FUTURE VISION BIE

By K B Hemanth Raj

Visit : https://hemanthrajhemu.github.io

A Small Contribution Would Support Us.

Dear Viewer,

Future Vision BIE is a free service and so that any Student/Research Personal **Can Access Free of Cost**.

If you would like to say **thanks**, you can make a **small contribution** to the author of this site.

Contribute whatever you feel this is worth to you. This gives **us support** & to bring **Latest Study Material** to you. After the Contribution Fill out this Form (https://forms.gle/tw3T3bUVpLXL8omX7). To Receive a **Paid E-Course for Free**, from our End within 7 Working Days.

Regards

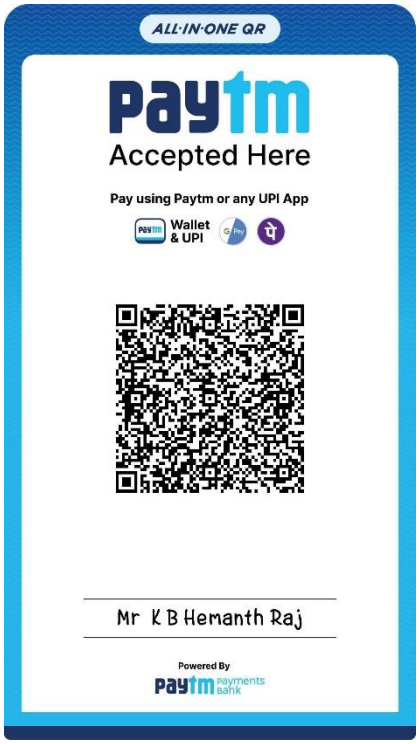
- K B Hemanth Raj (Admin)

Contribution Methods

UPI ID

1. futurevisionbie@oksbi
2. futurevisionbie@paytm

Scan & Pay



Account Transfer

Account Holder's Name: K B Hemanth Raj

Account Number: 39979402438

IFSC Code: SBIN0003982

MICR Code: 560002017

More Info: https://hemanthrajhemu.github.io/Contribution/

Gain Access to All Study Materials according to VTU,
CSE – Computer Science Engineering,
ISE – Information Science Engineering,
ECE - Electronics and Communication Engineering & MORE...

Stay Connected... get Updated... ask your queries...

Join Telegram to get Instant Updates: https://bit.ly/VTU_TELEGRAM

Contact: MAIL: futurevisionbie@gmail.com

INSTAGRAM: www.instagram.com/futurevisionbie/

WHATSAPP SHARE: https://bit.ly/FVBIESHARE

INTERNET OF THINGS TECHNOLOGY
15CS81

https://hemanthrajhemu.github.io

MODULE-2

Smart Objects: The "Things" in IoT, Sensors
and
Connecting Smart Objects

SMART OBJECTS: THE "THINGS" IN IOT, SENSORS

Introduction

- 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:** This section defines sensors, actuators, and smart objects and describes how they are the fundamental building blocks of IoT networks.
  - **Sensor Networks:** This section covers the design, drivers for adoption, and deployment challenges of sensor networks.

Sensors, Actuators, and Smart Objects

- Topics Covered
  - Sensors
  - Actuators
  - Micro-Electro-Mechanical Systems (MEMS)
  - Smart Objects
  - Smart Objects: A Definition
  - Trends in Smart Objects

Sensors

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

Sensors

- There are a number of ways to group and cluster sensors into different categories, including the following:
  - **Active or passive:** Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically require no external 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 (noninvasive).
  - **Contact or no-contact:** Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (nocontact).
  - **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).

Sensors

- **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.

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

Sensors

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

Sensors

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

Sensors

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, 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

- Power of sensors and IoT is in the area of precision agriculture (sometimes referred to as smart farming),
  - Uses a variety of technical advances to improve the efficiency, sustainability, and profitability of traditional farming practices.
    - GPS and satellite aerial imagery for determining field viability;
    - robots for high-precision planting, harvesting, irrigation
    - real-time analytics and artificial intelligence to predict optimal crop yield, weather impacts, and soil quality.

Sensors

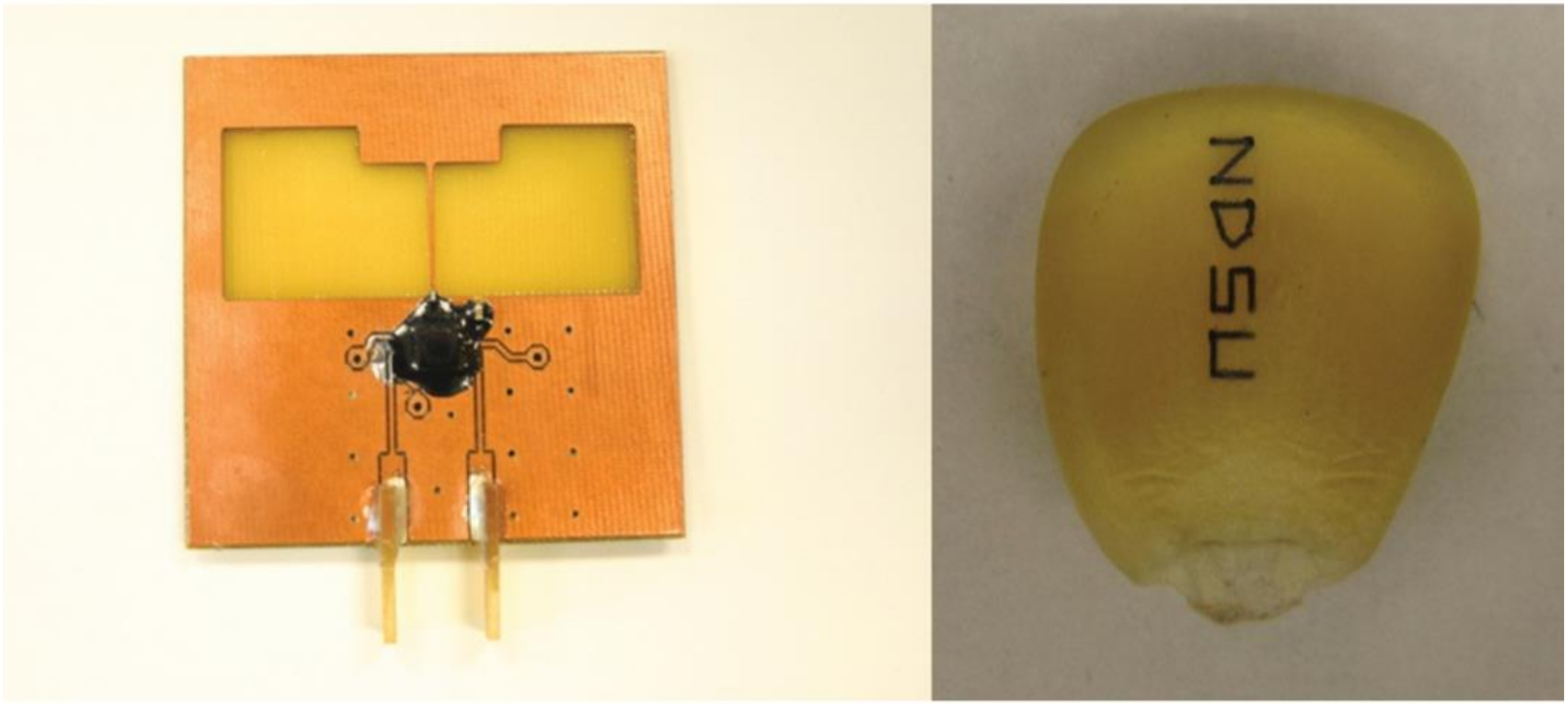


Figure 3-1 Biodegradable Sensors Developed by NDSU for Smart Farming
(Reprinted with permission from NDSU.)

Sensors

- Sensor deployments is mobile phones
- Smart homes with potentially hundreds of sensors,
- Intelligent vehicles with 100+ sensors each,
- Connected cities with thousands upon thousands of connected sensors
- As sensors are available in cheaper rate

Sensors

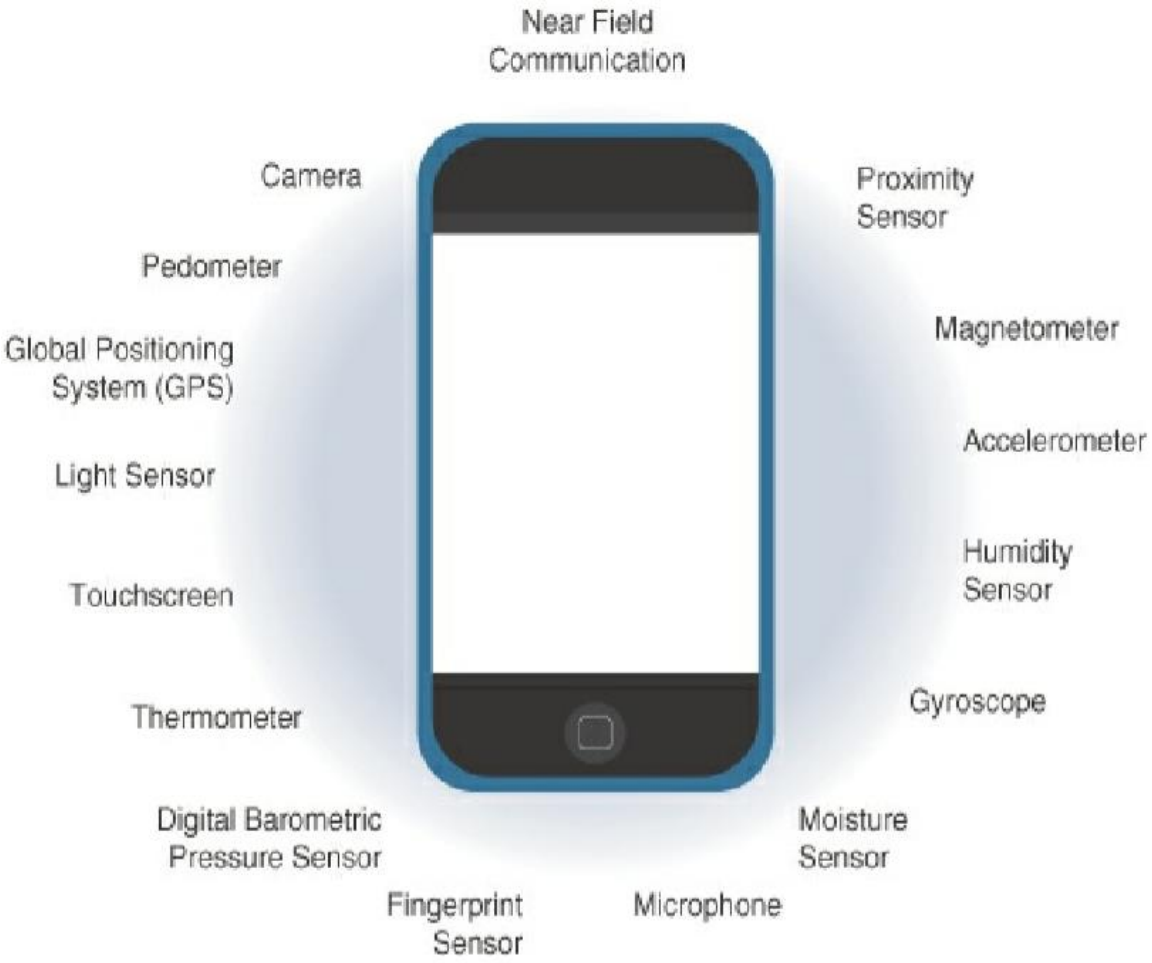


Figure 3-2 Sensors in a Smart Phone

Sensors

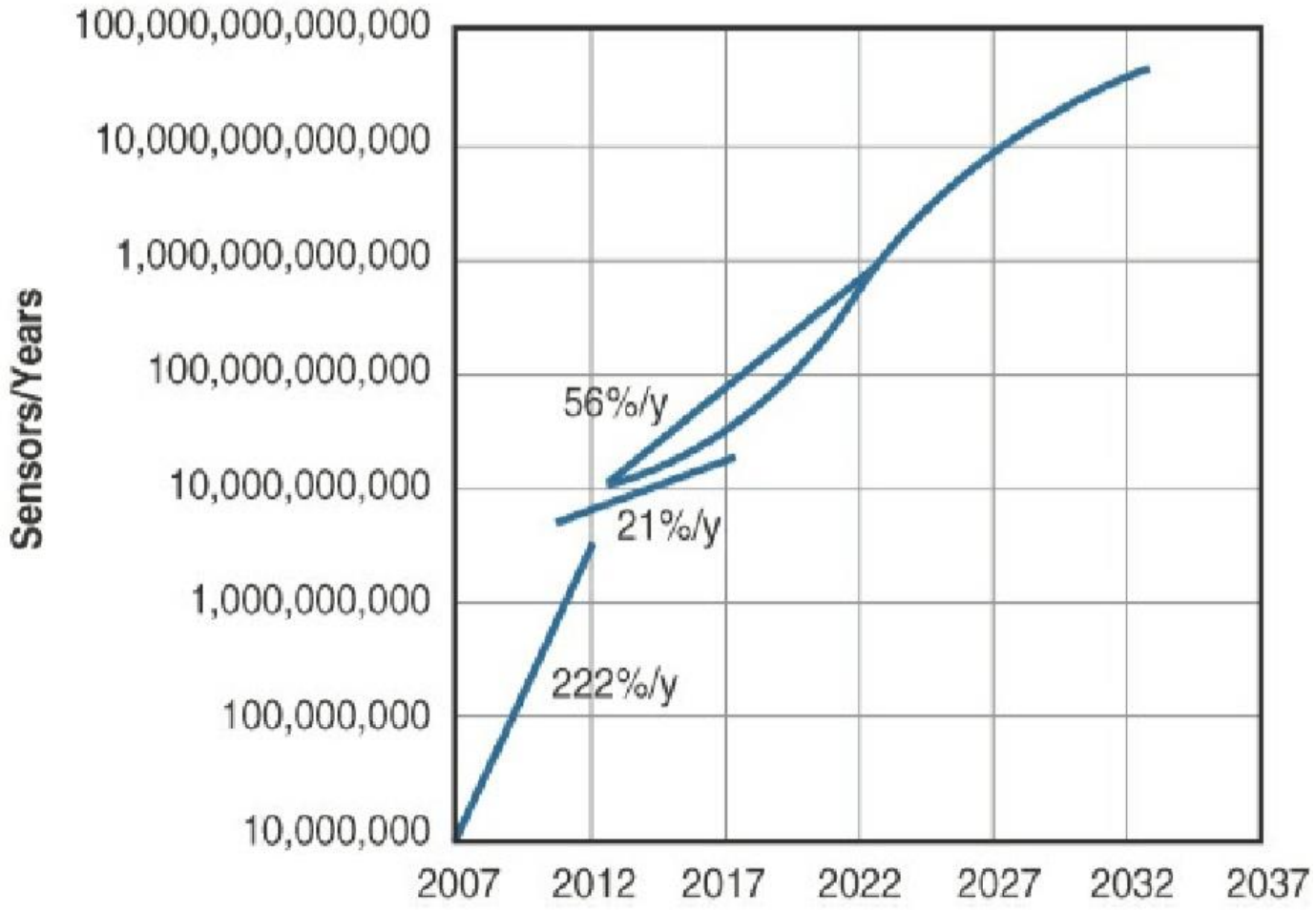


Figure 3-3 Growth and Predictions in the Number of Sensors

Actuators

- Actuators are natural complements to sensors.
- Actuators will 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.

