Jukka Kauranen

Choosing Right Wireless Network for IoT Devices

Helsinki Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Networking and Services

Master’s Thesis

13 Feb 2021

Abstract

Author(s) Title Number of Pages Date	Jukka Kauranen Choosing Right Wireless Network for IoT devices 54 pages 13 Feb 2021
Degree	Master of Engineering
Degree Programme	Information Technology
Specialisation option	Networking and Services
Instructor(s)	Ville Jääskeläinen, Supervisor

There exists tens of different wireless communication standards and proprietary solutions covering wide range of applications. This work focused solely on wireless standards for IoT use, and there are 20 of them. This work did not handle proprietary designs that fit things such as garage door openers, remote keyless entry on vehicles, tire pressure monitoring, or all those other unique ISM bands' wireless devices. Finding the right wireless standard for IoT is a challenge.

This thesis aims to study different wireless standards and technologies, find out their strengths and weaknesses, and help to choose the right wireless technology for IoT projects. The focus of the thesis was to find out how various wireless technologies are supported by home devices and how a home automation system can utilize and control their information. The study looked at four different home automation systems: IKEA Smart Home, Apple HomeKit, Arlo Surveillance Camera System, and Home Assistant software solution. The Home Assistant software was chosen, because it is an open system and supports a variety of hardware brands. The hardware platform for the Home Automation software was Raspberry Pi 3 Model B.

As a result, the study concluded that there are a wide variety of needs and requirements in the IoT environment. Several different wireless solutions are needed to solve these. The selected commonly used ten different techniques from NFC to GNSS can address over 80% of different needs and requirements.

Keywords	IoT, Internet of Things, wireless network, home automation

Table of Contents

List of Abbreviations

2FA	Two-Factor Authentication
3GPP	3rd Generation Partnership Project. A collaboration of telecommunication associations and companies which makes standards for mobile networks.
4G	4th Generation (mobile network)
5G	5th Generation (mobile networks or wireless systems)
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
802.15.4	IEEE 802.15.4 is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs)
AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
E2E	End-to-End
Gbps	Gigabits per second (1 000 000 000 bps)
GFSK	Gaussian Frequency Shifting
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema, Russia’s GNSS system
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAN	Home Area Network
HomeKit	Apple’s own-brand for smart home devices.
IoT	Internet of Things
IPsec	Internet Protocol Security
ISM	Industrial, Scientific, and Medical frequency band
Kbps	Kilobits per second (1000 bits per second)
LLC	Logical Link Control
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines, simplified term to LTE-MTC
LTE-MTC	Long Term Evolution-Machine Type Communication
M2M	Machine-to-Machine
MAC	Medium Access Control
Mbps	Megabits per second (1 000 000 bits per second)
MHz	Megahertz (1 000 000 Hz)
MIoT	Mobile Internet of Things, refers to LTE-M and NB-IoT
NB-IoT	NarrowBand – Internet of Things
NFC	Near-field communication
PHY	Physical Layer
RF	Radio Frequency
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition Systems

SC-FDMA	Single Carrier - Frequency Division Multiple Access
Sigfox	Sigfox is both the shorthand for a proprietary, narrowband, low-power WAN technology, and the name of the French company that makes it.
SMS	Short Message Service is a text messaging service component of most telephone, World Wide Web, and mobile device systems.
SSL	Secure Sockets Layer
TLS	Transport Layer Security
Zigbee	Zigbee is a low-cost, low-power, wireless mesh network standard targeted at battery-powered devices in wireless control and monitoring applications.
Z-Wave	Z-Wave is a wireless communications protocol used primarily for home automation.
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
Wi-Fi	Wi-Fi is a family of wireless network protocols, based on the IEEE 802.11 family of standards,
YAML	YAML Ain't Markup Language. YAML is a human friendly data serialization standard for all programming languages.

1 Introduction

The Internet of Things (IoT) consists of a network of physical devices, which are connected to the Internet. Companies can combine physical sensing with data analysis to create meaningful information. IoT platforms enable solutions in smart cities, smart grids, smart homes, and connected vehicles that could provide a significant qualitative improvement in people’s lives (Figure 1). IoT can also be an economic engine for growth as it increases productivity, reduces cost, and improves lives. [1]

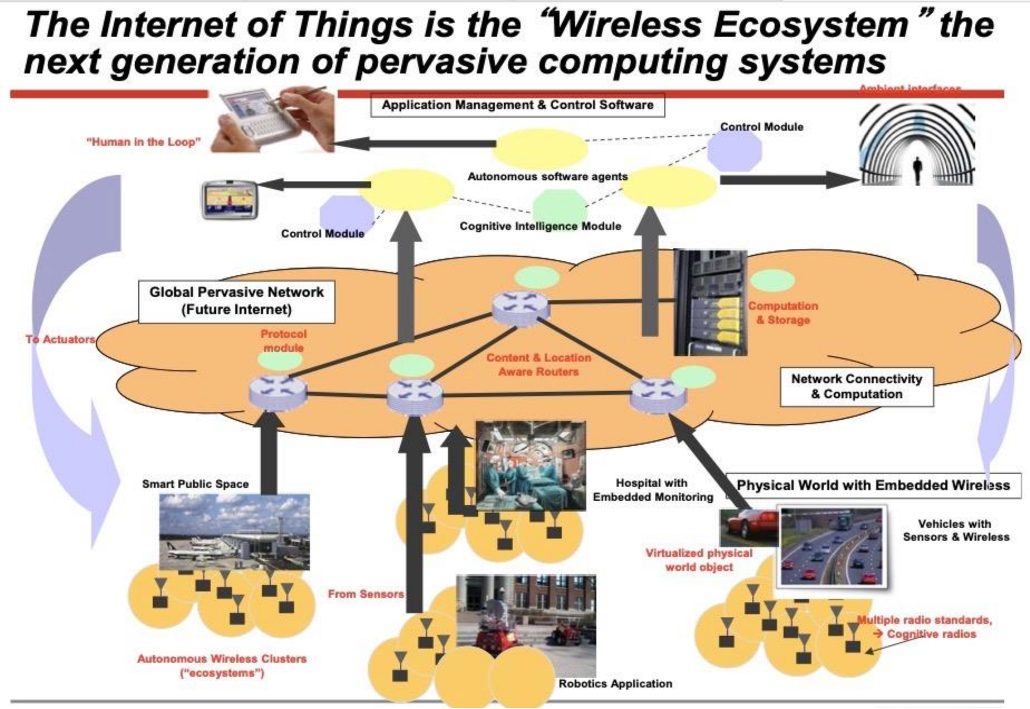

The Internet of Things is the “Wireless Ecosystem” the next generation of pervasive computing systems
Ambient interfaces
Application Management & Control Software
"Human in the Loop"
Control Module
Autonomous software agents
Control Module
Cognitive Intelligence Module
Global Pervasive Network (Future Internet)
Protocol module
To Actuators
Content & Location Aware Routers
Computation & Storage
Network Connectivity & Computation
Smart Public Space
Hospital with Embedded Monitoring
Physical World with Embedded Wireless
Vehicles with Sensors & Wireless
Virtualized physical world object
From Sensors
Multiple radio standards, → Cognitive radios
Autonomous Wireless Clusters ("ecosystems")
Robotics Application

