IoT Use Cases and Technologies

IoT Use Cases and Technologies

F. JOHN DIAN AND REZA VAHIDNIA

BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY
VANCOUVER, CANADA

Sample APA-style citation:

This textbook can be referenced. In APA citation style, it would appear as follows:

Dian, F. J. & Vahidnia, R. (2020). *IoT Use Cases and Technologies*. British Columbia Institute of Technology. https://pressbooks.bccampus.ca/iotbook/

Ebook ISBN: 978-1-990132-01-8
Print ISBN: 978-1-990132-00-1

Publisher: BCIT
Publication date: December 1, 2020

The authors and publisher of this book have used their best efforts in preparing this book. These efforts include the development, and research of the theories, technologies and standards. The authors and publisher make no warranty of any kind, expressed or limited, with regards to the documentation contained in this book.

This book was produced with Pressbooks (https://pressbooks.com) and rendered with Prince.

Dedicated to my beloved

Sheila and Daniel

F. John Dian

Contents

About the Authors

F. John Dian is a faculty at the Department of Electrical and Computer Engineering at British Columbia Institute of Technology (BCIT) in Vancouver, Canada. He received his Ph.D. degree from Concordia University, Montreal, Canada in Electrical and Computer Engineering in 2004. Dr. Dian has more than 20 years of experience in design and implementation of telecommunication circuits and system. Dr. Dian holds a certificate in business analytics from Harvard University, USA and co-chairs the center of excellence for analytics at BCIT. He has been recognized with several excellence in teaching and research awards. Dr. Dian is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and an active member of Association of Engineers and Geoscientists of British Columbia (APEGBC).

Reza Vahidnia is a faculty at the Department of Electrical and Computer Engineering at British Columbia Institute of Technology (BCIT) in Vancouver, Canada. . He received his Ph.D. degree from Ontario Tech University, Oshawa, Canada in Electrical and Computer Engineering in 2014. He has served as a senior IoT analyst at Rogers Communications Inc., and an IoT project manager at TELUS where he worked on several smart city and IoT initiatives. Dr. Vahidnia is a professional engineer (P.Eng) and an active member of the Association of Engineers and Geoscientists of British Columbia (APEGBC).

Preface

The phrase “Internet of Things” (IoT) alludes to the billions of physical devices connected to the Internet in order to exchange raw data and analyze the information. By collecting data from these devices and analyzing them, IoT makes the devices smarter, and the processes more efficient. IoT can bring endless opportunities to every aspect of our lives. For example, in a city environment, insights gained from that collected data can be used to manage resources and services more efficiently, leading to creating the concept of smart city. The city is smart, if it is connected. In a connected city, the traffic and transportation systems are managed more efficiently, the quality of urban services are improved, the performance of processes are enhanced, the consumption of resources are optimized, and the cost of services are reduced.

IoT is in early stages of its life. However, it is growing in a fast pace. As more and more IoT devices are deployed, we witness that every aspect of our lives is changed by the IoT.

This book sets out to introduce the IoT use cases and technologies. To demonstrate the effect of IoT and its potential to change our world, several practical examples are discussed. The book also discusses the existing wired and wireless communication technologies that have enabled IoT.

This book is organized in three chapters. The outline of this book is as follows: Chapter 1 introduces the fundamental concepts of IoT technology and explains IoT verticals, use cases and applications. Practical scenarios are discussed to demonstrate different applications of IoT in a variety of industries. Chapter 2 explains about wired IoT technologies as well as short range wireless communication technologies that have paved the way for IoT to be used for different applications in a variety of uses cases. Chapter 3 focuses on low power wide area technologies that provide long range connectivity for those applications where small amounts of data are transmitted often infrequently.

At the end of each chapter, there are several multiple choice and review questions which provide the readers with a better understanding of the topics that have been discussed in that chapter. The solution to those questions can be found at the end of the book.

Chapter 1: IoT Use Cases

1.1 Introduction

The Internet of Things (IoT) enables the power of the Internet and analytics to be given to the real world of physical objects. In IoT world, a physical object needs to be connected to the Internet using a connectivity method to send its data in order to be processed in real time or offline. This data could be used to control the object itself or control the other objects in a smarter manner. Therefore, we can look at the IoT as a network of connected objects which are able to exchange data and information via the Internet. Years ago, the idea of establishing a network of massive physical objects seemed impossible or at least impractical. The fact that a physical object needs to have a processor and a means to connect to other physical objects would impose challenges that made the widespread use of IoT impractical.

There is a broad range of physical objects that fall under that umbrella of connected Things. A Thing can be as simple as a temperature sensor that gathers the temperature data to monitor the temperature inside a building. An appliance can be considered as a Thing in which it can exchange data through the Internet with other objects that assist the appliance to manage its energy consumption more effectively, improve its performance, or increase safety of its operation.

Since the Things are connected to the Internet, they can send their data to a data center or cloud for processing. For most applications, the duration of sending data from the physical object to a remote data center, or even the round-trip time for transmitting the data to the cloud, processing and analyzing the data, and sending information back to the object is not too large to cause any problem. In situations that the delay is too large, edge-computing can be used. In edge computing, an edge device within relatively close distance to the physical objects can process the data, and send the information to the physical objects to reduce the delay. An edge device can also aggregate the data before sending it for further processing or storage.

Coca-Cola vending machine at Carnegie Mellon University might be considered as the first device that brought to light the concept of a network with smart devices. This vending machine could report its inventory remotely in 1982 before the era of modern Internet. Therefore, we may not name it as Internet of Things, but certainly was a network of things. A toaster that could be turned on and off remotely over the Internet was introduced in 1990 and can be considered as one of the first IoT devices. But, the term "Internet of Things" was coined by Kevin Ashton, to promote Radio Frequency Identification (RFID) technology in 1999. He used this term as a buzz word to get the attention of the management to RFID technology. The IoT concept did not gain much of popularity until 2010. Gartner added the name IoT on its "hype-cycle for emerging technologies" in 2011. Nowadays, IoT technology has made itself well established across many industries such as healthcare, energy and industrial automation. The use cases of IoT are increasing at a very fast pace. The number of IoT devices deployed is expected to grow exponentially, and we can expect increasing amount of data exchange through the Internet by the physical objects.

IoT is going to change every aspect of our life. The IoT chip designers and manufacturers are investing heavily in IoT technology. The number of IoT chip manufactures and IoT modules have been increased substantially during past years. The number of production of IoT modules are also increasing rapidly. These IoT modules, nowadays are part of different devices used by a variety of industries. The list of the industries that are using IoT is growing rapidly as well. Transportation, energy, smart cities, retail, agriculture, and healthcare are some examples of industries that utilize IoT technology.

IoT is changing telecommunication industry which provides connectivity for IoT. Telecommunication companies and service providers are trying to accommodate with the requirements needed by IoT. Due to its unique characteristics, IoT brings many changes to service providers. However, this is not new for telecommunication companies. Many years ago, telecommunication companies provided only voice services to their costumers. The need for data services introduced a substantial change in structure of these companies where they were able to successfully accommodate the new requirements and manage the needed modifications to their network. IoT has its own characteristics that are unique and somehow different than voice and data services already provided by service providers to people. The IoT devices usually need higher uplink bandwidth as compared to downlink, while humans generate more downlink traffic. The traffic generated by an IoT device can be significantly lower or higher as compared to the traffic generated by a person. For example, a metering device might need to transmit only several bytes per day, while an industrial machine installed in a smart factory might need to transmit several kilobytes of data per second. In most applications, the IoT device sends its data through the day periodically, while the people generate more traffic during the day as compared to the night time. Also, in some IoT applications, the IoT device sends its data after an event is detected, while the traffic generated by humans is not usually event based.

Since the huge amount of data produced by a staggering number of IoT devices needs to be stored, processed, and analyzed, IoT will continue to make new opportunities for cloud providers, application designers, data analyzers, and system integrators as more and more organizations realize the true power of IoT.

IoT can be categorized into three different clusters of verticals, use cases and applications, in which each vertical has several use cases and each use case can have several applications. IoT vertical indicates the use of IoT in a specific industry segment. An IoT vertical has unique regulatory bodies, supports specific standards, policies, procedures and protocols. Each vertical can be further divided into use cases. A use case usually is served by the same platform and they usually need similar methodology for processing, storing, and analyzing the data. For example, in the transportation vertical, there may be use cases related to autonomous vehicles. Each use case may include several applications. Applications often use similar solutions and software programs. Sometimes the IoT vertical is divided into sub verticals to make a four layer categorization. Unfortunately, the above mentioned taxonomy is not used in practice and there is no common agreement on IoT categorization. For example, you may find manufacturing as an IoT vertical in some documents, while it has been considered as a use case under industrial vertical in other places. The need for categorization comes from the fact that two similar applications, belonging to different use cases or even different verticals might be quite different due to their requirements in terms of regulatory bodies, standards, policies, protocols, platforms, processing and etc.

1.2 IoT connectivity

IoT can be implemented using many IoT connectivity schemes that connect an IoT device to the other devices through the Internet. In general, the Internet connection can be either wired, or wireless. Wired and wireless communications have their own advantages and disadvantages and should be chosen depending on the application. Understanding the benefits and drawbacks of wired and wireless connectivity schemes enables us to make an informed decision regarding IoT implementing solution. There are many factors that affect this selection. Example of these factors are the number of IoT nodes in the network, the location of nodes, the maximum range of the network, the required bandwidth or data rate, the maximum power consumption allowed, and the security requirements.

Wired connections are reliable, fast and very secure. They are more reliable than wireless connections since they are less prone to packet loss as a result of path loss or interferences from other electronic devices. However, they suffer from higher cost of implementation, and lack of support for mobility. Scalability is also another problem with wired networks. The wired IoT network is only practical if IoT devices not only are close to each other to reduce the cabling cost, but also at least one of them is located close enough to a wired Internet access point. For many IoT applications, wired connectivity is not very practical and wireless IoT implementations are the common solutions.

Short-range wireless technologies such Bluetooth, Zigbee or even WiFi are enablers of IoT. These technologies use the Industrial, Science, and Medicine (ISM) spectrum which make them very attractive. To connect the IoT devices to the Internet using these technologies, there is a need for an IoT gateway which on one hand is connected to the IoT physical device using short-range technologies and on the other hand is connected to the Internet. The IoT gateway is located at the edge of the local network, and sometimes has enough processing power to perform some computing at the edge. Figure 1.1 shows a situation that many IoT devices are connected to an IoT gateway to send their data to the Internet.

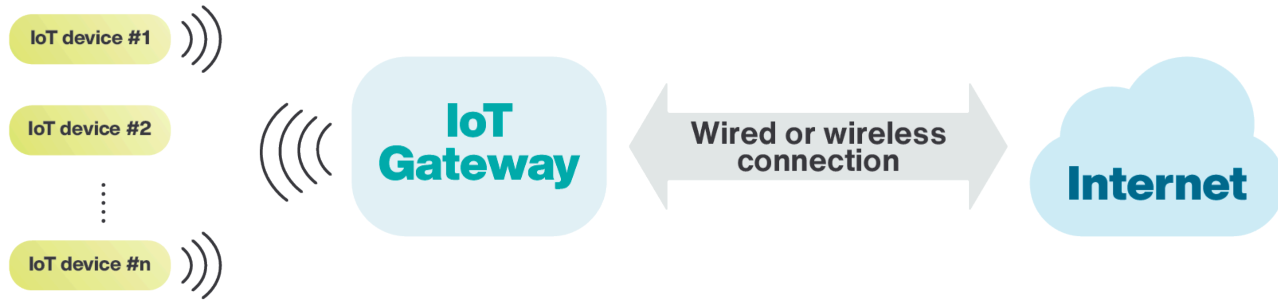


Figure 1.1: IoT gateway for the Internet connection

Wireless IoT is becoming a mature technology, expanding rapidly into more and more industries, and is creating a domain of devices that in many situations are battery operated. In many applications, it would be extremely challenging to replace these batteries. For this reason, low power consumption is one of the requirement of wireless IoT technology. Another reason for designing IoT devices with low power consumption comes from the fact that there will be a massive number of IoT devices in the future. If we can reduce the power consumption of each device, we consequently need less energy to be produced to power up these devices. While there are different sources of energy such as wind, and solar that are renewable and some what are clean, most of the energy generated today comes from burning fuel. To reduce the power consumption of the IoT devices, the device needs to go to sleep if it does not have anything to perform. The longer the device sleeps, the lower amount of energy is consumed which increases the life time of the battery. Since low power consumption is one of the most important characteristics of wireless IoT, technologies such as Bluetooth Low Energy (BLE) or Zigbee are often used in IoT applications. WiFi might be used in IoT applications that require higher bandwidth and the ones that power consumption is not a concern.

Besides short-range technologies that connect the IoT device to the Internet through gateway, there is another option that is particularly designed for providing long-range connectivity. A Low-Power Wide-Area Network (LPWAN) is a cellular network that provides long-range connectivity for devices that require low power consumption. The Cellular IoT (CIOT) networks have high reliability as well as availability and provide a good coverage. The CIoT technology can be divided into licenced and un-licenced technologies. The licenced-band IoT technology has superior performance in terms of expandability, interoperability, security, coverage, and Quality of Service (QoS). The most important unlicensed cellular technologies are Sigfox and Long Range Radio (LoRa).

The Third Generation Partnership Project (3GPP) is the global technical body which develops technical specifications for mobile communication systems. The 3GPP cellular IoT technologies belong to the category of LPWAN systems. The licenced-band CIoT has been implemented using different generations of cellular network. Many IoT applications can be implemented using existing second (2G), third (3G), and fourth (4G) generations of cellular technologies. Fourth generation of cellular network has made it possible to achieve larger bandwidth, lower latency and greater density. Cellular IoT can be enhanced substantially in terms of capacity, coverage, density per cell, latency, and power consumption by using fifth generation of cellular networks (5G). 3GPP has developed technical specifications in its Release 13, 14 and 15 for IoT applications using 2G, 3G, and 4G cellular technologies. 5G cellular network has been designed for three different types of applications. The first one is mobile broadband (cellphones). The second one is massive machine type communications (MTC). This category is designed specifically for IoT applications. The last one is ultra reliable and low latency communications which is made and tailored especially to be suitable for real time and safety applications. Therefore, 5G cellular network addresses the needs and requirements of IoT applications as part of its design.

1.3 Examples of IoT use cases and applications

IoT provides precise insights to many applications in different sectors of a variety of industries and businesses. It brings efficiency, safety and can revolutionize the way many businesses and industries operate. For instance, energy companies in the field of oil and gas have their operations spread across many remote locations. IoT technology can provide these companies with continuous monitoring of their remote sites. Manufacturing relies heavily on complex machineries to manufacture products. Therefore, manufacturers have an interest in improving the performance of these machines. Connecting the machines to the Internet can improve precision, increase safety and bring efficiency to the operation of these machines. In this section, we will discuss some use cases of IoT to give the readers some understanding of how IoT brings changes to various industries.

1.3.1 IoT for Research

Scientists, researchers, and conservationists study the behavior of animals and try to understand the factors that are important to their survival. The natural habitat of many animals is under threat due to factors such as climate change, or disruption in food chain. The population of many species are shrinking, and many are becoming extinct. To save these species, there is a need to find out everything about their behavior and living. Understanding the animals' travel habits and trajectories, or the locations that they search for food, are examples of important information that can help the scientists to save these endangered animals.

The data related to animal behavior can be obtained using IoT technology and through tagging the animals with sensors. A wearable IoT can be attached to the animal's body to sense parameters such as location, temperature, and type of activities. The collected data can be stored in a database and used by the scientists to identify the important factors that can address the animal's behavior. Scientists can use the data to design scientific models that can be used to protect endangered or threatened species. There are thousands of animals that are listed as endangered. Using the collected data, the scientists can better understand why the population is in decline and what solid actions need to be taken to help them survive. Figure 1.2 shows examples of using IoT to establish connected habitats for understanding the animals' behavior by tracking their location, monitoring their heath signals, or generating event-based images or establishing connected habitats.

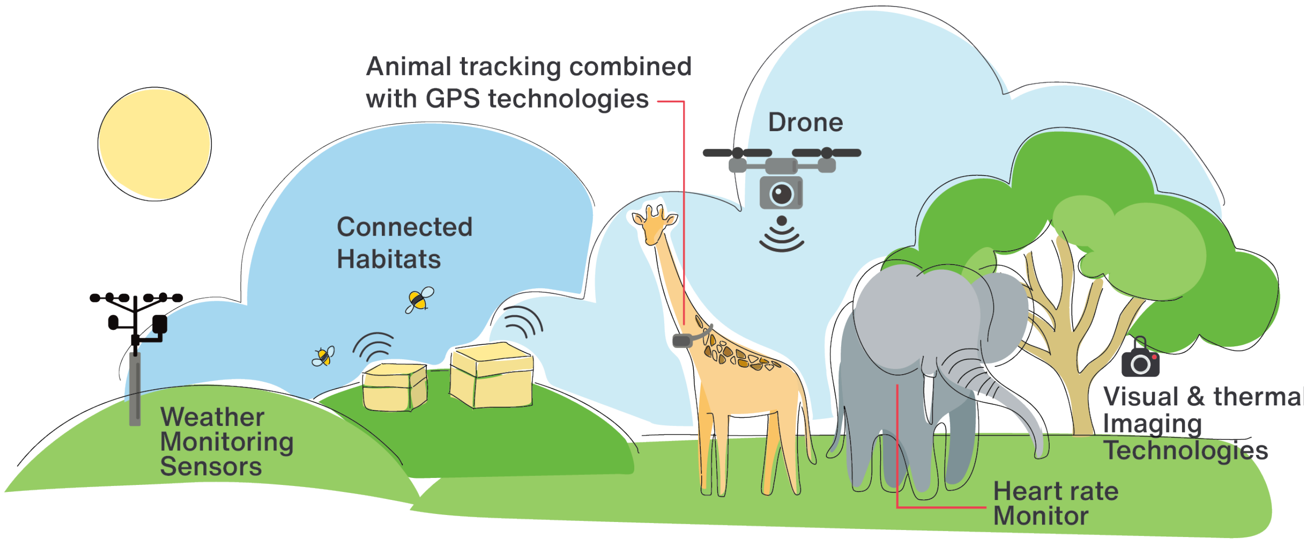


Figure 1.2: Use of IoT technology for research purposes on animal behavior

Cellular IoT technologies are designed to connect massive number of devices that can be spread over large geographical areas together. These technologies also try to be low in power consumption in such a way that battery operated devices can work for a long time before there is a need for battery replacement. Hence, wearable IoT devices can be used to monitor animals' life and behavior over a long period of time and in large geographical areas. Considering around 50 bytes of data in both uplink and downlink direction every two hours, a typical CIoT device equipped with a Lithium coin cell battery (with 660 mWh capacity) can work for up to 2 years without using any harvesting technique to charge the battery. Obviously, if the rate of data transmission is lower, the battery can last longer. For example, by sending 50 bytes of data every day, the battery can last for more than 30 years.

