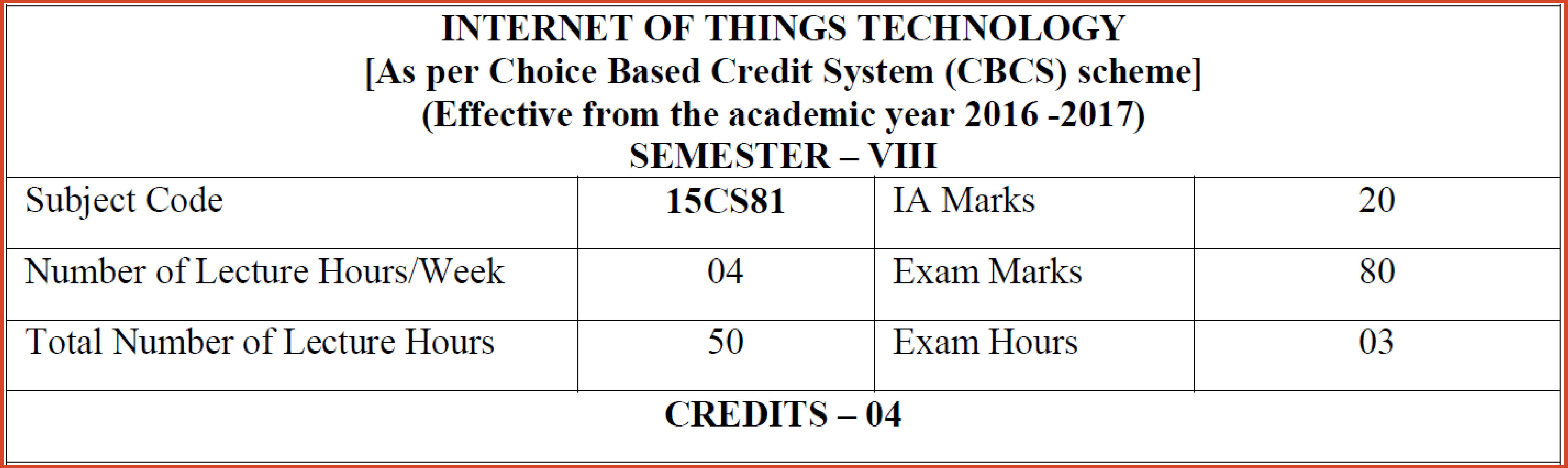


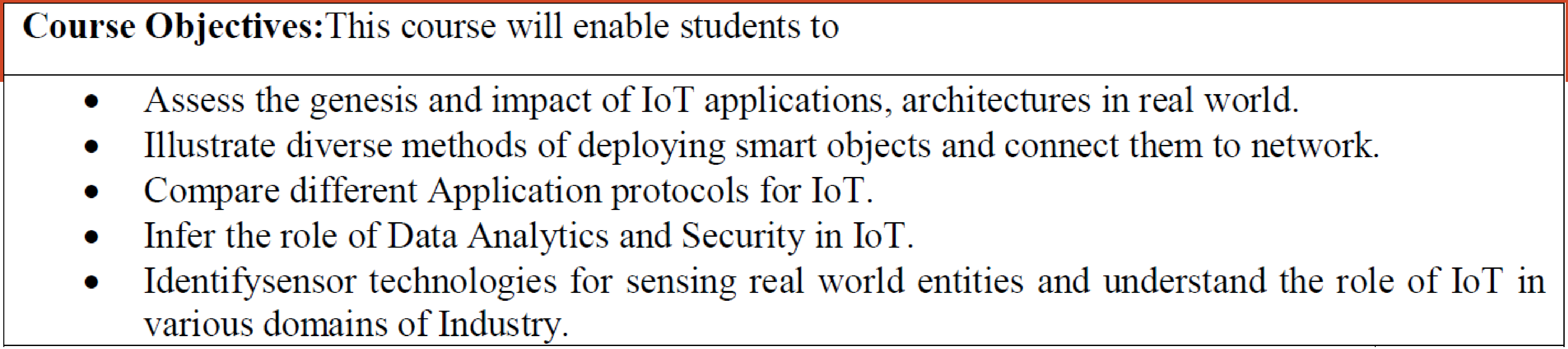
INTERNET OF THINGS TECHNOLOGY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – VIII

Subject Code	**15CS81**	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

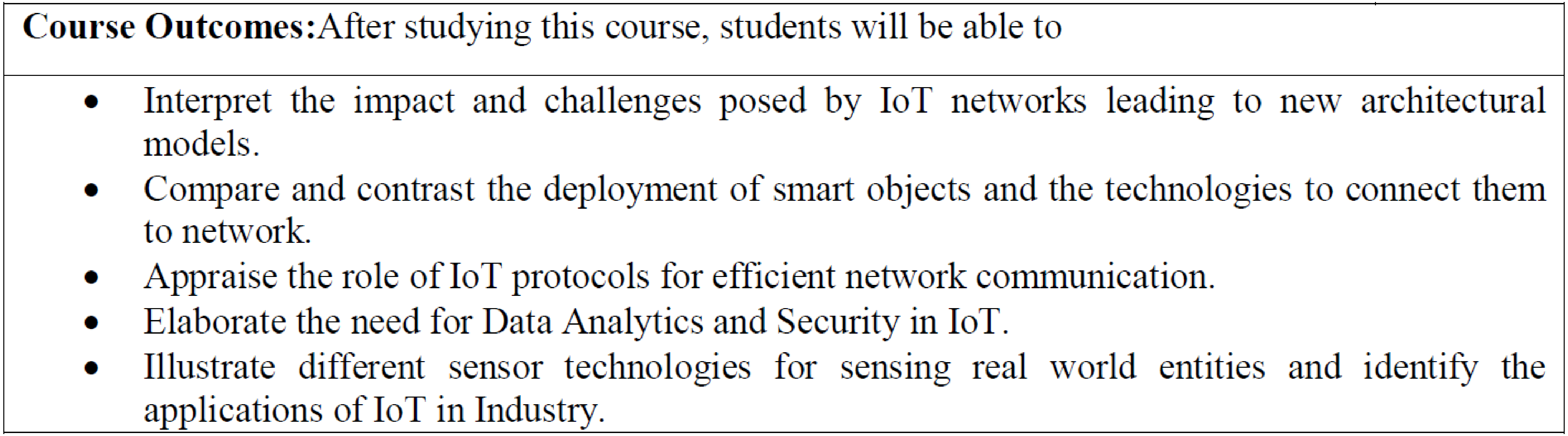
HKBK COLLEGE OF ENGINEERING, BENGALURU

Syllabus- Internet Of Things Technology



Course Objectives: This course will enable students to

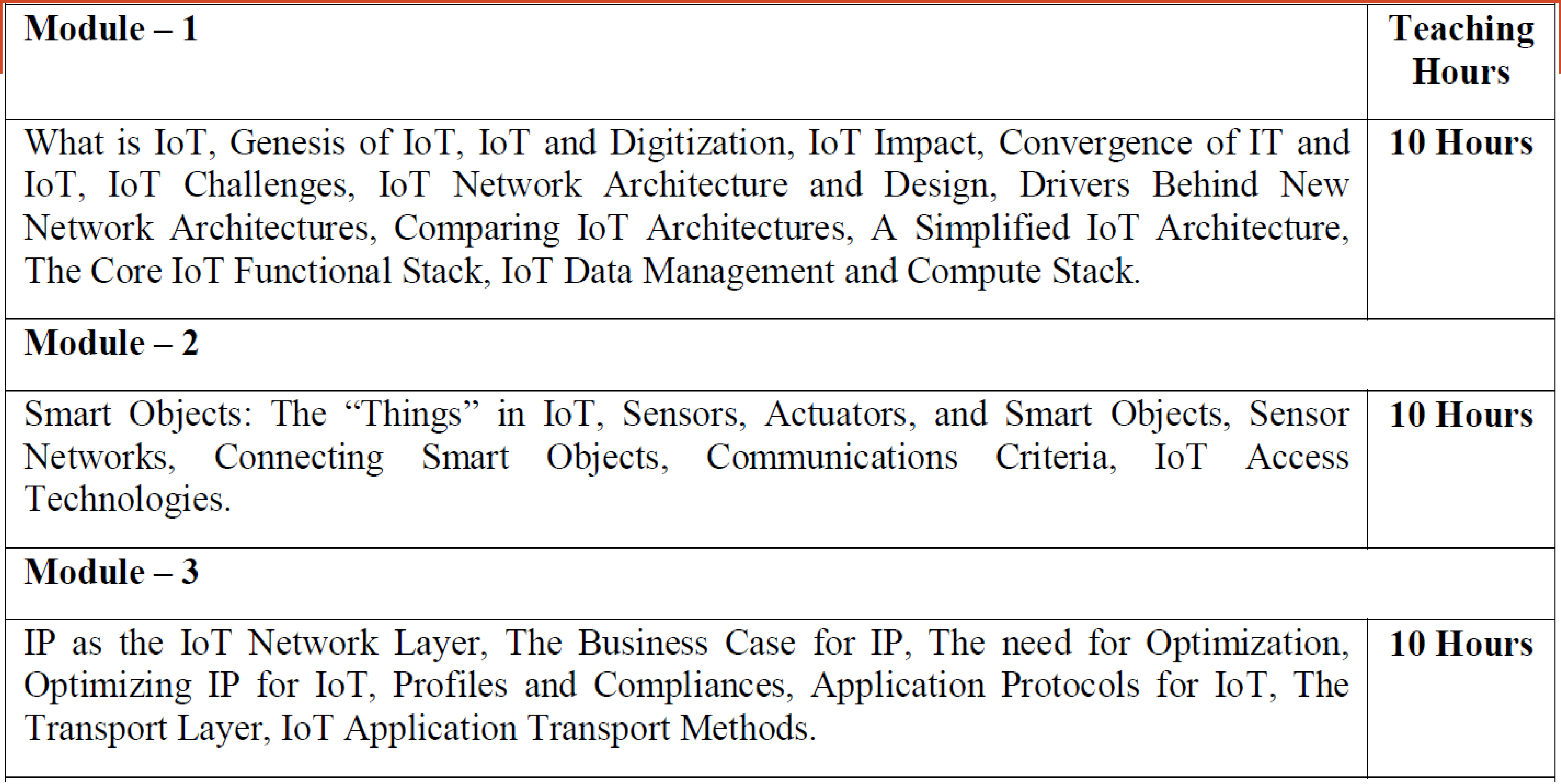
- Assess the genesis and impact of IoT applications, architectures in real world.
- Illustrate diverse methods of deploying smart objects and connect them to network.
- Compare different Application protocols for IoT.
- Infer the role of Data Analytics and Security in IoT.
- Identifysensor technologies for sensing real world entities and understand the role of IoT in various domains of Industry.



Course Outcomes: After studying this course, students will be able to

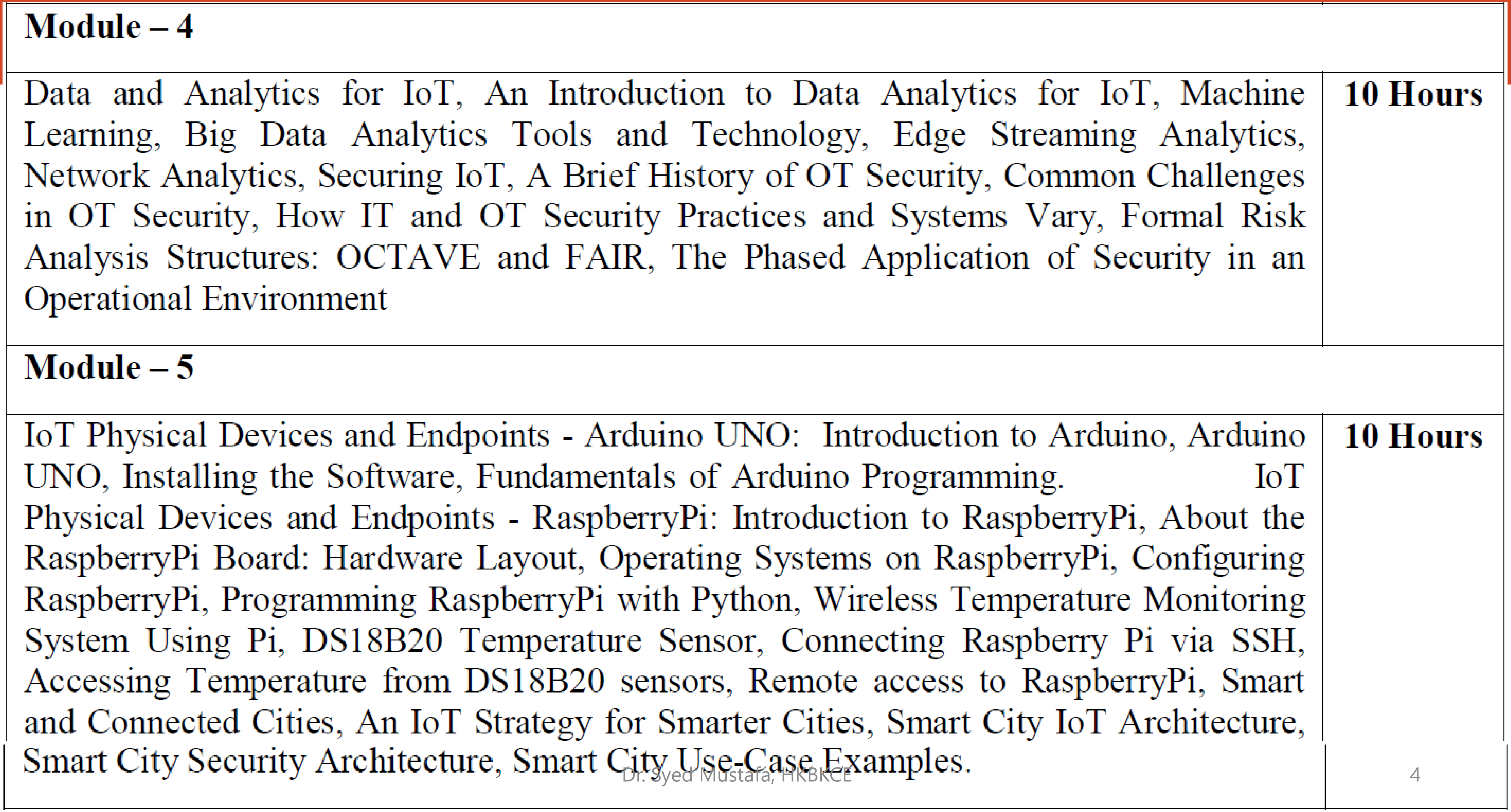
- Interpret the impact and challenges posed by IoT networks leading to new architectural models.
- Compare and contrast the deployment of smart objects and the technologies to connect them to network.
- Appraise the role of IoT protocols for efficient network communication.
- Elaborate the need for Data Analytics and Security in IoT.
- Illustrate different sensor technologies for sensing real world entities and identify the applications of IoT in Industry.

Syllabus- Internet Of Things Technology



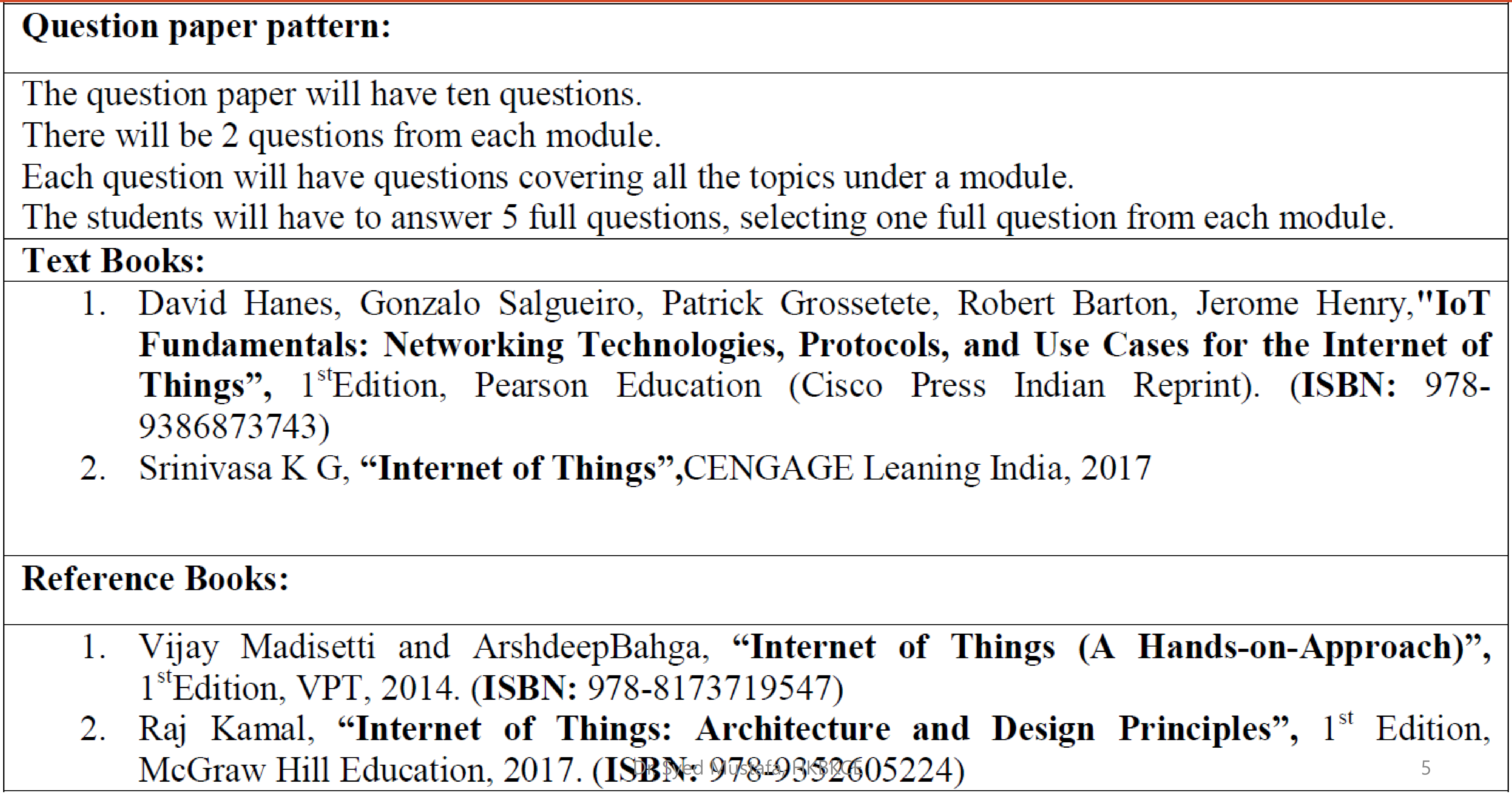
Module – 1	**Teaching Hours**
What is IoT, Genesis of IoT, IoT and Digitization, IoT Impact, Convergence of IT and IoT, IoT Challenges, IoT Network Architecture and Design, Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack.	**10 Hours**
Module – 2	
Smart Objects: The “Things” in IoT, Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access Technologies.	**10 Hours**
Module – 3	
IP as the IoT Network Layer, The Business Case for IP, The need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT, The Transport Layer, IoT Application Transport Methods.	**10 Hours**

Syllabus- Internet Of Things Technology



Module – 4	
Data and Analytics for IoT, An Introduction to Data Analytics for IoT, Machine Learning, Big Data Analytics Tools and Technology, Edge Streaming Analytics, Network Analytics, Securing IoT, A Brief History of OT Security, Common Challenges in OT Security, How IT and OT Security Practices and Systems Vary, Formal Risk Analysis Structures: OCTAVE and FAIR, The Phased Application of Security in an Operational Environment	**10 Hours**
Module – 5	
IoT Physical Devices and Endpoints - Arduino UNO: Introduction to Arduino, Arduino UNO, Installing the Software, Fundamentals of Arduino Programming. IoT Physical Devices and Endpoints - RaspberryPi: Introduction to RaspberryPi, About the RaspberryPi Board: Hardware Layout, Operating Systems on RaspberryPi, Configuring RaspberryPi, Programming RaspberryPi with Python, Wireless Temperature Monitoring System Using Pi, DS18B20 Temperature Sensor, Connecting Raspberry Pi via SSH, Accessing Temperature from DS18B20 sensors, Remote access to RaspberryPi, Smart and Connected Cities, An IoT Strategy for Smarter Cities, Smart City IoT Architecture, Smart City Security Architecture, Smart City Use-Case Examples.	**10 Hours**

Syllabus- Internet Of Things Technology



Question paper pattern:
The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.
Text Books:
1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry,**"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things"**, 1stEdition, Pearson Education (Cisco Press Indian Reprint). (**ISBN:** 978-9386873743) 2. Srinivasa K G, **"Internet of Things"**,CENGAGE Leaning India, 2017
Reference Books:
1. Vijay Madisetti and ArshdeepBahga, **"Internet of Things (A Hands-on-Approach)"**, 1stEdition, VPT, 2014. (**ISBN:** 978-8173719547) 2. Raj Kamal, **"Internet of Things: Architecture and Design Principles"**, 1st Edition, McGraw Hill Education, 2017. (**ISBN:** 978-9352605224)

Evaluation

- **Grade Percentage**
  - **S : 90% and above**
  - **A : 80% - 89%**
  - **B : 70% - 79%**
  - **F : less than 40%**

- **Syllabus Coverage Schedule**
  - **1st IA Test : 30% [Portion- first 1.5 Units]**
  - **2nd IA Test : 40% [Portion- next 2 Units]**
  - **3rd IA Test : 30% [Portion- Last 1.5 Units]**

Evaluation

- **Assignments**
  - **Total : 3**
  - **Each Assignment to be submitted before the IA test begins**

- **Attendance**
  - **Class Participation: 85%**

- **You may get detained if you miss (more than) ¼ of the whole classes**

- **Academic dishonesty (e.g. cheating, copying, late coming and etc.) will be taken seriously**

Announcement

Class Website

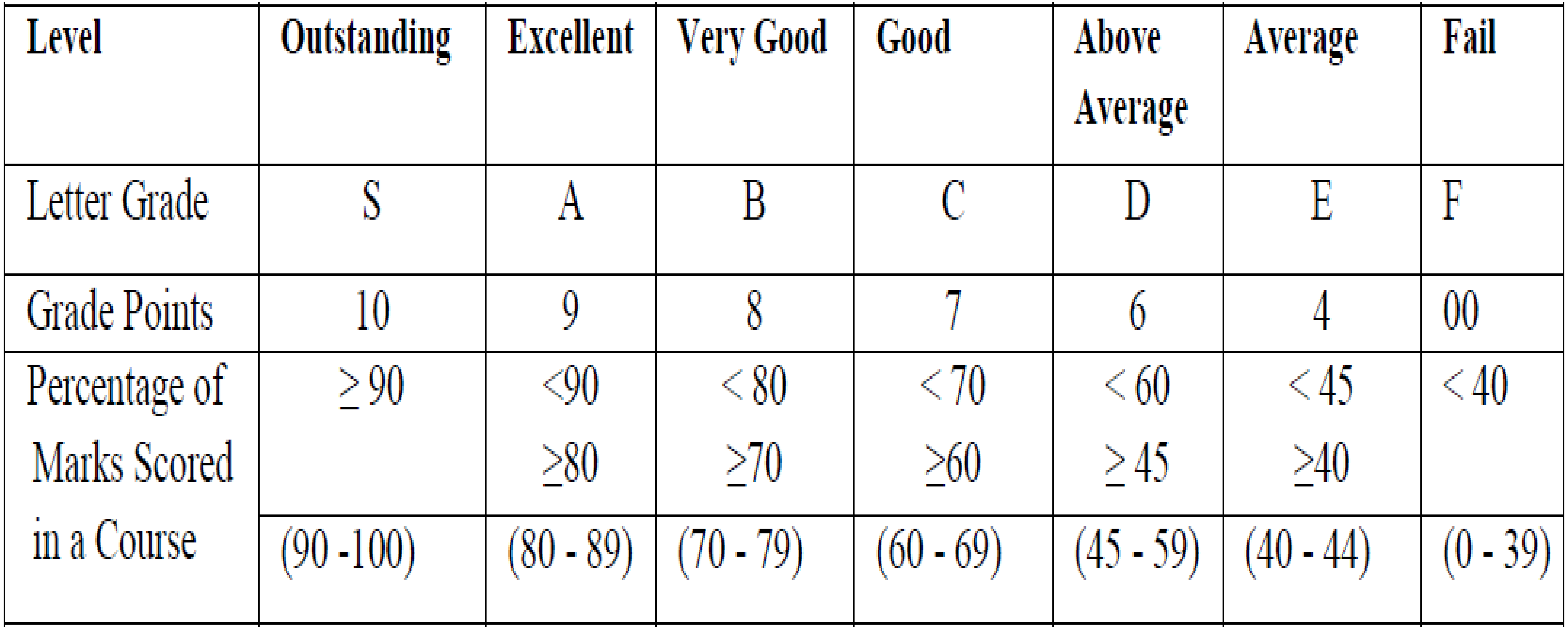
The link for the CMS portal is:

- **http://gg.gg/hkbkis or Google class room**

- **Class information such as lecture notes can be accessible through this website**

- **We will also use Moodle for online test**

Announcement



Level	Outstanding	Excellent	Very Good	Good	Above Average	Average	Fail
Letter Grade	S	A	B	C	D	E	F
Grade Points	10	9	8	7	6	4	00
Percentage of Marks Scored in a Course	≥ 90	<90 ≥80	< 80 ≥70	< 70 ≥60	< 60 ≥ 45	< 45 ≥40	< 40
	(90 -100)	(80 - 89)	(70 - 79)	(60 - 69)	(45 - 59)	(40 - 44)	(0 - 39)

Module – 2 Smart Objects: The “Things” in IoT

Smart Objects: The “Things” in IoT:

Sensors, Actuators, and Smart Objects:

- **This sections describe the capabilities, characteristics, and functionality of sensors and actuators.**
- **It gives detail how the economic and technical conditions are finally right for IoT to flourish.**

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- **A sensor 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 provide superhuman sensory capabilities**
- **Sensors can be readily embedded in any physical objects that are easily connected to the Internet by wired or wireless networks**

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- ➢ **There are a number of ways to group and cluster sensors into different categories, they are:**

1. Active or passive

2. Invasive or non-invasive

3. Contact or no-contact

4. Absolute or relative

5. Area of application

6. How sensors measure

7. What sensors measure:

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

1. **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).

