Ch-4 : Connecting Smart objects

Introduction

- IoT devices and sensors must be connected to the network for their data to be utilized.
- There are also a number of different protocols used to connect them.
- This chapter takes a look at the characteristics and communications criteria that are important for the technologies that smart objects employ for their connectivity,

Communications Criteria

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

Range

- Should indoor versus outdoor deployments be differentiated?
- Examples of short-range wireless (tens of meters) technologies Bluetooth
- Examples of medium-range wireless(tens to hundreds meters) technologies include Wi-Fi, WPAN.
- Examples of long-range Wireless are cellular (2G, 3G,4G)

Frequency Bands

- Radio spectrum is regulated by countries and/or organizations,
- For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
- For example, you can see the value of these frequencies by examining the cost that mobile operators pay for licenses in the cellular spectrum.
- For example(IOT), 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. In addition, the low data rate of this frequency matches the low volume of data that needs to be transmitted.

2.4-GHz and 5 GHz bands

- One of the two main frequency ranges used for wireless LAN communication lies between 2.400 and 2.4835 GHz. This is usually called the 2.4-GHz band, even though it does not encompass the entire range between 2.4 and 2.5 GHz.
- The other wireless LAN range is usually called the 5-GHz band because it lies between 5.150 and 5.825 GHz. The 5-GHz band actually contains the following four separate and distinct bands:

Tip You might have noticed that most of the 5-GHz bands are contiguous except for a gap between 5.350 and 5.470. At the time of this writing, this gap exists and cannot be used for wireless LANs. However, some governmental agencies have moved to reclaim the frequencies and repurpose them for wireless LANs. Efforts are also underway to add 5.825 through 5.925 GHz.

Regulatory Bodies

- The entire frequency spectrum is composed of all possible frequencies, from very low up to cosmic rays.
- The part of the spectrum that is usable for radio communication, the radio frequency (RF) portion, ranges from about 3 kHz to 300 GHz.
- To keep the RF spectrum organized and open for fair use, regulatory bodies were formed: ITU-R, FCC, ETSI, and Other Regulatory Bodies.
- A telecommunications regulatory body regulates or decides which part of the RF spectrum can be used for a particular purpose, in addition to how it can be used.

ITU-R (International Telecommunication Union Radiocommunication Sector)

- A country might have its own regulatory body that controls RF spectrum use within its borders, but RF signals can be more far-reaching than that.
  - For example, one purpose for shortwave radio stations is to broadcast from one country around the earth to reach other countries.
  - In a similar manner, one radio manufacturer might sell its equipment internationally, where a transmitter or receiver might be used in any global location.
- To provide a hierarchy to manage the RF spectrum globally, the United Nations set up the ITU-R. The ITU-R maintains spectrum and frequency assignments in three distinct regions:
  - Region 1: Europe, Africa, and Northern Asia.
  - Region 2: North and South America.
  - Region 3: Southern Asia and Australasia.

Cont.

- Most bands in the RF spectrum are tightly regulated, requiring you to apply for a license from a regulatory body before using a specific frequency.
- In contrast, the ITU-R allocated the following two frequency ranges specifically for industrial, scientific, and medical (ISM) applications. Although there are other ISM bands, too, there are mainly two that apply to wireless LANs:
  - 2.400 to 2.500 GHz.
  - 5.725 to 5.825 GHz.
- The purposes for these bands are broad and access is open to anyone who wants to use them(Free). In other words, the ISM bands are unlicensed and no registration or approval is needed to transmit on one of the frequencies.

Cont.

- Usually, unlicensed transmitters must stay within an approved frequency range and transmit within an approved maximum power level. Several national regulatory agencies are discussed in the following sections.

FCC (Federal Communications Commission)

- In the United States, the FCC regulates RF frequencies, channels, and transmission power. Some other countries choose to follow the FCC rules, too.
- In addition to the 2.4 – 2.5 GHz ISM band allocated by the ITU-R, the FCC has allocated the Unlicensed National Information Infrastructure (U-NII) frequency space in the 5-GHz band for wireless LAN use. U-NII is actually four separate sub-bands, as follows:
  - U-NII-1 (Band 1): 5.15 to 5.25 GHz.
  - U-NII-2 (Band 2): 5.25 to 5.35 GHz.
  - U-NII-2 Extended (Band 3): 5.47 to 5.725 GHz.
  - U-NII-3 (Band 4): 5.725 to 5.825 GHz (also allocated as ISM).

Cont.

- Transmitters in the 5-GHz bands must follow the FCC limits listed in Table 2-2.

Table 2-2 FCC Requirements in the 5-GHz U-NII Bands

Band	Allowed Use	Transmitter Max	EIRP Max
U-NII-1	Indoor only	17 dBm (50 mW)	23 dBm
U-NII-2	Indoor or outdoor	24 dBm (250 mW)	30 dBm
U-NII-2 Extended	Indoor or outdoor	24 dBm (250 mW)	30 dBm
U-NII-3	Indoor or outdoor	30 dBm (1 W)	36 dBm

ETSI (European Telecommunication Standards Institute)

- In Europe and several other countries, the ETSI regulates radio transmitter use. Like the FCC, the ETSI allows wireless LANs to be used in the 2.4-GHz ISM and most of the same 5-GHz U-NII bands; however, the U-NII-3 band is a licensed band and cannot be used.
- Table 2-3 lists the transmitter requirements for each of the bands.