1.3.2 Connected Street Lighting poles

In the past, the main reason for street lighting poles in urban areas was to provide visibility or safety. However, connecting these infrastructures to the Internet can provide a wide range of applications and opportunities and can be considered as a foundation for a smart city. Once the lighting systems and light poles are connected to the Internet, they can be used as the infrastructure for many smart city initiatives. For example, imaging sensors such as video surveillance cameras can be installed on the lighting poles for public safety purposes. Installing environmental monitoring sensors that can detect the air quality, or noise level can also be another example of sensors to change these infrastructures as environmental monitoring stations. Connected lighting poles can also be used as Wi-Fi access points which can consequently provide Internet access for some close by systems such as parking meters or pay stations. Connected light poles can be suitable locations to install street name signage or display systems to provide real-time information such as traffic to drivers, cyclists, pedestrians and residents.

Street lighting systems can be used to share real-time data regarding traffic and road conditions among cars and other road users such as pedestrians, or cyclists. By analyzing traffic data collected from the street lighting infrastructure and the vehicles on the road, these structures are able to alarm drivers about dangerous road conditions, traffic jams, and impending safety issues ahead.

In the past, connectivity was provided to street lighting system using gateways. These gateway systems usually get connected to small parts of street lights using technologies such as Power Line Communication (PLC). The deployment of CIoT, eliminates the need for proprietary gateways. Each light pole can directly communicate with a central management platform. Easy installation is an essential need for this application, due to the existence of many street light poles in the city. CIoT provides easy installation and eliminates the need of connection to a gateway which consequently reduces the cabling and installation costs. Due to its great coverage within cities and its high reliability, CIoT can provide connectivity for applications that require low data rate connectivity such as simple light dimming as well as the ones that require high data rate such as video surveillance.

Figure 1.3 shows the connected street lighting poles as a foundation for smart city. The street poles can signal the drivers of the pedestrian jaywalking, accident that has happened further down the road, or the existence of a pothole on the road.

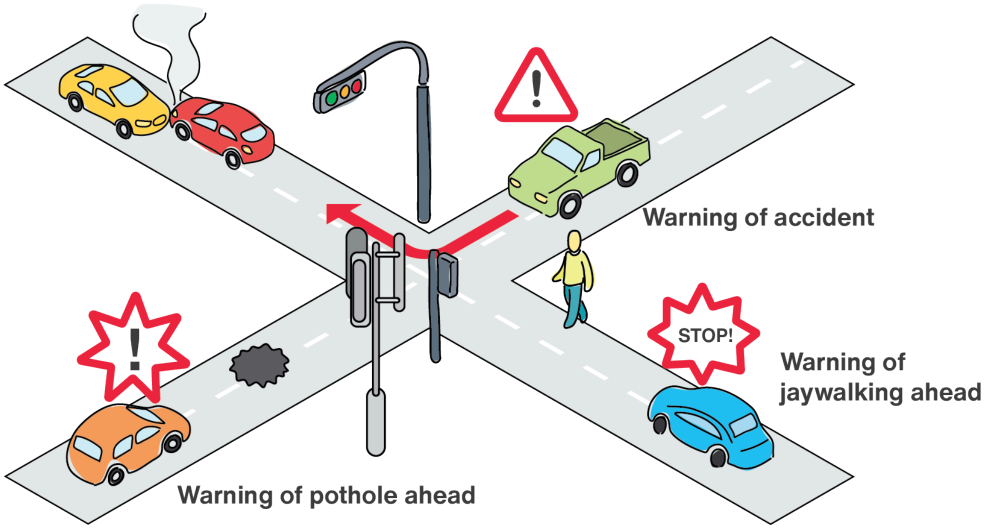


Figure 1.3: Connected street lighting pole as an IoT gateway to help drivers

In the near future, cars can communicate with road infrastructure, other vehicles and even pedestrians using IoT technologies such as cellular V2X (Vehicle-to-everything). Cellular V2X can improve road safety by generating warnings for potential hazards to the autonomous cars or smart car drivers. These warnings are delivered over the IoT network. Due to time-critical nature of these warnings, low-latency is an important factor in determining a suitable connectivity scheme. IoT with a cloud platform linking vehicles to road managed systems, bypasses the need for extensive fixed infrastructure. The handling of an entire ecosystem of interconnected vehicles and their connectivity with the road network is an important potential that can be provided by IoT technologies.

1.3.3 Industrial Use Cases

The use of IoT technologies in manufacturing is also called the Industrial Internet of Things (IIoT). Let us consider the use of IoT technology in a smart factory scenario as shown in Figure 1.4. An industrial company manufactures large machinery equipment in several different factories around the world. In each factory, 200 machinery equipment is built every day. This industrial company uses welding machine in its operation to build these equipment. Let's assume that 500 spots need to be welded to build any of these equipment. The company collects several different information for each welding spot that can produce 15 KB of data per second. The welding process for each spot takes 10 seconds. Example of data collected from each welding spot might be the time-based voltages, currents, and temperatures of the welding machines. The data is sent to the cloud and is stored in a database. This data can be used to track possible issues in any machinery equipment.

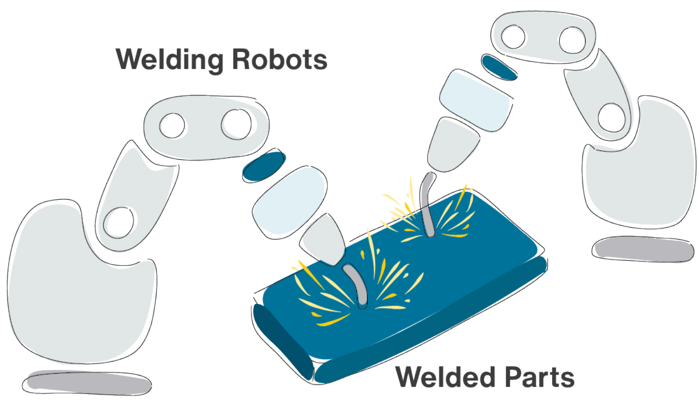


Figure 1.4: Welding robots in a smart factory generate huge amount of data

In this scenario, the company generates 15 GB of data per day from its welding machines in each factory. The welding data is not the only data that will be generated in a smart factory. The data from other operations also need to be collected. Integration and analyzing all information can be used to perform predictive maintenance, analyze the factory utilization in addition to track issues in a specific machinery equipment. A smart factory with many branches around the world can collect huge amount of data. Table 1.1 shows the symbols and units representing the size of data.

Huge amounts of data can be stored in data lakes. A data lake is a centralized storage that can store both the structured and unstructured data at any scale.

Structured data uses defined data types in such a way that they are searchable and usually are stored in relational databases; while unstructured data is not as easily searchable. Unstructured data has internal structure but is not structured using defined data types or schema. Audio, and video are examples of unstructured data. The manufacturer can run different types of analytics to create insight and make better decisions. There are many use cases for data lakes in manufacturing operations management.

Table 1.1: Symbols and units representing size of data

Size	Symbol	Meaning	Power
Kilo Bytes	K	1024 Bytes	10^3
Mega Bytes	M	1024 Kilo Bytes	10^6
Giga Bytes	G	1024 Mega Bytes	10^9
Tera Bytes	T	1024 Giga Bytes	10^{12}
Peta Bytes	P	1024 Tera Bytes	10^{15}
Exa Bytes	E	1024 Peta Bytes	10^{18}
Zetta Bytes	Z	1024 Exa Bytes	10^{21}
Yotta Bytes	Y	1024 Zetta Bytes	10^{24}
Ronna Bytes	T	1024 Yotta Bytes	10^{27}
Quecca Bytes	Q	1024 Ronna Bytes	10^{30}

1.3.4 IoT-based Attraction Centers

IoT can bring endless opportunities to attraction centers. People visiting an attraction center can be provided with wearable wristbands to access all amenities in the center, reserve rides or buy food. These wristbands are equipped with sensors that use short-range technologies such as RFID to connect people to a network of IoT gateways connected to the Internet. Using IoT technology, the attraction center can track the actions of visitors who have worn these wearable devices and optimize their services according to the visitors' demands. As it is shown in Figure 1.5, visitors can unlock doors and enter to different locations in the attraction center with valid admission, use fast track services to avoid the queues, and pay for the services. The wearable device acts as keys, credit cards, tickets, passes and more. The collected data is used to help the attraction center to anticipate the location, behavior, and interests of the visitors. One of the biggest challenges of any attraction center is to minimize the wait times for different attractions within the center. As each person swipes their IoT based wearable wristband at an attraction, vital information is transmitted real-time to the cloud or a private management platform through IoT gateways. This allows decisions to be made about adding staff or giving some incentives to visitors to go to another attraction in order to reduce the wait time.

Figure 1.5: Wearable wristband enables visitors to enter an attraction center.

1.3.5 Smart Grid Automation

IoT technology can help in the management and automation of the smart power grid as shown in Figure 1.6. The operations and maintenance of smart grid systems need to be optimized to meet the increasingly challenging requirements of their grid caused by factors such as the integration of renewables into the power grid, and tighter regulations. Power grid also needs to detect and respond to faults along the grid rapidly. Due to large variation in energy production of renewable energy and the challenging issues of integrating the renewable power to the micro grid, a reliable smart grid network requires real-time control and management of generated energy into the grid to avoid overload. Therefore, there is an extensive signaling between all micro-grid nodes. The signaling system needs to be fast and reliable.

Wired IoT systems, and wired optical systems are mostly in use today in smart grid systems. Cellular IoT can also be used for this application. Actually, CIOT is a better choice as compared to wired alternatives due to its lower cost and higher deployment flexibility. However, the wireless technology needs to provide a similar level of performance in terms of latency, data rate, and security.

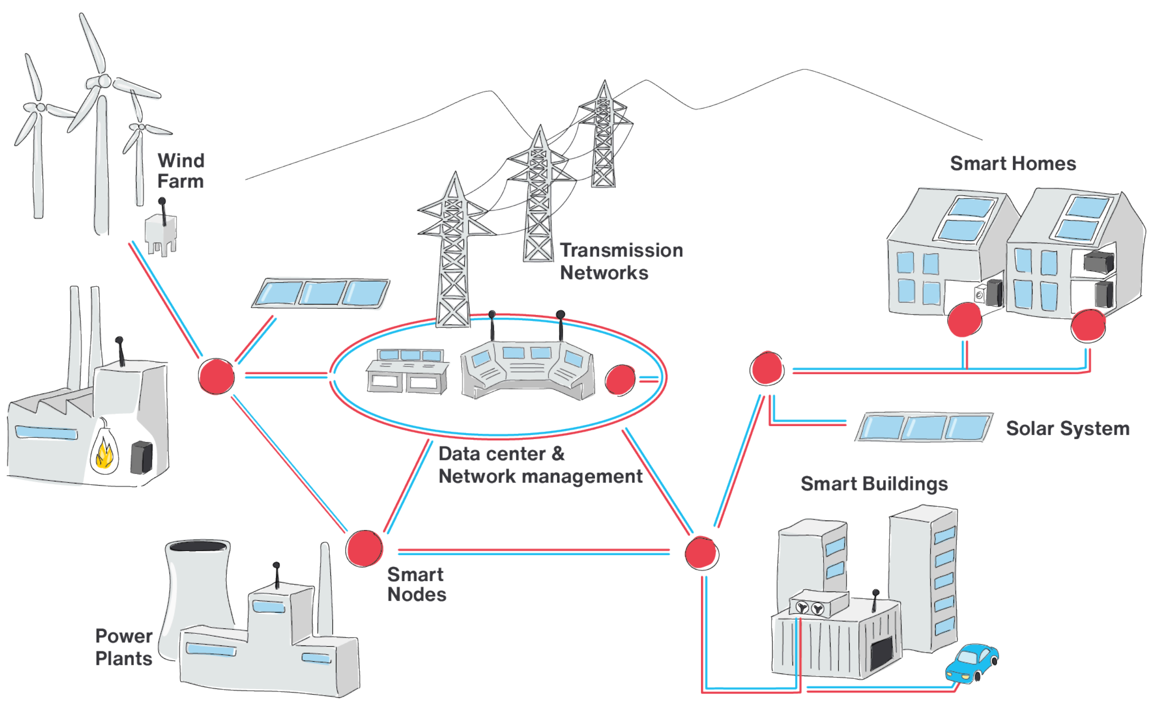


Figure 1.6: IoT technology helps in the management and automation of the smart power grid

1.3.6 Collaborative Robots

IoT technology can be used in orchestrating the operation of arm and mobile robots as shown in Figure 1.7. To be able to autonomously perform various tasks, each of these robots need to have many sensors as well as powerful processors to operate individually. There is a need for a centralized management system and more processing power to enable several robots to complete a complex task. It should be noted that providing enough processing power into these robots can be very costly, in particular for smaller robots. Providing connectivity using wired IoT might be challenging in situations where the robot is mobile such as Automated Guided Vehicles (AGV). Wireless IoT technology can be a better choice, but it should be able to provide the low latency requirement needed for this application. Using IoT technology, the robotic system can then offload part or all of this processing to the edge or cloud. Cloud computing of the data collected from each robot can be used to orchestrate the operations of each robot in a collaborative robots scenario.

Figure 1.7: IoT technology used in orchestrating the operation of mobile robots

1.3.7 Video Surveillance

To provide public safety in airports, transportation stations, or public events such as concerts, festivals, and election rallies, IoT-based public surveillance and security systems can be used. In general, IoT-based surveillance systems connect one or several cameras to the Internet directly or through IoT-gateways. Beside static installations, the surveillance system might be mobile. This includes cameras installed on vehicles such as police cars, buses and trains used in public transportation, wearable cameras worn by law enforcement officers, or even surveillance drones. Figure 1.8 shows an IoT-based surveillance system for a train station.

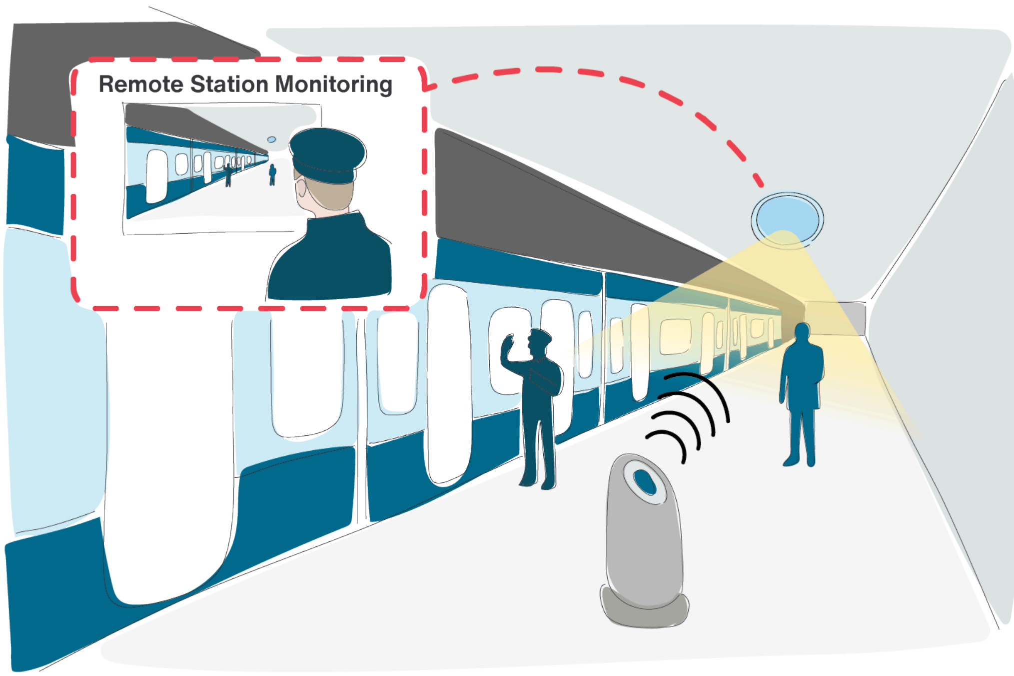


Figure 1.8: IoT-based metro station showing several cameras as part of its surveillance system. A fixed camera installed on the celling, and a mobile cart carrying a camera. The station is monitored remotely.

1.3.8 IoT-based Hand Sanitizing Station

The patients in hospitals and clinics may carry and spread different types of germs, bacteria and infectious diseases. This problem does not only belong to medical facilities. In any organization, people use their hands to open doors, shake hands with other people which expose their hands to germs and bacteria. Since a single doorknob could be touched by many people, it can cause spreading the disease in a workplace. Meeting rooms are often packed with employees, as well as clients who exchange handshakes, thus swapping germs. Installing hand sanitizer stations in an organization and encouraging regular use of these stations can lead to having a healthier work environment. In case of an epidemic or pandemic, installing hand sanitizer stations would be very effective. IoT-based hand sanitizing stations are sensor-activated and provide staff in an organization with sanitation reminders. These hand sanitizing stations are all connected directly to the Internet or via an IoT gateway. The sensors can identify each employee and record hand hygiene events. The system records when an employee enters or exits a room, and gives the employee specific amount of time to use any of the sanitizing stations in the area.