Actuators

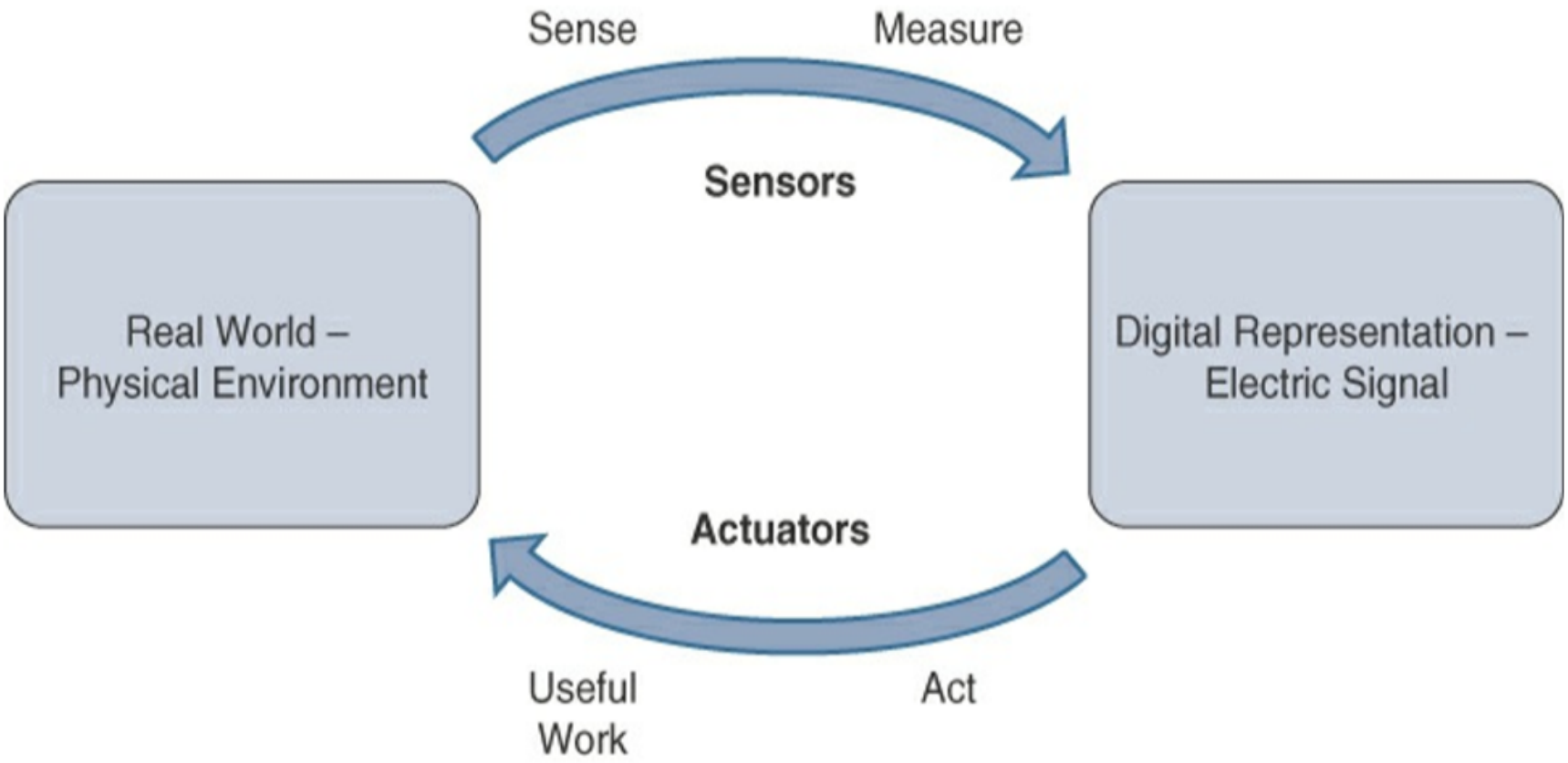


Figure 3-4 How Sensors and Actuators Interact with the Physical World

Actuators

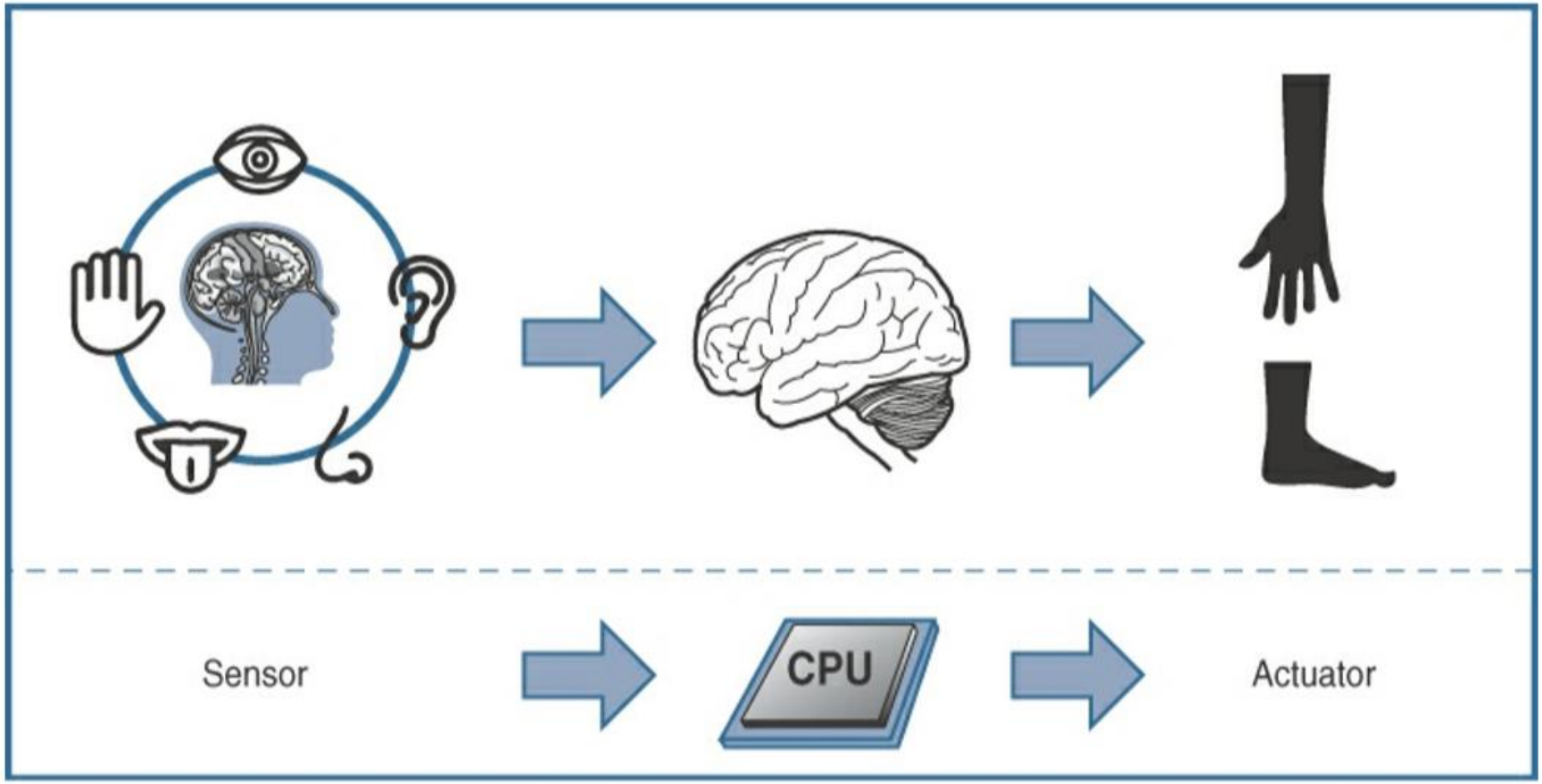


Figure 3-5 Comparison of Sensor and Actuator Functionality with Humans

Actuators

- Actuators 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.

Actuators

- **The most commonly used classification is 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

Table 3.2 Actuator Classification by Energy Type

Micro-Electro-Mechanical Systems (MEMS)

- Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale.
- 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.
  - For example,
  - inkjet printers use micropump MEMS.
  - Smart phones also use MEMS technologies like accelerometers and gyroscopes.

Micro-Electro-Mechanical Systems (MEMS)

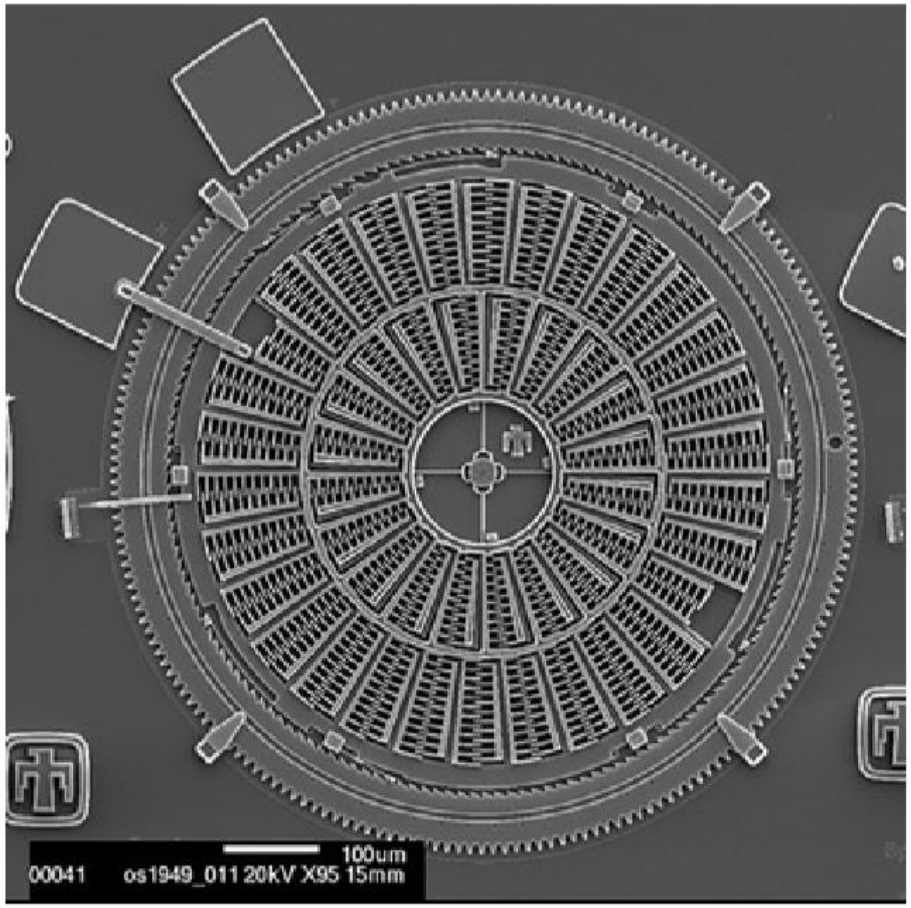


Figure 3-6 Torsional Ratcheting Actuator (TRA) MEMS (Courtesy Sandia National Laboratories, SUMMiT™ Technologies, www.sandia.gov/mstc.)

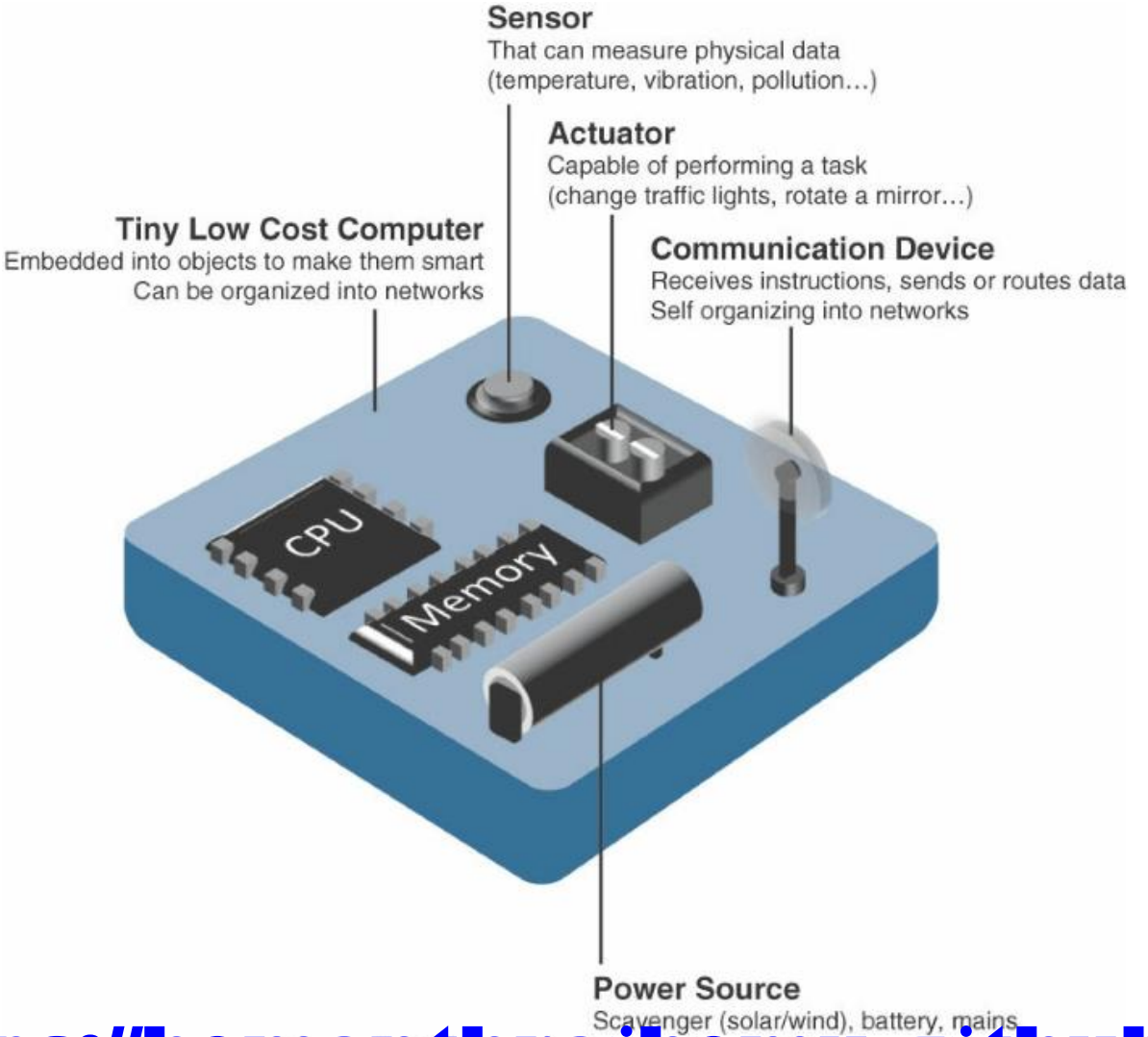
Micro-Electro-Mechanical Systems (MEMS)

- TRA (Torsional Ratcheting Actuator) MEMS is only a few hundred micrometers across;
  - a scanning electron microscope is needed to show the level of detail visible in the figure.
- Microscale sensors and actuators are immensely embeddable in everyday objects, which is a defining characteristic of IoT.

Smart Objects

- Smart Objects 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.
- Smart objects in IoT comes from being networked together rather than being isolated as standalone objects.
- This ability to communicate over a network has a multiplicative effect and allows for very sophisticated correlation and interaction between disparate smart objects.
  - For example, the smart farming
    - If a sensor is a standalone device that measures the humidity of the soil, it is interesting and useful.
    - If that same sensor is connected as part of an intelligent network that is able to coordinate intelligently with actuators to trigger irrigation systems.

Smart Objects



Smart Objects: A Definition

- A smart object, is a device that has, at a minimum, the following four defining characteristics:
  - **Processing unit:**
    - A smart object has some type of processing unit for
      - acquiring data, processing and analyzing sensing information received by the sensor(s),
      - coordinating control signals to any actuators, and controlling a variety of functions on the smart object,
      - including the communication and power systems.
      - The specific type of processing unit that is the most common is a microcontroller because of its small form factor, flexibility, programming simplicity, ubiquity, low power consumption, and low cost.

Smart Objects: A Definition

- **Sensor(s) and/or actuator(s):**
  - A smart object is capable of interacting with the physical world through sensors and actuators.
  - A smart object can contain one or multiple sensors and/or actuators, depending upon the application.
  - **Communication device:**
    - The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network).
    - Communication devices for smart objects can be either wired or wireless.
    - Overwhelmingly, in IoT networks smart objects are wirelessly interconnected for a number of reasons, including cost, limited infrastructure availability, and ease of deployment. There are myriad different communication protocols for smart objects.

Smart Objects: A Definition

- **Power source:**
  - The most significant power consumption usually comes from the communication unit of a smart object.
  - As with the other three smart object building blocks, the power requirements also vary greatly from application to application.
  - Typically, smart objects are limited in power, are deployed for a very long time, and are not easily accessible.
  - When the smart object relies on battery power, implies that power efficiency, judicious power management, sleep modes, ultra-low power consumption hardware, and so on are critical design elements.
  - For long-term deployments where smart objects are, for all practical purposes, inaccessible, power is commonly obtained from scavenger sources (solar, piezoelectric, and so on) or is obtained in a hybridized manner, also tapping into infrastructure power.

Trends in Smart Objects

- Smart objects will always be application-dependent variability, but these are broad generalizations and trends impacting IoT:
  - **Size is decreasing:**
    - Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.
  - **Power consumption is decreasing:**
    - The different hardware components of a smart object continually consume less power. This is especially true for sensors, many of which are completely passive. Some battery-powered sensors last 10 or more years without battery replacement.

Trends in Smart Objects

- **Processing power is increasing:**
  - Processors are continually getting more powerful and smaller. So they become increasingly complex and connected.
- **Communication capabilities are improving:**
  - Wireless speeds are continually increasing, but they are also increasing in range. IoT is driving the development of more and more specialized communication protocols covering a greater diversity of use cases and environments.
- **Communication is being increasingly standardized:**
  - There is a strong push in the industry to develop open standards for IoT communication protocols. In addition, there are more and more open source efforts to advance IoT.

Sensor Networks

- **Topics Covered**
  - **Wireless Sensor Networks (WSNs)**
  - **Communication Protocols for Wireless Sensor Networks**

Sensor Networks

- A **sensor/actuator network (SANET)**, as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment.
- 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.
  - Example: Smart homes are a type of SANET
    - networked with heating, ventilation, and air-conditioning (HVAC) actuators.

Sensor Networks

- The following are some advantages and disadvantages that a wireless-based solution offers:
  - Advantages:
    - Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
    - Simpler scaling to a large number of nodes
    - Lower implementation costs
    - Easier long-term maintenance
    - Effortless introduction of new sensor/actuator nodes
    - Better equipped to handle dynamic/rapid topology changes
  - Disadvantages:
    - Potentially less secure (for example, hijacked access points)
    - Typically lower transmission speeds
    - Greater level of impact/influence by environment

Wireless Sensor Networks (WSNs)

- Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as motes.
  - flexible deployments
  - variety of design constraints

- The following are some of the most significant limitations of the smart objects in WSNs:
  - Limited processing power
  - Limited memory
  - Lossy communication
  - Limited transmission speeds
  - Limited power

- These limitations greatly influence how WSNs are designed, deployed, and utilized.