2. **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).

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

3. 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).

4. 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).

Module – 2 Smart Objects: The "Things" in IoT

Sensors:

5. Area of application:

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

6. How sensors measure:

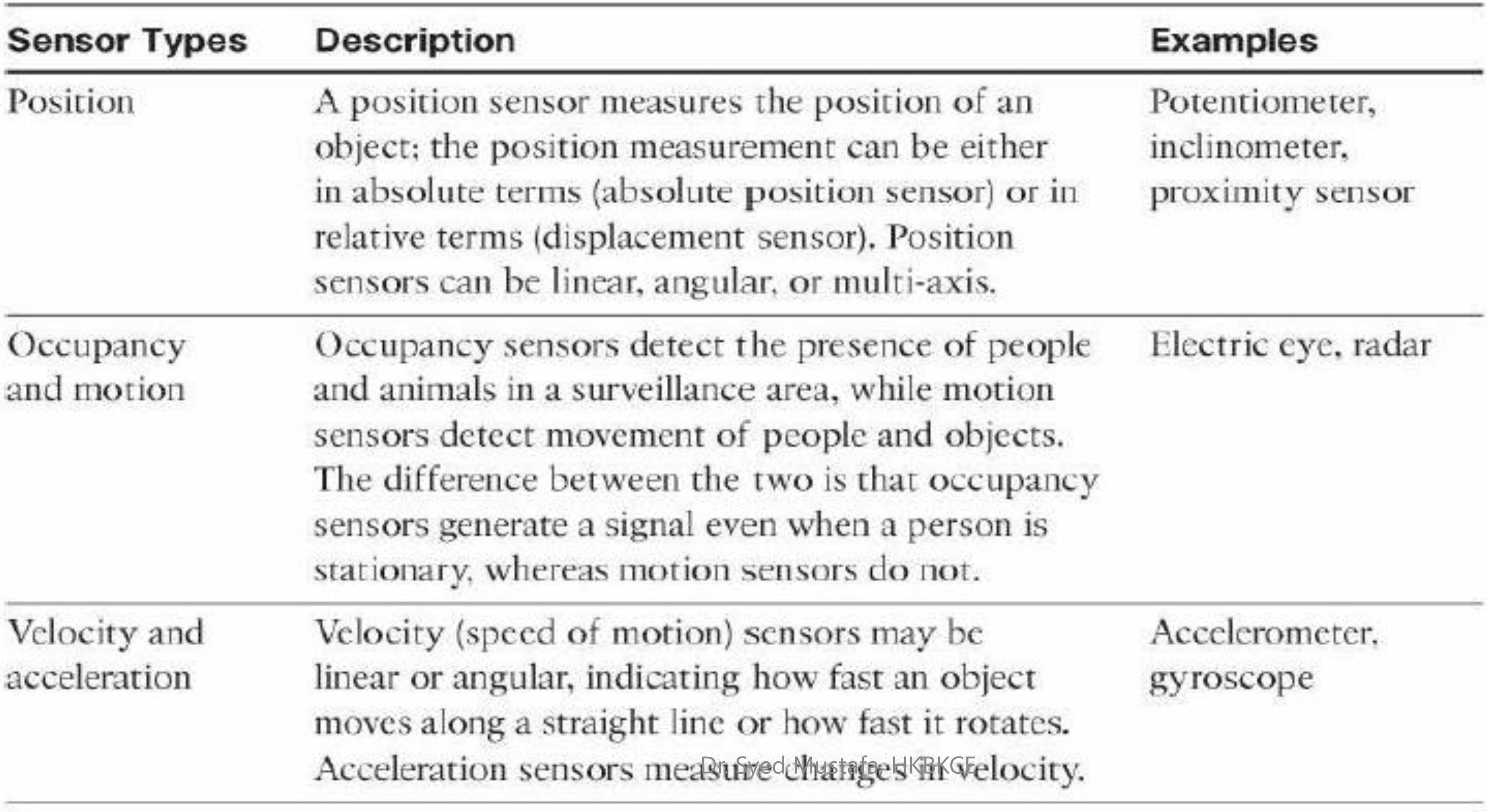
Sensors can be categorized based on the physical mechanism used to measure sensory input (for example, thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photoelastic).

7. What sensors measure:

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

Module – 2 Smart Objects: The “Things” in IoT

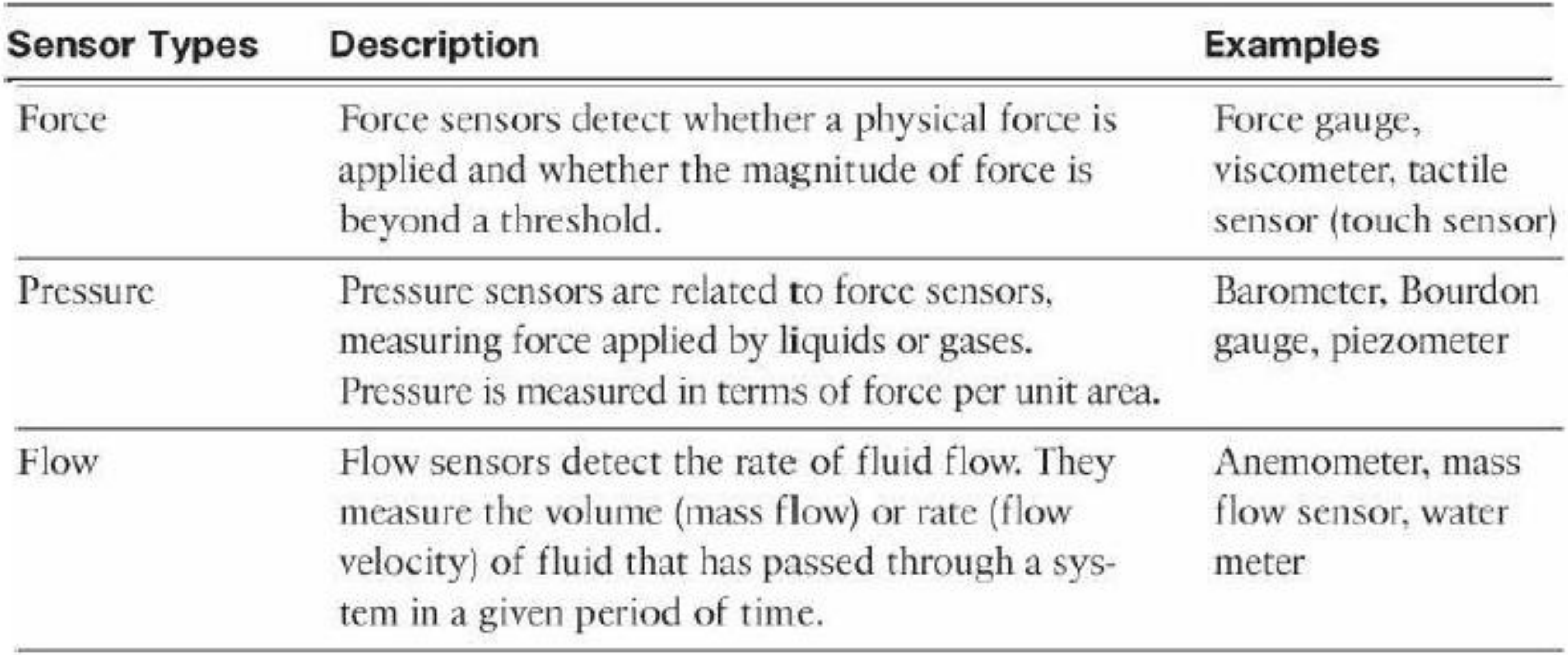
Sensors: Categorization based on what physical phenomenon a sensor is measuring:



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

Module – 2 Smart Objects: The “Things” in IoT

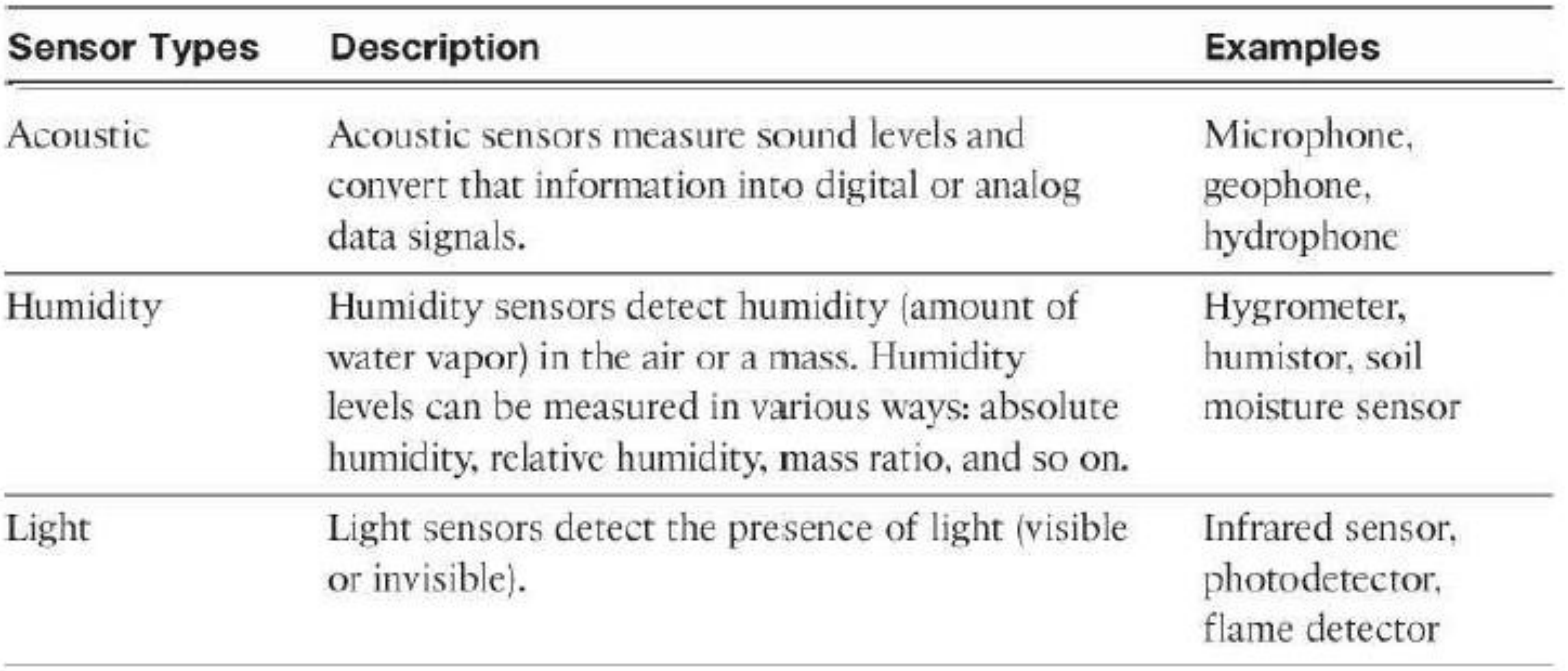
Sensors: Categorization based on what physical phenomenon a sensor is measuring:



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

Module – 2 Smart Objects: The “Things” in IoT

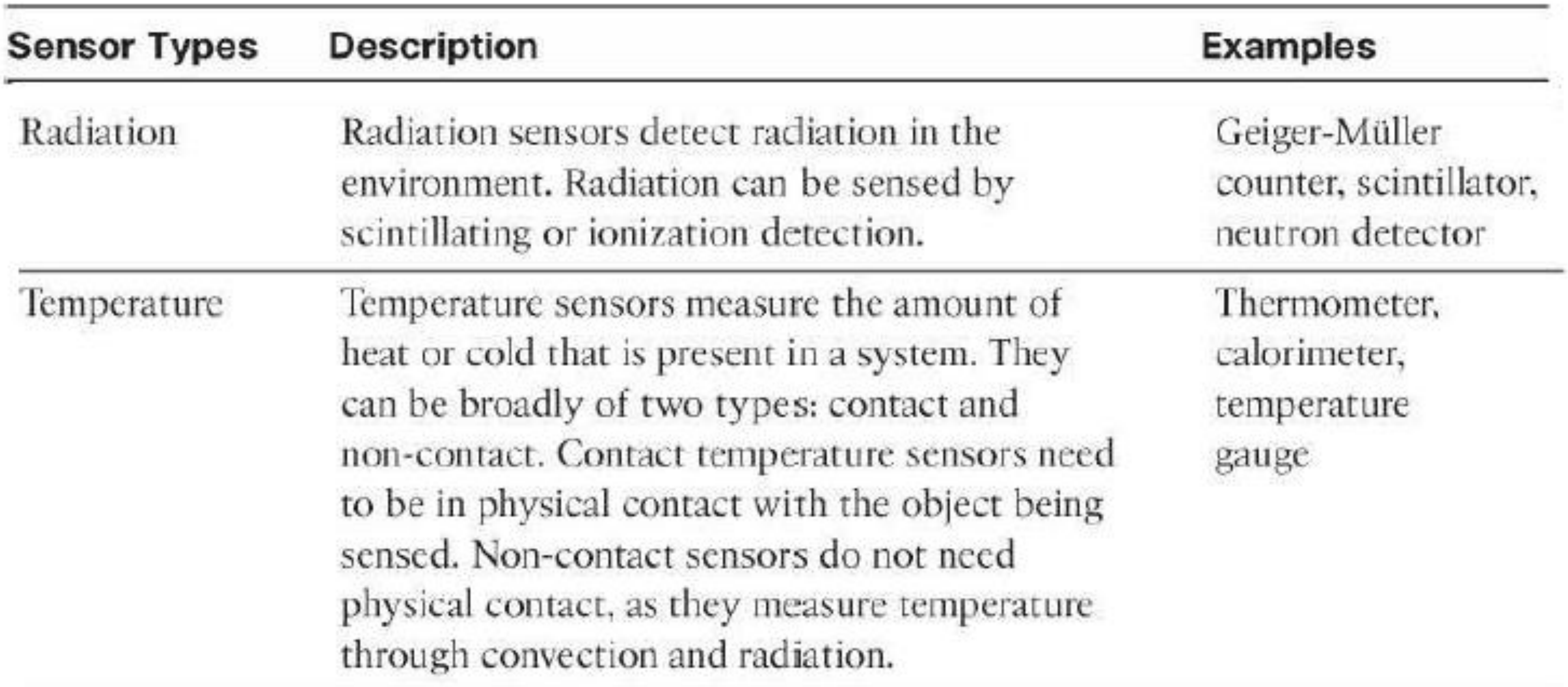
Sensors: Categorization based on what physical phenomenon a sensor is measuring:



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

Module – 2 Smart Objects: The “Things” in IoT

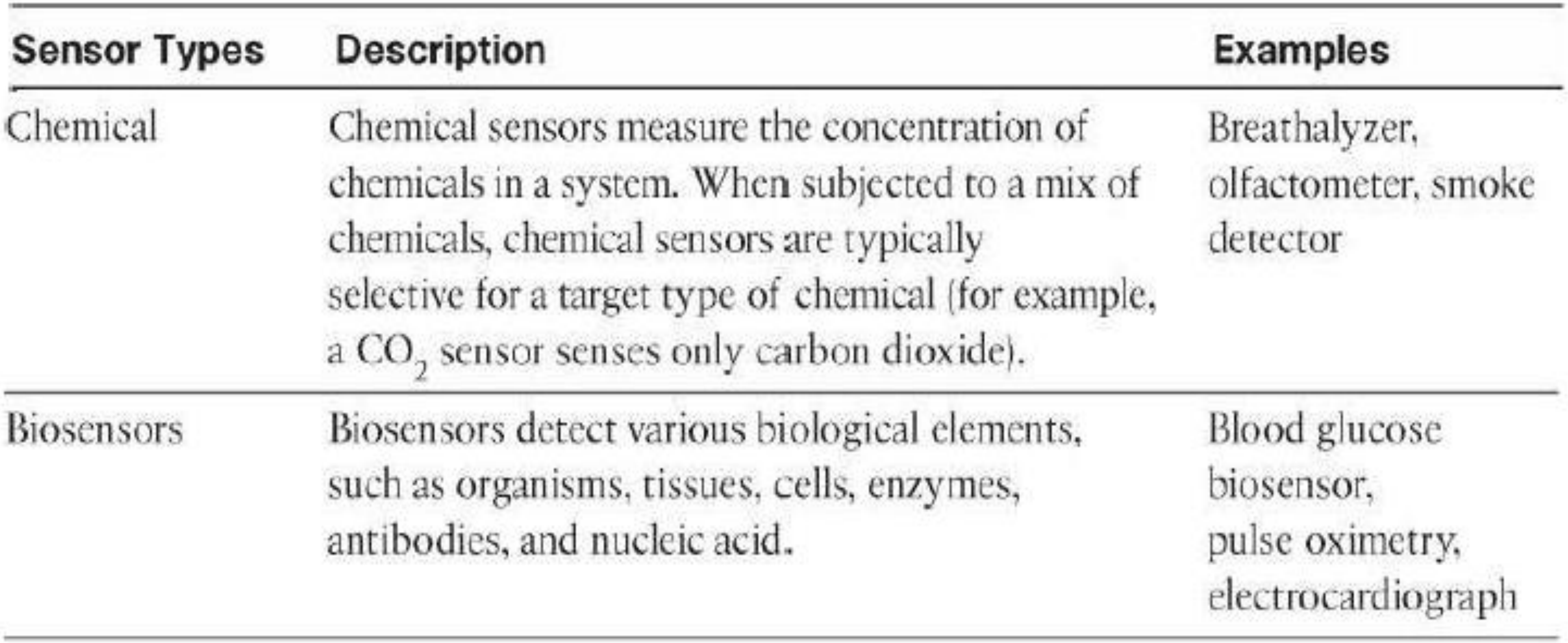
Sensors: Categorization based on what physical phenomenon a sensor is measuring:



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

Module – 2 Smart Objects: The “Things” in IoT

Sensors: Categorization based on what physical phenomenon a sensor is measuring:



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

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- **Sensors come in all shapes and sizes and can measure all types of physical conditions.**
- **A fascinating use case to highlight the power of sensors and IoT is in the area of precision agriculture (sometimes referred to as 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; and real-time analytics and artificial intelligence to predict optimal crop yield, weather impacts, and soil quality.**

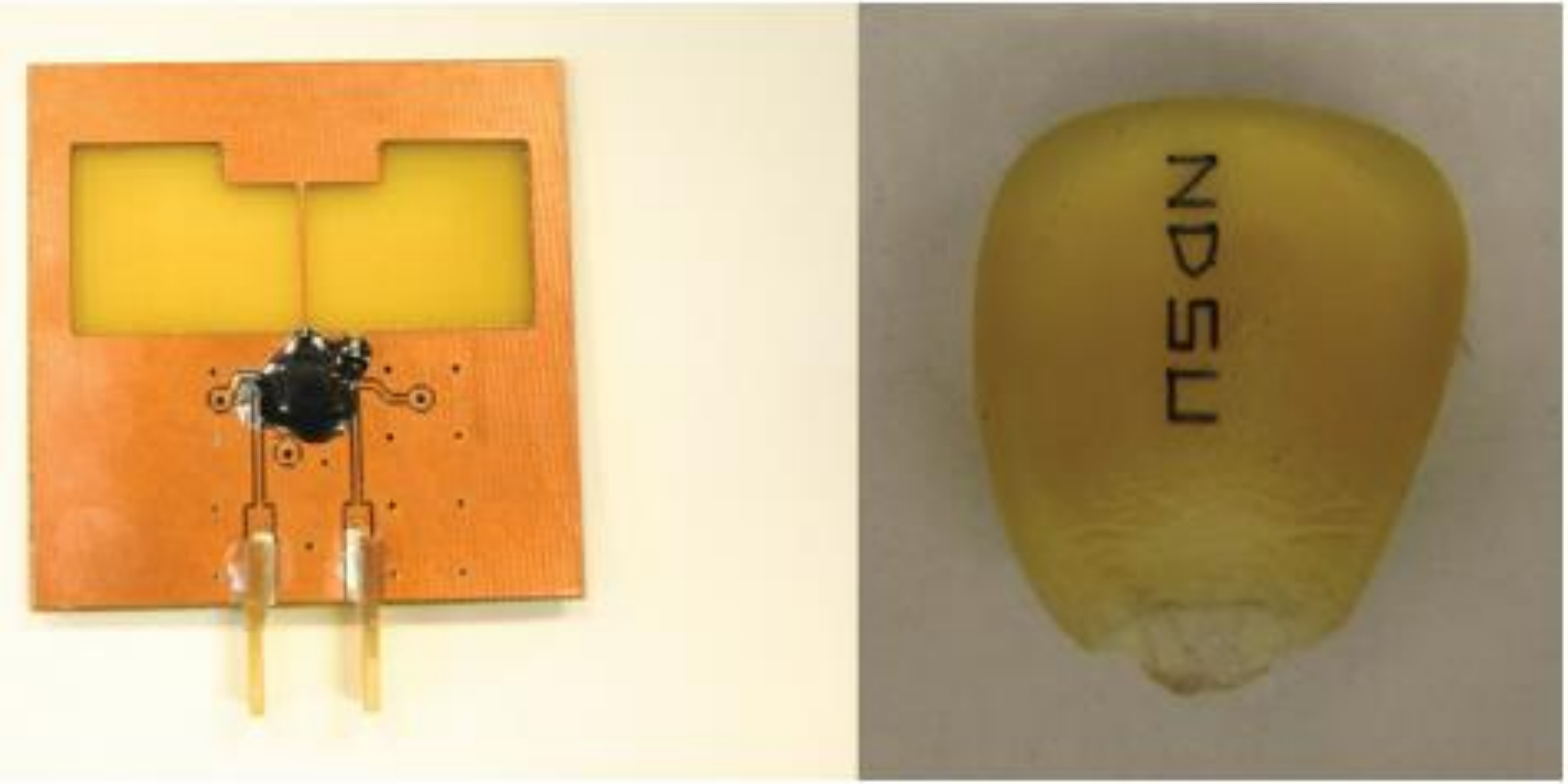
Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- 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.
- All this detailed sensor data can be analyzed to provide highly valuable and actionable insight to boost productivity and crop yield.
- Figure shows 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.

