Chapter 2: IoT Technologies

2.1 Introduction

There are two choices to connect IoT devices to the Internet: wired and wireless. The decision on which of these connectivity schemes must be selected depends mostly on the IoT application. One may think that wired networks are faster and more secure than wireless networks. Even though this might be true, the recent advancements in wireless technology and the newer wireless standards have reduced the speed and security gap between wired and wireless networks substantially. In general, there are IoT applications that prefer to use wireless connectivity schemes and there are other ones that wired solutions would be a better choice for them. There might be applications that can use both wired and wireless solutions, while there are some applications that only one of these solutions works for them. In this chapter and the next chapter, we will discuss both wired and wireless standards and solutions that are used for providing connectivity for IoT applications.

2.2 Wired IoT

Wired connections are reliable, secure and can support high data rate. Therefore, this type of connection can be considered as a suitable IoT connectivity scheme for stationary IoT devices that are close to each other. Higher cost of cable implementation, lack of support for mobility and scalability are the main reasons that make them less attractive for all IoT applications. The main wired technologies for connecting devices are Ethernet and Power Line Communication (PLC). We will discuss briefly about these two technologies in this section.

2.2.1 Ethernet

Ethernet is the most commonly used Local Area Network (LAN) technology which provides a wired connectivity scheme to connect many IoT devices together using an Ethernet switch. Connecting the Ethernet switch to an Internet Protocol (IP) router can give IP connectivity to all those IoT devices. Ethernet can provide IoT connectivity for stationary or fixed IoT devices. It is clear that the IoT devices need to be connected to an Ethernet switch using cables. The Ethernet technology requires that the distance between the devices and the switch be small in range of tens of meters. Therefore, due to the limitations required by Ethernet standard as well as the cost of cabling, the IoT devices that use Ethernet as IoT connectivity should be located very close to each other. In applications where the IoT devices are not mobile and their locations are close to each other, Ethernet can provide a networking solution with low latency and very fast data rate.

Ethernet was developed as a 10 Mbps network in 1980s and advanced to fast Ethernet (100 Mbps), gigabit Ethernet (1 Gbps), 10 Gbps, 40 Gbps, 100 Gbps, and above 100Gbps. The market drivers for higher speed Ethernet are the data centers or Internet media providers as well as video service providers. These types of high speed Ethernet technologies are also used by the Internet Service Providers (ISP) and enterprise LANs. Terabit Ethernet (TbE) is an Ethernet with speeds above 100 Gbps. IEEE P802.3bs Task Force has approved 200 Gbps and 400Gbps Ethernet standards and several networking manufacturers are offering devices operating in 200 Gbps and 400 Gbps. The road map for higher speed Ethernet expects speeds of 800 Gbps and 1.6 Tbps to become IEEE standards after 2020. The very high speed Ethernet is not a requirement for most IoT applications. On the contrary, many IoT devices produce small amount data. The data rate of the slowest Ethernet technology often is more than enough for those IoT applications. Even in the smart factories and industrial applications with high data rate requirements, the data rate of newer Ethernet standards would not be needed.

Traditional Ethernet does not support any quality of service and it supports only best-effort service. This reduces the complexity of the network and enables simple protocol operations which consequently brings down the cost of Ethernet interfaces. Regardless of the huge success of Ethernet during past decades, the lack of support for devices with different QoS requirements has become a major drawback for the use of this technology in some IoT applications. Ethernet was not originally designed to meet the requirements needed for guaranteed and real-time communication. For example, many automation applications has made modifications to the Ethernet which resulted in creation of several bus systems to handle time critical traffic more efficiently. Examples of these systems are Fieldbus (IEEE 1394), Ethernet for Controlled Automation Technology (EtherCAT), and Process Field Network (ProFiNet). There also exist many industrial Ethernet protocols that have been created by different manufactures and industry alliances. Note that some compatibility issues may arise due to the fact that most of the industrial Ethernet networks are not based on standards.

In a smart factory, data needs to be collected and analyzed in a timely manner and the real-time connectivity and availability is crucial in operation and processing. Unfortunately, traditional Ethernet does not support time synchronization using global timing information in its network elements. Traditional Ethernet also lacks a network management scheme for bandwidth reservation or policy enforcement schemes to ensure a guaranteed QoS level for its connected devices.