1.3.9 Railway Switch Monitoring System

Switches are one of the most important parts of a railway network. An unfortunate issue can arise when a mechanical part of a switch wears out, or fails to operate. These issues do not usually reveal themselves by regular inspections. An IoT-based switch monitoring system can collect several data from the switch such as the timing of switch operations, motor voltage and currents, and vibrations. Vibrations can be measured when the train passes, and with big data analytics, trends can be analyzed. Evaluation of this data will show deterioration of the switch mechanisms as well as the dynamic behavior of the switch under different weather conditions. Real-time warnings can be issued to the operation center when measurements indicate imminent failure.

1.3.10 Elevators at Railway Stations

The availability of elevators in the public transportation stations is important especially for the disabled or elderly customers and those with child carriages. IoT technology can help increase the availability as well as improved accessibility and safety for commuters. Integration of elevators from multiple manufacturers into one integrated monitoring platform, visibility into the real-time elevators status for passengers and commuters, predictive maintenance and improvement of elevators reliability and safety based on failure data, are examples of benefits that an IoT system can provide for this application. An IoT device installed in an elevator can monitor the changes in operating data. Examples of collected data are temperature, friction, tilt, or noise. Based on the real time data and analytics, it is possible to predict when the elevator needs maintenance. Not having insight on the elevator's conditions could result in equipment failure, and in turn causes disruptions. IoT devices can be used to keep track of wear and tear and use the information to predict the time that the maintenance will become necessary. The door open-close cycles, the amount of time it takes for the door to be closed, the amount of current it draws to open or close the door, the number of times the elevator's door has been opened from the last service can be examples of data used for predictive maintenance.

1.3.11 Smart Parking

Smart parking systems can detect the number of available parking spots as well as the locations of the cars parked in the parking lot. Smart parking system can also inform or guide the customers to vacant parking spots. In a busy parking lot, people may spend a lot of time trying to find a vacant parking location while they might none be available. IoT technology can provide the customers of a smart parking with real-time information in regards to the locations of available parking spaces.

In-ground or surface-mounted smart parking sensors that communicate with an IoT gateway can provide real-time parking data over the Internet. Figure 1.9.a shows an example of in-ground or surface-mounted smart parking sensor. Figure 1.9.b shows an application of smart parking using these sensors. The sensor provides an accurate vehicle detection in parking spaces using an IoT connectivity method. The collected information from the sensors can be saved on a local server or on the cloud. This information can be utilized by other applications and third parties such as parking management systems, parking enforcement, and mobile payment system that can utilize that data to provide further services to their customers.

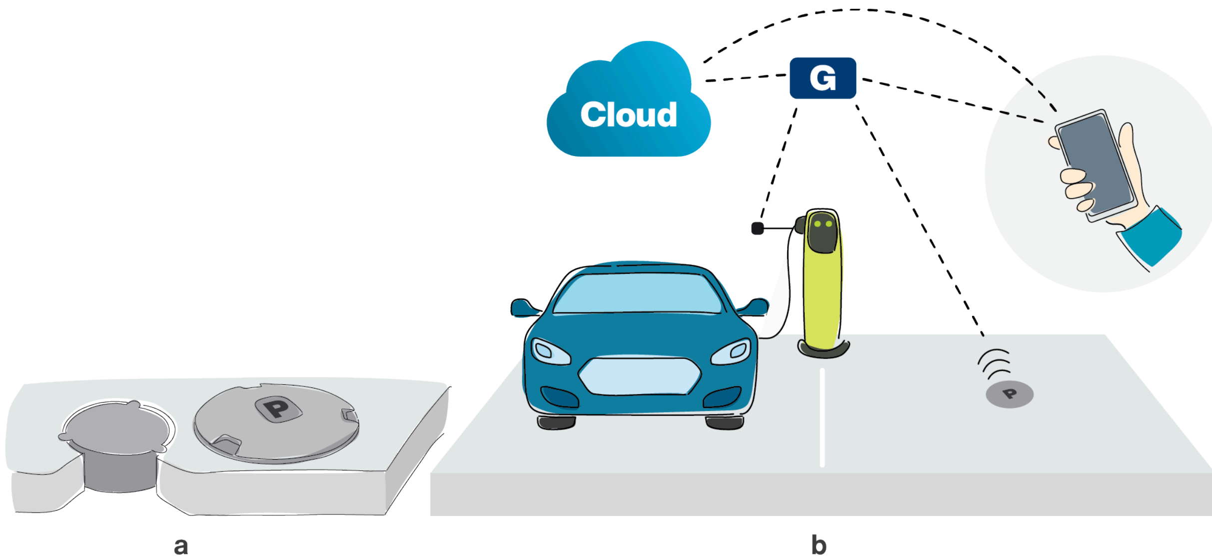


Figure 1.9: a) In-ground and surface-mounted smart parking sensors b) Smart parking system

1.3.12 IoT for Worker Safety

Construction industry suffers from high worker fatalities at construction and work sites every year caused by issues such as falls, electrocutions, risks associated with interacting with dangerous machinery, or being caught in or between objects. Despite advances in science and technology, works in challenging work environments will continue to exist. We can see similar problems in many other industries such as oil and gas, and mining where workers are remote and work in hazardous environments that present many challenges in regards to safety. For example, it is extremely challenging to extend oversight when workers are around heavy equipment, on a remote off-shore drilling rig, working on an underground location, performing inspection on telecommunication cell towers, or working in chemical processing plants.

Wearable IoT can provide worker safety, and reduce or eliminate many risks by collecting and analyzing real-time safety data to identify and prevent hazardous conditions before they happen. For example, for the operators of dangerous machinery equipment, a fatigue detection wearable IoT device can increase the safety of the workers on a construction site. A wearable device can also detect hazardous conditions in advance or collect the air quality data and alert the workers on the site. In the above mentioned scenarios, wearable IoT can ensure the workers' health or reduce risks for workers as well as costs for the employers. In general, IoT technology is used to monitor workers, sites, and equipment by collecting and analyzing sensor data in order to change the processes, or trigger alarms that can minimize the risks and the impact of possible incidents. The result of integration of IoT technology with analytics brings visibility to the situation of workers in extremely challenging environments.

Chapter 1 Exercises

1. Two similar applications, belonging to different use cases of the same vertical
    a. might be quite different in terms of their platforms, and processing, but are similar in terms of their regulatory bodies, and standards.
    b. might be quite different in terms of their platforms, processing, regulatory bodies, and standards.
    c. might be quite different in terms of their regulatory bodies, and standards, but are similar in terms of their platforms, and processing.
    d. are most likely similar in terms of their platforms, processing, regulatory bodies, and standards.
2. In what sense the IoT traffic is not the same as the traffic generated by human?
    a. IoT traffic is mostly periodic during the day, but human traffic is not.
    b. IoT uplink traffic is usually more than downlink, while it is the other way around for human generated traffic.
    c. IoT devices can generate very small or very large amount of data, while the traffic generated by human is typically large.
    d. All of the above
3. A wireless sensor network is _____
    a. an IoT network, if the number of devices are more than a threshold
    b. an IoT network, if it is connected to the Internet
    c. an IoT network, if it consumes low energy

d. not an IoT network

4. The term “Internet of Things” was first used by

    a. Kevin Ashton, to promote Radio Frequency Identification (RFID) technology
    b. Elon Musk, to introduce connected cars
    c. Charlie Kindel to introduce Alexa Smart Home
    d. Greg Kahn, to establish Internet of Things Consortium

5. Why is there a need for IoT gateway?

    a. To enable many IoT devices with different connectivity methods or protocols to connect to the Internet via the gateway
    b. To provide security in connection to the Internet
    c. To provide computation for IoT devices
    d. To provide data storage for IoT devices

6. Can IoT devices also play the role of IoT gateway?

    a. Yes, but only one IoT device can become the IoT gateway
    b. Yes, several IoT devices in the network may play the role of the IoT gateway
    c. No, IoT devices can not become IoT gateways
    d. No, unless many IoT devices lose their connection to the Internet

7. For stationary IoT devices directly connected to the power source and not using batteries, is low power consumption still a requirement?

    a. No, low power consumption is typically a requirement for battery operated devices.
    b. No, low power consumption is typically a requirement for mobile IoT devices that use wireless connectivity.
    c. Yes, due to existence of massive number of IoT devices, reducing the power consumption of each device reduces the energy that is needed to be produced to power these devices.
    d. It depends on the standard and protocol used for the IoT devices.

8. What is the principal idea to reduce the power consumption of IoT devices?

    a. Reduce the transmit power level.
    b. Increase the reception sensitivity level.
    c. The IoT device needs to go to sleep if it does not have anything to perform.

d. The IoT device aggregates its traffic to be sent as a larger chunk.

9. Technologies such as WiFi, BLE or Zigbee are part of

   a. Licenced LPWAN
   b. Un-licenced LPWAN
   c. Both A and B
   d. Non of the above

10. IIOT stands for

    a. Information Internet of Things
    b. Intelligent Internet of Things
    c. Industrial Internet of Things
    d. Infrastructural Internet of Things

11. Can IoT devices be used for medical purposes to treat the patients automatically?

    a. No, IoT devices can only collect health data for monitoring purposes.
    b. No, the collected health data can be analyzed to find a good course of action for treatment but cannot treat the patients.
    c. No, by analyzing the collected data, the information for treatment can be sent to a doctor's office, but not to the IoT device.
    d. Yes, by analyzing the collected data, the information for treatment can be sent to the IoT device. The IoT device should have the equipment needed for treatment.

12. What are the sensor(s) and connectivity options that you can find on an IoT medical device for a person with no mobility issues?

    a. An IoT device can have just one sensor such as body temperature sensor. The connectivity should be wireless.
    b. An IoT device can have one or several sensors such as body temperature, pulse, blood pressure. The connectivity should be wireless due to the patient's mobility.
    c. An IoT device can have one or several sensors such as body temperature, pulse, blood pressure. The connectivity should be wired connection for security purposes.
    d. An IoT device can have just one sensor such as body temperature sensor. The connectivity should be wired connection for security purposes.

13. Assume that IoT applications have generated more than 500 zettabytes of data in 2019. If the number of generated data increases by 4 times in 2020, how much data is generated in this year?

a. 2 Exabytes
b. 2 Yottabytes
c. 2 Ronnabytes
d. 2 Queccabytes

14. Which of the following is an example for smart grid edge device that plays the role of IoT gateway in utility use cases?
    a. Smart Meter
    b. Smart Home
    c. Smart phone
    d. Smart plug

Chapter 1 Review Questions

1. To find the trajectory of a bird during a year, an IoT device is installed on the body of the bird. Explain what types of IoT connectivity schemes can be used for this application?
2. Explain how a smart helmet can provide emergency support in case of an accident. Use a smart phone as an IoT gateway for this application.
3. Describe how a smart racket can be beneficial to train the tennis players.
4. Give an example of an IoT system that provides safety for the driver of a vehicle.
5. In the scenario explained in section 1.3.3, it was written that the industrial company generates 15 GB of data per day from its welding machines in each factory. Show how this has been calculated.

Answers to Exercises and Review questions are located at the end of the book: Chapter 1 Answers

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 compared to BPSK and FSK.

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.

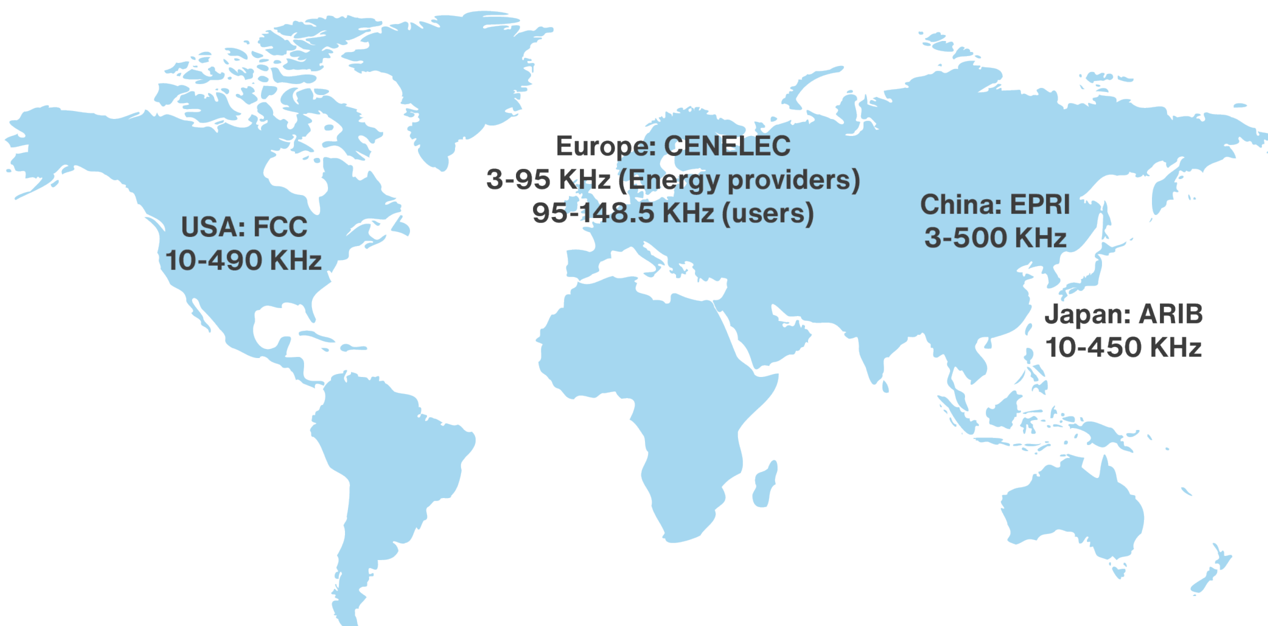


Figure 2.1: Frequency bands used in different part of the world for narrow band PLC technologies

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.

The first Wi-Fi standard was released in 1997. Since then, WiFi technology has been constantly evolving to provide faster speeds and larger coverage. The name of existing WiFi standards are listed in Table 2.2.

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

b. 6

c. 2000

d. 2200

9. An IoT device using Bluetooth 5 connectivity method is connected to an IoT gateway which has the central Bluetooth 5 module. If Bluetooth 5 is set to 1 Mbps physical layer, the IoT gateway can be put in 200 m distance. If the Bluetooth module is set to coded physical layer s=8, what is the maximum range in this case? (Hint: the readers need to study Appendix B to answer this question)

   a. 160m.

   b. 400m.

   c. 700m.

   d. 800m.

10. An IoT device using Bluetooth 5 connectivity method is connected to an IoT gateway which has the central Bluetooth 5 module. The IoT device wants to send data inside advertising packets. The size of its data is 60 bytes. Is this possible? (Hint: the readers need to study Appendix B to answer this question)

    a. Yes, Bluetooth 5 can send advertisement packets of up to 256 bytes in length. The data can be sent during advertisement and there is no need for connection. However, the possibility of collision exists.

    b. No, Bluetooth 5 can send advertisement packets of up to 31 bytes in length. The data can be sent during advertisement and there is no need for connection. However, the possibility of collision exists. But, since the size of packet is larger than 31 bytes, it is not possible.

    c. No, it is not possible to send data without establishing a connection first.

    d. No, unless the IoT gateway is allowing the data transfer during advertisement.

11. IoT devices that use Zigbee as their connectivity scheme to connect to an IoT gateway are operating in which frequency bands?

    a. 900 MHz.

    b. 4 GHz.

    c. 8 GHz.

    d. All of the above.

12. Why WiFi is an obvious choice for IoT connectivity in smart home?

a. Because in-building WiFi coverage is almost ubiquitous.
b. Because WiFi has the lowest power consumption among other short range wireless technologies in the market.
c. Because all smart home applications need very high-speed data transfer that only WiFi can provide.
d. All of the above.

Chapter 2 Review Questions

1. What are the main features of Ethernet TSN?
2. Tesla has a home charging station called Wall Connector, which has a WiFi connection.
   i. What do you think the WiFi connection is used for?
   ii. What other IoT connectivity scheme(s) you can suggest for this application?
3. An IoT device uses BLE connectivity method and it is connected to an IoT gateway. The central BLE resides inside the IoT gateway. The connection interval is set to 15 ms. The IoT device should send its information every 15 ms , but sometimes, the IoT device does not have any data to send. What should the IoT device do in this scenario?
4. Almost all smartphones have BLE module, but they do not have Zigbee. Does this limit the application of Zigbee as an IoT connectivity method?
5. Which solution (wireless or wired) is better for providing IoT connectivity in buildings with thick concrete walls?

Answers to Exercises and Review questions are located at the end of the book: Chapter 2 Answers

Chapter 3: LPWAN

3.1 Introduction

LPWAN stands for Low-Power Wide-Area Network. This technology provides low-power wide-area coverage which is a requirement for a vast majority of wireless sensor networks. It suits all IoT applications where small amounts of data are transmitted infrequently. Using LPWAN technologies, the IoT devices can also get connected to the Internet directly which eliminates the need for IoT gateways. Therefore, it is a perfect IoT connectivity solution for mobile IoT devices. LPWAN technologies can be divided into two main categories: the ones that use licensed frequency bands and the ones that operate at unlicensed frequencies. LPWAN technologies are more suitable for IoT applications that require long-range connectivity, low power consumption, and near real-time communication.

3.2 Unlicensed band LPWAN

The most important unlicensed cellular technologies are Sigfox and Long Range Radio WAN (LoRaWAN). LoRaWAN is a LPWAN protocol and system architecture developed by LoRa Alliance which provides low-power and long-range communication. LoRa Alliance is an open, non-profit association with many global members from telecommunication companies. LoRa (developed by Semtech) defines the physical layer of the system, which actually is a non-cellular modulation technology for LoRaWAN. Lora supports adaptive data rate by considering a trade off between data rate and range. It uses six spreading factors where the higher spreading factors provide longer range and lower data rate, and the lower spreading factors provide higher data rate at the expense of lower range. LoRaWAN supports both 250 kHz and 125 kHz bandwidth. Depending on the channel bandwidth and the spreading factor, the LoRa data rate varies between 300 bps and 50 kbps.

