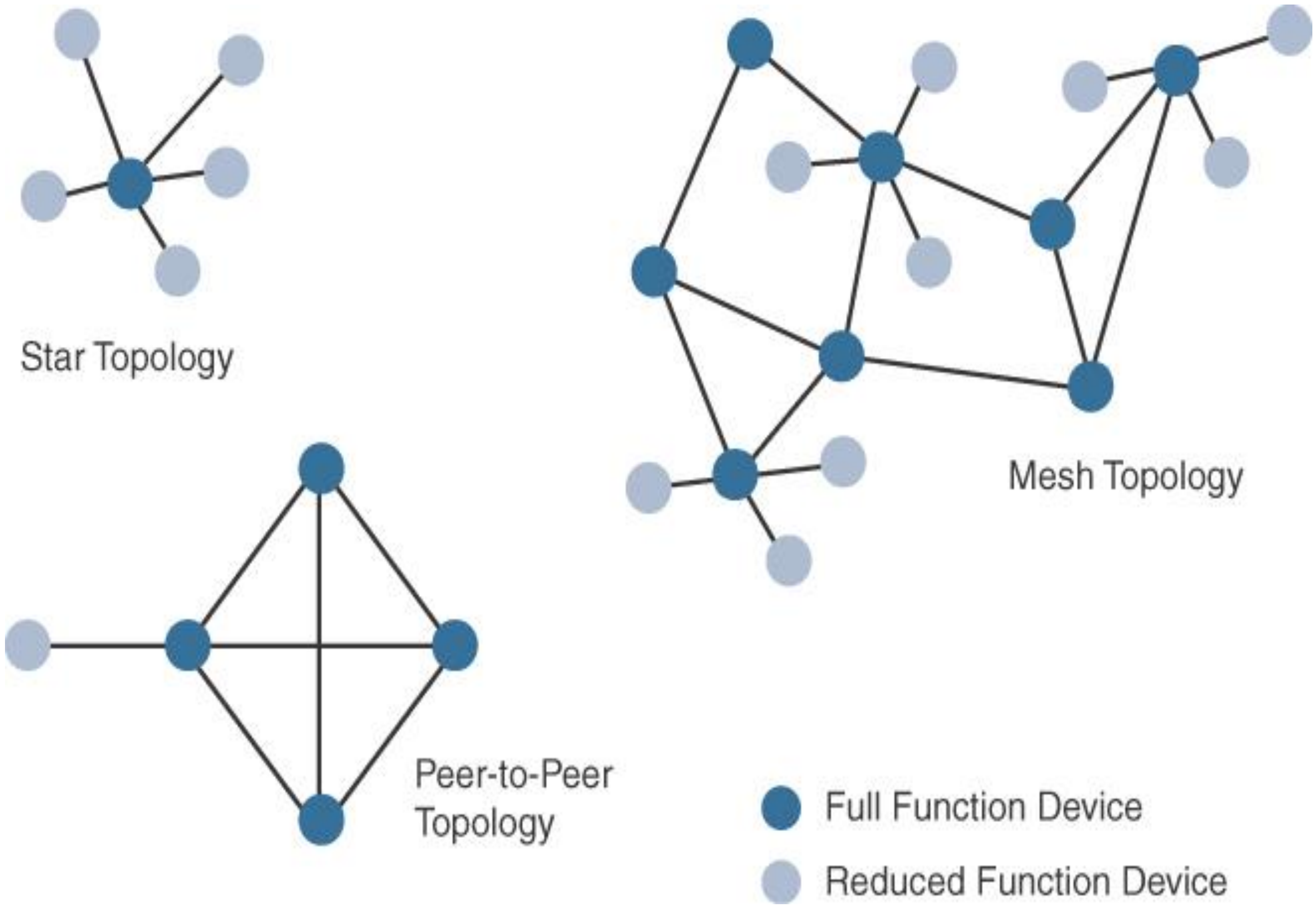
Power Consumption

- Powered nodes and battery-powered nodes
- **A powered node has a direct connection to a power source**, and **communications are usually not limited by power consumption criteria.**
- However, ease of **deployment of powered nodes is limited by the availability of a power source,** which makes **mobility more complex**
- **Battery-powered nodes bring much more flexibility to IoT devices.**
- These nodes are often ***classified by the required lifetimes of their batteries.***

- ***For battery-powered nodes, IoT wireless access technologies must address the needs of low power consumption and connectivity***
- A new wireless environment known as **Low-Power Wide-Area (LPWA)**
- Battery-powered nodes are often placed in a **"sleep mode" to preserve battery life when not transmitting**
- Wired IoT access technologies consisting of powered nodes are not exempt from power optimization

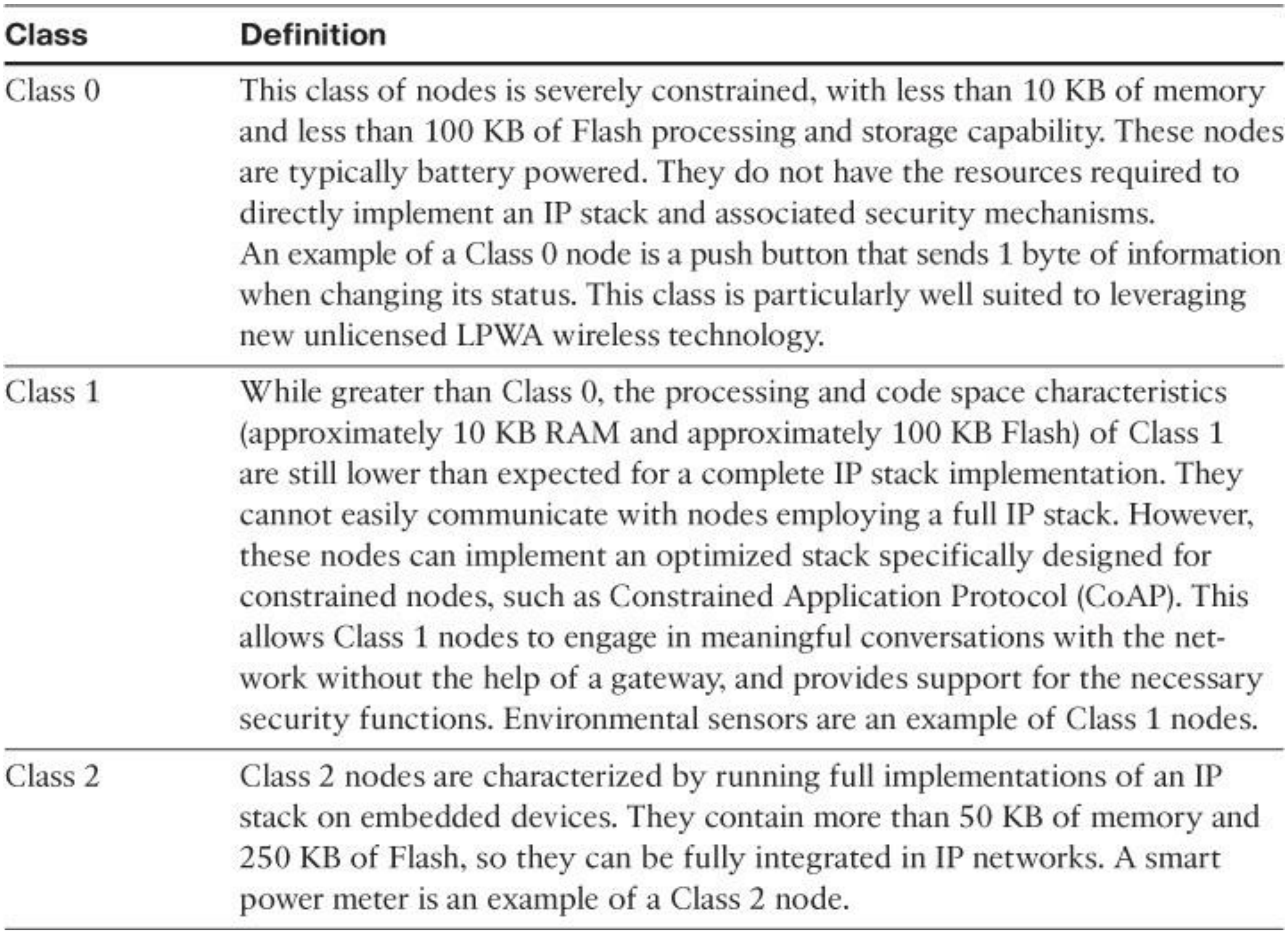
Topology

- Among the access technologies available for connecting IoT devices, three main topology schemes are dominant**: star, mesh, and peer-to-peer**
- For long-range and short-range technologies, **a star topology** is prevalent
- Star topologies utilize a single central base station or controller to allow communications with endpoints
- For medium-range technologies, **a star, peer-to-peer, or mesh topology is common**
- Peer-to-peer topologies **allow any device to communicate with any other device as long as they are in range of each other**



Ex: Indoor Wi-Fi deployments and Outdoor Wi-Fi deployments

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.