Module – 2 Smart Objects: The “Things” in IoT

Sensors:



Biodegradable Sensors Developed by NDSU for Smart Farming

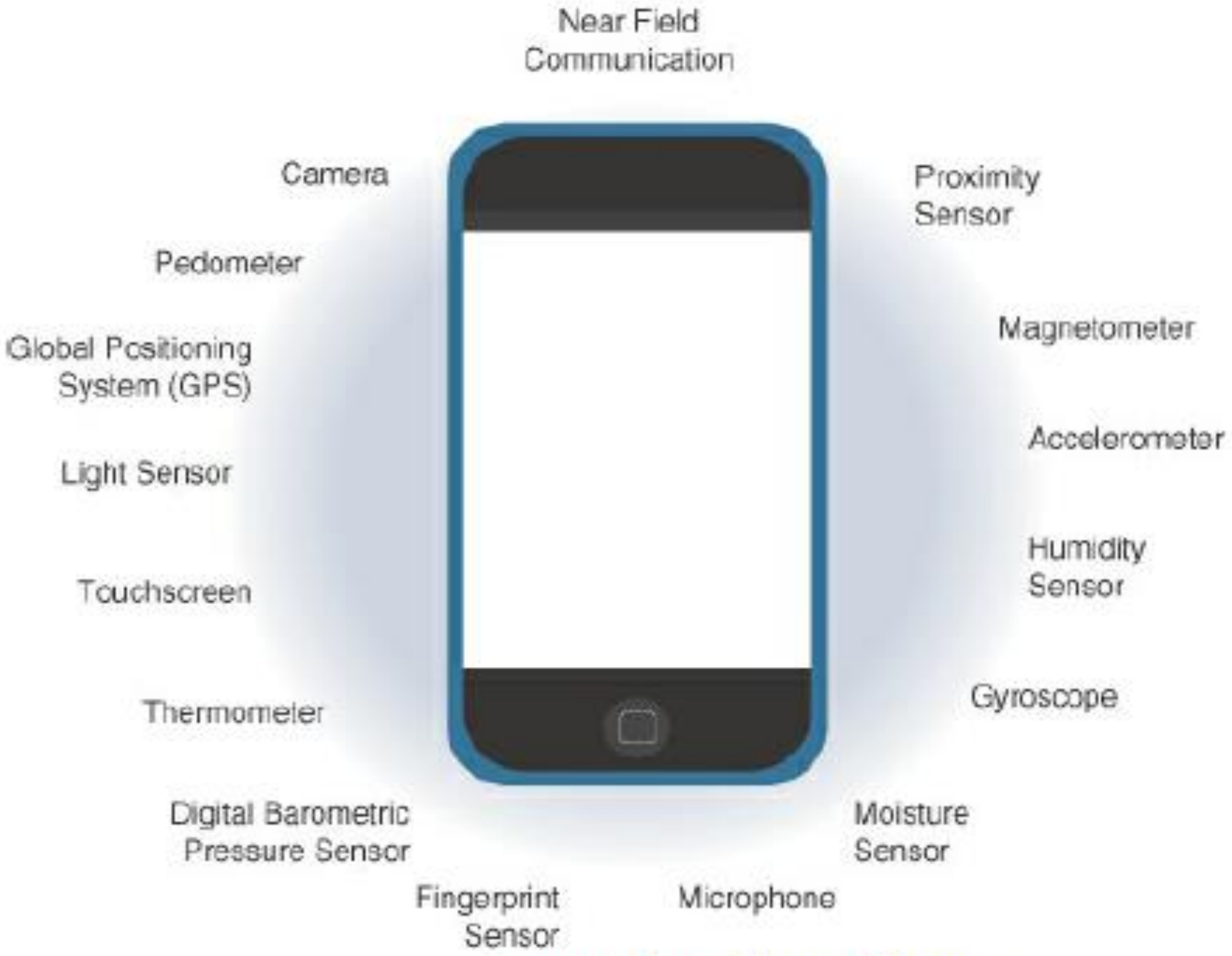
Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- IoT and by extension, networked sensors have been repeatedly named among a small number of emerging revolutionary technologies that will change the global economy and shape the future.
- The astounding volume of sensors is in large part due to their smaller size, their form factor, and their decreasing cost.
- These factors make possible the economic and technical feasibility of having an increased density of sensors in objects of all types.
- most significant accelerator for sensor deployments is mobile phones.
- More than a billion smart phones are sold each year, and each one has well over a dozen sensors inside it

Module – 2 Smart Objects: The “Things” in IoT

Sensors



Sensors in a Smart Phone

Module – 2 Smart Objects: The “Things” in IoT

Sensors:

- **There are smart homes with potentially hundreds of sensors, intelligent vehicles with 100+ sensors each, connected cities with thousands upon thousands of connected sensors, and the list goes on and on.**

- **Figure shows the explosive year-over-year increase over the past several years and some bold predictions for sensor numbers in the upcoming years.**

- **The sensor industry that this number will eclipse a trillion in the next few years.**

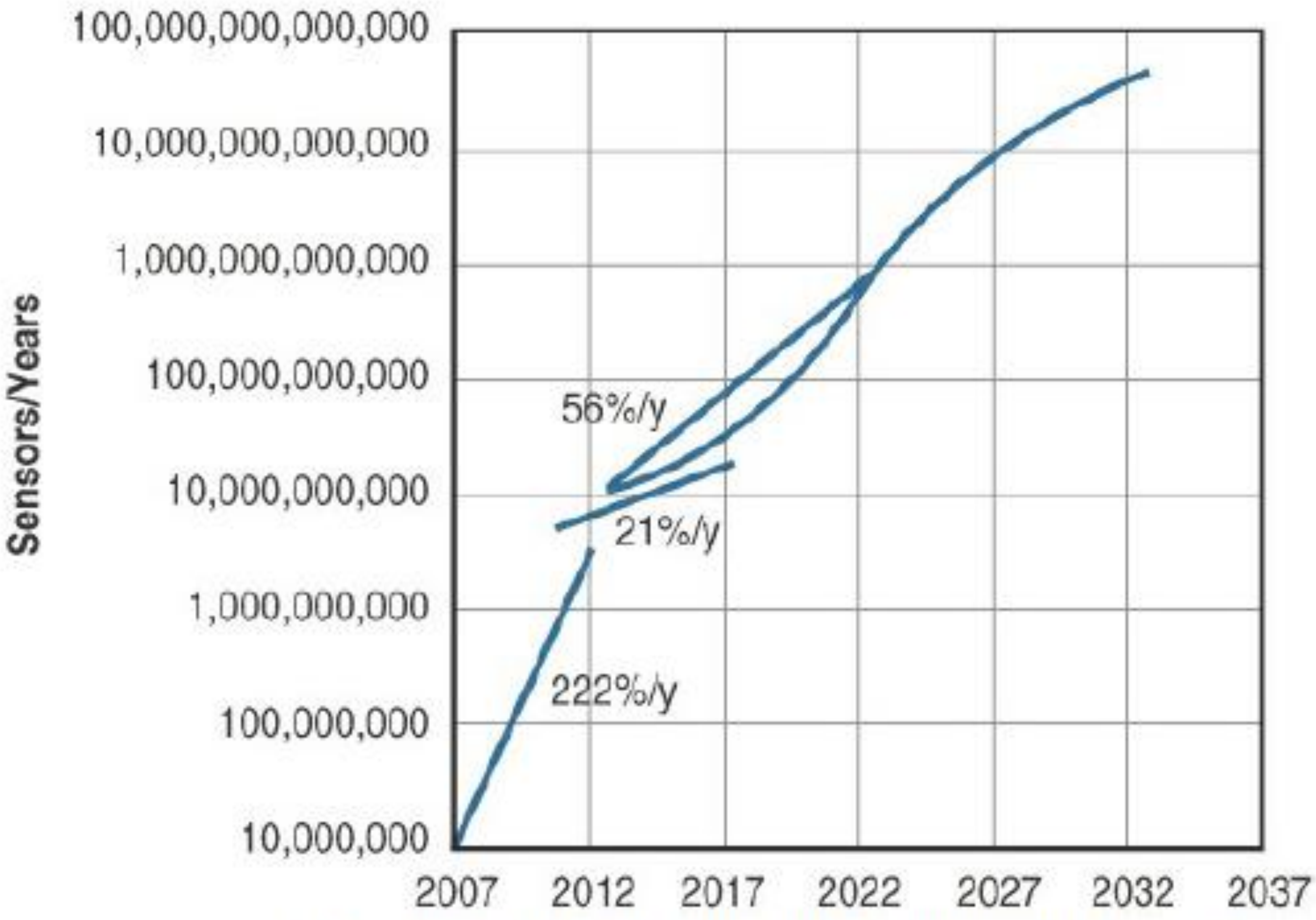
- **In fact, many large players in the sensor industry have come together to form industry consortia, such as the TSensors Summits (www.tsensorssummit.org), to create a strategy and roadmap for a trillion sensor economy.**

- **The trillion-sensor economy will be of such an unprecedented and unimaginable scale that it will change the world forever.**

- **This is the power of IoT.**

Module – 2 Smart Objects: The “Things” in IoT

Sensors:



Growth and Predictions in the Number of Sensors

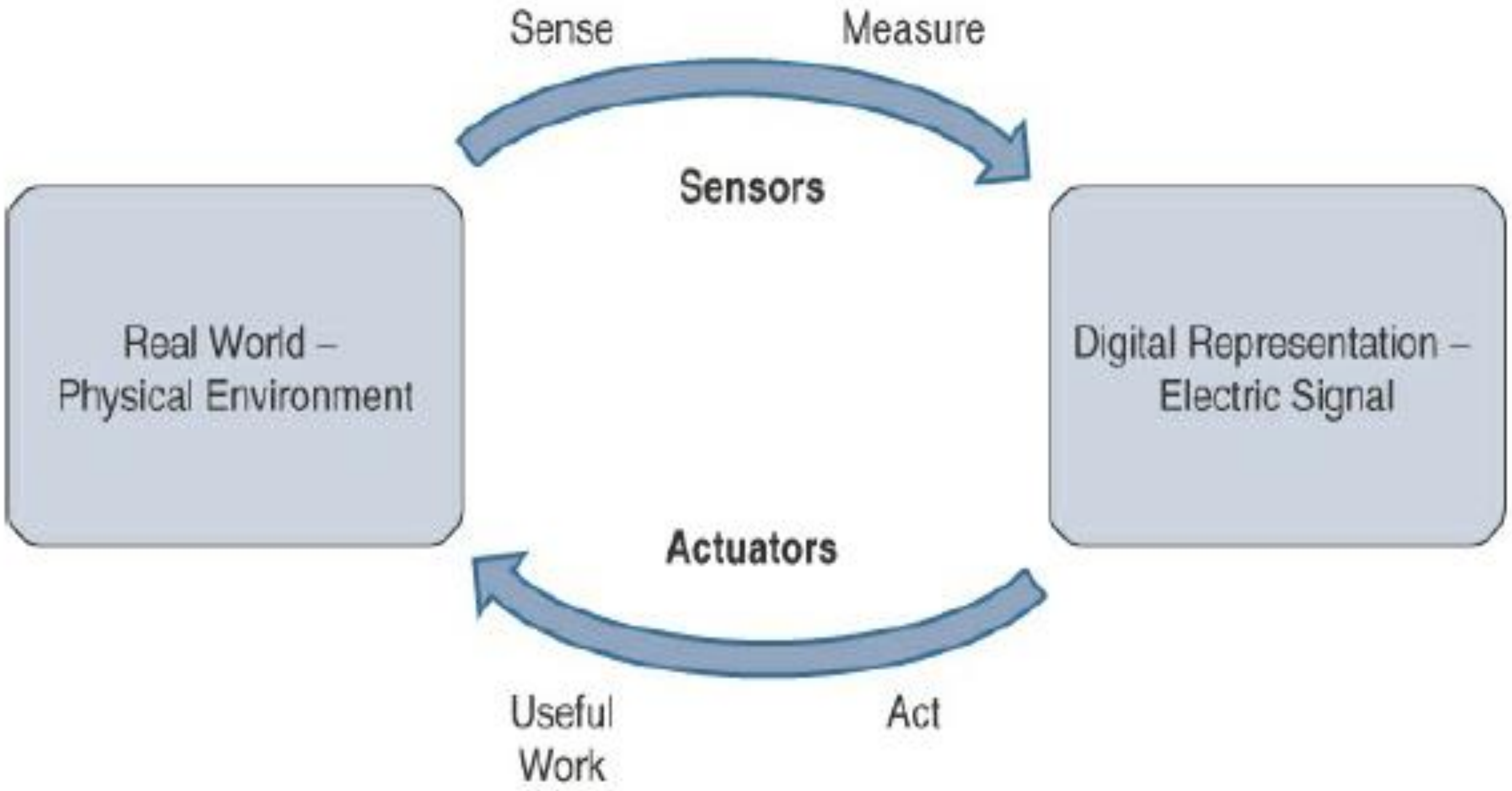
Module – 2 Smart Objects: The “Things” in IoT

Actuators:

- **Actuators are natural complements to sensors.**
- **Figure demonstrates the symmetry and complementary nature of these two types of devices.**
- **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, 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.**

Module – 2 Smart Objects: The “Things” in IoT

Actuators:



How Sensors and Actuators Interact with the Physical World

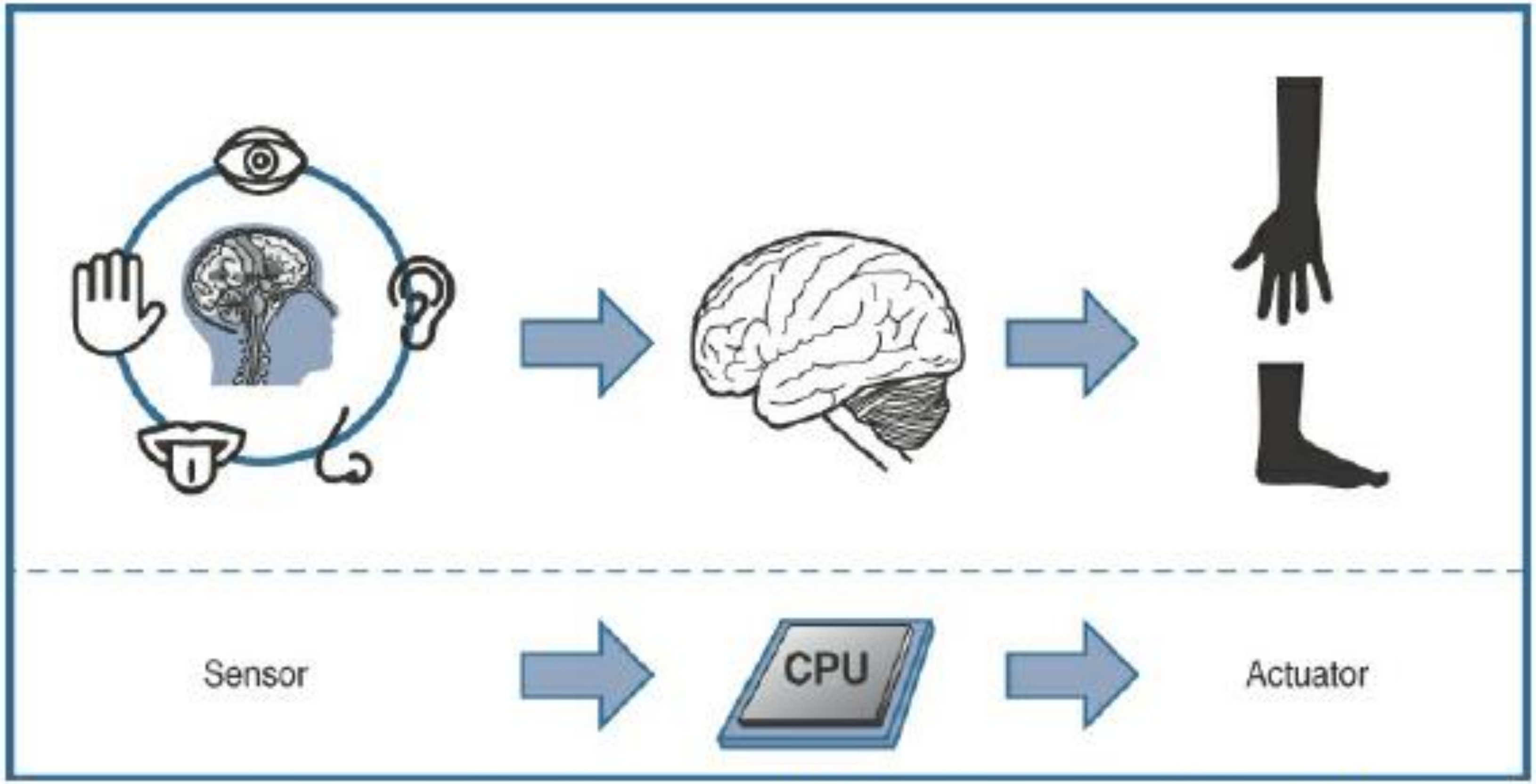
Module – 2 Smart Objects: The “Things” in IoT

Actuators:

- **IoT sensors are devices that sense and measure the physical world and (typically) signal their measurements as electric signals sent to some type of microprocessor or microcontroller for additional processing.**
- **Correspondingly, a processor can send an electric signal to an actuator that translates the signal into some type of movement (linear, rotational, and so on) or useful work that changes or has a measurable impact on the physical world.**
- **This interaction between sensors, actuators, and processors and the similar functionality in biological systems is the basis for various technical fields, including robotics and biometrics.**

Module – 2 Smart Objects: The “Things” in IoT

Actuators:



Comparison of Sensor and Actuator Functionality with Humans

Module – 2 Smart Objects: The “Things” in IoT

Actuators:

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

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

Module – 2 Smart Objects: The “Things” in IoT

Actuators:

1. **Type of motion:**

   Actuators can be classified based on the type of motion they produce

   (for example, linear, rotary, one/two/three-axes).

2. **Power:**

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

3. **Binary or continuous:**

   Actuators can be classified based on the number of stable-state outputs.

4. **Area of application:**

   Actuators can be classified based on the specific industry or vertical where they are used.

5. **Type of energy:**

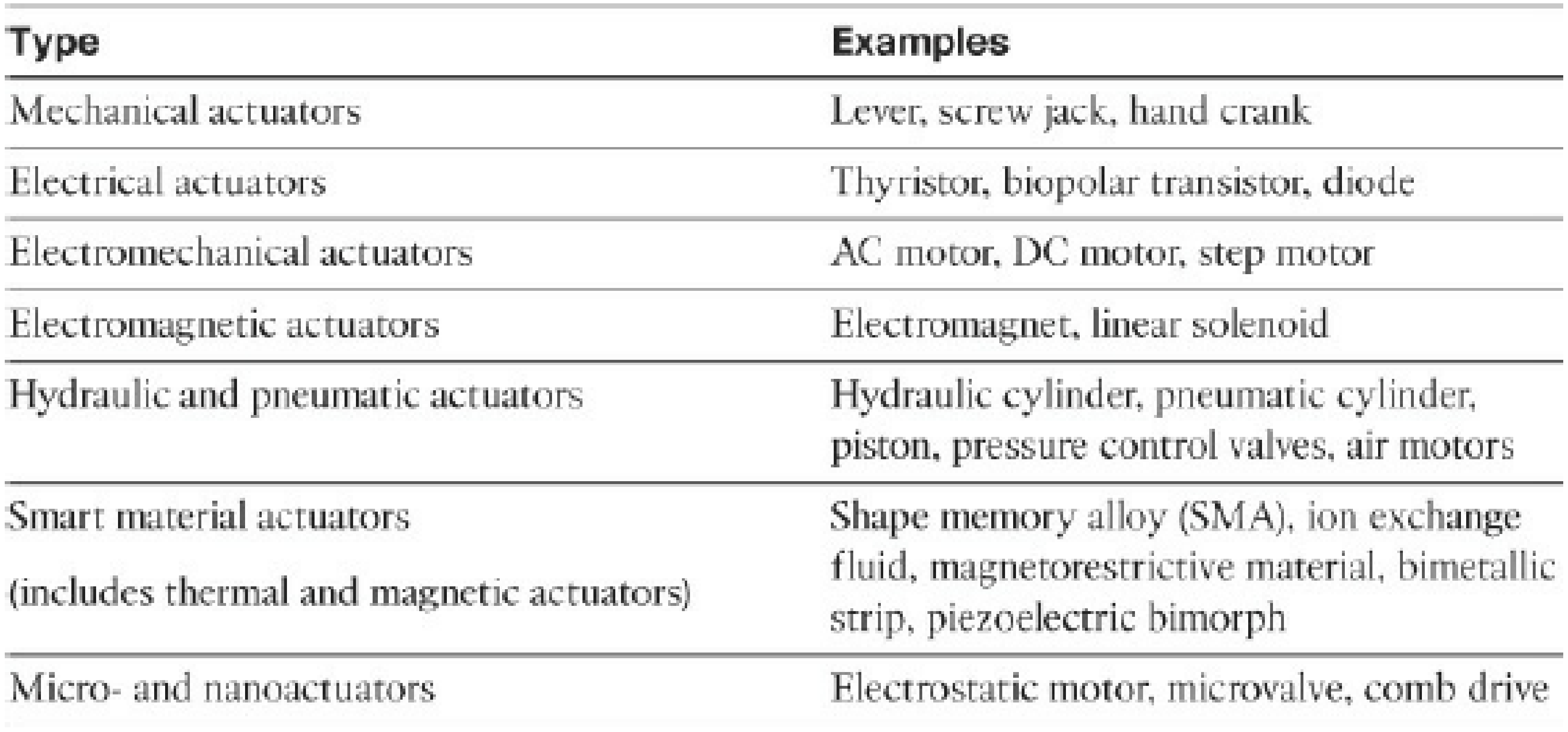
   Actuators can be classified based on their energy type

Module – 2 Smart Objects: The “Things” in IoT

Actuators:

The most commonly used classification is based on energy type.