Figure 1. IoT is the “Wireless Ecosystem” for the next generation computing systems [2]

IoT includes various technologies such as wireless and wired sensor networks and actuators, mobile phones, distributed intelligence of smart devices, and enhanced communication protocols through the Internet. The main idea behind IoT is to connect numerous heterogeneous devices through the Internet to operate intelligently, efficiently, and safely. [3]

Gartner, Inc. forecasts that 20,4 billion connected things will be in use worldwide in 2020. The consumer segment is 12,9 billion units in 2020. While consumers purchase more pieces of devices, businesses spend more money on devices. The combined hardware spending will reach nearly $ 3 trillion in 2020. [4]

Table 1: IoT Units Installed Base by Category (Millions of Units) [4]

Category	**2017**	**2018**	**2020**
Consumer	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,635.4	2,027.7	3,171.0
Grand Total	**8,380.6**	**11,196.6**	**20,415.4**

IoT is revolutionizing our lifestyle and creates steady economic growth. Everything and everyone can be connected. This vision redefines the way people interact with each other and with the surrounding things.

IoT includes many technologies such as near-field (NFC, RFID), short-range (BLE, WLAN, ZigBee, Z-Wave), and wide-area (LTE, NB-IoT, Sigfox, LoRaWAN, 5G) communication networks; device-to-device communications; device and application software for Big data, security, analytics, and cloud processing. Three main IoT components are the devices, the communication network, and the application servers. The devices sense physical characteristics (for example temperature) and send the data through the network to the servers. The servers process the data and make meaningful information. This output could be sent back through the network to the devices.

There are a wide variety of different needs and use cases for IoT solutions, which cannot be satisfied with one or two different wireless techniques. There are different wired and wireless techniques for IoT, which have their pros and cons. Most of these billions of new IoT devices are connected to the wireless networks. If one can use the power supply and either Ethernet cabling or WLAN with IoT, then there are not problems. Otherwise, compromises need to be made in terms of speed, price, power consumption, and coverage. The question is how to select the right wireless network for an IoT project and how the selection should be done in practice.

There will be billions of new Internet of Things (IoT) devices in the world in the next ten years. There are quite many different wireless networking techniques (such as NFC, RFID, BLE, WLAN 802.11, Zwave, ZigBee, Sigfox, NB-IoT, and LTE-M). The problem is how to choose the right wireless network for every IoT project. The target of this study is to understand customer's needs and advise customers of the right network solutions for IoT.

1.1 Outcome(s)

For this study one practical use case was selected, Home Automation. The outcome of the study includes following two things:

- Come up with recommendations on how to select and use different wireless network solutions for IoT, make recommendations for choosing the right wireless network for an IoT project.
- Study and test different wireless network techniques on the example of this one project.

This research also addresses security features of these wireless techniques and excludes wired network techniques.

1.2 Research Design

This thesis was carried out by the following research design (see Figure 2). In addition to Metropolia's courses, IoT techniques were studied at a separate IoT seminar. Customer needs were determined both from own work history experience and by through discussing with our organization's service managers. In addition to Metropolia's courses, information on wireless network technologies was collected from publications and websites of both manufacturers and standardization organizations. The home automation project investigated various IoT systems and wireless technologies. The project investigated how different systems and different wireless technologies can be combined into one automation-controlled entity. As a result, the most recommended wireless technologies for various applications were selected.

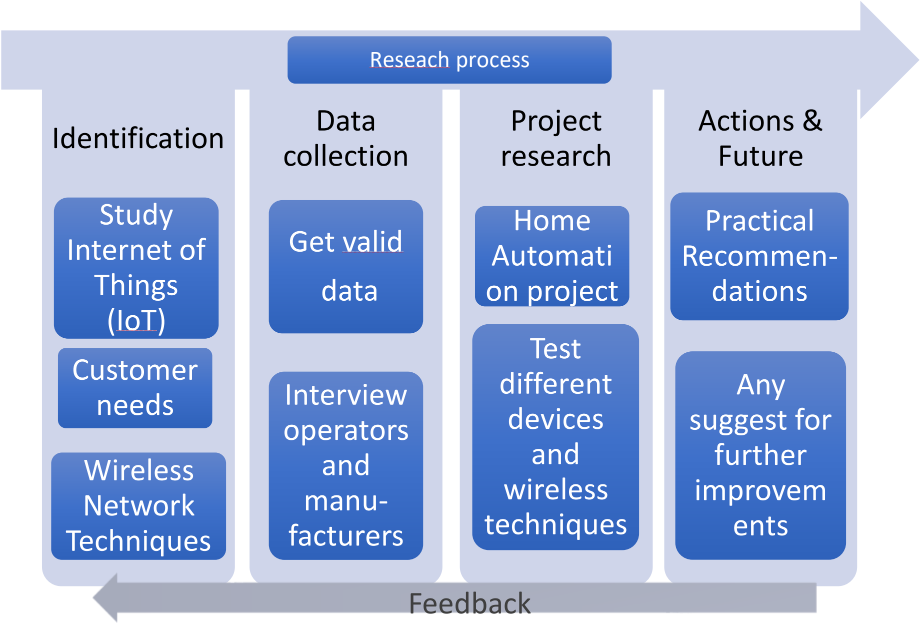

Reseach process
Identification
Study Internet of Things (IoT)
Customer needs
Wireless Network Techniques
Data collection
Get valid data
Interview operators and manu-facturers
Project research
Home Automati on project
Test different devices and wireless techniques
Actions & Future
Practical Recommen-dations
Any suggest for further improvem ents
Feedback

Figure 2. The research design of this study.

The thesis has been divided into 7 sections. The first section introduces the problem and describes research design methods. The second section introduces Internet of Things. The third section introduces customer needs and wireless techniques for IoT. The fourth section introduces Home Automation project and test of different wireless techniques and platforms. The fifth section shows results and analysis, and practical recommendations. The sixth section introduces discussions, conclusion and further improvements.

2 Internet of Things (IoT)

Here is described the history of IoT, main IoT features, security in shortly, and different wireless scenarios of IoT.

2.1 History

Modified Coke machine at the Carnegie Mellon University in 1982 was the first internet-connected appliance. Mark Weiser, the head of the Computer Science Laboratory, wrote September 1991 a fascinating article about “The Computer for the 21st Century, where he described “Ubiquitous computing”, which is very similar to nowadays IoT.

Kevin Ashton, the Executive Director of Auto-ID Labs at MIT, was the first to describe the Internet of Things in his speech in 1999: “Today computers, and, therefore, the Internet, is almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code. The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing, or recalling and whether they were fresh or past their best.” [5]

The supervisory control and data acquisition systems (SCADA) have been used since the 1960s to monitor and control systems and devices. These systems have used only with some purpose and have limited data analysis capabilities, and that’s why these are not real IoT systems.

