Survey of IoT

Smart City of Lappeenranta

A Degree Thesis

Submitted to the Faculty of the

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Ricard Leal Nadal

In partial fulfilment

of the requirements for the degree in

TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING

Advisor: Francesc Moll & Kari Smolander

Barcelona, January 2020

Abstract

The main objective of this project is to carry out a survey of the different Internet of Things data communications that exist at the moment.

It will describe what this new technology consists of and which data communications it has. It is going to be seen how IoT can change people's lives to improve them and make them easier.

The Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

In this project you will also see what are the problems that these new technologies currently host, and you will see how to classify them into groups according to their typology or purpose.

So, this topic would be an attractive idea to be treated since it is about the future and it is always important to keep up with the new technologies.

Acknowledgements

My thanks to all those who have contributed in some way to the development of this work.

First of all, thank the tutors of this work Francesc Moll and Kari Smolander for your dedication and trust me. I am also grateful to have been introduced to the world of research with IoT.

I would also like to make a special mention to all the people with whom I have lived this Erasmus and who has made this work a little easier. From the librarians to my roommate, thank you very much for your help.

Finally thank my family and my friends for being me supporting not only in the months of the project but also during all the years of the degree.

Revision history and approval record

Revision	Date	Purpose
0	23/11/2019	Document creation
1	07/01/2019	Document revision
2	24/01/2019	Final document

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Ricard Leal	rleal1997@gmail.com
Kari Smolander	kari.smolander@lut.fi
Francesc Moll	francesc.moll@upc.edu

Written by:		Reviewed and approved by:	
Date	21/01/2020	Date	25/0172020
Name	Ricard Leal	Name	Kari Smolander
Position	Project Author	Position	Project Supervisor

Table of contents

List of Figures

List of Tables:

1. Introduction

1.1. Context of the thesis

The **Internet of Things** or **IoT** is influencing our lifestyle from the way we react to the way we behave. From air conditioners that you can control with your Smartphone, to Smart Cars providing the shortest route, or your Smartwatch which is tracking your daily activities.

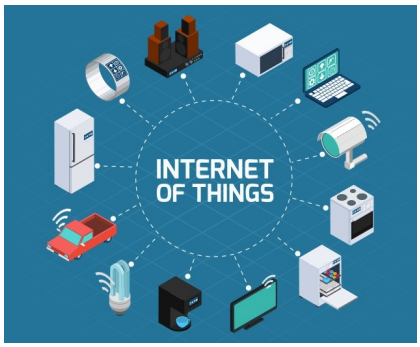

Figure 1. Concept of Internet of Things

IoT is a giant network with connected devices. These devices gather and share data about how they are used and the environment in which they are operated. It's all done using sensors. Those sensors are embedded in every physical device. It can be your mobile phone, electrical appliances, traffic lights and almost everything that you come across in day-to-day life. These sensors continuously emit data about the working state of the devices, but the important question is how they share this huge amount of data? And how do we put this data to our benefit?

IoT provides a common data communication for all these devices to dump their data. And a Common language for all the devices to communicate with each other. Data is emitted from various sensors and sent to IoT data communication security. IoT data communication integrates the collected data from various sources, further analytics is performed on the data and valuable information is extracted as per requirement. Finally, the result is shared with other devices for better user experience, automation and improving efficiencies.

1.2. Objectives

The main objectives of this project are to carry out an information search job. Thus, it will not be so much a practical project, but it will be more theoretical with some practical hypotheses at the end.

So, the principal objectives of this project will be:

- Know, investigate and deepen into an IoT data communications.
- Analyse possible incidents within this technology with a large audience.
- Investigate on the future tendencies of this technology.
- Discover how this technology can change our lives in the future.
- Classify all the types of IoT.

1.3. Requirements and specifications

Project requirements:

- As a main idea of this project, it should analyse and learn all the fields related with IoT and how it works.
- It must be able to analyse all the existing technologies that could currently face IoT.
- It has to understand how this new technology works and in what aspects can improve our quality of life.

Project specifications:

- This project must be understood by any engineer related to telecommunications.

- It will have to be able to clearly see the division of the different data communication of IoT.
- It will appreciate the different outputs that have this type of technology exemplifying each case.

1.4. Work plan

Basically, you can see the entire work plan in the Project Proposal. Being a research work, the time margins established at the beginning of the work have been met.

This project will try to explain the different IoT data communications that exist along with their advantages and disadvantages. In addition, it will show the different examples you can find nowadays and the different uses and how they can improve in the future.

1.4.1. Work Packages

WP#	Short title
1	Internet of Things
2	Definition of each data communication
3	Examples
4	Classification
5	Evolution through the future
6	Smart City
7	Smart City of Lappeenranta

Table 1. Different work packages

2. State of the art of Internet of Things

On this project it will be discussed the basics of Internet of Things, so you are going to get introduced to the different fundamental concepts behind IoT and the basic technologies connectivity devices that are required and an overall understanding about how IoT are made. To do this, first let you get motivated about why IoT is required.

At the present, what you enjoy as internet-based services is basically a connection of different computers and computing devices, so basically this capital is basically a global network or an internet work of different computers and computing devices. Now, what Internet of Things says is that the scope of this internet is going to be expanded, so it is going to be expanded beyond computing and computer devices being connected. It is going to interconnect different things such as physical objects that you can see around. For example, the lighting system in a room, the air conditioners and anything including things such as the toothbrush, the microwave, open the refrigerator, …

Why Internet of Things has become so popular? The reason why IoT has become that important is because is able to provide advanced level of service to the society, to the business and so on advanced levels of services can be offered with the help of IoT technology.

Nowadays IoT is one of the building blocks for the use of developing smart homes and smart cities, not only in our country but throughout the world there is a lot of interest on developing smart cities and smart homes. Thus, IoT is one of the enabling technologies to make the city smart and make the home smart.

IoT is an amazing new paradigm shift that's going on in computers, networking and technology and something that you should really know about and understand. Whenever you're thinking about technology, wherever you're thinking about where you should put your career in technology and where to make money, you should understand that in this business you must go through what are called paradigm shifts, where we start focusing on specific types of technology and basically trying to mine as much money as possible out of that.

Ten years ago, people didn't have personal computers generally and so there was a big wave of installing personal computers in everybody's home and then, it came up Internet, so everybody started using the Internet web pages and it appeared the dot-com boom. Past that, you know into the 2000s we've had things such as convergence that is where you stop having siloed different types of technology and you actually use TCP/IP and Ethernet connectivity for all of your different electronic communications whether it's email and file sharing, or voice over IP and digital surveillance.

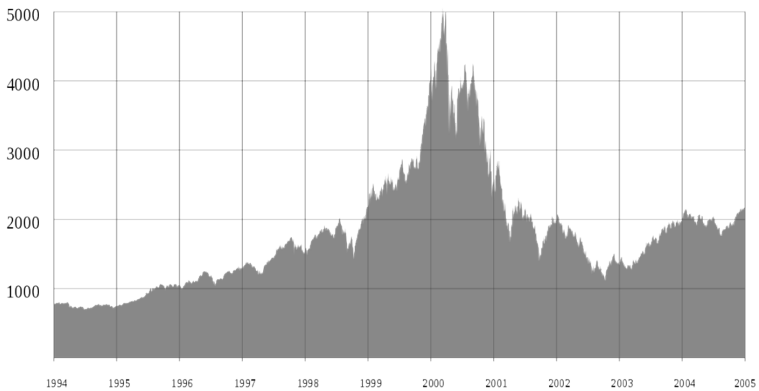

Figure 2. Evolution of the Internet

The basic concept of the Internet of Things is that everything, or almost everything, will be able to be connected in an Internet. What does that really mean? What that means is you know population have gone from computers being able to communicate with a network to such a device that can communicate between them. For example, the Nike Fitbit is actually this little puck thing you put in your running shoe and it tracks how far you run so basically, sends that information up to your iPod or your iPhone and looks at the data that's been sent to it, and figures out things like how many calories you've burnt over an amount of time. So basically, what you are looking at with the Internet of Things is at more and more of these computer type network devices that look less like computers that we would normally think about.

Figure 3. Example of IoT device: "Nike Fitbit"

Internet of Things it is thinking about how everything can be tagged up with some kind of computer readable information and how that data can be sent. So, the question at this moment is how we can put this computer network type device onto almost anything and then what we can do with it.

When talking about the Internet of Things, one of the important concepts here is that computers are not the way that you normally think about computers. When you normally think about computers, you think about monitors, keyboards, mouse, printers, … However, in the Internet of Things you just simply have to start thinking about input/output, so that a keyboard is an input device and a mouse. The output is sending that data out to the outside world.

Figure 4. Input/Output diagram

In Internet of Things the way these little devices communicate may not necessarily be with TCP/IP or wireless Ethernet. It may be through things like RFID (radio frequency ID tags), NFC (Near Field Communication), Bluetooth or other types of these keys wireless communication technologies that are not necessarily Wi-Fi.

Figure 5. Examples of wireless communication technologies (RFID, NFC and BLE)

When you are thinking about this technology you must ask yourself how this works in the real world. All of these little devices are communicating generally back to some kind of base station or controller or detector, and then that is the unit that has TCP/IP and Ethernet built in and then can send the communication off to the servers or out to the internet.

Another important issue when you are talking about IoT is how are these devices going to be powered. The amazing thing with this new type of technology that's being used with the Internet of Things is that they consume very little power so they will last a surprising amount of time. The power consumption of these devices takes much less power than you may realize. You must not only think about the way that they communicate data being different or the way that they collect data being different, but also the way they are powered.

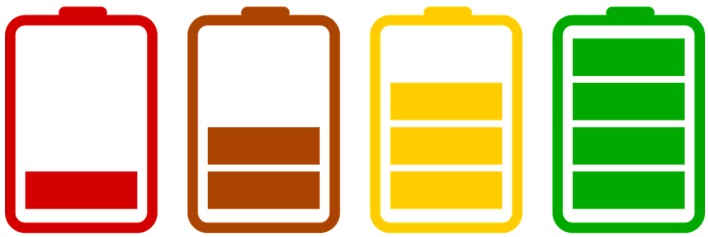

Figure 6. Illustrative power image

In other words, the Internet of Things tries to put computers that can communicate in shoes, to put these devices onto things like milk cartons, … just all kinds of different things that you can do.