Table shows actuators classified by energy type and some examples for each 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

Actuator Classification by Energy Type

Module – 2 Smart Objects: The "Things" in IoT

Actuators:

- **Sensors provide the information, actuators provide the action.**
- **The most interesting use cases for IoT are those where sensors and actuators work together in an intelligent.**
- **For example, the smart sensors used to evaluate soil quality (by measuring a variety of soil, temperature, and plant characteristics) can be connected with electrically or pneumatically controlled valve actuators that control water, pesticides, fertilizers, herbicides, and so on.**
- **Intelligently triggering a high-precision actuator based on well-defined sensor readings of temperature, pH, soil/air humidity, nutrient levels, and so on to deliver a highly optimized and custom environment-specific solution is truly smart farming.**

Module – 2 Smart Objects: The "Things" in IoT

Micro-Electro-Mechanical Systems (MEMS):

- **One of the most 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 integrate 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.**

Module – 2 Smart Objects: The “Things” in IoT

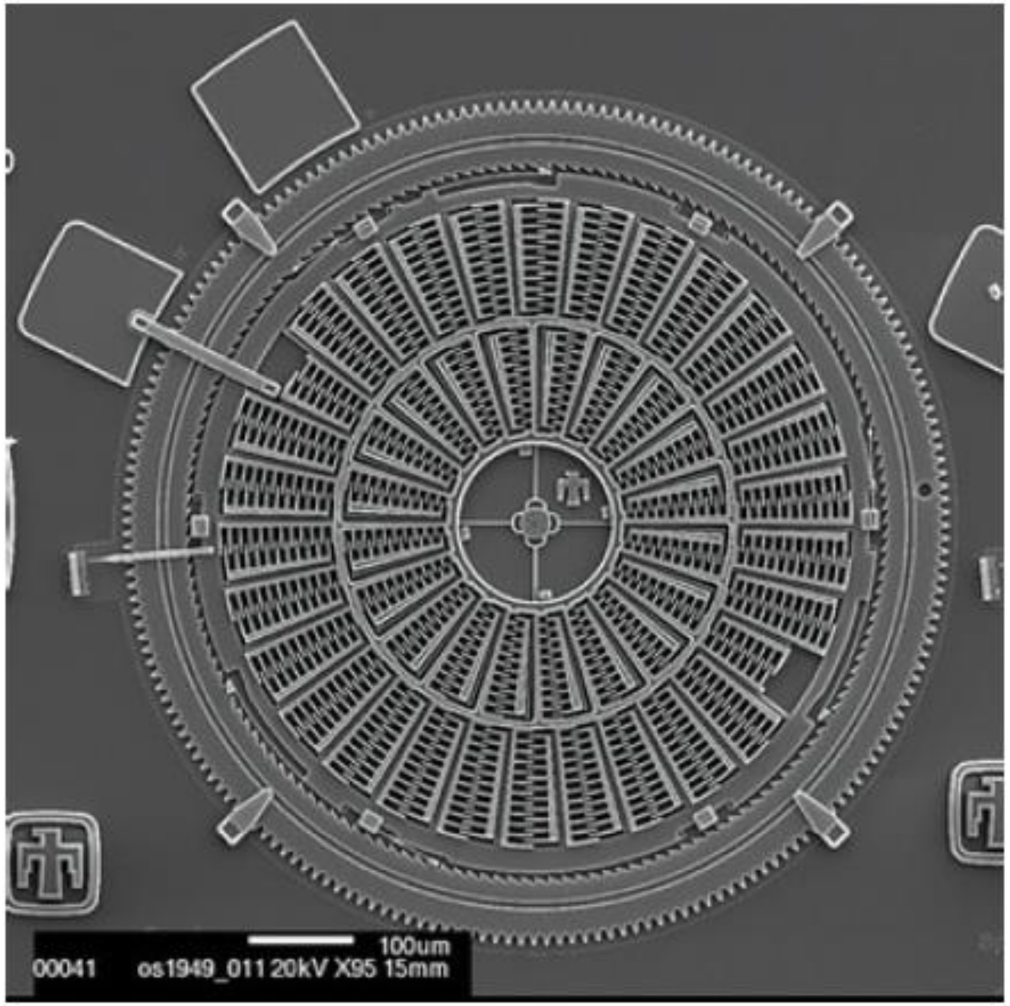
Micro-Electro-Mechanical Systems (MEMS):

- **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 micro pump MEMS.**
- **Smart phones also use MEMS technologies for things like accelerometers and gyroscopes.**
- **Automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers.**

Module – 2 Smart Objects: The "Things" in IoT

Micro-Electro-Mechanical Systems (MEMS):

- **Torsional ratcheting actuator (TRA) MEMS that was developed by Sandia National Laboratory as a low-voltage alternative to a micro-engine.**
- **This MEMS is only a few hundred micrometers across; a scanning electron microscope is needed to show the level of detail visible in the figure.**
- **Micro-scale sensors and actuators are immensely embeddable in everyday objects, which is a defining characteristic of IoT.**



Module – 2 Smart Objects: The "Things" in IoT

Smart Objects:

- **Smart objects are the building blocks of IoT.**
- **They transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way.**
- **If soil 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.**
- **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.**

Module – 2 Smart Objects: The “Things” in IoT

Smart Objects:

- **The term smart object is often used interchangeably with terms such as smart sensor, smart device, IoT device, intelligent device, thing, smart thing, intelligent node, intelligent thing, ubiquitous thing, and intelligent product.**

Definition:

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

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

Module – 2 Smart Objects: The “Things” in IoT

Smart Objects:

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

Module – 2 Smart Objects: The "Things" in IoT

Smart Objects:

2. **Sensor(s) and/or actuator(s):**

- **A smart object is capable of interacting with the physical world through sensors and actuators.**
- **A sensor learns and measures its environment, whereas an actuator is able to produce some change in the physical world.**
- **A smart object does not need to contain both sensors and actuators.**
- **In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.**

Module – 2 Smart Objects: The “Things” in IoT

Smart Objects:

3. 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.**
- **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.**

Module – 2 Smart Objects: The “Things” in IoT

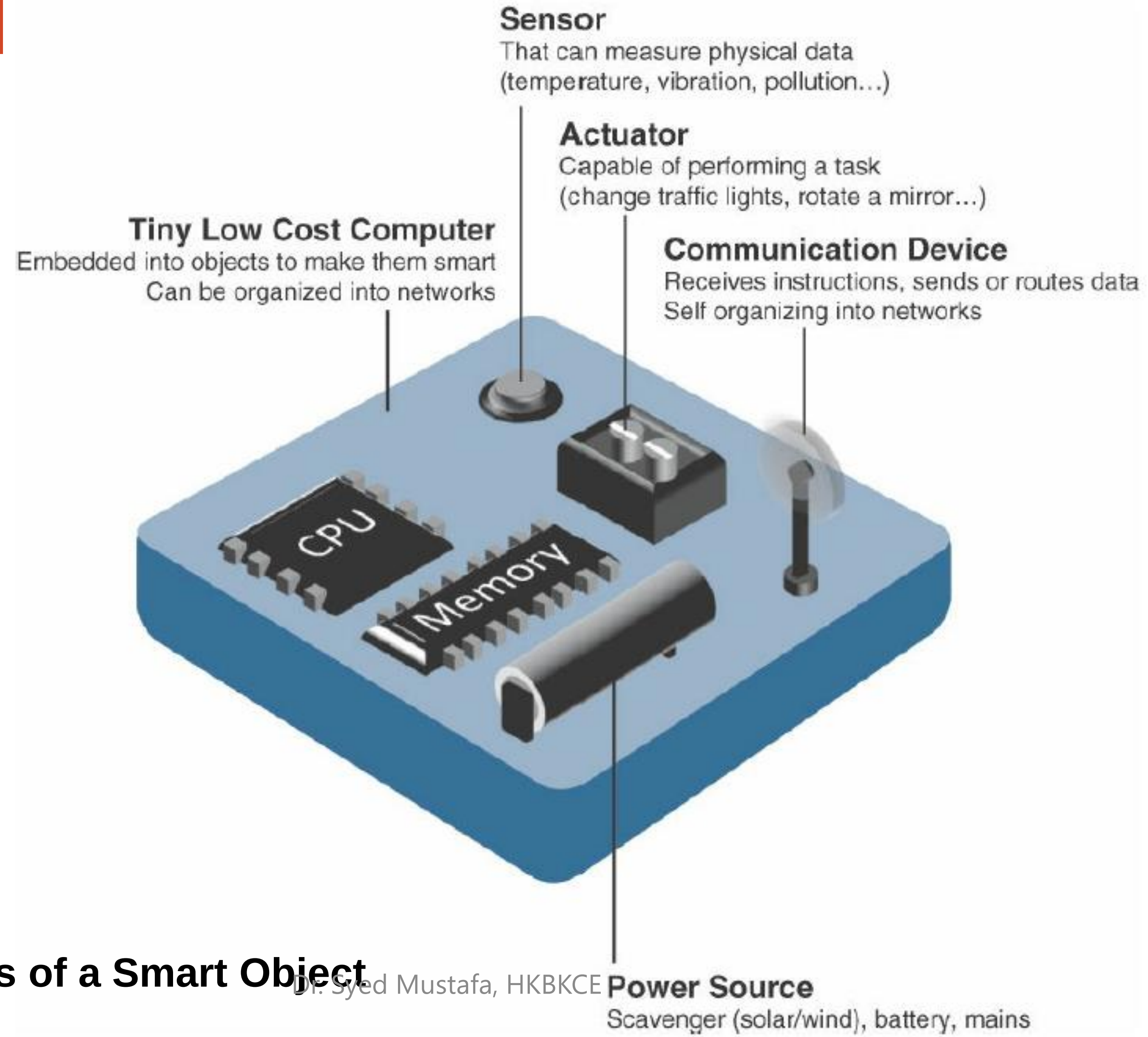
Smart Objects:

4. Power source:

- **Smart objects have components that need to be powered.**
- **Most significant power consumption comes from the communication unit of a smart object.**
- **The power requirements vary greatly from application to application.**
- **Smart objects are limited in power, are deployed for a very long time, and are not easily accessible.**
- **This combination, 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**

Module – 2 Smart Objects: The “Things” in IoT

Smart Objects:



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

Characteristics of a Smart Object

Module – 2 Smart Objects: The “Things” in IoT

Trends in Smart Objects:

Broad generalizations and trends impacting IoT:

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

Module – 2 Smart Objects: The “Things” in IoT

Trends in Smart Objects:

Broad generalizations and trends impacting IoT:

1. **Size is decreasing:**
   - **In reference to MEMS, there is a clear trend of ever-decreasing size.**
   - **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.**

2. **Power consumption is decreasing:**
   - **The different hardware components of a smart object continually consume less power.**
   - **This is especially truef or sensors, many of which are completely passive.**
   - **Some battery powered sensors last 10 or more years without battery replacement.**

Module – 2 Smart Objects: The “Things” in IoT

Trends in Smart Objects:

Broad generalizations and trends impacting IoT:

3. Processing power is increasing:

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

4. 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.**

Module – 2 Smart Objects: The “Things” in IoT

Trends in Smart Objects:

Broad generalizations and trends impacting IoT:

5. 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.**

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

- **A sensor/actuator network (SANET), is a network of sensors that sense and measure their environment and/or actuators that act on their environment.**
- **The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner.**
- **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.**

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

- **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.**

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

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

Advantages:

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

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

Disadvantages:

1. **Potentially less secure (for example, hijacked access points)**
2. **Typically lower transmission speeds**
3. **Greater level of impact/influence by environment**

Wireless Sensor Networks (WSNs):

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

The following are some of the most significant limitations of the smart objects in WSNs:

1. **Limited processing power**
2. **Limited memory**
3. **Lossy communication**
4. **Limited transmission speeds**
5. **Limited power**

Module – 2 Smart Objects: The “Things” in IoT

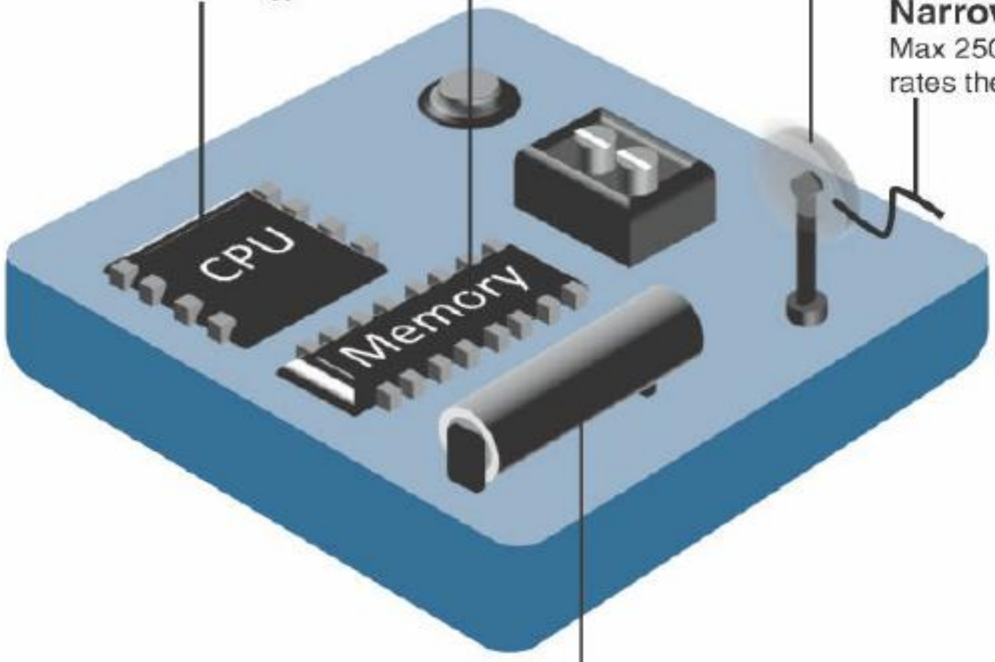
Sensor Networks:

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



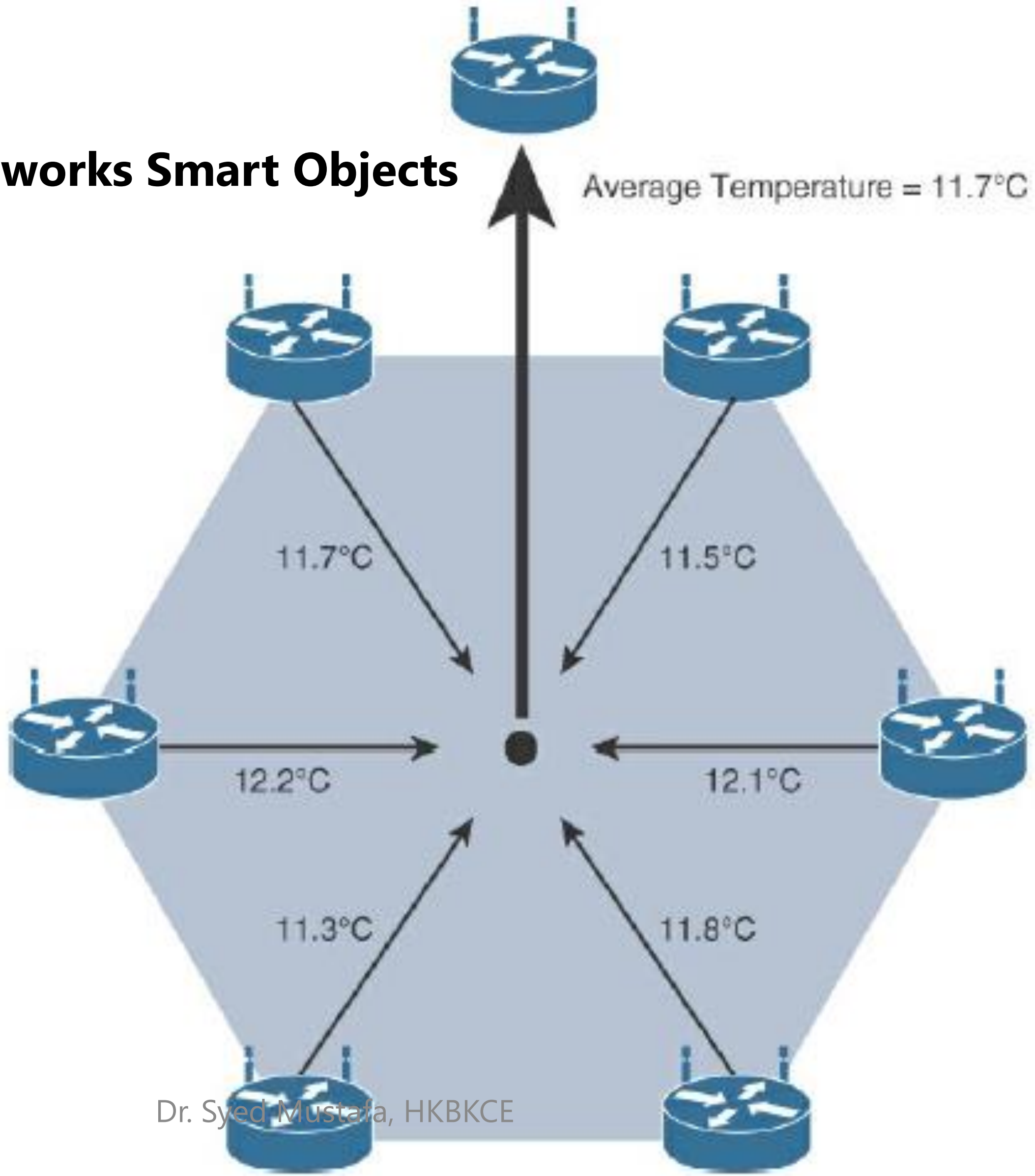
Power Consumption Is Critical
Energy efficiency is paramount
Battery powered devices must last years

Design Constraints for Wireless Smart Objects

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

Data Aggregation in Wireless Sensor Networks Smart Objects



Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

- **The 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.**

Module – 2 Smart Objects: The “Things” in IoT

Sensor Networks:

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.**

Module – 2 Connecting Smart Objects

Connecting Smart Objects:

“Communications Criteria,” describes the characteristics and attributes should be considered when selecting and dealing with connecting smart objects.

The various technologies used for connecting sensors can differ greatly depending on the criteria used to analyze them.

1. Range

2. Frequency Bands

3. Power Consumption

4. Topology

5. Constrained Devices

6. Constrained-Node Networks

Module – 2 Connecting Smart Objects

Communications Criteria:

1. Range:

How far does the signal need to be propagated?

what will be the area of coverage for a selected wireless technology?

Should indoor versus outdoor deployments be differentiated?

i. Short range:

The classical wired example is a serial cable.

Module – 2 Connecting Smart Objects

Communications Criteria:

1. Range:

i. 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).

Module – 2 Connecting Smart Objects

Communications Criteria:

ii. 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, although RF technologies do not have real maximum distances defined, as long as the radio signal is transmitted and received in the scope of the applicable specification.

Module – 2 Connecting Smart Objects

Communications Criteria:

ii. Medium range:

Examples of medium-range wireless technologies include IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN.

Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC) may also be classified as medium range, depending on their physical media characteristics.

Module – 2 Connecting Smart Objects

Communications Criteria:

iii. 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.

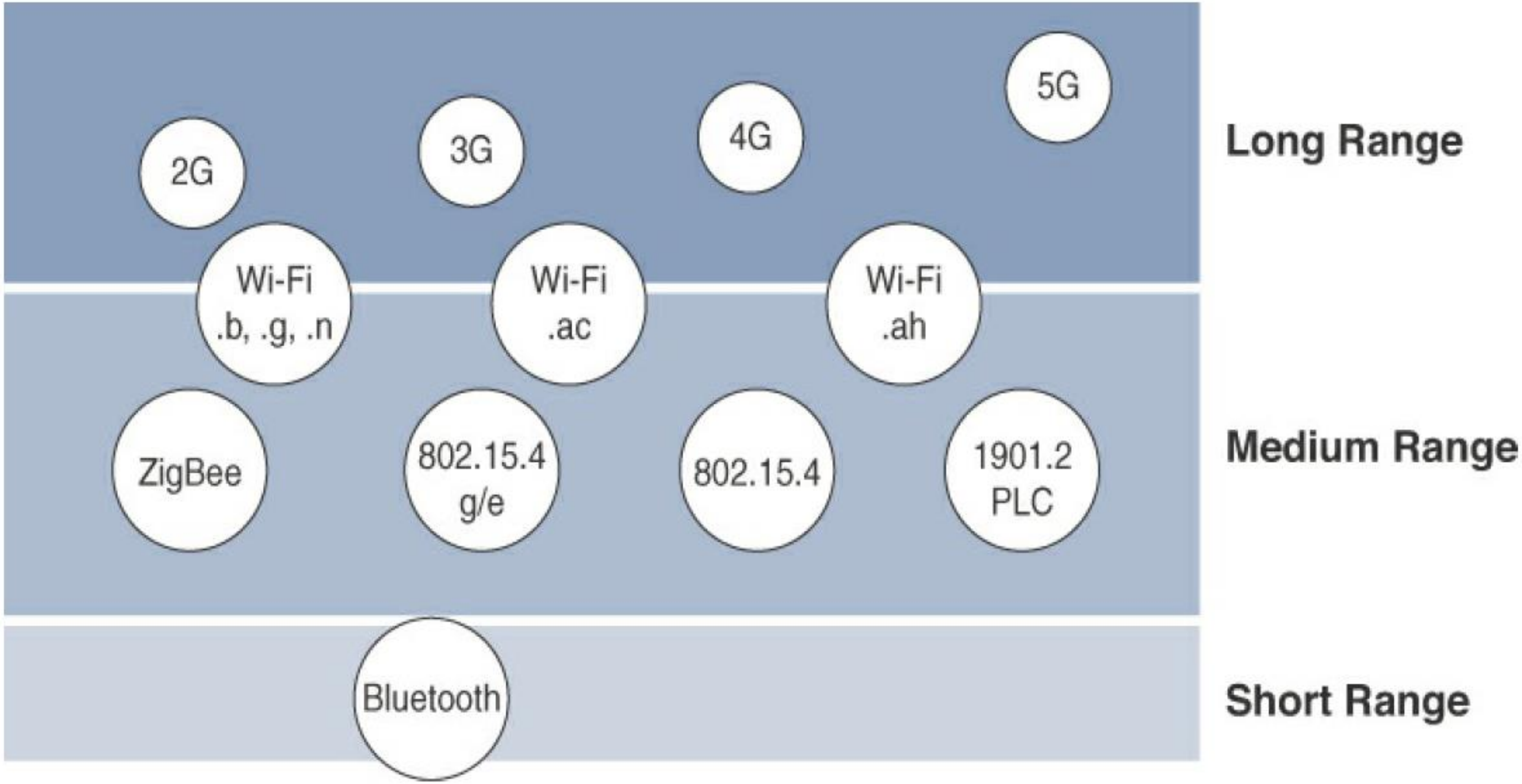
These technologies are therefore ideal for battery-powered IoT sensors.

IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications are classified as long range

Module – 2 Connecting Smart Objects

Communications

Criteria:



Wireless Access Landscape

2. 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.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **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 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.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands for short-range devices (SRDs).**
- **Unlicensed means that no guarantees or protections are offered in the ISM bands for device communications.**
- **For IoT access, these are the most well-known ISM bands:**
  1. **2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi**
  2. **IEEE 802.15.1 Bluetooth**
  3. **IEEE 802.15.4 WPAN(Wireless Personal Area Network).**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **The frequency of transmission directly impacts how a signal propagates and its practical maximum range.**
- **Some communications within the 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.**
- **Either for indoor or outdoor deployments, the sub-GHz frequency bands allow greater distances between devices.**
- **These bands have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles, while keeping the transmit power within regulation.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **The frequency of transmission directly impacts how a signal propagates and its practical maximum range.**
- **Some communications within the 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(Low-Power Wide-Area) technologies such as LoRa and Sigfox.**
- **Either for indoor or outdoor deployments, the sub-GHz frequency bands allow greater distances between devices.**
- **These bands have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles, while keeping the transmit power within regulation.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies.**
- **Most IoT sensors do not need to send data at high rates.**
- **Therefore, the lower transmission speeds of sub-GHz technologies are usually not a concern for IoT sensor deployments.**
- **For example, in most European countries, the 169 MHz band is often considered best suited for wireless water and gas metering applications.**
- **This is due to its good deep building basement signal penetration, the low data rate of this frequency matches the low volume of data that needs to be transmitted.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **Several sub-GHz ranges have been defined in the ISM band.**
- **The most wellknown ranges are centered on 169 MHz, 433 MHz, 868 MHz, and 915 MHz.**
- **most IoT access technologies tend to focus on the two sub-GHz frequency regions around 868 MHz and 915 MHz.**
- **These main bands are commonly found throughout the world and are applicable to nearly all countries.**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **The European Conference of Postal and Telecommunications Administrations (CEPT), in the European Radio communications Committee (ERC)Recommendation 70-03, defines the 868 MHz frequency band.**
- **CEPT was established in 1959 as a coordinating body for European state telecommunications and postal organizations.**
- **India, the Middle East, Africa, and Russia have adopted the CEPT definitions.**
- **Recommendation 70-03 mostly characterizes the use of the 863–870 MHz band, the allowed transmit power, or EIRP (effective isotropic radiated power), and duty cycle (that is, the percentage of time a device can be active in transmission).**

Module – 2 Connecting Smart Objects

Frequency Bands:

- **EIRP is the amount of power that an antenna would emit to produce the peak power density observed in the direction of maximum antenna gain.**
- **The 868 MHz band is applicable to IoT access technologies such as IEEE 802.15.4 and 802.15.4g, 802.11ah, and LoRaWAN.**
- **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.**
- **However, parameters such as transmit power, antennas, and EIRP must be properly designed to follow the settings required by each country's regulations.**

Module – 2 Connecting Smart Objects

3. 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.**
- **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.**

Module – 2 Connecting Smart Objects

3. Power Consumption:

- **For devices under regular maintenance, a battery life of 2 to 3 years is an option.**
- **IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes.**
- **This has led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA)**
- **It is possible to run just about any wireless technology on batteries.**
- **However, in reality, no operational deployment will be acceptable if hundreds of batteries must be changed every month**

Module – 2 Connecting Smart Objects

4. 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, as seen with cellular, LPWA, and Bluetooth networks.**
- **Star topologies utilize a single central base station or controller to allow communications with endpoints.**

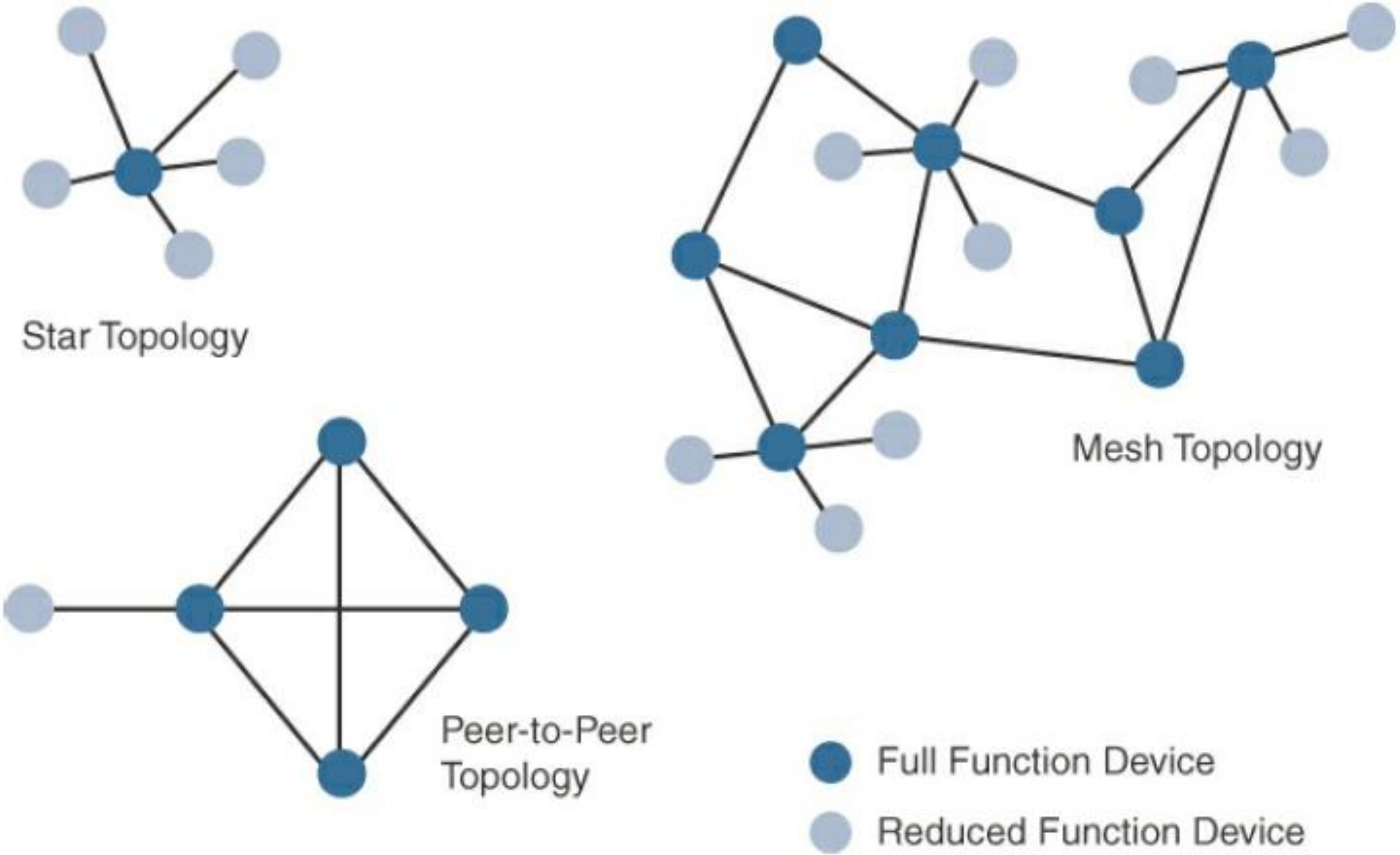
Module – 2 Connecting Smart Objects

4. Topology:

- **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.**
- **Obviously, peer-to-peer topologies rely on multiple full-function devices.**
- **Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.**

Module – 2 Connecting Smart Objects

4. Topology:



Star, Peer-to-Peer, and Mesh Topologies

Module – 2 Connecting Smart Objects

4. Topology:

For example,

indoor Wi-Fi deployments are mostly a set of nodes forming a star topology around their access points (APs).