Constrained-Node Networks

- IEEE 802.15.4 and 802.15.4g RF, IEEE 1901.2a PLC, LPWA, and IEEE 802.11ah access technologies
- Constrained-node networks **are often referred to as low-power and lossy networks (LLNs).**
- **Low power** – **battery powered constraints**
- **Lossy network** -- **network performance may suffer from interference and variability due to harsh radio environments**
- Protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics: ***data rate and throughput***, ***latency*** and ***determinism***, and ***overhead and payload.***

Data Rate and Throughput

- The data rates available from IoT access technologies range from **100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac**
- However, the ***actual throughput is less***
- Therefore, understanding the bandwidth requirements of a particular technology, its applicability to given use cases, the capacity planning rules, and the expected real throughput are important for proper network design and successful production deployment

- Technologies not particularly designed for IoT, such as cellular and Wi-Fi, match up well to IoT applications with high bandwidth requirements
- For example, nodes involved with video analytics have a need for high data rates, IoT endpoints are not constrained in terms of computing or network bandwidth, the design guidelines tend to focus on application requirements, such as latency and determinism

- Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints.
- For example, Bluetooth sensors that are now appearing on connected wearables fall into this category.
- In this case, the solutions focus more on footprint and battery lifetime than on data rate.
- The IoT access technologies developed for constrained nodes are optimized for low power consumption, but they are also limited in terms of data rate

- Another characteristic of IoT devices is that a majority of them initiate the communication.
- Upstream traffic toward an application server is usually more common than downstream traffic from the application server.
- Understanding this behavior also helps when deploying an IoT access technology, such as cellular, that is asymmetrical because the upstream bandwidth must be considered a key parameter for profiling the network capacity

Latency and Determinism

- Latency expectations of IoT applications should be known when selecting an access technology
- This is particularly true for ***wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviors***

- **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

- When considering constrained access network technologies, it is important to **review the MAC payload size characteristics required by applications**
- 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

IoT Access Technologies

- **The following topics are addressed for each IoT access technology:**

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

IoT Access Technologies

- IEEE 802.15.4
- IEEE 802.15.4g and 802.15.4e
- IEEE 1901.2a
- IEEE 802.11ah
- LoRaWAN
- NB-IoT and other LTE Variations

IEEE 802.15.4

- Wireless access technology for **low-cost and low-data-rate devices that are powered or run on batteries**

- This access technology enables **easy installation while remaining both simple and flexible**

- IEEE 802.15.4 is commonly **found in the following types of deployments:**
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls

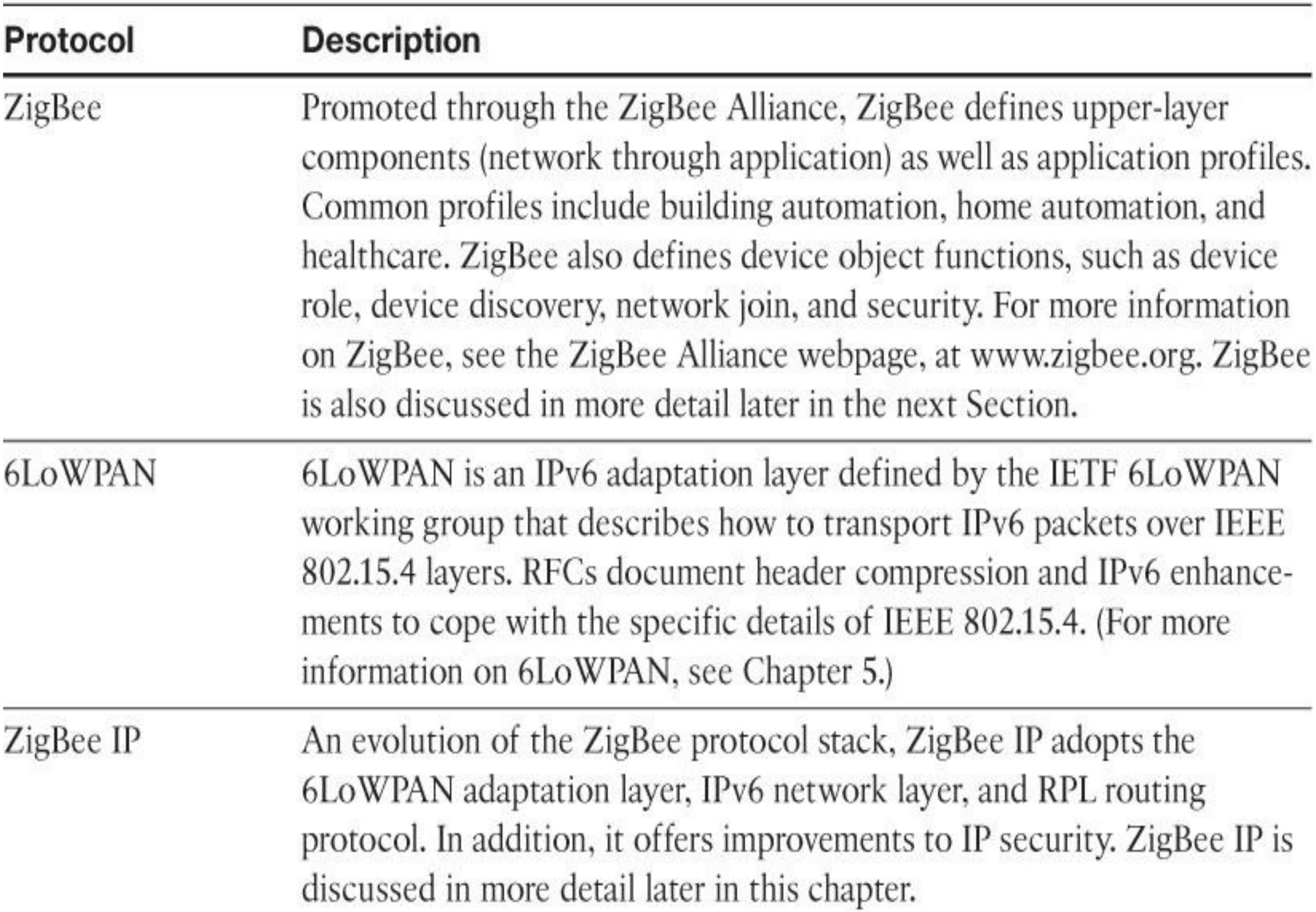
- **Drawbacks** of this includes *MAC reliability*, *unbounded latency,* and *susceptibility to interference and multipath fading*
- The negatives around reliability and latency often have to do with the Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm.
- CSMA/CA is an access method 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