This innovative technology is something that you should be thinking about how to deploy either to your business or to your clients with these devices they're becoming more and more inexpensive. There's still a little expensive but they're getting less and less expensive every day, thus it will soon come to the point that basically this communication can be installed into almost anything. when it is manufactured and

That's where all the money is right now, and everything is going through this whole concept of the Internet of Things because this is where a lot of money and a lot of possibility. What IoT is trying to show the people is that imagination is the limit.

2.1. Main characteristics

- Efficient, scalable and associated architecture
- Unambiguous naming and addressing
- Abundance of sleeping nodes, mobile and non-IP devices
- Intermittent connectivity

There are too much characteristics of IoT. So, first of all, IoT must be efficient. It has to serve efficiently the requirements of the applications for which they are deployed. They have to be scalable because in IoT systems, there is a large number of things, it may be working within several billions and trillions of things. So, even if the number of sensors and the sensing devices are going to increase, the overall network performance should not be compromised. So, you know this is a challenge in terms of the network.

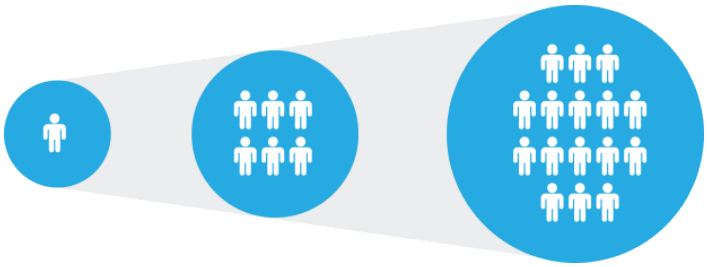

Figure 7. Aggrupation of people thanks to IoT

Moreover, there has to be unambiguous naming and addressing architecture. Thus, all these different devices may have witnessed addressing in the IPV4 context. It must name and address different mechanisms of naming and addressing with the help of IP technology. What is going to happen is, there will be a bigger problem with naming and addressing. So, you need a new mechanism for naming and addressing of the different nodes.

So, another thing is that in terms of the resource requirements, each of these nodes are typically very low power. They have very low resources and they have put to the sleeping mode, so they have to go through a sleep cycle. That means whenever they are not being used, they are not being active. These devices can be mobile, they can move.

So, IP based addressing may not be always very suitable in this sort of scenario. Then, what are the different alternatives? There are different researchers globally who are working on how IoT technology can be a different form of naming in order to support this IoT technology. Intermittent connectivity is another characteristic that is typical of IoT. These devices can be constantly in movement, so they get the network and the subnetworks partitioned. One device which is in connectivity with another device at a later instant of time may not be connected.

Figure 8. No Wi-Fi

2.2. Sensing and actuation

One of the very essential components of Internet of Things is sensors and the other one is actuators. Whereas, the sensors basically sense the physical phenomena that are occurring around them and the actuators are based on the sensed information. The actuators actuate, that means they perform some actions on the physical environment. So, they take some actions based on what has been sensed.

2.2.1. Sensors

A sensor it detects or senses the changes in the ambient conditions, or it can also sense the state of another device. Maybe one sensor can check, can sense how and what is the state of another device.

Here you can see some sensors examples: (obstacle detection, ultrasonic, camera sensor, temp/hum sensor)

Figure 9. Examples of different sensors: obstacle detection, ultrasonic, camera sensor and temperature sensor

The sensors can be classified based on the output where sensors can be analogical or digital, and, based on the data type, where they can be scalar or vector sensors.

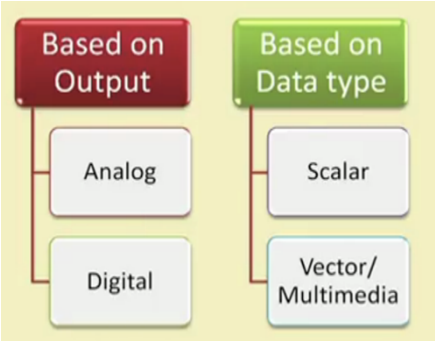

Figure 10. Sensors' classification

Analog sensors produce a continuous output signal or voltage which is generally proportional to the quantity being measured. Physical quantities such as temperature, speed, pressure, … are all analog quantities as they tend to be continuous in nature.

Digital sensors produce discrete digital output signals or voltages that are a digital representation of the quantity being measured. These sensors produce a binary output signal in the form of a logic “1” or a logic “0”. The digital signal only produces discrete values, which may be output as a single “bit”, or by combining the bits to produce a single “byte” output.

Scalar sensors produce output signal or voltage which is generally proportional to the magnitude of the quantity being measured. Physical quantities such as temperature, colour, pressure, … are all scalar quantities as only their magnitude sufficient to convey an information. For example, the temperature of a room can be measured using a thermometer, which responds to temperature changes irrespective of the orientation of the sensor or its direction.

Vector sensors produce output signal or voltage which is generally proportional to the magnitude, direction, as well as the orientation of the quantity being measured. Physical quantities such as sound, image, velocity, acceleration, … are all vector quantities, as only their magnitude is not sufficient to convey the complete information. For example, the acceleration of a body can be measured using an accelerometer, which gives the components of acceleration of the body with respect to the coordinate axes.

2.2.2. Actuators

An actuator is a component of a machine or system that moves or controls the mechanism ort the system. An actuator is the mechanism by which a control system acts upon an environment. So, this requires a control signal and a source energy.

Upon receiving a control signal, the actuator responds by converting the energy into a mechanical motion. The control system can be simple, software-based, a human, or any other input.

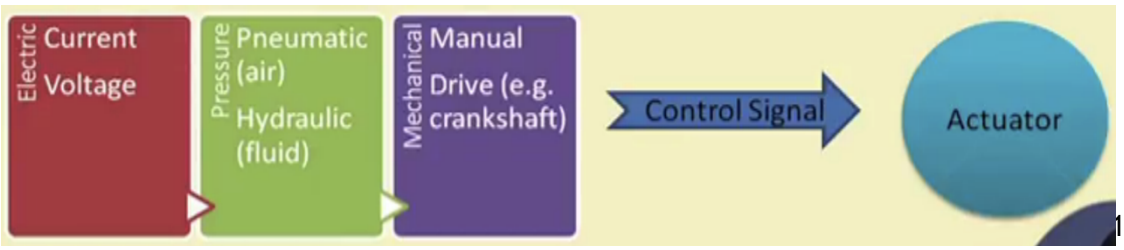

Figure 11. Sensor-actuator diagram

There are many types of actuators. The most important ones, and the ones which could best fit with Internet of Things are:

- **Hydraulic:** a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation.
- **Pneumatic:** converts energy formed by vacuum or compressed air at high pressure into either linear or rotatory motion.
- **Electrical:** powered by a motor that converts electrical energy into mechanical torque.
- **Thermal/Magnetic:** apply thermal or magnetic energy.
- **Mechanical:** converts rotatory motion into linear motion to execute some movement.

2.3. Networking basics

First, it must be said that IoT has evolved too much. When you talk about IoT, if you think about IoT, what do you have? In the form below you can see the IoT components.

Figure 12. Networking basics process

These physical objects are fitted with different sensors and these sensors basically sense different physical phenomena that are occurring around them. These sensors fitted things, sensors actuators and different other emirate devices, are one component of the IoT, however these become different nodes in the network as these are the individual nodes in the network. Now, these nodes need to communicate with other nodes, and the information that is sensed by one of these sensors must be taken and sent to the other sensor nodes, the destination nodes. First, this information has to flow through the local network and then, if the destination is outside from the local network, it must be sent through the internet.

Typically, if you are talking about IoT, the information is going to flow through the internet, or some other wide area network, to the intended destination node. There it may be some analytic engine which is running on some backend server which can run on these servers' decisions about actuation. So, what you can see is that from sensors to actuators, through the local area network to the internet, you will use backend services analytics which includes again some complex algorithms. Basically, IoT will require a very complex system involving sensors, actuators, networks, local area, wide area internet and different servers, different algorithms, machine learning and so on. All must be executed together to make the system work as one single entity.

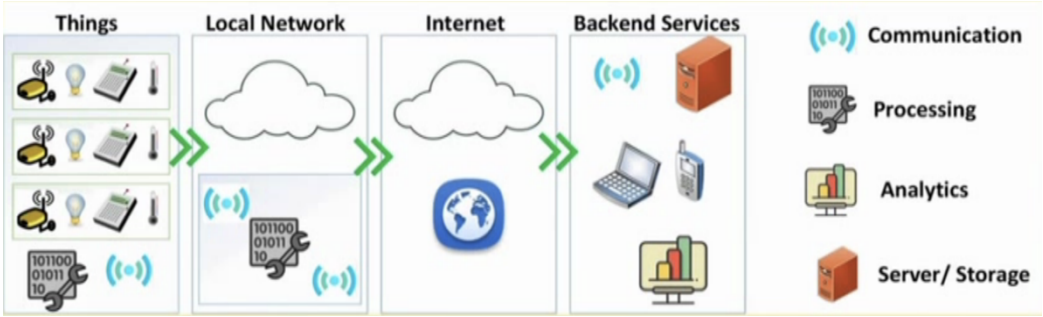

Figure 13. IoT Scenario

So, these are the different basic components of IoT. This is the scenario where IoT works. First you find the different devices that can different physical objects which are fitted with different sensors. These things could be telephones, lightning systems, cameras, sensors, … These things must be able to communicate with another device with the help of wireless technologies like Zigbee, Bluetooth, Wi-Fi and so on. This wireless basically helps the different devices to talk to another one and change information. Then, they will go through a local network and they will go through the internet. After that, in order to analyse all the data proceeded, the backend services will be used, which will involve servers' processors.