Meanwhile,

outdoor Wi-Fi may consist of a mesh topology for the backbone of APs, with nodes connecting to the APs in a star topology.

Similarly, IEEE 802.15.4 and 802.15.4g and even wired IEEE 1901.2a PLC are generally deployed as a mesh topology.

Module – 2 Connecting Smart Objects

4. Topology:

- **A mesh topology helps cope with low transmit power, searching to reach a greater overall distance, and coverage by having intermediate nodes relaying traffic for other nodes.**
- **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.**
- **An intermediate node or full-function device (FFD) is simply a node that interconnects other nodes.**
- **A node that doesn’t interconnect or relay the traffic of other nodes is known as a leaf node, or reduced-function device (RFD).**

Module – 2 Connecting Smart Objects

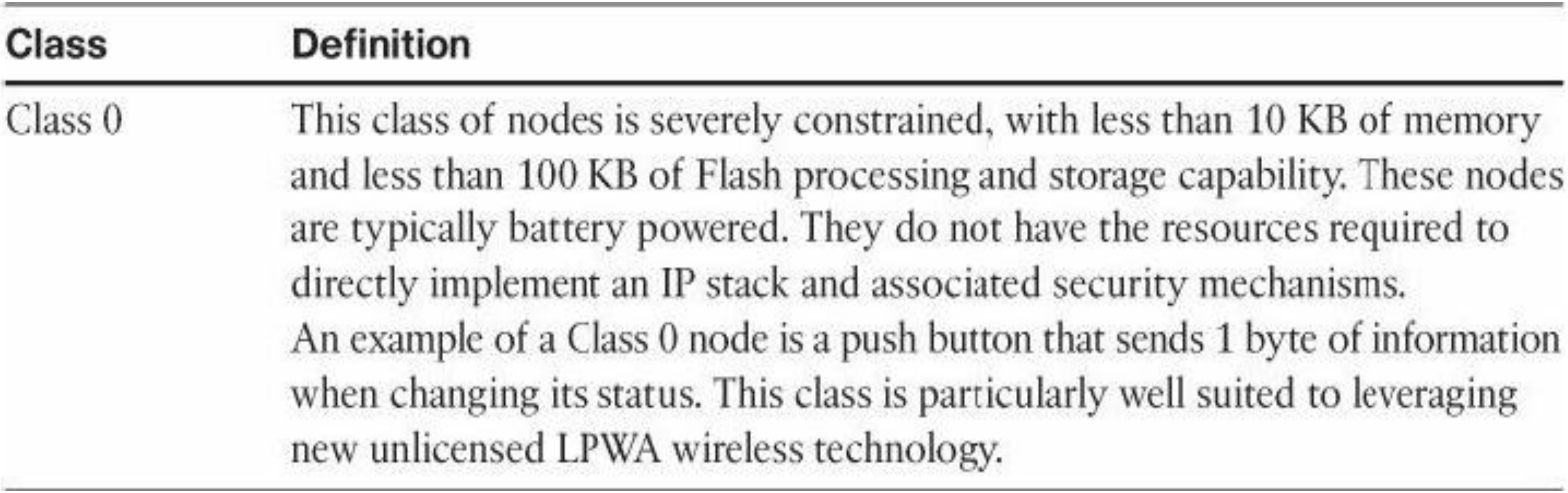
5. Constrained Devices:

- **The Internet Engineering Task Force (IETF) acknowledges in RFC 7228 that different categories of IoT devices are deployed.**
- **While categorizing the class of IoT nodes is a perilous exercise, with computing, memory, storage, power, and networking continuously evolving and improving, RFC 7228 gives some definitions of constrained nodes.**
- **These definitions help differentiate constrained nodes from unconstrained nodes, such as servers, desktop or laptop computers, and powerful mobile devices such as smart phones.**
- **Constrained nodes have limited resources that impact their networking feature set and capabilities.**

Module – 2 Connecting Smart Objects

5. Constrained Devices:

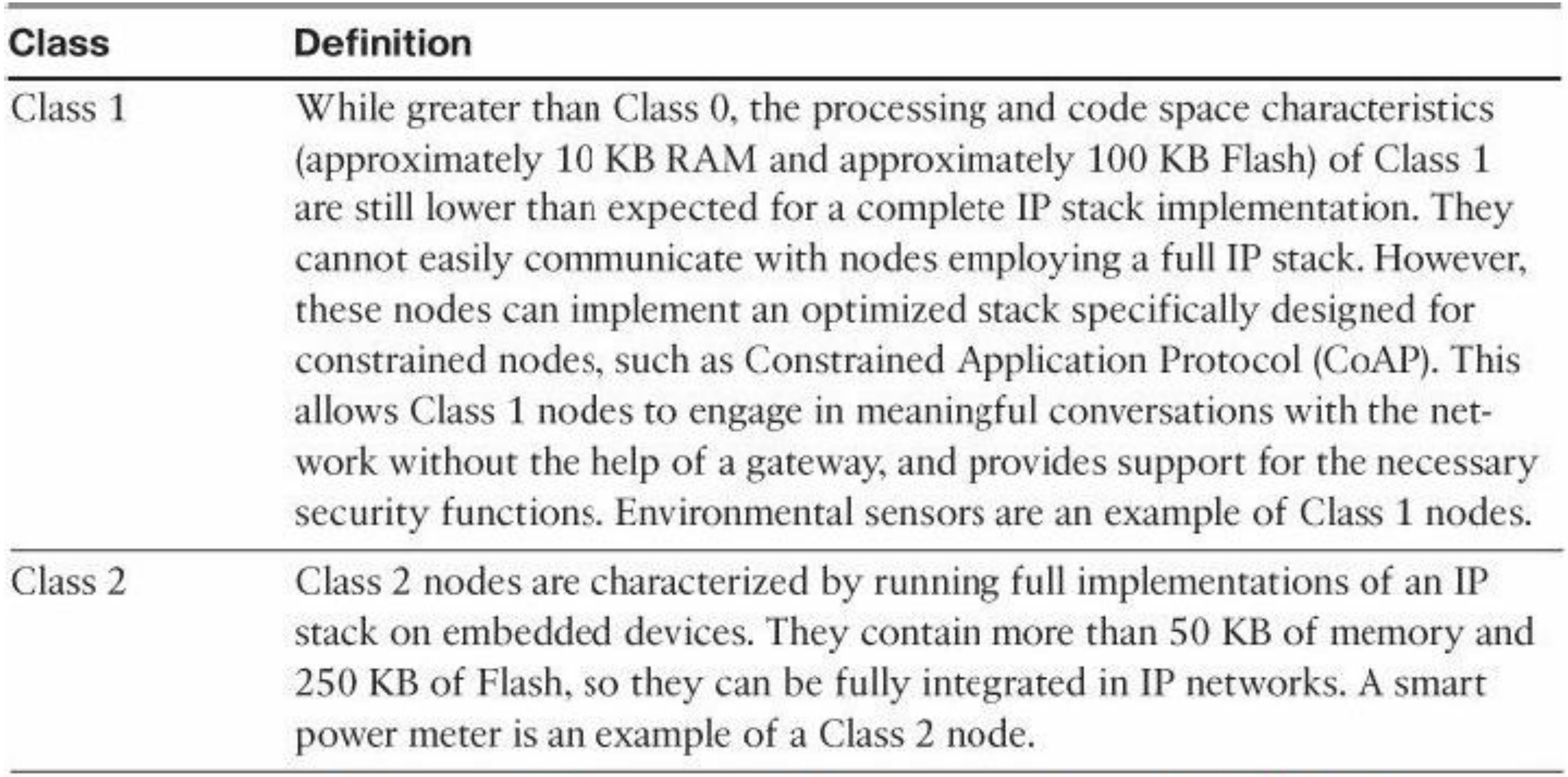
- **some classes of IoT nodes do not implement an IP stack.**
- **According to RFC 7228, constrained nodes can be broken down into the classes**



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.

Module – 2 Connecting Smart Objects

5. Constrained Devices:



Class	Definition
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

Classes of Constrained Nodes, as Defined by RFC 7228

6. Constrained-Node Networks:

- While several of the IoT access technologies, such as Wi-Fi and cellular, are applicable to laptops, smart phones, and some IoT devices, some IoT access technologies are more suited to specifically connect constrained nodes.
- Typical examples are 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 in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes.

Module – 2 Connecting Smart Objects

6. Constrained-Node Networks:

- **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 must be evaluated in the context of the following characteristics for use-case applicability:**
    - **data rate and throughput, latency and determinism, and overhead and payload.**

Module – 2 Connecting Smart Objects

6. Constrained-Node Networks:

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.**
- **Technologies not particularly designed for IoT, such as cellular and Wi-Fi, match up well to IoT applications with high bandwidth requirements.**
- **Nodes involved with video analytics have a need for high data rates.**
- **These nodes are found in retail, airport, and smart cities environments for detecting events and driving actions.**

Module – 2 Connecting Smart Objects

6. Constrained-Node Networks:

Data Rate and Throughput:

- **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.**

Module – 2 Connecting Smart Objects

6. Constrained-Node Networks:

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.**

Module – 2 Connecting Smart Objects

6. Constrained-Node Networks:

Overhead and Payload:

- **The minimum IPv6 MTU(maximum transmission unit) size is expected to be 1280 bytes.**
- **Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs.**
- **For example, the payload size for IEEE 802.15.4 is 127 bytes and requires an IPv6 payload with a minimum MTU of 1280 bytes to be fragmented.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

Topics that are addressed for each IoT access technology:

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

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 802.15.4

- **IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.**
- **This access technology enables easy installation using a compact protocol stack while remaining both simple and flexible.**

Module – 2 IoT Access Technologies

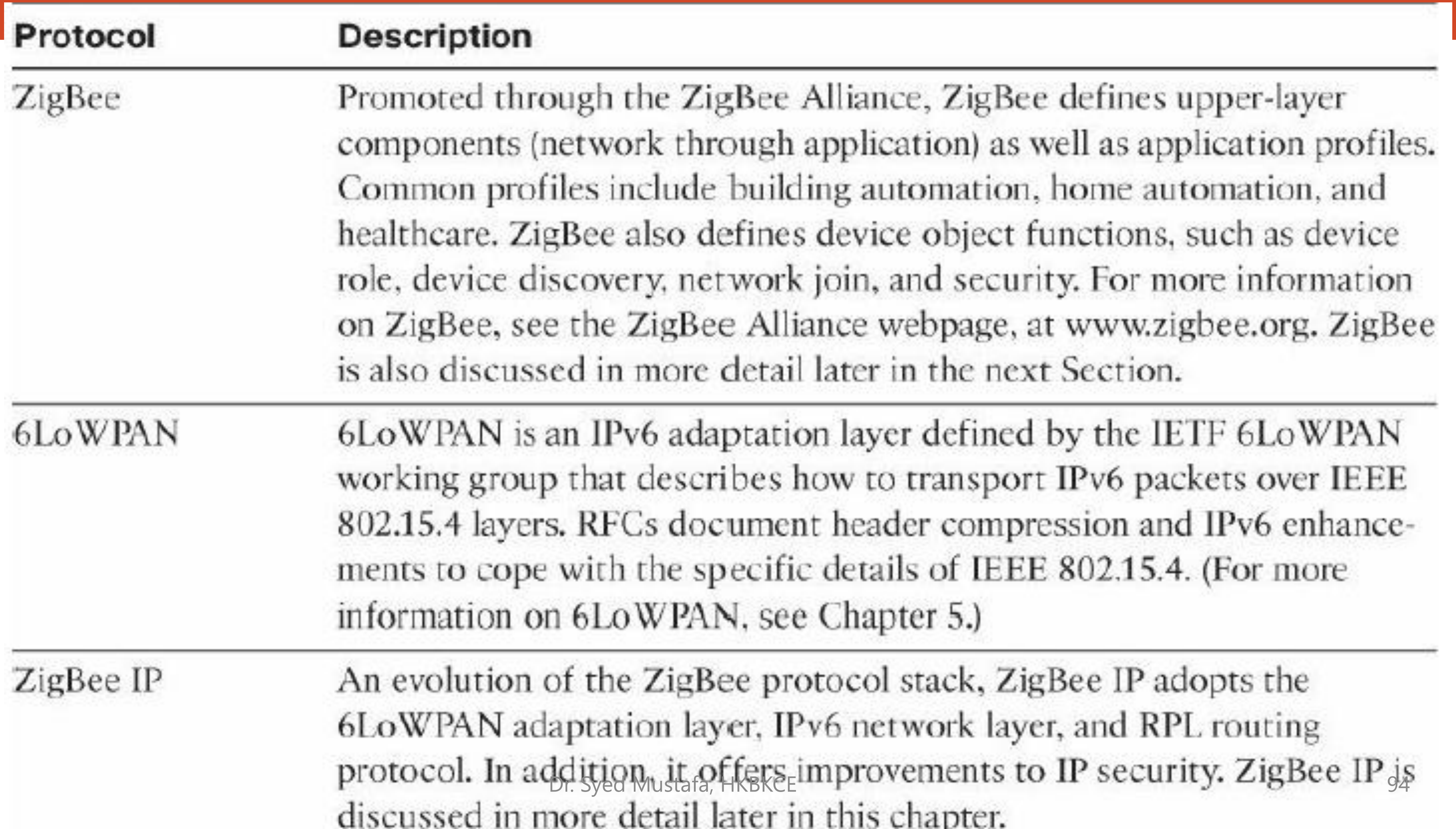
IoT Access Technologies: IEEE 802.15.4

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 standard has solution for low complexity wireless devices with low data rates that need many months or even years of battery life.
- Since 2003, the IEEE has published several iterations of the IEEE 802.15.4 specification, each labeled with the publication’s year.
- For example, IEEE 802.15.4-2003 was published in 2003, 802.15.4-2006 was released in 2006, and 802.15.4-2011 and 802.15.4-2015 were issued in 2011 and 2015, respectively.

Module – 2 IoT Access Technologies

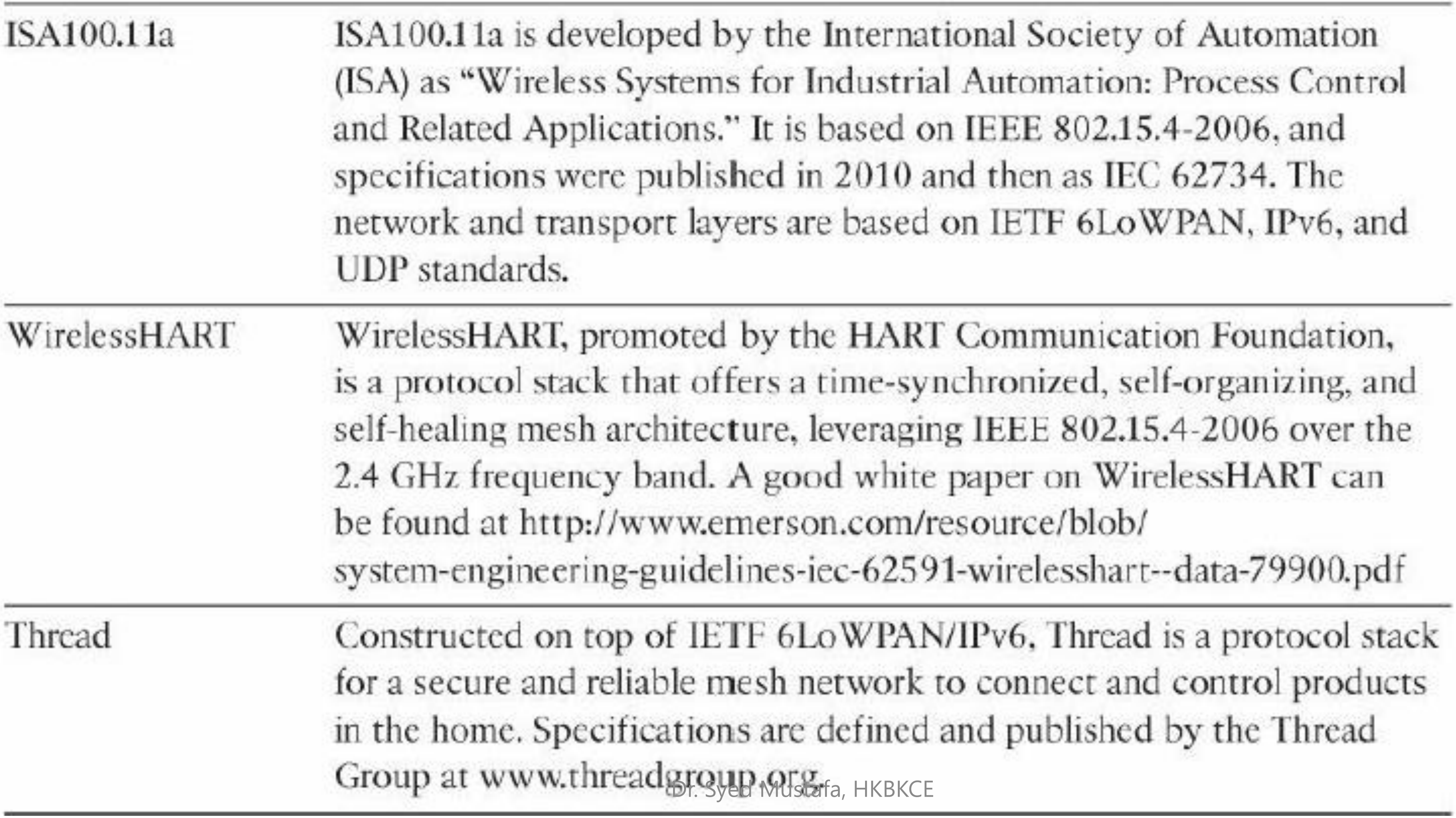
Protocol Stacks Utilizing IEEE 802.15.4



Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.

Module – 2 IoT Access Technologies

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.

IoT Access Technologies: IEEE 802.15.4

ZigBee:

- Based on the idea of ZigBee-style networks in the late 1990s, the first ZigBee specification was ratified in 2004, shortly after the release of the IEEE 802.15.4 specification the previous year.
- industry support has grown to more than 400 companies that are members of the ZigBee Alliance.
- Similar to the Wi-Fi Alliance, the Zigbee Alliance is an industry group formed to certify interoperability between vendors and it is committed to driving and evolving ZigBee as an IoT solution for interconnecting smart objects.