LoRaWAN defines the protocols over the LoRa physical layer. It is the network architecture which operates in a non-licensed band. The most commonly used frequency bands of LoRaWAN are 433 MHz in Asia, 868 MHz in Europe and 915 MHz in North America. The adaptive data rate provided by LoRa technology will enable optimization of power consumption for different IoT applications. LoRaWAN can provide between 2 to 5 km coverage in rural areas, and around 15 km in urban areas. The maximum data rate of around 100 kbps in both uplink and downlink directions is possible with LoRaWAN in North American deployment. The maximum data rate in Europe is usually lower than North America's.

Sigfox, the other most widely deployed LPWAN technology, was established in France in 2009 and has deployed networks in many countries since 2012. Sigfox operates in 868 MHz/902 MHz ISM frequency band, and can provide coverage of 30-50 km in rural areas, and 3-10 km in urban areas. The number of devices per access point is as high as one million devices. Due to using ultra narrow spectrum of 100 Hz, the uplink and downlink data rates are very low. The maximum data rate of Sigfox is around 100bps. Even though Sigfox provides bidirectional communication, its downlink capacity is constrained. Mobility is also a drawback for Sigfox, since mobility is difficult to be established using this technology.

3.3 Licenced band LPWAN

The 3rd Generation Partnership Project is the global technical body which develops technical specifications for mobile communication system. 3GPP was formed in 1998 with the objective to develop new technologies for the third generation of cellular networks. However, it has consequently worked on specifications for the fourth generation and fifth generation of cellular network. 3GPP represents seven regional telecommunications standard development organizations in Europe, America and Asia known as organizational or primary partners. 3GPP writes technical specifications, to be transferred into standards by the organizational partners. The 3GPP organizes its work into different segments. Each segment is represented by a Technical Specification Groups (TSG). Examples of these groups are Radio Access Networks (RAN), Services and Systems Aspects (SA), and Core Network and Terminals. RAN defines the radio communications between the mobile device and the network. SA defines the architecture and services of the network, while CT defines the core network. The project management among these groups is done by the Project Coordination Group (PCG). Each TSG is supported by several Working Groups (WGs). Organizational partners have the authority to create the TSG and PCG groups. Figure 3.1 demonstrates the 3GGP organization.

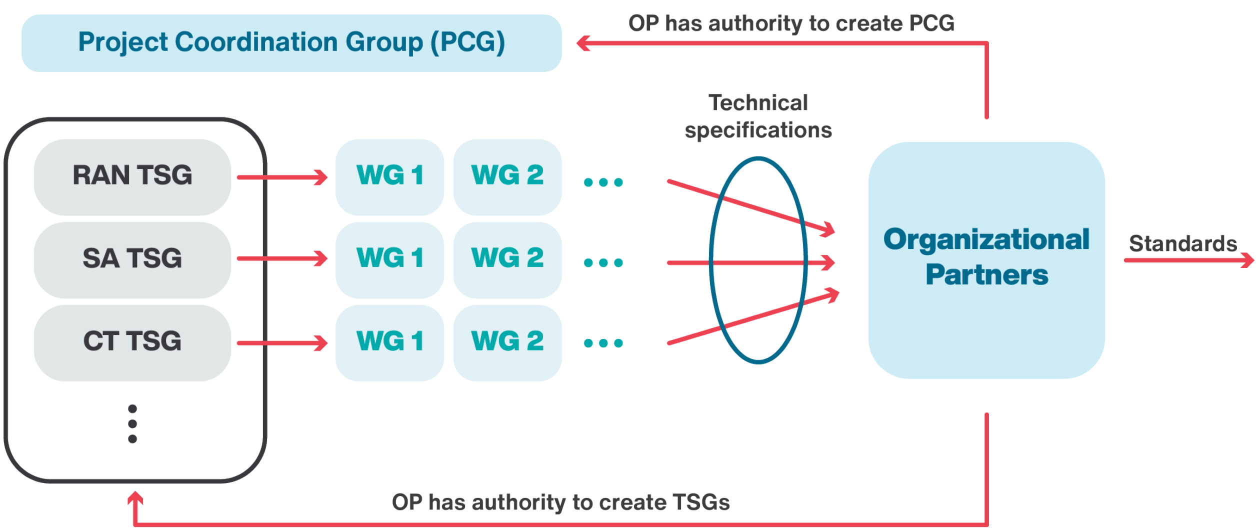


Figure 3.1: 3GPP organization

3GPP has organized its work in terms of release numbers. For example, 4G was first introduced with Release 8 and continues to evolve in higher releases. It should be noted that a specific release number does not belong to a specific generation of mobile network. For example, 3G technologies continued to evolve in Release 8+ in parallel with 4G. Similarly, 3GPP introduced 5G technologies from Release 15+, but will continue to evolve 4G in parallel. Beside broadband communication of voice and data, 3GPP considers Machine to Machine (M2M) communications. Even though M2M is discussed in earlier releases, Release 12 was the first release with considerable extension especially for managing M2M communication in high density areas with large numbers of devices. This release also introduces M2M communication with efficient transmissions of small size data and energy consumption optimization. 3GPP Release 13 introduced three categories of IoT technologies. These three categories are Extended Coverage GSM Internet of Things (EC-GSM-IoT), LTE for Machine-Type Communications (LTE-M), and Narrow band Internet of Things (NB-IoT). We will briefly explain about EC-GSM-IoT in the next section of this chapter. The rest of the chapter is dedicated to the detailed explanation about LTE-M and NB-IoT technologies. EC-GSM-IoT is backward compatible with the GSM which is one of the second generations of cellular network. LTE-M is also backward compatible solution based on LTE which is the fourth generation of cellular network. NB-IoT is based on LTE, but comes with significant modifications to legacy LTE. In 3GPP Release 14, and 15, the enhancements of both LTE-M and NB-IoT continued to provide cellular connectivity for more diverse applications.

3.3.1 EC-GSM-IoT

The Global System for Mobile Communications (GSM) is one of the second generation of cellular network developed in Europe. It was the most widely used cellular technology which still has global coverage. The first generation of cellular network was analog, while the second generation was based on digital technology. Therefore, in GSM, voice is converted to digital and a digital modulation for transmission is used. In terms of switching, GSM uses circuit switching for both voice and data transmission. There are two other cellular technologies that are based on GSM. The first one is called General Packet Radio Service (GPRS), which uses packet switching for its data transmission and still uses circuit switching for its voice transmission. The second one is Enhanced Data Rates for GSM Evolution (EDGE) which further enhances its packet switched data transmission to achieve higher data rate. Later on, with deployment of 3rd and 4th generation of cellular network, which supported much higher data rate, the GSM/EDGE network was mainly used for two purposes. One was for voice transmission and the other one was to serve as a fallback solution for data services. For this reason, GSM/EDGE continued to be an important part of cellular technology. Due to the fact that GSM has a good coverage around the world especially in Europe, Middle East and African countries, it can also be used for MTC as well as IoT. GSM usually works in 50 MHz spectrum in global 850, 900, 1800, and 1900 MHz depending on the region of deployment as shown in Table 3.1. Path loss depends on frequency and lower path loss can be achieved in lower frequencies. Global availability of GSM in lower frequency bands of either 850 or 900 MHz band has enabled GSM to provide a good coverage. Compared to more advanced generations of cellular networks, GSM uses a simpler technology. This means that the price of GSM mobile devices is considerably cheaper as compared to 3G, 4G and 5G technologies. This also makes GSM an attractive choice for IoT technology. For these reasons, 3GPP Release 13 considered EC-GSM-IoT as an IoT technology. In this book, we mainly focus on the other two 3GPP technologies introduced in Release 13, LTE-M and NB-IoT. These two technologies are further enhanced in newer releases and are the main focus of this book.

Table 3.1: GSM spectrum in different regions of the globe

GSM band	F(MHz)	Uplink	Downlink	Region
GSM-850	850	824.2 - 848.8	869.2 - 893.8	America (North, Caribbean, Latin)
E-GSM-900	900	880.0 - 915.0	925.0 - 960.0	Asia pacific, Europe, Middle East, Africa
R-GSM-900	900	876.0 - 915.0	921.0 - 960.0	Asia pacific, Europe, Middle East, Africa, Rail way system
DCS-1800	1800	1710.2 - 1784.8	1805.2 - 1879.8	Asia pacific, Europe, Middle East, Africa
PCS-1900	1900	1850.2 - 1909.8	1930.2 - 1989.8	America (North, Caribbean, Latin)

3.3.2LTE-based cellular IoT technologies

LTE-M and NB-IoT were introduced in Release 13 of LTE technology to extend LTE with features to support MTC and IoT. These technologies later got enhanced in Release 14 and 15 of LTE technology. We first explain the legacy LTE system and then discuss LTE-M and NB-IoT.

3.3.2.1 LTE

LTE physical channel bandwidth can be 1.4, 3, 5, 10, 15, and 20 MHz. Mobile Network Operators (MNOs) have the option to deploy LTE with one of these bandwidths. For example, if the MNO deploys LTE with 10 MHz physical channel bandwidth, all data and signalling physical channels must be mapped to this 10

MHz bandwidth. In terms of duplexing scheme, LTE supports both Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD) for its uplink and downlink transmissions.

We should look at the physical channel both in terms of time and frequency. From the time perspective, physical channel is divided into radio frames. Each radio frame is composed of 10 sub-frames. Each of these sub-frames consists of two time slots. Each time slot is 0.5 msec. Therefore, the duration of a radio frame is 10 msec. From the frequency perspective, the bandwidth of LTE physical channel is divided into what is called Physical Resource Blocks (PRBs). The bandwidth of each PRB is 180 KHz. Each resource block consists of 12 subcarriers. These subcarriers are separated by 15 KHz. Therefore, with transmission bandwidth of 1.4 MHz, there will be 6 PRBs, while there exist 100 PRBs with the maximum bandwidth of 20 MHz. Each radio frame contains user data, control information, and synchronization information.

To reduce the interference with neighboring bands, some part of the bandwidth is considered as guard band. The guard band occupies 10% of the bandwidth if the available channel bandwidth is 3, 5, 10, 15, or 20 MHz except for 1.4 MHz implementation where the guard band occupies 23%. For example, in 1.4 MHz bandwidth deployment, there are 6 PRBs, each occupying 180 KHz. This makes 1.08 MHz out of 1.4 MHz of the bandwidth, which is 77% of the total bandwidth. Therefore, 23% of the bandwidth is used for guard band. In case of 20 MHz bandwidth, there are 100 PRBs which occupy 18 MHz out of 20 MHz bandwidth. Therefore, 2 MHz, or 10% of the total bandwidth is allocated for the guard band.

An example of downlink radio frame structure is shown in Figure. 3.2. As you can see in this figure, each radio frame has ten sub-frames. Since each sub-frame is divided into two slots, each radio frame has 20 slots. The duration of each slot is 0.5 ms. So the duration of each sub frame is 1 ms. The duration of a radio frame is 10ms. Also, it can be seen that a PRB has 12 subcarriers of 15 KHz. Therefore, there is 72 subcarrier in the 1.4 MHz deployment scenario.

The downlink, and similarly uplink are composed of different channels. What is called a channel represents specific locations in each radio frame that carries data or specific type of control information. The information in different channels might be coded or modulated differently. For example, we will see later that a specific signaling information may exist in specific sub-frames and for this reason not all sub-frames are the same. Some channels may exist in all sub-frames, while some of them only occupy specific sub-frames or slots of a sub-frame. Hereunder, we take a look at some of these channels.

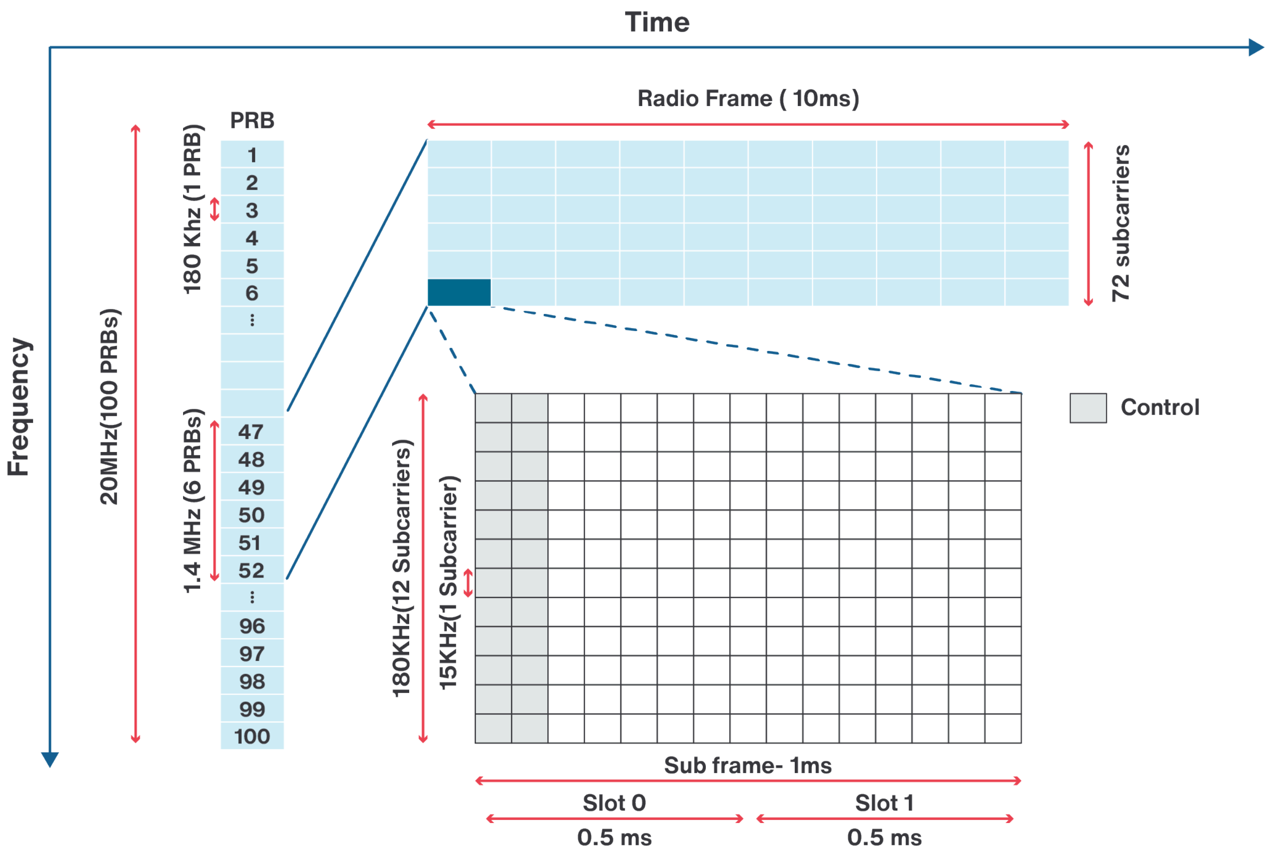


Figure 3.2: Downlink radio frame structure

The synchronization signals have their own locations within sub frames 0 and 5 of a radio frame. Downlink synchronization signals can be used for several reasons such as detecting the frame boundaries. There are two synchronization signals in the LTE. The first one is called the Primary Synchronization Signal (PSS) and the second one is called the Secondary Synchronization Signal (SSS). When an LTE phone turns on, it looks at the subcarriers of sub frame 0 and 5 to find the synchronization signals. These synchronization signals are used for frame timing acquisition and cell differentiation.

Downlink Control Information (DCI) contains the required information to control the downlink data transfer. The physical channel for carrying DCI is called Physical Downlink Control Channel (PDCCH). DCI can use different size symbols based on the parameters such as bandwidth, or frame structure. The number of symbols that carry the DCI in a sub-frame is defined in the Physical Control Format Indicator Channel (PCFICH). The control information such as PDCCH and PDCFICH are located within the first slot (Slot 0) of each sub-frame and occupy up to three columns. The number of control columns is different in each sub-frame.

The user data is carried using the Physical Downlink Shared Channel (PDSCH). In each sub frame, the columns for PDSCH information are located after the columns for the control information.

Master Information Block (MIB) has the essential cell parameters such as bandwidth and frame timings. MIB exists in the Physical Downlink Broadcast Channel (PBCH) which is located within the first sub-frame (Sub-frame 0). When a phone is turned on, it does not know the bandwidth deployment of the operator. So, the phone needs to find this information by reading the MIB. The MIB is sent over four radio frames. The MIB information can be decoded from each of these radio frames. Therefore, there is no need to wait for all 4 frames, if the signal is strong enough.

The Automatic Repeat Request (ARQ) information is located in the Physical Hybrid Automatic Repeat Request Indicator Channel (PHICH). LTE uses ARQ scheme for error correction. The tower sends a Hybrid Automatic Repeat Request (HARQ) indicator to the cellphone to indicate a positive acknowledgement (ACK) or negative acknowledgement (NACK) for the data sent using the uplink shared channel. These indicators are transmitted through the PHICH.

There are four downlink reference signals CRS, DM-RS, CSI-RS, and PRS. These reference signals are necessary for data demodulation and are located throughout the data and control channels. PDSCH and four other physical channels (PDCCH, PHICH, PDCFICH, and PBCH provide all the user data, control information, and system information needed for unicast data transmission. All these channels are shown in Figure 3.3.

The uplink radio frame and sub-frame structure in both time and frequency are similar to the downlink frame. In terms of channels, there are several uplink physical channels in LTE. We now discuss these channels.