2.3.1. Functional components of IoT

- Component for interaction and communication with other IoT devices.
- Component for processing and analysis of operations.
- Component for Internet interaction.
- Components for handling Web services of applications.
- Component to integrate application services.
- User interface to access IoT.

2.3.2. IoT service-oriented architecture

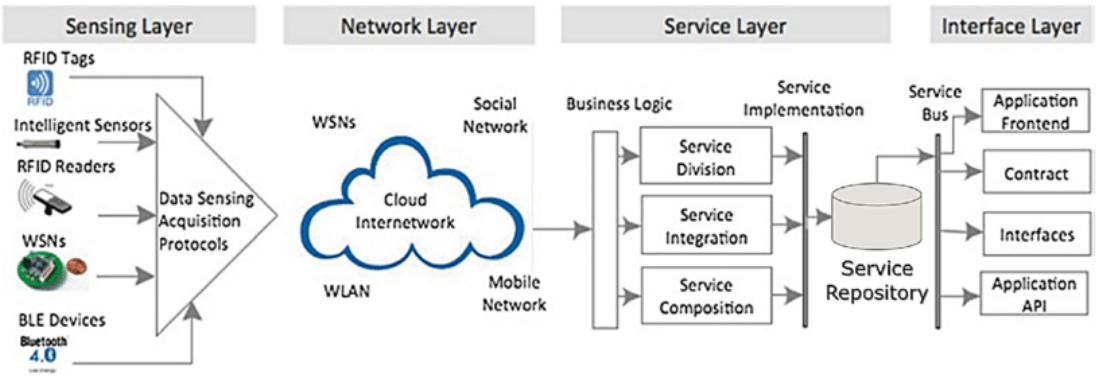

Figure 14. IoT Architecture

Seeing the image above, you can see that the IoT architecture is based on the sensing layer, the network layer, the service layer and the interface layer.

Sensing layer basically takes care of sensing through different RFIF tags sensors which acquire data and is sent to the next layer higher up which is the network layer.

The network layer basically serves sensor networks, social networks and other networks, and data bases interne.

Then, it moves on to the service layer which deals mostly with the service delivery such as service, division service, integration service, repository service and logic by business.

Finally, you can find the interface layer where you have the application frontend, the contract, the interface and the application.

Moreover, there is also a security layer which includes the ones commented before so this layer span all the other ones horizontally.

3. Description of each IoT data communication

The Internet of Things (IoT) starts with connectivity, but since IoT is a widely diverse and multifaceted realm, you certainly cannot find a one-size-fits-all communication solution. There are too many data communications when talking about IoT, but here it will be showed the six most common types of IoT wireless technologies.

Each solution has its strengths and weaknesses in various network criteria and is therefore best suited for different IoT use cases.

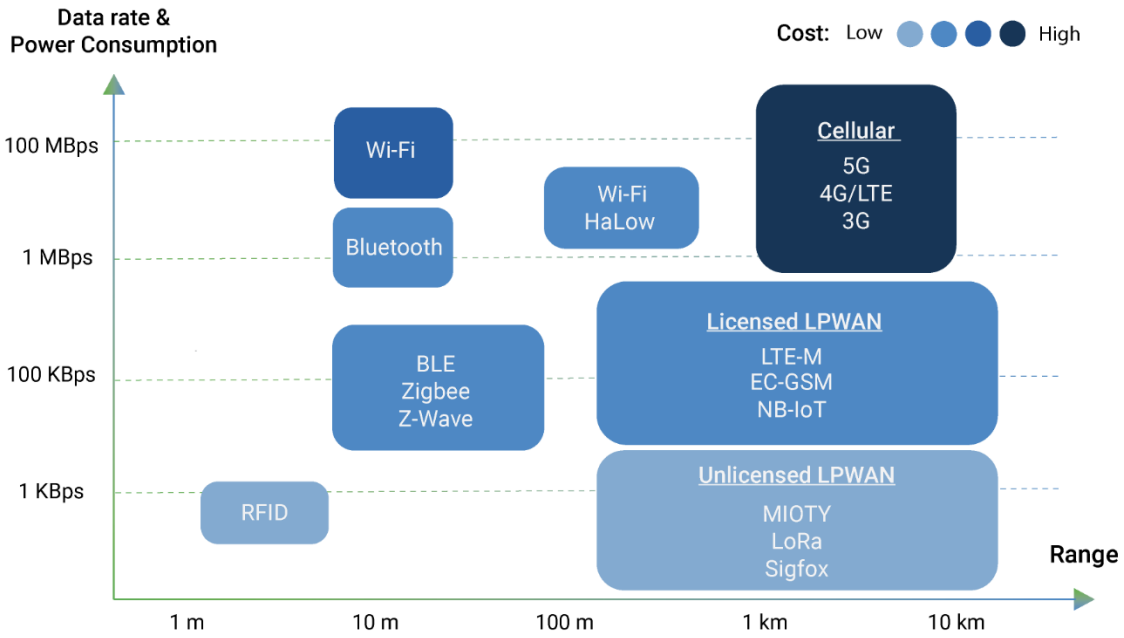

Figure 15. Data rate - Range IoT data communications comparison

In the previous graph, you can see the speed of the data communications and their power consumption compared to the range of distance they can reach. In addition, the cost of each data communication is indicated according to the hue of the colour. Thus, analysing it a little, the Cellular data communication has the highest distance range, the highest power consumption as well and has a very high cost. On the other hand, it can be seen that the cheapest data communications are RFID and Unlicensed LPWAN, where the former has an extremely low distance range while the latter has a much wider range. Then, there is the Zigbee data communication and the Licensed LPWAN which show an average cost and the second one covers a wider range of distances. Finally, there are the Wi-Fi and Bluetooth data communications which show an average cost and a range of distances over the average.

3.1. LPWANs

Low Power Wide Area Networks (LPWANs) are the new phenomenon in IoT. By providing long-range communication on small, inexpensive batteries that last for years, this family of technologies is purpose-built to support large-scale IoT networks sprawling over vast industrial and commercial campuses.

LPWANs can literally connect all types of IoT sensors – facilitating numerous applications from remote monitoring, smart metering and worker safety to building controls and facility management. Nevertheless, LPWANs can only send small blocks of data at a low rate, and therefore are better suited for use cases that don't require high bandwidth and are not time sensitive.

Also, not all LPWANs are created equal. Today, there exist technologies operating in both the licensed (NB-IoT, LTE-M) and unlicensed (e.g. MIOTY, LoRa, Sigfox etc.) spectrum with varying degrees of performance in key network factors. For example, while power consumption is a major issue for cellular-based, licensed LPWANs; Quality-of-Service and scalability are main considerations when adopting unlicensed technologies. Standardization is another important factor to think of if you want to ensure reliability, security, and interoperability in the long run.

3.1.1. How does it work?

The penetration of IoT undoubtedly implies important challenges for the world of monitoring. Initially it is easy to understand that the quantity and heterogeneity of the devices that can be included in an IoT solution implies a challenge for the group that must establish a monitoring data communication that covers said devices.

Theoretically you must consider an infinite number of devices as well as you must assume that most of them are "non-IT" and otherwise diverse from each other. This implies that much of the IT device monitoring scheme will not be applicable to an IoT monitoring project.

On the other hand, there is the fact that there are different schemes and technologies that can be used to develop the IoT project. An IoT project via a cloud service is different if we undertake the project of creating our own IoT network; If our solution points to IoT based on 5G, the scenario is completely different than if we assume an IoT project based on LPWAN. Thus, we are at the point where the lack of standardization in protocols and IoT architecture implies a challenge for monitoring.

However, in the case of LPWAN as the basis for an IoT project, they play against the very fact that they are networks whose communications platform is designed to transmit low volumes of data and that depending on the implementation the communication of the devices it can be unidirectional.

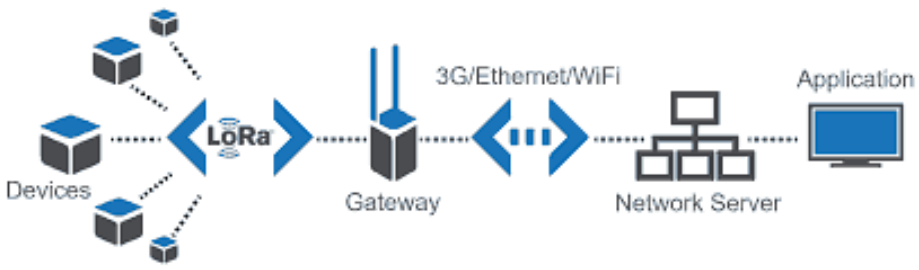

Figure 16. LPWAN diagram process

3.2. Cellular (3G/4G/5G)

Well-established in the consumer mobile market, **cellular networks** offer reliable broadband communication supporting various voice calls and video streaming applications. On the downside, they impose very high operational costs and power requirements.

While cellular networks are not viable for the majority of IoT applications powered by battery-operated sensor networks, they fit well in specific use cases such as connected cars or fleet management in transportation and logistics. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services can all rely on the ubiquitous and high bandwidth cellular connectivity.

Cellular next gen 5G with high-speed mobility support and ultra-low latency is positioned to be the future of autonomous vehicles and augmented reality. 5G is also expected to enable real-time video surveillance for public safety, real-time mobile delivery of medical data sets for connected health, and several time-sensitive industrial automation applications in the future.

3.2.1. How does it work?

In essence, a mobile phone is a receiver-transmitter that receives and sends radio frequency electromagnetic waves. The terminal converts the sound waves of our voice into electromagnetic waves, which travel through the air, being received and forwarded to the recipient of the message through one or more repeating antennas. Once they reach the recipient's phone, they are converted back into sound so that he can hear the message.