Connecting things to the Internet is a newer idea that is occurring on a large scale. By connecting a wide variety of devices and applications, humans can interact with the physical world. The Internet of Things (IoT) can be viewed as bringing the physical world into the digital realm by increasing knowledge and awareness. [6]

2.2 Applications

The main idea of the IoT is to connect numerous different kinds of devices through the Internet to operate intelligently and efficiently. The IoT consists of a network of physical devices connected with remote computational capabilities. By combining physical sensing with data analysis to create meaningful information, IoT platforms enable solutions in the realms of smart cities, smart grids, smart homes, and connected vehicles that could provide a significant qualitative improvement in people’s lives. IoT has also been seen as an economic engine for growth as it increases productivity, reduces cost, and improves lives.

The notion of IoT is broad and encompasses many technologies, including near field, short-range and wide-area communication networks; a device to device communication; device technologies for sensing, actuation, and energy harvesting; device and application software platforms for big data, security, streaming analytics, and cloud processing.

The three main components of most IoT-enabled applications are the devices, the network, and the application servers. The devices sense a physical characteristic of the environment (e.g., temperature or presence of an object) and send the information through a communication network. The data is aggregated and processed by servers to provide meaningful information or an actionable output. This output could be sent back through the network to trigger a set of actuator devices (e.g., a switch for triggering a motor or alarm). This basic framework could enable new classes of applications and servers, such as the management of autonomous vehicle fleets, enabling more energy-efficient cities and homes, and the ubiquitous tracking of assets.

The IoT communication network is often known as a machine-to-machine (M2M) network to distinguish it from networks that are used by humans. While the network consists of wired and wireless devices, the trend is for devices to be wirelessly connected to the network edge to enable lower-cost installation, easier physical reconfiguration, and mobile applications.

IoT use cases are, for example:

- Smart cities to street lighting, parking and waste management
- Healthcare to patient monitoring in real-time
- Consumer to people tracking and pet tracking
- Smart building to energy and water measuring
- Logistics to key inventory
- Vehicle asset tracking and analyze driving
- Smart buildings to alarm systems, access controls, smart metering (energy and water), physical security, light, and temperature settings
- Environment and agriculture to environmental and pollution monitoring
- Autonomous vehicles

2.3 Security

Security is one of the challenging concerns in the IoT environment. IoT applications must be secure. As the IoT market expands, protecting the company's data and Intellectual Property (IP) is more important than ever. The future challenge for IoT is to authenticate IoT user's authentication. With the new standard and self-configuring protocol, authentication becoming more complicated compared to the traditional approach. With the help of two-factor authentication, it's a little bit easier to control different application.

Therefore, confidentiality must be maintained, and the message needs to be hidden from third parties. IoT requires an End-to-End (E2E) message security. Also, the stored data, such as message and personal data on the IoT device, should be hidden from unauthorized entities.

Interestingly, most of the research in IoT focused on privacy, which is also an essential ingredient of secure IoT. In any application, integrity is a much more critical component compare to others such as availability because privacy may lead to some embarrassment, but integrity, especially if its medical device or car's braking system can easily cost someone's life. For many years Public Key Infrastructure (PKI) and Keyless Signature Infrastructure (KSI) are both used for data security and have complementary roles. PKI is best used for authentication and secure communication on the network. KSI can be used for integrity proof.

In the traditional system, access controls are only targeted to a system where all users are known to the system. In IoT, it should consider an open and closed system where an unknown party plays an important role. The usage control model (UCON) has three decision factors (authorizations, obligation, and conditions) and two decision properties (mutability and continuity). Communication in the IoT should be protected by providing security services and using standardized security mechanisms at different layers.

The link-layer security protects communication on a per-hop base where every node in the communication path has to be trusted. A single pre-shared key is used to protect all communication. Typically, if an attacker compromises one device and access one key, it means that the whole network is compromised. However, in this link-layer as its per-hop security, only one hop/device is compromised, and it can be detected at an initial state. Still, link-layer protection is limited, but it's quite flexible, which operates with multiple protocols on different layers.

As IoT implemented on the Internet, it uses network IP Security (IPsec) provided by the Network layer. IPsec delivers end to end security with authentication as well as confidentiality and integrity. IPsec operates at the network layer, and that’s why IPsec can be used with any transport layer protocol, including TCP, UDP, and HTTP. IPsec uses the Authentication header (AH) for data integrity and data origin authentication. IPsec uses the Encapsulated Security Payload (ESP) protocol for confidentiality and authentication. Other possible security protocols for IoT are transport-layer security (TLS) or its predecessor, Secure Sockets Layer (SSL).

Securing communication is very important in IoT, but most of the application developers forget about securing data that is generated from all IoT devices. Most Internet devices are small and, due to their limited size, do not have enough capabilities to protect them from hardware-related security threats. One security solution is not enough to secure everything. That's why there is a need to use different security solutions on different communication technology.[7]

2.4 Wireless Networks

Wireless communications started with Marconi’s radio innovation in 1894. The two major wireless network access technologies are mobile cellular and Wi-Fi. These radio systems operate 450 MHz – 5 GHz areas, where the radio wave travels a direct path from the transmitting antenna to the receiving antenna. This is called the line of sight (LOS) propagation. The power of a radio wave is reduced with distance and frequency. The loss or attenuation is proportional to 20 times the logarithm of frequency and distance. So if the distance or frequency is doubled, one needs four times higher transmission power to get the same signal power (free-space loss). However, the lower the frequency the lower the data rate it can support.

In real life, antennas are not isotropic, and there are many different obstacles to propagation in the environment. Low power consumption of IoT devices is important, and therefore making longer wireless connections is a challenge. [8] pages 173-186

