Degree Thesis, Åland University of Applied Sciences, Bachelor of Information Technology

IoT Communication

- Multiple Ways to Connect Devices from Field

Renate Silina

2024:38

Date of Approval: 2025-01-22
Academic Supervisor: Jonas Waller

EXAMENSARBETE
Högskolan på Åland

Utbildningsprogram:	Informationsteknik
Författare:	Renate Silina
Arbetets namn:	IoT anslutning- flera sätt att ansluta enheter från fältet
Handledare:	Jonas Waller
Uppdragsgivare:	

Abstrakt

I mitt examensarbete skriver jag om IoT-enheter och anslutningsmöjligheter. Jag undersöker och jämför några av de vanligaste IoT-teknologierna. Bakgrunden och mitt syfte är att lära mig om IoT. Undersöka hur IoT-enheter fungerar, hur de är anslutna till internet och vad kan göras med inläst data. Jag kommer också att undersöka och jämföra olika leverantörer för uppkoppling av IoT-enheter.
Mina forskningsfrågor är följande, vad är IoT och hur fungerar det? Vilka är de vanligaste sätten att ansluta sig till IoT-enheter? Vad är IoT-enheter och vad mäter de? Vad kan man göra med enhetsdata? Vilka för- och nackdelar har alternativa metoder för kommunikation? Hur väljer man det bästa alternativet för ett nytt projekt?
Jag kommer att studera några av de mest använda teknologierna för kommunikation med IoT-enheter. Dessa teknologier är LoRa, Sigfox och NB-IoT.
Mitt resultat och slutsats är att det finns många IoT-enheter och tjänster att välja mellan. Ingen teknologi uppfyller alla krav. Allt beror på tillämpning. IoT är gynnsamt för alla sorter av projekt, både på privat- och företagsnivå. Det är en teknik som utvecklas och växer snabbt.

Nyckelord (sökord)

IoT, LoRaWAN, Sigfox, NB-IoT

Högskolans serienummer:	ISSN:	Språk:	Sidantal:
2024:38	1458-1531	Engelska	36

Inlämningsdatum:	Presentationsdatum:	Datum för godkännande:
2024-12-26	2024-12-12	2025-01-22

DEGREE THESIS
Åland University of Applied Sciences

Degree Programme:	Information technology
Author:	Renate Silina
Title:	IoT Connectivity- Multiple Ways to Connect Devices from Field
Academic Supervisor:	Jonas Waller
Commissioned by:	

Abstract

In my thesis I write about IoT devices and connectivity options. I am investigating and comparing some of the most common IoT connectivity technologies.
The background and my purpose is to learn about IoT. How IoT devices work, how they are connected to the internet and what can be done with the data. I will also examine and compare different connectivity providers for IoT devices.
My research questions are as follows; what is IoT and how does it work? Which are the most common ways of connecting with IoT devices? What are IoT devices and what do they measure? What can be done with device data? What pros and cons do the different communication methods have? How to choose the best alternative for a new project?
The three most common communication methods I will be looking at are LoRa, Sigfox and NB-IoT.
My result and conclusion is that there are many IoT devices and services to choose from. There is no overall best way that will stand out. Everything depends on the use case. IoT is beneficial for all kinds of projects, both on private and enterprise level. It is a fast developing and growing technology.

Keywords

IoT, LoRaWAN, Sigfox, NB-IoT

Serial number:	ISSN:	Language:	Number of pages:
2024:38	1458-1531	English	36

Handed in:	Date of presentation:	Approved:
2024-12-26	2024-12-12	2025-01-22

TABLE OF CONTENTS

1. INTRODUCTION

This thesis will cover Internet of Things (IoT), different technologies and device connectivity. IoT device usage is growing rapidly. There is a large variety of devices that are connected through the internet. These devices can be anything from industrial monitoring systems to smart watches on our wrists. Most of us use many such devices every day. My goal is to learn more in detail about IoT device utilization. When it comes to usage of these devices there are quite a few different methods to choose from. All of the methods differ in some ways and are a good fit for different use cases. I will look closer into a few, most common methods of connectivity. I will make a comparison for strengths and weaknesses for these methods. I will also bring up multiple factors that are important when choosing different devices. There are quite a lot of things to consider when searching for devices for any use case. Some significant things are price, energy usage, data transfer rates, range, time consumption and the difficulty level of implementation.

1.1 IoT

IoT stands for Internet of Things. It is a collective term that refers to devices that are connected to the network and are exchanging data with other systems and devices.
These devices are low power devices such as sensors or meters. They are used to measure and control events and other devices in our environment.
IoT has not always been a common trend. It would not be possible without factors like broadband internet and a steady hardware and software production. It was not until in the early 2010 that IoT began to grow in popularity due to high speed internet being more available and reduction in software prices. Some other factors for IoT becoming more common is because people are using more and more devices like smart wearables, smart home appliances and smartphones. IoT devices are often referred to as smart devices to imply that they are able to gather as well as share information. More people are becoming aware of the importance of IoT as it can be used to help increase efficiency and save money for people, businesses and even cities (Mohn, 2024).

Devices like this can be used for a lot of things. To better understand the variety and scale of IoT device usage, it can be divided into a few different areas. One of the areas are devices that are created for consumers. These devices are made for personal usage and make our everyday lives easier. Some examples of these devices are smart home appliances, smart watches, voice assistants and smart home automation devices like lights and security systems. Devices like these are often based on a larger platform supplied by a manufacturer, for example Apple or Google. They provide multiple devices for different types of usage. These devices are connected to one application dedicated for viewing and controlling all of the devices.

Another area for IoT devices is commercial usage for organizations, for example health, transportation and automation. There are a variety of devices designed for medical and healthcare. Health devices can be for example wristbands, blood pressure or heart monitors, pacemakers, and advanced hearing aids. These devices are used to monitor, collect, process,

and alert important health data. For transportation purposes IoT devices can be of help for all kinds of systems. Vehicle control, smart parking, traffic control like digital traffic signs, logistics and toll collection are some examples. Home automation devices can be used for organizational buildings. Energy management systems, mechanical controls, electronic, and security systems.

Industrial IoT devices and applications can be used within manufacturing, construction, agriculture, and maritime. There are devices that are used for smart manufacturing applications. They help automate, control, measure and optimize large-scale manufacturing operations. In agriculture IoT devices and applications are used for monitoring different data on a farm. Soil content and weather conditions are some of many different data measurement examples on a farm. With various sensors on the farm important data can be monitored and viewed remotely. This solution helps lower the costs, increase efficiency and productivity. Another use for IoT devices with sensors are boats and yachts. Important statistics can be remotely observed. For instance batteries and engine rooms for maintenance, also for alarming in case of flooding or fire.

Many things on the infrastructure level are monitored and controlled using IoT devices and applications. Some of the most common ones are bridges, railways, and offshore wind farms. Already connected devices can help with data analytics and better usage overview. IoT solutions are being applied for energy management, environmental monitoring, military systems, and operations. Smart cities are under construction where IoT devices are used in controlling and monitoring both infrastructure and environment (*Internet of Things*, 2024).

However, there are also some concerns regarding IoT. Some of the main issues are security, privacy, cooperation between different services, ethics, and law. The biggest one of these is security as it has a big impact on most of the other concerns. It is a great deal of work to secure IoT communications. Every application layer needs to be secured for an overall protected communication. IoT service providers have come far with securing the communications. As the internet has grown to be a big part of our everyday lives, new threats and ways to attack important and personal data are discovered every day. This makes security a task that constantly needs improving. Another big concern is the environmental impact of Iot devices and systems. One of the main challenges is energy consumption as it increases at a high pace due to continuous expansion of new devices (Kumar et al., 2019).

1.2 IoT system architecture

To get data from a physical IoT device to an end user application requires many steps. This architecture consists of devices, sensors and network gateways. Furthermore, it involves cloud providers, data processing, storage solutions and platforms for user interaction (José, 2023). Depending on the IoT system and its usage purpose the architecture can differ. However, the core-most structure of the different ecosystems is the same. For an architecture to work, there are four layers involved: the devices, communication and data consumption, storage and processing, and applications. These different layers can be seen in figure 1.

Device layer consists of different IoT devices that can sense, measure or control things in the environment. Each device can be used for different purposes. Some can gather environmental data like humidity or sound. Other devices may be used for controlling events in surrounding devices like motion detectors. These devices gather information and transmit it on to servers.

Communication layer is the next layer in the system. It is a network layer that sends the information from the device to the internet via a gateway. Some extra operations are often carried out in this layer, for example additional processing and information resolving. Security parts like authentication, encryption and virus prevention can also be included in this layer. Information from the gateway is sent to the cloud (The IoT Academy, 2023). For this communication to work between all network connected devices a messaging protocol is necessary. This enables devices and computers to understand data and command exchange by defining different rules (Itsekson, 2022). Commonly used protocols for this connection are HTTP/HTTPS, Constrained application protocol (CoAP9) and MQTT.

Next is the data processing and storage layer. This layer processes readings from several sensors. Data for this step is received from gateways and edge devices. Depending on the implementation, this layer can be found inside or outside the gateway (The IoT Academy, 2023). This layer obtains raw data from several sensors, processes and analyzes it using techniques such as machine learning algorithms. This step helps filter out irrelevant data, improves the quality of information and helps decision making (José, 2023). This layer is specifically important for applications with edge analytics when real-time data is vital. Driver assists in vehicles are a good example of this when real-time data is of the utmost importance.