Cellular technology requires a large number of base stations to cover the geographic area of a given territory; In a big city there can be hundreds of these stations. Each operator in a given geographical area has a control centre (MTSO), which is responsible for identifying and channelling all telephone connections that occur between users and base stations in that region. A phone call is made following the following steps, which are illustrated in the figure:

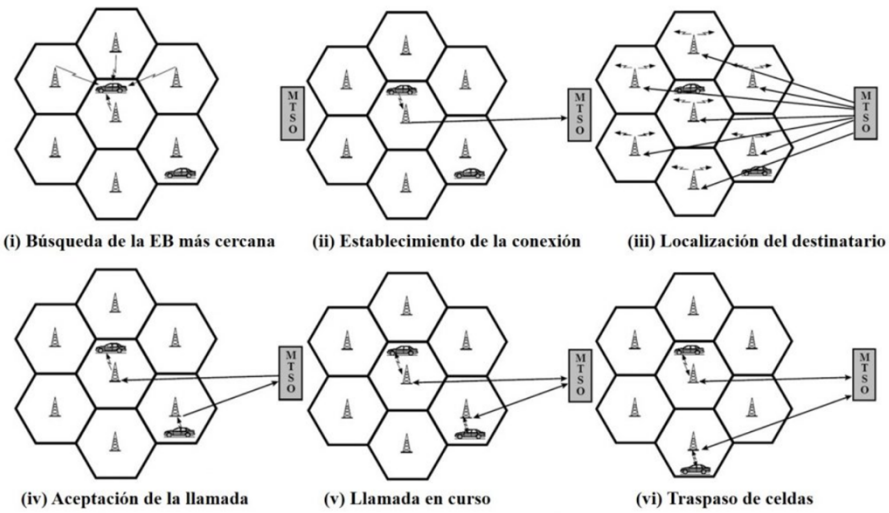

Figure 17. Cellular diagram process

i. When turning on the mobile phone, it searches for a signal to confirm that the service is available. Once it receives it from the nearest base station, the telephone connects to it and transmits certain identification numbers, so that the network verifies data such as the telephone company to which the user is assigned and their telephone number.
ii. Next, the mobile phone sends a message to the base station requesting a connection to the telephone number with which you wish to speak. The message is received by the MTSO that controls the zone.

iii. The MTSO searches for the recipient's phone, sending messages to several base stations. Once the base station closest to the receiving telephone is located, the MTSO accepts the call and decides which of the channels that the telephones can use to communicate is free.
iv. The MTSO establishes the connection between the two telephones, through the base stations to which each one is connected.
v. From that moment, the call is made.
vi. As the user moves inside the cell, the base station will notice that the intensity of the signal emitted by the mobile varies. In the meantime, the base station of the cell towards which it is approaching in its displacement will notice that the signal becomes increasingly intense. The two base stations coordinate with each other through the MTSO and at some point, the phone receives a signal that tells it to change to the frequency of the new station, having moved to another cell. This change (handoff) prevents the conversation between two phones from being interrupted because the signal strength is insufficient.

3.3. Zigbee and other mesh protocols

Zigbee is a short-range, low-power, wireless standard (IEEE 802.15.4), commonly deployed in mesh topology to extend coverage by relaying sensor data over multiple sensor nodes. Compared to LPWAN, Zigbee provides higher data rates, but at the same time, much less power-efficiency due to mesh configuration.

Because of their physical short-range (< 100m), Zigbee and similar mesh protocols (e.g. Z-Wave, Thread etc.) are best-suited for medium-range IoT applications with an even distribution of nodes in close proximity. Typically, Zigbee is a perfect complement to Wi-Fi for various home automation use cases like smart lighting, HVAC controls, security and energy management, etc. – leveraging home sensor networks.

Until the emergence of LPWAN, mesh networks have also been implemented in industrial contexts, supporting several remote monitoring solutions. Nevertheless, they are far from ideal for many industrial facilities that are geographically dispersed, and their theoretical scalability is often inhibited by increasingly complex network setup and management.

3.3.1. How does it work?

A network formed by ZigBee devices can have different topology: star, tree and mesh. Of these three, the most used is the mesh organization. What this topology means is that a ZigBee node can be connected in turn to others over the same network. In this way, communication between all nodes is ensured because there will always be a way to go in case of a fall. Of course, the coordinating node is the one that directs the passage of messages between each node of the mesh.

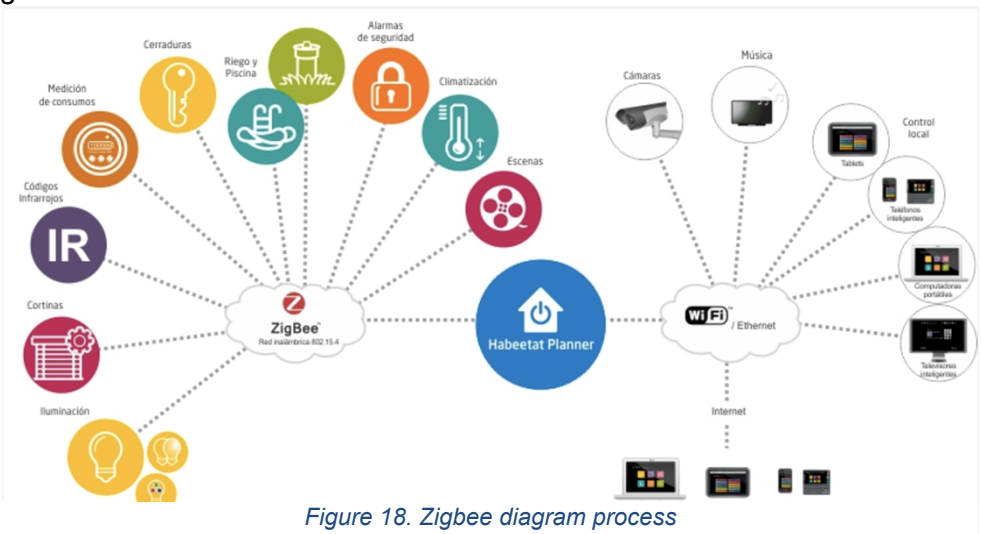

Figure 18. Zigbee diagram process

Speaking of the types of devices, there are three categories of nodes:

- **Zigbee Coordinator:** most complete node and is responsible for controlling the entire network and the paths for its communication
- **Router Zigbee:** interconnects the nodes to be able to execute user code, that is, it offers an application level within the protocol tower
- **Zigbee device:** receives information and communicates only with the parent node

3.4. Bluetooth and BLE

Defined in the category of Wireless Personal Area Networks, **Bluetooth** is a short-range communication well-positioned in the consumer marketplace. The new Bluetooth Low-Energy, also known as Bluetooth Smart, is further optimized for Consumer IoT applications thanks to low power consumption.

BLE-enabled devices are mostly used in conjunction with electronic devices – often smartphones – that serve as a hub for transferring data to the cloud. Nowadays, BLE is widely integrated in fitness and medical wearables (e.g. smartwatches, glucose meters, pulse oximeters etc.) as well as Smart Home devices (e.g. door locks) – whereby data is conveniently communicated to and visualized on smartphones. In retail contexts, BLE can be coupled with beacon technology for enhanced customer services like in-store navigation, personalized promotions, and content delivery.

3.4.1. How does it work?

The Bluetooth network transmits data through low power radio waves. It communicates at a frequency of 2.45 gigahertz (to be exact between 2,402 GHz and 2,480 GHz). This frequency band has been cancelled by international agreement for the use of industrial, scientific and medical devices (ICM).

However, a number of devices have the advantage of being able to use this same frequency band. Baby monitors, garage door monitors and the new generation of wireless phones have made use of frequencies in the ICM band. Having certain that Bluetooth and these other devices do not interfere with the other party that has been crucial to the design of the process.

The low power limits the Bluetooth device to a range of approximately 10 meters (32 feet), eliminating the possibility of interference between your computer system and your home television or telephone. Even with low power, Bluetooth does not need line of sight for devices to communicate with each other. The walls of your house will not stop a Bluetooth signal, making it an appropriate device to control several devices that are in different rooms.

The broad spectrum that transmits automatically is used from each Bluetooth transmitter, so it is unlikely that two transmitters are on the same frequency at the same time. This same technique minimizes the risk that Bluetooth devices, such as cordless phones or

baby monitors, will be interrupted. This is because any interference on a certain frequency will last only a small fraction of a second.

When enabled Bluetooth devices are within the range of another, an electronic conversation takes place to determine if the two have data to share or if one needs to control the other. The user does not have to press a button or give a command - the electronic conversation happens automatically.

Once the conversation has happened, the devices - whether they are part of a computer system or a stereo - form a network. The Bluetooth system creates a network with a personal area or piconet, which can fill a room or may not cover more distance than there is between the mobile phone in your belt and the headset of your head. Once the piconet is established, the members jump frequency, randomly and in unison, so they will remain in contact with each other and avoid other piconets that may be operating in the same room.

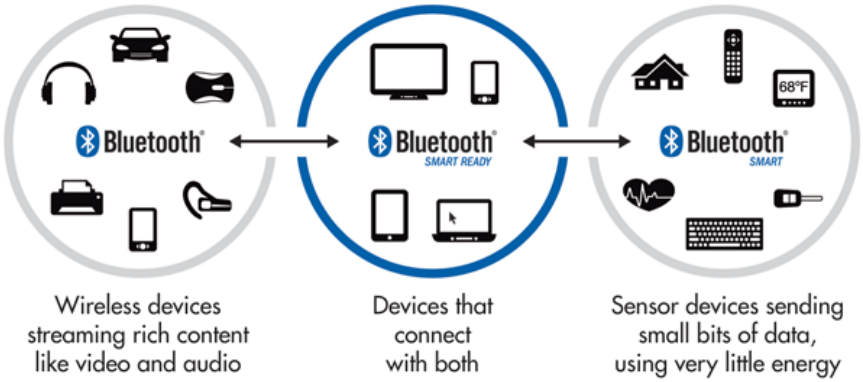

Figure 19. Bluetooth diagram process

3.5. Wi-Fi / Wi-Fi HaLow

There is virtually no need to explain **Wi-Fi** (IEEE 802.11a/b/g/n), given its pervasiveness in both enterprise and home environments. However, in the IoT world, Wi-Fi plays a less significant role.

Except for few applications like digital signages and indoor security cameras, Wi-Fi is not often a feasible solution for connecting IoT end devices because of its major limitations in coverage, scalability and power consumption. Instead, the technology can perform as a back-end network for offloading aggregated data from a central IoT hub to the cloud, especially in the Smart Homes. Critical security issues often hinder its adoption in industrial and commercial use cases.