Standardization and Alliances

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

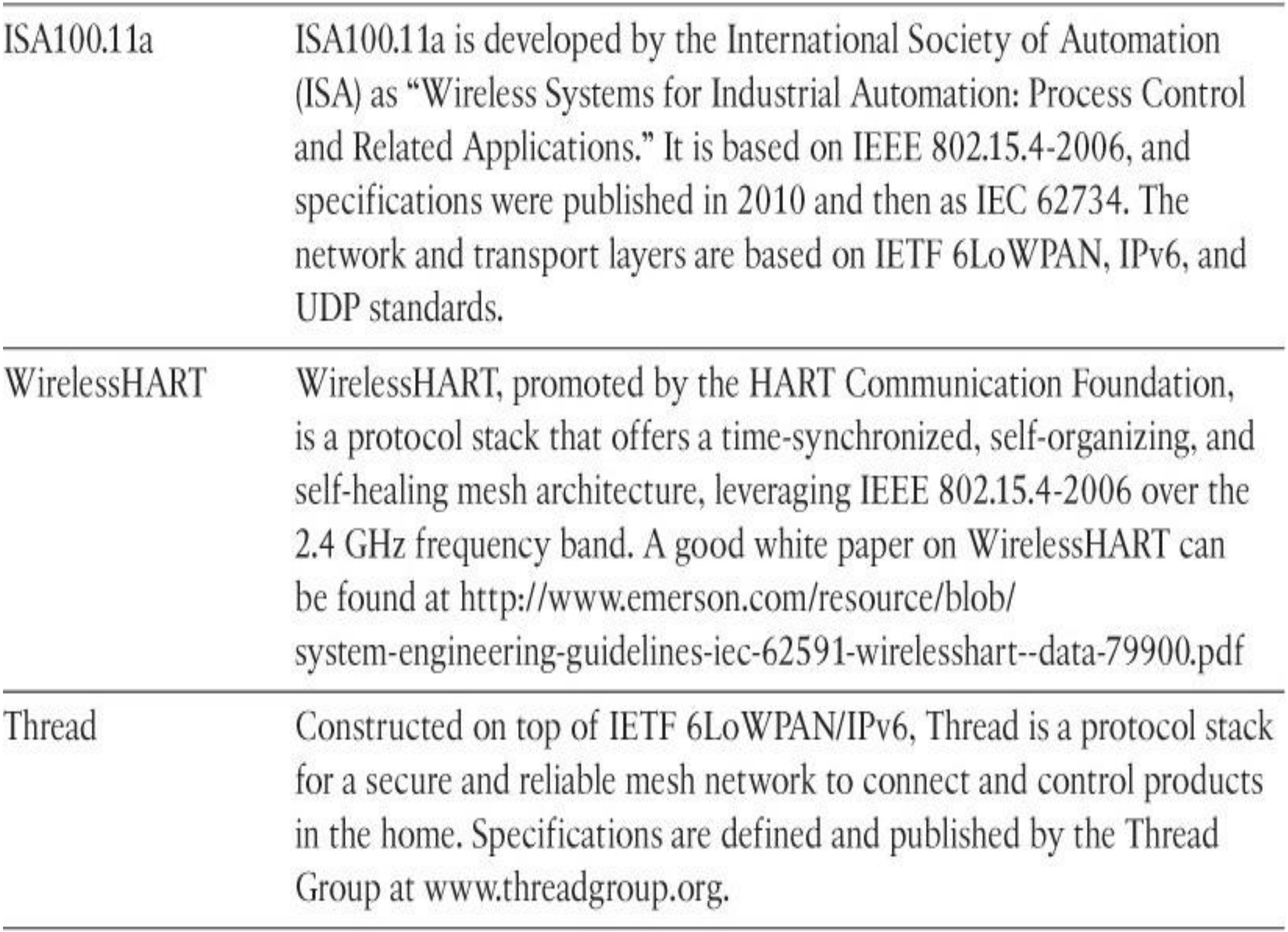
- This is a **well-known solution** for *low complexity* ***wireless devices with low data rates that need many months or even years of battery life.***

- IEEE 802.15.4-2003 , 802.15.4-2006 , 802.15.4-2011 and 802.15.4-2015



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.

Protocol Stacks Utilizing IEEE 802.15.4



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

- 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***

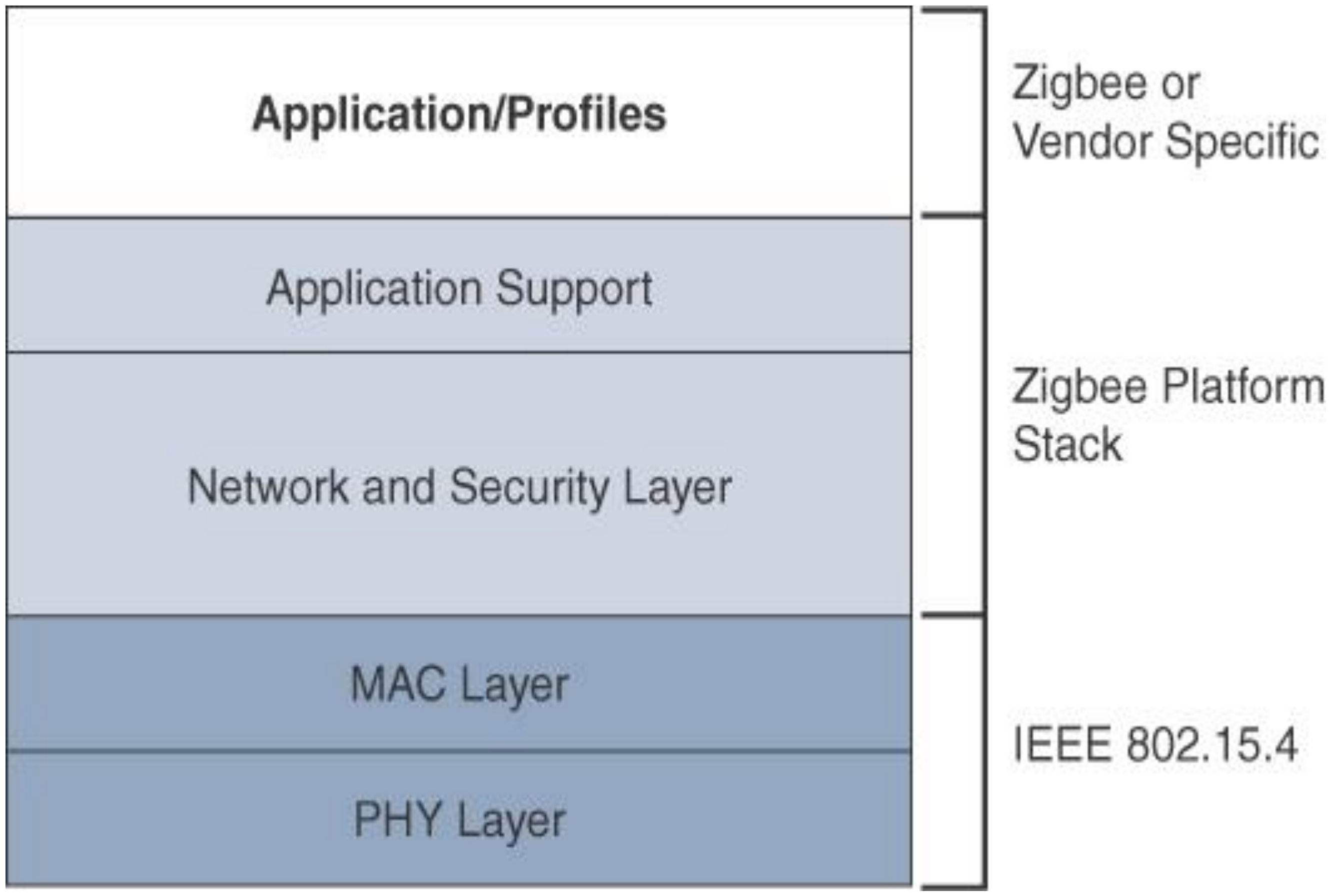
- The Zigbee specification has undergone several revisions.
- In the 2006 revision, sets of commands and message types were introduced, and increased in number in the 2007 (called Zigbee pro) iteration, to achieve different functions for a device, such as metering, temperature, or lighting control

- 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, **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***

The traditional ZigBee 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.**

- **ZigBee uses Ad hoc On-Demand Distance Vector (AODV) routing *across a mesh network*.**
- Interestingly, this routing algorithm does not send a message until a route is needed.
- Assuming that the next hop for a route is not in its routing table, a network node broadcasts a request for a routing connection.
- This causes a burst of routing related traffic, but after a comparison of various responses, the path with the lowest number of hops is determined for the connection.

- **The application support layer** *interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.*

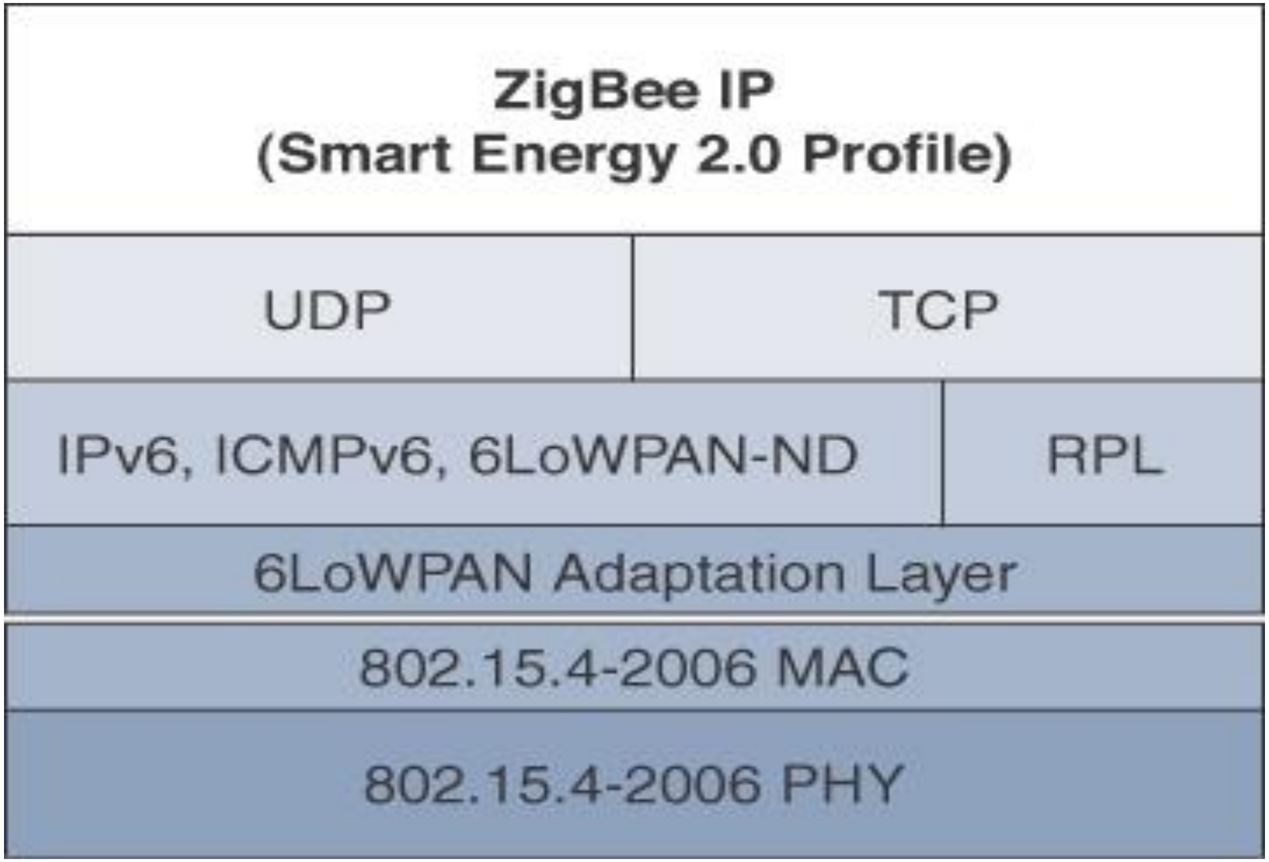
- **ZigBee predefines many application profiles** for certain industries, and vendors can optionally create their own custom ones at this layer.