Application layer gets the processed data from the cloud. This layer is hosted in the cloud where end user applications can access it (The IoT Academy, 2023). These user interfaces are built to make the end user experience as smooth and effortless as possible, for example turning on a light by one simple click in the app (José, 2023).

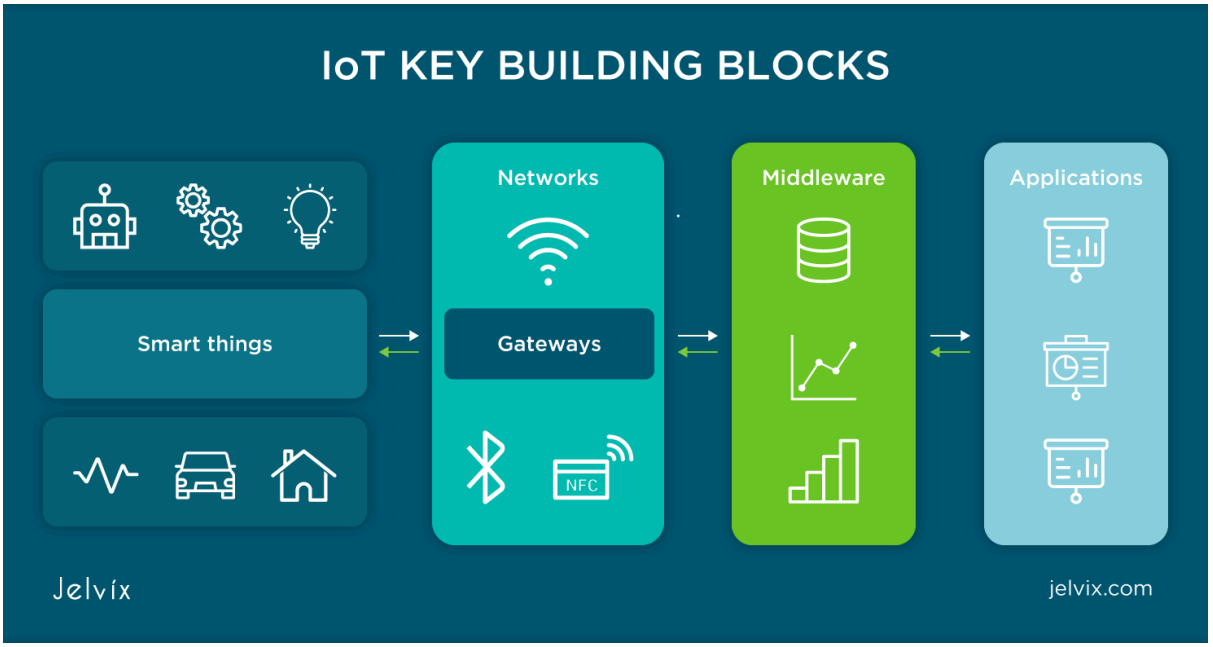

Figure 1. IoT key building blocks (Itsekson, 2022).

1.3 Different IoT solutions

There are multiple types of wireless networks used in IoT solutions. The four main solutions are cellular, Local Area Network (LAN/PAN), Low Power Wide Area Networks (LPWAN) and Mesh Protocols. Each solution is more or less suitable depending on the use case. The

main differences between these wireless networks are data range, power consumption, scalability, costs for connection, and usage. A good overview of these network types can be seen in figure 2.

1.3.1 Local and personal area networks

Local area (LAN) and personal area (PAN) networks are another wireless network solution. Most commonly used solutions that belong to this category are WiFi and bluetooth. Bluetooth requires little power and energy usage. However, it is best suitable for personal and small-scale solutions due to very limited range. Using Wifi the scalability increases, but it contributes to higher power consumption. Use cases that best fit these solutions are smaller scale, in-home and in-building projects. This is the case mainly because of the range deficiency compared to other available solutions.

1.3.2 Low Power Wide Area Networks

Low Power Wide Area Networks (LPWAN) are best solutions for larger scale, wide range use cases with small data size requirements. This category fits well for industrial, scientific, and medical use cases, for example, solutions for smart cities and buildings with temperature, pressure, water monitoring or smart lightning. Methods belonging to low-power wide-area networks are designed to be reliable, secure and power efficient.

1.3.2.1 Cellular LPWAN

Cellular is one widely used method. It is well known because it uses mobile connectivity solutions. Pros of using cellular solutions are good data transfer speeds and long range. The downside of these solutions are often power consumption and battery life. Two of the most popular methods that use cellular networks and can operate in a 4G band are LTE-M and NB-IoT. They are licensed LPWAN technologies which lead to benefits in scalability and service quality.

- LTE-M is a radio technology that reuses LTE installed bases and is optimized for higher bandwidth and mobile connections. It supports low power consumption and great connection density. It is however, compared to NB-IoT, a more expensive solution due to requirements of increased bandwidth and a gateway for communication.

- NB-IoT is a narrowband IoT protocol that uses already established mobile networks. It is low on costs and power consumption and supports a large number of connections. Unlike LTE-M it lacks support for full mobility like voice over network. However, it is cheaper due to lower power consumption and longer battery life. In this case the sensor data is sent directly to a server which erases demand for a gateway.

1.3.2.2 Non-cellular LPWAN

To achieve long range and low power usability the non-cellular LPWAN downgrades bandwidth. The two most popular solutions in this category are SigFox and LoRaWAN. Both of them are well suitable for battery powered IoT devices. Unlike LTE-M and NB-IoT these LPWAN technologies are unlicensed.

- Sigfox uses ultra narrow band (UNB) technology to manage low data transfer speeds and very low energy consumption. The range of device communication with this

technology can be at most 30-50 kilometers which puts it somewhere between wifi and cellular solutions. Sigfox uses industrial, scientific, and medical frequency bands hence no need to obtain licenses.

- LoRaWAN, like Sigfox, is a good alternative for low power and long range communication. LoRaWAN is reaching up to 15 kilometers of coverage and has a 10 year support for battery powered IoT devices.

1.3.3 Mesh protocols

Mesh protocols are an alternative method to communicate with sensors. Unlike above mentioned technologies, data is not transferred directly from each sensor to a central hub. Instead it distributes the communication between sensors to reach the gateway. Mesh protocols are best suited for close range IoT projects such as smart in-building meters and city street light management. Most well known protocols that belong to this category are Zigbee and radio frequency identification (RFID).

- Zigbee uses a mesh network technology allowing each device to pass signals to other devices. Due to this communication technique Zigbee devices can use different vendors while maintaining seamless connection between them. This leads to an increased number of communication paths and eliminates the risk of single-point signal failure. In contrast to LPWAN, it can provide a larger quantity of data transfers while keeping down the power efficiency. Zigbee mesh protocol is available for unlicensed use anywhere in the world which makes it a great solution for mid range IoT projects.

- Radio frequency identification protocol (RFID) uses wireless microchips embedded in IoT devices. Small data amounts are transferred using radio waves. These chips are well suited for measuring and monitoring data to help manage supply chain ecosystems. Example use cases include automated checkouts, warehouse management, security access control, payments, and medical monitoring (Muts, 2023).

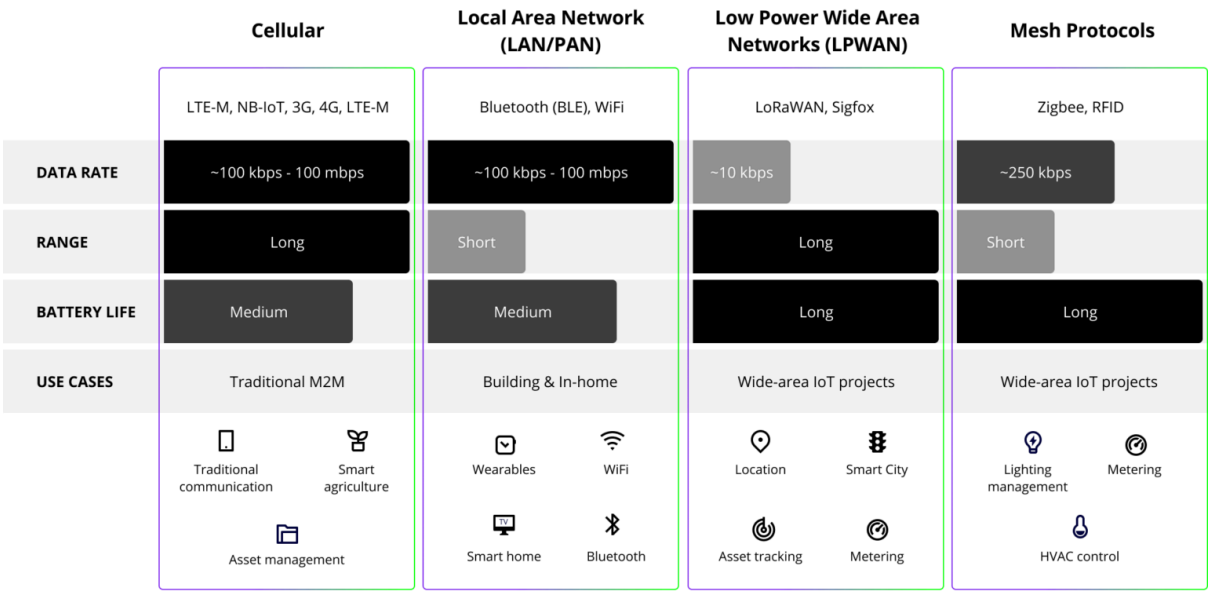

Figure 2. Different types of IoT wireless networks (Muts, 2023).