A new, less known derivative of Wi-Fi – Wi-Fi HaLow (IEEE 802.11ah) – introduces noticeable improvements in range and energy efficiency that cater to a wider array of IoT use cases. Nonetheless, the protocol has received little traction and industry support so far, partly because of its low security. HaLow also operates in the 900 MHz frequency band only available in the USA, making it far from a global solution.

3.5.1. How does it work?

A wireless network (without cables) uses radio waves in the same way as mobile or cell phones, televisions and radios themselves. In fact, communication through a wireless network is very similar to the two radio communication channels. This is what is happening:

1. The **wireless adapter** of a computer translates the data into a radio signal and transmits it using an antenna.
2. A **wireless router** receives the signal and decodes it. The router sends the information to the Internet using a physical, wired, Ethernet connection.

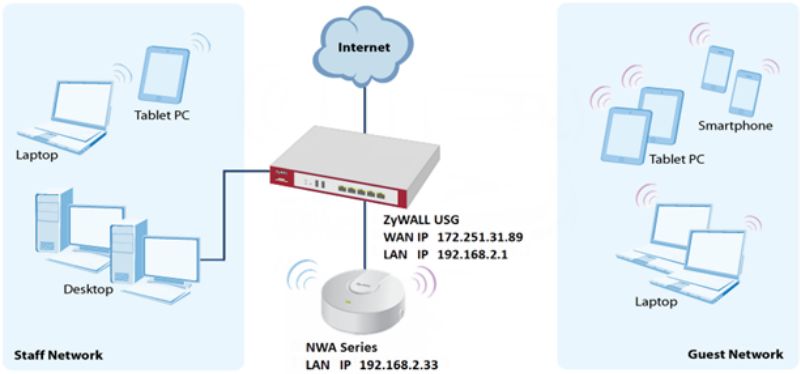

Figure 20. Wi-Fi diagram process

3.6. RFID

Radio Frequency Identification (RFID) uses radio waves to transmit small amounts of data from an RFID tag to a reader within a very short distance. Till now, the technology has facilitated a major revolution in retail and logistics.

By attaching an RFID tag to all sorts of products and equipment, businesses can track their inventory and assets in real-time – allowing for better stock and production planning as well as optimized supply chain management. Alongside increasing IoT adoption, RFID continues to be entrenched in the retail sector, enabling new IoT applications like smart shelves, self-checkout, and smart mirrors.

3.6.1. How does it work?

The reader launches a radio frequency signal through which the RFID tag is activated and emits a response.

The identification code is unique and could even be customized at the time.

Radio frequency communication requires the integration of a radio frequency antenna, the characteristics of which depend on the frequency band in which the system operates.

Currently, RFID systems present in the market usually use the following frequency bands:

- **Band 125 Khz**, the only one used by the old identification cards in the first proximity readers on the market; good reach but low security, you can make a replay attack very easily.
- **Band 13.56 MHz** widely used by other systems in identification and theoretically better application security and to store information in its memory.

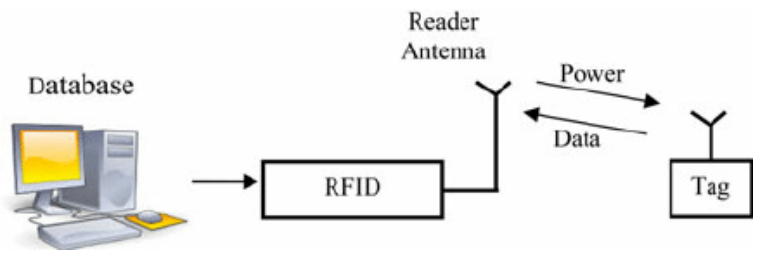

Figure 21. RFID diagram process

4. Classification

So, it seems a good option when it comes to classifying the different data communications, the table below is shown. In this, it can be seen in which sectors it would be very useful to use such data communications, in which they could be used moderately and in which their use is not applied. It will also be used to count the advantages and disadvantages of each of the data communications.

Key IoT Verticals	LPWAN (Star)	Cellular (Star)	Zigbee (Mostly Mesh)	BLE (Star & Mesh)	Wi-Fi (Star & Mesh)	RFID (Point-to-point)
Industrial IoT	●	○	○			
Smart Meter	●					
Smart City	●					
Smart Building	●		○	○		
Smart Home			●	●	●	
Wearables	○			●		
Connected Car					○	
Connected Health		●		●		
Smart Retail		○		●	○	●
Logistics & Asset Tracking	○	●				●
Smart Agriculture	●					

● Highly applicable ○ Moderately applicable

Table 2. IoT data communications classification

To quickly sum up, each IoT vertical and application has its own unique set of network requirements. Choosing the best wireless technology for your IoT use case means accurately weighing criteria in terms of range, bandwidth, QoS, security, power consumption, and network management.

4.1. LPWAN

As you can see in the table above, LPWAN would be very useful for technologies used with considerably large distances due to its range. In this case, you can talk about a Smart City or a Smart Building since they cover a fairly high range of distances.

In the case of LPWAN, we also find different platforms as you can see in the following table. Each provides the same base but with some slightly different details that can be better adjusted to what the customer is looking for.

	SIGFOX	LoRa	clean slate cIoT	NB LTE-M Rel. 13	LTE-M Rel. 12/13	EC-GSM Rel. 13	5G (targets)
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

Table 3. LPWAN models and characteristics

4.1.1. Advantages

There are three technical advantages of LPWAN that match the requirements of IoT. These are:

- **The geographical scope**: LPWAN is designed for wireless data transport between devices separated by distances in the range of kilometres and not meters.
- **The amount of data transmitted:** the idea of LPWAN is to regulate the non-constant transport of small amounts of data.
- **Low power consumption:** the protocol is based on the use of devices whose batteries allow for a duration of years instead of weeks and months.

4.1.2. Disadvantages

The disadvantages that can be pointed out are the following:

- The low transmission speed does not allow handling large volumes of data so elements such as photos and videos are completely discarded. As already mentioned, LPWAN allows the creation of networks of sensors and devices; however, it must be said that even in these networks the volumes of telemetry data that can be transported cannot be very large, which discards very complex elements or from which much information is required.
- There are reports of signal attenuation problems when the LPWAN network includes devices located in buildings or separated by physical elements, operating more efficiently in open spaces with secured sight lines.
- Connectivity between the devices and their application or server it is not constant and can be unidirectional; from the device to a capture element, which hinders activities such as the control of movement of objects in real time. Although, it must be said that most LPWAN implementations allow bi-directional communications.
- Another element with which LPWAN implementations have that fighting is the reliability of transmissions. LPWAN implementations introduce different encryption and authentication processes to resolve this protocol deficiency.

4.2. Cellular

Looking at the first table, it can be seen that the Cellular data communication could best fit with the connected health. So, it could have an important role in the future medicine.

4.2.1. Advantages

Some of the great thing that this option provide to the user are:

- Faster speed: the great 4G LTE connection is that it offers a faster connection to the Internet; it is said to be about 10 times faster than the previous 3G, according to speed tests. The same happens with the speed of loading and unloading of data that can be between 50 and 60 megabytes (the rise) and 150 megabytes per second (the descent).
- The download of complex software and applications is also more agile, reaching over 40 megabytes per second, depending on the location.
- Some online applications gain in sharpness and high definition, so it happens in streaming music, radio, television and videoconferences.

4.2.2. Disadvantages

As always, everything has a coin and the 4G connection was not going to be the exception. Some of its cons are;

- Although one of its initial objectives is to expand the availability of the Internet connection, at least for now, it is a goal that it fails to meet. It is a recent technology that is present in the large cities of a few countries in North America, Europe and South America.
- There is no doubt that the LTE network will be extended more and more, but for now it provides a geographically limited service, so if you leave the covered areas you will be without it.
- On the other hand, the 4G network is compatible only with certain models of devices that integrate an LTE antenna and a chip compatible with it. Of course, you will always have the alternative of getting an LTE router to access this network.
- Battery consumption: it is shown that the 4G LTE network consumes more battery. However, this is offset by the fact that the download speed, which, as it is faster, will spend less energy on other device resources.

4.3. Zigbee

This data communication is very important in smart homes. Its technology allows to be very useful within the same house.

4.3.1. Advantages

The main advantages of Zigbee are:

- Ideal for point to point and point to multipoint connections.
- Designed for information routing and network cooling.
- It operates in the free band of ISM 2.4 GHz for wireless connections.
- Optimal for networks with low data transfer rates.
- Reduces waiting times for sending and receiving packages.
- Provides long battery life.
- Provides secure connections between devices.
- They are cheaper and of simpler construction
- Zigbee has a low level of radiation and therefore can be used in the medical sector.
- Range from 10m to 75m.

4.3.2. Disadvantages

However, the disadvantages of this technology are:

- The transfer rate is very low.
- It only manipulates small texts compared to other technologies.
- Zigbee works so that it cannot be compatible with Bluetooth in all its aspects because they do not have the same transfer rates, nor the same support capability for nodes.
- It has less coverage because it belongs to WPAN type wireless networks.

4.4. BLE

Bluetooth is a communication protocol for technological devices and has its advantages and disadvantages. It is mainly used in cases where the distances are really short, such as in a house or some devices wireless.

4.4.1. Advantages

The advantages of BLE are:

- Eliminates all types of cables because the protocol is by radio frequencies.
- No type of connector is used.
- It is very easy to create a wireless network between several devices to be able to synchronize and exchange information.
- It is completely free to use the service.
- It does not take away too much autonomy to the gadgets that use Bluetooth because it handles little power.
- The speeds are high (24MB / s both).

4.4.2. Disadvantages

Then, this side also has some weak points:

- Security is an unfavourable factor of Bluetooth.
- The reduced scope by the protocol to exchange information is due to the low power it handles.

4.5. Wi-Fi

This technology allows to establish a connection at distances not too large and thanks to a router. Therefore, it is widely used in confined spaces. You can always use amplifiers to have a larger useful area.