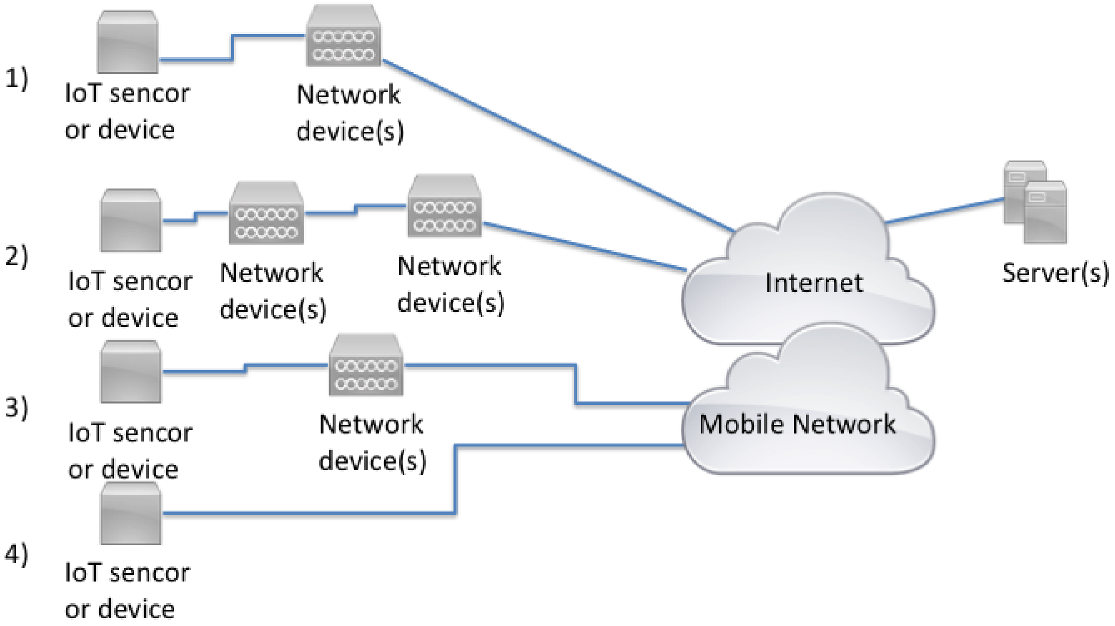


Figure 3. Different IoT Wireless cases

In Figure 3, there are four different IoT Wireless scenarios. The 1) is the case where IoT sensor or device is connected using Personal Area or Local Area Wireless techniques to the Network device(s), which is then connected with wires to the Internet. The 2) is the case where IoT sensor is connected using Personal Area or Local Area Wireless techniques to the Network device(s). The Network device is connected using Local Area Wireless techniques to the other Network device(s), which is then connected with wires to the Internet. The 3) is the case where IoT sensor or device is connected using Personal Area or Local Area Wireless techniques to the Network device(s), which is then connected with Wide Area Wireless techniques to Mobile Network, which is connected to the Internet. The 4) is the case where IoT sensor or device is connected with Wide Area Wireless techniques to Mobile Network, which is connected to the Internet. In this Figure Network device(s) can be one or more Network devices as Wireless Access Points, Gateways, Switches, Routers, and Security devices. Information from the IoT sensors and devices is transferred to the server(s). In many cases, Edge computing solutions are used between IoT devices and the server(s).

3 Wireless Techniques for IoT

IoT applications have two major wireless dimensions: mobility and geographical area. The Wireless techniques for IoT can be divided into three main groups in geographical area: Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), and Wireless Wide Area Network (WWAN).

This work has focused solely on wireless standards (real standards or open de facto standards), which can be used for IoT, and there are over 20 of them. Many of these wireless techniques use the Industrial, Scientific and Medical (ISM) worldwide radio frequency bands which are not licensed. There are two main ISM bands for Europe: 2.400-2.4835 GHz and 5.725-5.850 GHz. This work does not handle proprietary designs that fit things such as garage door openers, remote keyless entry on vehicles, weather stations, tire pressure monitoring, or all those other unique ISM bands wireless devices.

To decide which technology to use, here are the key questions for decision making:

- What is the maximum range of a link?
- What is the power consumption?
- What is the maximum data rate used in the application? Streaming video, measuring temperature every minute, or something in between these?
- What is the required latency?
- Is there a need for one-way or two-way communication?
- What is the frequency band of operation?
- How many nodes are there?
- What is the network typology?
- How large is the network?
- Are there other wireless services/devices that could cause interference?
- What kind of licensing and certification are required to use the standard?
- Are chips and/or modules available from multiple vendors?
- What are the needs for security?
- What are the prices for devices, support and data communications?

There are several design factors to consider when choosing a wireless technology:

- Range or distance to the gateway: A few centimeters within a room or over a kilometer in a rural area.
- The environment: Hazardous surroundings at the factory, outdoors in the weather, noise from electrical equipment or EMI.
- Need for encryption or authentication: What is the demand for data security?
- Power consumption: Battery life; energy efficiency; the possible need for an ac power connection.
- Capacity: Number of connected devices.
- Quality of service and reliability.
- Network topology: Star, mesh, or other.
- Simplex or duplex: One-way vs. two-way communications.
- Suitable and available spectrum: Licensed or unlicensed.
- Available ICs, modules, and equipment.
- Cost: Design, manufacturing, or Internet access service expense.

- Development platform: What kind of OS is needed, and are there other needs for the software?
- Internet access: Cellular, DSL, cable, fiber, satellite.

[6] pages 189-214, [9], [10]

3.1 Wireless Personal Area Network (WPAN)

The Wireless Personal Area Network and connections range vary from the few centimeters of Near-field communication (NFC) to 100 meters of Bluetooth Low Energy (BLE).
WPAN networks for IoT:

- ANT+
- Bluetooth Low Energy (BLE)
- NFC
- RFID
- Z-Wave
- IEEE 802.15.4 based networks:
    - Thread (6LoWPAN)
    - ZigBee
    - Wi-SUN
    - WirelessHART

3.1.1 ANT+

Adaptive Network Topology + (ANT+) is a successor to Adaptive Network Topology (ANT). ANT is a proprietary multicast wireless sensor technology of ANT Wireless (a division of Garmin Canada, formerly Dynastream). ANT+ was the first ultra-low-power wireless standard, and it was introduced in 2004 (ANT+ Alliance). ANT+ branded devices have been certified to be interoperable with other ANT+ branded devices (like Garmin, Suunto).
Features of Ant+:

- Ultra-low-power, can use “sleep mode”
- Standardisation: The ANT+ Alliance is an open special interest group of companies. The Alliance ensures standardized communications with other products. Garmin Canada manages ANT+ Alliance. There are over 350 members.
- Duplex two-way communications
- Topology: point-to-point, star, or mesh
- Uses 2.457 GHz RF frequency, unlicensed ISM band
- Range: max 30 m
- Chip manufacturers: Nordic Semiconductor and Texas Instruments
- Over 100 Million installed nodes. There are over 400 certified ANT+ products.
- Typical use cases: heart rate monitoring and bicycle cadence sensors

[11]

3.1.2 RFID

Radio Frequency Identification (RFID) is used mostly for tags or labels attached to the objects. RFID tags can be passive, active (has a battery), or a battery-assisted passive.
A passive RFID tag is the cheapest and smallest because it has no battery. Instead of the battery, it uses radio energy from the reader. A battery-assisted passive (BAP) RFID tag has a small battery, and an RFID reader activates it. A typical RFID tag has a microchip attached to a radio antenna on a substrate. The microchip can store up to 2 kilobytes of data. A reader can read the data stored on an RFID tag. The typical reader has one or more antennas that send radio waves and receive signals back from the RFID tag.