Wireless Sensor Networks (WSNs)

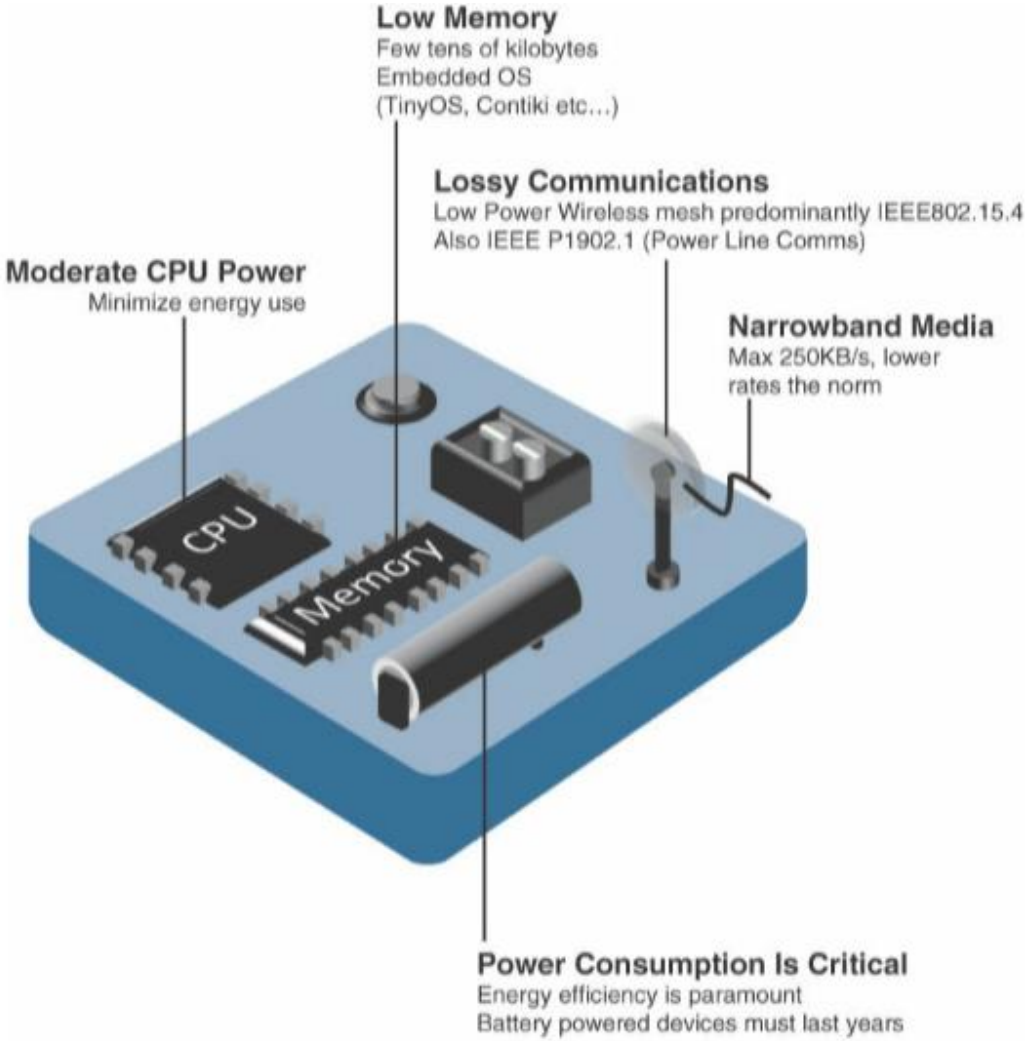


Figure 3-8 Design Constraints for Wireless Smart Objects

Wireless Sensor Networks (WSNs)

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

- 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.

- 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,

Wireless Sensor Networks (WSNs)

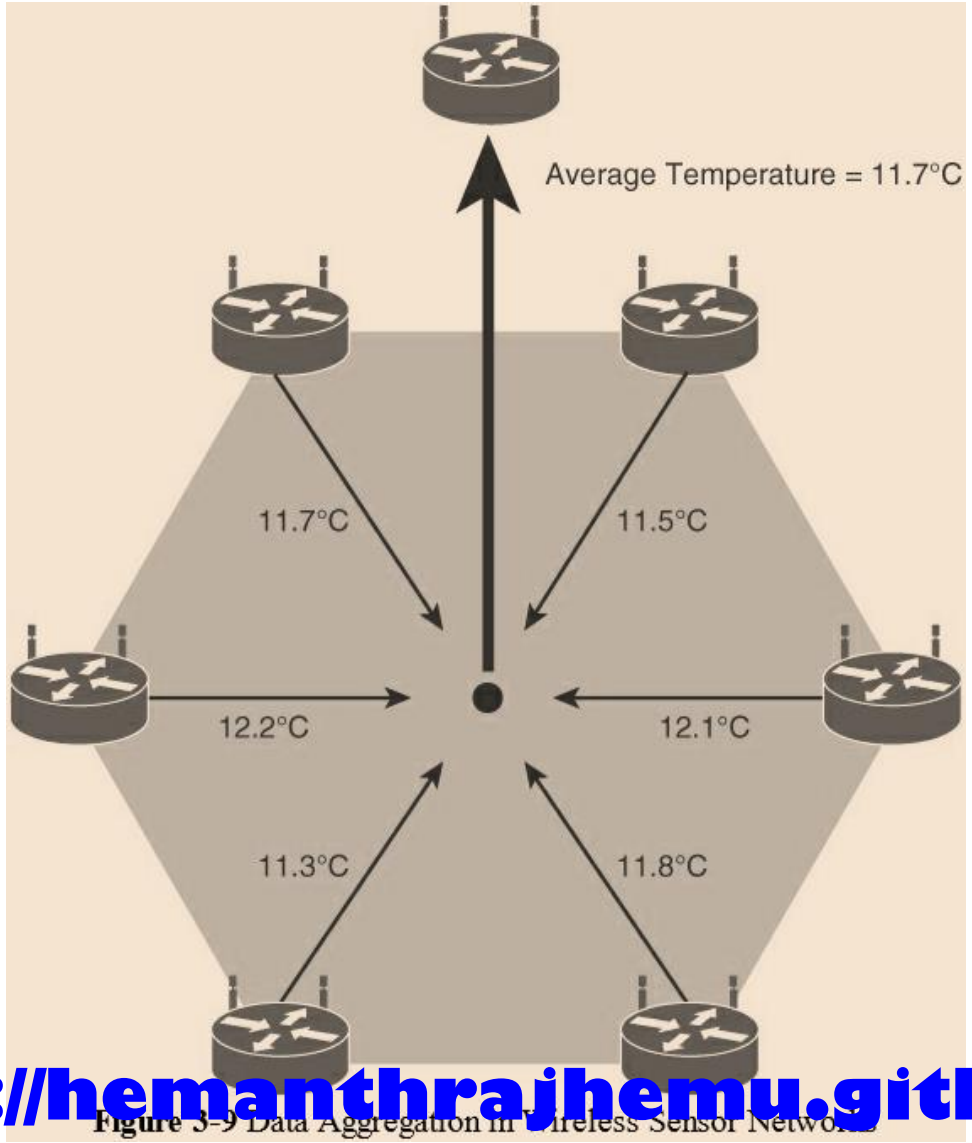


Figure 3-9 Data Aggregation in Wireless Sensor Networks

Wireless Sensor Networks (WSNs)

- 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, in some medical use cases sensors
    - Sends **periodically**, such as temperature or blood pressure readings
    - blood pressure or temperature readings are triggered to be sent only when **certain critically low or high readings** are measured

Wireless Sensor Networks (WSNs)

- As WSNs grow to very large numbers of smart objects, there is a trend toward ever increasing levels of autonomy.
  - For example, manual configuration of thousands of smart objects is impractical and unwieldy, so smart objects in a WSN are typically self-configuring or automated by an IoT management platform in the background.
    - For example, "smart dust" applications,
      - in which very small sensor nodes (that is, MEMS) are scattered over a geographic area to detect vibrations, temperature, humidity, and so on.

Wireless Sensor Networks (WSNs)

- Self organization is required for networking the scads of wireless smart objects such that these nodes autonomously come together to form a true network with a common purpose.
- This capability to self-organize is able to adapt and evolve the logical topology of a WSN to optimize communication

Wireless Sensor Networks (WSNs)

- Autonomous techniques, such as **self-healing, self-protection, and self-optimization,** are often employed to perform these functions on behalf of an overall WSN system.
- IoT applications are often mission critical, and in large-scale WSNs, the **overall system can't fail if** the environment suddenly changes, wireless communication is temporarily lost, or a limited number of nodes run out of battery power or function improperly.

Communication Protocols for Wireless Sensor Networks

- WSNs are becoming increasingly heterogeneous, with more sophisticated interactions.
- WSNs are seeing transitions from homogenous wireless networks made up of mostly a single type of sensor to networks made up of multiple types of sensors that can even be a hybridized mix of many cheap sensors with a few expensive ones used for very specific high-precision functions.
  - For Example: WSN that has multiple types of sensors, and one of those types is a temperature sensor that can be flexibly used concurrently for environmental applications, weather applications, and smart farming applications.

Communication Protocols for Wireless Sensor Networks

- Coordinated communication with sophisticated interactions by constrained devices within such a heterogeneous environment is quite a challenge.
  - For example:
    - Any communication protocol must be able to scale to a large number of nodes.
    - When selecting a communication protocol, must care about the requirements of the specific application and consider the communication protocol offers low power consumption, maximum transmission speed, range, tolerance for packet loss, topology optimization, security, and so on.
- The fact that WSNs are often deployed outdoors in harsh and unpredictable environments adds yet another variable to consider because obviously not all communication protocols are designed to be equally rugged.

Communication Protocols for Wireless Sensor Networks

- Sensors produce large amounts of sensing and measurement data.
- 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.

- Data transmission over various networking application like multivendor environments, these communication protocols must be standardized.
  - Standardization means, communication protocols is a complicated task, requiring protocol definition across multiple layers of the stack, as well as a great deal of coordination across multiple standards development organizations.

CONNECTING SMART OBJECTS

Introduction

- A number of different protocols used to connect sensors, actuators, and smart objects with considering the **Communication Criteria and IoT Access Technologies.**

COMMUNICATION CRITERIA

Introduction

- Topics Covered:
  - Communications Criteria
    - Range: signal propagation and distance.
    - Frequency Bands: licensed and unlicensed spectrum
    - Power Consumption: stable power source or battery powered.
    - Topology: various layouts that may be supported for connecting multiple smart objects.
    - Constrained Devices: limitations of certain smart objects from a connectivity perspective.
    - Constrained-Node Networks: challenges that are often encountered with networks connecting smart objects.

Communications Criteria Range

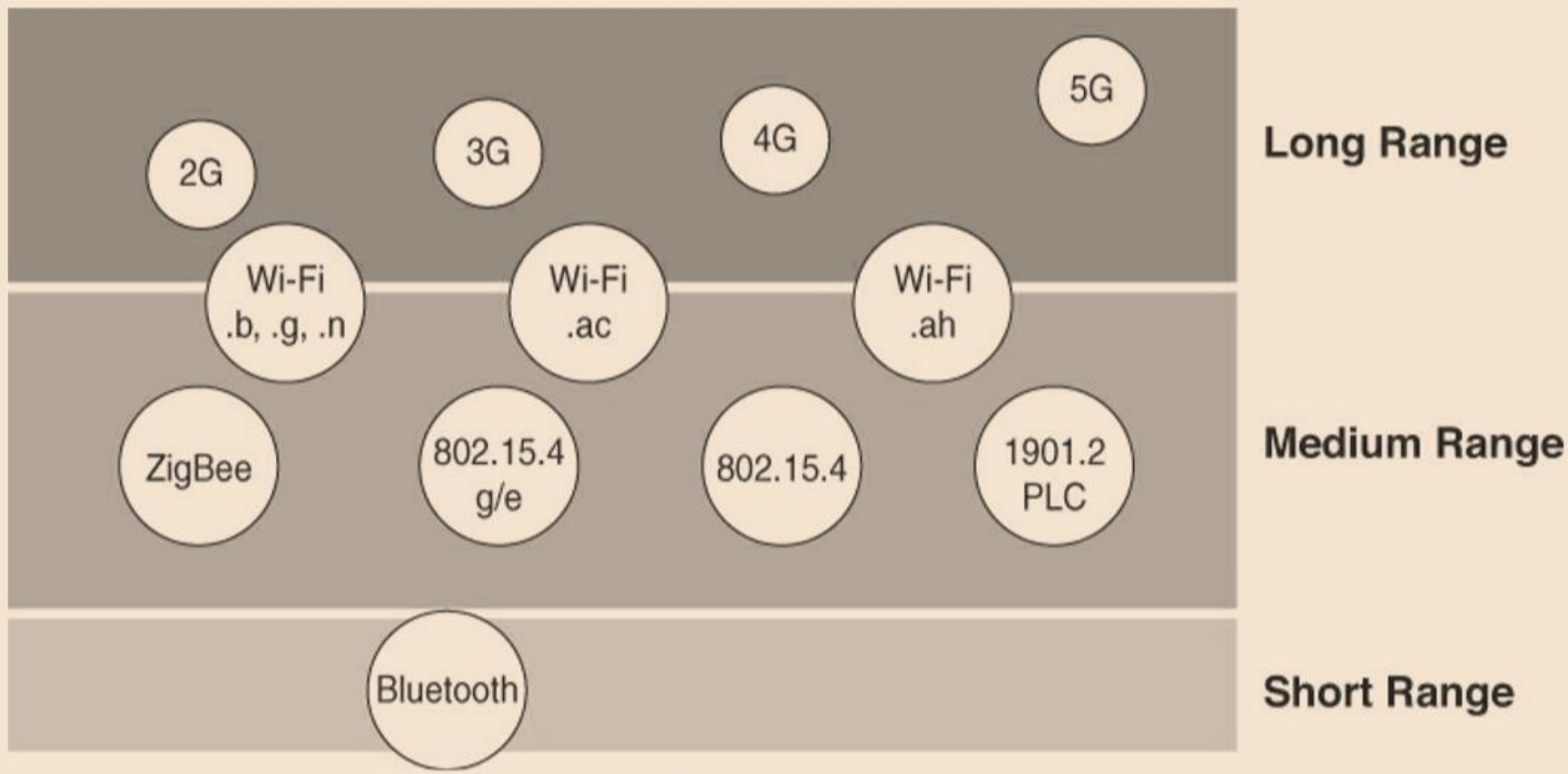


Figure 4-1 Wireless Access Landscape

https://hemanthrajhemu.github.io

Communications Criteria Range

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

Communications Criteria Range

- **Long range:**
  - Distances greater than 1 mile between two devices
    - Wireless examples are cellular (2G, 3G, 4G) IEEE 802.11 Wi-Fi
    - Low-Power Wide-Area (LPWA) technologies have the ability to communicate over a large area without consuming much power. These technologies are therefore ideal for battery-powered IoT sensors.
    - Industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications.

Communications Criteria Frequency Bands

- Radio spectrum is regulated the **International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).**
  - For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
- **The spectrum for various communications uses is often viewed as a critical resource.**
  - For example, mobile operators pay for licenses in the cellular spectrum.

Communications Criteria Frequency Bands

- **Frequency bands leveraged by wireless communications are split between licensed and unlicensed bands.**

- **ITU Licensed spectrum**
  - is generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.
  - Examples of licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.

Communications Criteria Frequency Bands

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

- Unlicensed spectrum it can suffer from more interference because other devices may be competing for the same frequency in a specific area.
- Licensed spectrum are more reliable

Communications Criteria Frequency Bands

- ISM bands operate in the sub-GHz range.
  - Sub-GHz bands are used by protocols such as IEEE 802.15.4, 802.15.4g, and 802.11ah, and LPWA technologies such as LoRa and Sigfox.
  - Sub-GHz ranges are 169 MHz, 433 MHz, 868 MHz, and 915 MHz.
  - For example, European countries, the 169 MHz band is best suited for wireless water and gas metering applications.

- The European Conference of Postal and Telecommunications Administrations (CEPT), in the European Radiocommunications Committee (ERC) Recommendation 70-03, defines the 868 MHz frequency band for telecommunications and postal organizations.
- The 868 MHz band is applicable to IoT access technologies such as IEEE 802.15.4 and 802.15.4g, 802.11ah, and LoRaWAN.

Communications Criteria Frequency Bands

- Frequencies and corresponding regulations of a country when implementing or deploying IoT smart objects.
- Smart objects running over unlicensed bands can be easily optimized in terms of hardware supporting the two main worldwide sub-GHz frequencies, 868 MHz and 915 MHz.