- As mentioned previously, ***Home Automation and Smart Energy are two examples of popular application profiles.***

ZigBee IP

- With the introduction of ZigBee IP, the support of IEEE 802.15.4 continues, but the IP and TCP/UDP protocols and various other open standards are now supported at the network and transport layers.
- The ZigBee-specific layers are now found only at the top of the protocol stack for the applications

The ZigBee IP stack



ZigBee IP
(Smart Energy 2.0 Profile)

UDP

TCP

IPv6, ICMPv6, 6LoWPAN-ND

RPL

6LoWPAN Adaptation Layer

802.15.4-2006 MAC

802.15.4-2006 PHY

- ZigBee IP supports 6LoWPAN as an adaptation layer.
- The 6LoWPAN mesh addressing header is not required as ZigBee IP utilizes the mesh-over or route-over method for forwarding packets.
- ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes.
- At the network layer, all ZigBee IP nodes support IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND), and utilize RPL for the routing of packets across the mesh network.
- Both TCP and UDP are also supported, to provide both connection-oriented and connectionless service.

Physical Layer

- The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands
- The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation.
- DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth.

Modulation

- In the modulation process, some parameter of the carrier wave (such as amplitude, frequency or phase) is varied in accordance with the modulating signal . This modulated signal is then transmitted by the transmitter
- In the modulation process, two signals are used namely the modulating signal and the carrier
- The modulating signal is nothing but the baseband signal or information signal while the carrier is a high frequency sinusoidal signal

- **Advantages of Modulation**
- Reduction in the height of antenna
- Avoids mixing of signals
- Increases the range of communication
- Multiplexing is possible
- Improves quality of reception

- For the transmission of radio signals, the antenna height must be multiple of λ/4 ,where λ is the wavelength .
- $\lambda = c / f$
- where c : is the velocity of light
- f: is the frequency of the signal to be transmitted
- The minimum antenna height required to transmit a baseband signal of f = 10 kHz is calculated as follows :

$$\textit{Minimum antenna height} = \frac{\lambda}{4} = \frac{c}{4f} = \frac{3 \times 10^{8}}{4 \times 10 \times 10^{3}} = 7500 \textit{ meters i.e.} 7.5 \textit{ km}$$

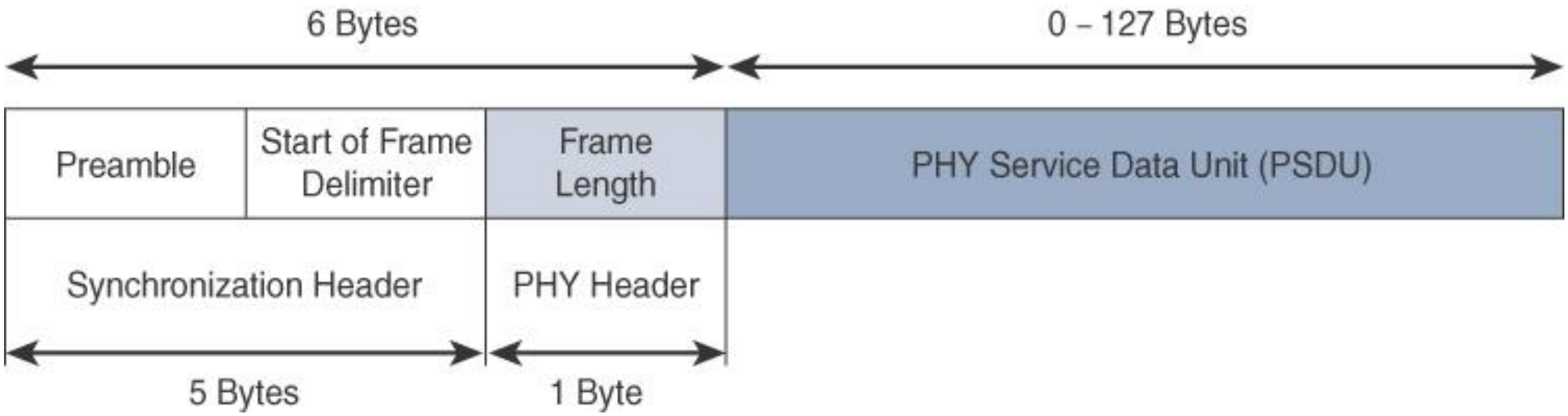
- The original physical layer transmission options were as follows:
- 2.4 GHz, 16 channels, with a data rate of 250 kbps
- 915 MHz, 10 channels, with a data rate of 40 kbps
- 868 MHz, 1 channel, with a data rate of 20 kbps
- IEEE 802.15.4-2006, 802.15.4- 2011, and IEEE 802.15.4-2015 introduced additional 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 signalled by phase changes.
- An offset function that is present during phase shifts allows data to be transmitted more reliably.

- **BPSK PHY:**
- This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation.
- BPSK specifies two unique phase shifts as its data encoding scheme.

- **ASK PHY:**
- This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation.
- PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS.
- ASK uses amplitude shifts instead of phase shifts to signal different bit values

The frame for the 802.15.4 physical layer



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

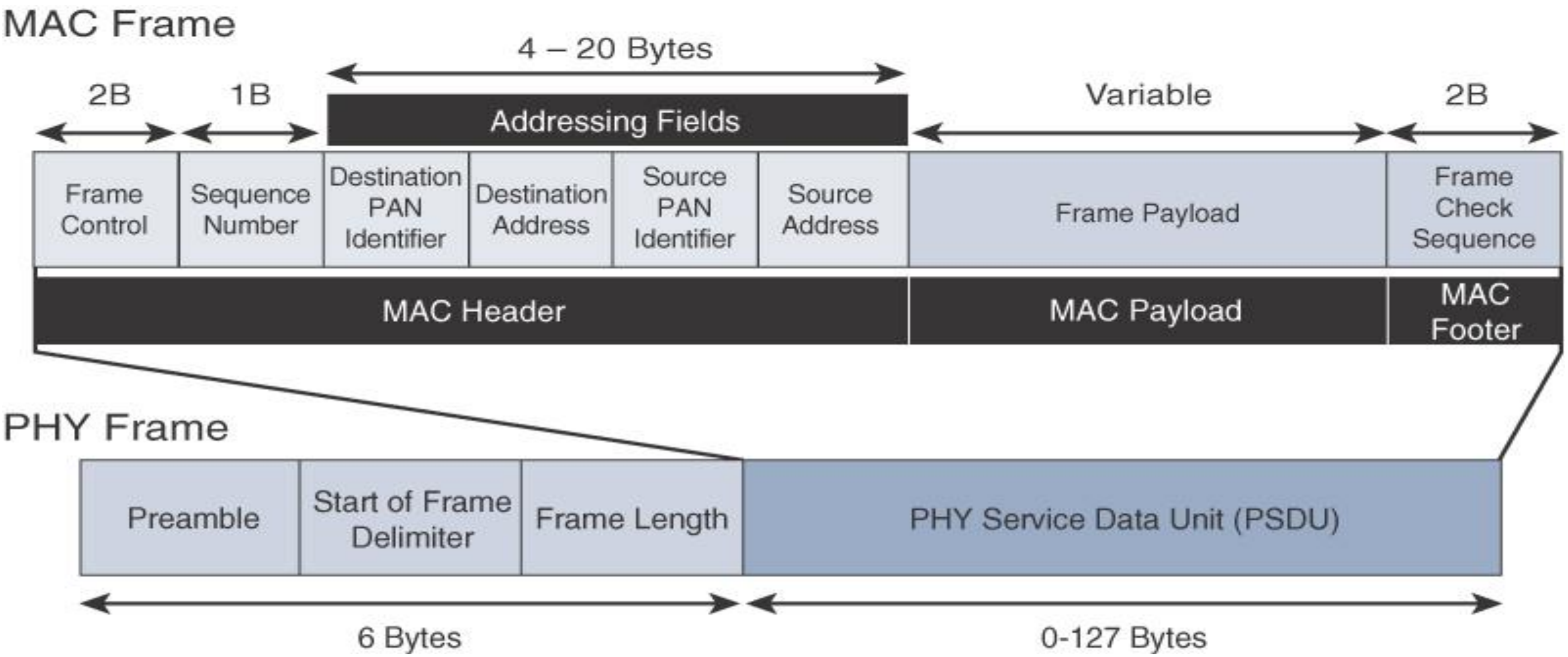
- The PHY Header portion of the PHY frame is frame length value. It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY.
- The PSDU is the data field or payload
- The maximum size of the IEEE 802.15.4 PSDU is 127 bytes. This size is significantly smaller than the lowest MTU setting of other upper-layer protocols, such as IPv6, which has a minimum MTU setting of 1280 bytes. Therefore, fragmentation of the IPv6 packet must occur at the data link layer for larger IPv6 packets to be carried over IEEE 802.15.4 frames.