4.5.1. Advantages

Having a Wi-Fi connection represents many advantages, such as:

- Wireless connectivity and zero cables.
- The comfort it offers is far superior to wired networks because anyone who has access to the network can connect from different points within a sufficiently wide range of space.
- Choice of several free or secure signals.
- Wi-Fi networks allow access to multiple devices without any problem or expense in infrastructure.

4.5.2. Disadvantages

Each situation of advantages can offer us certain disadvantages, of which some can be mentioned:

- Connection failed.
- Limited distance for signal reception.
- Ease of security hacking.
- Electricity consumption is quite high compared to other standards.

- The Wi-Fi system has a lower speed compared to a wired connection.
- It should be noted that this technology is not compatible with other types of wireless connections such as Bluetooth, GPRS, UMTS and others.

4.6. RFID

Finally, this data communication is characterized by being used in sectors where the range of distances is very low. When it works in its range, it is a technology that works very well.

4.6.1. Advantages

Some of its advantages are:

- Large data storage capacity.
- High accuracy and reliability in the readings.
- They have a long service life.
- High data reading speed.
- Does not require direct line of sight.
- Hard to fake.
- Integration with other control systems.

4.6.2. Disadvantages

However, its main disadvantages can be seen below:

- An RFID system requires the purchase of tags, readers and a software infrastructure which would imply a high cost of material.
- These devices with the use of radio frequency waves could interfere with this data communication.
- RFID tags must be physically attached, injected or not attached to the products they represent, in case of showing any type of damage as they are exposed it would not work properly.
- As RFID systems become less expensive and more sophisticated, privacy issues have surfaced.

5. Evolution through the future

The internet landscape is burgeoning. It's not just about computers, laptops, tablets, and smartphones anymore. Now a multitude of devices are internet-connected. The list of "smart" devices includes washing machines, robotic vacuum cleaners, door locks, toys, and toasters. The Internet of Things is the umbrella term for anything that connects to the internet.

Here you can see how is going to evolve IoT in the next years:

- **By 2025, it is estimated that there will be more than to 21 billion IoT devices**
  A quick look back shows where IoT devices are going. Consider: In 2016, there were more than 4.7 billion things connected to the internet, according to IOT Analytics. Fast-forward to 2021? The market will increase to nearly 11.6 billion IoT devices.
- **Cybercriminals will continue to use IoT devices to facilitate DDoS attacks**
  In 2016, the world was introduced to the first "Internet of Things" malware — a strain of malicious software that can infect connected devices such as DVRs, security cameras, and more.
  What happened next? The malware turned the affected devices into a botnet to facilitate a Distributed Denial of Service (DDoS) attack, which aims to overwhelm websites with internet traffic. The attack ended up flooding one of the largest website hosting companies in the world, bringing a variety of major, well-known websites and services to a halt for hours.
  This particular strain of malware is called "open source," which means the code is available for anyone to modify.
- **More cities will become "smart"**
  Consumers won't be the only ones using IoT devices. Cities and companies will increasingly adopt smart technologies to save time and money.
  That means cities will be able to automate, remotely manage, and collect data through things like visitor kiosks, video camera surveillance systems, bike rental stations, and taxis.
- **Artificial intelligence will continue to become a bigger thing**
  Smart home hubs, thermostats, lighting systems, and even coffee makers collect data on your habits and patterns of usage. When you set up voice-controlled devices, you allow them to record what you say to them and store those recordings in the cloud. In most cases, the data is collected to help facilitate what is called machine learning.
  Machine learning is a type of artificial intelligence that helps computers "learn" without someone having to program them. The computers are programmed in a way that focuses on data that they receive. This new data can then help the machine "learn" what your preferences are and adjust itself accordingly. For instance, when a video website suggests a movie you might like, it's likely learned your preferences based on your past choices.
- **Routers will continue to become more secure and smarter**
  Because most consumer IoT devices reside in the home and can't have security software installed on them, they can be vulnerable to attacks. Why? A lot of manufacturers work to get their IoT products to market quickly, so security may be an afterthought. This is where the home router plays a very important role. The router is essentially the entry point of the internet into your home.
  While many of your connected devices cannot be protected, the router has the ability to provide protection at the entry point. A conventional router provides some security, such as password protection, firewalls, and the ability to configure them to only allow certain devices on your network.
  Router makers will likely continue to seek new ways to boost security.
- **5G Networks will continue to fuel IoT growth**

Major wireless carriers will continue to roll out 5G networks in 2019. 5G — fifth-generation cellular wireless — promises greater speed and the ability connect more smart devices at the same time.
Faster networks mean the data accumulated by your smart devices will be gathered, analysed and managed to a higher degree. That will fuel innovation at companies that make IoT devices and boost consumer demand for new products.

- **Cars will get even smarter**
  The arrival of 5G will shift the auto industry into a higher gear. The development of driverless cars — as well as the connected vehicles already on the road — will benefit from data moving faster.
  You might not think of your car as an Internet of Things device. But new cars will increasingly analyse your data and connect with other IoT devices — including other high-tech vehicles on four wheels.
- **5G's arrival will also open the door to new privacy and security concerns**
  In time, more 5G IoT devices will connect directly to the 5G network than via a Wi-Fi router. This trend will make those devices more vulnerable to direct attack, according to a recent Symantec blog post.
  For home users, it will become more difficult to monitor all IoT devices, because they will bypass a central router.
  On a broader scale, the increased reliance on cloud-based storage will give attackers new targets to attempt to breach.
- **IoT-based DDoS attacks will take on more dangerous forms**
  Botnet-powered distributed denial of service (DDoS) attacks have used infected IoT devices to bring down websites. IoT devices can be used to direct other attacks, according to a Symantec blog post.
  For instance, there may be future attempts to weaponize IoT devices. A possible example would be a nation shutting down home thermostats in an enemy state during a harsh winter.
- **Security and privacy concerns will drive legislation and regulatory activity**
  The increase in IoT devices is just one reason security and privacy concerns are rising.
  In mid-2018, the European Union implemented the General Data Protection Regulation. GDPR has led to similar security and privacy initiatives in several nations around the world. In the United States, California recently passed a tougher privacy law.
  What does this mean for you? Such efforts could give you more control over your data.
- **The devices will be more vocal**
  Electronic devices increasingly have more virtual assistants to help users and give greater freedom of movement. Thus, voice control in smart home devices such as Amazon's Alexa centre or Apple's Siri is increasingly being implemented in more homes and workplaces.

The Internet of Things has opened a world of possibilities not only for consumers, but also for the various industries that have found in this technology an ally to connect all objects with their processes, in the same network. Because of this, business models have been transformed to optimize times and allow data collection, as well as intelligent information analysis.

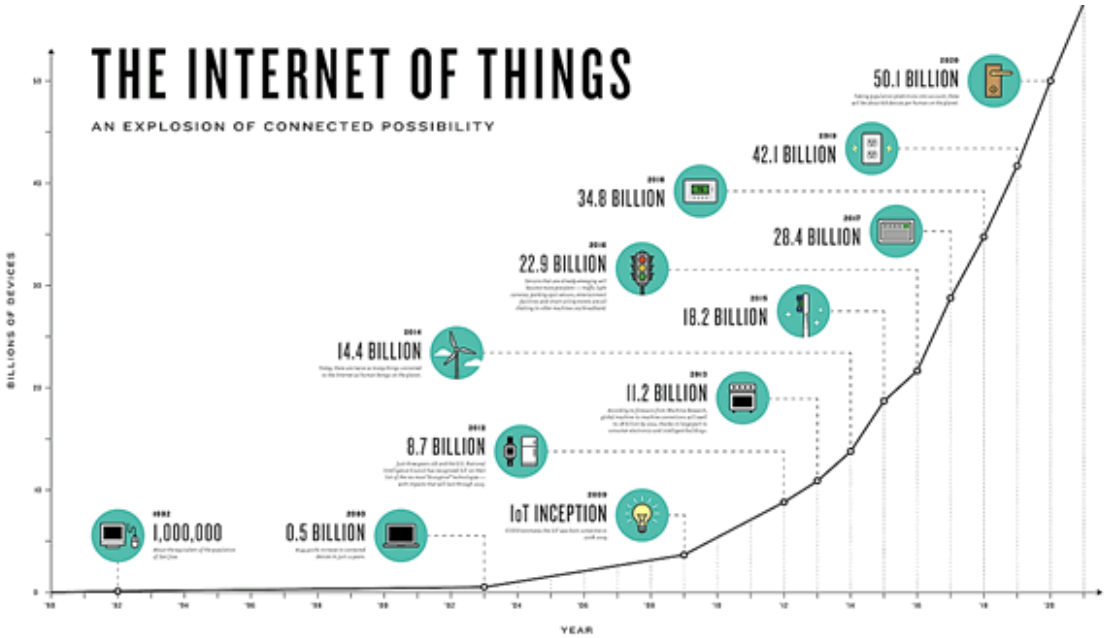

Figure 22. Evolution of devices connected to IoT

Depending on the industry, IoT may affect the following ways:

- For the Health Industry, the Internet of Things will allow doctors to monitor patients 24/7, which will reduce costs and improve patient health because the diagnoses will be 100% personalized. Also, the devices used in hospitals will be connected to the network and will provide large flows of information.
- In the Environment, IoT will play a very important role, because sensors that collect real-time data on temperature, humidity and even the amount of carbon dioxide in the air can be installed. Also, in conjunction with Augmented Reality (AR), it will allow governments to implement technologies that help them protect endangered areas.
- Over the next few years, you will see the number of smart cities grow, as more and more countries are implementing sensors across their entities in order to have a better response time to natural disasters, as well as expedite the transit of citizens through the streets, since the data can avoid road congestion at peak times.

Connecting devices and machinery to obtain relevant data in real time is undoubtedly an imperative of the Digital Economy. As you could see, its potential reaches a great diversity of industries, and it can even be said that it has the potential to completely transform all aspects of people's lives.

6. Smart City

The city of the future is smart. It's entirely interconnected, will regulate traffic, save energy, fight crime assisted by big data and the Internet of Things.