2. WHAT IS LORAWAN

LoRaWAN is one of the connectivity alternatives for IoT devices. This communications network manages data transmission between gateways and end-node devices to wirelessly connect them to the internet. It uses Low Power Wide Area (LPWA) networking protocol which makes it great for battery powered devices that require low power consumption. It supports long range and can be used to connect devices to the internet in regional, national or even global networks. LoRaWAN offers bi-directional, end-to-end secure communication with great flexibility and localization services (LoRa Alliance, 2020).

LoRaWAN provides multiple network deployment models to suit a variety of different customer types. There are four different models which are private, public, hybrid, and community networks. Private networks can be built when and where desired. They can be set up independent of network operators and other users. This option provides best coverage and complete control of all data traffic. Creating a private network requires setting up a gateway and choosing your own core connection option. If complete privacy is not a demand, it is easier to connect using a public network. In that case connection is made by paying a network operator that has an already existing network set-up. The downside of public networks can be location coverage. If there is a need to cover more range a hybrid network could be a better option. Hybrid networks can move connections between public and private networks to cover a wider range of tracking. There is also a fourth option, community networks. This network model allows connections to existing networks. These connections are created and hosted by other users and shared for public use (LoRa Alliance, 2023).

2.1. LORAWAN technology explanation

Communication is managed through LoRa-modulated radio frequency (RF) messages from an IoT device to a LoRaWAN gateway. These devices are most often battery powered sensors. Gateways receives LoRa messages and forwards them to the network server. Cellular, Wifi, Ethernet, fiber-optic or 2.4 GHz radio links are the network types connecting gateways to network servers. Network servers manage all connections between devices, gateways and applications. Servers has built in security and encryption features for communications. Network servers route downlink messages back to end devices and forward uplink payload data to the application servers. Application servers process the received data and send any created downlink payloads back through the network server. Figure 3 shows the main building blocks for communication flow in LoRaWAN network architecture.

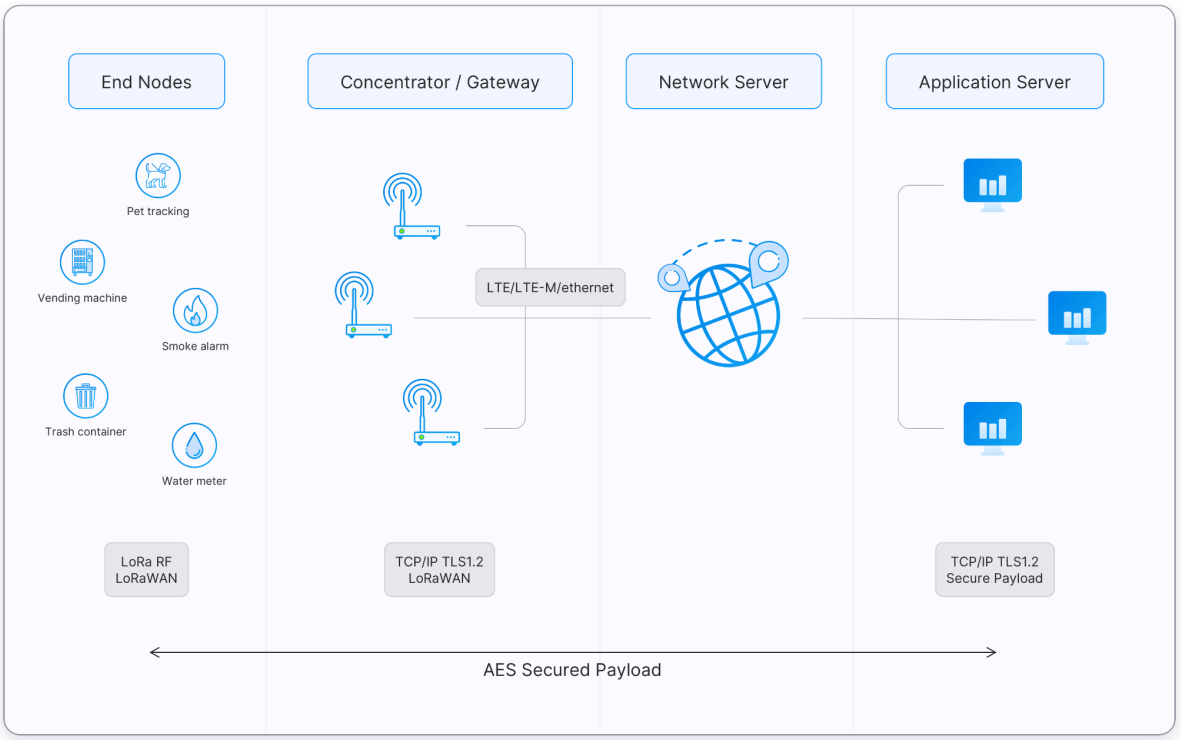

Figure 3. A typical LoRaWAN network architecture (The Things Network, n.d.-b).

LoRa is a wireless modulation technique that codes information on radio waves using Chirp Spread Spectrum (CSS) technology. Spread Spectrum is a technique in telecommunications and radio communications. It spreads a generated signal with a certain bandwidth in the frequency domain over a wider frequency band. Chirp is a spread spectrum technique that uses wideband linear frequency modulated chirp pulses to encode information (*Chirp Spread Spectrum*, 2024). Using this technique ensures that the signal can be received across large distances and is robust against disturbances. LoRa is suitable for sensors that operate in low power mode because it transmits small chunks of data with low bit rates. In comparison to technologies like Wi-Fi or Bluetooth, using LoRa, data can be transmitted at a longer range. LoRaWAN is a top layer of LoRa modulation that defines how devices use the hardware. This top layer is used for changing configurations like the format of the messages and the schedule of the device data transmits (The Things Network, n.d.-d). LoRa and LorWAN together make a networking protocol to wirelessly connect IoT devices to the internet. This protocol is defined as a Low Power Wide Area (LPWA) network (*LoRa*, 2024).

3. WHAT IS SIGFOX

Sigfox is another popular wireless connectivity alternative for IoT devices. Like LoRaWAN, SigFox also uses low power, wide area (LPWAN) networking protocol. Sigfox network is designed for wirelessly connecting sensors and devices to the internet. It is a suitable networking option when energy usage matters, like for battery operated devices and sensors. Choosing Sigfox grants a variety of advantages. Battery in devices lasts for years. No configurations needed makes setting up simple. Every step in the design is optimized to be as cost efficient as possible. Storage is not a problem and communication happens with small notifications. Sigfox is made to be complementary. It is possible to use it together with other network alternatives like Wi-fi, bluetooth, NB-IoT, or LoRaWAN. All benefits combined makes Sigfox a good alternative in large IoT project use cases.

Sigfox's global network is managed by different local network operators. Setting up a device on the network requires a subscription to a local network provider with connection to the network. Subscription grants access to the local network and provides a cloud based service to manage all connected devices. An active subscription also grants support for implementation and troubleshooting.

The most common Sigfox connection model is via public networks. It uses an already established connection by a local network operator. If the desired area is not covered by a public network a connectivity-as-a service option is available. This option helps to extend the range of the network by renting Sigfox base stations and hosting own access points (Sigfox, 2023a).

The Sigfox network is growing in popularity and size. It offers global coverage. As of right now, there are 76 countries with either live coverage or under roll-out development (Sigfox, 2022a).

3.1 Sigfox technology explanation

Sigfox is a wireless network technology for connecting IoT devices, such as sensors, to customers’ end platforms. As shown in figure 4, the communication flows from connected devices to Sigfox base stations. From there the messages get sent to Sigfox cloud platform that distributes them to end customer platforms and web applications. Devices use radio antennas to broadcast information to base stations. Base stations are local antennas that receive messages over the air. They are a part of the public network and listen to all messages sent by active devices in the surrounding area. Base stations are deployed by local operators, usually on high points or towers. They have built in low-noise amplifiers and access points. Amplifiers are used to increase signal and filter noise. Access points are used to receive messages and forward them to the cloud.

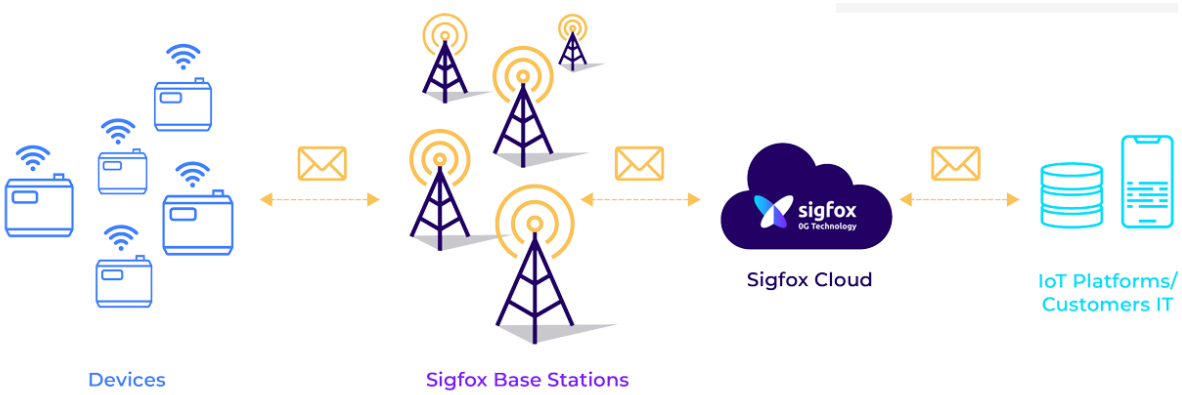

Figure 4. Sigfox communication (Sigfox, 2023a).