For this purpose and due to existence of traditional Ethernet shortcomings, IEEE 802.1 TSN Task Group has defined a set of Ethernet sub-standards called Time-Sensitive Networking (TSN) or Ethernet TSN. TSN extends Ethernet standards to create a convergence between time critical data and less time critical data. The most important parameter for time critical data is availability. Ethernet TSN defines the physical layer (Layer 1) and data link layer (Layer 2) based on Open Systems Interconnection (OSI) model. It should also be noted that the Internet Engineering Task Force (IETF) has formed the DETerministic NETwork (DETNET) working group which works on the network layer (Layer 3) and higher layer techniques for adaption to the new requirements.

A TSN flow is identified by a traffic class which is characterized according to the QoS properties such as latency, jitter and bandwidth. A TSN packet contains a Virtual Local Area Network (VLAN) tag based on 802.1Q standard and a Priority Code Point (PCP). The value of PCP and VLAN tag are application oriented. Using these values, different traffic with different requirements can be differentiated. Industrial automation applications sometimes need low latency and jitter requirements in range of micro seconds and high bandwidth requirements in gigabit range, while power grid applications may need less bandwidth and can tolerate higher latency measures.

TSN guarantees the latency for real time critical data. Both time sensitive and non-time sensitive data traffic can coexist in the network using the same infrastructure. In other words, we can have several devices connected to a TSN switch with time sensitive data, while exist other devices that generate non-critical data. To be able to provide a sense of time to the network, it is essential that all network equipment such as switches and terminals on the network are time synchronized and have the same understanding of time. To be able to guarantee the timely delivery of packets, traffic scheduling is also needed besides time synchronization. All devices connected to a TSN Ethernet switch are time synchronized and know the network scheduling information as regards to packets forwarded to them by the TSN switches. Each switch in the network has several queues and performs packet forwarding based on the schedule that can calculate, predict and ensure the timely delivery of the packets.

Ethernet TSN defines a concept called Preemption which reduces the transmission latency for high priority frames. It allows high priority packets to interrupt low priority ones in transmission, which minimizes the latency of high priority traffic. This feature is especially effective on lower-speed networks such as standard Ethernet or fast Ethernet carrying large Ethernet packets. Since Ethernet uses a variable length packet forwarding scheme, a large size low-priority packet might be delayed by higher-priority traffic in the network. In a high traffic situation, this large size low-priority packet might even be dropped. Preemption fragments the large packets into smaller pieces which get reassembled in the next TSN switch in order to maximize the bandwidth utilization. This allows for small pieces of large low-priority packets to go through the network any chance that they get.

2.2.2 Power Line Communications (PLC)

With the advancement in digital signal processors which enable the use of sophisticated modulation techniques, it is completely possible for the IoT devices to utilize power line for data transmission. This opens up opportunities for the use of PLC technology as a wired medium for networking applications which minimizes the cost to deploy infrastructure for wired connectivity. PLC can be categorized into narrow band and broadband technologies.

Narrow band PLC operates at frequencies between 3 KHz and 500 kHz and can be used for data rates of up to hundreds of kbps, and has a range of up to several kilometers. There are some Narrow-Band PLC (NB-PLC) technologies capable of communicating through transformers which can provide longer distances without the need for repeaters. It is clear that the cost of PLC deployment is substantially increased as the number of repeaters increases.

Broadband PLC works at higher frequencies of 1.8 MHz to 250 MHz, and can be used for data rates up to several hundreds of Mbps over shorter distances. In general, lower frequencies can pass through the transformers more effectively than the higher frequencies. Therefore, the broadband PLC provides shorter distances.

The most important narrow band PLC technologies are listed in Table 2.1. Most standards have been developed in order to bring reliability and interoperability to provide connectivity for applications such as home networking or smart grid. As it is seen in Table 2.1, various technologies including Orthogonal Frequency Division Multiplexing (OFDM), Binary Phase Shift Keying (BPSK), and Frequency Shift Keying (FSK) have been used in PLC standards. The narrow band PLC can be further categorized into those that make use of technologies such as OFDM and those that use simpler ones such as BPSK and FSK. OFDM is computationally more expensive, but offers higher data rates as

Table 2.1: The most common narrow band PLC standards

Standard	Freq. band (KHz)	Technology	Data rate
G3-PLC	35.9-90.6	OFDM	5-45 kbps
PRIME	42-89	OFDM	21-130 kbps
IEEE P1901.2	9-500	OFDM	Up to 500 kbps
ITU-T G.hnem	3-500	OFDM	Up to 1 Mbps
EIA 709.1.2	86-131	BPSK	3.6-5.4 kbps
KNX	125-140	FSK	1.2 kbps
IEC61334	20-100	FSK	2.4 kbps

The frequency bands allocated to narrow band PLC technologies as well as the standardization bodies are different in different parts of the world. European Committee for Electro-technical Standardization (CENELEC), Association of Radio Industries & Businesses (ARIB), Electric Power Research Institute (ERRI) and Federal Communications Commission (FCC) are the most important standardization bodies in the world. Figure 2.1 shows the frequency bands used in different parts of the world for narrow band PLC technologies.