Communications Criteria
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.
  - deployment of powered nodes is limited by the availability of a power source
- **Battery-powered nodes**
  - Often classified by the required lifetimes of their batteries.
    - A node need 10 to 15 years of battery life, such as on water or gas meters

Communications Criteria Power Consumption

- IoT wireless access technologies
  - wireless environment known as **Low-Power Wide-Area (LPWA)**
- Wired IoT access technologies
  - consisting of powered nodes are not exempt from power optimization
  - For example, deployment of smart meters over PLC, the radio interface on meters can't consume 5 to 10 watts of power

Communications Criteria Topology

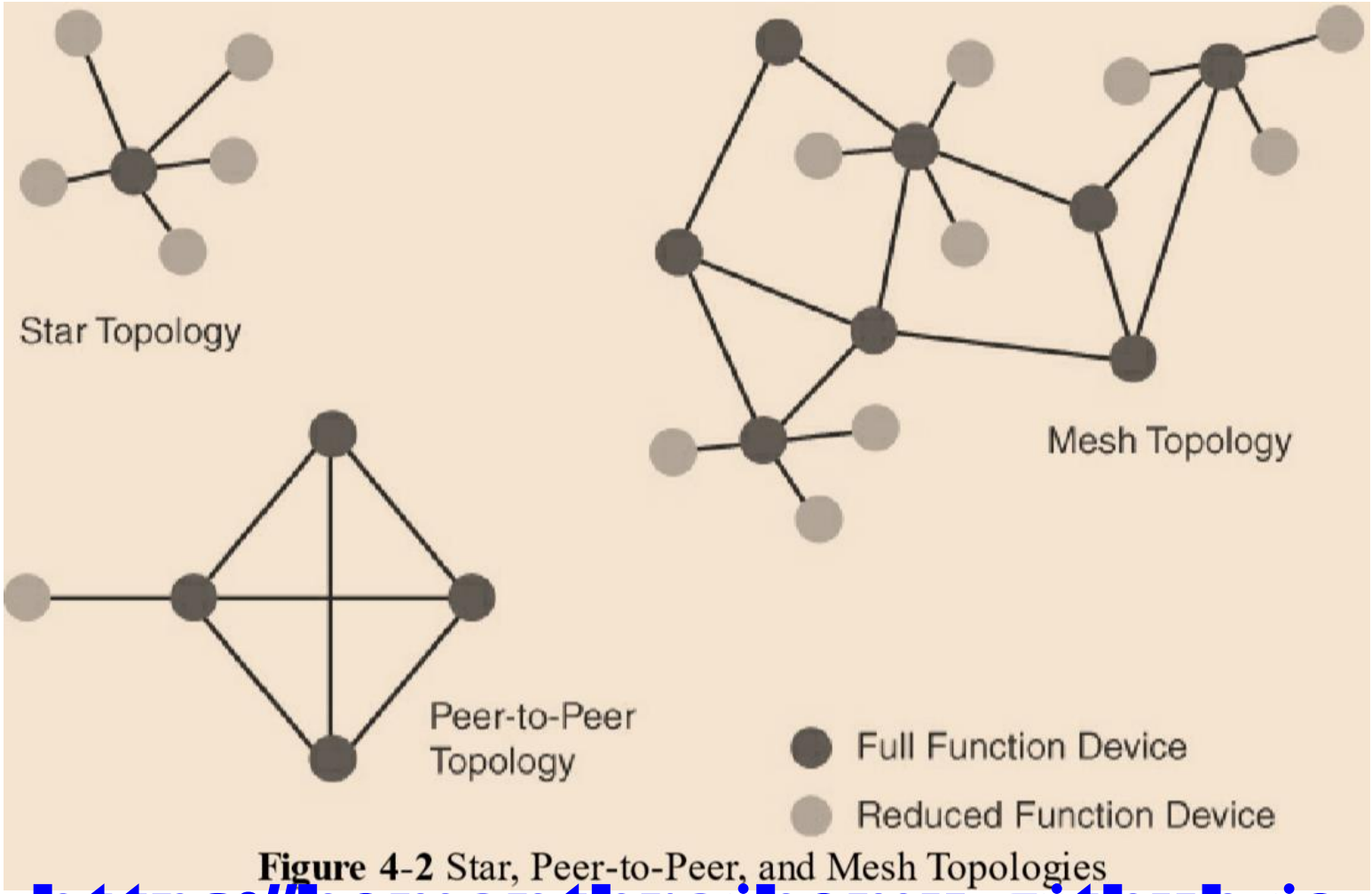


Figure 4-2 Star, Peer-to-Peer, and Mesh Topologies

Communications Criteria Topology

- IoT devices uses, three main topology schemes are dominant: star, mesh, and peer-to-peer.
  - Star Topology
    - Star topologies utilize a single central base station or controller to allow communications with endpoints.
    - Long-range, medium-range technologies and Shortrange technologies,
    - For Example: Cellular, LPWA, indoor Wi-Fi deployments and Bluetooth networks.
  - Peer-to-peer Topology
    - Allow any device to communicate with any other device as long as they are in range of each other
    - medium-range technologies
    - rely on multiple full-function devices
  - Mesh topology
    - helps cope with low transmit power, searching to reach a greater overall distance, and coverage by having intermediate nodes relaying traffic for other nodes.
    - medium-range technologies, Long-range
    - For example: outdoor Wi-Fi, IEEE 802.15.4 and 802.15.4g and even wired IEEE 1901.2a PLC

Communications Criteria Topology

- Mesh topology requires the implementation of a Layer 2 forwarding protocol known as mesh-under or a Layer 3 forwarding protocol referred to as mesh-over on each intermediate node.
- Powered nodes, mesh topology requires a properly optimized implementation for battery-powered nodes.
- Battery-powered nodes, in the case of mesh topology, either the battery-powered nodes act as leaf nodes (or reduced-function device RFD) or as a "last resource path" to relay traffic when used as intermediate nodes.
- For battery-powered nodes, the topology type and the role of the node in the topology (for example, being an intermediate or leaf node) are significant factors for a successful implementation.

Communications Criteria Constrained Devices

- Constrained nodes have limited resources that impact their networking feature set and capabilities.
- The Internet Engineering Task Force (IETF) acknowledges in RFC (Request for Comments) 7228 that different categories of IoT devices are deployed.

Communications Criteria 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.

Table 4-1 Classes of Constrained Nodes, as Defined by RFC 7228

Communications Criteria Constrained-Node Networks

- Topics Covered:
  - Data Rate and Throughput
  - Latency and Determinism
  - Overhead and Payload

Communications Criteria Constrained-Node Networks

- Constrained-node networks are often referred to as **low-power and lossy networks (LLNs).**
  - **Low-power** indicate powered and battery powered constrained nodes
  - **Lossy networks** indicates that network performance may suffer from interference and variability due to harsh radio environments
- Layer 1 and Layer 2 protocols that can be used for constrained-node networks.

Communications Criteria Constrained-Node Networks

- **Data Rate and Throughput:**
- The data rates available from IoT access technologies like Sigfox, LTE, and IEEE 802.11ac.
- Throughput is less than the data rate.
- Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints.
  - For example, Bluetooth sensors
- Constrained nodes are limited in terms of data rate, which depends on the selected frequency band, and throughput.

Communications Criteria Constrained-Node Networks

- LPWA networks,
  - which are designed with a certain number of messages per day or per endpoint rather than just having a pure bandwidth usage limit in place.
- LLN constrained nodes
  - that send only one message a day, real throughput is often very important for constrained devices implementing an IP stack.
  - throughput is a lower percentage of the data rate
- Two-way communication handling, and the variable data payload size, which reduces the throughput.

Communications Criteria Constrained-Node Networks

- **Latency and Determinism**
- Latency depends on IoT access technology.
  - 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.

Communications Criteria Constrained-Node Networks

- **Overhead and Payload**
- For constrained access network technologies, the MAC payload size decides the requirement for applications and IP.
  - For example, minimum IPv6 MTU size is expected to be 1280 bytes.
  - Fragmentation of the IPv6 payload has to be taken into account by link layer access protocols.
- LLNs are able to transport IP,
  - such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization.
  - For example,
    - IEEE 802.15.4 payload size is 127 bytes
    - IPv6 payload size is 1280 bytes
    - IEEE 802.15.4g payload size is 2048 bytes
- LPWA technologies offer small payload sizes
  - LoRaWAN technology payload size is 19 bytes

IOT ACCESS TECHNOLOGIES

Introduction

- Topics Covered:
  - IoT Access Technologies
    - IEEE 802.15.4: an older but foundational wireless protocol for connecting smart objects.
    - IEEE 802.15.4g and IEEE 802.15.4e: are targeted to utilities and smart cities deployments.
    - IEEE 1901.2a: which is a 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: which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

Introduction

- 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

IEEE 802.15.4

- IEEE 802.15.4
  - is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.
- IEEE 802.15.4 is commonly found in the following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls

IEEE 802.15.4

- IEEE 802.15.4 focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading.
  - The reliability and latency degraded because of 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.

IEEE 802.15.4 Standardization and Alliances

- Low-data-rate PHY and MAC layer in wireless personal area networks (WPAN).
  - This standard have low-complexity wireless devices with low data rates with good battery life.
- IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks (as shown in next slide)
  - ZigBee
  - 6LoWPAN
  - ZigBeeIP
  - ISA100.11a
  - WirelessHART
  - Thread

IEEE 802.15.4 Standardization and Alliances

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.

IEEE 802.15.4 Standardization and Alliances

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.

Table 4-2 Protocol Stacks Utilizing IEEE 802.15.4

IEEE 802.15.4 - ZigBee

- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth, interoperate and low power needs.
- Sets of Commands and Message
  - Sets of commands and message types are called clusters.

- ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy

IEEE 802.15.4 - ZigBee

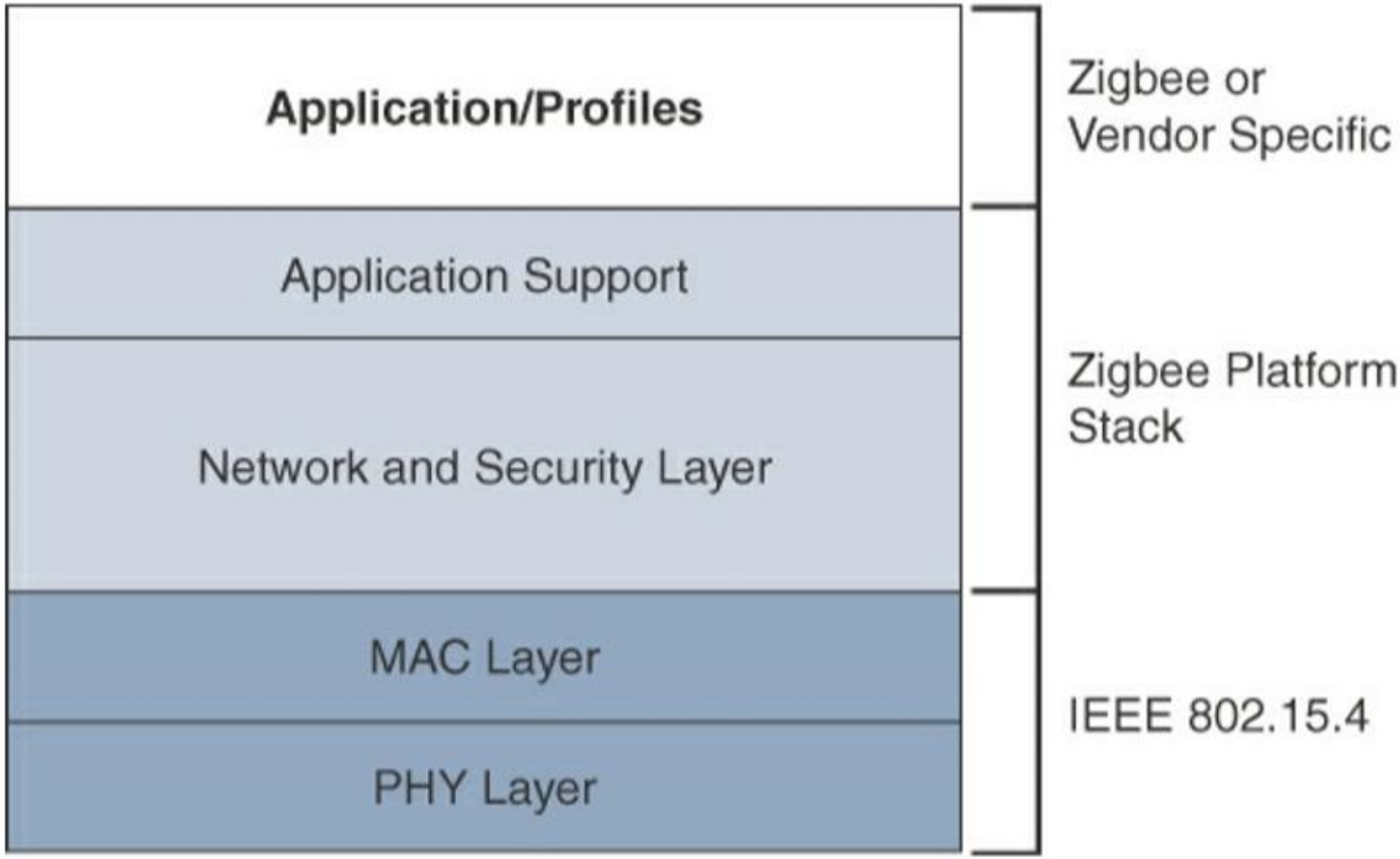


Figure 4-3 High-Level ZigBee Protocol Stack

IEEE 802.15.4 - ZigBee

- ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers
- Network and security layer and application support layer that sit on top of the lower layers.
- The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications.
  - 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.
- **Network layer**
  - For forming the appropriate topology, which is a mesh, star or tree.
- **Security layer**,
  - ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.
- **Application Layer**
  - Interfaces the lower portion of the stack dealing with the network of ZigBee devices and with the higher-layer applications.

IEEE 802.15.4 - ZigBeeIP

- ZigBee IP
  - IEEE 802.15.4 , IP and TCP/UDP protocols and various other open standards are supported at the network and transport layers.
  - Open standards like LLNs, IPv6, 6LoWPAN, and RPL. These provides for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.
- ZigBee IP Applications like
  - Smart Energy (SE) Profile 2.0 or SE 2.0
  - smart metering and residential energy management systems

IEEE 802.15.4 - ZigBeeIP

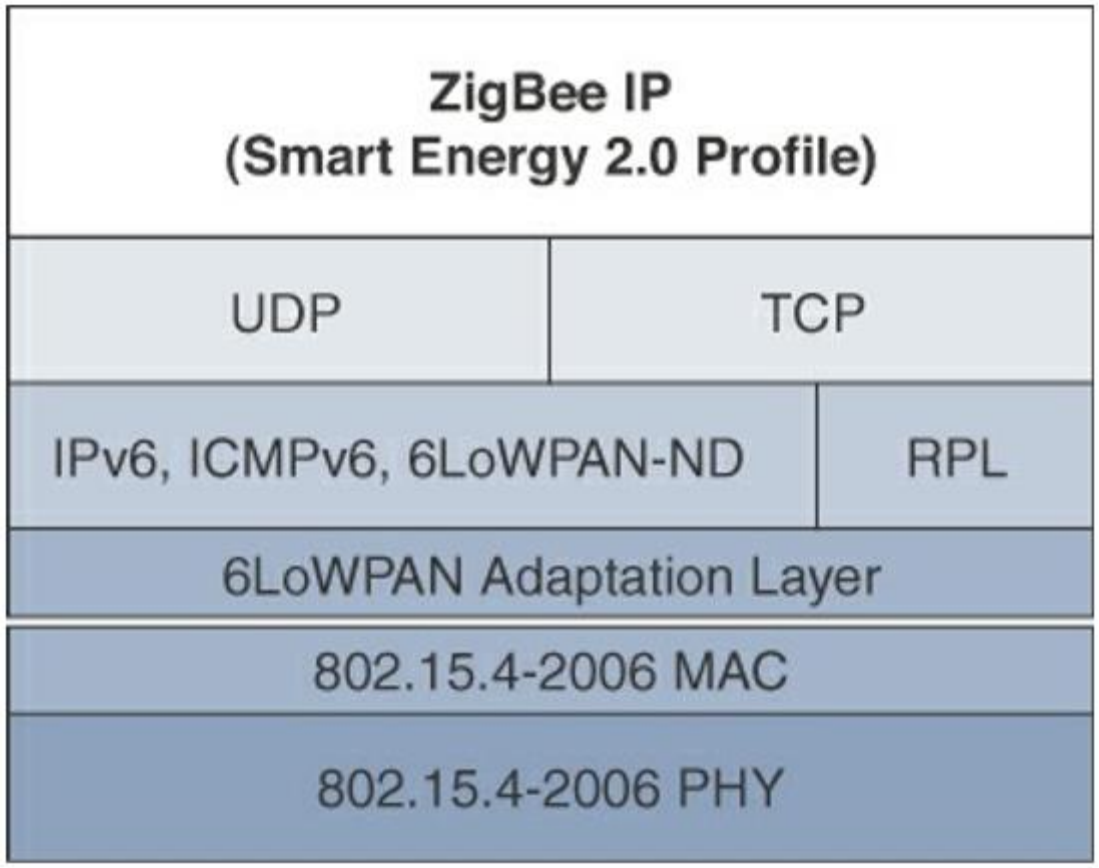


Figure 4-4 ZigBee IP Protocol Stack

IEEE 802.15.4 - ZigBeeIP

- **6LoWPAN as an adaptation layer**
  - ZigBee IP utilizes the mesh-over or route-over method for forwarding packets.
  - It support of 6LoWPAN's fragmentation and header compression schemes.
- **Network layer**,
  - 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.