Transmitted payloads are little in size, only 12 bytes not including headers (Sigfox, 2023a). Sigfox encodes information from frequency waves using two frequency modulation schemes. These are differential binary phase-shift keying (DBPSK) and Gaussian frequency shift keying (GFSK). The differential binary phase-shift keying is a process that is widely applied for wireless communications such as local area networks, radio frequency identification protocols, and Bluetooth. This process transports data by changing the phase of a constant frequency carrier wave by differing the sine and cosine inputs at a precise time (*Phase-Shift Keying*, 2024). Gaussian frequency shift keying is a filter that reduces interference with other channels. Rather than directly modulating the frequency with the digital data symbols, "instantaneously" changing the frequency at the beginning of each symbol period, Gaussian frequency-shift keying filters the data pulses with a Gaussian filter to make the transmissions smoother (*Frequency-Shift Keying*, 2023). By merging these adjustments appropriate radio frequency bands can be used. Sigfox uses ultra narrowband signals. It requires little energy, can pass through solid objects and is wide-reach. The network protocol used is called Low Power Wide Area network protocol (LPWAN). The use of LPWAN enables long range and low bit rate communication. Sigfox transmissions require a mobile operator or traffic (*Sigfox*, 2023b).

4. WHAT IS NB-IOT

NB-IoT or narrowband internet of things is an alternative way to connect IoT devices to the internet. It is a low-power wide-area network (LPWD) radio technology that operates over existing cellular networks. NB-IoT provides strong security and privacy features integrated from mobile networks covering confidentiality, entity authentication, equipment identification, and data integrity. NB-IoT is suitable for use cases where devices are stationary and have small-scale data transmissions. It offers more channels than LTE or Wi-Fi. It can achieve a longer range than other similar technologies due to extended wavelength. NB-IoT also improves signal travel through obstacles and structures by increased transmission power. Improved signal travel results in much improved indoor coverage. This technology is also optimized for low data usage. Compared to regular 4G LTE networks this solution is more cost effective and beneficial for better end device battery life. However this solution comes with some downsides. Battery power is highly affected if the device is moving. When traveling around more power is demanded in order to stay connected to the mobile network. Power efficiency restricts high data transfer rates leading to no video or voice communication support. Because this technology is relatively new, roaming agreements between mobile network operators are still under construction. Roaming availability affects end devices working range.

This technology is well suited for a variety of use cases. It is widely used for controlling and monitoring different systems. Some general examples are smart metering, lighting, facility management, and environmental monitoring (Narrowband, 2024c).

4.1 NB-IoT technology explanation

NB-IoT uses cellular bands for communication using 180kHz or 200 kHz narrow spectrum frequency bands. It is developed with focus on reliability rather than speed. Latency is ranging from 1,6 to 10 seconds providing transfers with bandwidth up to 250 kbit/s. NB-IoT devices are often referred to as nodes or user equipment (UE). NB-IoT is a half-duplex communication system (Kamal, 2022). In a half-duplex system, communication occurs in one direction at a time. Both devices are able to communicate in both directions but not at the same time. This resembles a walkie-talkie communication, when a user wants to talk a button is first pressed. The button press turns on a transmitter and turns off the receiver. When the sentence is over the button is released. Transmitter is shut down and the receiver is turned back on. Systems of this sort share only one channel for communication in both ways. This approach results in saved bandwidth (*Duplex (telecommunications)*, 2023). The majority of NB-IoT enabled devices use this communication technique to operate. It basically simulates telecommunication operation architecture. When a NB-IoT enabled device has information to transmit it becomes active. It then enters the linked mode (also known as RCC connected). Afterwards it transmits the data and possibly makes more resource requests. The connected time for a device is usually selected and configured beforehand. When the time runs out the device first becomes inactive (also known as RCC idle). Following RCC idle the device eventually disconnects (Kamal, 2022).

NB-IoT offers three different choices for communication. Sharing LTE band with other devices, replacing current deployments using GSM band or using space between LTE channels (Kamal, 2022).

The difference between these communication types is the supported frequency spectrums which can be seen in figure 5. The choice of sharing LTE band with other devices is also known as an in-band deployment. This deployment operates in existing network bands utilizing the same resource blocks as telecommunication carriers. Another operating option is replacing current deployments, also known as standalone deployment type. This type simply uses new bandwidth. The third operating option is sharing the space between channels. This option is known as a guard band deployment. This deployment uses a reserved bandwidth in the guard band of an existing network (RF Wireless World, n.d.). Guard band is an unused frequency band placed between other bands to reduce interference between them.

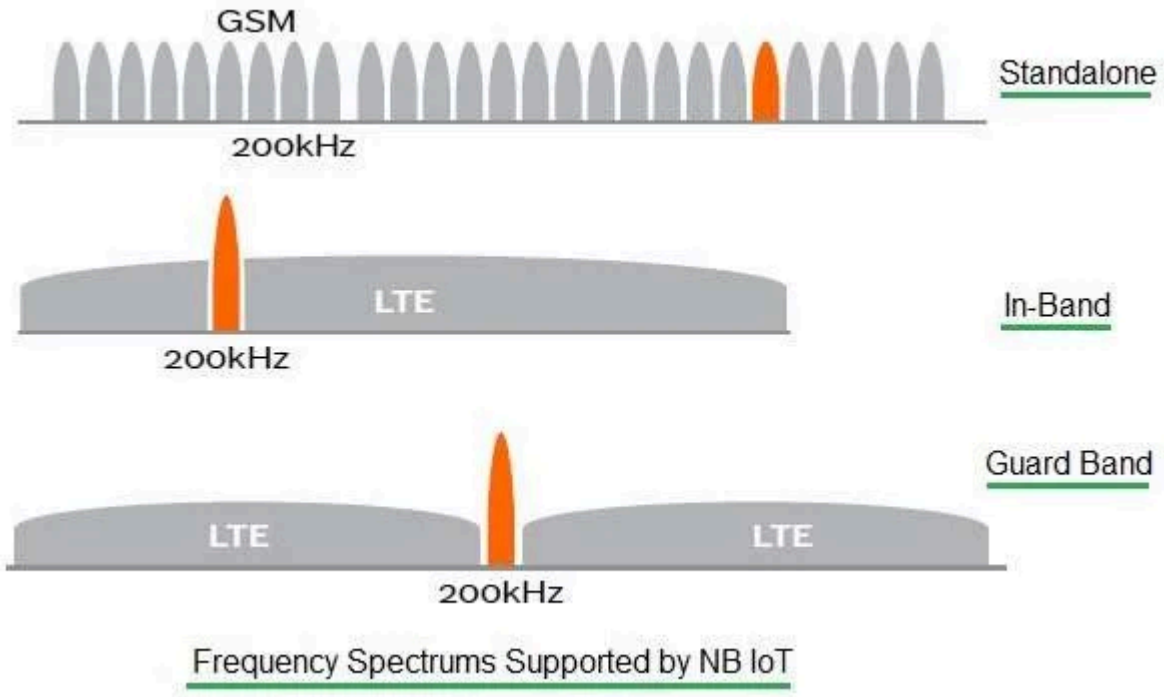

Figure 5. Frequency spectrums supported by NB-IoT (RF Wireless World, n.d.).

5. COMPARING TECHNOLOGIES

The largest and most common IoT technologies right now are LoRaWAN, SigFox and NB-IoT. Some aspects of these technologies are quite similar, but others quite different. Comparing various important operations of these technologies gives a better understanding of how they diversify. Furthermore, it improves the knowledge of what purposes and use cases they benefit most.

5.1 Ecosystems

Ecosystems are important for establishing the availability range of different technologies.

- LoRaWAN, looking at the ecosystem, this technology is managed and developed by LoRa Alliance, an open, non-profit association with over 500 members. It is a secure carrier-grade IoT low power wide area network connectivity. All members collaborate and share experiences to promote and advance the protocol as the leading global open standard (Digita, n.d.).

- NB-IoT technology is managed and developed by the 3rd Generation Partnership Project (3GPP) and GSM, global system for mobile communications, Association. These are two telecommunication standardization associations that aim to improve the benefits of mobile networks and devices (Digita, n.d.).

- Sigfox is another LPWAN technology. It is owned by UnaBiz and managed by local Sigfox operators. It has more than 800 partners that collaborate to provide and commercialize Sigfox technology. This public network relies on the infrastructure deployed through cities and countries by Sigfox local operators (Sigfox, 2023a).

5.2 Frequency spectrum

Frequency spectrum is important when it comes to device communication.