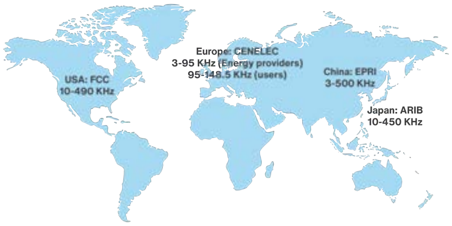

Figure 2.1: Frequency bands used in different part of the world for narrow band PLC technologies

One of the most important advantages of PLC over wireless is related to its performance in metropolitan areas and dense urban regions where attenuation of wireless signals are high. In these areas, high-rise apartment buildings are common and the electricity meters are often located in the basements of the tall buildings. One of the applications for smart city use case is related to smart metering which enables the smart meter to transmit energy consumption data from a residential unit to the utility in real time. The IoT connectivity for smart meters in urban areas where wireless coverage might be poor can be provided by narrow band PLC.

One of the fundamental differences between narrow band and broadband PLC is the carrier frequencies they use and their bandwidth. Narrow band PLC typically uses carrier frequencies lower than 500 kHz in which due to the high noise floor, the available bandwidth is reduced. Broadband PLC uses carrier frequencies between 2 and 30 MHz where the noise is less which results in a much higher Signal-to-Noise Ratio (SNR). Examples of broadband PLC include HomePlug 1.0, HomePlug AV, and HomePlug Green PHY. HomePlug Powerline Alliance was formed by several companies in 2000 to create a standard that the existing electrical wiring inside houses can use as a medium in such a way that the connected devices to electrical power can communicate with each other and the Internet. Examples of these connected devices would be smart meters, home appliances and plug-in electric vehicles. HomePlug 1.0 specification was published in 2001 which supports 14 Mbps data rate. In 2005, HomePlug AV specification was published. This technology increased the peak data rates from 14 to 200 Mbps. HomePlug Green PHY specification and HomePlug AV2 specifications are subsets of HomePlug AV and were introduced in late 2011 and early 2012, respectively. HomePlug Green supports a peak rate of 10 Mbps and is specifically designed to use up to 75% less energy than HomePlug AV. HomePlug AV2 supports the data rates above 1 Gbps.

2.3 Wireless IoT Technologies

A wireless network can have many advantages as compared to the wired networks. The main advantage is that the nodes of this network can be mobile. Wireless technology is the only option for mobile IoT devices. Expandability is another advantage offered by wireless technology. The wireless networks can be easily expanded, while additional wiring is usually needed for expanding the wired networks. Wireless technology is usually more cost effective, due to the ease of installation as compared to wired solutions. In this section, we will discuss some of the existing wireless short-range technologies that empowered the IoT technology with the appropriate connectivity.

2.3.1 Short-range technologies

In this sub-section, we will discuss three most important short-range wireless technologies used in IoT applications. This includes Bluetooth Low Energy (BLE), Zigbee and WiFi.

2.3.1.1 BLE

BLE is the power-optimized alternative to the legacy Bluetooth technology. It is developed by the Bluetooth Special Interest Group (SIG) and introduced its version 4.0 specifications in 2010. BLE is suited for applications that are battery operated and need to consume as less power as possible. This enables BLE to be used in IoT applications that have the same requirements in terms of power consumption.

To provide short-range connectivity to an IoT gateway using BLE technology, each IoT device as well as the IoT gateway need to have a BLE module. Depending on the requirements imposed by a specific application, the BLE module can be programmed in three different modes of operation. These three different operation modes are advertising, scanning, and initiating modes which are used in discovery process to find the existing BLE devices in the network. The BLE device that sends advertising messages to discover its surrounding nodes is called an advertiser. An advertiser as its names suggests, sends advertising messages. By the same token, a BLE module in the initiating mode is called initiator and a BLE module in the scanning mode is called an initiator. The scanner and initiator have almost the same functionalities. The difference between a scanner and an initiator is that a scanner only discovers the advertiser without requesting any further communication, while an initiator can also request a connection with the advertiser after receiving an advertising message. The scanner wakes up periodically to discover other BLE modules in range and listens to the advertising messages.