IoT Access Technologies: IEEE 802.15.4

<u>ZigBee:</u>

- **ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs.**
- **products that are ZigBee compliant and certified by the ZigBee Alliance should interoperate even though different vendors may manufacture them.**
- **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.**
- **These sets of commands and message types are called clusters.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

ZigBee:

- **For home automation, ZigBee can control lighting, thermostats, and security functions.**
- **ZigBee Smart Energy brings together a variety of interoperable products, such as smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water.**
- **These ZigBee products are controlled by the utility provider and can help coordinate usage between homes and businesses and the utility provider itself to provide more efficient operations.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

ZigBee:

- **ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers.**
- **ZigBee specifies the 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

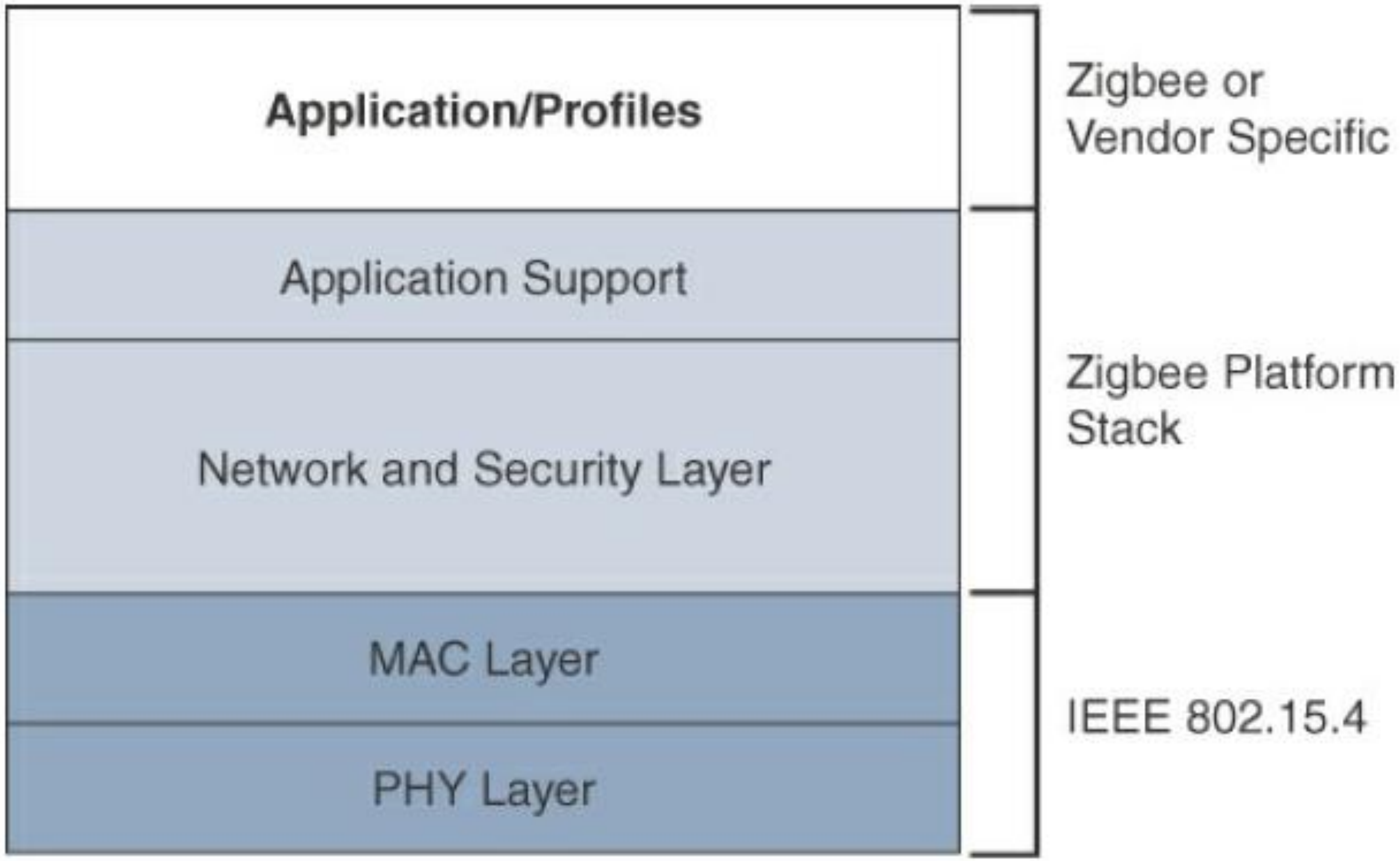
ZigBee:

- **The network layer is also responsible for forming the appropriate topology, which is often a mesh but could be a star or tree as well.**
- **From a security perspective, ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.**
- **The application support layer interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

ZigBee:



Application/Profiles

Application Support

Network and Security Layer

MAC Layer

PHY Layer

Zigbee or Vendor Specific

Zigbee Platform Stack

IEEE 802.15.4

High-Level ZigBee Protocol Stack

IoT Access Technologies: IEEE 802.15.4

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

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

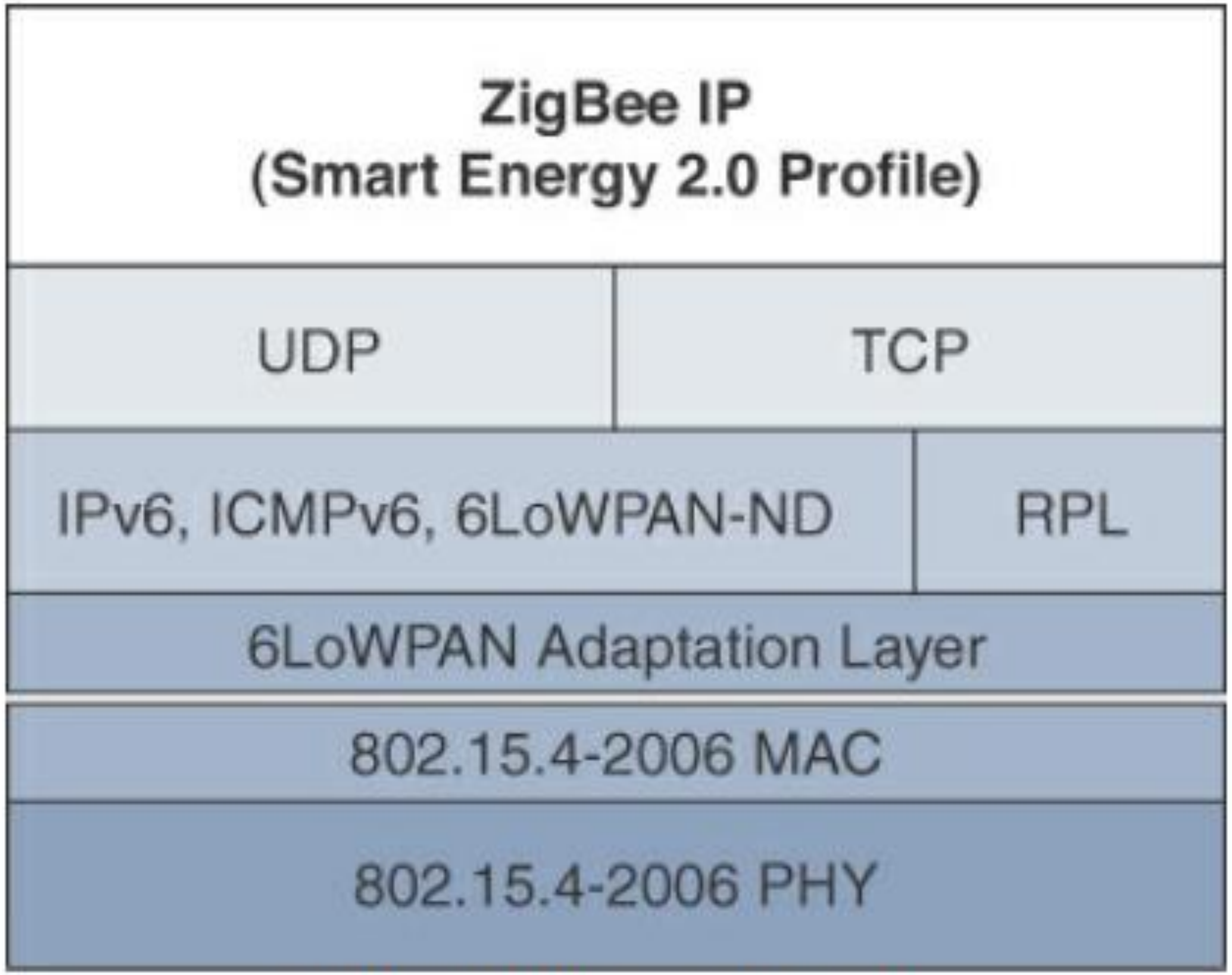
<u>ZigBee IP:</u>

- **They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.**
- **ZigBee IP is a critical part of the Smart Energy (SE) Profile 2.0 specification from the ZigBee Alliance. SE 2.0 is aimed at smart metering and residential energy management systems.**
- **In fact, ZigBee IP was designed specifically for SE 2.0 but it is not limited to this use case.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

ZigBee IP:



ZigBee IP Protocol Stack

IoT Access Technologies: IEEE 802.15.4

ZigBee IP:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

<u>Physical Layer:</u>

- **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.**

IoT Access Technologies: IEEE 802.15.4

Physical Layer:

- **The original physical layer transmission options were as follows:**
  - **2.4 GHz, 16 channels, with a data rate of 250 kbps**
  - **915 MHz, 10 channels, with a data rate of 40 kbps**
  - **868 MHz, 1 channel, with a data rate of 20 kbps**
- **only the 2.4 GHz band operates worldwide.**

IoT Access Technologies: IEEE 802.15.4

<u>Physical Layer:</u>

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 phaseshift 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

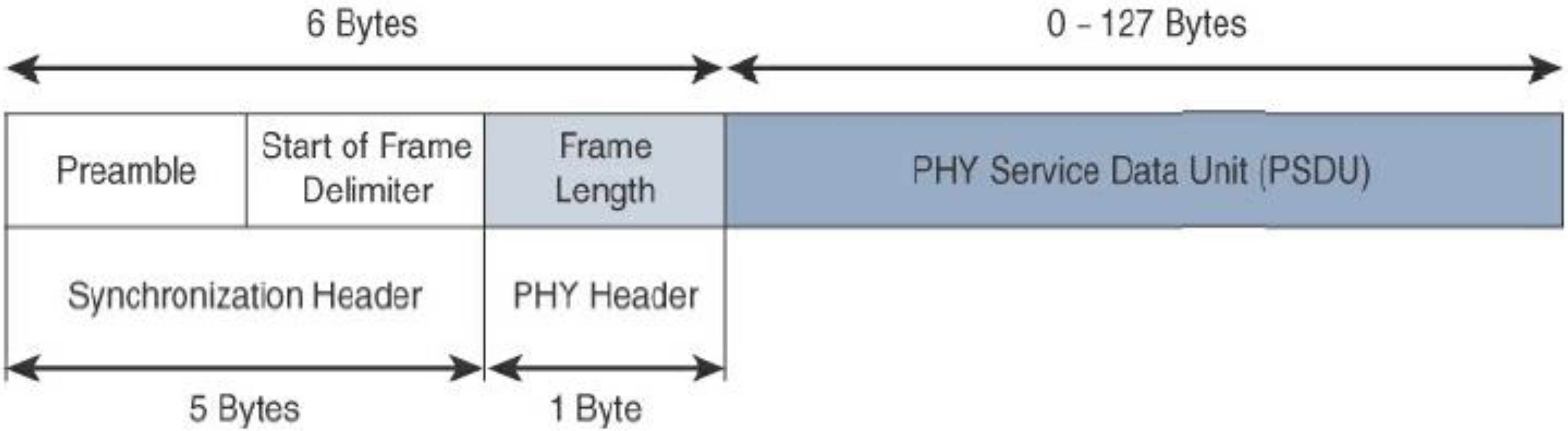
Physical Layer:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

Physical Layer:



IEEE 802.15.4 PHY Format

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 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 (for parallel construction) 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

Physical Layer:

- The PHY Header portion of the PHY frame shown in Figure is simply a 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.

IoT Access Technologies: IEEE 802.15.4

MAC Layer:

The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated.

The 802.15.4 MAC layer performs the following tasks:

- **Network beaconing for devices acting as coordinators (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**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

MAC Layer:

The MAC layer achieves these tasks by using our types of MAC frames are specified in 802.15.4:

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

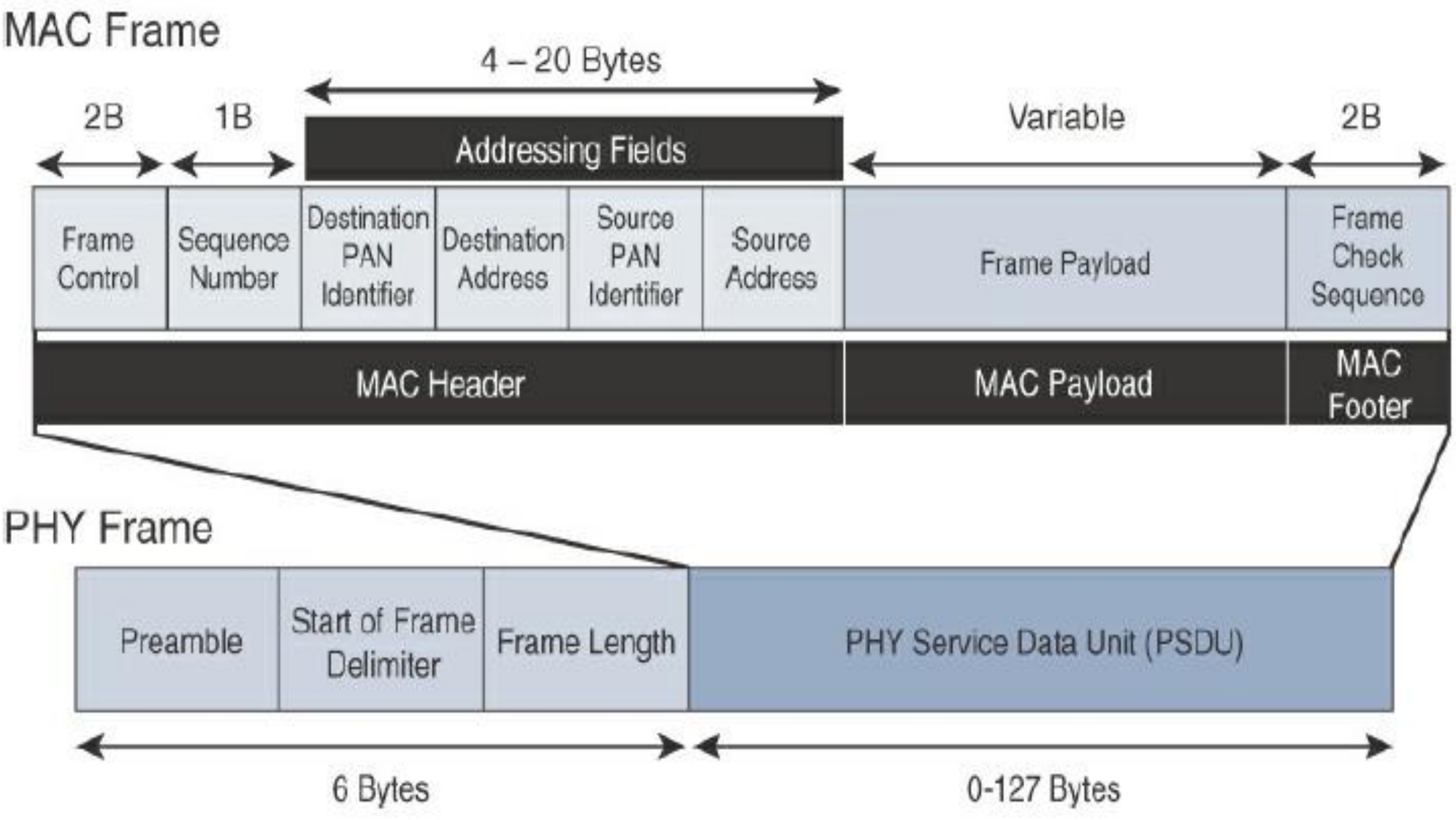
Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

<u>MAC Layer:</u>

Notice that the MAC frame is carried as the PHY payload.

The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.



IEEE 802.15.4 MAC Format

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

MAC Layer:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

MAC Layer:

- **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.**

Module – 2 IoT Access Technologies

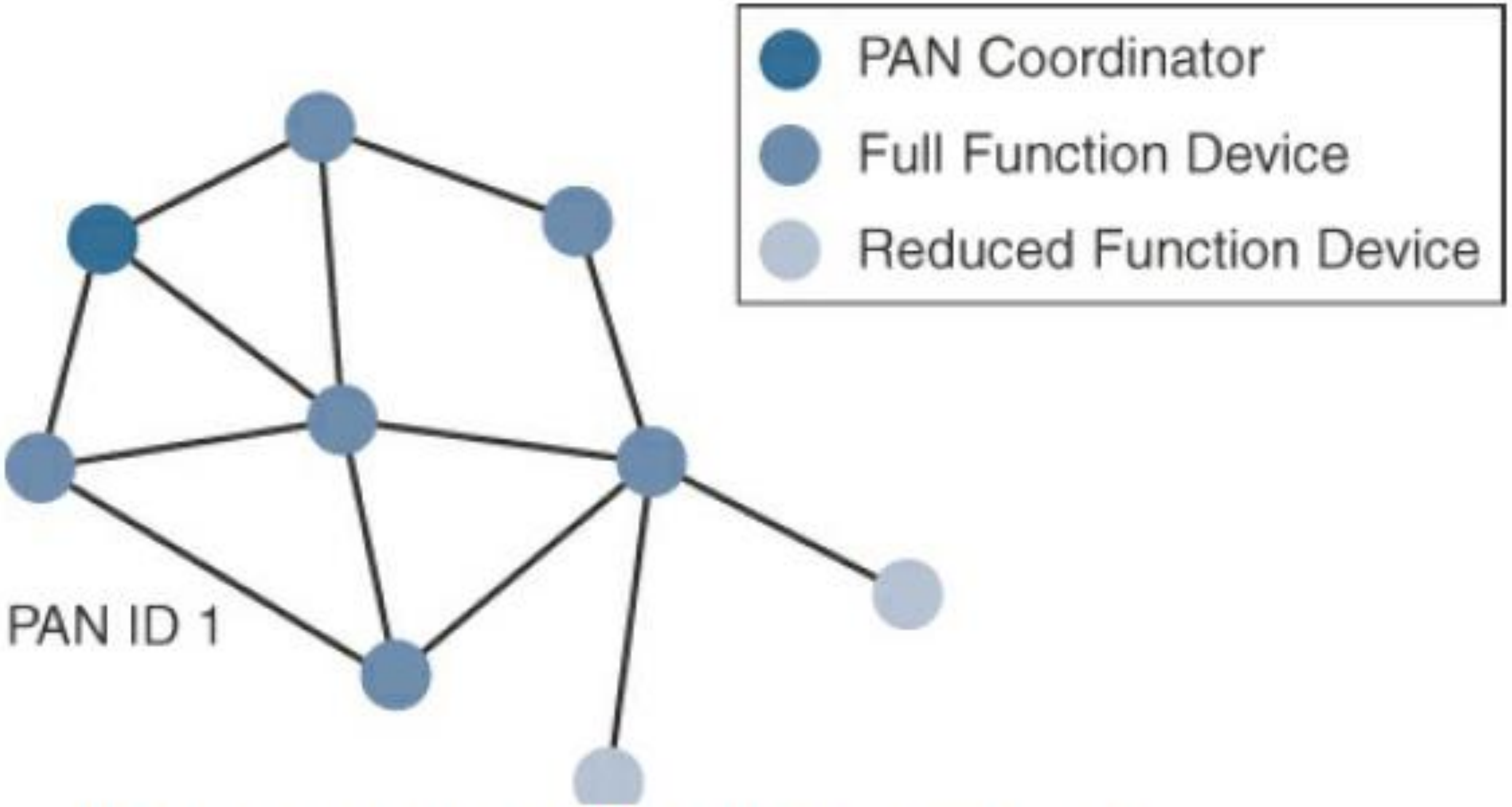
IoT Access Technologies: IEEE 802.15.4

<u>Topology:</u>

- **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.**

IoT Access Technologies: IEEE 802.15.4

Topology:



802.15.4 Sample Mesh Network Topology

IoT Access Technologies: IEEE 802.15.4

Topology:

- **Full-function devices (FFDs) and reduced-function devices (RFDs) are defined in IEEE 802.15.4.**
- **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.**
- **Notice in Figure that 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

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.**
- **Established by the US National Institute of Standards and Technology in 2001, AES is a block cipher, which means it operates on fixed-size blocks of data.**
- **The use of AES by the US government and its widespread adoption in the private sector has helped it become one of the most popular algorithms used in symmetric key cryptography.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

Security:

- **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.**
- **Enabling these security features for 802.15.4 changes the frame format 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

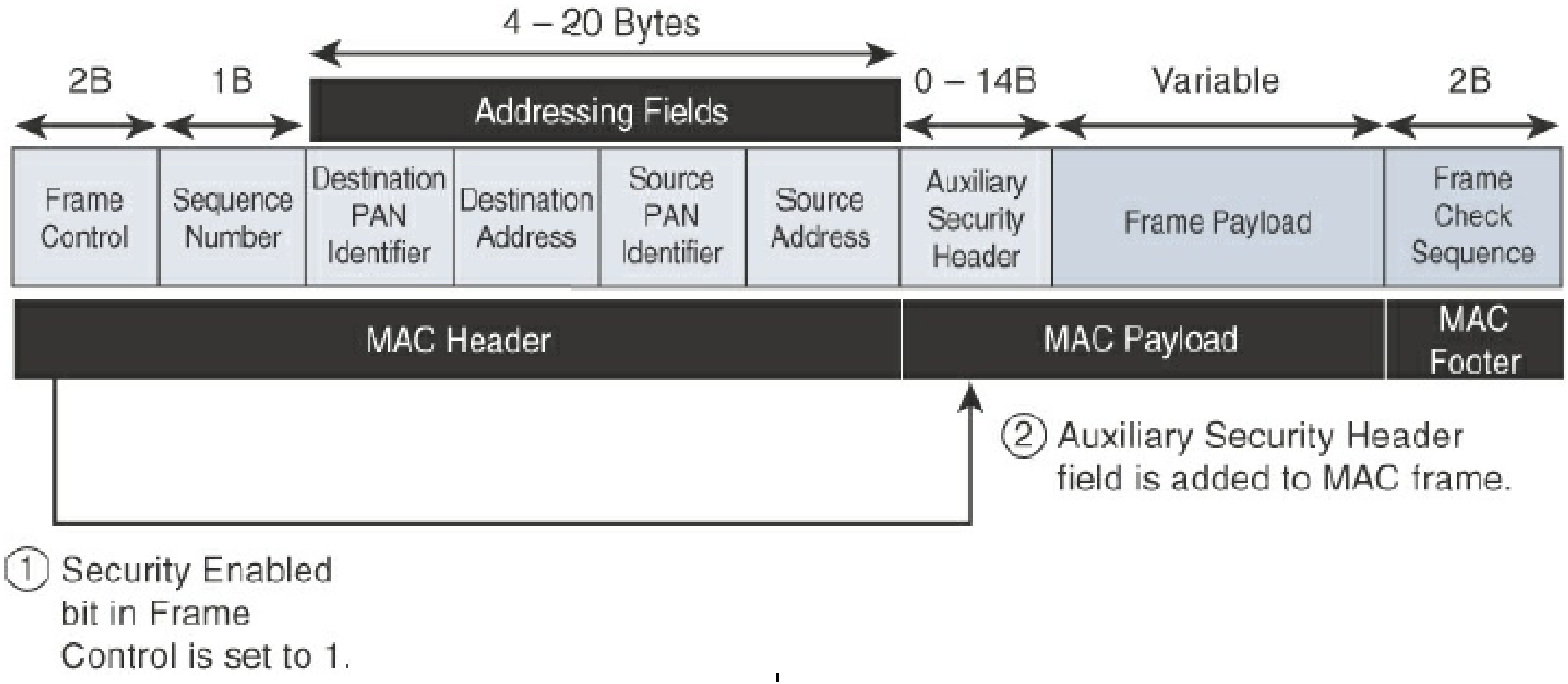
Security:

- **This Security Enabled 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.**
- **Next Figure shows the IEEE 802.15.4 frame format at a high level, with the Security Enabled bit set and the Auxiliary Security Header field present.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

Security:



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

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

<u>Competitive Technologies:</u>

- **The IEEE 802.15.4 PHY and MAC layers are the foundations for several networking profiles that compete against each other in various IoT access environments.**
- **These various vendors and organizations build upper-layer protocol stacks on top of an 802.15.4 core.**
- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

Competitive Technologies:

- **Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military forces for many years, mainly for logistics purposes.**
- **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.**
- **Frequencies of 433 MHz, 868 MHz, and 915 MHz have been defined, enabling data rates up to 166.667 kbps and a maximum payload of 256 bytes.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

IEEE 802.15.4 Conclusions:

- **The IEEE 802.15.4 wireless PHY and MAC layers are mature specifications that are the foundation for various industry standards and products**
- **The PHY layer offers a maximum speed of up to 250 kbps, but this varies based on modulation and frequency.**
- **The MAC layer for 802.15.4 is robust and handles how data is transmitted and received over the PHY layer.**
- **Specifically, the MAC layer handles the association and disassociation of devices to/from a PAN, reliable communications between devices, security, and the formation of various topologies.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4

IEEE 802.15.4 Conclusions:

- **The topologies used in 802.15.4 include star, peer-to-peer, and cluster trees that allow for the formation of mesh networks.**
- **From a security perspective, 802.15.4 utilizes AES encryption to allow secure communications and also provide data integrity. The main competitor to IEEE 802.15.4 is DASH7, another wireless technology**
- **IEEE 802.15.4 has an edge in the marketplace through all the different vendors and organizations that utilize its PHY and MAC layers.**
- **For IoT sensor deployments requiring low power, low data rate, and low complexity, the IEEE 802.15.4 standard deserves strong consideration.**

Module – 2 IoT Access Technologies

IoT Access Technologies: 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.

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

Smart grid is associated with the modernization of the power grid and utilities infrastructure by connecting intelligent devices and communications.

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.