- In frequency range LoRaWAN has a slight advantage. It is optimized for long-range applications that require low power. It operates in a license-free ISM radio band frequency range and is freely accessible to both device manufacturers and network operators (Digita, n.d.).

- NB-IoT uses the frequency range of mobile phone networks. This range is optimized exclusively for frequency efficiency. However, the license fees for using the networks are significantly high, making it affordable for only a few operators (Digita, n.d.).

- Sigfox uses public, unlicensed ISM and SRD frequency bands worldwide. Range as well as radiated power, radio regulations and rules differ between geographical zones. In some zones there might be further specific local regulations and rules for the frequency bands (Sigfox, n.d.-b).

5.3 Coverage and deployment

When it comes to implementation, coverage and availability is important.

- LoRaWAN is currently used by 121 public network operators in 58 countries as well as in numerous private business networks (Digita, n.d.).

- Sigfox operates in more than 70 countries, with more than 11 million devices connected. It is also compatible with other networks (Sigfox, 2022b).

- The GSMA, global system for mobile communications, representing NB-IoT, LTE and other mobile network technologies, has announced that NB-IoT networks are soon expected to be launched in 40 countries (Digita, n.d.).

Furthermore, the installation options for device placement are also of significance.

- LoRaWAN networks offer versatile implementation options. Devices can be installed both indoors and outdoors. Network options are public, private and hybrid. In urban environments signals can penetrate deep inside buildings. In more open, less populated areas a router signal reach can exceed 40 kilometers (Digita, n.d.).

- NB-IoT uses a mobile communication infrastructure. Only network option is public with the requirement to be in range to a mobile network base station tower (Digita, n.d.). NB-IoT can be set up both indoors and outdoors with transmission ranging from one km in urban areas and around 10 km in less populated places ([Amazon Web Services], 2025).

- Sigfox network is public. Devices rely on existing infrastructure. Sigfox uses base stations for connectivity. They also have solutions like renting base stations or getting an SDR dongle in case the area is not yet covered. Sigfox devices can be installed both indoors and outdoors and has a global reach (Sigfox, 2023a). Sigfox's average transmission range is around 10 km in densely populated areas and 40 km in rural areas (Sigfox, n.d.-a).

5.4 Protocol, transmission and reception

Protocols are a set of predetermined rules for connection to the network and transmission of data. A well designed protocol can lead to power gains by optimizing the devices sending and receiving protocols. This is an important aspect for device communication.

- LoRaWAN protocol allows asynchronous, periodical transmission of data, meaning the data is only sent when necessary. This transmission model increases the battery life and reduces costs made by battery replacement (Digita, n.d.).

- NB-IoT on the other hand, requires a synchronous, consistent connection with the mobile network independent of whether there is any data to send or not. This method puts a strain on the battery and therefore increases the costs of replacement (Digita, n.d.).

- Sigfox uses an ultra-narrowband protocol that is designed for small, infrequent data transmissions. This protocol is cost-effective but less suitable in use cases that need higher data rates (Narrowband, 2024a).

5.5 Power utilization for reception and transmission

Protocols play a big part in the resulting operational power needed for the devices.

- Reception current consumption with LoRaWAN technology is on average 5 mA (milliamperes). Transmission operating power is located between 18 mA and 84 mA depending on the transmit level. Overall, both reception and transmission operational power required for LoRaWAN technology is 3-5 times lower compared to NB-IoT and SigFox technologies (Digita, n.d.).

- Compared to these other solutions NB-IoT requires the most power to operate. It consumes an average 110 mA, for device-network communication which happens for tens of seconds at a time. Reception power consumption is around 40 mA. NB-IoT protocol has an overall negative effect on battery life in devices with required service life of 3, 5 or over 10 years. These sensors consume between 100 and 220 mA depending on the transmit power level (Digita, n.d.).

- Sigfox power consumption rate is somewhere between the two mentioned above. This is considering both reception and transmission. Power needed at the reception is around 13 mA. The transmission current consumption can differ considerably between regions. Same Sigfox module consumes around 52 mA in the EU and 230 mA in the US (Libelium, n.d.).

5.6 Data transfer

Depending on the importance of amount and frequency for receiving measurement data this aspect can lead to an easy decision between these technologies.

- The LoRaWAN protocol dynamically adjusts the device's data transfer rate based on the distance from sensor to router resulting in optimized transmission duration and reduced usage of bandwidth. Transmission speed is quite low, reaching a maximum of approximately 50 kbps (Digita, n.d.). Furthermore, consider duty cycle restrictions. Duty cycle specifies when a resource, in this case frequency band, is busy. These limitations are in place mostly due to governmental regulations. In most regions the uplink airtime is set to 1%. If connected to a public network this limitation results in a maximum of 10 messages per day (The Things Network, n.d.-a).

- NB-IoT technologies maximum transfer rate is five times faster, 250 kbps. Therefore, it is beneficial in situations where power is available and application requires a high data transfer rate (Digita, n.d.). Unlike LoRaWAN and Sigfox, NB-IoT has no duty cycle restrictions. This means that there are no daily message limitations (*Narrowband IoT*, 2024).

- Sigfox data transfer rate depends on the region. It can either be 100 bps or 600 bps. Maximum messages per day depends on the device location. Complying with the regional regulations in Europe, for example, allows for 140 messages per day (Sigfox, n.d.-a).

5.7 Moveability

Moveability or transportability sensors are most often used if there is a need to track moving assets.

- LoRaWAN can support such sensors and track their movement from between places. In many use cases sufficient location accuracy can be achieved even without GPS positioning (Digita, n.d.).

- NB-IoT technology is currently a less optimal choice for tracing moving devices. The cause is limitations to cell signal tower reselection in standby mode (Digita, n.d.).

- Sigfox devices support moveability. The network is regionalized and split into six geographical zones. Sigfox offers a feature, named Monarch, which automatically switches between the different geographical zones allowing devices to move easily between them (Sigfox, n.d.-a).

6. ABOUT DEVICES

There are some big differences between devices depending on which technology they are made for. Looking more in depth into devices, their settings, capabilities and connectivity plans is needed for getting a much better understanding about what these devices are and how they work. Below, I have gathered detailed information about one device from SigFox and one from LoRaWAN, both measuring indoor environments, temperature and humidity.

6.1 SigFox AirWits R4.1

SigFox AirWits R4.1			
Size	80x80x27mm	**Sensors**	Sensirion SHT30
Weight	110g	**Environment (operating conditions)**	Temperature 0 to 50C Humidity 0 to 95%
IP rating	IP20	**Radio configurations**	Sigfox RCZ1, RCZ2, RCZ4
Batteries	3xAA 3.6V Lithium, 8100mAh	**Antenna**	Internal helical antenna
Battery life	5 years (30 min measuring interval)	**Communication**	Uplink & Downlink
Humidity range	0 - 95 %	**Temperature range**	0 - 50°C

Default settings for this device are 30 minutes of uplink reporting time, meaning that the device will send the last measurement result every 30 minutes. This device is configured to be in full transmit power.

This device supports downlink messages which are used to change the device configurations. New settings can be applied approximately every 24 hours. There is a possibility to change uplink reporting time and measurement time. Uplink report time is ranging from 10 min to 24h. For device models that are in radio configuration zone 1 (RCZ1), an adaptive power control feature is available. With this feature enabled, the device optimizes transmission power to create less nonessential interference to the radio network and save battery (ManualsLib, 2020).

These configurable settings have a considerable effect on device battery life. Setting measurement and transmission times to shortest possible intervals and with adaptive power mode disabled, the device battery life will be a lot shorter. On the other hand, with measurement and transmission times set to longest intervals and power mode enabled the battery life will extend considerably. Something else to note about the battery life is that

power consumption varies depending on the environment that device is operating in as well as the device settings.

To be able to connect SigFox devices, a subscription needs to be purchased. There are two plans available, discovery and enterprise. Discovery plan fits smaller projects and is limited to 1000 devices. Price is pay per device. There are however more choice options that, if necessary will make the cost higher. These options are a number of messages per day and a location service that does not require GPS, global positioning system. The cost of one device can be between 5,76€ up to 11,01€. This connectivity plan is valid for one year (Sigfox, n.d.-c).

The enterprise plan is better for larger scale projects, supporting more than a 1000 devices. It is priced according to the number of devices with volume based discounts. To enroll in this subscription local IoT connectivity operator needs to be contacted. Enterprise plan offers connectivity ranging from 1 up to 10 years (Sigfox, n.d.-d).

Sigfox has a couple of solutions for connecting, handling and reading the device data. One option is to communicate through api's that users create themselves. The other alternative is to use their FoxerIoT platform. It is a complete all in one online platform that offers simple device management and monitoring. With this platform users can add devices, alter settings, view alerts and readings. FoxerIoT platform includes customizable dashboards and widgets for monitoring alerts and devices (FoxerIoT, 2019). If comparing both solutions, the second option is faster to adapt and easier to use. However, it is far more limited than the first option, custom api communication. With FoxerIoT, unlike custom api, only the dashboard can be shared for viewing outside the user account. FoxerIoT offers only one dashboard in the platform which can become quite overwhelming, hard to navigate and even messy if many devices are used. Furthermore, the platform could use a bit of modernization. In the end it all depends on personal needs and preferences.