After receiving an advertising message by a scanner or initiator, they can initiate a connection. Connections enable a reliable communication for data transmission. More details about BLE advertising and connection mode can be found in Appendix A.

Bluetooth 4 introduced BLE in 2010 as part of its specifications and was an important step to improve the performance of classic Bluetooth toward a technology for IoT applications. Bluetooth 5 specifications which were released in 2016, introduced new features such as improved frequency hopping scheme, additional physical layer transmission methods, advertising extension modes, periodic advertisement, and increased transmit power. The new features of Bluetooth 5, not only increased the range or data rate, but also increased its performance in both advertising and data transfer modes. More details about Bluetooth 5 can be found in Appendix B.

2.3.1.2 Zigbee

Zigbee is defined and developed by Zigbee Alliance and is based on the IEEE 802.15.4 standard. It operates in 2.4 GHz ISM band globally, 915 MHz in Americas, and 868 MHz in Europe. Zigbee uses mesh topology and can achieve a maximum data rate of 250 kbps in 2.4 GHz band. As a short-range wireless technology, it can provide ranges up to 100 meters depending on the transmit power level and indoor conditions. Zigbee has a large addressing space and can support a maximum of 64K IoT devices. Also, larger networks can be supported by linking multiple Zigbee networks. For applications such as smart meters that are usually installed in locations with poor radio quality, linking multiple networks can provide scalability. In addition, it can increase the reliability as backup routes also can be established and used in case of failure. Smart home and smart building use cases with applications tailored to lighting, home automation and security have widely used Zigbee as their IoT connectivity solution. Even though, Zigbee modules do not exist in most of the existing smartphones, tablets, or computers, Zigbee is used as the only technology in home products such as Samsung Smart Things, and Philips Hue. Street lighting is an excellent example that can be controlled using Zigbee mesh topology, since it is capable of providing functionalities such as remote management for a large network of devices.

Self forming and self healing are two important features of Zigbee technology. Self forming means that the Zigbee network can configure itself automatically. Self healing means that it can reconfigure itself dynamically in situations that Zigbee nodes become faulty, removed or disabled. Interoperability is one of the important features of Zigbee modules. Interoperability is important, since there might be Zigbee modules from many different manufacturers especially in home automation and industrial devices.

2.3.1.3 WiFi

In general, IoT applications have diverse requirements in terms of range, data rate, energy efficiency and the cost of devices. WiFi is a wireless technology that provides local area network connectivity and is well suited to support IoT applications that require high data rate and a reasonably low latency. Due to the existence of in-building WiFi connectivity, it becomes a good choice for some IoT applications.

Table 2.2: Names of existing WiFi standards

Standard	Meaning	Year
802.11	Standard WiFi	1997
802.11 b		1999
802.11 a		1999
802.11 g	WiFi 3	2003
802.11 n	WiFi 4	2009
802.11 ac	WiFi 5	2014
802.11 ad	Milimeter wave	2010
802.11 ah	WiFi Halow	2017
802.11 ax	WiFi 6	2019

802.11b used the same 2.4 GHz frequency band with a bandwidth of 83 MHz and supported a maximum data rate of 11 Mbps and had a range up to 150 feet. This technology used spread spectrum technology and became very popular due to its cost. Almost at the same time, 802.11a standard introduced a WiFi technology that operated in 5 GHz frequency band, and used OFDM technology for its operation. Due to utilizing larger bandwidth (300 MHz), use of OFDM technology and higher frequency band which is less prone to noise, 802.11a could support maximum data rate of 54 Mbps. 802.11a did not become very popular mainly because its cost was higher than 802.11b.

802.11g used both capabilities of 802.11a and 802.11b. It supports data rates of up to 54 Mbps similar to 802.11a. It also uses the 2.4 GHz frequency for greater range and it is backward compatible with 802.11b. Therefore, 802.11g access points can work with 802.11b wireless network interface cards. 802.11g became a standard in 2003 and is also referred to as WiFi 3.

802.11n operated in both the 2.4 GHz and 5 GHz bands. It supported a maximum data rate of 600 Mbps. The main reasons for its better performance was the use of modified OFDM, an enhancement in Layer 2 design, utilizing higher channel bandwidth, and support of up to four spatial streams Multiple Input Multiple Output (MIMO) for spatial multiplexing. MIMO allows multiple transmitters or receivers to operate simultaneously at one or both ends of the link and provides a substantial increase in data rate. In 2018, WiFi Alliance decided to use a better naming system for WiFi standards and called 802.11n as WiFi-4.