MAC Layer

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

- The MAC layer achieves these tasks by using various predefined frame types
- 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

IEEE 802.15.4 MAC Format



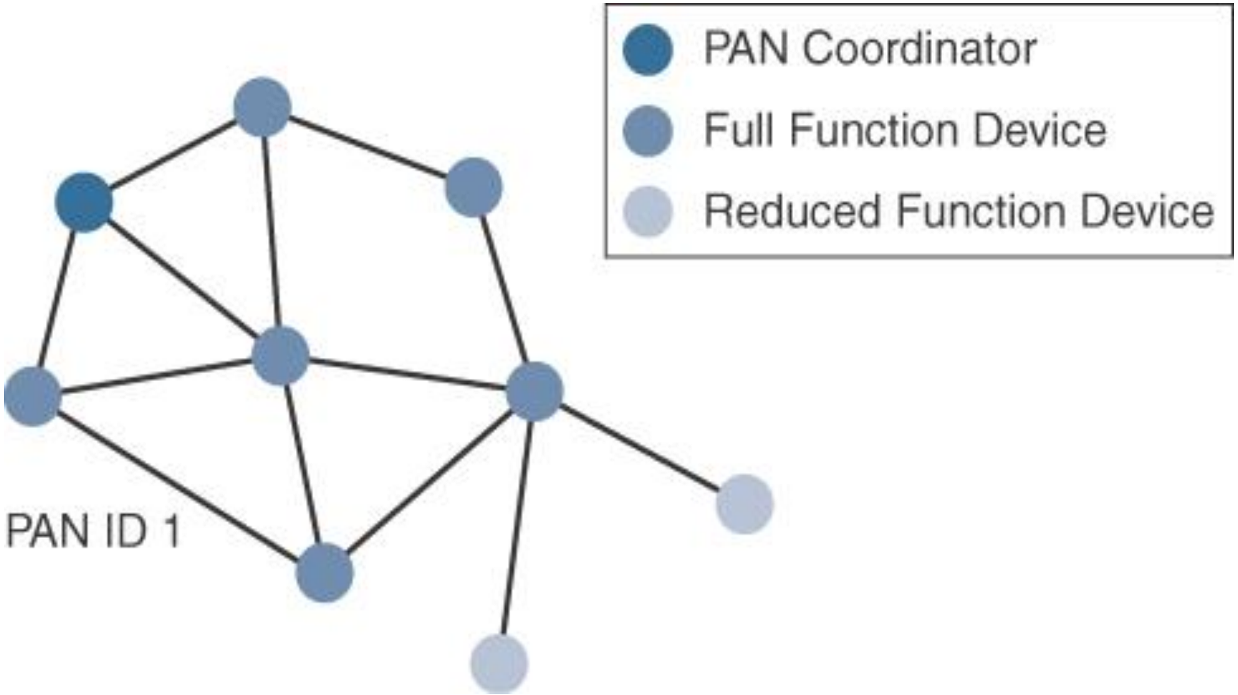
- The MAC Header field is composed of the Frame Control, Sequence Number and the Addressing fields.
- The Frame Control field defines attributes such as frame type, addressing modes, and other control flags.
- The Sequence Number field indicates the sequence identifier for the frame.
- The Addressing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

- The MAC Payload field varies by individual frame type.
- For example, beacon frames have specific fields and payloads related to beacons, while MAC command frames have different fields present.
- The MAC Footer field is nothing more than a frame check sequence (FCS).
- An FCS is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the data in the frame.

- IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address, based on EUI-64.
- However, because the maximum payload is 127 bytes, 802.15.4 also defines how a 16-bit “short address” is assigned to devices.
- This short address is local to the PAN and substantially reduces the frame overhead compared to a 64-bit extended MAC address

Topology

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


PAN Coordinator
Full Function Device
Reduced Function Device
PAN ID 1

- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN.
- A single PAN coordinator is identified for PAN ID 1.
- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

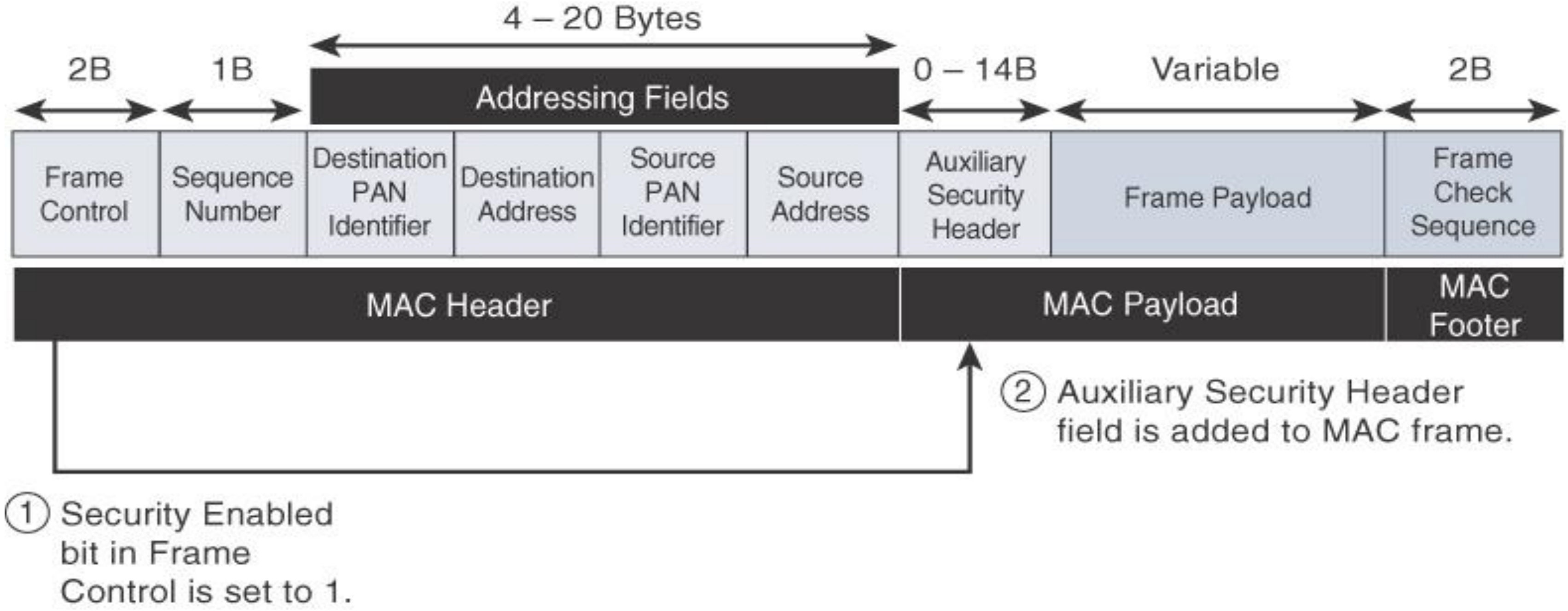
- The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology.
- This function can be done at Layer 2 and is known as *mesh-under*.
- The routing function can occur at Layer 3, using a routing protocol, such as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL).
- This is referred to as *mesh-over*

Security

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data
- AES is a block cipher, which means it operates on fixed-size blocks of data
- symmetric key - means that the same key is used for both the encryption and decryption of the data
- In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent.
- This is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption

- Using the Security Enabled field in the Frame Control portion of the 802.15.4 header is the first step to enabling AES encryption.
- This field is a single bit that is set to 1 for security.
- Once this bit is set, a field called the Auxiliary Security Header is created after the Source Address field, by stealing some bytes from the Payload field.