IEEE 802.15.4 - 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.
  - These standards is based on DSSS (direct sequence spread spectrum), is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth.
- The original physical layer transmission options were as follows:
  - 2.4 GHz, 16 channels, with a data rate of 250 kbps
  - 915 MHz, 10 channels, with a data rate of 40 kbps
  - 868 MHz, 1 channel, with a data rate of 20 kbps
  - Note - only the 2.4 GHz band operates worldwide

IEEE 802.15.4 - Physical Layer

- Additional PHY communication options are:
  - **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.
- These improvements increase the maximum data rate

IEEE 802.15.4 - Physical Layer

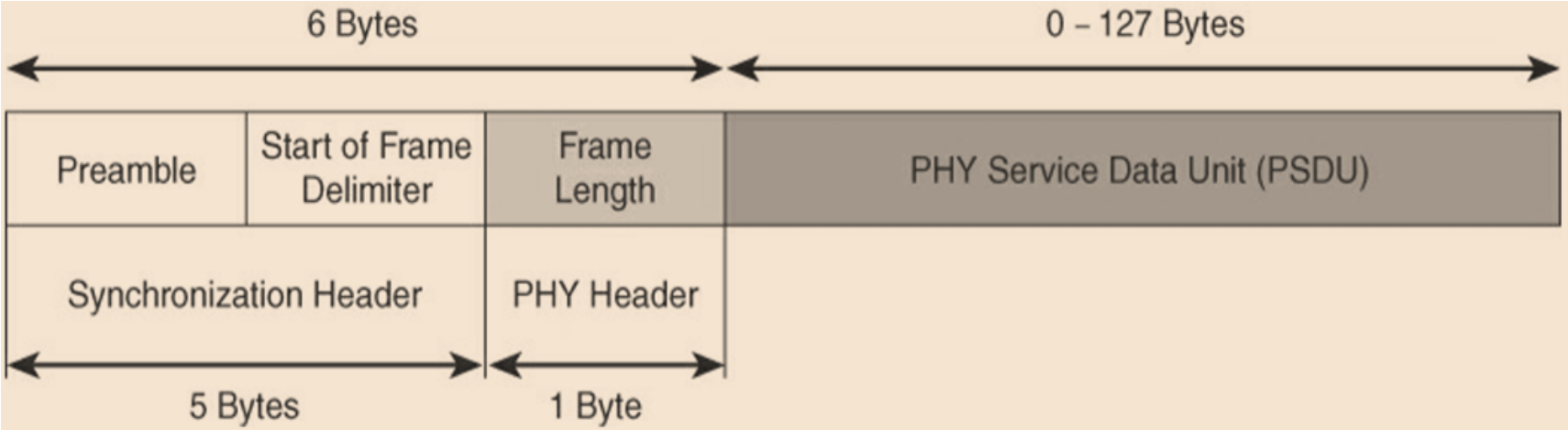


Figure 4-5 IEEE 802.15.4 PHY Format

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

IEEE 802.15.4 - Physical Layer

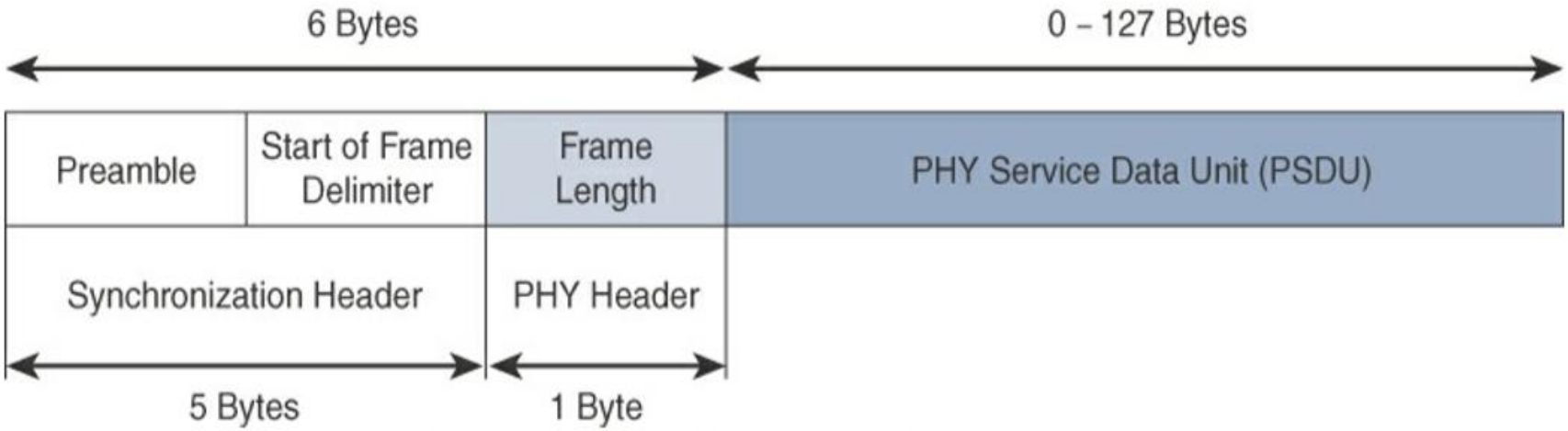


Figure 4-5 IEEE 802.15.4 PHY Format

- **The PHY Header**
  - **Frame length value:** It lets the receiver know how much total data to expect in the PSDU.
- **PSDU (PHY service data unit)** is the data field or payload.
  - Maximum size of the PSDU is 127 bytes

IEEE 802.15.4 - MAC Layer

- MAC layer performs the following tasks:
  - Manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated.
  - The scheduling and routing of data frames are coordinated
  - 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

IEEE 802.15.4 - MAC Layer

- 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
- The 802.15.4 MAC frame broken down into the
  - MAC Header,
  - MAC Payload,
  - MAC Footer fields.

IEEE 802.15.4 - MAC Layer

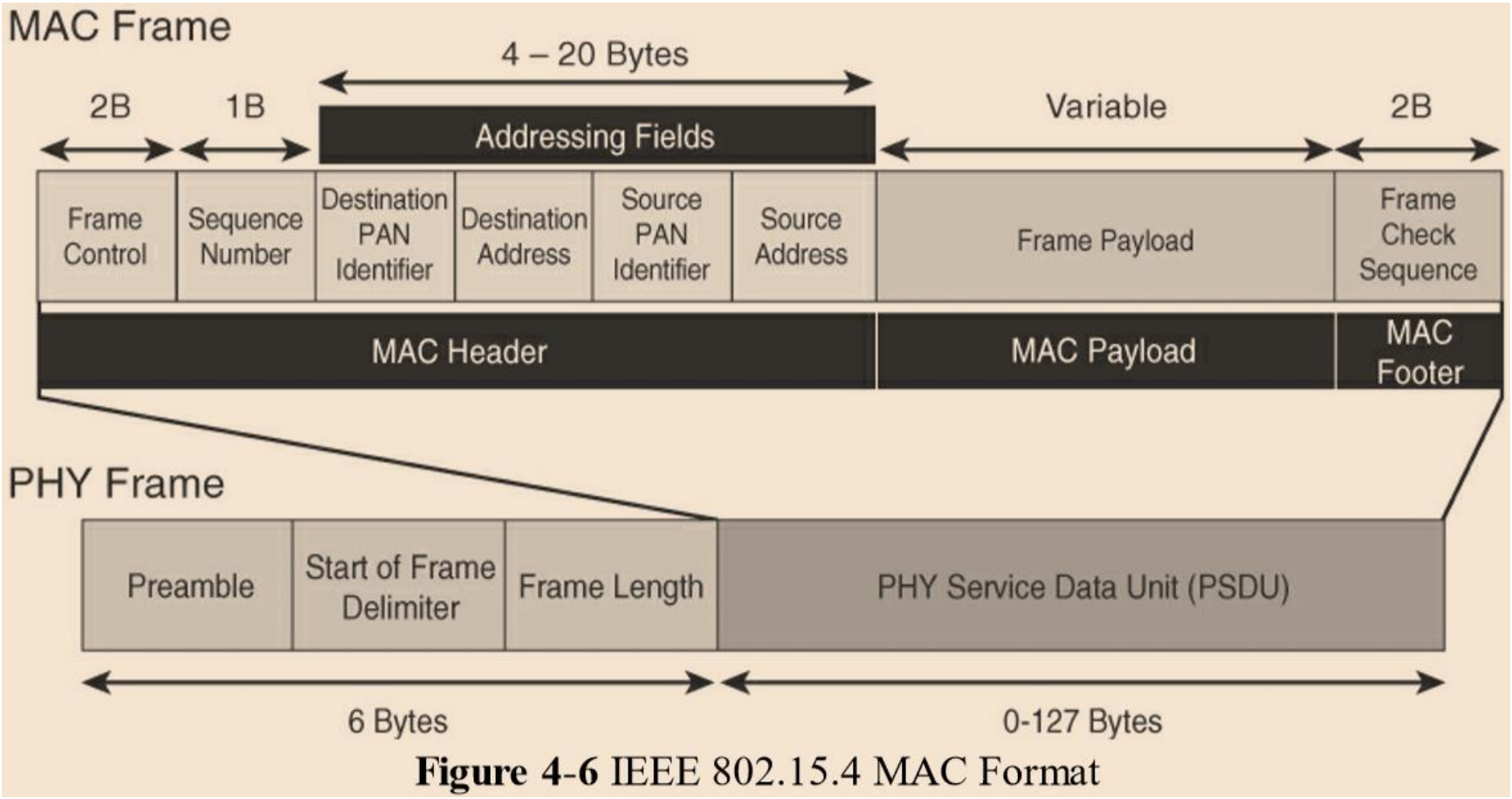
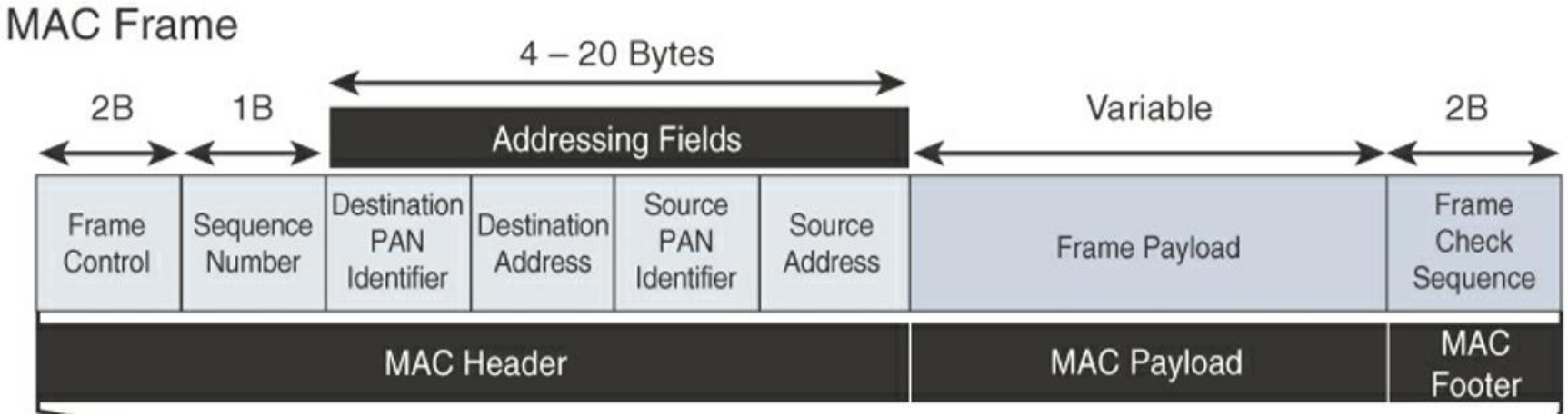


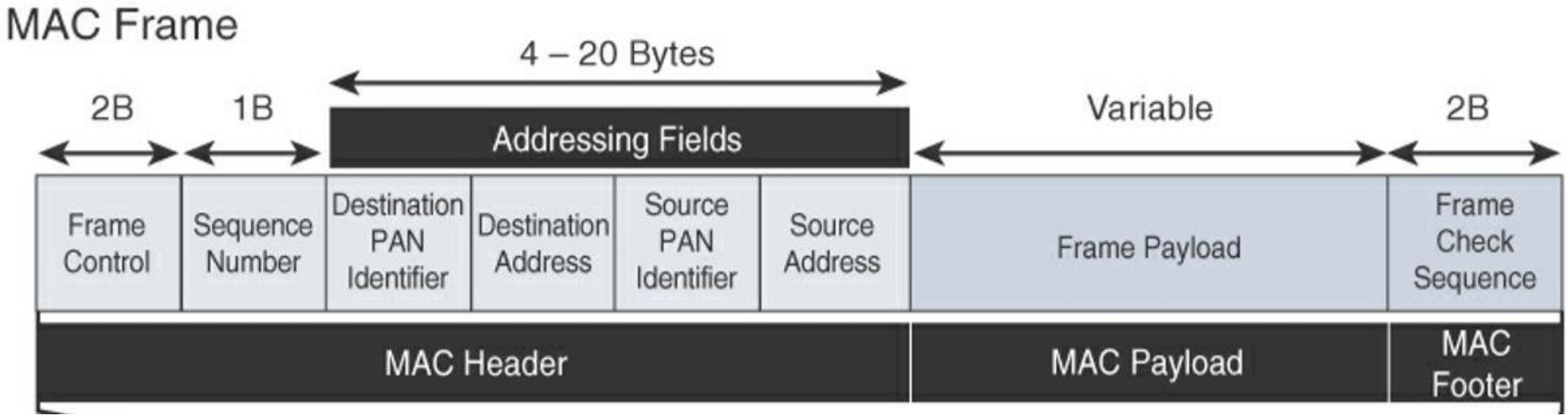
Figure 4-6 IEEE 802.15.4 MAC Format

IEEE 802.15.4 - MAC Layer



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

IEEE 802.15.4 - MAC Layer



- The MAC Payload field varies by individual frame type. maximum payload is 127 bytes, and also defines how a 16-bit "short address" is assigned to devices)
  - For example,
    - Beacon frames have specific fields and payloads related to beacons,
    - 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 - Topology

- 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.

- 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

IEEE 802.15.4 - Topology

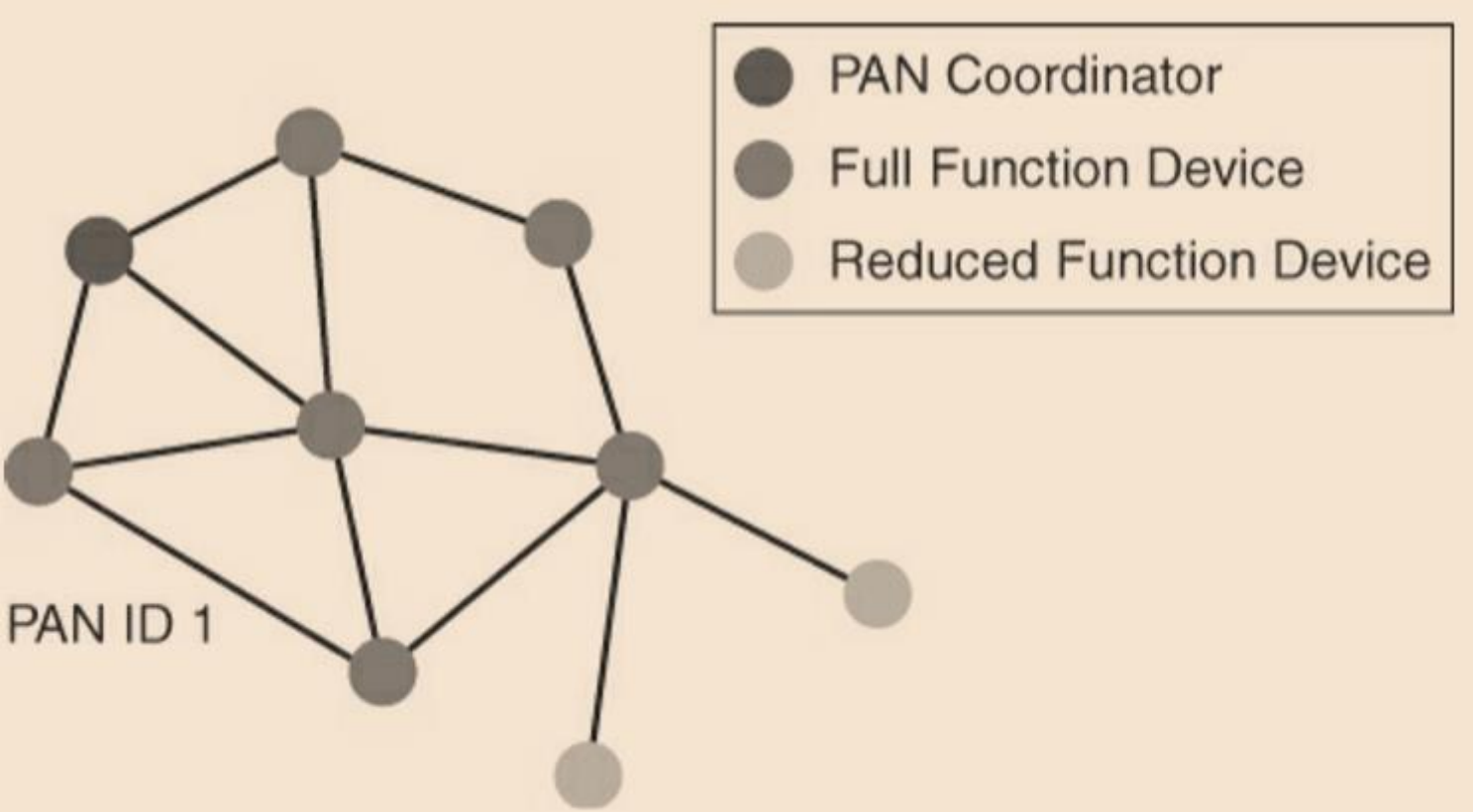


Figure 4-7 802.15.4 Sample Mesh Network Topology

IEEE 802.15.4 - Topology

- 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 with PAN ID E.g. PAN ID1.
  - FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

IEEE 802.15.4 - Security

- IEEE 802.15.4 uses **Advanced Encryption Standard (AES)** with a 128-bit key length as the base encryption algorithm for securing its data and also validates the data that is sent
  - Validation 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.
  - AES is a block cipher, which means it operates on fixed-size blocks of data.