802.11 ac, also called WiFi 5, was a huge step in WiFi evolution. It supported maximum data rate of above Gigabits per second. The technology operated exclusively in the 5 GHz frequency band, supported up to eight spatial streams, utilized higher bandwidth of up to 160 MHz, and took advantage of denser modulation technique. 802.11ac uses 256 Quadrature Amplitude Modulation (QAM) up from 64QAM used in 802.11n.

802.11 ad (WiGig) operates on 60 GHz band (millimeter waves). The spectrum for this technology is different in different parts of the world. In North America, 802.11 ad uses 57-64 GHz. WiGig is a very high data rate and low distance technology. 60 GHz was not a license exempt band, but it became license exempt band after 2013. Due to existence of a large spectrum of 7 GHz, it is possible to implement simple modulation techniques to achieve very high data rates. For example, 7 Gbps can be achieved by using simple 1b/Hz modulation techniques instead of using more complex methods. Due to small wavelength (millimeter wave), many antennas can be put in a chip to make the antenna array. Due to the use of directional antenna and very short distance coverage of this technology, the technology introduces low interference and inherent security.

802.11 ax is one of the newest generation of Wi-Fi standard which is also called Wi-Fi 6. Wi-Fi 6 offers higher data rates and capacity, up to 9.6 Gbps, and operates in both 2.4 GHz and 5 GHz spectrum. There also exists Wi-Fi 6E that supports an all-new 6 GHz spectrum, which has higher throughputs and lower latency.

802.11ah (Wi-Fi HaLow) is a below one gigahertz wireless technology which operates in 900 MHz license-exempt bands. Since it uses a lower frequency band, it can offer longer range wireless connectivity and therefore can provide robust connectivity in challenging environments. It also provides lower power consumption as compared to other WiFi technologies and for this reason meets the requirements for IoT.

Chapter 2 Exercises

1. Which of the following statements is correct?
    a. Traditional Ethernet does not support QoS and only provides best-effort services.
    b. Lack of support for devices with different QoS requirements has become a major drawback to traditional Ethernet in the IoT domain.
    c. Traditional Ethernet was designed to meet the requirements needed for guaranteed and real-time communication.
    d. Both a and b.
2. Ethernet TSN defines a concept called Preemption to
    a. allow low priority packets to interrupt the transmission of high priority packets.
    b. increase the throughput of the system.
    c. reduce of transmission latency for high priority frames.
    d. All of the above.
3. Ethernet TSN
    a. guarantees the latency for real-time critical data.
    b. does not guarantees, but it does its best effort to reduce latency for real time critical data.
    c. does not guarantees, but it does its best effort to reduce latency for all types of data.
    d. guarantees the latency for non-real time critical data.
4. Terabit Ethernet (TbE) is an Ethernet standard which
    a. is widely used for IoT applications in smart factory.
    b. is not a requirement for most IoT applications.
    c. is usually used for Internet service providers' (ISP) core routing.
    d. Both b and c
5. Narrowband PLC operates at frequencies between
    a. 3 KHz and 500 kHz and can be used for data rates of up to 100s of kbps.
    b. 3 KHz and 500 kHz and can be used for data rates of up to 100s of Mbps.
    c. 8 MHz to 250 MHz and can be used for data rates of up to 100s of kbps.
    d. 8 MHz to 250 MHz and can be used for data rates of up to 100s of Mbps.
6. To connect smart meters to the Internet
    a. Narrow band PLC is always a better IoT connectivity scheme as compared to wireless schemes.
    b. Broadband PLC is always a better IoT connectivity scheme as compared to wireless schemes.
    c. Narrow band PLC is a better IoT connectivity scheme as compared to wireless schemes in metropolitan areas and dense urban regions.
    d. Any wireless option can provide better IoT connectivity as compared to PLC , since PLC has a low performance.
7. An IoT device using BLE connectivity method wants to connect to an IoT gateway which has the central BLE module. For this purpose, the IoT device sends the advertising message to the central BLE which resides on the gateway. Which device initiates the connection?
    a. The BLE on the IoT device.
    b. The BLE on the IoT gateway.
    c. Either of them can initiate a connection.
    d. It depends on the one that has been configured to send the Connect Request packet.
8. An IoT device using BLE connectivity method is connected to an IoT gateway which has the central BLE. The connection time is set to 7.5 ms. What is the value of interval parameter in the Connect Request packet? (Hint: the readers need to study Appendix A to answer this question)
    a. 5