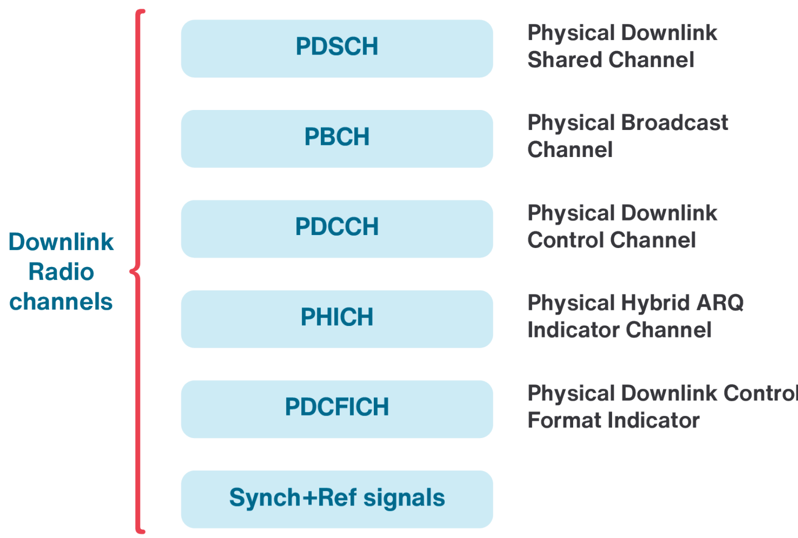


Figure 3.3: Downlink radio channels

1. Physical Random Access Channel (PRACH) is used for initial access of an IoT device to the network. Using this channel, the random access preambles are sent in the uplink direction. The IoT device uses PRACH to transmit a preamble to initiate random access.
2. Physical Uplink Control Channel (PUCCH) carries the uplink control information (UCI), including scheduling requests, acknowledgments (ACKs/NACKs), and reports of measurements for the downlink channel.
3. Physical Uplink Shared Channel (PUSCH) carries the user data transmitted by UE. It should be noted that the UE should have received an uplink scheduling grant before its data is transmitted through PUSCH.
4. There are a couple of uplink reference signals in uplink radio frame. One is the Demodulation Reference Signals (DMRS) and the other one is the Sounding Reference Signal (SRS). DRMS is used for channel estimation and demodulating the uplink control and data information. SRS enables the scheduler to allocate the data to portions of the uplink bandwidth where the channel responses are

better.

We discussed briefly some of the main downlink and uplink channels in legacy LTE to give the reader an understanding of the frame structure and channels in LTE.

3.3.2.2 LTE-M

LTE-M tries to modify and optimize the LTE technology to achieve deeper coverage, lower power consumption, longer battery life, lower device cost, and larger device density per cell without loosing capacity. LTE-M technology modifies the legacy LTE to ensure that the technology is suitable for IoT applications in terms of performance and functionality.

As we mentioned in the previous section, scalable carrier bandwidths from 1.4 MHz to 20 MHz, utilizing 6 to 100 resource blocks are supported by LTE. LTE-M uses part of the existing bandwidth for IoT. The bandwidth of LTE-M in Release 13 was limited to 1.4 MHz (1.08 MHz plus guard-band). It should be noted that the LTE-M network supports two Coverage Enhancement (CE) modes, the mandatory mode A and the optional mode B. CE mode A supports only moderate coverage enhancements, while mode B supports very deep coverage. LTE-M also supports a maximum data channel bandwidth of 5MHz in uplink. The control signaling is still restricted to 1.4 MHz in order to re-use as much as possible of the Rel-13 design. There is no change in duplexing scheme in this release. The LTE-M bandwidth is increased to support maximum channel bandwidths of 5 or 20 MHz for mode A and mode B in downlink, respectively.

To reduce complexity, LTE-M devices can support half-duplex communications. LTE-M in Release 13, 14 and 15 support half-duplex FDD in addition to TDD. In full duplex FDD, the data transmission and reception can be done simultaneously, while in half-duplex operation, a device should alternate between transmission and reception as shown in Figure 3.4. Using HD-FDD can reduce the data rate, but devices that only support HD-FDD are less complex, and therefore, less costly.

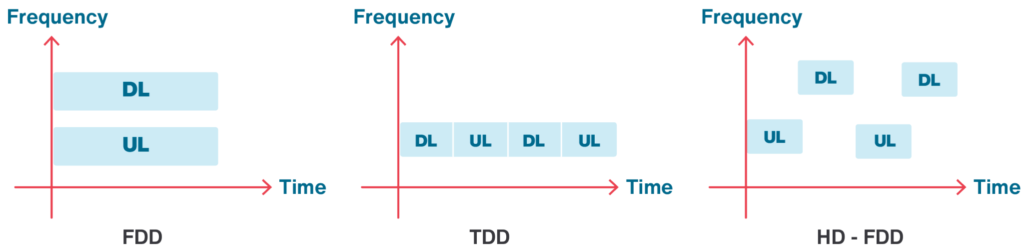


Figure 3.4: Comparison among FDD, TDD and HD-FDD

A comparison between some channels and signals in LTE and LTE-M is listed in Table 3.2. As seen in this table, the LTE-M signalling is very similar to the legacy LTE. In LTE-M, there have been more changes to PDCCH control channel compared to the other channels. In this regard, a new channel called MPDCCH which stands for MTC physical downlink control channel has been introduced. MPDCCH is a special type of PDCCH designed for IoT operation. Most channels in LTE-M are very similar to legacy LTE, except that the repetition and frequency hopping have been added to most of the channels.

Table 3.2: A comparison between some channels and signals in LTE and LTE-M

Channel Name	UL/DL	LTE-M	Important changes
PSS /SSS	DL	Similar to Legacy LTE	No change
Reference signals	DL	Similar to Legacy LTE	No change
PBCH	DL	Similar to Legacy LTE	Repetition is added to coverage enhancement. Frequency tracking under low SNR regimes.
PDCCH	DL	Similar to legacy LTE (with some changes)	MPDCCH channel is added; New format to consider new set of DCI. Repetition and frequency hopping is allowed.
PDSCH	DL	Similar to Legacy LTE. (with small changes)	Repetition and frequency hopping is allowed.
DMRS	UL	Similar to Legacy LTE.	No change
PRACH	UL	Similar to Legacy LTE. (with small changes)	Repetition is allowed. Frequency hopping needs to be executed.
PUCCH	UL	Similar to Legacy LTE. (with small changes)	Repetition and frequency hopping is allowed.
PUSCH	UL	Similar to Legacy LTE. (with small changes)	Repetition and frequency hopping is allowed. 64 QAM modulation is not allowed.

A simple example of downlink data transfer is shown in Figure 3.5. The data transfer starts with the base station sending a DCI signal to the IoT device. The base station then sends the data to the IoT device in downlink direction. The IoT device receives the data and sends an acknowledgement to the base station. There is a timing that needs to be respected during the operation. T_D represents the cross sub-frame delay, while T_{DUS} and T_{UDS} represent downlink to uplink switching time and uplink to downlink switching time, respectively. The T_D, T_{DUS}, and T_{UDS} values for LTE-M are 1ms, 3ms, and 3ms, respectively.

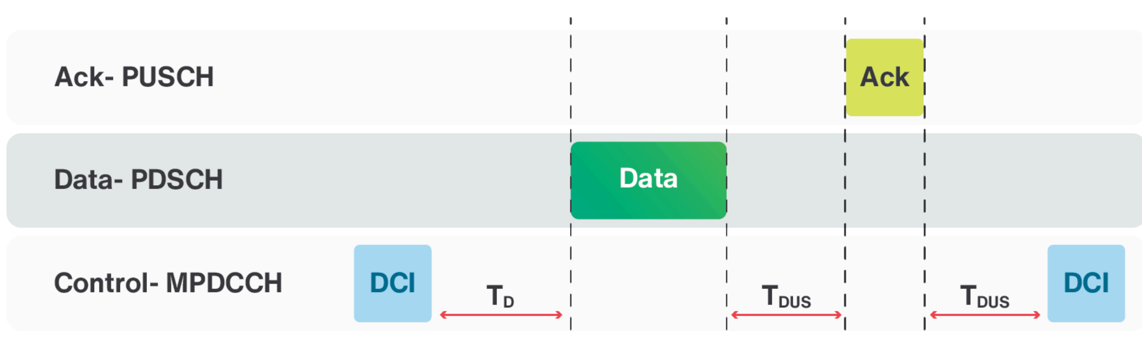


Figure 3.5: Downlink data transfer

The uplink data transfer is shown in Figure 3.6. The data transfer starts with the base station sending a DCI signal to the IoT device. The IoT device then sends the data to the base station. The base station receives the data and sends an acknowledgement to the IoT device. There is a timing that needs to be respected during this operation.

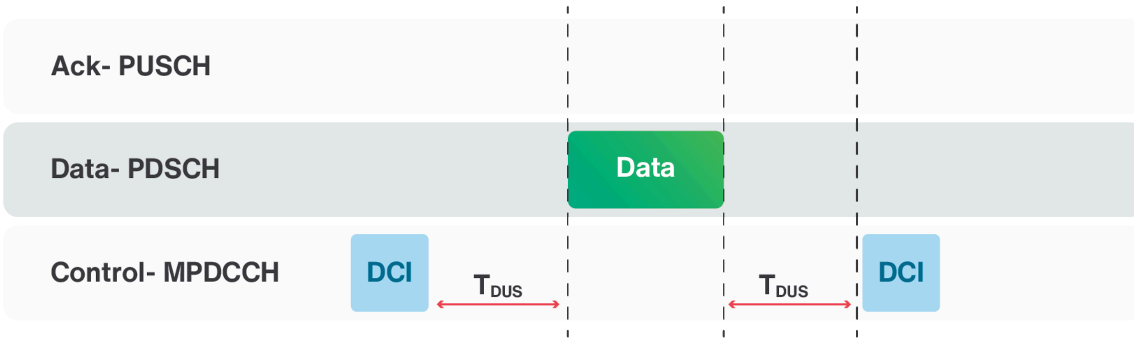


Figure 3.6: Uplink data transfer

To increase the data rate, the legacy LTE uses the HARQ process. The number of HARQ processes in LTE-M has been increased in some scenarios. In ARQ, when a receiver receives a corrupted packet, the receiver discards the corrupted packet and asks for a retransmission of the same packet by sending a NAK packet to the transmitter. If in the new retransmission, the packet arrives with errors, the receiver discards the packet again and requests for a new retransmission of the same packet. The HARQ technique uses the ARQ along with soft combining (an error correction technique), which does not discard the received corrupted data. In soft combining, the receiver buffers the corrupted packets and tries to perform error correction.

HARQ process for downlink in LTE-M is similar to legacy LTE except that the repetition of each transmission is allowed. However, HARQ process for uplink is different from the legacy LTE. The most critical difference is that the base station does not send any ACK/NACK. Instead of NAK in MPUSCH channel, it will send another DCI to ask the IoT device for another transmission.

It is clear that increasing the number of concurrent HARQ processes can increase the data rate. Figure 3.7 shows 2 HARQ processes in downlink. The timing for sending two packets can be calculated as $2 \times T_{DCI}+T_D+T_{Data1}+T_{Data2}+T_{DUS}+T_{ACK}+T_{UDS}$ as shown in Figure 3.7, where T_{DCI} is the time needed to send the DCI packet and T_{Data1} and T_{Data2} are the duration of Data1 and Data2 packets.

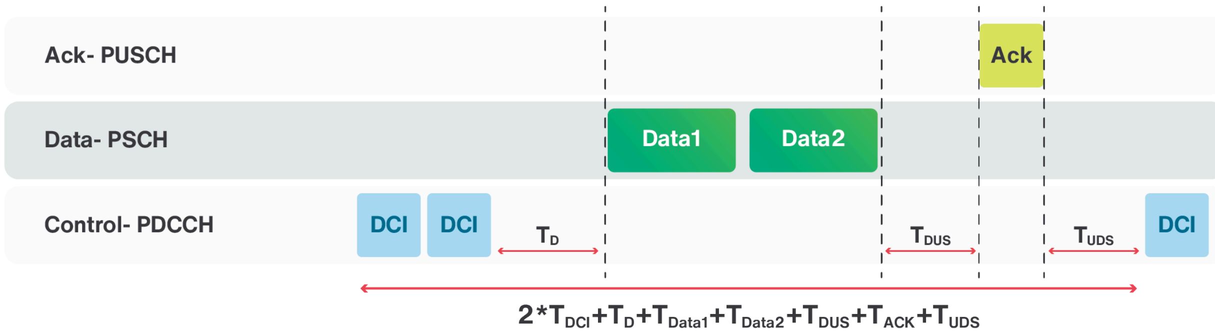


Figure 3.7: Downlink data transfer with 2 HARQ processes

The peak data rate for LTE-M depends on many factors. Some of these factors are the spectrum, the Transport Block Size (TBS), and the maximum number of HARQ processes. In general, increasing the TBS value results in higher data rate. Increasing HARQ processes can also increase the data rate. However, this happens mostly in good radio conditions.

In LTE-M Release 13, the spectrum is 1.4 MHz. LTE-M Release 13 provides a theoretical peak data rate of 1 Mbps using 1000 bytes of TBS and by using eight HARQ processes in both uplink and downlink directions. LTE-M Release 14 introduces Cat-M2 devices with the spectrum of 5 MHz and allows Cat-M2 devices to use a larger TBS as compared to Cat-M1 devices. The TBS for Cat-M2 devices can be up to 6968 bytes in uplink direction and 4008 bytes in downlink direction. It can also benefit from a maximum of ten HARQ processes in downlink and a maximum of eight HARQ processes in uplink. Therefore, the peak data rate is increased to 4Mbps in downlink and 7Mbps in uplink direction. To be able to transmit more consecutive TBS in downlink and increase the peak data rate for LTE-M in HD-FDD mode, Release 14 introduced a method to bundle HARQ-ACK for several TBS into a single transmission. LTE Release 14 also introduces non-balanced (non-BL) version with a spectrum of 20 MHz in downlink and 5 MHz in uplink. In Release 15, LTE-M supports better modulation scheme to increase the data rate, while the peak data rate for the IoT device is not increased. A summary of some of the parameters related to LTE-M technology in different 3GPP releases is listed in Table 3.3.

Table 3.3: A summary of some of the parameters related to LTE-M technology in different 3GPP releases

	Cat-M1 R13	Cat-M1 R14	Cat-M2 R14	Non-BL R14	LTE-M R15
Max. DL BW (MHz)	1.4	1.4	5	20	5
Max. UL BW (MHz)	1.4	1.4	5	5	5
Max. DL TBS (bits)	1000	2984	4008	4008	4008
Max. DL Data rate (Mbps)	<1	1	4	27	>4
Max. UL TBS (bits)	1000	2984	6968	6968	4008
Max. UL. Data rate (Mbps)	<1	3	7	7	7
Max. HARQ	8	8	10	10	10

Example 3.1:

LTE-M supports up to 52000 devices per cell in Release 13. The number of supported devices is increased substantially in higher releases. Let us consider a situation where three groups of IoT devices are connected to a given cell to transfer data. The first group contains 16000 weather monitoring devices, which send 100 bytes of data hourly. The second group consists of 16000 tracking devices, which transmit 50 bytes of data every 4 hours. The third group contains 16000 industrial machines, where each machine sends 25 bytes every 15 minutes. These devices are transferring data with an average of 7.56 kbps as shown in Table 3.4.

Table 3.4: information about three groups of IoT devices in example 3.1

Group #	# of devices	# of bits	Frequency of transmission	Average data rate
1	16000	100*8	every 3600 s	16000*100*8/3600=3.56 kbps
2	16000	50*8	every 14400 s	16000*50*8/14400=0.44 kbps
3	16000	25*8	every 900 s	16000*25*8/900=3.56 kbps
All groups				3.56+0.44+3.56=7.56 kbps

The maximum data rate of LTE-M is 1 Mbps which is much higher than the average data rate of 7.56 kbps in this case. One may think that the system can work with all IoT devices in this example without any issues. But, this is not a correct idea. Let us assume that 10% of IoT devices in each group send their data at the same time. For example, 1600 IoT devices belonging to the first group will send their data simultaneously which generates (1600×100×8) = 1.6 Mbits of data. This huge amount of data cannot be transferred with a network that can handle maximum data rate of 1 Mbps without causing any congestion. Many IoT applications are sending data when an event is triggered. In a practical situation, an emergency situation may cause many IoT devices to initiate the uplink access procedure simultaneously. Hence, we should expect degradation of system performance in such scenarios.

3.3.2.3 NB-IoT

Since there are many IoT applications that send small amounts of data (lower than the amount typically transmitted by LTE-M IoT devices), a special category, called NB-IoT, has been considered in LTE specifications. NB-IoT uses a small bandwidth for data transmission and reduces the bandwidth to 200 kHz (180 kHz plus guard-band) as compared to 1.4 MHz used in LTE-M in Release 13.

NB-IoT can be deployed in three different modes to provide the limited bandwidth required for IoT applications. The first mode of deployment is in-band mode in which one PRB in LTE spectrum is dedicated for NB-IoT both in the DL and UL. The second mode of deployment is called the guard-band mode which is similar to in-band mode, but as the name implies, the spectrum resides in the guard-band of LTE spectrum. The last mode of deployment is called standalone mode in which NB-IoT occupies a 200 KHz bandwidth in the GSM spectrum. The comparison of these three deployment modes are shown in Figure 3.8. These deployment modes provide flexibility in IoT system design and enable the integration of 4G, 3G and 2G cellular technologies for IoT connectivity.

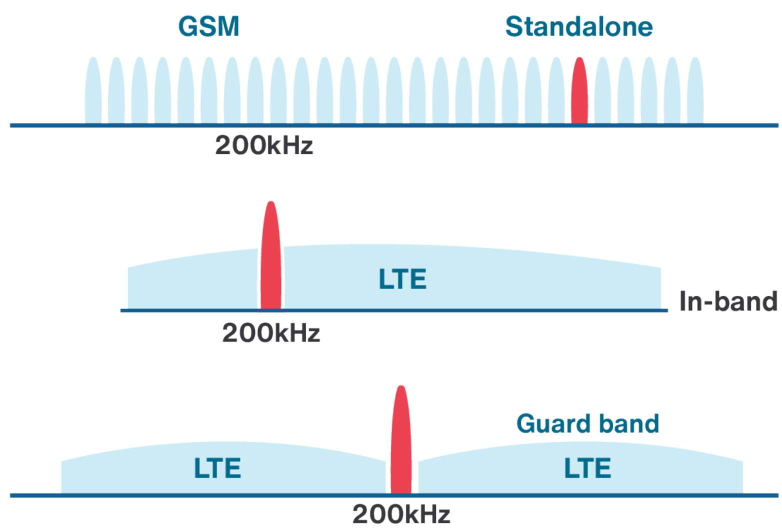


Figure 3.8. NB-IoT different modes of deployments

One of the objectives of NB-IoT is to provide connectivity to massive number of IoT devices. For this purpose, in NB-IoT a Resource Unit (RU) can be allocated to multiple UEs, while the legacy LTE network allocates an RU only to one IoT device in the uplink.