IEEE 802.15.4 - Security

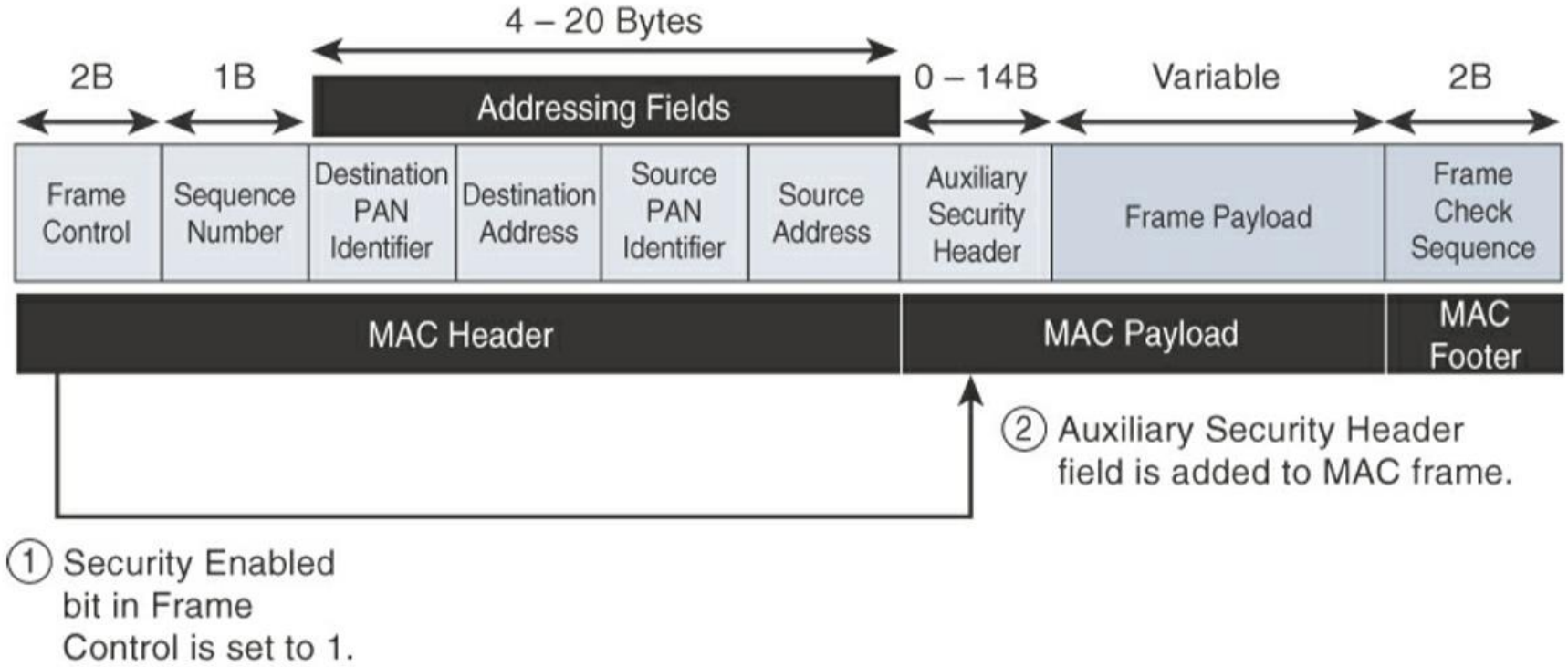


Figure 4-8 Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions

IEEE 802.15.4 - Security

- Security features of 802.15.4 slightly and consumes some of the payload.
- 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.

IEEE 802.15.4 - Competitive Technologies

- A competitive radio technology that is different in its PHY and MAC layers is DASH7.
  - DASH7 was originally based on the ISO18000-7 standard and positioned for industrial communications, whereas IEEE 802.15.4 is more generic.
- Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military forces for many years.
- Active RFID utilizes radio waves generated by a battery-powered tag on an object to enable continuous tracking.
- The current DASH7 technology offers low power consumption, a compact protocol stack, range up to 1 mile, and AES encryption.

IEEE 802.15.4g and 802.15.4e

- **IEEE 802.15.4e** enhanced the IEEE 802.15.4 MAC layer capabilities in the areas of
  - frame format, security, determinism mechanism, frequency hopping, reliability, unbounded latency, and multipath fading
  - improvements to better cope with certain application domains, such as factory and process automation and smart grid.

IEEE 802.15.4g and 802.15.4e

- **802.15.4g seeks** to optimize large outdoor wireless mesh networks for field area networks (FANs).
  - New PHY definitions are introduced, as well as some MAC modifications needed to support their implementation.
  - This focus of mainly on smart grid, smart utility network communication
  - Also used in IoT Applications like:
    - 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

- IEEE 802.15.4u defines the PHY layer characteristics for India (865–867 MHz).

IEEE 802.15.4g and 802.15.4e Standardization and Alliances

- 802.15.4g-2012 and 802.15.4e-2012 led to additional difficulty in achieving the interoperability between devices and mixed vendors that users requested.
- To guarantee interoperability, the Wi-SUN Alliance was formed. (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

Table 4-3 Industry Alliances for Some Common IEEE Standards

IEEE 802.15.4g and 802.15.4e Physical Layer

- In IEEE 802.15.4g
  - payload size of 127 bytes was increased for the SUN PHY to 2047 bytes.
    - This provides a better match for the greater packet sizes found in many upper-layer protocols
  - the error protection was improved by evolving the CRC from 16 to 32 bits.

IEEE 802.15.4g and 802.15.4e Physical Layer

- Data must be modulated onto the frequency using at least one of the following PHY mechanisms:
  - 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 (MRO-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.

IEEE 802.15.4g and 802.15.4e MAC Layer

- The following are some of the main enhancements to the MAC layer:
  - **Time-Slotted Channel Hopping (TSCH):**
    - Channel hopping, also known as frequency hopping, utilizes different channels for transmission at different times.
    - TSCH divides time into fixed time periods, or "time slots," which offer guaranteed bandwidth and predictable latency.
      - In a time slot, one packet and its acknowledgement can be transmitted, increasing network capacity because multiple nodes can communicate in the same time slot, using different channels.
      - A number of time slots are defined as a "slot frame," which is regularly repeated to provide "guaranteed access."
    - The transmitter and receiver agree on the channels and the timing for switching between channels through the combination of a global time slot counter and a global channel hopping sequence list, as computed on each node to determine the channel of each time slot.
    - TSCH adds robustness in noisy environments and smoother coexistence with other wireless technologies,

IEEE 802.15.4g and 802.15.4e MAC Layer

- **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.

- **Enhanced beacons (EBs):**
  - 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.

IEEE 802.15.4g and 802.15.4e MAC Layer

- **Enhanced beacon requests (EBRs):**
  - 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:**
  - 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 and 802.15.4e MAC Layer

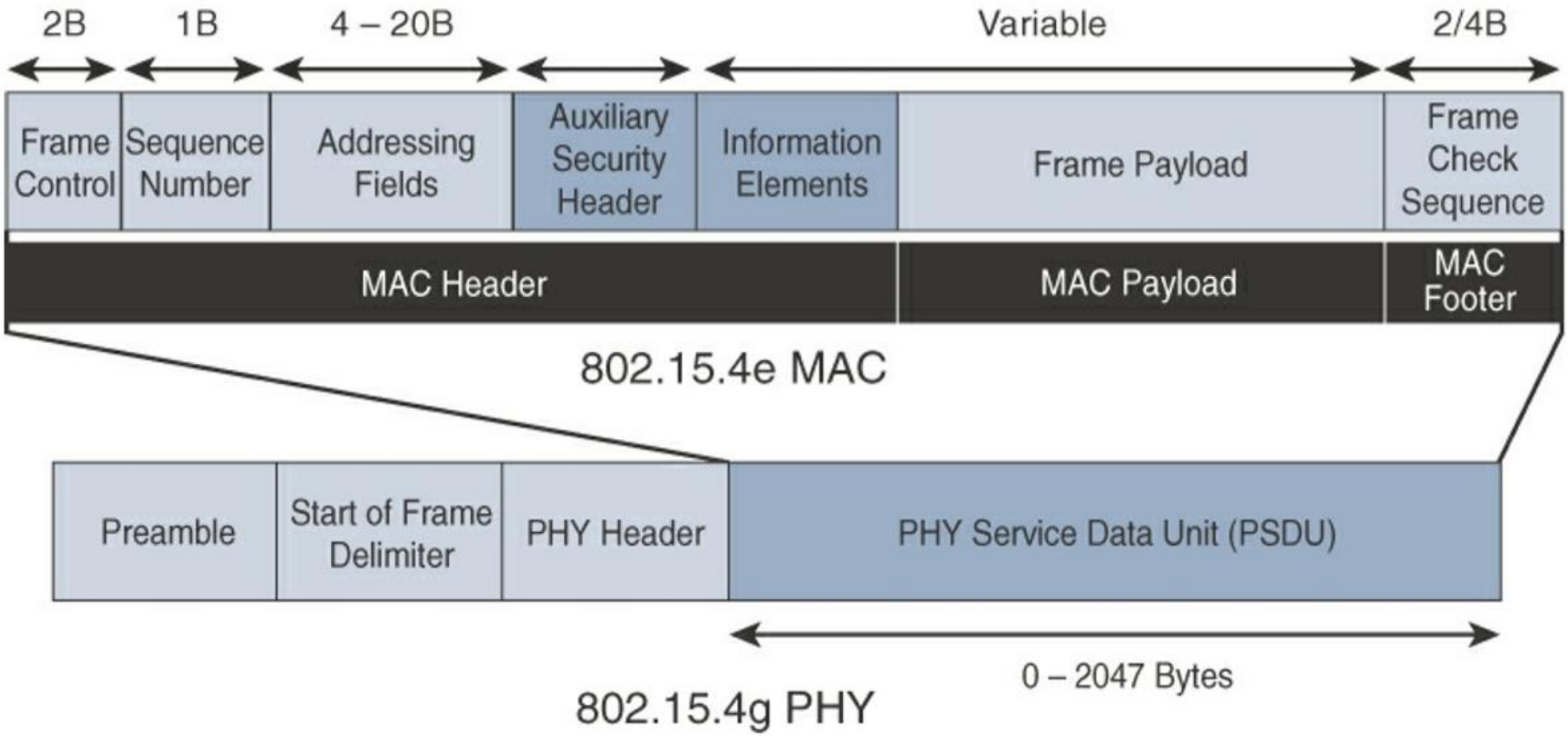


Figure 4-9 IEEE 802.15.4g/e MAC Frame Format

IEEE 802.15.4g and 802.15.4e MAC Layer

- 802.15.4g supporting payload up to 2047 bytes and 802.15.4 supporting payload only 127 bytes.
- The **Auxiliary Security header** provides for the encryption of the data frame.
  - This field is optionally supported in both 802.15.4e-2012 and 802.15.4.
- **IE field** contains one or more information elements that allow for additional information to be exchanged at the MAC layer.

IEEE 802.15.4g and 802.15.4e Topology

- Mesh topology.
  - This is because the best choice for use cases in the industrial and smart cities areas where 802.15.4g-2012 is applied.
  - A mesh topology allows deployments to be done in urban or rural areas, expanding the distance between nodes that can relay the traffic of other nodes.

IEEE 802.15.4g and 802.15.4e Security

- Encryption is provided by AES

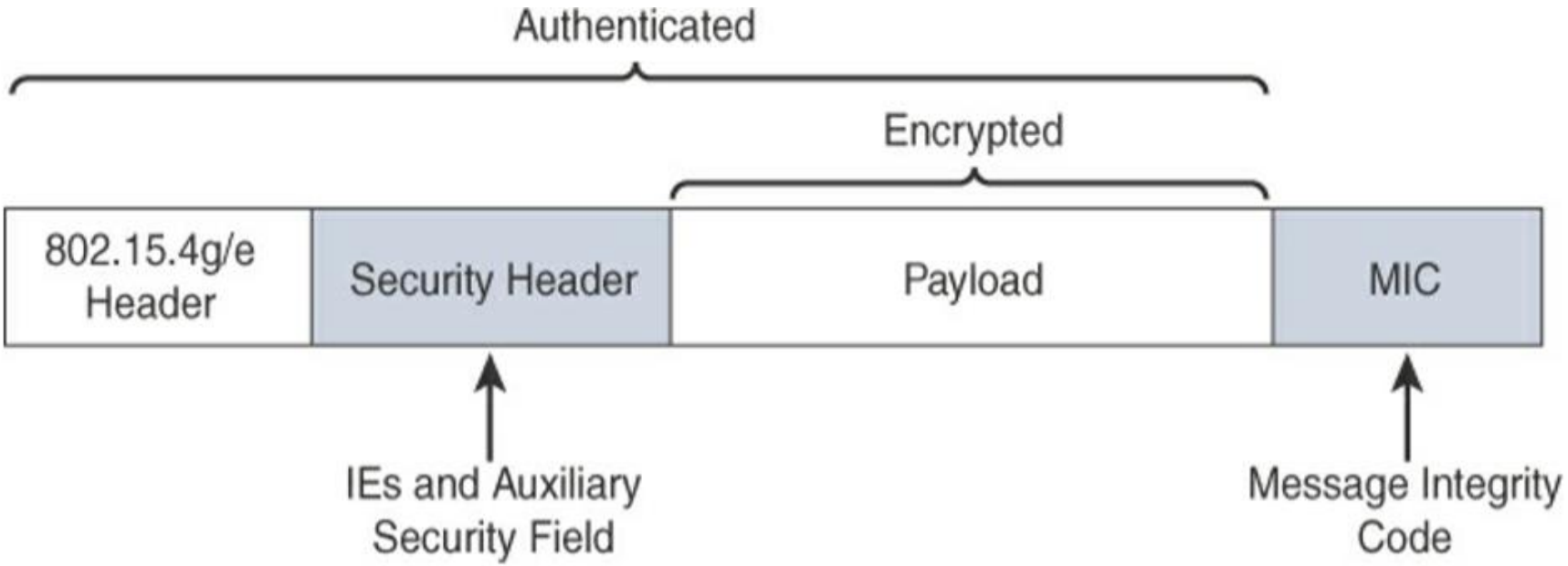


Figure 4-10 IEEE 802.15.4g/e MAC Layer Security

IEEE 802.15.4g and 802.15.4e Security

- The full frame in Figure 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
  - 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. Without key management support, weak keys are often the result, leaving the security system open to attack.

IEEE 802.15.4g and 802.15.4e Competitive Technologies

- Competitive technologies to IEEE 802.15.4g and 802.15.4e parallel the technologies that also compete with IEEE 802.15.4, such as DASH7

IEEE 1901.2a

- A wired technology
- Standard for Narrowband Power Line Communication (NB-PLC).
  - A narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power.

IEEE 1901.2a

- Applications like
  - 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.

IEEE 1901.2a Standardization and Alliances

- First generations of NB-PLC
  - Often suffered from poor reliability, low throughput (in the range of a few hundred bits per second to a maximum of 2 kbps), lack of manageability, and poor interoperability.
- Recent NB-PLC standards are based on orthogonal frequency-division multiplexing (OFDM).
  - Its interoperability
- IEEE 1901.2 working group standardized the NB-PLC PHY and MAC layers
- HomePlug Alliance
  - made the decision to offer the alliance's broadband power line networking technology to a broader audience by making its technical specifications publicly available.

https://hemanthrajhemu.github.io

IEEE 1901.2a Physical Layer

- NB-PLC is defined for frequency bands from 3 to 500 kHz.
- The IEEE 1901.2 standard includes (based on world regions):
  - European CENELEC A and B bands
    - European Committee for Electrotechnical Standardization (CENELEC)
    - A and B bands refer to 9–95 kHz and 95–125 kHz,
    - useful frequency due to its higher throughput and reduced interference.
  - US FCC-Low and FCC-above-CENELEC
    - Federal Communications Commission (FCC)
    - FCC-Low band encompasses 37.5–117.1875 kHz, and the FCC-above-CENELEC band is 154.6875–487.5 kHz.
  - Japan ARIB bands:
    - Association of Radio Industries and Businesses (ARIB)
    - frequency bands are ARIB 1, 37.5–117.1875 kHz, and ARIB 2, 154.6875–403.125 kHz.

IEEE 1901.2a Physical Layer

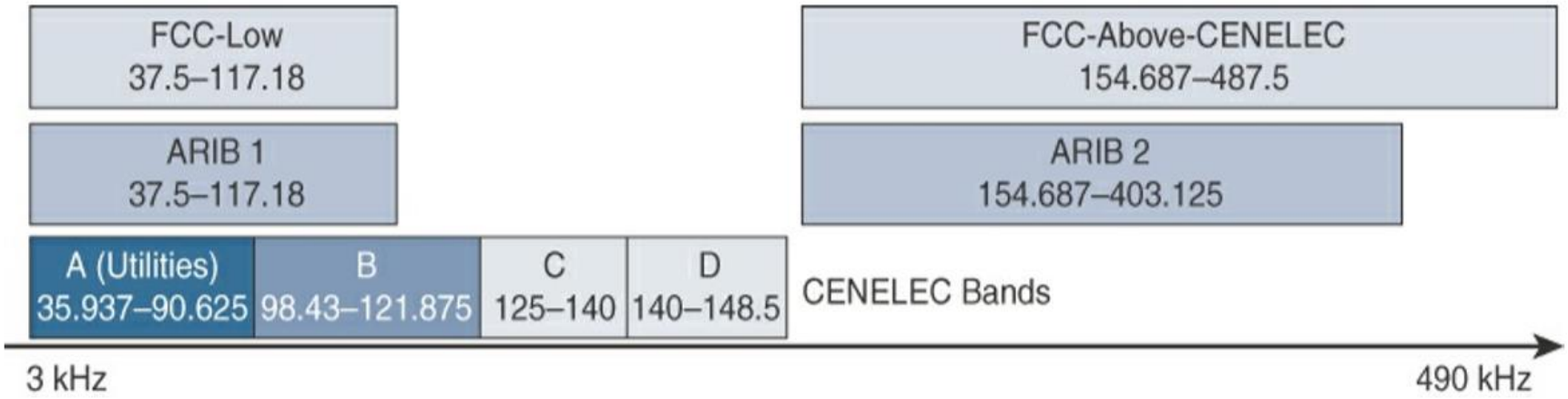


Figure 4-11 NB-PLC Frequency Bands

IEEE 1901.2a Physical Layer

- IEEE 1901.2a supports the largest set of coding technique:
  - Robust modulation (ROBO),
  - Differential binary phase shift keying (DBPSK),
  - Differential quadrature phase shift keying (DQPSK),
  - Differential 8-point phase shift keying (D8PSK)
  - 16 quadrature amplitude modulation (16QAM)
- IEEE 1901.2a, the data throughput rate has the ability to dynamically change, depending on the modulation type and tone map.
  - CENELEC A band, the data rate ranges from 4.5 kbps
    - in ROBO mode to 46 kbps with D8PSK modulation.
  - For the FCCabove-CENELEC frequencies, throughput varies from 21 kbps
    - in ROBO mode to a maximum of 234 kbps using D8PSK.
- Segmentation:
  - size of the MAC payload is too large to fit within one PHY service data unit (PSDU), the MAC payload is partitioned into smaller segments.