Table 2-3 ETSI Requirements in the 2.4- and 5-GHz Bands

Band	Allowed Use	EIRP Max
2.4 GHz ISM	Indoor or outdoor	20 dBm
U-NII-1	Indoor only	23 dBm
U-NII-2	Indoor only	23 dBm
U-NII-2 Extended	Indoor or outdoor	30 dBm
U-NII-3	Licensed	N/A

Other Regulatory Bodies

- A country might have its own or it can adhere to all or parts of the regulations of a larger, more established regulatory body. Countries that use a common set of RF regulations are known as a regulatory domain.
- For example, a Cisco wireless device that is compatible with the American regulatory domain can also be used in Canada, many Latin and South American countries, and in the Philippines.
- Cisco manufactures wireless devices for use in at least 13 different regulatory domains. The basic wireless LAN operation is identical in all domains, but the frequency ranges, channels, and maximum transmit powers can differ.

IEEE Standards Body

- The IEEE Computer Society develops and maintains standards on a variety of topics related to computing, including Ethernet and wireless LANs.
- The IEEE 802 standards all deal with local-area networks and metropolitan-area networks (LANs and MANs, respectively).
- The standards mainly deal with the physical and data link layers of the OSI model, and with transporting variable-size data packets across a network media.
- As you explore the portion of the 802 standards that are dedicated to wireless LANs, you will find that they focus on accessing the shared RF media (physical layer or Layer 1) and on sending and receiving data frames (data link layer or Layer 2).

IEEE Working Groups

- To develop networking standards, the IEEE is organized into working groups, which have an open membership.
  - Notice that the eleventh working group, 802.11, is responsible for the wireless LAN standards.
  - As amendments are introduced, their names become 802.11a, 802.11b, 802.11c, and so on.

Table 2-4 Example IEEE 802 Working Groups

Name	Description
802.1	Network bridging (includes Spanning Tree Protocol)
802.2	Link-layer control
802.3	Ethernet
802.4	Token Bus
802.5	Token Ring MAC layer
...	
802.11	Wireless LANs
...	
802.15	Wireless PANs (personal-area networks such as Bluetooth, ZigBee, and so on)

Power Consumption

- While the definition of IoT device is very broad, there is a clear delineation between powered nodes and battery-powered nodes.
- Battery-powered nodes bring much more flexibility to IoT devices.
- 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). And (RPL) routing protocol for low power and lossy networks.

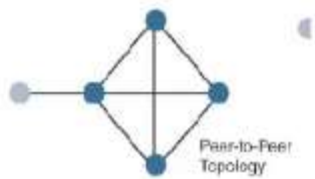
Topology

- 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 (Bluetooth networks)
- Star topologies utilize a single central base station or controller to allow communications with endpoints.

Star Topology

Topology

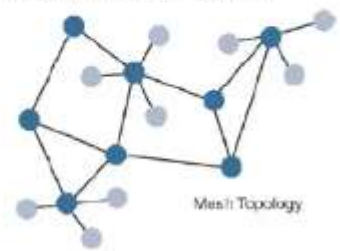
- ✓For medium-range technologies, a star, peer-to-peer, or mesh topology is common.
- Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other
- Obviously, peer-to-peer topologies rely on multiple fullfunction devices.
- Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.



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 to 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
- 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

mesh topology requires a properly optimized implementation for battery-powered nodes. Battery-powered nodes are often placed in a "sleep mode" to preserve battery life when not transmitting.



Constrained Devices

- 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. Therefore, some classes of IoT nodes do not implement an IP stack

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

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

A low-power wide-area network or low-power wide-area network or low-power network is a type of wireless telecommunication wide area network designed to allow long-range communications at a low bit rate among things

Constrained-Node Networks

- While several of the IoT access technologies, such as Wi-Fi , are applicable to laptops, smart phones, and some IoT devices, some IoT access technologies are more suited to specifically connect constrained nodes.
- 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
- Lossy networks indicates that network performance may suffer from interference and variability due to harsh radio environments

Constrained-Node Networks

- 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: a data rate: the rate at which bits are transmitted. In some LANs (eg Wi-Fi) the data rate can vary with time. Throughput refers to the overall effective transmission rate, taking into account things like transmission overhead, protocol inefficiencies and perhaps even competing traffic.
- The data rates available from IoT access technologies range from 100 bps to tens of megabits per second.

Constrained-Node Networks

- Latency and Determinism: is the amount of time it takes a packet of data to leave your computer and receive a response back from the end point.
- latency may range from a few milliseconds to seconds, and applications and protocol stacks must cope with these wide ranging values. Note: packet loss and retransmissions due to interference, collisions, and noise are normal behavior in LLN.