NB-IoT can also use either a 15 kHz or 3.75 kHz subcarrier spacing in uplink. The base station decides which subcarrier spacing needs to be used. In case of 15 kHz subcarrier spacing, the resource grid for the uplink is similar to downlink, while the resource grid for a slot in a 3.75 kHz subcarrier spacing has a modified structure. The symbol duration for 3.75 kHz subcarrier spacing has four times the symbol duration compared to 15 kHz, which results in a slot length of 2 ms.

For coverage enhancement and providing connectivity to the IoT devices located in poor radio connection, NB-IoT has an additional coverage of 20 dB as compared to the legacy LTE network. This is done by repetitions of up to 128 in uplink and up to 2048 repetitions in downlink direction. It is clear that repetition increases the delay, and enhancing the coverage comes at the expense of an increase in latency.

A comparison between some channels and signals in LTE and NB-IoT is listed in Table 3.5. As seen in this table, the NB-IoT has made substantial modifications to the LTE signaling and has introduced many new channels in contrary to LTE-M which is very similar to the legacy LTE.

Table 3.5: A comparison between some channels and signals in LTE and NB-IoT

Channel Name	UL/DL	NB-IoT	Important changes
PSS /SSS	DL	NPSS and NSSS signals	No change
Reference signals	DL	Similar to legacy LTE. (with small changes)	No change
PBCH	DL	Several changes to the legacy LTE	A new channel is added. The message size is reduced to 1600 bits in stead of 1920 bits. MIB info has been updated. Repetition is added to coverage enhancement.
PDCCH	DL	Several changes to the legacy LTE	NPDCCH channel is defined; New format to consider new set of DCI. Repetition is allowed.
PDSCH	DL	Several changes to the legacy LTE	NPDSCH channel is added. Repetition is allowed. Fragmentation is performed. Maximum TBS is 680 bits.
DMRS	UL	Several changes to the legacy LTE	Single tone and multi tone reference signals
PRACH	UL	Several changes to the legacy LTE	NPRACH channel is defined. Frequency hopping needs to be executed. Repetition is allowed. A new subcarrier spacing of 3.75KHz is added for single tone.
PUCCH	UL	No dedicated channel any more	
PUSCH	UL	Several changes to the legacy LTE	NPUSCH channel is defined. Repetition needs to be executed. QAM modulation is not allowed.

NB-IoT Release 14 supports a maximum of 2536 bits as TBS in either uplink or downlink using one HARQ process. It also supports a maximum of two HARQ processes with 1352 and 1800 bytes in uplink and downlink, respectively. For NB-IoT Release 14, the downlink peak data rate is 80 kbps and the supported uplink peak data rate is 105 kbps. NB-IoT optimizes the signaling of small-sized data to increase the network capacity to serve very large number of devices. Table 3.6 compares some of the NB-IoT parameters in different NB-IoT releases.

Table 3.6: comparison of NB-IoT parameters in different NB-IoT releases.

	Cat-NB1 R13	Cat-NB2 R14	NB-IoT R15
Max. DL BW (MHz)	0.2	0.2	0.2
Max. UL BW (MHz)	0.2	0.2	0.2
Max. DL TBS (bits)	680	2536	2536
Max. DL Data rate (Mbps)	0.025	0.127	>0.127
Max. UL TBS (bits)	1000	2536	2536
Max. UL. Data rate (Mbps)	0.062	0.159	>0.159
Max. HARQ processes	2	2	2

Chapter 3 Exercises

1. Which sentence is correct about the spectrum and data rate of the LoRaWAN and Sigfox?
    a. The spectrum of the LoRaWAN is larger and its data rate is higher than Sigfox.
    b. The spectrum of Sigfox is larger and its data rate is higher than the LoRaWAN.
    c. LoRaWAN uses larger spectrum than Sigfox, but has adaptive data rate and therefore its data rate might be higher or lower than Sigfox.
    d. LoRaWAN uses smaller spectrum than Sigfox. However, since it is using a better modulation technique has higher data rate.
2. Which of the following technologies can be used for tracking of a car in a city?
    a. NB-IoT Release 13.
    b. LTE-M.
    c. Sigfox.
    d. LoRaWAN.
3. Is LoRaWAN a cellular wide area network?
    a. Yes, it is cellular. LTE-M, NB-IoT, and Sigfox are cellular as well.
    b. Yes, it is cellular. LTE-M, NB-IoT are cellular, but Sigfox is not cellular.
    c. No, it is not cellular. LTE-M, NB-IoT, and Sigfox are cellular as well.

    d. No, it is not cellular. LTE-M, NB-IoT are cellular. But, Sigfox is not cellular.

4. What is the difference between LoRa and LoRaWAN?
    a. They are the same.
    b. LoRa defines the physical layer of the system, LoRaWAN defines the protocols over LoRa and it is the network architecture which operates in a non-licensed band.
    c. LoRa defines the gateway architecture, LoRaWAN defines the protocols from gateway to a WAN.
    d. LoRa is developed by LoRa Alliance and LoRaWAN by Semtech.

5. What spectrum is used in LTE development? What about LTE-M?
    a. LTE uses 1.4, 3, 5, 10, 15, or 20 MHz spectrum. LTE-M always uses 1.4 MHz.
    b. LTE uses 1.4, 3, 5, 10, 15, or 20 MHz spectrum. LTE-M uses 1.4 in Release 13 and 5 MHz in Release 14 and above.
    c. LTE uses 15 or 20 MHz spectrum. LTE-M always uses 1.4 MHz.
    d. LTE uses 15, or 20 MHz spectrum. LTE-M uses the same as LTE.

6. The signaling channels used for LTE-M are …
    a. exactly the same as LTE.
    b. completely different than LTE.
    c. very similar with some differences.
    d. mostly different, but there are a few similarities.

7. The signaling channels used for NB-IoT are …
    a. exactly the same as LTE.
    b. are completely different than LTE.
    c. are very similar with some differences.
    d. are mostly different, but there are a few similarities.

8. What does Half Duplex –FDD (HD-FDD) mean?
    a. The duplexing is FDD , but spectrum is half of entire spectrum.
    b. The duplexing is FDD, but the data transmission and reception can be done simultaneously.
    c. The duplexing is FDD, but the device should alternate between transmission and reception.
    d. The duplexing is FDD half of the time, and the other half can be anything else such as TDD.

9. What is the duration of each LTE radio frame? Each radio frame is divided into how many sub-frames?

    a. 10 ms, 10.

    b. 100 ms, 100.

    c. 10 ms, 100.

    d. 100 ms, 10.

10. What is the Physical Random Access Channel (PRACH) used for in the LTE-M system?

    a. Access permission of an IoT device to the network for initiating data transfer.

    b. Sending scheduling requests.

    c. Sending reference signals.

    d. Sending data packets.

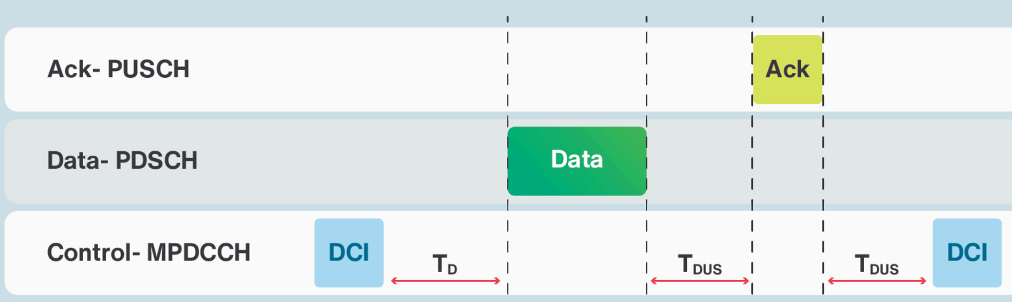
11. A simple example of downlink data transfer is shown below. The data transfer starts with the base station sending a DCI signal to the IoT device. The base station then sends the data to IoT device. The IoT device receives the data and sends an acknowledgement to the base station. There are timings that need to be respected during the operation which are called and . What is the range of duration of TD, TDUS and TUDS?

    a. One to several microseconds.

    b. One to several milliseconds.

    c. Tens of milliseconds.

    d. One to several seconds.

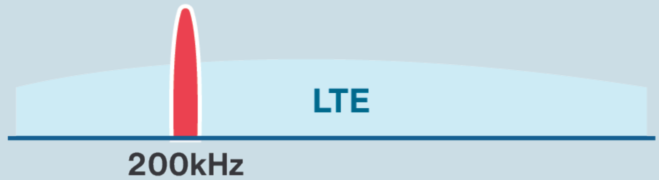


12. What NB-IoT deployment is shown below?

    a. In-band.

    b. Standalone.

    c. Guard-band.



d. Out of band.

13. NB-IoT has an additional coverage of 20 dB as compared to the legacy LTE network. How is this 20dB achieved?
    a. By increasing the transmit power.
    b. By changing the frame structure.
    c. By introduction of repetitions.
    d. All of the above.

Chapter 3 Review Questions

1. What standards are developed by 3GPP?
2. Does a 3GPP release number represent a specific cellular technology?
3. GSM is an older technology. Why GSM is still an attractive choice for IoT technology?
4. Compare LTE-M and NB-IoT in terms of data rate, spectrum and mobility.

Answers to Exercises and Review questions are located at the end of the book: Chapter 3 Answers

Appendix A

In BLE terminology, scan interval (T) is the duration of time between two consecutive times that the scanner wakes up to receive the advertising messages. The scan interval is shown in Figure A.1. When the scanner wakes up, it enables its reception to be able to listen to the advertising messages for a duration of T_S, which is called the scan window. The value of scan interval should always be greater than or equal to the scan window. The values of T and T_S should always be in the range of $0 \leq T_S \leq T \leq 10.24$ s. In general, BLE modules use three different channels for advertising which are called Channel 37, 38 and 39. When a BLE module becomes a scanner or initiator, it scans these three advertising channels one by one in sequence of Channel 37, 38, and 39, according to a round-robin fashion, as shown in Figure A.1.

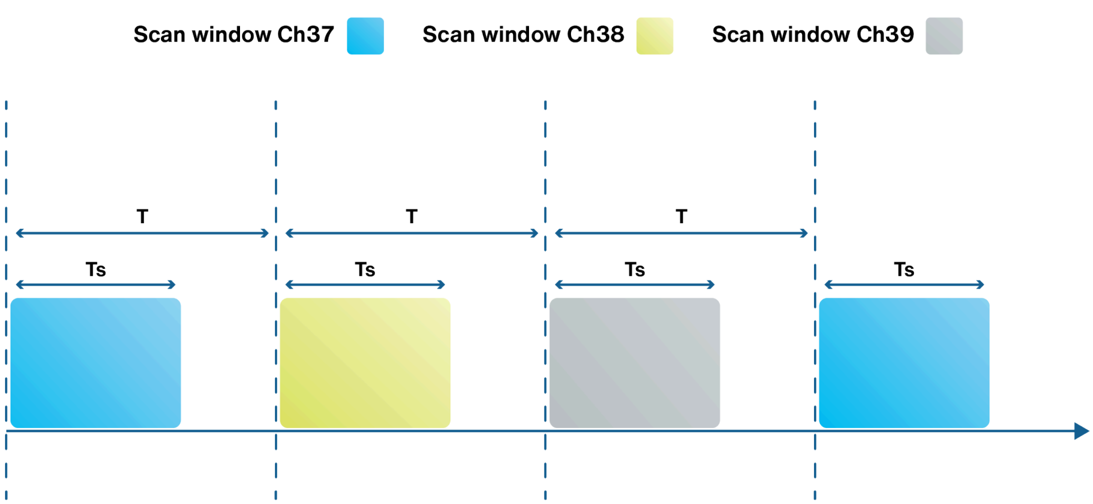


Figure A.1: BLE scanning/ initiating process

The advertiser periodically generates advertising events. Each advertising event consists of a sequence of advertising messages. T_{ad} is the duration of time that will take for the advertiser to send an advertising message on a predefined advertising channel during each advertising event. At that time, the advertiser goes into the reception mode and listens for the duration of T_r on the same channel. Then, as shown in Figure A.2, the advertiser moves to the next advertising channel.

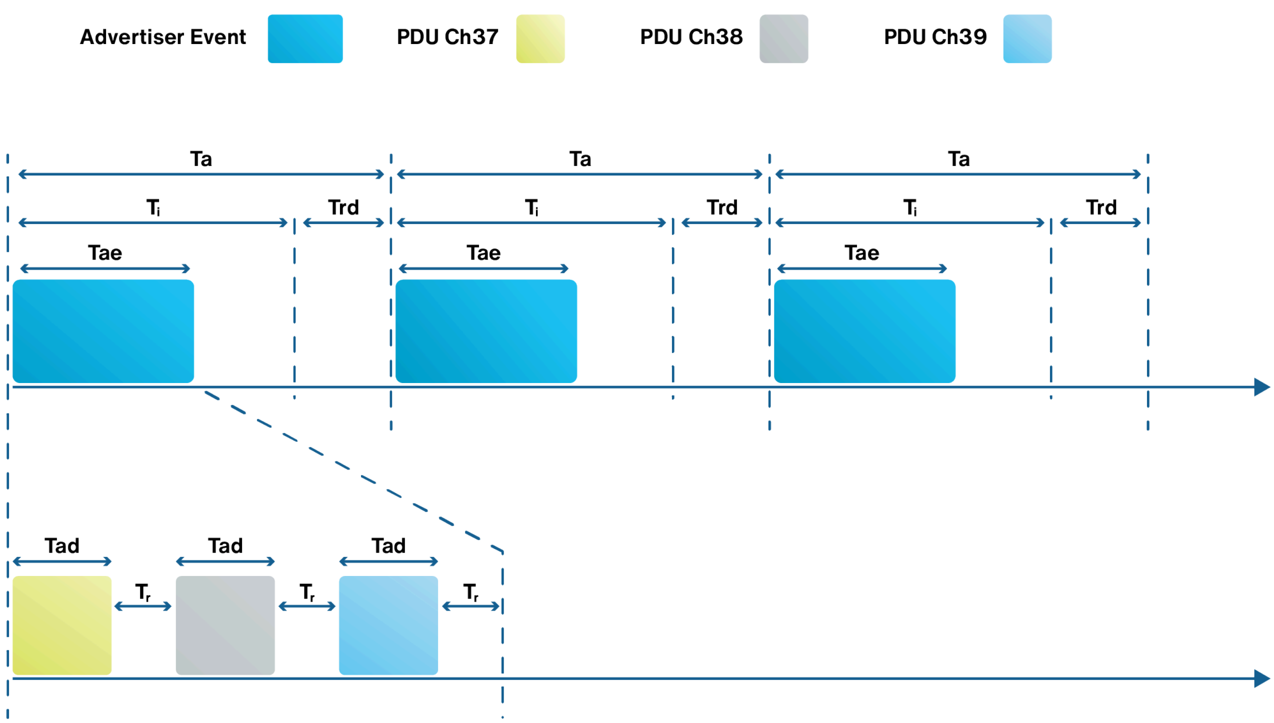


Figure A.2: Advertising process

Two types of scanning are defined for a BLE device which are called passive scanning and active scanning. In passive scanning, a scanner receives advertisement messages, but does not send any packet to the advertiser, while in active scanning, the scanner listens to advertisement messages and after receiving an advertisement message, it sends a scan request packet to the advertiser. The scan request packet can help the scanner to learn more about the advertiser. For example, the scanner can ask about supported services by the advertiser. In response, the advertiser can send a list of its supported services.

The value of T_{ad} is determined by the size of an advertising message. The size of each advertising message can be as small as 80 bits or as long as 376 bits. The value of T_r is adjusted to the tolerable time for the advertiser to wait for the scanner's reply. The value of T_a represents the interval between two advertising events and consists of a fixed interval, T_i, and a variable interval which can be represented as a pseudorandom delay T_{rd} . Based on BLE specifications, 20 ms ≤ T_i ≤ 10.24 s, 0 ≤ T_{rd} ≤ 10 ms, and the value of T_i should be a multiple of 0.625 ms.

Since there is possibility of receiving several scan request messages from an advertiser by multiple scanners, it is likely that the packets collide with each other. If such a situation arose, each scanner should use a back-off strategy to minimize the possibility of collisions.

After receiving an advertising message by a scanner or initiator, they can initiate a connection. Connections enable a reliable communication for data transmission. To ensure robust delivery of data, Cyclic Redundancy Checks (CRC), acknowledgements, and retransmissions of lost or corrupted data are considered in BLE connections. BLE uses Adaptive Frequency Hopping (AFH) to detect and adapt hopping sequences dynamically to the surrounding environment and provide a robust physical layer. Data encryption is also supported by connections. A connection is initialized when a scanner (central BLE) sends a Connect Request packet. When the advertiser receives a Connect Request message and accepts this request, it stops advertising and follows the parameters in the Connect Request packet to start a connection. An advertiser checks several conditions before accepting the connection request. The advertiser needs to be enabled to accept connections and should not have any whitelist or if it has one, the initiator's address should be in the whitelist. After establishing the connection, the initiator becomes the central node and the advertiser becomes the peripheral node. The central BLE node sends a connection event message on every connection interval. And the peripheral BLE node opens the scan window on every connection interval after the first connection event. The peripheral then sends a connection event packet toward the central node which acts as an acknowledgment. This packet may contain the user data as well.

The connection parameters provide information about the communication between the central and peripheral BLE node and are included in the Connect Request packet. A Connect Request packet contains several fields. The most important fields of this packet are interval, latency, and timeout. Connection Interval (CI) is the time between two BLE connection events. The peripheral BLE node specifies the minimum and maximum values of interval, but the CI value for communication is set by the central node when the BLE connection is first established. Some central BLE devices ignore the maximum and minimum values specified by the peripheral and use some default CI values instead. The duration of CI is equal to the interval times 1.25 ms. The BLE specifications state that the interval can be any value between 6 and 3200. In other words, the connection interval time can accept any value in the range of 7.5 ms to 4000 ms. Latency field defines the number of connection events the peripheral BLE node is allowed to skip the transmission. If the peripheral node does not have any data to send, it has the option to skip several connection events. This can provide some reduction in power consumption for the peripheral device. It should be noted that the peripheral BLE node should not stay too long in the sleep mode to lose its connection to the central BLE node. The number of consecutive connection events that the central BLE node continues its operation without receiving any data is defined as timeout.