RFID Auto-ID tag standards

- Class 0: Basic read-only passive tag where the tag was programmed at the time the tag chip was made
- Class 1: Basic read-only passive tag with one-time non-volatile programming capability
- Class 2: Passive tag with 65K of read-write memory
- Class 3: A battery-assisted passive with up 65K read-write memory and battery to provide increased range
- Class 4: An active tag using a battery to enable extra functionality and increased range
- Class 5: An active tag that provides additional circuits for communication with other class 5 tags

The range of the RFID system can be categorized

- Close range – within 1 cm
- Remote range – between 1 cm and 1 m
- Long-range – more than 1 m
- The range of active RFID tags can be many meters, even 100 m

Passive RFID tags:

- Advantage: long lifetime, cheap, does not need the battery and small size
- Disadvantage: limited range, limited features, and possible privacy implications
- Passive low-frequency (LF) systems use 125 kHz and 134 kHz. These are used for animal identification, access control, and some industrial applications. Range is usually 10 cm.
- Passive high-frequency systems use 13,56 MHz. These are used for access control, smart cards, and item identification. Range is up to 0.5 m.

- Passive ultrahigh-frequency (UHF) systems use 865-868 MHz. These are used for inventory tracking, item identification, and other applications. ETSI EN 302-208 defines transmit powers up to 2 watts effective radiated power (ERP). Range is up to 10 m.

A battery-assisted passive (BAP) RFID:

- Gen 2 EU RFID tags use 860 MHz
- Range is up to 50 m

Active RFID tags:

- Advantage: longer range and more features
- Disadvantage: needs a battery, more expensive, shorter lifetime and bigger size
- Most active RFID systems use 860 MHz or 2.45 GHz.
- Range is up to 100 m

Features of RFID:

- The global RFID market was 16.45 billion dollars in 2016 and is projected to grow to 22 billion dollars by 2020
- Unlicensed ISM band
- Typical use cases: Access control, Agriculture, Asset management, Contactless ticketing, Healthcare, IoT, Logistics, Manufacturing, Retail, Security, and Transport.
- Unauthorized reading of RFID tags is a risk to privacy

[12]

3.1.3 NFC

Near Field Communication (NFC) is a newer, more finely modified version of RFID. It can operate at a maximum range of about 10 cm, typically about 4 cm, and can be used both one- or two-way communications. NFC technology is simple and safe two-way interactions between electronic devices. NFC technology allows consumers to perform contactless transactions, access digital content, and connect electronic devices with a single tap. NFC devices use globally available unlicensed radio frequency 13,56 Megahertz (MHz) (ISO/IEC 18000-3), and data rates vary from 106 – 424 kilobits per second (kbps). NFC devices can have three modes:

- NFC reader/writer, which enables the device to read information stored in NFC tags.
- NFC peer-to-peer, which enables two NFC-enabled devices to communicate with each other.
- NFC card emulation, which enables devices, like smartphones, to act like smart cards.

NFC can be categorized into two classes:

- Passive NFC – which has not a power source, typically NFC tags, small transmitters. Typical examples are the new bank cards with contactless payment.

- Active NFC – devices that can send as well receive data. The best example is a new Smart Phones. Most of the nowadays Smart Phones have NFC features, for example, Apple iPhone SE/6/6s/6Plus/Watch and newer models, Google Nexus 5 and newer models, Huawei Honor 6/Mate 8 and newer models, Microsoft Lumia 640 and newer models, Nokia 3/5/6/603/700/701, Samsung Galaxy A3/Ace 2 and newer models.

NFC tags are for passive data storing, which can be read (sometimes also written) by an NFC device. These typically contain 96-8192 bytes.

NFC devices can be used in commerce for contactless payments and electronic tickets, for electronic identity documents and keycards, for smart NFC tags and gaming (for example, Nintendo Wii U/3DS, Xbox 360 and PlayStation 4).

Features of NFC:

- Ultra-low-power
- Standardization: Readers and cards compliant to the ISO/IEC 14443 standard, Cards compliant to the ISO/IEC 15693 standard, Devices compliant to the ISO/IEC 18092 standard, Devices compliant to the ISO/IEC 18092 standard, and Devices compliant to the ISO/IEC 18092 standard
- Duplex two-way communications
- Topology: point-to-point with two devices
- Uses 13,56 MHz RF unlicensed ISM band frequency
- Range: max 10 cm
- Communication speed: up to 424 Kbps
- Chip manufacturers: NXP, Broadcom, Samsung Semiconductors, Texas Instruments, and Qualcomm
- Over 2 Billion NFC-enabled devices and is compatible with hundreds of millions of contactless cards and readers installed nodes.
- Unauthorized reading of NFC tags is a risk to privacy
- Typical use cases: Retail and Payment using NFC and smartphones, Bluetooth/Wi-Fi pairing, and Public Transportation.

[12], [13], [14]

3.1.4 Bluetooth Low Energy (BLE)

Bluetooth has evolved for 20 years, expanding the universe of innovative ways to connect. Bluetooth is an innovative connection for wireless audio, portable devices, asset tracking, or building automation. Bluetooth Special Interest Group (SIG) has formed in 1998, starting with only five companies (Ericsson, Intel, Nokia, IBM, and Toshiba), but the end of the first year there was more than 400 members. Bluetooth SIG is the organization at the heart of Bluetooth technology, serving industry-leading member companies (now over 33 000 member companies) all over the world. Bluetooth 4.2 was released in 2011. Bluetooth 5 was released in 2016, and it is backward compatible with 4.2. The Bluetooth design idea is to support different ranges between two devices.

Table 2. Bluetooth Releases and Features

Specifications / Features	Bluetooth 4.2, LE 1M	Bluetooth 5, LE 2 M	Bluetooth 5, LE Coded
Data Rate	1 Mbps	2 Mbps	125 / 500 kbps
Range	Up to 100 m	Up to 100 m	Up to 400 m, up to 1 km outdoor

Bluetooth comes in two radios: Classic and Low Energy. Bluetooth Classic enables wireless printers, wireless headsets, and wireless speakers. Bluetooth Low Energy (BLE) uses less power and enables areas such as health care, heart rate monitoring, smartphones, beacons, and IoT devices. Bluetooth is a full protocol stack, where the bottom layer is called the Physical Layer (PHY). The Physical Layer defines the modulation scheme, the number of channels, the error correction, and much more. Low Energy Physical Layer names are LE 1M, LE 2M, and LE Coded. LE 1M is the PHY used in Bluetooth 4 (also available in Bluetooth 5), and it uses Gaussian Shift Keying and has a 1 mega symbol per second speed (Ms/s). Bluetooth 5 has two new PHY variants (LE 2M and LE Coded) to the PHY specification used in Bluetooth 4. LE 2M uses 2-level Gaussian Frequency Shift Keying (GFSK) and double the symbol rate of LE 1M, and speed is 2 mega symbol per second. The LE Coded PHY allows the range to quadrupled compared to LE 1M, without increasing the transmission power required. [15]

Bluetooth is now an industrial-grade connectivity solution for the Internet of Things (IoT) for decades to come.