Module – 2 IoT Access Technologies

IoT Access Technologies: 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 technology applies to IoT use cases such as :

- **Distribution automation and industrial supervisory control and data acquisition (SCADA) environments for remote monitoring and control .**
- **Public lighting**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

- **Environmental wireless sensors in smart cities**
- **Electrical vehicle charging stations**
- **Smart parking meters**
- **Microgrids**
- **Renewable energy**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

<u>Standardization and Alliances</u>

- **Because 802.15.4g-2012 and 802.15.4e-2012 are simply amendments to IEEE 802.15.4-2011, the same IEEE 802.15 Task Group 4 standards body authors, maintains, and integrates them into the next release of the core specification.**
- **The additional capabilities and options provided by 802.15.4g-2012 and 802.15.4e-2012 led to additional difficulty in achieving the interoperability between devices and mixed vendors that users requested.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

Standardization and Alliances

- **To guarantee interoperability, the Wi-SUN Alliance was formed. (SUN stands for smart utility network.)**
- **This organization is not a standards body but is instead an industry alliance that defines communication profiles for smart utility and related networks.**
- **These profiles are based on open standards, such as 802.15.4g-2012, 802.15.4e-2012, IPv6, 6LoWPAN, and UDP for the FAN profile.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

<u>Physical Layer:</u>

- **In IEEE 802.15.4g-2012, the original IEEE 802.15.4 maximum PSDU or payload size of 127 bytes was increased for the SUN PHY to 2047 bytes.**
- **This provides a better match for the greater packet sizes found in many upper-layer protocols.**
- **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.**

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

Physical Layer:

- **The SUN PHY, as described in IEEE 802.15.4g-2012, supports multiple data rates in bands ranging from 169 MHz to 2.4 GHz.**
- **These bands are covered in the unlicensed ISM frequency spectrum specified by various countries and regions.**
- **Within these bands, data must be modulated onto the frequency using at least one of the following PHY mechanisms to be IEEE 802.15.4g compliant:**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

Physical Layer:

- **Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK):**
  - **Offers good transmit power efficiency due to the constant envelope of the transmit signal**
- **Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM):**
  - **Provides higher data rates but may be too complex for low-cost and low-power devices**
- **Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying (MR-O-QPSK):**
  - **Shares the same characteristics of the IEEE 802.15.4-2006 O-QPSK PHY, making multi-mode systems more cost effective and easier to design**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

<u>MAC Layer:</u>

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

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

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

1. **Time-Slotted Channel Hopping (TSCH):**

- **TSCH is an IEEE 802.15.4e- 2012 MAC operation mode that works to guarantee media access and channel diversity.**
- **Channel hopping, also known as frequency hopping, utilizes different channels for transmission at different times.**
- **TSCH divides time into fixed time periods, or "time slots," which offer guaranteed bandwidth and predictable latency.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

1. **Time-Slotted Channel Hopping (TSCH):**

- **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, especially for industrial use cases.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

2. 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

3. **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

4. 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.**
- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

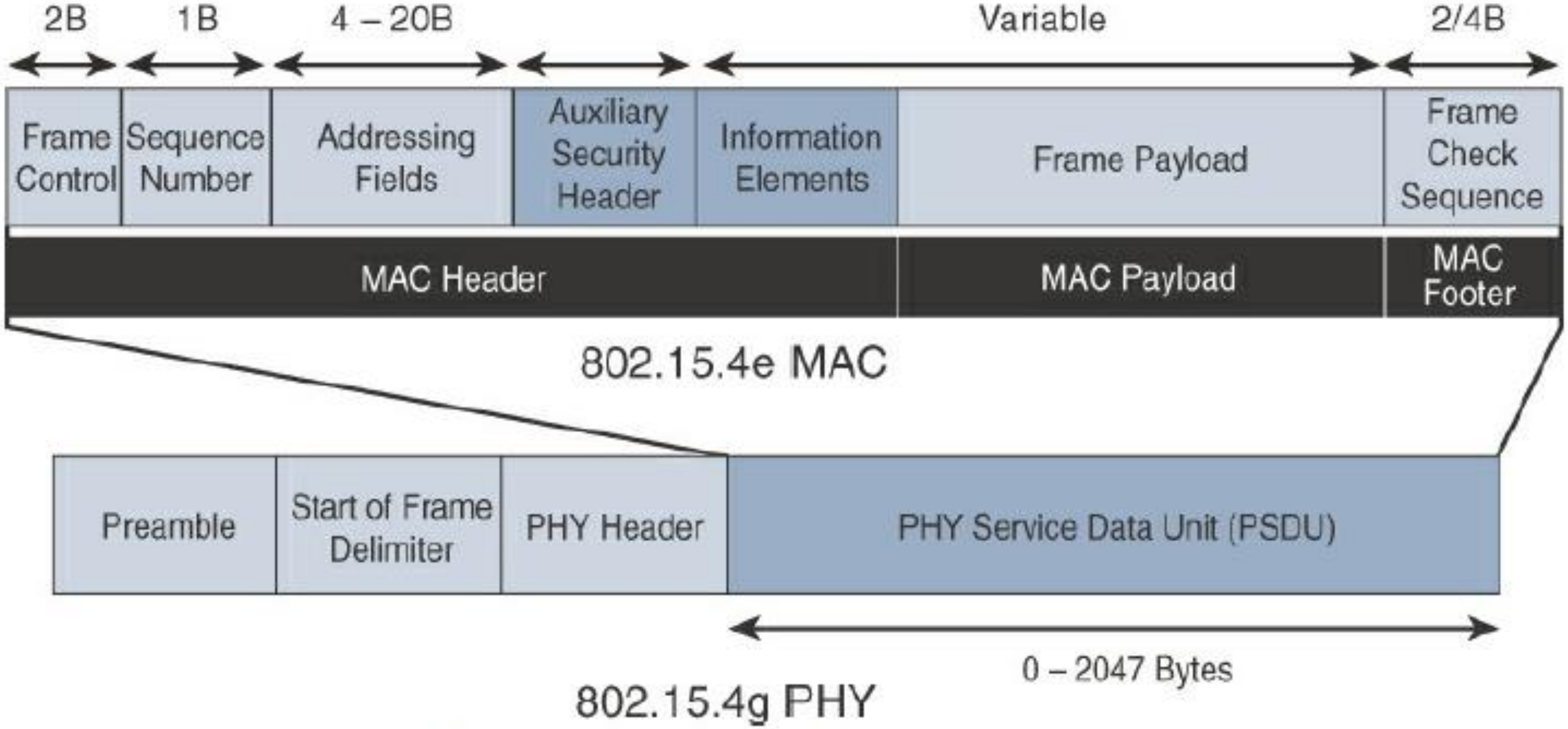
5. Enhanced Acknowledgement:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:



IEEE 802.15.4g/e MAC Frame Format

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

MAC Layer:

- The 802.15.4e MAC is similar to the 802.15.4 MAC
- 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.
- This field is optionally supported in both 802.15.4e-2012 and 802.15.4, starting with the 802.15.4-2006 specification.
- the IE field contains one or more information elements that allow for additional information to be exchanged at the MAC layer.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

Topology:

- Deployments of IEEE 802.15.4g-2012 are mostly based on a mesh topology.
- because a mesh topology is typically the best choice for use cases in the industrial and smart cities areas where 802.15.4g-2012 is applied.
- A mesh topology allows deployments to be done in urban or rural areas, expanding the distance between nodes that can relay the traffic of other nodes.
- Support for battery-powered nodes with a long lifecycle requires optimized Layer 2 forwarding or Layer 3 routing protocol implementations.
- This provides an extra level of complexity but is necessary in order to cope with sleeping battery-powered nodes.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

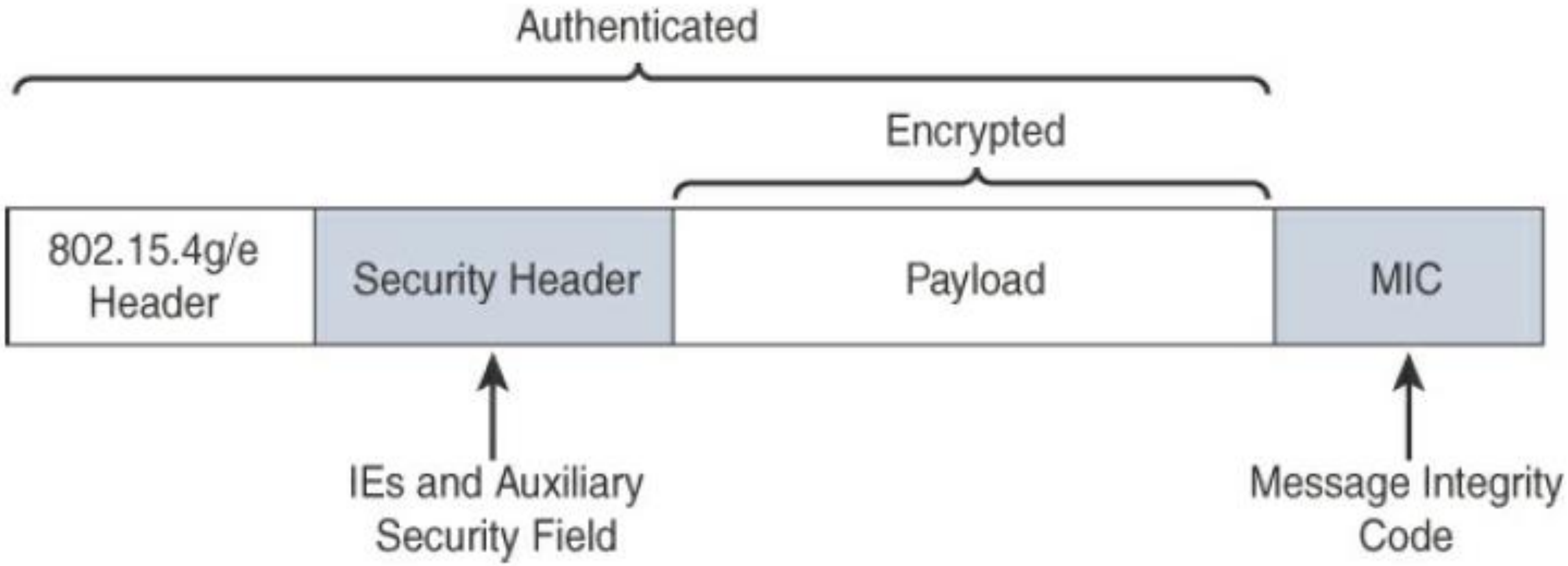
Security:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

Security:



IEEE 802.15.4g/e MAC Layer Security

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

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 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.

Module – 2 IoT Access Technologies

IoT Access Technologies: 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 802.15.4 is well established and already deployed in many scenarios, mostly indoors.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

IEEE 802.15.4g and 802.15.4e Conclusions:

- **IEEE 802.15.4g and 802.15.4e are simply amendments to the IEEE 802.15.4 standard.**
- **They are mature specifications that are integrated into IEEE 802.15.4-2015.**
- **They have been successfully deployed in real-world scenarios, and already support millions of endpoints.**
- **IEEE 802.15.4g focuses mainly on improvements to the PHY layer, while IEEE 802.15.4e targets the MAC layer.**

IoT Access Technologies: IEEE 802.15.4g and 802.15.4e

IEEE 802.15.4g and 802.15.4e Conclusions:

- **These improvements overcome many of the disadvantages of IEEE 802.15.4, such as latency and vulnerability to multipath fading.**
- **The Wi-SUN Alliance is an important industry alliance that provides interoperability and certification for industry implementations.**
- **Utilizing 802.15.4g as a foundation, the alliance releases profiles, such as the FAN profile, to help promote the adoption of the technology while guaranteeing interoperability between vendors.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

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

- **This is a standard for Narrowband Power Line Communication (NB-PLC).**

- **NB-PLC leverages a narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power.**

IoT Access Technologies: IEEE 1901.2a

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.**
  - **This is true particularly in Europe, where PLC is the preferred technology for utilities deploying smart meter solutions.**
- **Distribution automation:**
  - **NB-PLC can be used for distribution automation, which involves monitoring and controlling all the devices in the power grid.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

NB-PLC is often found in use cases such as the following:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

NB-PLC is often found in use cases such as the following:

- **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.**

IoT Access Technologies: IEEE 1901.2a

Physical Layer:

- NB-PLC is defined for frequency bands from 3 to 500 kHz.
- The IEEE 1901.2 working group has integrated support for all world regions in order to develop a worldwide standard.
- Specifications include support for CENELEC A and B bands, US FCC-Low and FCC-above-CENELEC, and Japan ARIB bands.
- CENELEC is the French Comité Européen de Normalisation Électrotechnique, which in English translates to European Committee for Electrotechnical Standardization.
- This organization is responsible for standardization in the area of electrical engineering for Europe.
- The CENELEC A and B bands refer to 9–95 kHz and 95–125 kHz, respectively.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

Physical Layer:

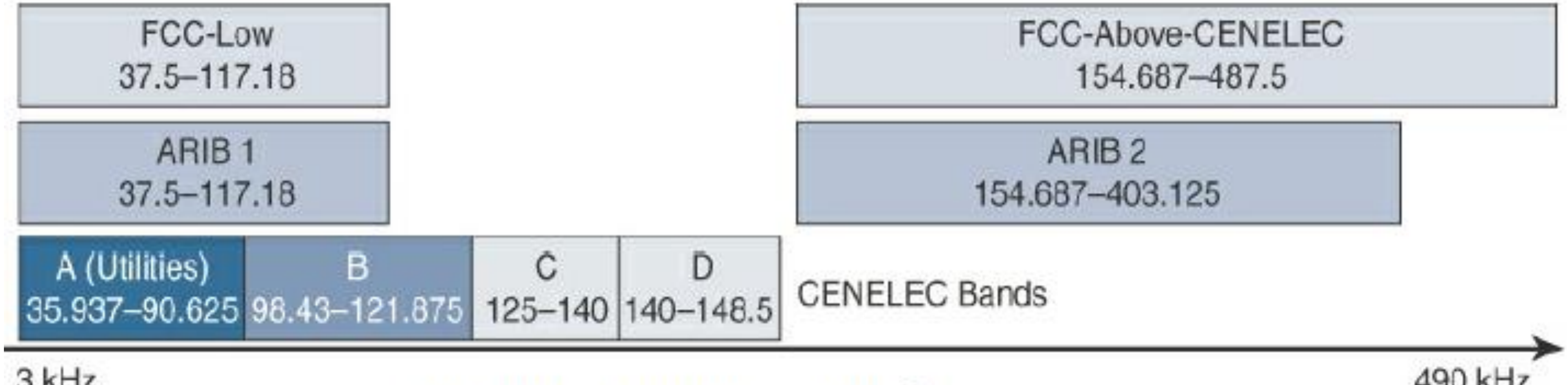
- The FCC is the Federal Communications Commission, a US government organization that regulates interstate and international communications by radio, television, wire, satellite, and cable.
- The FCC-Low band encompasses 37.5–117.1875 kHz, and the FCC-above-CENELEC band is 154.6875–487.5 kHz.
- The FCC-above-CENELEC band may become the most useful frequency due to its higher throughput and reduced interference.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

Physical Layer:

- Figure shows the various frequency bands for NB-PLC. most well-known bands are regulated by CENELEC and the FCC, but the Japan Association of Radio Industries and Businesses (ARIB) band is also present. The two ARIB frequency bands are ARIB 1, 37.5–117.1875 kHz, and ARIB 2, 154.6875–403.125 kHz.



NB-PLC Frequency Bands

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

Physical Layer:

- IEEE 1901.2a supports the largest set of coding and enables both robustness and throughput.
- The standard includes tone maps and modulations, such as robust modulation (ROBO), differential binary phase shift keying (DBPSK), differential quadrature phase shift keying (DQPSK), differential 8-point phase shift keying (D8PSK) for all bands, and optionally 16 quadrature amplitude modulation (16QAM) for some bands.
- ROBO mode transmits redundant information on multiple carriers, and DBPSK, DQPSK, and D8PSK are all variations of phase shift keying, where the phase of a signal is changed to signal a binary data transmission.
- ROBO utilizes QPSK modulation, and its throughput depends on the degree to which coding is repeated across streams.
- For example, standard ROBO uses a repetition of 4, and Super-ROBO utilizes a repetition of 6.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

Physical Layer:

- One major difference between IEEE 802.15.4g/e and IEEE 1901.2a is the full integration of different types of modulation and tone maps by a single PHY layer in the IEEE 1901.2a specification.
- The PHY payload size can change dynamically, based on channel conditions in IEEE 1901.2a.
- Therefore, MAC sublayer segmentation is implemented. If the 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.
- MAC payload segmentation is done by dividing the MAC payload into multiple smaller amounts of data (segments), based on PSDU size.
- The segmentation may require the addition of padding bytes to the last payload segment so that the final MPDU fills the PSDU.
- All forms of addressing (unicast and broadcast) are subject to segmentation.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

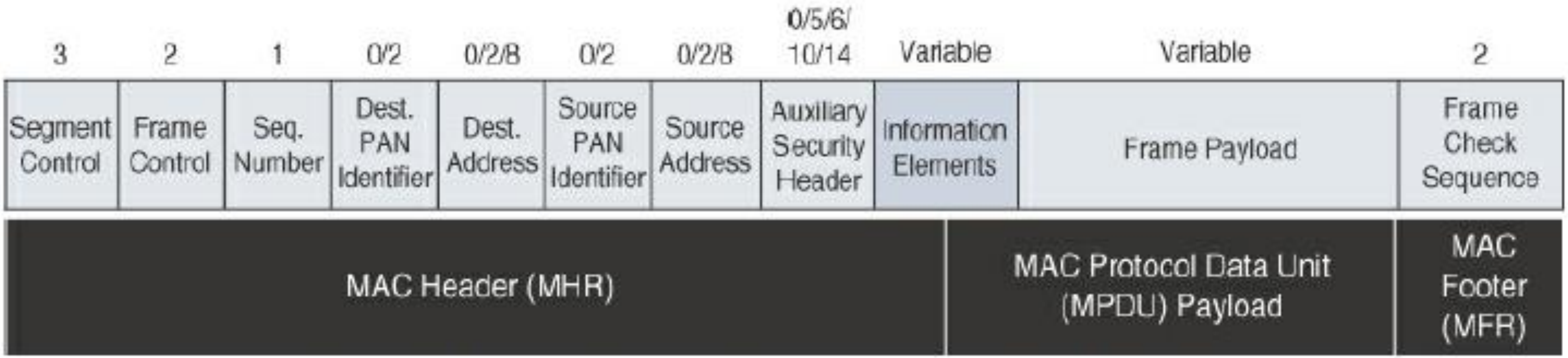
MAC Layer

- **The MAC frame format of IEEE 1901.2a is based on the IEEE 802.15.4 MAC frame but integrates the latest IEEE 802.15.4e-2012 amendment, which enables key features to be supported.**
- **One of the key components brought from 802.15.4e to IEEE 1901.2a is information elements.**
- **With IE support, additional capabilities, such as IEEE 802.15.9 Key Management Protocol and SSID, are supported.**
- **Figure provides an overview of the general MAC frame format for IEEE 1901.2.**
- **Note that the numeric value above each field in the frame shows the size of the field, in bytes.**

Module – 2 IoT Access Technologies

IoT Access Technologies: <u>IEEE 1901.2a</u>

<u>MAC Layer</u>



3	2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	Variable	Variable	2
Segment Control	Frame Control	Seq. Number	Dest. PAN Identifier	Dest. Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Information Elements	Frame Payload	Frame Check Sequence
MAC Header (MHR)									MAC Protocol Data Unit (MPDU) Payload	MAC Footer (MFR)

General MAC Frame Format for IEEE 1901.2

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

MAC Layer

- **IEEE 1901.2 has a Segment Control field.**
- **This is a new field that was not present in MAC frame for 802.15.4 and 802.15.4e.**
- **This field handles the segmentation or fragmentation of upper-layer packets with sizes larger than what can be carried in the MAC protocol data unit (MPDU).**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 1901.2a

Topology

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

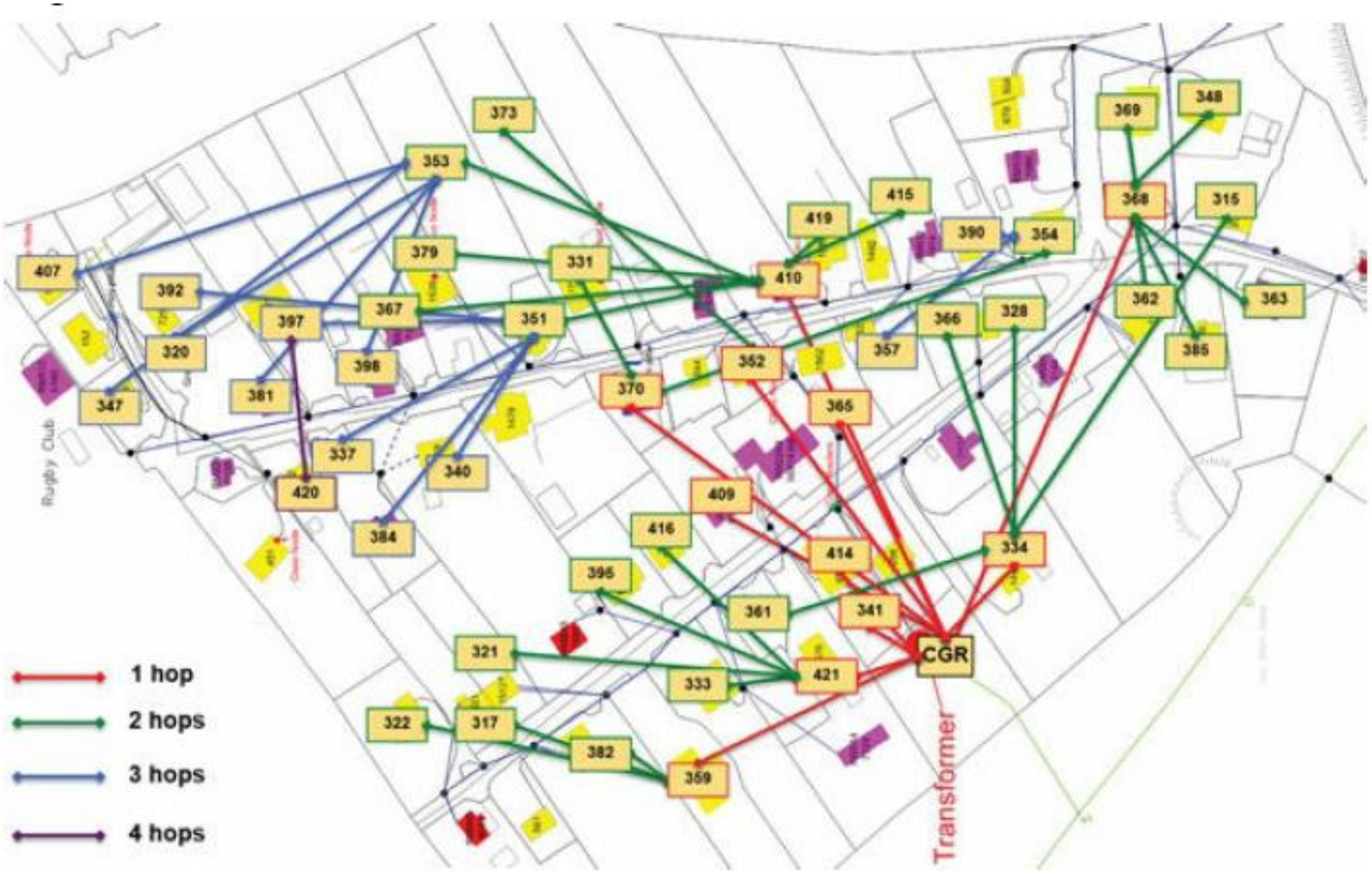
Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

Topology

- ➢ **Figure highlights a network scenario in which a PLC mesh network is applied to a neighborhood.**



IPv6 Mesh in NB-PLC

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

Security

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

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

Security

The 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

Security

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

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).

Both of these technologies were initially developed to address a single use case:

Smart metering deployment in Europe over the CENELEC A band.

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 1901.2a

IEEE 1901.2a Conclusions

IEEE 1901.2a is an open PHY and MAC standard approach to enable the use of Narrowband Power Line Communication.

The set of use cases for this standard depends on and also benefits from the physical power lines that interconnect the devices.

The IEEE 1901.2a standard leverages the earlier standards G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904).

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 802.11ah:

- **Wi-Fi lacks sub-GHz support for better signal penetration, low power for battery-powered nodes, and the ability to support a large number of devices.**
- **For these reasons, the IEEE 802.11 working group launched a task group named IEEE 802.11ah to specify a sub-GHz version of Wi-Fi.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

IEEE 802.11ah:

Three main use cases are identified for IEEE 802.11ah:

- **Sensors and meters covering a smart grid:**
  - **Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors**
- **Backhaul aggregation of industrial sensors and meter data:**
  - **Potentially connecting IEEE 802.15.4g subnetworks**
- **Extended range Wi-Fi:**
  - **For outdoor extended-range hotspot or cellular traffic offloading when distances already**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

Standardization and Alliances:

- In July 2010, the IEEE 802.11 working group worked on an "industrial Wi-Fi" and created the IEEE 802.11ah group.
- The 802.11ah specification would operate in unlicensed sub-GHz frequency bands, similar to IEEE 802.15.4 and other LPWA technologies.
- The industry organization that promotes Wi-Fi certifications and interoperability for 2.4 GHz and 5 GHz products is the Wi-Fi Alliance.
- The Wi-Fi Alliance is a similar body to the Wi-SUN Alliance.
- For the 802.11ah standard, the Wi-Fi Alliance defined a new brand called Wi-Fi HaLow.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

Physical Layer:

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

For example, various countries and regions use the following bands for IEEE 802.11ah:

868–868.6 MHz for EMEAR, 902–928 MHz and associated subsets for North America and Asia-Pacific regions, and 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779– 787 MHz for China.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

MAC Layer:

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

Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:

1. **Number of devices: Has been scaled up to 8192 per access point.**
2. **MAC header: Has been shortened to allow more efficient communication.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

MAC Layer:

Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:

3. **Null data packet (NDP) support: Is extended to cover several control and management frames.**
   - **Relevant the controinformation is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided.**
   - **This change makes l frame exchanges efficient and less power-consuming for the receiving stations.**
4. **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

MAC Layer:

Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:

5. **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.
6. **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.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

MAC Layer:

Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:

7. 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.