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



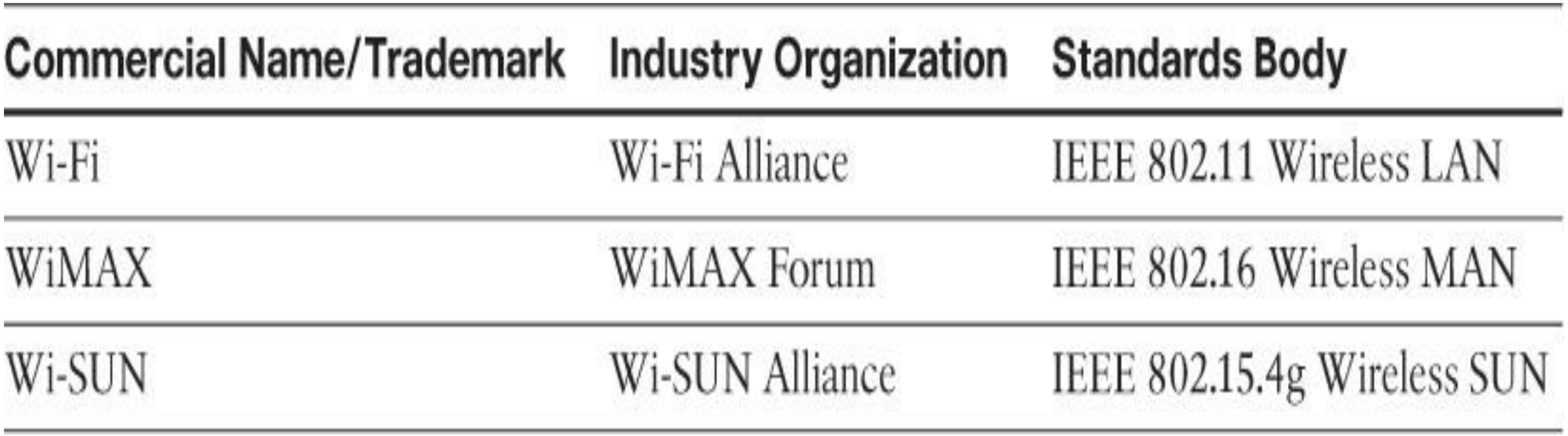
IEEE 802.15.4g and 802.15.4e

- The IEEE 802.15.4e amendment of 802.15.4-2011 expands the MAC layer feature set to remedy the disadvantages associated with 802.15.4, including MAC reliability, unbounded latency, and multipath fading
- Also made improvements to better cope with certain application domains, such as factory and process automation and smart grid
- IEEE 802.15.4e-2012 enhanced the IEEE 802.15.4 MAC layer capabilities in the areas of frame format, security, determinism mechanism, and frequency hopping

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

- 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**
- To guarantee interoperability, the Wi-SUN Alliance was formed. (SUN stands for *smart utility network*.)



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

- 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.
- For example, the default IPv6 MTU setting is 1280 bytes.
- Fragmentation is no longer necessary at Layer 2 when IPv6 packets are transmitted over IEEE 802.15.4g MAC frames.
- The error protection was improved in IEEE 802.15.4g by evolving the CRC from 16 to 32 bits

- 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
- 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 (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
- Enhanced data rates and a greater number of channels for channel hopping are available, depending on the frequency bands and modulation

MAC Layer

- **Time-Slotted Channel Hopping (TSCH):**
- It 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

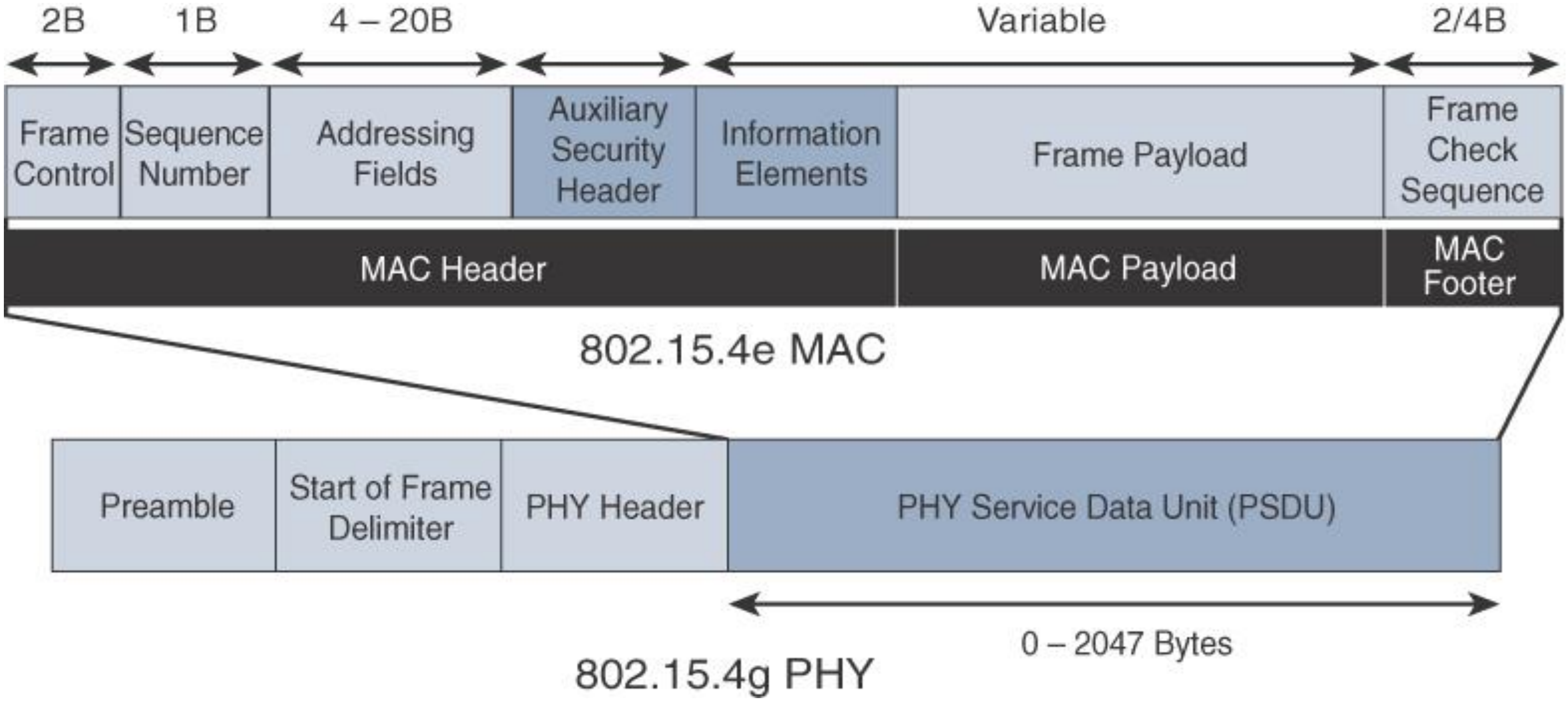
- **Information elements:**
- Information elements (IEs) allow for the exchange of information at the MAC layer in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).
- Specified in a tag, length, value (TLV) format, the IE field allows frames to carry additional metadata to support MAC layer services
- These services may include IEEE 802.15.9 key management, Wi-SUN 1.0 IEs to broadcast and unicast schedule timing information, and frequency hopping synchronization information for the 6TiSCH architecture.

- **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.