Features of Bluetooth Low Energy:

- Very low-power, transmit power from Class 3: 1 mW to Class 1: 100 mW
- Standardization: IEEE 802.15.1
- Duplex two-way communications
- Topology: point-to-point, broadcast, and mesh networking
- Uses 2.4 GHz (2400 to 2483.5 MHz) unlicensed ISM spectrum band
- Range: typically 50 m indoors, 100 m outdoors, max 1 km outdoors (LE Coded S=2, max power, and suitable antennas)
- Communication speed: data rates from 125 Kbps to 2 Mbps

- Chip manufacturers: Murata, Qualcomm, Intel, Broadcom, Panasonic, Texas Instruments, Fujitsu, Hosiden, STMicroElectronics, Laird, Taiyo Yuden, Cypress Semiconductor, Microchip Technology, and Silicon Labs
- In 2019, 4 billion devices shipped with Bluetooth® technology.
- Security: 128-bit AES
- Typical use cases: Medical devices, heart rate monitoring, smartphones, remote controllers, home automation, industrial sensors, and beacons.

3.1.5 Z-Wave

Z-Wave is a low-power mesh-network technology for the smart-home industry, which has a sizeable interoperable ecosystem. Zensys originally developed Z-Wave as a proprietary wireless standard. Sigma Designs acquired Zensys in 2008, and Silicon Labs acquired Sigma Design's Z-Wave Business in 2018. Z-Wave is now an open standard, based on the International Standard PHY MAC ITU-T G.9959. Silicon Labs and Z-Wave Alliance announced plans to open the Z-Wave Specification as a ratified, multi-source wireless standard available to all silicon and stack vendors for development. The stack is openly licensed; products need to be certificated to ensure interoperability. The Z-Wave Public Specification, released in late 2016, along with robust certification, ensures that all the device and service makers implement communication using the same data sources.

The ITU-T G.9959 recommendation defines:

- One node in the domain operates as a domain master
- Each domain may contain up to 232 nodes (including the domain master)
- The recommendation is limited to PHY, MAC, segmentation and reassembly (SAR), and LLC layers of ITU-T G.9959 radio communications TRXs

The Z-Wave wireless mesh networking technology, any node can talk to other nodes directly or indirectly. A master controller node controls additional nodes. The nodes can communicate directly with one another, which is within range. Each node (non-battery) device can be a signal repeater; the more devices there are, the stronger the network becomes.

Features of Z-Wave:

- Very low-power, 1 mW
- Standardization: ITU-T G.9959 recommendation
- Duplex two-way communications
- Topology: mesh networking
- Uses 868.4 MHz / 869.85 MHz in the EU, Part 15 unlicensed ISM spectrum band
- Range: typically 30 m indoors
- Communication speed: data rates 9600 bps, 40 kbps, and 100 kbps

- Chip manufacturers: Silicon Labs
- Market position: One of the leading smart home technology. Over than 2400 certified interoperable products and more than 700 supporting companies around the world. There are over 100 million Z-Wave products worldwide.
- Security: AES 128
- Typical use cases: home automation, building monitoring & controlling, and status reading applications

[16]

3.1.6 IEEE 802.15.4

IEEE 802.15.4 category is one of the most significant standards for low-data rate WPANs. Several of the standards are based upon the IEEE 802.15.4 standard, ZigBee, Thread, WirelessHART, and Wi-SUN. The IEEE 802.15.4 is the protocol and compatible interconnection for data communication devices using low-data-rate, ultra-low-power, ultra-low-cost, and ultra-low-complexity short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN). It was released in 2003, and the newest standard is IEEE 802.15.4-2015. The 802.15.4 standard only specifies the lowest two layers of the protocol stack, which are the Physical layer (PHY) and Medium Access Control (MAC) layer. There can be two different types of device types: a full-functioning device (FFD) and a reduced-function device (RFD). An FFD can be a personal area network (PAN) coordinator. An RFD cannot be a PAN coordinator. An RFD is for straightforward applications such as a light switch or a passive infrared sensor. A WPAN includes at least one FDD, operating as the PAN coordinator. IEEE 802.15.4 WPAN can operate either star topology or peer-to-peer topology. Security is based on symmetric-key cryptography and uses keys that are provided by higher-layer processes.

Features of 802.15.4:

- Ultra-low-power, 0.5 - 1 mW
- Standardization: IEEE 802.15.4
- Duplex two-way communications
- Topology: basic star and Peer-to-peer
- Uses 868 to 868.6 MHz in the EU and 2.4 to 2.4835 GHz Worldwide, unlicensed ISM spectrum band
- Range: typically 10 - 75 m indoors
- Communication speed: data rate 20 kbps
- Enhancements to the 802.15.4 standard: ZigBee, Thread, WirelessHART, and Wi-SUN
- Market position: By 2023, 4.5 billion cumulative 802.15.4 mesh devices are projected sold worldwide. The majority of these using smart home protocols like ZigBee and Thread. [30]
- Security: symmetric-key cryptography

- Typical use cases: home automation, building monitoring & controlling, and status reading applications

[17]

3.1.7 ZigBee

ZigBee is a high level of communication protocols used to create personal area networks with small, low-power digital radios. ZigBee is based on the IEEE 802.15.4 standard. ZigBee is an open wireless standard from the ZigBee Alliance and was established in 2004. The IEEE 802.15.4 standard covers layer 1 (PHY) and layer 2 (MAC), while the ZigBee stack software covers the upper network and application layers. ZigBee wireless technology is a standard enabling control and monitoring capabilities for industrial and residential applications within a +100-meter range.

Features of ZigBee:

- Very low-power, 0.5 - 1 mW
- Standardization: IEEE 802.15.4, ZigBee is open wireless standard from the ZigBee Alliance, which has more than 220 members
- Duplex two-way communications
- Topology: point-to-point, star, and wireless mesh networking, up to 65k nodes
- Uses 868 to 868.6 MHz in the EU and 2.4 to 2.4835 GHz Worldwide, unlicensed ISM spectrum band
- Range: up to 100 m
- Communication speed: data rate 20 kbps
- Security: AES-128
- Chip manufacturers: Atmel, Digi International, Freescale Semiconductor, GreenPeak Technologies, NXP Semiconductors, Renesas Electronics, Silicon Laboratories, STMicroelectronics, and Texas Instruments
- Market position: 300 million Certified Products deployed all over the globe
- Typical use cases: Home automation, Smart lighting, Smart energy, building automation, health care, and status reading applications.

[16]

3.1.8 Thread

Thread is a wireless mesh networking protocol based on IEEE 802.15.4 radio standard. It enables device-to-device and device-to-cloud communications. The Thread Group is a non-profit organization responsible for the certification of Thread products, announced in 2014. Thread is an IP-based (6LoWPAN) wireless networking protocol providing the connecting products in the home. 6LoWPAN stands for “IPv6 Over Low Power Wireless Personal Networks.” The main goal of 6LoWPAN is to transmit and receive IPv6 packets over 802.15.4 links.