IEEE 1901.2a MAC Layer

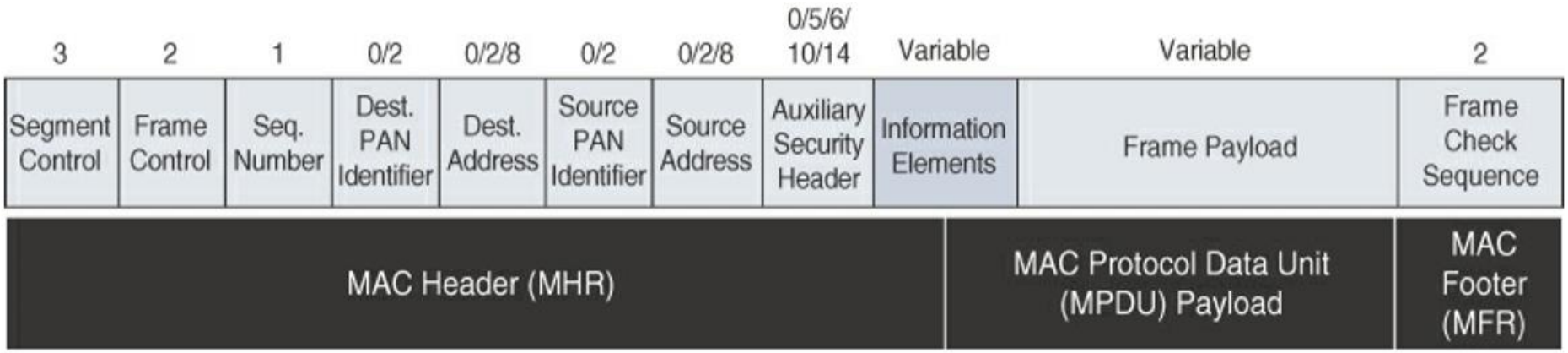


Figure 4-12 General MAC Frame Format for IEEE 1901.2

- IE support, IEEE 802.15.9 Key Management Protocol and SSID
- Segmentation or fragmentation of upper-layer packets with sizes larger than what can be carried in the MAC protocol data unit (MPDU).

IEEE 1901.2a Topology

- Use cases and Deployment topologies for IEEE 1901.2a are tied to the physical power lines.
- Mesh networks offer the advantage of devices relaying the traffic of other devices so longer distances can be segmented.
- The IEEE 1901.2a standard offers the flexibility to run any upper-layer protocol.
  - So, implementations of IPv6 6LoWPAN and RPL IPv6 protocols are supported

IEEE 1901.2a Topology

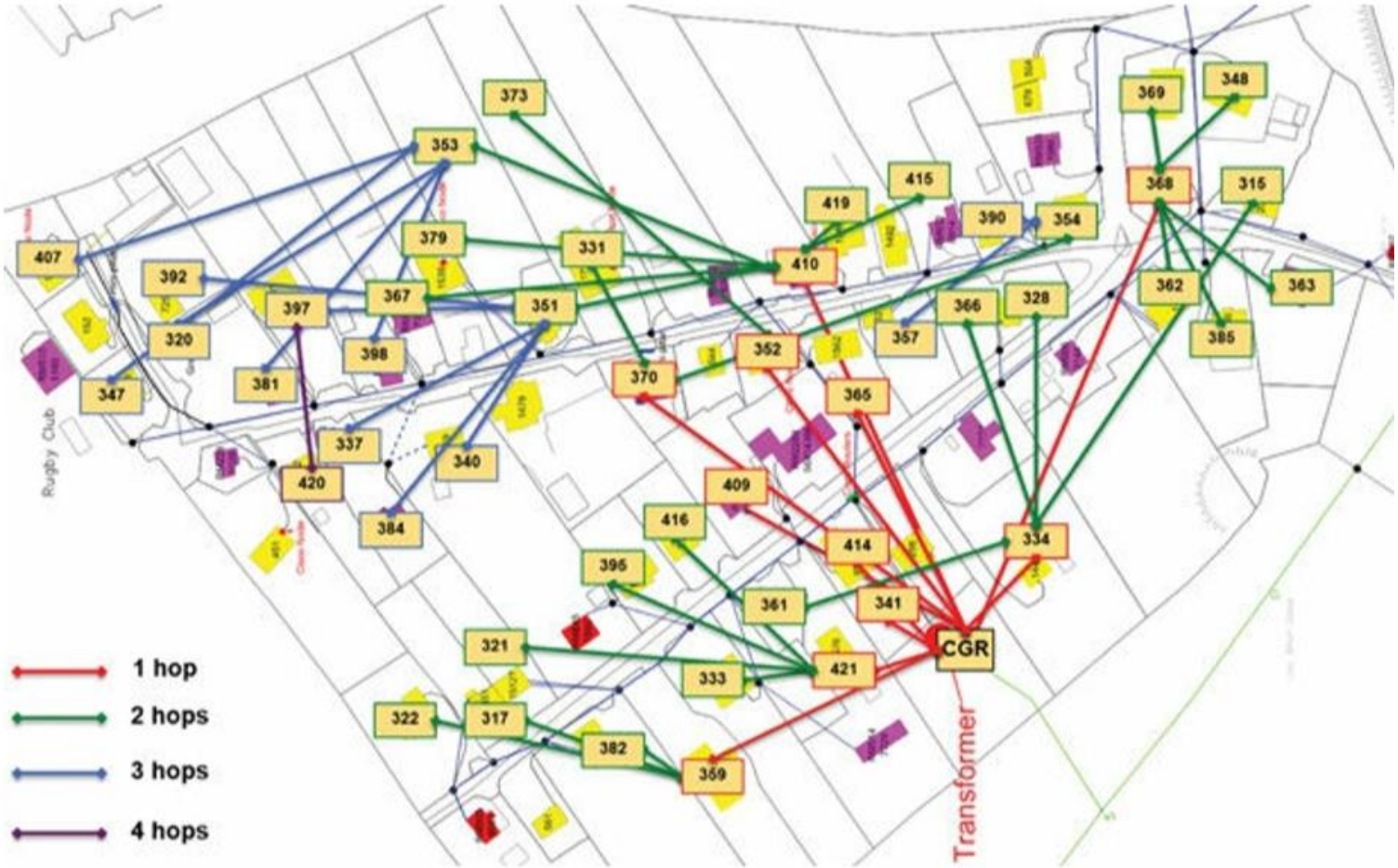


Figure 4-13 IPv6 Mesh in NB-PLC

https://hemanthrajhemu.github.io

IEEE 1901.2a Security

- Security offers similar features to IEEE 802.15.4g
- These differences are mostly tied to the PHY layer fragmentation capabilities of IEEE 1901.2a and include the following:
  - The Security Enabled bit in the Frame Control field should be set in all MAC frames carrying segments of an encrypted frame.
  - If data encryption is required, it should be done before packet segmentation. During packet encryption, the Segment Control field should not be included in the input to the encryption algorithm.
  - On the receiver side, the data decryption is done after packet reassembly.
  - When security is enabled, the MAC payload is composed of the ciphered payload and the message integrity code (MIC) authentication tag for non-segmented payloads. If the payload is segmented, the MIC is part of the last packet (segment) only. The MIC authentication is computed using only information from the MHR of the frame carrying the first segment.

IEEE 1901.2a Competitive Technologies

- In the domain of NB-PLC, two technologies compete against IEEE 1901.2a: G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904).
- G3-PLC
  - mandates data link layer protocol options for bootstrapping and allocating device addresses, and it is incompatible with IEEE 802.15.4g/e and an end-to-end IPv6 model.
  - PRIME is more like an ATM approach, with a Layer 7 protocol (that is, DLMS/COSEM) that runs directly on top of Layer 2. Adding IP support requires that Layer 3 protocols be added.

IEEE 802.11ah

- In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology.
- IoT wireless access technology, either for connecting endpoints such as fog computing nodes, high-data-rate sensors, and audio or video analytics devices or for deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments.

IEEE 802.11ah

- Applications like:
  - Sensors and meters covering a smart grid: Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors
  - Backhaul aggregation of industrial sensors and meter data: Potentially connecting IEEE 802.15.4g subnetworks
  - Extended range Wi-Fi: For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough

IEEE 802.11ah Standardization and Alliances

- The IEEE 802.11ah group called "industrial Wi-Fi"
- The 802.11ah specification would operate in unlicensed sub-GHz frequency bands and other LPWA technologies.
- Wi-Fi certifications and interoperability for 2.4 GHz and 5 GHz products is the Wi-Fi Alliance.
- Wi-Fi Alliance called Wi-Fi HaLow.
  - The HaLow brand exclusively covers IEEE 802.11ah for sub-GHz device certification.

IEEE 802.11ah Physical Layer

- IEEE 802.11ah essentially provides an additional 802.11 physical layer operating in unlicensed sub-GHz bands.
  - For example,
  - Following bands for IEEE 802.11ah:
  - 868–868.6 MHz for EMEAR,
  - 902–928 MHz and associated subsets for North America and Asia-Pacific regions,
  - 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779–787 MHz for China.

IEEE 802.11ah MAC Layer

- Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:
  - **Number of devices:** Has been scaled up to 8192 per access point.
  - **MAC header:** Has been shortened to allow more efficient communication.
  - **Null data packet (NDP) support:** Is extended to cover several control and management frames. Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided. This change makes the control frame exchanges efficient and less power-consuming for the receiving stations.
  - **Grouping and sectorization:** Enables an AP to use sector antennas and also group stations (distributing a group ID). In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window.

IEEE 802.11ah MAC Layer

- **Restricted access window (RAW):** Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access to the wireless network. By providing more efficient access to the medium, additional power savings for battery-powered devices can be achieved, and collisions are reduced.
- **Target wake time (TWT):** Reduces energy consumption by permitting an access point to define times when a device can access the network. This allows devices to enter a low-power state until their TWT time arrives. It also reduces the probability of collisions in large cells with many clients.
- **Speed frame exchange:** Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP). This reduces contention on the medium, minimizes the number of frame exchanges to improve channel efficiency, and extends battery life by keeping awake times short.

IEEE 802.11ah Topology

- While IEEE 802.11ah is deployed as a star topology, it includes a simple hops relay operation to extend its range.
- One 802.11ah device to act as an intermediary and relay data to another (like Mesh topology).

- Sectorization
  - is a technique that involves partitioning the coverage area into several sectors to get reduced contention within a certain sector.
  - Limiting collisions in cells that have many clients.
  - Coverage area of 802.11ah access points is large, and interference from neighboring access points is problematic.

IEEE 802.11ah Topology

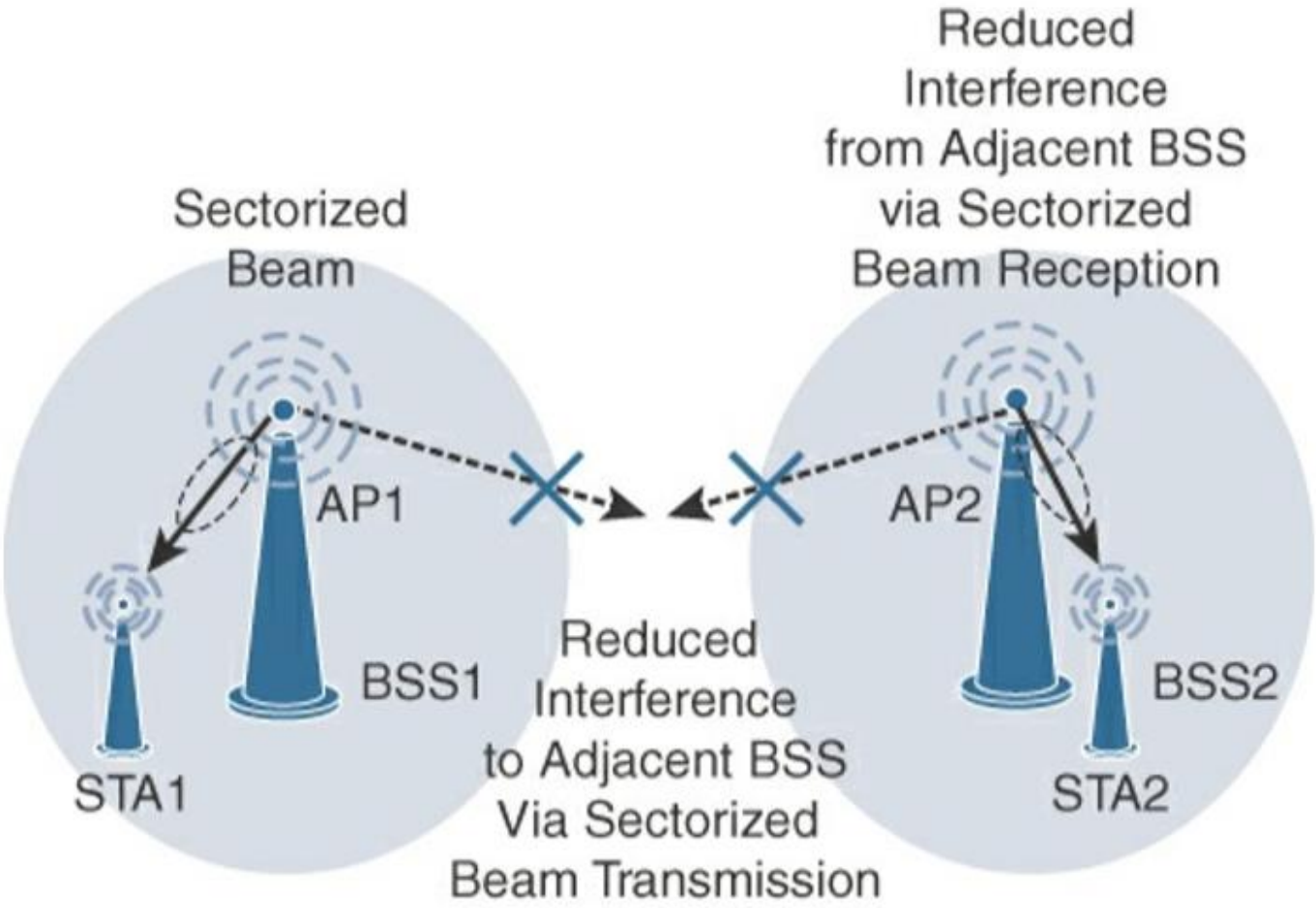


Figure 4-14 IEEE 802.11ah Sectorization

IEEE 802.11ah Security

- This include IEEE 802.15.4, IEEE 802.15.4e, and IEEE 1901.2a, and the security information for them is also applicable to IEEE 802.11ah.

IEEE 802.11ah Competitive Technologies

- Competitive technologies to IEEE 802.11ah are IEEE 802.15.4 and IEEE 802.15.4e,

LoRaWAN

- Long Range Wide-Area Network

LoRaWAN
Standardization and Alliances

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

LoRaWAN
Standardization and Alliances

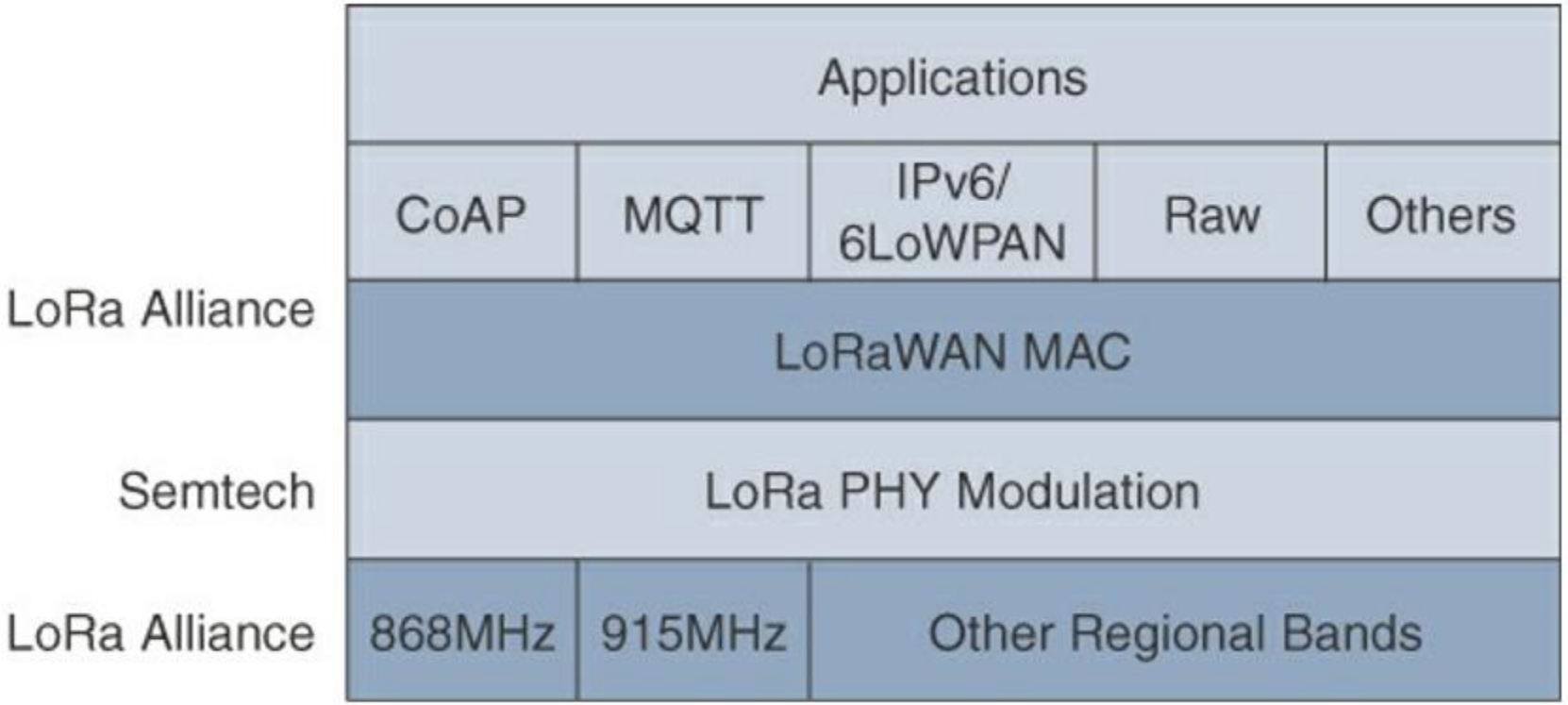


Figure 4-15 LoRaWAN Layers

LoRaWAN Physical Layer

- Semtech LoRa modulation
  - is based on chirp spread spectrum modulation,
    - which trades a lower data rate for receiver sensitivity to significantly increase the communication distance.
  - it allows demodulation below the noise floor,
  - offers robustness to noise and interference,
  - manages a single channel occupation by different spreading factors.
  - Enables LoRa devices to receive on multiple channels in parallel.