6.2 LORAWAN Elsys ERS Lite

LoRaWAN Elsys ERS Lite			
Size	86x86x27mm	**Sensors**	
Weight	80g	**Environment (operating conditions)**	Temperature 0 to 50C Humidity 0 to 85%
IP rating	indoor	**Radio configurations**	EU 863-870
Battey	1xAA 3.6V Lithium, 14505mAh	**Antenna**	-
Battery life	<10 years	**Communication**	Uplink & Downlink
Temperature range	0 to 40C Accuracy +/- 0.2C	**Humidity range**	0 to 100% Accuracy +/- 2%

Range for this device is around 8 km depending on the environment, like building structure and terrain. The device sends information about battery usage. This makes it easier to monitor battery life and know when the battery needs to be changed (Elsys, 2019), (Elsys, 2020).

Default sample time for this device is 1 every 5 minutes. Every reading and sending time can be changed (Elsys, 2024a). LoRaWAN sensors have a spreading factor for better data accuracy. If the signal needs to travel long distances, a higher spreading factor will be best suited and deliver the most accurate data. For short distances a lower factor will perform well. However, the spreading factor also makes a big impact on battery life. The higher the spreading factor, the more power will be required. Another big factor to battery life is sample time. If the device is set to sample and send data often and is located far away, the battery life won't be quite as long lasting (The Things Network, n.d.-c).

The device webpage, Elsys, has a battery calculator for sensor battery life. In the calculator users can enter different settings and see how the choices affect battery life. For example, taking the device above, with all settings left on default with 5 min sample time and highest spreading factor of 12 the battery will drain in little over a year. Doubling the sample time will have an impact and double the battery life time. However the biggest impact comes from the spreading factor (SP) so if sample time is left at 5 min but the SP is set to lowest of 7, the battery will last for well over a decade (Elsys, 2024b).
LoRaWAN devices also require connectivity subscriptions. These plans and prices are provided by the local IoT connectivity supplier that is a member of LoRa alliance.

7. INSTALLING DEVICES

To understand the installation process of IoT devices I have examined the platforms and devices that are set up on school premises. Multiple devices from LoRaWAN and SigFox are set up in school in connection with their previous student projects. Furthermore, I have read through multiple instruction manuals for various devices compatible with previously mentioned technologies. Having done all that, I have got a reasonable perception of how the installation and connection process is done. There are different ways to go about this. Every connection provider has a different set of options for this goal. Below I have done a short walkthrough of installing devices based on what I have learned from the setups at school.

Installing a wireless sensor device is not a particularly difficult task. Before that a device of choice needs to be purchased. Device connection and uptime requires a subscription plan that can be obtained from a provider. One thing to note is that the device needs to be compatible with the chosen technology that a provider offers. For example if the chosen device is LoRaWAN compatible, the connection subscription solution needs to be of the same technology. Data about operators in partnership can most often be found on websites for the different technologies. Otherwise local operators can be contacted for the information. All the IoT connectivity solutions have their own subscriptions and multiple different variations to choose from.

The core principles for IoT device installation are the same between all connection providers but the level of installation difficulty differs between them. The part that is most time consuming is entering all data into the service provider platform. Next step is setting up and connecting various servers needed for the connections. This step is needed when setting up LoRaWAN devices. However, this step is not always required. With some options it can be as easy as entering the sensor code in the platform and the connection goes up. This option is available for SigFox devices with the foxeriot platform.

When the device is connected the next step is to understand and change the device settings as desired. On some devices there are many settings that can be altered. There are also some devices where the opportunity to change the settings can be far more limited. Most common settings these devices have are sample and transmission times. This means that the frequency of readings, how often measurement data is sent and how often the device receives downlink messages can be altered.

Most of the IoT devices are almost maintenance free. However little maintenance can often be needed. There might arise a need to change the reading and sending times. Most of these devices are battery powered so replacement is needed once in a while. Batteries in these devices are often quite special and need to be ordered from the device manufacturers. How often the replacement needs to be done depends on the device type and applied setting configurations.

Making the device data nicely presented and saved might require some work with api’s and creation of servers. This is the case with LoRaWAN devices. The same can be done with SigFox devices but using their complete platform, none of that needs to be done.

As previously mentioned, these are only two of many alternative ways to connect IoT devices. There are many more, even multiple for every different connection provider. Hopefully the number of connection plans will keep increasing to suit as many use cases as possible.

8. CHOOSING THE BEST ALTERNATIVE

Depending on the use case, finding the best wireless sensor device solution can be tricky. There are a lot of things to consider. Importance ranking might be the easiest way to decide on the best fitting solution. In some areas there might arise a need for sacrificing or altering some requirements, while other areas might be more beneficial than required. Listed below are some of the most important parts to think about as well as one, made up**,** suggestion comparison of importance rankings addressing these topics.

- Needs
    - What should be measured
    - Where do the measurements take place
    - Make a list of the most important requirements for the use case. Firstly, requirements that most definitely need to be met. Secondly, those that are more flexible and can be adjusted. Finally, the aspects that are less important. At this point it is good to look at things like
        - Most important measurements
        - Indoor/outdoor
        - Range of data transmission, environment, structures, connectivity points
        - Amount of data per transmission
        - How often does the data collection happen
        - Battery life
        - Future and scalability
        - Importance of the pricing.
- Look into available connectivity options. Compare and rank the different technologies
    - Availability
    - Which fits the needs best, next best and so on
    - Is there and in that case what are the possible compromises
    - Best benefits in some areas.
- Devices
    - Find most suitable devices for the measurement needs
    - Compare different manufacturers
    - Pricing
    - Put this data to previous technology comparisons.
- Compare subscription plans
    - All technologies have different subscription plans.
- Finally choose the best fitting option
    - Making some adjustments
    - Making sacrifices in some areas to make it fit the use case.

The final comparison can look something like this. This is not a real case, only a made up suggestion of comparing the technologies previously discussed in this thesis. Table below shows a comparison between different technology devices that measure movement detection. Yes and No reveals if the requirement is available. Scale 1 to 3 is used to give points depending on how the device matches the desired functionality. For example, first field availability, all of these technologies are available but the closest is a SigFox base station,

which gives the best range and therefore the highest ranking of three points. If the values are identical for all, the same points are given, for example Indoor/Outdoor requirements in the table below.

Needs		LoRaWAN		SigFox		NB-IoT	
Availability and range		Yes	2	Yes	3	Yes	1
What should the device measure	Movement detection	Yes	2	Yes	3	Yes	1
Is multiple measurements desired	Not important	Yes	3	Yes	2	No	1
Coverage indoor or outdoor	Indoor	Yes	1	Yes	1	Yes	1
Type of area and range or communication	Rural <5km	3km	2	10km	3	1km	1
Amount of data per transmission	Only data regarding movement needed	Most measurements, most data per transmission	1	Multiple measurements, more data	2	No	3
Data collection periodicity	2-3	10	1	No restrictions	3	140	2
Battery life length	Multiple years	1,5-10	3	<8	2	<5	1
Scalability	Not important	good	1	good	1	good	1
Pricing	Not important	73-187/device	3	93/device	2	98/device	1
Tot		**19**		**22**		**13**	
Subscription monthly		15	1	9	3	17	2
Final		**20**		**25**		**15**	

9. SENSORS AT SCHOOL

At Åland University Of Applied Sciences many students have done projects with IoT devices. As a result of that, we have sensors that are installed on school premises, measuring multiple different environmental variables. SigFox and LoRaWAN are the technologies that have been chosen in school projects.

9.1 Data collection

I have made a website, shown in figure 8 and 9, to collect all sensor data. The sensor data is collected from SigFox devices that are connected to the foxeriot portal in previous school projects. I have gathered all Sigfox-data measurements in a dashboard, and customized the data displaying charts on the foxeriot platform and included the dashboard in my website. The website also describes the different sensor measurements. This way all the data is collected and presented at one place. It is also easier to look up the meaning of sensor measurements and important thresholds as I have included detailed information about that.