Features of Thread:

- Very low-power, 1 mW
- Standardization: IEEE 802.15.4, Thread Group (Sponsors: Apple, ARM Holding, Nest Labs/Google, Siemens, Qualcomm, NXP Semiconductors, Silicon Labs, Somfy, Yale), open IPv6 standard network protocol RFC 4291
- Duplex two-way communications
- An open protocol that carries IPv6 natively (6LoWPAN)
- Topology: robust wireless mesh network with no single point of failure, up to 250 devices
- Uses 2.4 to 2.4835 GHz Worldwide, unlicensed ISM spectrum band
- Range: up to 100 m
- Communication speed: data rate 250 kbps
- Security: AES-128
- Chip manufacturers: ARM, NXP Semiconductors, Silicon Laboratories, STMicroelectronics, Texas Instruments, and Qualcomm
- Market position: Thread is one of the technologies in the new Project Connected Home over IP (CHIP).
- Typical use cases: Home automation: access control, climate control, energy management, lighting, safety, and security.

[17], [40]

3.1.9 Wi-SUN

Wireless Smart Ubiquitous Network (Wi-SUN) established in 2011. It is a wireless technology based on the IEEE 802.15.4g standard, also known as the Smart Utility Networks (SUN), approved 2012. Wi-SUN Alliance is a global industry alliance that promotes the Wi-SUN. Initially, Japan-based, now expanding globally (US, Asia, Europe).

Features of Wi-SUN:

- Ultra-low-power, < 1 mW, 2 μA resting, 8 mA listening
- Standardization: IEEE 802.15.4g, IPv6, 6LoWPAN
- Duplex two-way communications
- Topology: usually mesh networks with redundancy
- Uses 868 MHz (EU), 920 MHz (Japan), unlicensed ISM spectrum band
- Range: up to 1 km outside
- Communication speed: data rate up to 300 kbps, latency 20 ms
- Security: AES-128, X.509 certificates
- Chip manufacturers: Renesas, Silicon Labs
- Market position: Wi-SUN Alliance has more than 100 member companies and more than 90 Wi-SUN compatible products. Tens of millions of connected endpoints have installed.

- Typical use cases: Smart Utility Networks, Smart Cities, Smart Metering, Smart Streetlights, and automated control and monitoring.

[18], [19]

3.2 WirelessHART

WirelessHART is an industrial wireless network based on the Highway Addressable Transducer Protocol (HART). HART is a communications protocol that offers data access between field devices and host application systems. HART is a widely used field communication protocol, and there are 40 million devices worldwide. WirelessHART adds wireless features to the HART, it is based on 802.15.4, and it was introduced in 2007. The WirelessHART network consists of these three elements: Wireless field devices connected to process, Gateways enabling communications between field devices and host applications, and Network manager.
Features of WirelessHART:

- Ultra-low-power, < 10 mW, battery life 5-7 years
- Standardization: IEEE 802.15.4, IEC 62591
- Omni-directional, Half-duplex communications
- Topology: star and robust mesh networks with redundancy, one gateway can support up to 80 devices, built-in time synchronization
- Uses 2.4 GHz, unlicensed ISM spectrum band, 16 channels, channel hopping technique
- Range: up to 100 m
- Communication speed: data rate up to 250 kbps
- Security: AES-128, a unique encryption key for each message
- Manufacturers: ABB, Emerson, Endress+Hauser, Siemens
- Market position: HART is the largest digital industry communications technology. WirelessHART adds wireless capability to HART and maintains compatibility with existing HART communications technology.
- Typical use cases: Smart Factory, Process measurement, and Control applications.

[20], [22]

3.3 Wireless Local Area Network (WLAN)

The Wireless Local Area Network and connections range vary from the tens of meters to the few hundred meters. Wireless Local Area Networks are typically used inside buildings, but also outdoors. Wireless Local Area Networks based on IEEE 802.11 standards are wireless versions of IEEE 802.3 wired Ethernet networks. IEEE 802.11 a/b/g use single-input and single-output (SISO) radios.

Wi-Fi Alliance (from 2000) is the worldwide network of companies that drives global Wi-Fi adoption and evolution and ensures interoperability, security, and reliability. Wi-Fi is one of the greatest successes with billions of devices shipped each year, and global economic value is expected to reach $3.5 trillion by 2023. [51]

History of IEEE 802.11:

- 1997: 802.11 2.4 MHz, typical 2 Mbps / max 2 Mbps, SISO
- 1999: 802.11b 2.4 MHz, typical 11 Mbps / max 11 Mbps, SISO
- 2003: 802.11a 5 MHz, typical 54 Mbps / max 54 Mbps, SISO
- 2003: 802.11g 2.4 MHz, typical 54 Mbps / max 54 Mbs, SISO
- 2008: 802.11n, Wi-Fi 4, 2.4 & 5 MHz, typical 300 Mbps, max 450 Mbps, SU-MIMO
- 2014: 802.11ac wave 1, Wi-Fi 5, 5 MHz, typical 870 Mbps, max 1300 Mbps
- 2016: 802.11ac wave 2, Wi-Fi 5, 5 MHz, typical 1200, max 1700 Mbps
- 2019: 802.11ax, Wi-Fi 6, 2.4 & 5 MHz

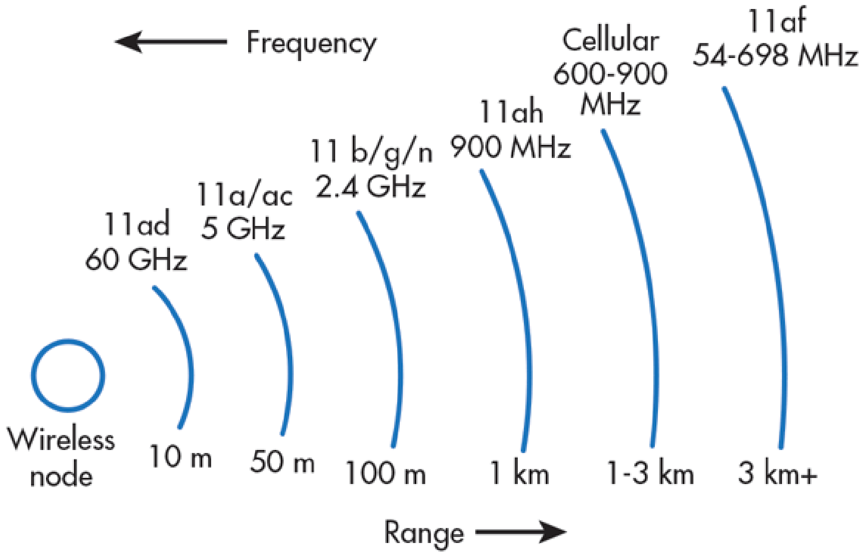


Figure 4. These are the approximate maximum ranges of 802.11 wireless technologies. Environment, obstacles, etc. can shorten or lengthen these ranges. [52] page 1

3.3.1 IEEE 802.11n

IEEE 802.11n was ratified in July 2009, and it is backward compatible with 802.11a, 802.11b, and 802.11g. The IEEE 802.11n provides much better performance than these earlier standards.

With 802.11n, a device can transmit multiple spatial streams at once but only directed to a single address. For individually addressed frames, this means that only a single device (or user) gets data at a time. This technology can be called Single User - Multiple-Input and Multiple-Output (SU-MIMO). MIMO combines multiple send and receive antennas and multiple spatial streams of data sending at the same time.