LoRaWAN Physical Layer

- 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 singlehop wireless connection to communicate with one or many gateways.

LoRaWAN Physical Layer

- 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.
    - Endpoints at the edge of the link budget communicate at the lowest data rate and highest transmit power.

- 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.

LoRaWAN Physical Layer

Configuration	863–870 MHz bps	902–928 MHz bps
LoRa: SF12/125 kHz	250	N/A
LoRa: SF11/125 kHz	440	N/A
LoRa: SF10/125 kHz	980	980
LoRa: SF9/125 kHz	1760	1760
LoRa: SF8/125 kHz	3125	3125
LoRa: SF7/125 kHz	5470	5470
LoRa: SF7/250 kHz	11,000	N/A
FSK: 50 kbps	50,000	N/A
LoRa: SF12/500 kHz	N/A	980
LoRa: SF11/500 kHz	N/A	1760
LoRa: SF10/500 kHz	N/A	3900
LoRa: SF9/500 kHz	N/A	7000
LoRa: SF8/500 kHz	N/A	12,500
LoRa: SF7/500 kHz	N/A	21,900

Table 4-4 LoRaWAN Data Rate Example

LoRaWAN MAC Layer

- The MCA 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.
- There are three classes of LoRaWAN devices:
  - **Class A: This class is the default implementation.** Optimized for battery-powered nodes, 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".** 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 MAC Layer

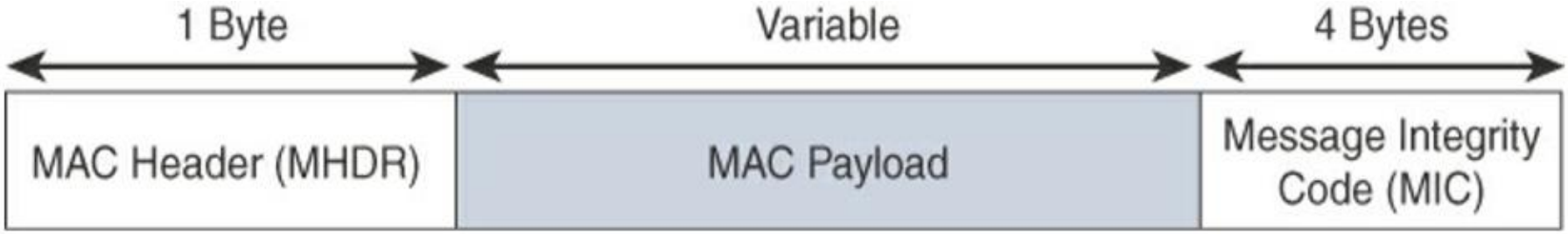


Figure 4-16 High-Level LoRaWAN MAC Frame Format

- 1byte 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

LoRaWAN MAC Layer

- 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.

LoRaWAN Topology

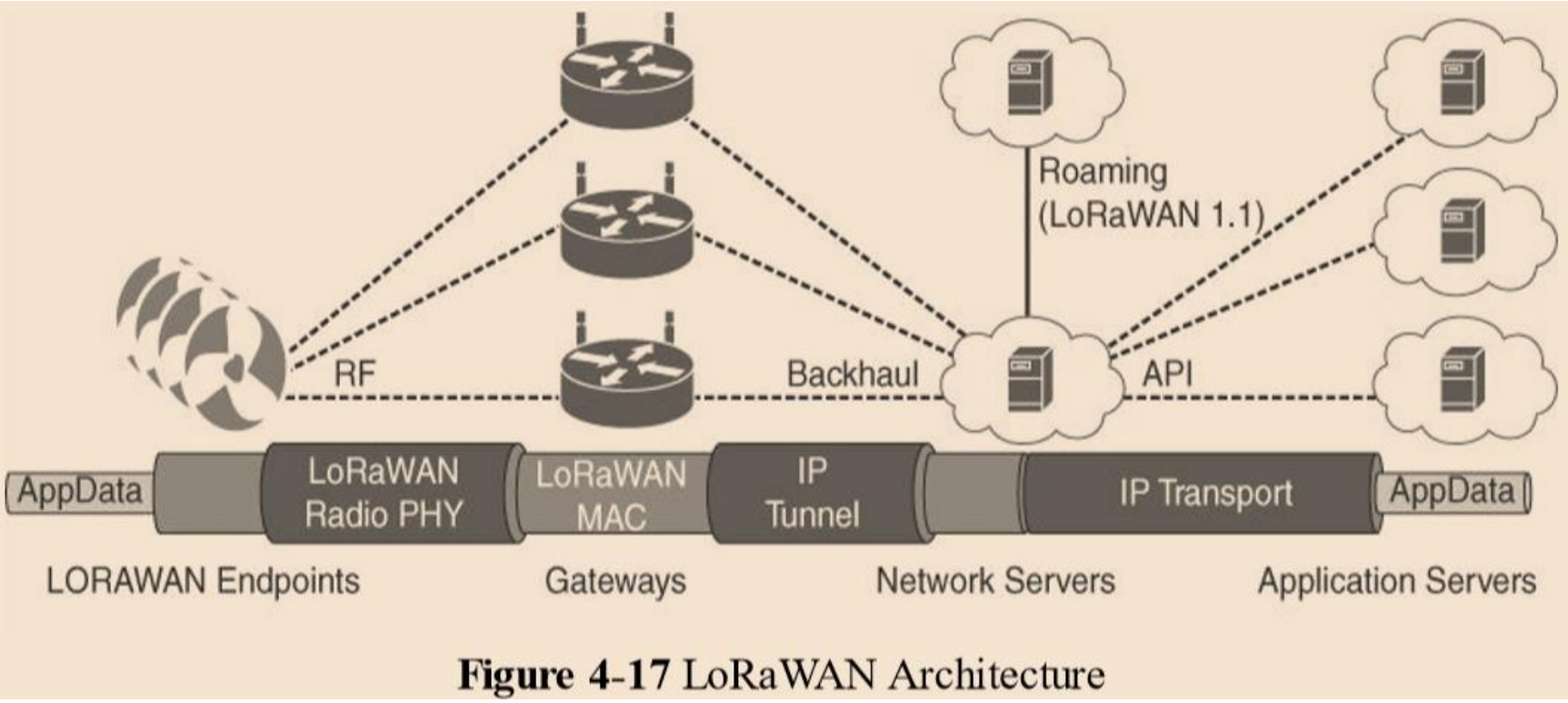


Figure 4-17 LoRaWAN Architecture

LoRaWAN Topology

- A "star of stars" topology
- The infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server.
- Gateways connect to the backend network using standard IP connections, and endpoints communicate directly with one or more gateways
- LoRaWAN gateways act as bridges that relay between endpoints and the network servers.
  - Multiple gateways can receive and transport the same packets. When duplicate packets are received, de-duplication is a function of the network server.
- The LoRaWAN network server manages the data rate and radio frequency (RF) of each endpoint through the adaptive data rate (ADR) algorithm.

LoRaWAN Topology

- LoRaWAN endpoints transport their selected application data over the LoRaWAN MAC layer on top of one of the supported PHY layer frequency bands.
- The application data is contained in upper protocol layers.
- These upper layers could just be raw data on top of the LoRaWAN MAC layer, or the data could be stacked in multiple protocols.
  - For example, upper-layer protocols,
  - ZigBee Control Layer (ZCL), Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), or with/without IPv6/6LoWPAN layer.

LoRaWAN Security

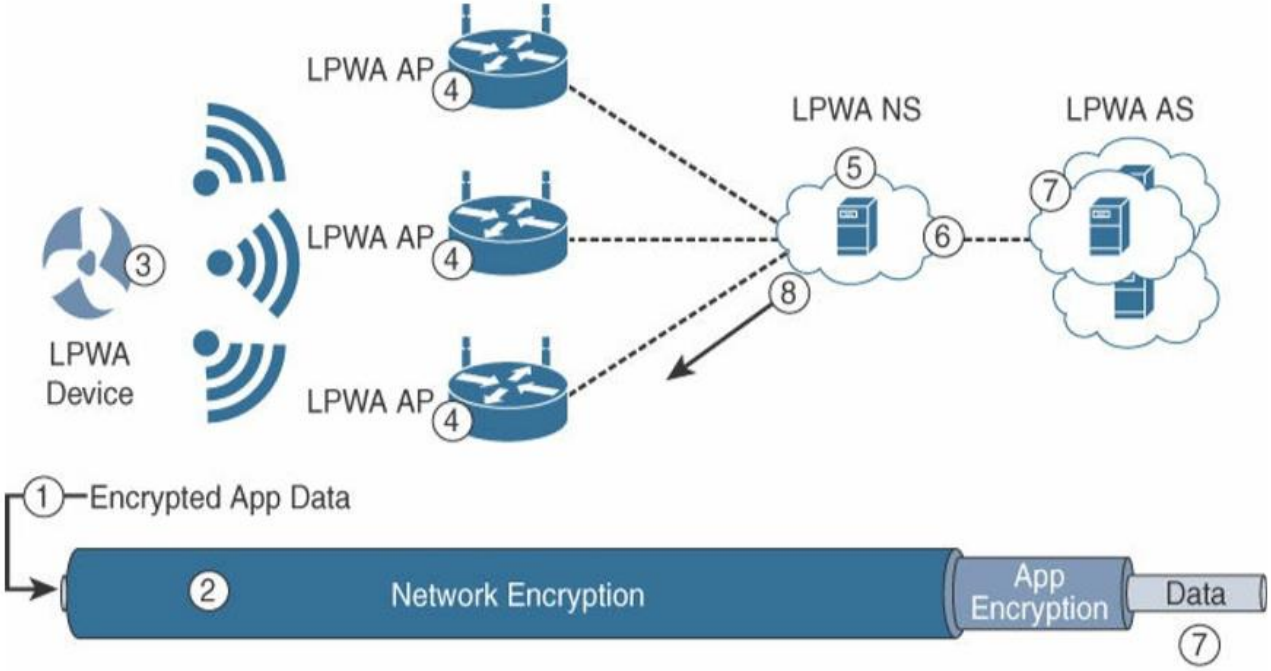


Figure 4-18 LoRaWAN Security

LoRaWAN Security

- LoRaWAN endpoints must implement two layers of security,
  - Protecting communications
  - Data privacy across the network.

LoRaWAN Security

- **Protecting communications**
  - Also called "network security" but applied at the MAC layer,
  - guarantees the authentication of the endpoints by the LoRaWAN network server.
  - 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.

LoRaWAN Security

- **Data privacy :**
  - An application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server.
  - It computes and checks the application-level MIC, if included.
    - This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access.
  - Endpoints receive their AES-128 application key (AppKey) from the application owner.
    - This key is most likely derived from an application-specific root key exclusively known to and under the control of the application provider.

LoRaWAN Security

- 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.

LoRaWAN
Competitive Technologies

- LPWA solutions and technologies are split between unlicensed and licensed bands.
- The licensed-band technologies are dedicated to mobile service providers.

LoRaWAN 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
Geolocation	Yes (LoRa GW version 2 reference design)	No	No
Roaming	Yes (LoRaWAN 1.1)	No	Yes
Specifications	LoRA Alliance	Proprietary	Proprietary

Table 4-5 Unlicensed LPWA Technology Comparison

NB-IoT and Other LTE Variations

- Existing cellular technologies, (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 device, the aim was to both align with specific IoT requirements, such as low throughput and low power consumption, and decrease the complexity and cost of the LTE devices.
- This resulted in the definition of the LTE-M work item.
- NB-IoT specifically addresses the requirements of a massive number of low-throughput devices, low device power consumption, improved indoor coverage, and optimized network architecture.

NB-IoT and Other LTE Variations Standardization and Alliances

- The 3GPP organization includes multiple working groups focused on many different aspects of telecommunications (for example, radio, core, terminal, and so on).
- Aligned with 3G, LTE, or GSM, the IoT-related contribution is handled by either 3GPP or the GSM EDGE Radio Access Networks (GERAN) group.

NB-IoT and Other LTE Variations

LTE Cat 0

- A new user equipment (UE) category, Category 0,
- with devices running at a maximum data rate of 1 Mbps, supported by both the network and end devices, operate in existing LTE systems with bandwidths up to 20 MHz.
  - **Cat 0 characteristics**
  - **Power saving mode (PSM):**
    - This new device status minimizes energy consumption. Energy consumption is expected to be lower with PSM than with existing idle mode. 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 reestablish its network connection.
  - **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.

NB-IoT and Other LTE Variations
LTE-M

- These are the main characteristics of the LTE-M:
  - 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. A paging cycle is a periodic check-in with the network. This extended "sleep" time between paging cycles extends the battery lifetime for an endpoint significantly.

NB-IoT and Other LTE Variations

NB-IoT:

- The work on NB-IoT started with multiple proposals pushed by the involved vendors, including the following:
  - Extended Coverage GSM (EC-GSM), Ericsson proposal
  - Narrowband GSM (N-GSM), Nokia proposal
  - Narrowband M2M (NB-M2M), Huawei/Neul proposal
  - Narrowband OFDMA (orthogonal frequency-division multiple access), Qualcomm proposal
  - Narrowband Cellular IoT (NB-CIoT), combined proposal of NB-M2M and NBOFDMA
  - Narrowband LTE (NB-LTE), Alcatel-Lucent, Ericsson, and Nokia proposal
  - Cooperative Ultra Narrowband (C-UNB), Sigfox proposal

NB-IoT and Other LTE Variations

NB-IoT:

- Three modes of operation are applicable to NB-IoT:
- Standalone:
  - A GSM carrier is used as an NB-IoT carrier, enabling reuse of 900 MHz or 1800 MHz.
- In-band:
  - Part of an LTE carrier frequency band is allocated for use as an NB-IoT frequency. The service provider typically makes this allocation, and IoT devices are configured accordingly.
- Guard band:
  - An NB-IoT carrier is between the LTE or WCDMA bands. This requires coexistence between LTE and NB-IoT bands.

NB-IoT and Other LTE Variations Topology

- NB-IoT is defined with a link budget of 164 dB; compare this with the GPRS link budget of 144 dB, used by many machine-to-machine services.

NB-IoT and Other LTE Variations Competitive Technologies

- In licensed bands, it is expected that 3GPP NB-IoT will be the adopted LPWA technology when it is fully available.

Main Characteristics of different Access Technologies

Characteristic	IEEE 802.15.4	IEEE 802.15.4g and IEEE 802.15.4e	IEEE 1901.2a	IEEE 802.11ah	LoRaWAN	NB-IoT
Wired or wireless	Wireless	Wireless	Wired	Wireless	Wireless	Wireless
Frequency bands	Unlicensed 2.4 GHz and sub-GHz	Unlicensed 2.4 GHz and sub-GHz	Unlicensed CENELEC A and B, FCC, ARIB	Unlicensed sub-GHz	Unlicensed sub-GHz	Licensed
Topology	Star, mesh	Star, mesh	Mesh	Star	Star	Star
Range	Medium	Medium	Medium	Medium	Long	Long
Data rate	Low	Low	Low	Low–high	Low	Low

FUTURE VISION BIE

By K B Hemanth Raj

Visit : https://hemanthrajhemu.github.io

Quick Links for Faster Access.

CSE 8th Semester - https://hemanthrajhemu.github.io/CSE8/

ISE 8th Semester - https://hemanthrajhemu.github.io/ISE8/

ECE 8th Semester - https://hemanthrajhemu.github.io/ECE8/

8th Semester CSE - TEXTBOOK - NOTES - QP - SCANNER & MORE

17CS81 IOT - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS81/

17CS82 BDA - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS82/

17CS832 UID - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS832/

17CS834 SMS - https://hemanthrajhemu.github.io/CSE8/17SCHEME/17CS834/

8th Semester Computer Science & Engineering (CSE)

8th Semester CSE Text Books: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Text-Book.html

8th Semester CSE Notes: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Notes.html

8th Semester CSE Question Paper: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Question-Paper.html

8th Semester CSE Scanner: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Scanner.html

8th Semester CSE Question Bank: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Question-Bank.html

8th Semester CSE Answer Script: https://hemanthrajhemu.github.io/CSE8/17SCHEME/Answer-Script.html

Contribution Link:

https://hemanthrajhemu.github.io/Contribution/

Stay Connected... get Updated... ask your queries...

Join Telegram to get Instant Updates:
https://telegram.me/joinchat/AAAAAFTtp8kuvCHALxuMaQ

Contact: MAIL: futurevisionbie@gmail.com

INSTAGRAM: www.instagram.com/futurevisionbie/