Appendix B

At the physical layer, Bluetooth 5 supports speed of 2 Mbps. It doubles the symbol rate as compared to BLE V 4.2 in order to increase the data rate at the cost of slight reduction in the communication range. To be compatible with BLE, Bluetooth 5 also supports the data rate of 1 Mbps. At this data rate, each bit maps to a single radio symbol. To provide long-distance connections, Bluetooth 5 introduced the coded scheme at 1 Mbps physical layer as a new particular connection type that its primary goal is to improve the range of connectivity but with a lower bit rate. The coded physical layer provides relative data rates of 500 kbps or 125 kbps, using a forward error correction technique which replaces each bit into 2 or 8 bits, respectively. It is clear that the forward error correction provides better tolerance for bit errors. This results in improving the range of communication. The packet structure of un-coded 1 Mbps and 2 Mbps as well as coded physical layer is shown in Figure B.1.

Each packet in Figure B.1 starts with a preamble. A Bluetooth 5 receiver will use the preamble for frequency synchronization, automatic gain control training, and symbol timing estimation.

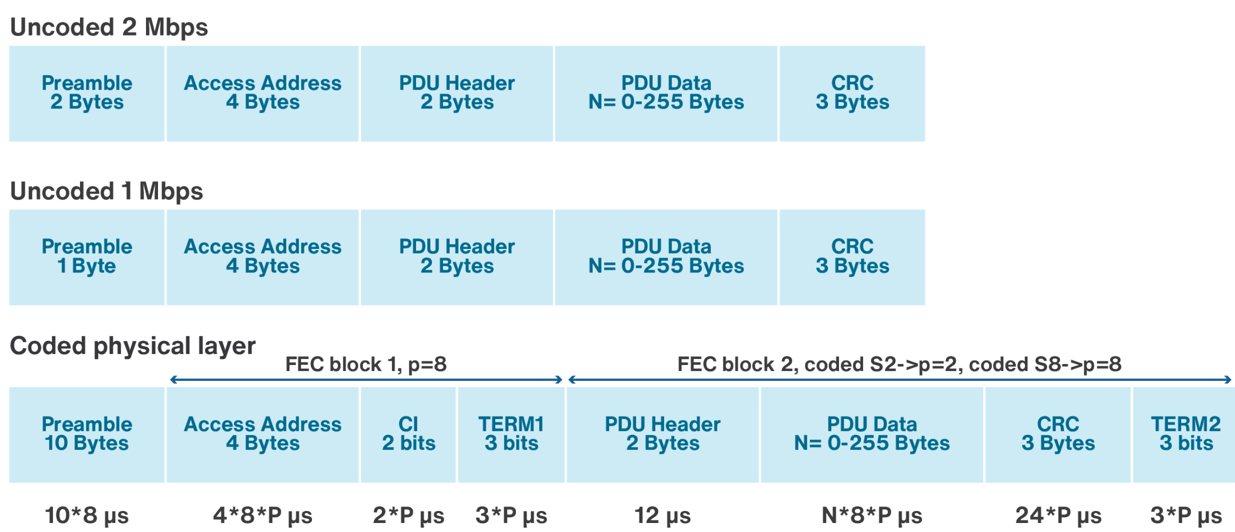


Figure B.1: The packet structure of uncoded 1 Mbps and 2 Mbps as well as the coded physical layer in Bluetooth 5

The preamble for the uncoded 1 Mbps and 2 Mbps physical layers consists of an alternating sequence of 0 and 1, where the LSB of the access address determines the first bit of this sequence. The preamble for the coded physical layer is fixed and consists of 10 repetitions of 0x3C.

Each link layer connection between any two nodes as well as each periodic advertisement is identified by a different Access Address (AA). The packet structure for coded physical layer contains there sections of preamble, FEC block 1 and FEC block 2. FEC block 1 has three fields: AA, Coding Indicator (CI), and Term 1 as shown in Figure B.1. The coding indicator consists of two bits, 00 indicates that FEC Block 2 is encoded using S8, and 01 indicates that FEC Block 2 is encoded using S2. Figure B.2 shows the way that FEC encoder and pattern mapper generate S2 or S8. As it is shown in this figure, S2 shows a situation that the input bits only go through the FEC encoder and the bits after leaving the FEC encoder are doubled. S8 shows that the input bits go through both the FEC encoder and the pattern mapper. The input bits are first doubled by FEC encoder and those bits are then quadrupled by the pattern mapper. Term1 is made of three consecutive zeros. It indicates a termination sequence which resets the FEC encoder.

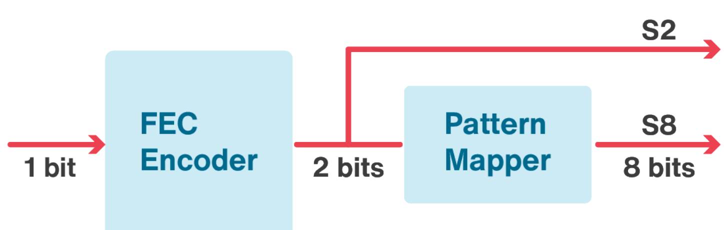


Figure B.2: FEC encoder and pattern mapper in Bluetooth 5

The Protocol Date Unit (PDU) in Bluetooth 5 is either an advertising channel PDU or a data channel PDU. In uncoded physical layer, the PDU follows the access address field. An advertising channel PDU might be on the primary advertising channel or the secondary advertising channel. The data channel PDUs are the ones that are transmitted on a data channel. For error detection, there is a 3-byte CRC for each PDU. For coded physical layer, everything in FEC Block 2 is encoded according to the CI field in Block 1. Three consecutive zeros (Term2) terminate the transmission and reset the FEC encoder for Block 2.

For a *N* bit PDU (excluding the PDU header) and based on various types of physical layer (PHY), the information related to the physical layers of Bluetooth 5 is listed in Table B.1. The value of x represents the range achievable using 1 Mbps physical layer. If the other physical layer is used, the estimate of the range in terms of x is presented.

Table B.1: Various information related to the physical layers of Bluetooth 5

Bluetooth 5 -PHY	Packet duration	Relative data rate	CRC	FEC	Range
PHY 2M	44+4N μs	2Mbps	Yes	No	0.8*x
PHY 1M	80+8N μs	1Mbps	Yes	No	x
PHY coded s=2	462+16*N μs	500Kbps	Yes	Yes	2*x
PHY coded s=8	720+64*N μs	125Kbps	Yes	Yes	4*x

The bit data path for un-coded 1Mbps and 2Mbps PHYs as well as the coded PHY is shown in Figure B.3.

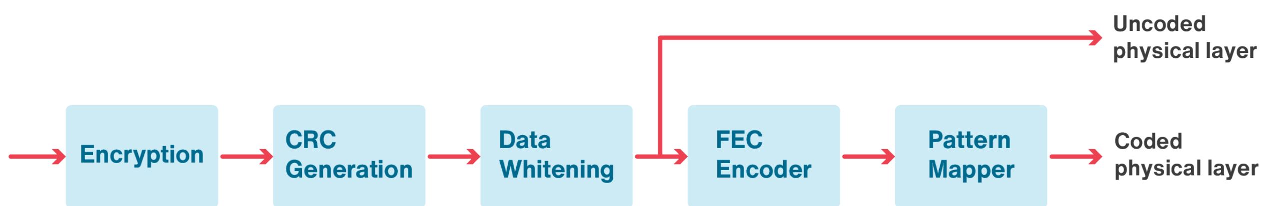


Figure B.3: Transmitter bit data path for un-coded 1M and 2M physical layers in BLE 5

Data is encrypted (if needed) and CRC is added to the data. Data whitening process is then applied to both the PDU and CRC fields in order to prevent long sequences of repetitive bits (e.g., 00000000 or 11111111). Data whitening uses a 7-bit Linear Feedback Shift Register (LFSR) with taps at bit four and bit seven. For the coded physical layer, data also needs to pass through the FEC encoder and pattern mapper as it was explained earlier. At the receiver, the received packets also go through several processes similar to the transmitter side but in reverse order as shown in Figure B.4.

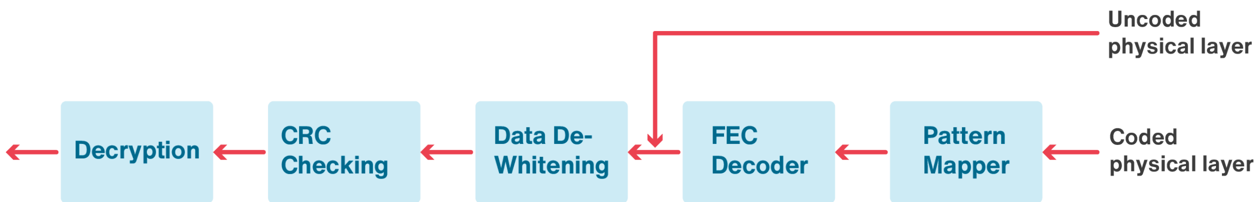


Figure B.4: Receiver bit data path for un-coded 1M and 2M physical layers in Bluetooth 5

The extended advertising mode is an effective method to improve the performance of connectionless communication of advertising messages among nodes. This is done by integrating the advantage of random access control method used in advertising channels and a scheme of chained advertising information in data channels. In general, advertisements are used by nodes to send data that can be discovered and processed by observer nodes. This enables Bluetooth nodes to send data to multiple nodes at the same time, without having a connected peer-to-peer communication. To exploit the advantages of advertising, Bluetooth 5 introduces significant changes to advertising process. To provide backwards compatibility and interoperability, the three advertisement channels are going to remain similar to BLE 4.2. However, they are now called primary advertisement channels.

Bluetooth 5 has realized the popularity of its advertisement scheme in many IoT applications and therefore in addition to the existing three primary advertisement channels, it uses any of the remaining 37 data channels as secondary advertisement channels. This can help Bluetooth 5 to broadcast more advertisements as well as to offload the traffic of the primary channels. In other words, by using advertising extension, Bluetooth 5 offloads advertising data from only three advertising channels to all data channels. The peripheral nodes can send short extended advertising message in the primary advertising channels. The extended advertising message includes a pointer to a secondary advertising channel which is chosen randomly from the data channels. Table B.2 summarizes the differences between BLE and Bluetooth 5 advertising channel schemes in terms of advertising channels, the length of advertising messages and the physical layer modes of operation.

Table B.2: Differences between BLE version 4 and Bluetooth 5 advertising channel schemes

Bluetooth	Advertising channels	Length	PHY
4	3 channels (37,38,39)	0-31 Bytes	1 Mbps
5	3 Primary (37,38,39) 37 secondary	0-31 B (primary) 0-255 B (secondary)	1M, coded (primary) 1M, 2M, coded (secondary)

To allow the transmission of larger advertising data and to remove the need to duplicate the data payload on all three advertising channels, Bluetooth 5 allows a smaller packet sent on the three primary advertising channels to point to a larger packet sent at a later time on one of the 37 data channels. In Bluetooth 5, the maximum size of a single advertising packet can be 255 bytes of data, up from 37 in BLE 4.2. Advertising messages can now be chained together. This will allow for larger advertising packets as shown in Figure B.5. The maximum size of a chained advertising packet is 1650 bytes.

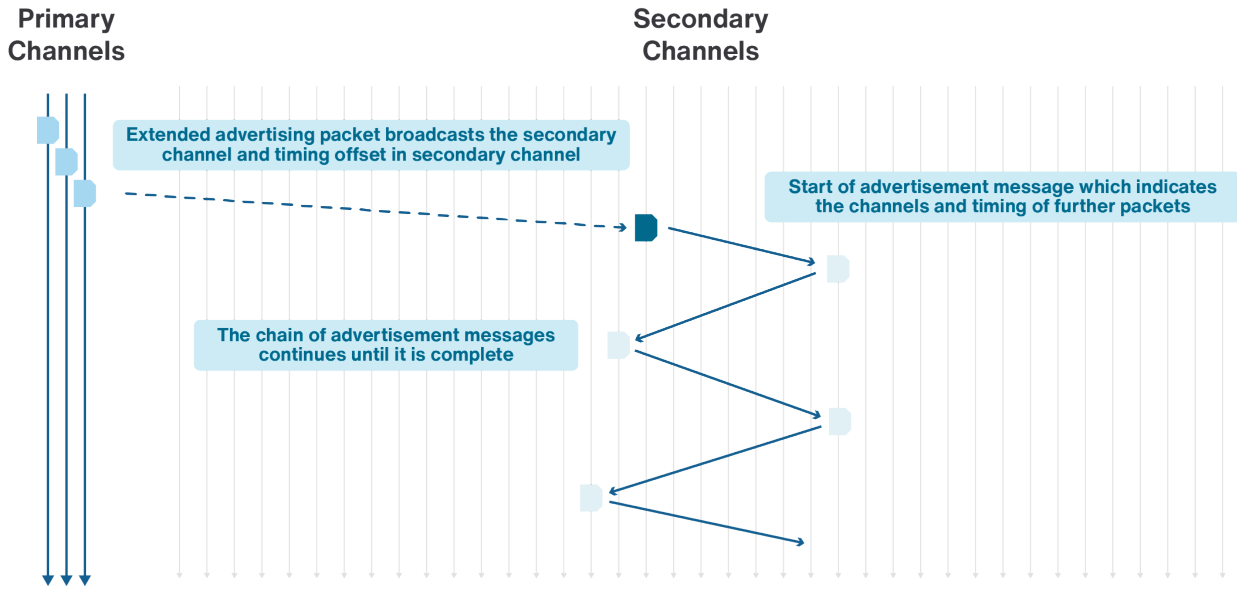


Figure B.5: Chained advertising packets

Periodic advertisement is another feature added to Bluetooth 5 in which a periodic advertiser broadcasts the packets, with size of up to 255 octets and with a regular interval ranging from 7.5 ms to almost 82 s. This is accomplished by hopping between the secondary channels in a predefined pseudo-random pattern. A scanner device is able to receive data from one or even several non-overlapping periodic advertisers. Higher data throughput is achievable by combining periodic advertisements with chained packets. This equips Bluetooth 5 with a more efficient and reliable solution for data broadcast than the one exists in BLE. Since advertising packets can be sent periodically, observers are allowed to join and lock on to a stream of advertising data. For instance, the periodic advertising can be used for sending synchronous data, like audio broadcasts. In this case, the new primary advertisement message points to an auxiliary packet which in turn specifies a "connectionless" chain of packets which hop at a known interval. This is illustrated in Figure B.6.

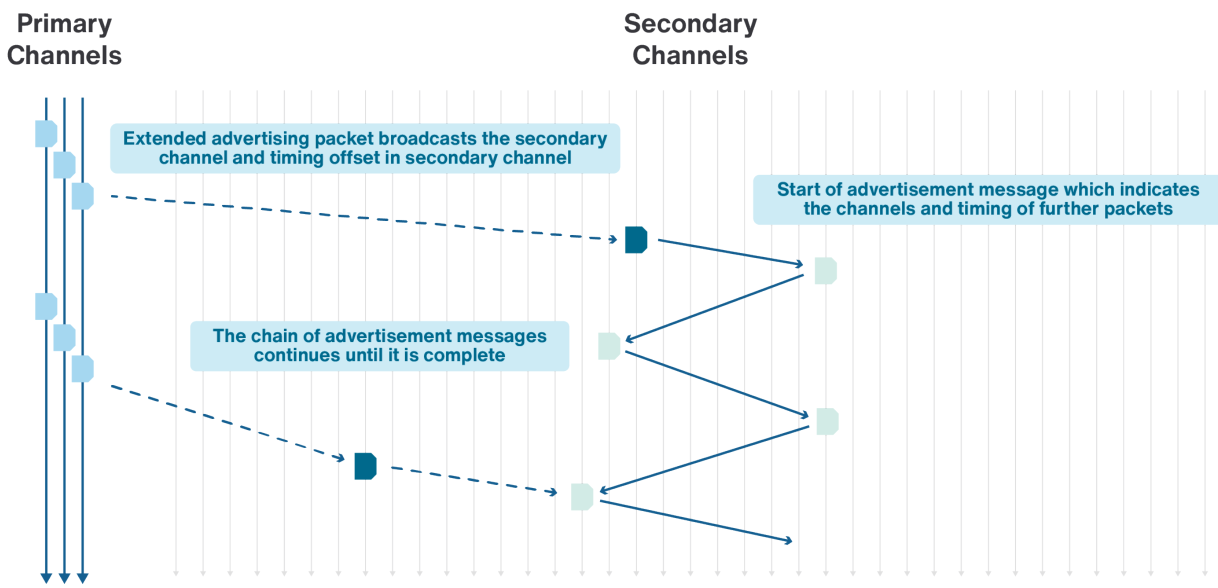


Figure B.6: periodic advertisements

Maximum transmit power in Bluetooth 5 is +20dBm, up from +10dBm in BLE. It is clear that increasing the transmit power has direct relationship with the maximum range that the technology can support. There might be some restrictions to use +20dBm globally due to various regulatory bodies.

Chapter 1 Answers

Answers to Exercises

1. **a**. Since they belong to the same vertical, they should be similar in terms of their regulatory bodies, and standards. However, since they do not belong to the same use case, they might be quite different in terms of their platforms and processing.
2. **d**. The traffic generated by people when talking on the phone or receiving data is somewhat different as compared to the IoT traffic. All three choices of a, b, and c are important differences between these two types of traffics.
3. **b**. A WSN network has nodes that communicate with each other, but might be local and not connected to the Internet.
4. **a**. The concept of remote device connection existed before the era of modern Internet. The first connected vending machine was invented in 1990. But, the term “IoT” first used by Kevin Ashton, to promote Radio Frequency Identification (RFID) technology.
5. **a**. An IoT gateway enables many IoT devices with no Internet connectivity to connect to the Internet via the gateway.
6. **b**. In an IoT network, several IoT devices might play the role of IoT gateways, if they have access to the Internet. For example, in a local area network with mash topology where more than one IoT device is connected to the Internet, all connected devices can be programmed to play the role of the IoT gateway.
7. **c**. Due to the existence of massive number of IoT devices, it would be beneficial to consider low power consumption as a requirement for IoT. Reducing the power consumption of each device reduces the total energy needed to be produced to power these devices.
8. **c**. An IoT device can reduce its power consumption by reducing the time that the radio is active. It is clear that when an IoT device goes to sleep and inactivates its radio, the device becomes unreachable. Therefore, the IoT device needs to go to sleep if it does not have anything to perform. Fortunately, in many IoT applications, that is the case.
9. **d**. The technologies such as Zigbee, BLE, or WiFi are short-range wireless

technologies. LPWAN technologies are related to wide area networks and they can provide long range connectivity.