Module – 2 IoT Access Technologies

IoT Access Technologies: 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.**
- **It allows one 802.11ah device to act as an intermediary and relay data to another.**
- **This relay operation can be combined with a higher transmission rate or modulation and coding scheme (MCS).**
- **This means that a higher transmit rate is used by relay devices talking directly to the access point.**

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

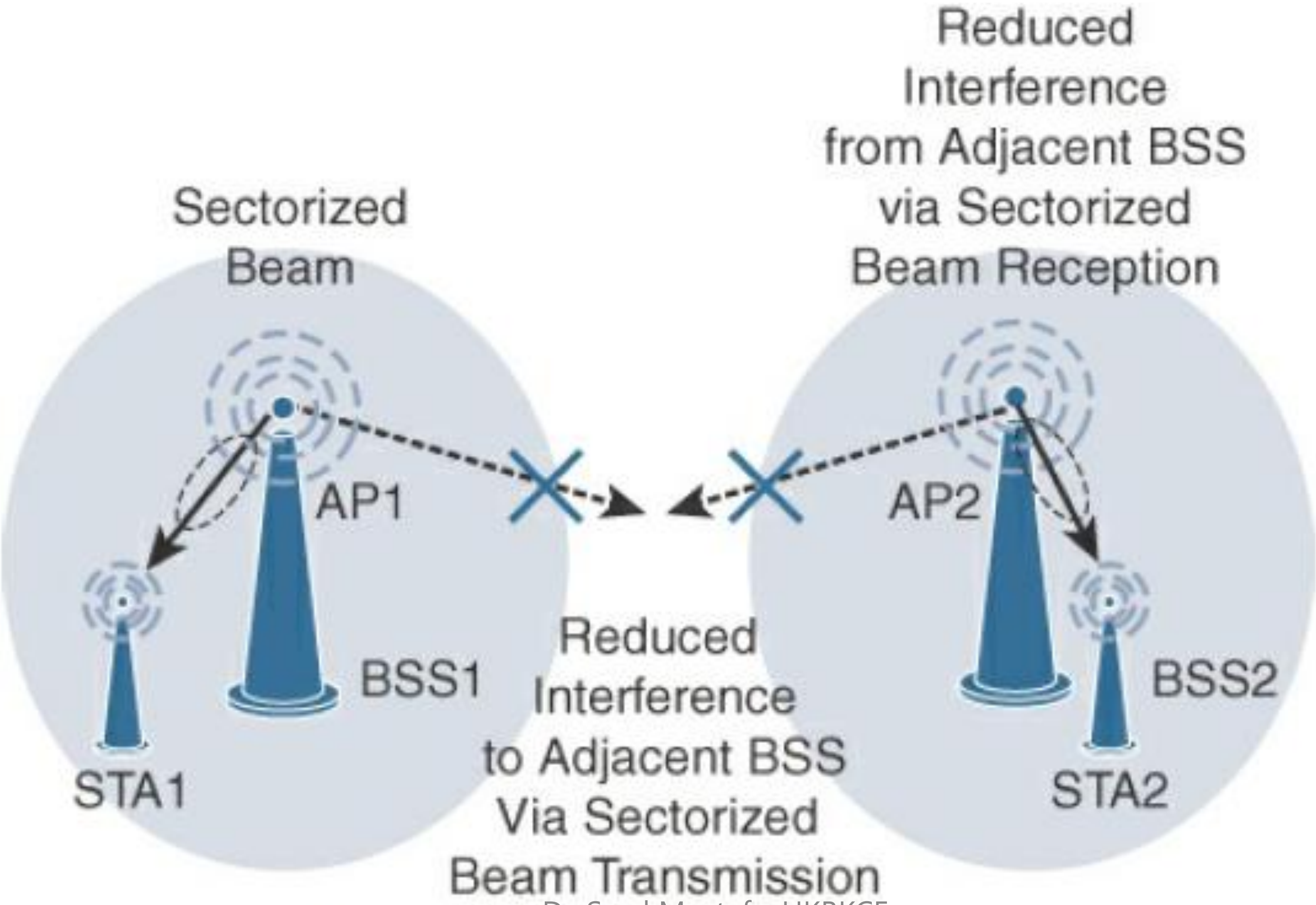
Topology:

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

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

Topology:


Sectorized Beam
Reduced Interference from Adjacent BSS via Sectorized Beam Reception
AP1
AP2
STA1
STA2
BSS1
BSS2
Reduced Interference to Adjacent BSS Via Sectorized Beam Transmission

IEEE 802.11ah Sectorization

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

Security:

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

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

Competitive Technologies:

Competitive technologies to IEEE 802.11ah are IEEE 802.15.4 and IEEE 802.15.4e, along with the competitive technologies highlighted in each of their sections.

Module – 2 IoT Access Technologies

IoT Access Technologies: IEEE 802.11ah:

IEEE 802.11ah Conclusions:

- **The IEEE 802.11ah access technology is an ongoing effort of the IEEE 802.11 working group to define an "industrial Wi-Fi."**
- **Currently, this standard is just at the beginning of its evolution.**
- **This specification offers a longer range than traditional Wi-Fi technologies and provides good support for low-power devices that need to send smaller bursts of data at lower speeds.**

Module – 2 IoT Access Technologies

IoT Access Technologies:

LoRaWAN:

- **It is a new set of wireless technologies known as Low-Power Wide-Area (LPWA).**
- **Particularly well adapted for long-range and battery-powered endpoints, LPWA technologies open new business opportunities to both services providers and enterprises considering IoT solutions.**

IoT Access Technologies: LoRaWAN:

Standardization and Alliances:

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

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

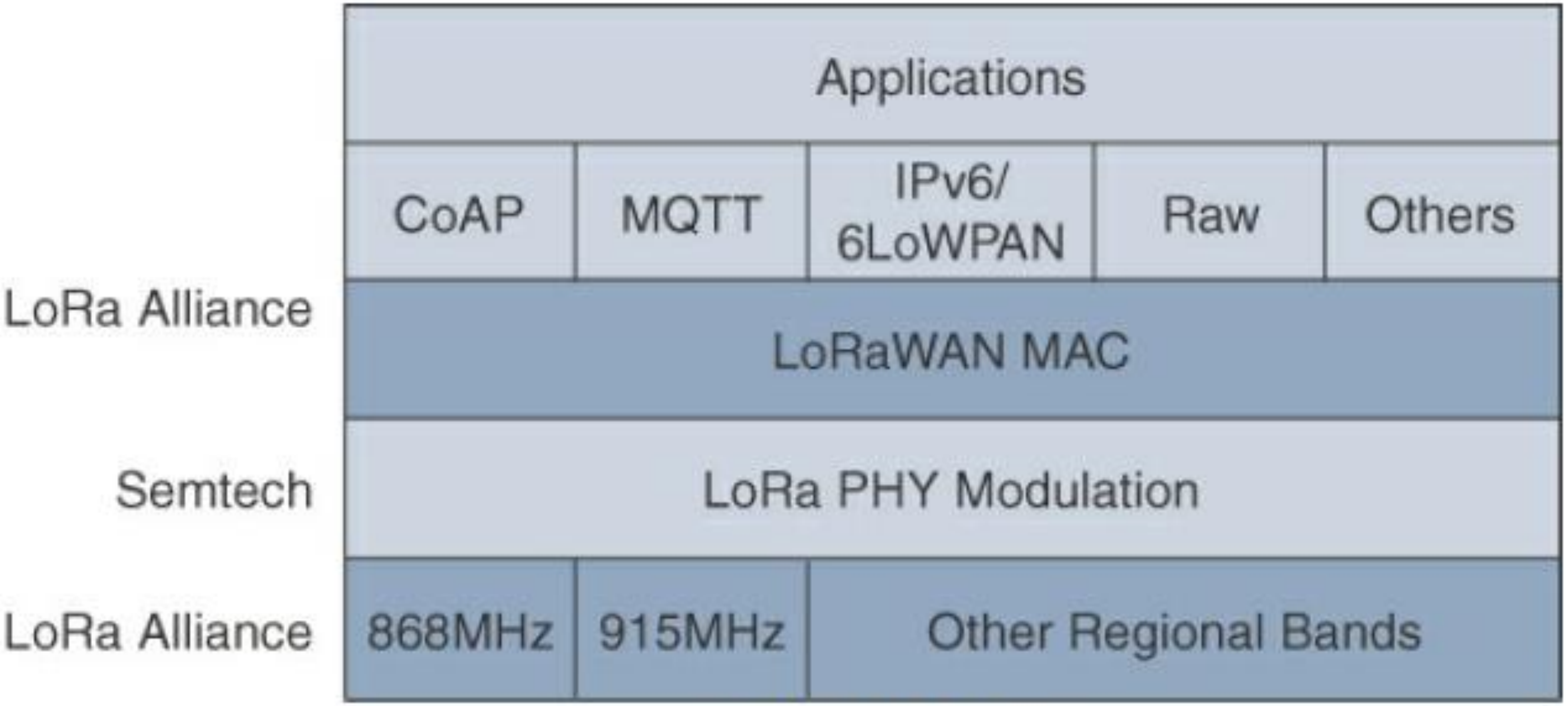
Standardization and Alliances:

- **Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors.**
- **To differentiate from the physical layer modulation known as LoRa, the LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols.**
- **Next Figure provides a high-level overview of the LoRaWAN layers.**
- **In this figure, notice that Semtech is responsible for the PHY layer, while the LoRa Alliance handles the MAC layer and regional frequency bands.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Standardization and Alliances:



LoRaWAN Layers

Module – 2 IoT Access Technologies

IoT Access Technologies: 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.**
- **In addition, it allows demodulation below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.**
- **This enables LoRa devices to receive on multiple channels in parallel.**
- **LoRaWAN 1.0.2 regional specifications describe the use of the main unlicensed sub-GHz frequency bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz, as well as regional profiles for a subset of the 902– 928 MHz bandwidth.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Physical Layer:

- **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).**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Physical Layer:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

MAC Layer:

- **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**

IoT Access Technologies: LoRaWAN:

MAC Layer:

The LoRaWAN specification documents three classes of LoRaWAN devices:

1. **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.**

IoT Access Technologies: LoRaWAN:

MAC Layer:

2. 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.

3. Class C:

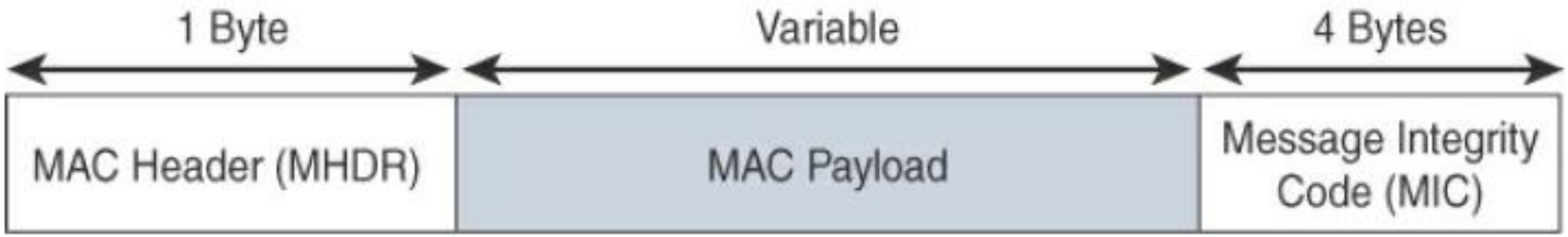
- This class is particularly adapted for powered nodes.
- This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

MAC Layer:

- **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.**



1 Byte	Variable	4 Bytes
MAC Header (MHDR)	MAC Payload	Message Integrity Code (MIC)

High-Level LoRaWAN MAC Frame Format

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

MAC Layer:

- **In version 1.0.x, LoRaWAN utilizes six MAC message types.**
- **LoRaWAN devices use join request and join accept messages for over-the-air (OTA) 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.**
- **Uplink messages are sent from endpoints to the network server and are relayed by one.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

MAC Layer:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

MAC Layer:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

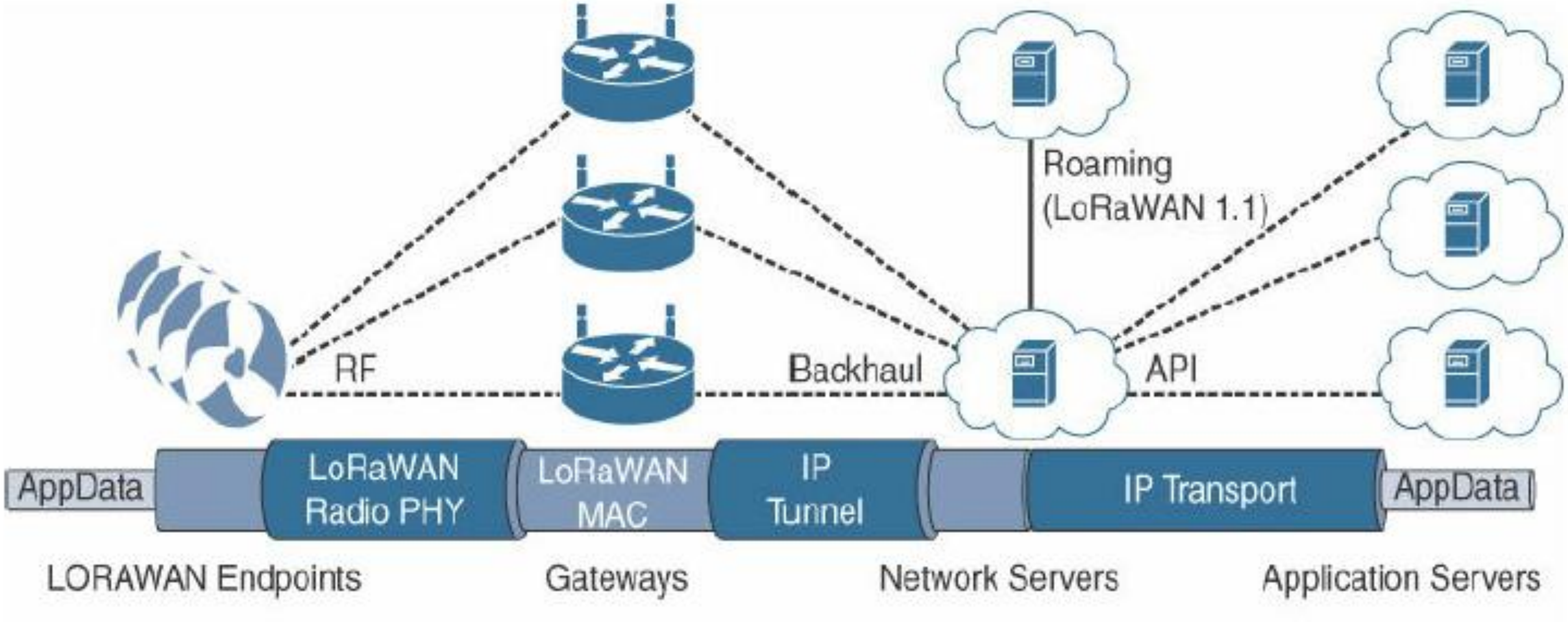
Topology:

- **LoRaWAN topology is often described as 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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Topology:



LoRaWAN Architecture

Module – 2 IoT Access Technologies

IoT Access Technologies: 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 be raw data on top of the LoRaWAN MAC layer, or the data could be stacked in multiple protocols.**
- **For example, it has upper-layer protocols, such as ZigBee Control Layer (ZCL), Constrained Application Protocol (CoAP), or Message Queuing Telemetry Transport (MQTT), with or without an IPv6/6LoWPAN layer.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Topology:

- **Figure also shows how 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, deduplication 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.**
- **ADR is a key component of the network scalability, performance, and battery life of the endpoints.**
- **The LoRaWAN network server forwards application data to the application servers**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Security:

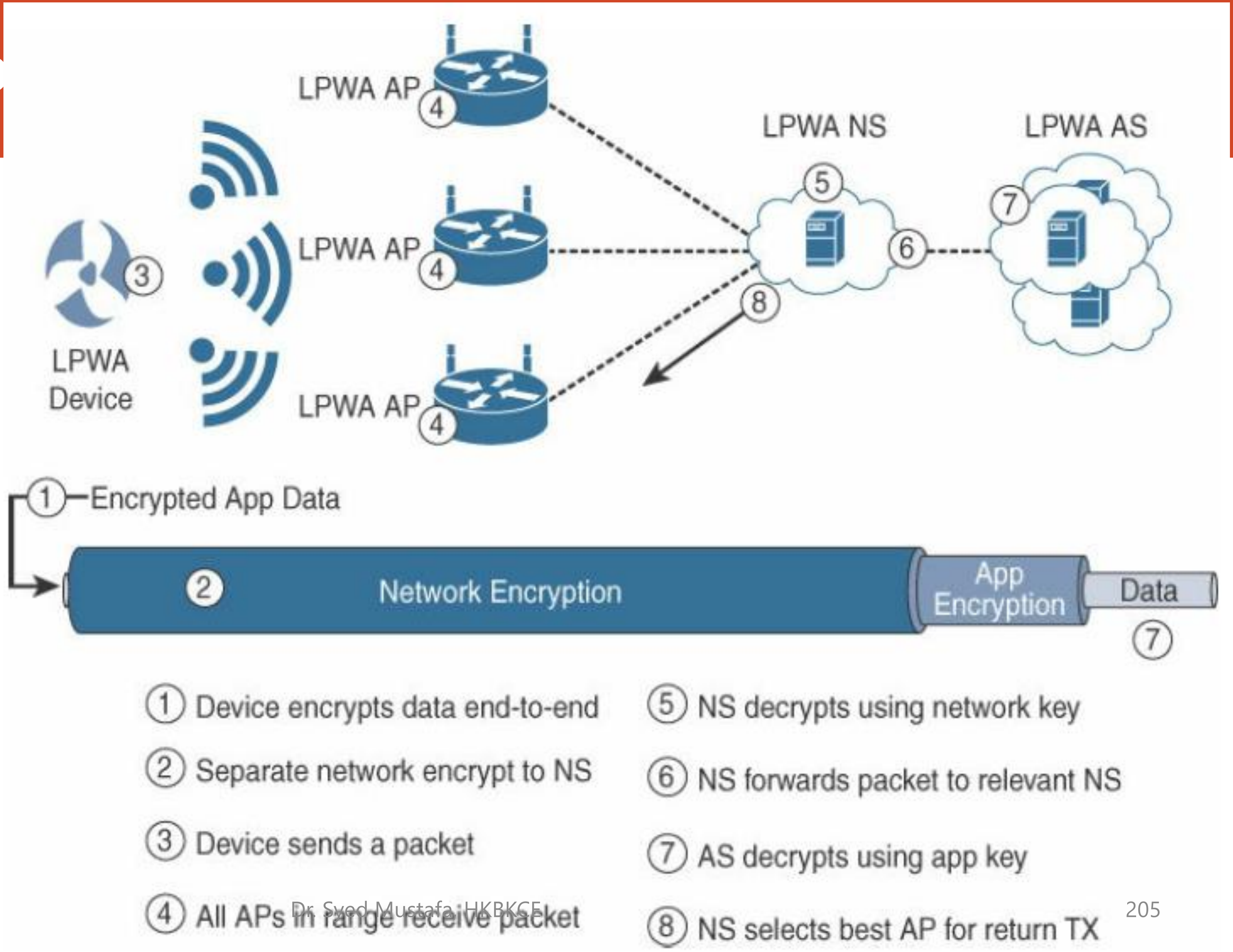
- **Security in a LoRaWAN deployment applies to different components of the architecture.**
- **LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.**
- **The first layer, called "network security" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server.**
- **Also, it protects LoRaWAN packets by performing encryption based on AES.**

Module – 2 Io

IoT Access Technologies:

LoRaWAN:

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

IoT Access Technologies: LoRaWAN:

Security:

- **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Security:

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

IoT Access Technologies: 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:

1. **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.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

Security:

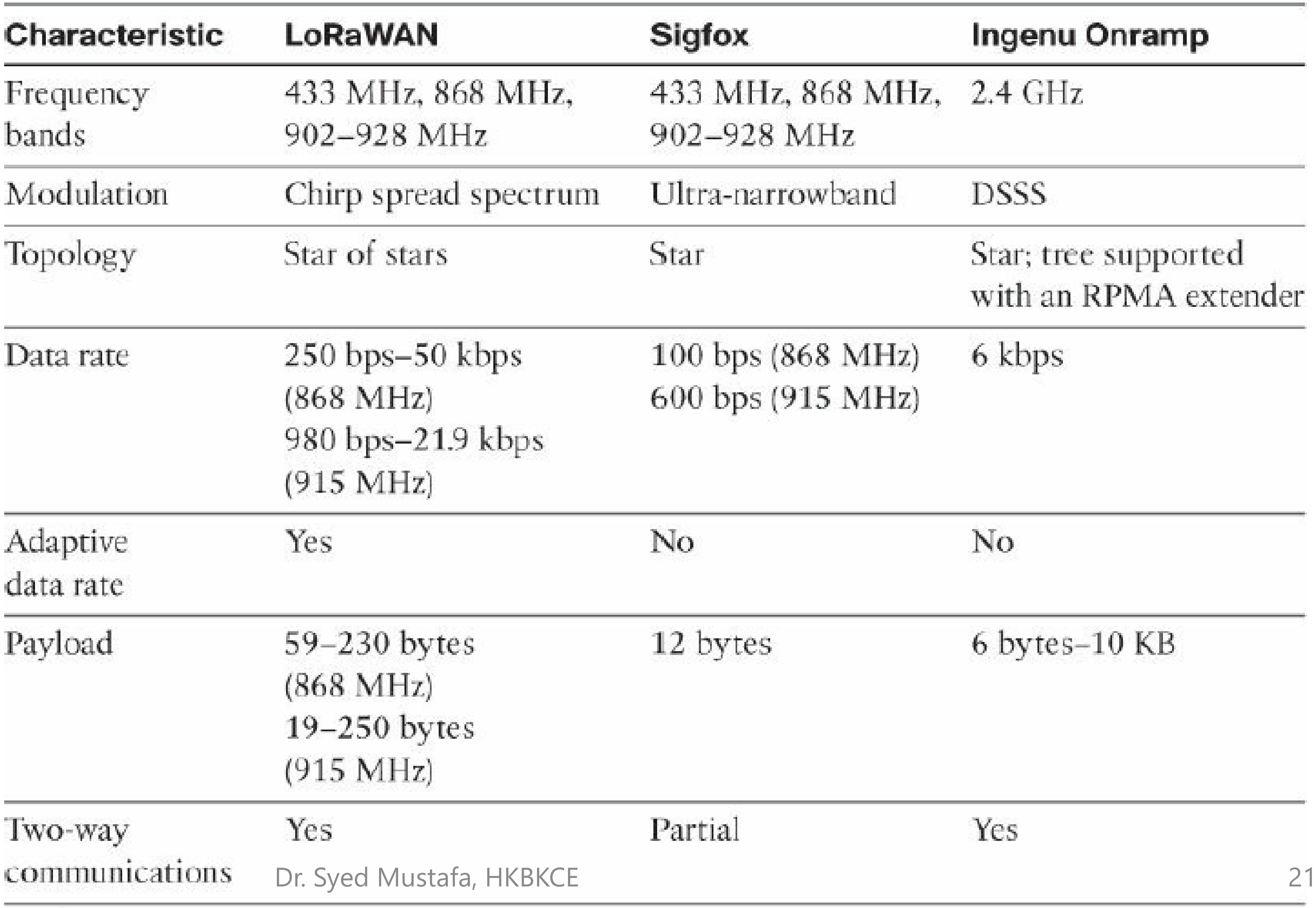
2. Over-the-air activation (OTAA):

- 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.

Module – 2 IoT Access Technologies

IoT Access Technologies: 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

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

LoRaWAN Conclusions:

- **The LoRaWAN wireless technology was developed for LPWANs that are critical for implementing many new devices on IoT networks.**
- **The term LoRa refers to the PHY layer, and LoRaWAN focuses on the architecture, the MAC layer, and a unified, single standard for seamless interoperability.**
- **LoRaWAN is managed by the LoRa Alliance, an industry organization.**

Module – 2 IoT Access Technologies

IoT Access Technologies: LoRaWAN:

LoRaWAN Conclusions:

- **The PHY and MAC layers allow LoRaWAN to cover longer distances with a data rate that can change depending on various factors.**
- **The LoRaWAN architecture depends on gateways to bridge endpoints to network servers.**
- **From a security perspective, LoRaWAN offers AES authentication and encryption at two separate layers.**