IEEE 802.15.4g/e MAC Frame Format



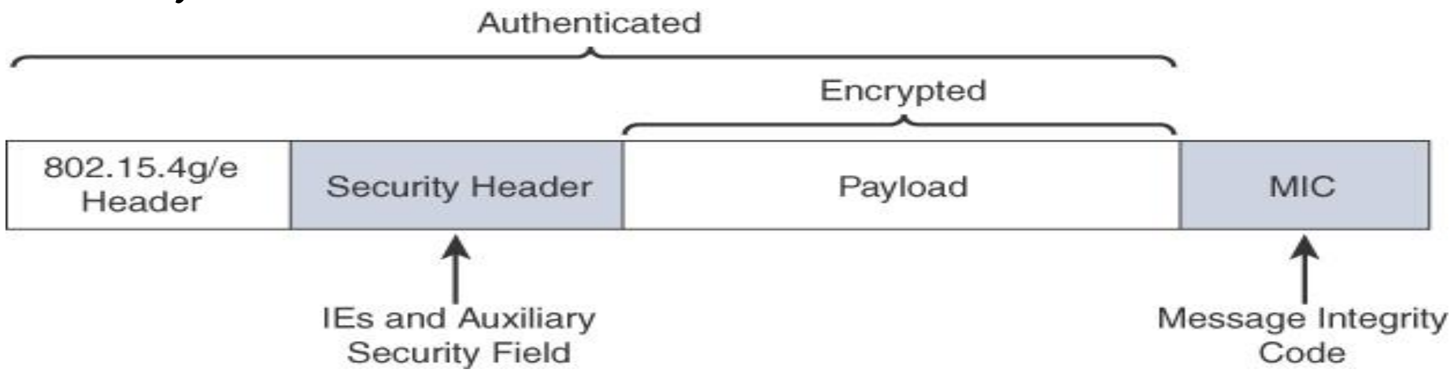
- The main changes shown in the IEEE 802.15.4e header are the presence of the Auxiliary Security Header and Information Elements field.
- The Auxiliary Security header provides for the encryption of the data frame
- The IE field contains one or more information elements that allow for additional information to be exchanged at the MAC layer.

Topology

- Deployments of IEEE 802.15.4g-2012 are mostly based on a mesh topology
- Mesh topology is typically the best choice for use cases in the industrial and smart cities areas
- 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.
- Encryption is provided by AES, with a 128-bit key.
- In addition to the Auxiliary Security Header field initially defined in 802.15.4-2006, a secure acknowledgement and a secure Enhanced Beacon field complete the MAC layer security



- The full frame gets authenticated through the MIC at the end of frame.
- The MIC is a unique value that is calculated based on the frame contents.
- The Security Header field denoted is composed of the Auxiliary Security field and one or more Information Elements fields.
- Integration of the Information Elements fields allows for the adoption of additional security capabilities, such as the IEEE 802.15.9 Key Management Protocol (KMP) specification.
- KMP provides a means for establishing keys for robust datagram security

IEEE 1901.2a

- 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.

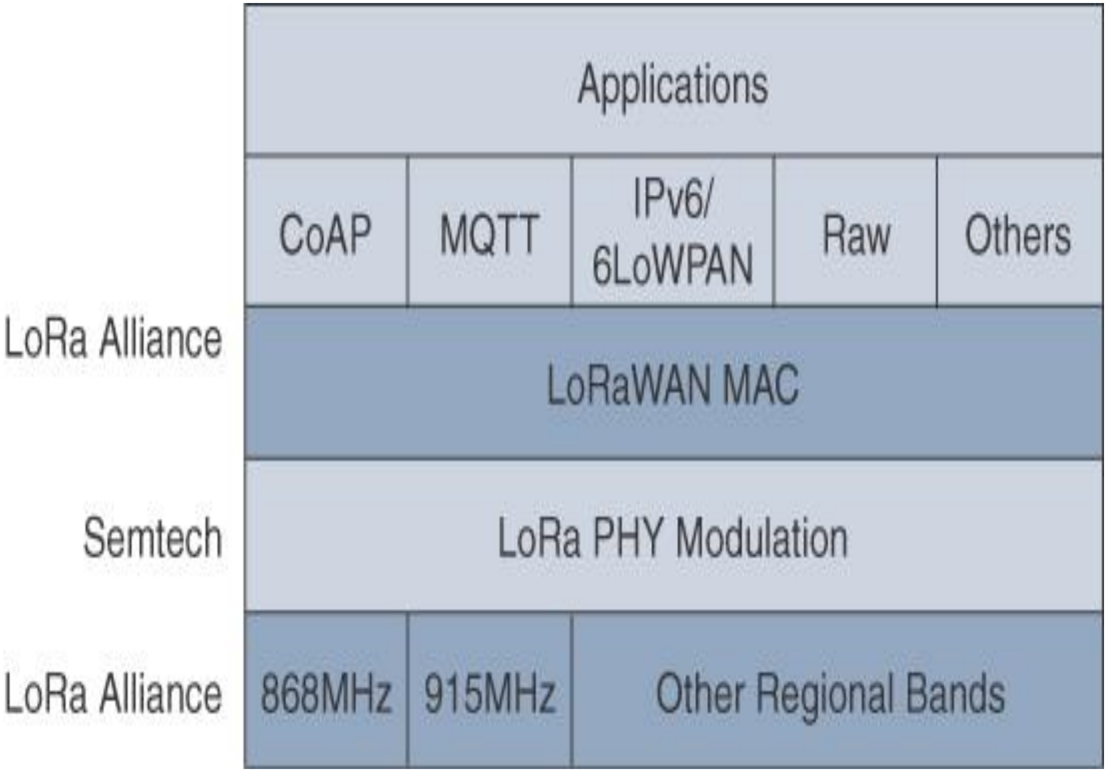
- NB-PLC is often found in use cases such as the following:
- **Smart metering:**
- NB-PLC can be used to automate the reading of utility meters, such as electric, gas, and water meters
- **Distribution automation:**
- NB-PLC can be used for distribution automation, which involves monitoring and controlling all the devices in the power grid.

- **Public lighting:**
- A common use for NB-PLC is with public lighting—the lights found in cities and along streets, highways, and public areas such as parks.
- **Electric vehicle charging stations:**
- NB-PLC can be used for electric vehicle charging stations, where the batteries of electric vehicles can be recharged.
- **Microgrids:**
- NB-PLC can be used for microgrids, local energy grids that can disconnect from the traditional grid and operate independently.
- **Renewable energy:**
- NB-PLC can be used in renewable energy applications, such as solar, wind power, hydroelectric, and geothermal heat.

LoRaWAN

- Low-Power Wide-Area (LPWA) adapted for long-range and battery powered endpoints
- LoRaWAN is unlicensed-band LPWA technology
- 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

LoRaWAN Layers



Applications

CoAP | MQTT | IPv6/ 6LoWPAN | Raw | Others

LoRa Alliance — LoRaWAN MAC

Semtech — LoRa PHY Modulation

LoRa Alliance — 868MHz | 915MHz | Other Regional Bands

Physical Layer

- Semtech LoRa modulation is based on chirp spread spectrum modulation
- Chirp - Compressed High Intensity Radar Pulse
- Lower data rate and increase the communication distance

- Understanding LoRa gateways is critical to understanding a LoRaWAN system.
- A LoRa gateway is deployed as the center hub of a star network architecture.
- It uses multiple transceivers and channels and can demodulate multiple channels at once or even demodulate multiple signals on the same channel simultaneously.
- LoRa gateways serve as a transparent bridge relaying data between endpoints, and the endpoints use a single-hop wireless connection to communicate with one or many gateways.

- The data rate in LoRaWAN varies depending on the frequency bands and adaptive data rate (ADR).
- ADR is an algorithm that manages the data rate and radio signal for each endpoint.
- The ADR algorithm ensures that packets are delivered at the best data rate possible and that network performance is both optimal and scalable.
- Endpoints close to the gateways with good signal values transmit with the highest data rate, which enables a shorter transmission time over the wireless network, and the lowest transmit power.
- Meanwhile, endpoints at the edge of the link budget communicate at the lowest data rate and highest transmit power.

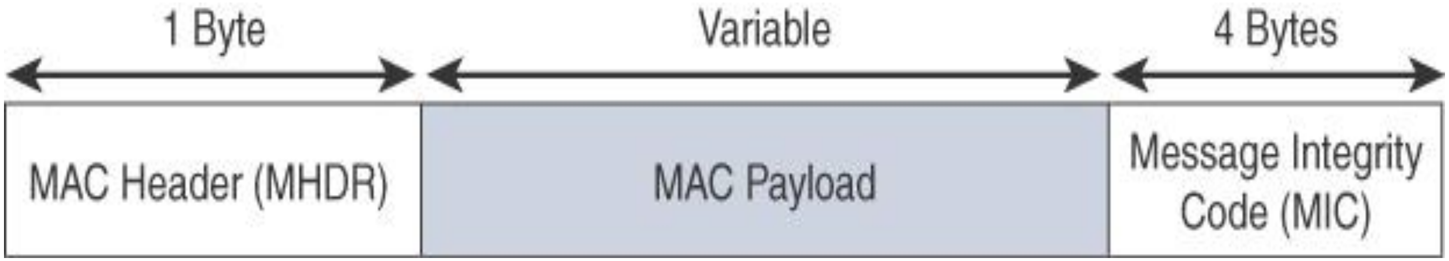
- An important feature of LoRa is its ability to handle various data rates via the spreading factor.
- Devices with a low spreading factor (SF) achieve less distance in their communications but transmit at faster speeds, resulting in less airtime.
- A higher SF provides slower transmission rates but achieves a higher reliability at longer distances.