10. **c**. IIoT stands for Industrial Internet of things. The term XIoT where X can be different letter, has been widely used in IoT related articles and documents.
11. **d**. It is possible for an IoT device to send the medical data of a patient to the Internet. After the data is analyzed, the information for treatment can be sent to the same IoT device. In fact, the IoT device should have the equipment needed for treatment. For example, an IoT device may send the glucose level of a patient and receive a command that automatically adjusts the insulin pump.
12. **b.** An IoT device can have one or several sensors such as body temperature, pulse, blood pressure. The connectivity should be wireless due to the patient's mobility.
13. **b.** 500×4=2000 zettabytes which is equal to 2 yottabytes.
14. **a.** smart meter can play the role of an IoT gateway.

Answers to Review Questions

1. Due to the mobility of the bird and the need for a connectivity scheme for providing a good coverage, cellular IoT is preferred.

2. A sensor (or a collection of sensors) is mounted on the helmet and is connected to a Bluetooth device. The Bluetooth device on the helmet is paired with the Bluetooth device on the smartphone. In this scenario, the smart phone plays the role of an IoT gateway. Once the helmet hits a hard object such as ice, or cement, the smart helmet will send the accident-related data to the smart phone. An app on the smartphone determines the severity of the crash based on the data. If the injury is severe, the location data in addition to the health data will be sent to an emergency contact. The smartphone can also send the data to the cloud, so that more processing and analysis can be performed.

3. Sensors can be embedded in the handle of racket to collect and send data. The data indicates the player's performance metrics regarding the type of shots (forehand/backhand), its power and effect, and the frequency that the ball is hitting the best spot of the racket during the game. This data can be used for training purposes to improve the performance of the players.

4. To determine the drowsiness of a driver, IoT glasses can determine the eye closure ratio as a sign of driver fatigue. The glasses can send the data related to eye closure ratio to the Internet. If this ratio is smaller than a standard threshold, the driver should be alerted.

5. From each welding spot 15 KB of data is generated per seconds. Since welding operation for each spot takes 10 seconds, 150 KB of data is generated in 10 seconds. There are 500 spots per each equipment. Therefore, 150 × 500 KB= 75 MB of data is generated for each equipment. A factory builds 200 equipment per day. So, the total amount of generated data would be 200 × 75 MB= 15 GB.

Chapter 2 Answers

Answers to Exercises

1. **d.** Traditional Ethernet does not support any quality of service metrics. That is one of the issues with traditional Ethernet. Choice c is wrong, since traditional Ethernet was not designed to meet the requirements needed for guaranteed and real-time communications. In other words, traditional Ethernet supports only the best-effort service.
2. **c.** preemption allows high priority packets to interrupt low priority ones. This is exactly opposite of choice a. It does not change the throughput of the system. It just reduces the transmission latency for high priority frames at the expense of increasing the latency for low priority frames.
3. **a**. Ethernet TSN guarantees the latency for real time critical data, but not for non-real time data. It is not based on best effort and therefore b and c are not correct.
4. **d**. Terabit Ethernet (TbE) is very fast and therefore is not widely used for IoT applications anywhere. It is usually used for Internet service provider's (ISP) core routing. So, both b and c are correct.
5. **a.** Narrowband PLC operates at frequencies between 3 KHz and 500 kHz. The broadband PLC works in frequencies between 1.8 MHz to 250 MHz. Narrowband PLC can be used for data rates of up to 100s of kbps.
6. **c.** Narrowband PLC is a better IoT connectivity scheme as compared to wireless schemes in metropolitan areas and dense urban regions, since in these regions attenuation of wireless signals is high.
7. **b.** The BLE on IoT gateway plays the role of a central node (master) and sends the Connect Request packet. The BLE node on the IoT device plays the role of advertiser and after connection is established becomes a peripheral BLE node.
8. **b**. The value of connection interval (CI) is equal to Interval × 1.25ms. Therefore, Interval needs to be 6.
9. **d**. If the Bluetooth module is set to PHY coded s=8, the maximum range is four times larger than when PHY 1Mbps is used. This is explained in Table 2.2. So, the range would be 200× 4= 800 m.

10. **a**. Bluetooth 5 can send advertisement packets of up to 256 bytes in length. The size has been increased from maximum 32 bytes in BLE 4.2. The data can be sent during advertisement and there is no need for connection. However, the possibility of collision exists.
11. **b.** Zigbee operates on 2.4 GHz globally.
12. **a.** It is true that in-building WiFi coverage is almost ubiquitous. So, answer a is correct. WiFi does not have the lowest power consumption among other short-range wireless technologies in the market. Actually, BLE and Zigbee draw less current as compared to WiFi. Answer c is wrong, since many smart home applications do not need very high-speed data transfer. It is true that WiFi can provide higher data rate as compared to other short-range wireless technologies. WiFi can provide substantially higher data rates as compared to BLE or Zigbee.

Answers to Review Questions

1. Time synchronization, traffic scheduling based on QoS, and frame preemption.
   i. Monitoring charge on the computer or phone, receiving notifications when charge is complete, over-the-air firmware updates, remote service if necessary, taking advantage of offpeak or low-rate charging time, negotiating for charging slots that does not overload the system.
   ii. Technologies such as Homeplug Green
2. The number of connection events the peripheral BLE node can skip is defined as latency parameter. If the peripheral node does not have any data to send, it has the option to skip several connection events. This can provide some reduction in power consumption for the the peripheral device.
3. Yes, in many IoT applications smartphones play the role of IoT gateway. Since most smartphones, tablets and computers do not have Zigbee module, they cannot be used as IoT gateway.
4. In a smart building use case, where the building has thick concrete walls, or specific thermal insulation material, the implementation of wireless technology may introduce many challenging issues and if possible the wired connectivity solution is preferable.

Chapter 3 Answers

Answers to Exercises

1. **a**. In general, Sigfox is a very low data rate network which uses a very small spectrum. LoRaWAN supports both 250 kHz and 125 kHz bandwidth. Depending on spreading factor and channel bandwidth, the LoRa data rate is between 300 bps and 50 kbps. Sigfox uses ultra narrow spectrum of 100 Hz, the amount of uplink as well as downlink data rate is very low. The maximum data rate of Sigfox is around 100 bps. Choice c is not correct. It is correct that the LoRa uses six spreading factors where higher spreading factor provide longer range and lower data rate, and lower spreading factors provide higher data rate at the expense of lower range. However, still with the highest spreading factor, the maximum data rate of LoRa is higher.
2. **b**. NB-IoT and Sigfox do not support mobility. LTE-M supports mobility even with high speed vehicles. The LoRaWAN supports mobility, but LTE-M has better features.
3. **c**. LTE-M, NB-IoT, and Sigfox are cellular. LoRaWAN is not based on cellular network.
4. **b**. They are not the same. LoRa defines the physical layer (L1) of the system, LoRaWAN defines the protocols over the LoRa and it is the network architecture which operates in a non-licensed band. LoRa is developed by Semtech and LoRaWAN by LoRa Alliance.
5. **b**. Operators have deployed LTE-M network using 1.4, 3, 5, 10, 15, or 20 MHz spectrum. There are some early deployments that are based on 1.4 MHz spectrum. LTE-M uses 1.4 in Release 13 and 5 MHz in Release 14 and above. Therefore, if an operator uses 1.4 MHz spectrum for LTE, LTE-M Release 14 cannot be deployed in that center.
6. **c**. LTE-M signaling is very similar to legacy LTE. In LTE-M, there have been more changes to PDCCH control channel compared to the other channels. The new channel is called MPDCCH which stands for MTC physical downlink control channel. MPDCCH is a special type of PDCCH designed for IoT operation. Most channels in LTE-M are very similar to legacy LTE, except that the repetition and

frequency hopping have been added to channels.

7. **d**. They are mostly different, but there are a few similarities. NB-IoT has made substantial changes to the LTE signaling and has introduced many new channels in contrary to LTE-M that was very similar to legacy LTE.
8. **c**. The duplexing is FDD, but the device should alternate between transmission and reception.
9. **a**. Each radio frame in LTE is 10ms, and is divided to 10 sub-frames. Each sub-frame has two slots each 0.5ms.
10. **a**. Access permission of a UE to the network for initiating data transfer. When a UE wants to transfer data, it should start a process called random access. To do that, the UE should send a preamble in Physical Random Access Channel (PRACH).
11. **b**. It is one to several milliseconds. The values of T_D, T_{DUS}, T_{UDS} for LTE-M are 1ms, 3ms, 3ms, respectively.
12. **a**. the correct answer is in-band mode. In this mode of deployment, one PRB in LTE spectrum is dedicated for NB-IoT in both the DL and UL. The rest of LTE spectrum is dedicated to non-IoT data transfer.
13. **c**. By introduction of repetitions. NB-IoT neither increases the power transfer, nor changes the frame structure. It uses repetitions to gain 20 dB to reach to the locations with poor radio condition.

Answers to Review Questions

1. The Third Generation Partnership Project (3GPP) is the global technical body which develops technical specifications for mobile communication system. It is not for standardization. 3GPP writes technical specifications, to be transferred into standards by the organizational partners. Therefore, the 3GPP partners are responsible for standard based on technical specifications produced by 3GPP. Overall, we can say that the 3GPP and its partners have made standards for 2G, 3G, 4G and 5G cellular networks.
2. For example, 4G was first introduced in Release-8 and is continued to evolve in higher releases.
3. Global availability of GSM in lower frequency bands of either 850 or 900 MHz band has enabled GSM to provide a good coverage. GSM using a simpler

technology as compared to more advanced generations of cellular network. This means that the price of GSM mobile devices would be cheaper as compared to 3G, 4G and 5G technologies. This also makes GSM an attractive choice for IoT technology.

4. LTE-M has higher data rate, uses larger spectrum, and provides mobility. NB-IoT has lower data rate, uses smaller spectrum, and does not support mobility.

Abbreviations

A

AA Access Address

ACK Acknowledgement

AFH Adaptive Frequency Hopping

ARIB Association of Radio Industries & Businesses

AGV Automated Guided Vehicles

ARQ Automatic Repeat Request

B

BPSK Binary Phase Shift Keying

BLE Bluetooth Low Energy

C

CIOT Cellular Internet of Things

CI Coding Indicator (for Blurtooth 5)

CI Connection Interval (BLE)

CE Coverage Enhancement

CRC Cyclic Redundancy Checks

D

DMRS Demodulation Reference Signals

DETNET DETerministic NETwork

DCI Downlink Control Information

E

ERRI Electric Power Research Institute

EDGE Enhanced Data Rates for GSM Evolution

EtherCAT Ethernet for Controlled Automation Technology

EC-GSM-IoT Extended Coverage GSM Internet of Things

FEC Forward Error Coding

F

FCC Federal Communications Commission

FDD Frequency Division Duplexing

FSK Frequency Shift Keying

G

GPRS General Packet Radio Service

GSM Global System for Mobile Communications

H

HARQ Hybrid Automatic Repeat Request

I

IIOT Industrial Internet of Things

ISM Industrial, Science, and Medicine

IETF Internet Engineering Task Force

IP Internet Protocol

IoT Internet of Things

ISP Internet Service Provider

L

LFSR Linear Feedback Shift Register

LoRa Long Range Radio

LPWAN Low-power Wide Area Network

LTE *Long-Term Evolution*

LTE-M LTE for Machine-Type Communications

M

M2M Machine To Machine

MTC Machine Type Communications

MIB Master Information Block

MNO Mobile Network Operators

MIMO Multiple Input Multiple Output

N

NB-IoT Narrowband Internet of Things

NB-PLC Narrow-Band PLC

NACK Negative Acknowledgement

O

OFDM Frequency Division Multiplexing

P

PCFICH Physical Control Format Indicator Channel

PBCH Physical Downlink Broadcast Channel

PDSCH Physical Downlink Shared Channel

PRACH Physical Random Access Channel

PRB Physical Resource Blocks

PUCCH Physical Uplink Control Channel

PUSCH Physical Uplink Shared Channel

PLC Power Line Communication

PCP priority Code Point

Profinet Process Field Network

PCG Project Coordination Group

PDU Protocol Date Unit

Q

QAM Quadrature Amplitude Modulation

QoS Quality of Service

R

RAN Radio Access Networks

RU Resource Unit

RFID Radio Frequency Identification

S

SA Systems Aspects

SNR Signal-to-Noise Ratio

SRS Sounding Reference Signal

SIG Special Interest Group

T

TSG Technical Specification Groups

TbE TeraBit Ethernet

TDD Time Division duplexing

TSG Technical Specification Groups

TBS Transport Block Size

V

V2X Vehicle-To-Everything

VLAN Virtual Local Area Network

W

WG Working Groups

#

3GPP Third Generation Partnership Project

References

1. Third Generation Partnership Project, Technical Report 36.888 v12.0.0, Study on Provision of Low-cost Machine-Type Communications (MTC) User Equipment (UEs) Based on LTE, 2013.
2. Third Generation Partnership Project, Technical Report 45.820 v13.0.0, Cellular System Support for Ultralow Complexity and Low Throughput Internet of Things, 2016.
3. Third Generation Partnership Project, Technical Specification 23.060 v14.0.0, General Packet Radio Service (GPRS); Service Description; Stage 2, 2016.
4. Third Generation Partnership Project, Technical Specification 24.008 v14.0.0, Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3, 2016.
5. Third Generation Partnership Project, Technical Specification 36.211 v14.0.0, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation, 2016.
6. Third Generation Partnership Project, Technical Specification 36.306 v14.0.0, Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Radio Access Capabilities, 2016.
7. Third Generation Partnership Project, Technical Report 38.913, v14.2.0, Technical Specification Group Radio Access Network; Study on Scenarios and Requirements for Next Generation Access Technologies; (Release 14), March 2017.
8. Third Generation Partnership Project, Technical Specifications 36.331 v13.3.0, Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Radio Resource Control (RRC); Protocol Specification, 2016.
9. Cisco, The Zettabyte Era: Trends and Analysis, Cisco White Paper, 2016.
10. Sigfox, About Sigfox, 2016. Available: http://makers.sigfox.com/.
11. Sigfox, Sigfox Coverage, 2016. Available: http://www.sigfox.com/coverage.
12. LoRa Alliance, LoRa AllianceWide Area Networks for IoT, 2016. Available: https://www.lora-alliance.org/.
13. LoRa Alliance Technical Marketing Workgroup 1.0, LoRaWAN, What Is it?, A Technical Overview of LoRa and LoRaWAN, White Paper, November 2015.

14. E. Dahlman, S. Parkvall, J. Sko¨ld, 4G: LTE/LTE-Advanced for Mobile Broadband, Academic Press, Oxford, 2011.
15. O. Liberg, M. Sundberg, E. Wang, J. Bergman, J.Sachs, "Cellular Internet of Things: Technologies, Standards, and Performance", Academic Press, ISBN: 978-0-12-812458-1, Oct. 2017.
16. GSMA, "IoT Device Connection Efficiency Guidelines" Version 5.0, January 2018.
17. S. Vitturi, C. Zunino and T. Sauter, "Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G," in Proceedings of the IEEE, vol. 107, no. 6, pp. 944-961, June 2019, doi: 10.1109/JPROC.2019.2913443.
18. F. John Dian, R. Vahidnia and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 69200-69211, 2020, doi: 10.1109/ACCESS.2020.2986329.
19. F. J. Dian and R. Vahidnia, "LTE IoT Technology Enhancements and Case Studies," in IEEE Consumer Electronics Magazine, doi: 10.1109/MCE.2020.2986834.
20. F. J. Dian, R. Vahidnia, "Formulation of BLE Throughput Based on Node and Link Parameters," IEEE Canadian journal of Electrical and Computer Engineering, vol. 43, no. 4, pp. 261-272, Fall 2020, doi: 10.1109/CJECE.2020.2968546.
21. F. J. Dian, A. Yousefi, S. Lim, "A practical study on Bluetooth Low energy (BLE) throughput," in IEEE IEMCON, pp. 768-771, Vancouver, Nov. 2018.
22. F. J. Dian, "Low-power Synchronized Multi-channel Data Acquisition Communication System," in IEEE CCWC, pp. 1027-1031, Las Vegas, Jan. 2019.
23. F. J. Dian, A. Yousefi, K. Somaratne , "A study in accuracy of time synchronization of BLE devices using connection-based event," in IEEE IEMCON, pp. 595 – 601, Vancouver, OCT. 2017.
24. F. J. Dian, A. Yousefi, K. Somaratne, "Performance evaluation of time synchronization using current consumption pattern of BLE devices," in IEEE CCWC, pp. 906-910, Las Vegas, Jan. 2018.
25. F. J. Dian, "An analytical scheme for power consumption of battery-operated peripheral BLE nodes," in 9th IEEE CCWC, pp. 1021-1026, Las Vegas, Jan. 2019.
26. F. J. Dian, A. Yousefi, S. Lim, "Time scheduling of central BLE for connection events," in IEEE IEMCON, pp. 763-767, Vancouver, Nov. 2018.
27. A. Yousefi, F. J. Dian, K. Somaratne "Analysis of time synchronization based on current measurement for Bluetooth Low Energy (BLE)," in IEEE IEMCON, pp. 602 – 607, Vancouver, OCT. 2017.
28. K. Somaratne, F. J. Dian, A. Yousefi, "Accuracy analysis of time synchronization

using current consumption pattern of BLE devices," in IEEE CCWC, pp. 841-844, Las Vegas, Jan. 2018.