- Overhead and Payload

IOT ACCESS TECHNOLOGIES

- Each IoT access technology must address:

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

✓Physical layer: The wired or wireless methods and relevant frequencies

✓MAC layer: Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control

✓Topology: The topologies supported by the technology

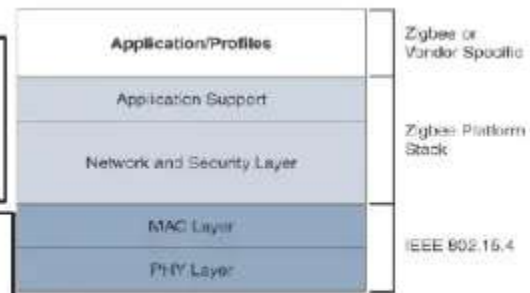
✓Security: Security aspects of the technology

ZigBee (IEEE 802.15)

- ZigBee aimed for smart objects and sensors that have low bandwidth and low power needs.
- The main areas where ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy.
- ZigBee-based devices can handle various functions, from measuring temperature and humidity to tracking assets

The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications

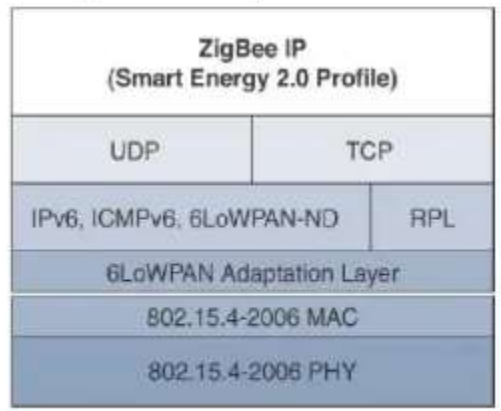
for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.



ZigBee IP

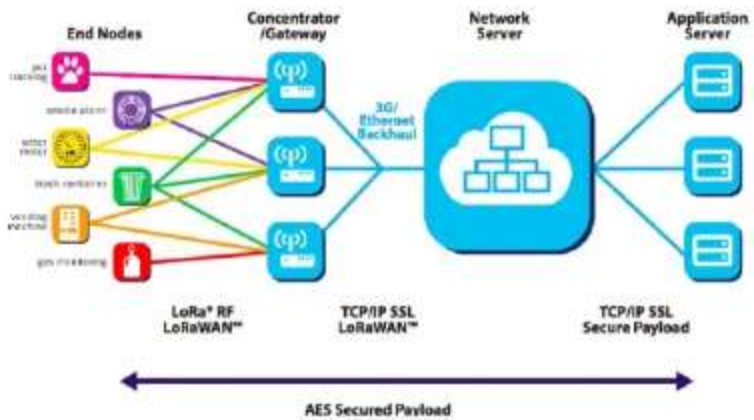
- ZigBee IP was created to embrace the open standards coming from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL. They provide for low-bandwidth, low-power, and cost-effective communications when onnecting smart objects.

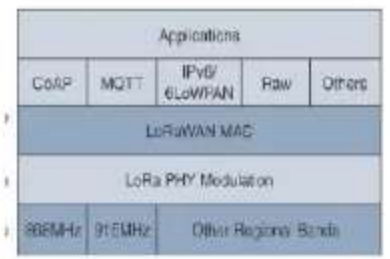
Unlike traditional ZigBee, ZigBee IP supports 6LoWPAN as an adaptation layer, The 6LoWPAN mesh addressing header is not required as ZigBee IP utilizes the mesh-over or route-over method for forwarding packets. ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes.



LoRa

- LoRa is a long-range wireless communication protocol that chieves its extremely long range connectivity, possible 100km.
- LoRa enables long-range transmissions (more than 10 km in rural areas) with low power consumption.
- A low-power wide-area network (LPWAN) is a type of wireless telecommunication wide area network designed to allow long range communications at a low bit rate among things (connected objects).
- LoRA, LoRaWAN operates on open licensed-free spectrum





LoRa

- ✓Communication between the sensor nodes and the base stations goes over the wireless channel utilizing the LoRa physical layer, whilst the connection between the gateways and the central server are handled over a backbone IP-based network.
- The PHY and MAC layers allow LoRaWAN to cover longer distances with a data rate that can change depending on various factors
- End Nodes transmit directly to all gateways within range, using LoRa.
- ✓Gateways relay messages between end-devices and a central network server using IP.

LoRa

- End Nodes
  The End Nodes are LoRa embedded sensors. The nodes typically have,
  - ✓Sensors (used to detect the changing parameter eg. temperature, humidity, accelerometer, gps),
  - ✓LoRa transponder to transmit signals over LoRa patented radio transmission method, and optionally a micro-controller (with on board Memory).
- Gateways
  The LoRa sensors transmit data to the LoRa gateways. The LoRa gateways connect to the internet via the standard IP protocol and transmit the data received from the LoRa embedded sensors to the Internet i.e. a network, server or cloud.

LoRa

- The network servers connect to the gateways and data packets, and then routes it to the relevant application.
- Application Servers
  The Application can typically be built over IoT platforms like AWS IoT using Lambda, DynamoDb or S3 services
- LoRaWAN applications: Smart cities operators, broadcasters, and mobile and non-mobile services providers