More than half of the world's population lives in cities, and this number is steadily rising resulting in enormous challenges. More people, more traffic, more pollution, more energy consumption, more water usage, more waste, … Smart cities are supposed to help cope with these problems.

In smart cities regular streetlights are replaced by smart poles which connect to other Internet of Things devices and provide broadband. Thanks to driverless cars accidents hardly ever happen. And drones and robots deliver goods even coffee. In this future city salad grows underground at the urban farm. Augmented and virtual reality make processes more efficient. One example is that firefighters on duty can be assisted by the control centre and tech helps to find and correct system errors to prevent damage before it happens.

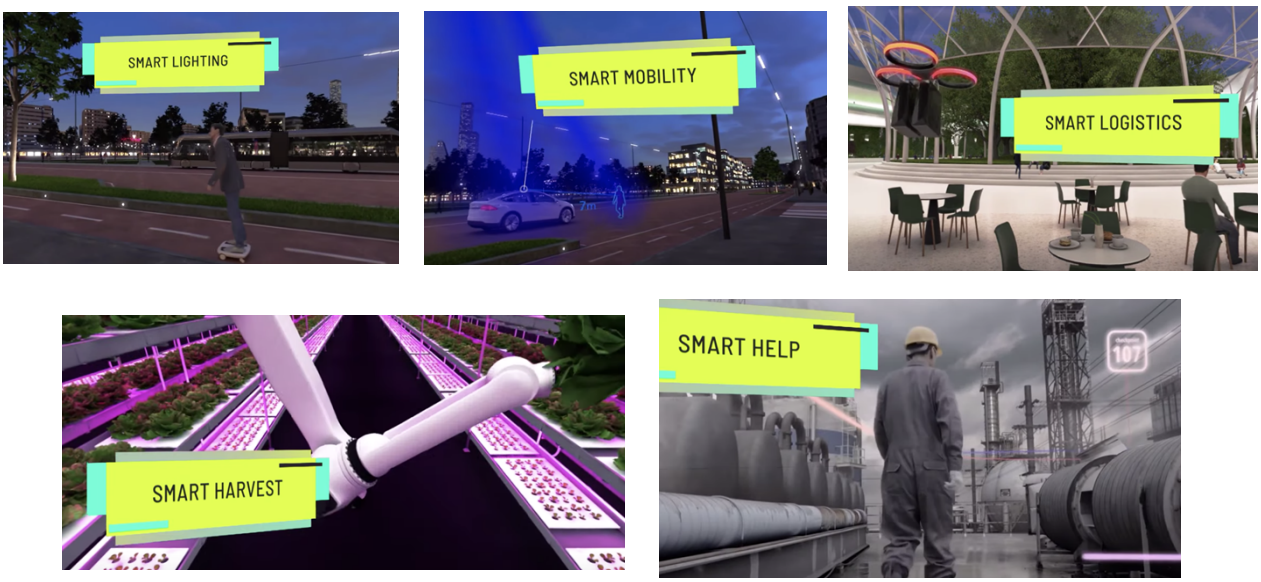

Figure 23. Examples of smart sectors in a Smart City

In order for these ideas to become reality, technical preconditions are essential. A central role falls to the new mobile communication standard 5G. It's the engine for the Internet of Things and enables interconnected infrastructures on a grand scale.

An expert on smart cities is Jonas Böhm. He's a researcher at the Institute for Technology Management at the University of St. Gallen and has published a book with guidelines for cities that want to become smart.

> *"We want to improve people's lives. That's how I would summarize the goal of a smart city. In order to do this, it's important for citizens to be able to properly explain what kind of city they'd like to live in. That's the starting point and we can begin designing a smart city based on those demands."*

For turning your city in a smart one, you'd have to consider the following:

1. make your city interconnected by adding sensors that collect data
2. data needs to be prepared and analysed
3. small solutions for your city can be found

To build a smart city you must do three things:

1. connect devices
2. collect data
3. assess this data to find solution for the citizens

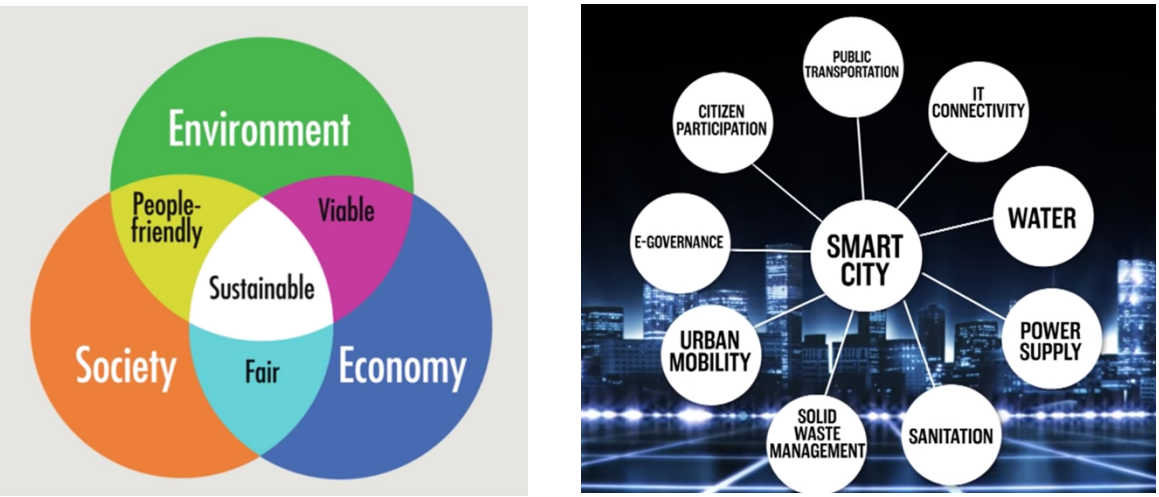

Figure 24. Attributes and summary of a Smart City

In order for these systems to work, vast amounts of data on all citizens are required, but who ensures that the data is safe and who has access to it? different solutions exist

Data is essential for a smart city; it provides the basis for designing intelligent applications for the city. However, what about data protection? To be clear in a smart city there is no protection from data being collected, but on the other hand it's precisely this data that provides the basis for implementing and controlling the city system. As a result, very careful and conscientious decisions need to be made regarding how the data is handled. If the city controls data, this can be advantageous when it comes to data protection, but most cities lack the technical expertise to process and analyse the data. For this reason, many cities cooperate with big tech companies. They have the capacity and the algorithms needed to work with data masses.

A part of privacy, there is another problem. Smart streetlamps, parking lot sensors or garbage bins are connected to the Internet and offer potential gateways for hackers. Theoretically one weak link is all it takes to shut down the city's central servers and cyber terrorists could go even further. Estonia demonstrates how to protect oneself. In terms of digital administration, Estonia leads the way in Europe. Estonians can vote online and almost all public services are digitally accessible, but this also increases vulnerability. In 2007 Estonia was targeted by cyberattacks from a global network of connected BOTS or botnet. Both online banking and government websites were affected. In response, Estonia has implemented annual international training on fighting attacks from hackers.

Cybersecurity is also crucial for smart cities. They are becoming a steadily increasing economic factor, so tech companies use smart cities around the world to test their future technologies. The big question is does this benefit the citizens? Here there are two points of importance:

- who controls the applications?
- who owns the data?

6.1. Actual examples

Which is the benefit from the smart city?

In **Santander** (Spain) the city saves taxes by using resources more efficiently with the help of sensors. Public spaces are only irrigated when they're too dry. Garbage bins are only emptied once they're full.

In **Helsinki** garbage trucks have become obsolete waste is transferred to underground collection points without noise or pollution.

In **Rio de Janeiro** a smartphone app is enabling residents to shape their surroundings. The app smart favela creates a three-dimensional avatar of the shanty towns. When city planners come up with new ideas, these can be looked at on the app and then citizens can vote on them.

In **Palo Alto**, in the US, parking lots now have sensors. These notify citizens whenever a parking space is free. The city's traffic is constantly recorded.

Smart robot cops are supposed to make **Dubai** safer. The police robots are equipped with cameras and can find persons through facial recognition tech. Reports can be filed on a touchpad.

Figure 25. Example of Robot Cops in Dubai

In **Rehoboth** (Ukraine) citizens can view the incomes of civil servants and check on how politicians have voted in the City Council. City owned businesses lay bare their accounts using open data in the fight against corruption.

In **Darmstadt** (Germany) interconnected sensors assess the air quality and send this information to a data centre which analyses air pollution and if necessary, reports bad air quality

7. Smart City of Lappeenranta

This project will also try to show some ideas that could be applied in the city of Lappeenranta so that it can be converted into a Smart City.

Lappeenranta is a city in Finland on the shores of Lake Saimaa, the largest in Finland, in the southeast of the country, about 30 km from the Russian border. This city is characterized by its cold weather and the few hours of sunshine there is. So, the biggest problems that can appear in this city are the heavy winter snowfall, and the ice.

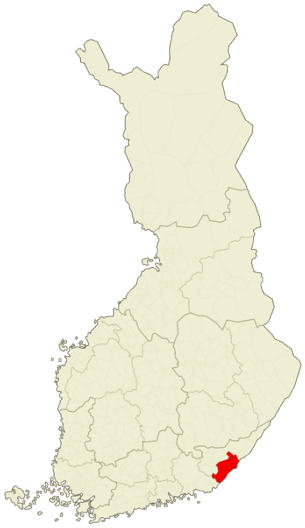

Figure 26. Lappeenranta location in Finland

In order to turn this small city into a Smart City, this project wants to show some ideas that could help to futurize it and thus make Lappeenranta a city with many more comforts and in accordance with sustainability and minimum energy consumption.

In the first place, it has been thought that a good measure to reduce electricity consumption would be to activate sensors in streetlights. These sensors would detect that from a certain percentage of darkness the lights should come on. As Finland has a few hours of sun, these sensors would enable the lights to be activated without the need for someone to program the hours. It should be taken into account that on cloudy days there is sometimes little light, but it still looks enough. Therefore, these sensors would have to be programmed correctly.