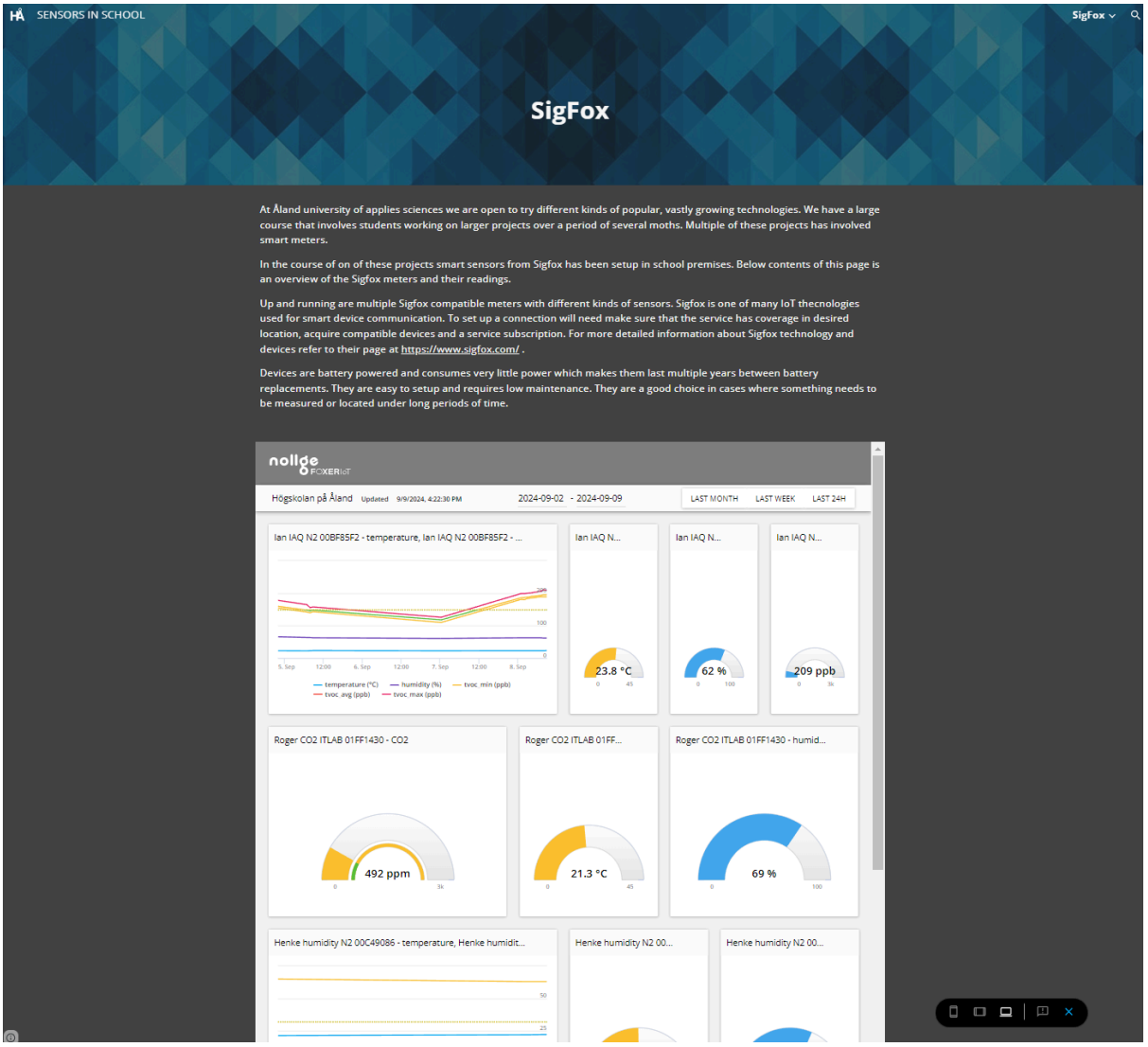

Figure 8. Website with collected sensor data.

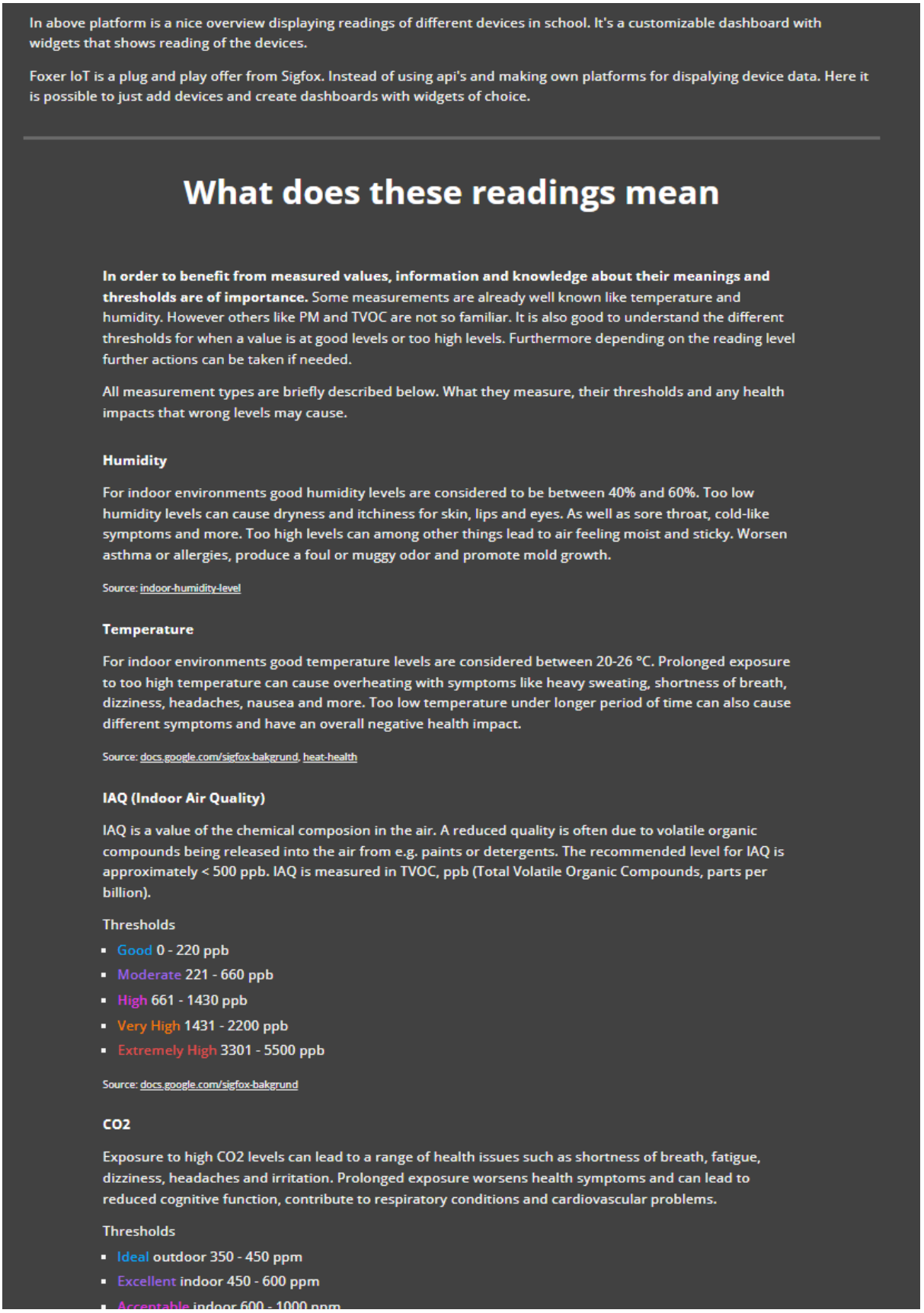

Figure 9. Website with collected sensor data.

9.2 Data analysis

Sensor data in real time is really useful. However, if there is a possibility for logging and storing the data it can be quite beneficial for almost all kinds of use cases. If measurements are stored over longer periods of time they can be analyzed. Many interesting and important conclusions can be made. These analytics can be beneficial to make every day processes more efficient.

The data from SigFox sensors on the foxeriot platform is quite recent. These devices are measuring and sending data once every 24h. The platform also saves sensor measurements starting from when the initial connection is made. For an example of data analysis I have chosen to look at the IAQ, indoor air quality, levels in a classroom over a period of one month. To be able to analyze this data we need to understand what IAQ is and how to read the measurements tvoc_avg (ppb). IAQ stands for indoor air quality. It is measured in Tvoc, ppb which stands for Total Volatile Organic Compounds in parts per billion. A recommended threshold for Tvoc is between 0 - 220 ppb. That means that if the value is rising the air quality is getting worse. When all the measurement values are understood the graph below can be analyzed. Measured data ranges from the beginning of August to the beginning of September. A spike in IAQ is seen at the beginning of September. In August summer break is ongoing and in September school begins again. One possible conclusion to be drawn here is that the reason for the IAQ spike at the beginning of September is due to students being in the classroom again, figure 10.

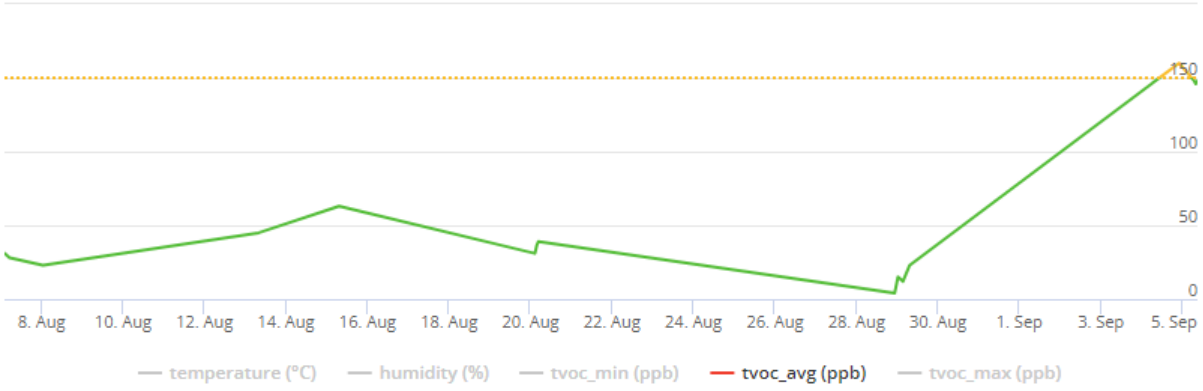

Figure 10. IAQ data measurements over a month.