MAC Layer

- 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.

- LoRaWAN messages, either uplink or downlink, have a PHY payload composed of a 1-byte MAC header, a variable-byte MAC payload, and a MIC that is 4 bytes in length.
- The MAC payload size depends on the frequency band and the data rate, ranging from 59 to 230 bytes for the 863–870 MHz band and 19 to 250 bytes for the 902–928 MHz band

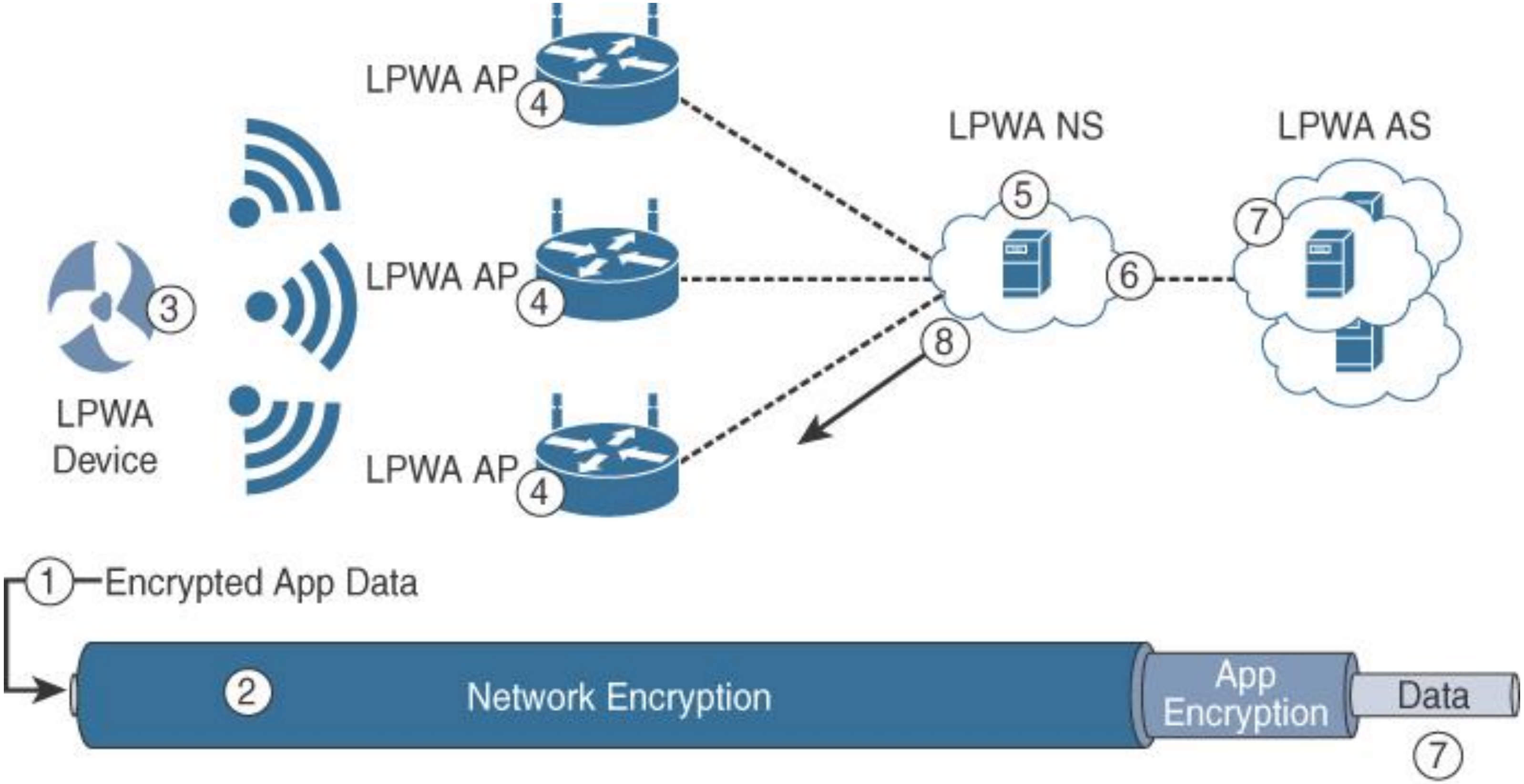


- In version 1.0.x, LoRaWAN utilizes six MAC message types.
- LoRaWAN devices use join request and join accept messages for activation and joining the network.
- The other message types are unconfirmed data up/down and confirmed data up/down.
- A "confirmed" message is one that must be acknowledged, and "unconfirmed" signifies that the end device does not need to acknowledge.
- "up/down" is simply a directional notation identifying whether the message flows in the uplink or downlink path.
- Uplink messages are sent from endpoints to the network server and are relayed by one or more LoRaWAN gateways.
- Downlink messages flow from the network server to a single endpoint and are relayed by only a single gateway

- LoRaWAN endpoints are uniquely addressable through a variety of methods, including the following:
- An endpoint can have a global end device ID or DevEUI represented as an IEEE EUI-64 address.
- An endpoint can have a global application ID or AppEUI represented as an IEEE EUI-64 address that uniquely identifies the application provider, such as the owner, of the end device

- In a LoRaWAN network, endpoints are also known by their end device address, known as a DevAddr, a 32-bit address.
- The 7 most significant bits are the network identifier (NwkID), which identifies the LoRaWAN network.
- The 25 least significant bits are used as the network address (NwkAddr) to identify the endpoint in the network.

Security



1. Device encrypts data end-to-end
2. Separate network encrypt to NS
3. Device sends a packet
4. All APs in range receive packet
5. NS decrypts using network key
6. NS forwards packet to relevant NS
7. AS decrypts using app key
8. NS selects best AP for return TX

- 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

- LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated.
- This can be achieved through one of the two join mechanisms:
- **Activation by personalization (ABP):**
- Endpoints don’t need to run a join procedure as their individual details, including DevAddr and the NwkSKey and AppSKey session keys, are preconfigured and stored in the end device.
- This same information is registered in the LoRaWAN network server

- **Over-the-air activation (OTAA):**
- Endpoints are allowed to dynamically join a particular LoRaWAN network after successfully going through a join procedure.
- The join procedure must be done every time a session context is renewed.
- During the join process, which involves the sending and receiving of MAC layer join request and join accept messages, the node establishes its credentials with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey.
- The AppKey is then used to derive the session NwkSKey and AppSKey keys

NB-IoT and Other LTE Variations

- Existing cellular technologies, such as GPRS, Edge, 3G, and 4G/LTE, are not particularly well adapted to battery-powered devices and small objects specifically developed for the Internet of Things
- LTE -M
- The new LTE-M device category was not sufficiently close to LPWA capabilities
- A new narrowband radio access technology called Narrowband IoT (NB-IoT)

- It addresses the requirements of a massive number of low-throughput devices, low device power consumption, improved indoor coverage, and optimized network architecture

LTE Cat 0

- The first enhancements to better support IoT devices in 3GPP occurred in LTE Release 12.
- A new user equipment (UE) category, Category 0, was added, with devices running at a maximum data rate of 1 Mbps
- Category 0 includes important characteristics to be supported by both the network and end devices

- **Power saving mode (PSM)**
- This new device status minimizes energy consumption
- PSM is defined as being similar to “powered off” mode, but the device stays registered with the network.
- By staying registered, the device avoids having to reattach or re-establish its network connection
- The device negotiates with the network the idle time after which it will wake up.
- When it wakes up, it initiates a tracking area update (TAU), after which it stays available for a configured time and then switches back to sleep mode or PSM.
- A TAU is a procedure that an LTE device uses to let the network know its current tracking area, or the group of towers in the network from which it can be reached

- **Half-duplex mode**
- This mode reduces the cost and complexity of a device’s implementation because a duplex filter is not needed.
- Most IoT endpoints are sensors that send low amounts of data that do not have a full duplex communication requirement.

- **LTE-M**
- LTE Release 13
- **Lower receiver bandwidth**
- Bandwidth has been lowered to 1.4 MHz versus the usual 20 MHz. This further simplifies the LTE endpoint
- **Lower data rate**
- Data is around 200 kbps for LTE-M, compared to 1 Mbps for Cat 0.

- **Half-duplex mode**
- Just as with Cat 0, LTE-M offers a half-duplex mode that decreases node complexity and cost
- **Enhanced discontinuous reception (eDRX)**
- This capability increases from seconds to minutes the amount of time an endpoint can “sleep” between paging cycles