Another measure would be garbage collection. In this city the containers are inside small houses. Then some sensors should be placed inside the containers that they would detect when they are full. In addition, since they are inside a small house, a small screen could be placed at the entrance to show the level of fullness of each container. Thus, the citizen only when entering would already know where he could throw the garbage and would be a time saver. Once the containers are full, the pickup truck could make the most optimal route in the city to pick up the trash.

In addition, roads should have sensors to detect if they are frozen or snowy. In this way, from a certain level of freezing or snow, a warning could be sent to the central control system to pass the snowblower, or to warn that there is enough ice for the vehicles to put the skewers on the wheels for everyone's safety.

Figure 27. Skewers on the wheels when there is snow

Related to the above, when sending this warning of ice or snow to the central, all vehicles (buses, cars, vans, ...) could be linked to the central and in this way activate a system of autocolocation of skewers. For this, the wheels should already be prepared so that with the press of a single button the spikes come out. With this, it would greatly increase the quality and life safety of citizens and would be much more comfortable for everyone.

Following the issue of cars, another important factor would be to apply an antifreeze system. In this city it is very easy to wake up with all the snow or frozen cars, and it is very heavy

to have to remove the snow from your vehicle every morning. For this reason, thanks to the snow and ice detection sensors discussed above, from the plant, a warning could be sent to all vehicles to activate a body heating system so that, every day upon waking they will find the vehicles in perfect condition to go to work.

Moreover, this city is also characterized by the possession of the second largest lake in Europe. So, this is of vital importance in the city. A sensor should be applied to know the thickness of ice in the lake. In this way, you could know when it would be possible to ride on it or even drive with your car to shorten the routes. For that, it would only be necessary to activate a traffic light at the entrance of the lake which would be green when the thickness of the lake was large enough to be safe to drive with the car.

Finally, there is the use of the bus. This is widely used in Lappeenranta, since the distances if you are not in the centre are relatively long so either you have a car, or you have to use a bus. At the moment, there is already a web page which tells you when the buses pass at each stop. Although this application is quite correct, it often fails at the time of arrival either because the bus has advanced, or in the most common case, has been delayed. And who likes to be waiting for the bus at -10ºC? Therefore, each bus should have a geolocable chip so that in the application you could see where your bus is. Therefore, each person could interpret at what time they have to leave the house depending on where the bus passed, and they could not blame the application for being cold in the street.

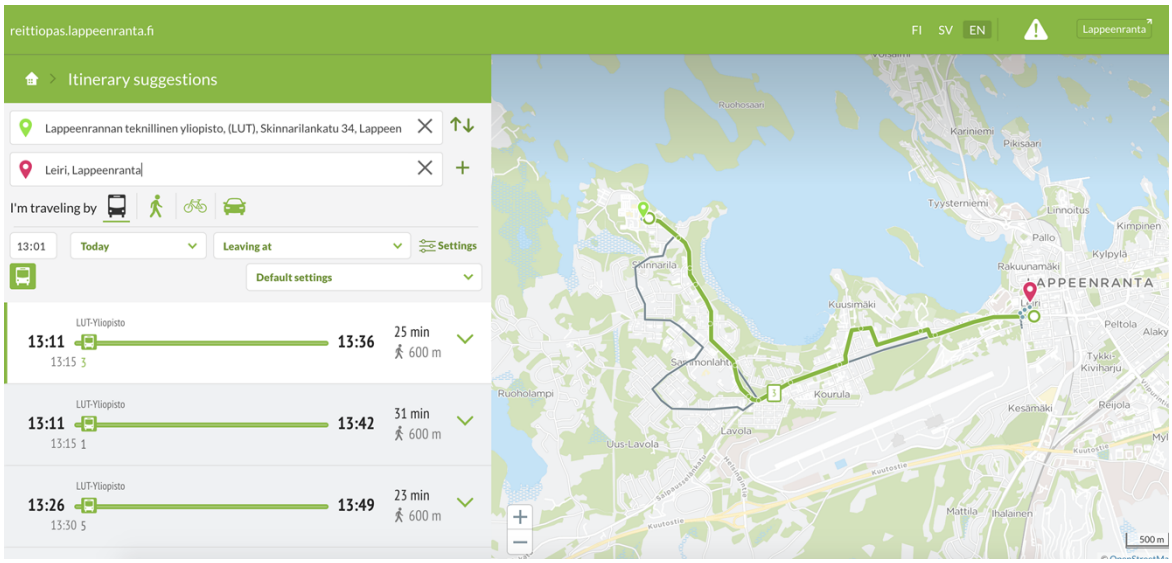

Figure 28. Actual application for the bus times (lappeenranta.digitransit.fi)

8. Conclusions

As stated in the introduction and it has been observed throughout the thesis, research, innovations and applications in technology every moment breaks more paradigms and barriers that society currently has, accelerating as we improve.

This implies that a point is being reached where what movie directors imagined years ago is becoming a reality, for example, shoes that you can print, smart cities and automatic farms for a system. Of course, even if they are not perfect today, they will eventually be.

IoT is making the world a better place, getting people connected in a way never seen before. When you say connecting, it means that those who seek solutions are achieving the potential to reach a greater number of people. With this, we want to emphasize that a new industrial revolution is being experienced.

IoT is an unstoppable technological trend. The advantages are unquestionable and will even appear new. The main inconveniences such as security, privacy and fear of "dehumanization" must be resolved unquestionably, above companies and governments.

Personally, this project has helped me learn to conduct a search on a subject of which I knew very little. Basically, I have learned to do a thesis on my own, with a lot of freedom, and these four months have helped me to nourish myself from books, articles and websites. Many of these I read and did not serve me that much, but others were very helpful. So, a research thesis requires many hours of searching.

Reviewing the work, a little, we have found six main data communications that act in the IoT. Each of these presents its advantages and disadvantages clearly. By having this variety, it makes it possible to apply one of the different technologies in each sector.

In addition, the idea of Smart City has also been discussed, which will be the future for large capitals, and later for all populations. This idea will make life easier and more comfortable for the population, making everything much more optimal, from life in your own home, to the garbage truck route.

Finally, some ideas have been shown to apply in the Finnish city of Lappeenranta in the future, to make it a safer city with an attraction for tourists.

Bibliography:

[1] Pfister, C. *Getting started with the Internet of things*. 2nd ed. Sebastopol: O'Reilly, 2011.

[2] BehrTech. (2020). *6 Leading Types of IoT Wireless Technologies | BehrTech Blog*. [online] Available at: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/ [Accessed 23 Jan. 2020].

[3] Waher, P. (2009). *Learning Internet of Things*. 1st ed.

[4] Etezadzadeh, C. (2016). *Smart City - Future City?*. 5th ed. Wiesbaden: Springer Vieweg.

[5] IEEE Internet of Things Journal. (2016). *IEEE Internet of Things Journal*, 3(5), pp.C3-C3.

[6] Barrio Andrés, M. (2018). *Internet de las cosas*. 1st ed. Madrid: Reus.

[7] López i Seuba, M. (2019). *Internet de las cosas*. 1st ed. Madrid: Ra-Ma.

[8] Witkowski, K. (2017). Internet of Things, Big Data, Industry 4.0 – Innovative Solutions in Logistics and Supply Chains Management. *Procedia Engineering*, 182, pp.763-769.

[9] Feki, M., Kawsar, F., Boussard, M. and Trappeniers, L. (2013). The Internet of Things: The Next Technological Revolution. *Computer*, 46(2), pp.24-25.

[10] Su, K., Li, J. and Fu, H. (2011). Smart city and the applications. 2011 International Conference on Electronics, Communications and Control (ICECC).

[11] Lombardi, P., Giordano, S., Farouh, H. and Yousef, W. (2012). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, 25(2), pp.137-149.

[12] Hall, R.E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., and Von Wimmersperg, U. *The vision of a smart city*. United States: N. p., 2000. Web.

[13] Vicent Ferrer. (2020). *Qué es RFID y cómo funciona - Historia, Tipos y tecnologías*. [online] Available at: https://vicentferrer.com/que-es-rfid-y-como-funciona/ [Accessed 23 Jan. 2020].

[14] Culturación. (2020). *Ventajas y desventajas del WiFi - Culturación*. [online] Available at: https://culturacion.com/ventajas-y-desventajas-del-wifi/ [Accessed 23 Jan. 2020].

[15] Mukhopadhyay, S. and Suryadevara, N. (2014). Internet of Things: Challenges and Opportunities. *Internet of Things*, pp.1-17.

[16] Chunxiao Fan, Zhigang Wen, Fan Wang and Yuexin Wu (2011). A middleware of Internet of Things (IoT) based on ZigBee and RFID. *IET International Conference on Communication Technology and Application (ICCTA 2011)*.

[17] Uckelmann, D., Harrison, M. & Michahelles, F., 2014. *Architecting the Internet of Things*, Berlin: Springer Berlin.

[18] Cano, J., Jimenez, C.E. & Zoughbi, S., 2015. A smart city model based on citizen-sensors. *2015 IEEE First International Smart Cities Conference (ISC2)*.

Glossary

$IoT - Internet\ of\ Things$

TCP/IP – $Transmission\ Control\ Protocol/Internet\ Protocol$

$RFID - Radio\ Frequency\ Identification$

$NFC - Near\ Field\ Communication$

$BLE - Bluetooth$

$ID - Identification$

$LPWAN - Low\ Power\ Wide\ Area\ Networks$

$ADAS - Advanced\ Driver\ Assistance\ Systems$

$5G - 5th\ Generation$

$MTSO - Mobile\ Telephone\ Switching\ Office$

$ICM - Information\ Classification\ and\ Management$

$LTE - Long\ Term\ Evolution$

$WPAN - Wireless\ Personal\ Area\ Network$

$ISM - Industrial, Scientific\ and\ Medical$

$GPRS - General\ Packet\ Radio\ Service$

$UMTS - Universal\ Mobile\ Telecommunications\ System$

$DDoS - Distributed\ Denial\ of\ Service$

$GDPR - General\ Data\ Protection\ Regulation$

$US - United\ States$