10. SUMMARY

IoT is a growing concept. There are many IoT devices with all sorts of sensors. There are also many technologies for managing device communication. Providers around the world are offering a variety of connectivity methods. More smart devices are continuously added to the different networks. The most increasing field is different wearables and smart appliances for personal use. However the bigger, more extensive projects with smart measuring devices are not far behind in increasing usage. Projects using IoT devices are a great way to monitor and control events as well as collect and analyze measurement data. They can also be used to increase efficiency and decrease the costs of different processes. These smart devices open up many possibilities. The most difficult part is choosing the best alternative. The rest, like installation, configuration, connectivity, and usage, is very easy. The different connectivity solutions are also growing and expanding the coverage as the device usage and popularity increases. Looking at coverage can be a good summary of how large these technologies have become. Sigfox has live coverage in more than 70 countries and many more countries are under rollout (Sigfox, 2022a). In 2023, LoRaWAN had approximately 200 operators in over 100 countries providing almost world wide coverage (*LoRa*, 2017). Narrowband IoT (NB-IoT) has a coverage in 28 countries of which 99 % has national coverage (Narrowband, 2024b).

The hardest part is finding the sensors. LoRaWAN has the largest, most diverse assortment with many devices having not only one but multiple sensors for different kinds of measurements all in one. SigFox offers are almost satisfactory. NB-IoT has quite a poor device assortment.

Recently a news platform wrote about the Åland Islands planning on adopting IoT devices in the near future. It was really exciting news. The plan is to set up cameras and sensors around the city of Mariehamn. These devices will contribute to the city's development. They will help the technical sector, infrastructure and government to save money as well as make the city more functional for residents. With these devices the city will be able to monitor things like population flows, temperatures, stormwater collection, noise, and many more (Grandell-Sonck, 2024).

Project managers have also thought about safety concerns that people might feel towards many new cameras in town. They have taken extra precautions towards the potential issue and made adjustments. In the article it is stated that there won't be any privacy problems. Camera images will not be saved, people's faces will be blurred. They have also taken precautions to prevent successful attacks into the city's cameras (Grandell-Sonck, 2024).
It is really great to see that more and more places take advantage of IoT for monitoring areas, making improvements for citizens based on the analysis of the gathered data. Furthermore, using the monitored data to increase the effectiveness of different processes and as a result saving money. It is very welcome to see that even the Åland Islands, as of this year, will be following the same path and begin implementing various IoT devices to monitor and improve day-to-day processes.

However, it should not be overlooked that there are still ongoing issues in this area. Energy consumption is a big environmental concern as the number of connected devices is growing

rapidly every day. IoT providers need to address this issue by researching the area and making continuous development for improving the devices to be more economical and energy efficient. There are also other areas of concern regarding the IoT communication. Some of the most important are security, privacy, ethics, and law. There are multiple rules and regulations that need to be met in order to apply regional and worldwide standards. Security and privacy goes hand in hand. There are many building blocks for communication, including authorization and authentication, firmware, software, web applications and transport layer encryption. Securing all of these components can be challenging in order to protect vulnerable data and gain trust in people using these solutions (Kumar et al., 2019).

REFERENCE LIST

[Amazon Web Services]. (2025). *NB-IoT*. https://docs.aws.amazon.com/whitepapers/latest/implementing-lpwan-solutions-with-aws/nb-iot.html

Chirp spread spectrum. (2024, January 10). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Chirp_spread_spectrum&oldid=1194731725

Digita. (n.d.). *10 faktaa LoRaWAN- ja NB-IoT-tekniikasta*. Retrieved September 8, 2024, from https://www.digita.fi/etusivu/palvelut-yrityksille/digitan-iot-palvelut/lorawan-teknologia/10-faktaa-lorawan-ja-nb-iot-tekniikasta/

Duplex (telecommunications). (2023, December 9). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Duplex_(telecommunications)&oldid=1189125500

Elsys. (2019). *Elsys ERS Lite* [Dataset]. https://elsys.se/public/datasheets/ERS_Lite_datasheet.pdf

Elsys. (2020). *Elsys ERS Lite Operating Manual* [Dataset]. https://elsys.se/public/manuals/Operating%20Manual%20ERS%20Lite.pdf

Elsys. (2024a). *Application Settings*. https://www.elsys.se/en/application-settings/

Elsys. (2024b). *Battery life calculator*. https://www.elsys.se/en/battery-life-calculator/

FoxerIoT. (2019). *Features – FoxerIoT*. https://web.foxeriot.com/features/

Frequency-shift keying. (2023, July 25). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Frequency-shift_keying&oldid=1167131761

Grandell-Sonck, H. (2024, September 11). *Snart dyker kameror och sensorer upp i gatubilden i Mariehamn – det här handlar det om*. Ålands Radio & Tv Ab. https://alandsradio.ax/nyheter/snart-dyker-kameror-och-sensorer-gatubilden-mariehamn-har-handlar-om

Internet of things. (2024, February 10). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Internet_of_things&oldid=1205755460

Itsekson, A. (2022, January 30). *What Are the 7 Layers of IoT Architecture? Jelvix*. https://jelvix.com/blog/iot-architecture-layers

José, L. (2023, September 16). *Unpacking IoT architecture: Layers and components explained*. Device Authority Ltd. https://www.deviceauthority.com/blog/unpacking-iot-architecture-layers-and-components-explained/

Kamal, R. (2022, October 10). *Narrowband IoT: What it is and how it works*. Intuz. https://www.intuz.com/blog/narrowband-iot-what-it-is-and-how-it-work

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, *6*(1), 1–21.

Libelium. (n.d.). *Hardware*. Retrieved September 8, 2024, from https://development.libelium.com/sigfox_networking_guide/hardware

LoRa. (2017, January 11). *Wikipedia*. https://en.wikipedia.org/wiki/LoRa

LoRa. (2024, February 14). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=LoRa&oldid=1207270049

LoRa Alliance. (2020, October 21). *What is LoRaWAN®*. https://lora-alliance.org/about-lorawan/

LoRa Alliance. (2023, November 20). *LoRaWAN® Network Options*. https://lora-alliance.org/lorawan-network-options/

ManualsLib. (2020, November 3). *Technical Specification - Connected Inventions AirWits R4.1 User Manual*. https://www.manualslib.com/manual/1910273/Connected-Inventions-Airwits-R4-1.html

Mohn, E. (2024). *Internet of Things. - EBSCO*. Internet of Things. https://research-ebsco-com.ha.idm.oclc.org/c/vxrdyo/viewer/html/u7nfds2opf

Muts, I. (2023, June 6). *4 Types of IoT Networks: Overview & Use Cases*. Euristiq. https://euristiq.com/types-of-iot-networks/

Narrowband. (2024a). *Battle of IoT Protocols: NB-IoT, LoRa, and Sigfox*. https://www.narrowband.com/nb-iot-vs-lora-vs-sigfox

Narrowband. (2024b). *Narrowband-IoT Coverage*. https://www.narrowband.com/nb-iot-coverage

Narrowband. (2024c). *What is Narrowband IoT?* https://www.narrowband.com/what-is-narrowband-iot

Narrowband IoT. (2024, April 1). *Wikipedia*. https://en.wikipedia.org/wiki/Narrowband_IoT

Phase-shift keying. (2024, January 12). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Phase-shift_keying&oldid=1195219489

RF Wireless World. (n.d.). *NB IoT tutorial-features,Spectrum,applications of NB IoT*. Retrieved February 16, 2024, from https://www.rfwireless-world.com/Tutorials/NB-IoT-tutorial.html

Sigfox. (n.d.-a). *Qualification*. Retrieved September 8, 2024, from https://build.sigfox.com/study

Sigfox. (n.d.-b). *Radio Configuration*. Retrieved September 8, 2024, from https://support.sigfox.com/docs/radio-configuration

Sigfox. (n.d.-c). *Subscription, discovery*. Retrieved September 8, 2024, from https://buy.sigfox.com/buy/597f2a8ad0f4ae00015df187/discovery

Sigfox. (n.d.-d). *Subscription, enterprise*. Retrieved September 8, 2024, from https://buy.sigfox.com/buy/597f2a8ad0f4ae00015df187/enterprise

Sigfox. (2022a, October 26). *Coverage*. https://www.sigfox.com/coverage/

Sigfox. (2022b, October 26). *Sigfox 0G Technology by Unabiz*. Sigfox 0G Technology. https://www.sigfox.com/

Sigfox. (2023a, March 27). *What is Sigfox*. https://www.sigfox.com/what-is-sigfox/

Sigfox. (2023b, September 27). *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Sigfox&oldid=1177386783

The IoT Academy. (2023, July 24). *IoT Architecture: Detailed Explanation of the 4 IoT Layers*. https://www.theiotacademy.co/blog/iot-architecture/

The Things Network. (n.d.-a). *Duty Cycle*. Retrieved September 8, 2024, from https://www.thethingsnetwork.org/docs/lorawan/duty-cycle/

The Things Network. (n.d.-b). *LoRaWAN Architecture*. Retrieved February 16, 2024, from

https://www.thethingsnetwork.org/docs/lorawan/architecture/

The Things Network. (n.d.-c). *Spreading Factors*. Retrieved September 8, 2024, from https://www.thethingsnetwork.org/docs/lorawan/spreading-factors/

The Things Network. (n.d.-d). *What are LoRa and LoRaWAN*. Retrieved February 16, 2024, from https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/