Wi-Fi Alliance has made a consumer-friendly generation name Wi-Fi 4 for IEEE 802.11n.

Features of Wi-Fi 4 / IEEE 802.11n:

- Power consumption: > 800 mW, in sleeping mode 50 mW
- Standardization: IEEE 802.11n, backward compatible with IEEE 802.11a & IEEE 802.11g
- Single User Multiple-Input and Multiple-Output (SU-MIMO) support (downlink), multiple spatial streams (mandatory 1, max 4)
- Topology: star and mesh networks
- Uses 2.4 and 5GHz, unlicensed ISM spectrum band, multiple channels
- Range: up to 70 m, outdoor 250 m
- Communication speed: Typical 300 Mbps, Product max 450 Mbps, Standard max 600 Mbps
- Modulation: CCK, DSSS, or OFDM
- Channel width: 20 or 40 MHz
- Security: AES-128
- Chip manufacturers: Broadcom, Qualcomm Atheros, MediaTek, Marvell, Intel, Realtek, STMicroelectronics, Texas Instruments, Cypress Semiconductor, Microchip
- Market position: Over billion Wi-Fi chipsets are shipped.
- Typical use cases: Office WLAN and Home WLAN connecting laptops, notebooks, notepads, smartphones, and printers to connect to each other and access the Internet without wires.

[56]

3.3.2 IEEE 802.11ac

IEEE 802.11ac was the next of the IEEE 802.11 standard after 802.11n. IEEE 802.11ac has a new technology called multiuser MIMO (MU-MIMO). Here an Access Point can use its antenna resources to transmit multiple frames to different clients, all at the same time and over the same frequency spectrum. If 802.11n is like a hub, 802.11ac can be thought of as a wireless switch (on the downlink).

Wi-Fi Alliance has made a consumer-friendly generation name Wi-Fi 5 for IEEE 802.11n.

Features of Wi-Fi 5 / IEEE 802.11ac:

- Power consumption: > 900 mW, in sleeping mode 50 mW
- Standardization: IEEE 802.11ac
- Communication speed: Wave1: Typical 870 Mbps, Product max 1300 Mbps, Standard max 6900 Mbps; Wave2 Typical 1730 Mbps, Product max 3500 Mbps, Standard max 6900 Mbps
- RF Bands: 802.11ac is a 5 GHz (unlicensed ISM spectrum band) only technology (so dual-band APs and clients continue to use 802.11n at 2.4 GHz), multiple channels
- Modulation: BPSK, QPSK, 16QAM, 64QAM, or 256QAM (Optional)
- Channel width: 20, 40, 80, or 160 MHz
- Multiuser Multiple-Input and Multiple-Output (MU-MIMO) support (downlink), multiple spatial streams (max 8)
- Topology: star and mesh networks
- Range: up to 70 m, outdoor 250 m
- Modulation: CCK, DSSS, or OFDM
- Channel width: 20, 40, 80, and 160 (Optional) MHz
- Security: AES-128
- Chip manufacturers: Broadcom, Qualcomm Atheros, MediaTek, Marvell, Intel, Realtek
- Market position: Wi-Fi Chipsets market in 2019 was over 16 billion US$
- Typical use cases: Office WLAN and Home WLAN, Wireless Display, Outdoor campus/auditorium, and Manufacturing floor automation

[57]

3.3.3 IEEE 802.11ax

IEEE 802.11ax has maximum compatibility, coexisting efficiently with IEEE 802.11a/n/ac devices. IEEE 802.11ax lets access points to support more clients in dense environments and provide a better experience for typical WLAN networks.

802.11ax has OFDMA, a new channel access mechanism (like cellular/LTE radio networks but in an unlicensed spectrum). OFDMA ensures data transmission to multiple clients both in Downlink (DL) and Reverse (UL).

Access-point can talk to the client (and vice versa) at data rates as low as 375 Kbps, by using only one 2 MHz resource units within 20 MHz channel width. 802.11ax has a new power-saving mode called Target-Wakeup Time (TWT). With TWT, the station can request a schedule to wake up at any time in the future. The result is significant power savings for battery-powered IoT devices.

Wi-Fi Alliance has made consumer-friendly generation name Wi-Fi 6 for IEEE 802.11n.

Features of Wi-Fi 6 / IEEE 802.11ax:

- Power consumption: > 900 mW, in sleeping mode 50 mW. Target Wake Time (TW) allows devices wake up different periods reducing power consumption.
- Modulation: BPSK, QPSK, 16QAM, 64QAM, 256QAM, or 1024 QAM
- Orthogonal Frequency Division Multiple Access (OFDMA)
- Channel width: 20, 40, 80, or 160 MHz
- Standardization: IEEE 802.11ax
- Communication speed: 600 Mbps – 4.8 Gbps
- RF Bands: 2.4 and 5 GHz unlicensed ISM spectrum band, multiple channel
- Modulation: BPSK, QPSK, 16QAM, 64QAM, 256QAM, or 1024 QAM
- Channel width: 20, 40, 80, or 160 MHz
- Multiuser Multiple-Input and Multiple-Output (MU-MIMO), multiple spatial streams (max 12)
- Topology: star and mesh networks
- Range: up to 70 m, outdoor 250 m
- Security: AES-128
- Chip manufacturers: Broadcom, Qualcomm Atheros, Intel, Marvell
- Products: Samsung Galaxy S10 & Galaxy Note 10, Apple iPhone 11 & 11 Pro, Lenovo ThinkPad X1 Extreme Gen 2, HPE Aruba AP-500 series WLAN Access Points, Cisco Catalyst 9100 Access Points, Cisco Meraki MR 45 & MR 55 Access Points
- Market position: 1 billion Wi-Fi 6 chipsets will ship by 2022
- Typical use cases: Office WLAN, High-density WLAN environments, Real-time applications such as 4K video

[58]

3.4 Wireless Wide Area Network (WWAN)

Wireless Wide Area Network refers to mostly outdoor wireless networks with operating distances of more than 1 km. These networks are Mobile networks (2G, 3G, 4G, NB-IoT, LTE-M, 5G), Sigfox, LoRaWAN, and Satellite networks. SMS works over the Mobile networks.

3.4.1 SMS

The Short Message Service (SMS) provides a method for sending messages of limited size (max 160 7-bit characters or 140 8-bit bytes) to and from GSM/UMTS/EPS SMS mobile devices. The mobile device can send SMS to the Short Message Service Center (SMSC), which acts as a store and forward-center for short messages. If the response is inactive, then SMSC will hold the message. The GSM/UMTS/EPS Public Land Mobile Network (PLMN) and 3GPP need to support the transfer of short messages between Short Message Service Centers and mobiles. The SMS message sending started in 1992. Nokia made the first mobile phone that was able to send messages in 1993. IoT devices can use SMS can for asset tracking, as well as environmental and agricultural sensors. By using SMS messages, it is possible to manufacture a device in which battery life is years.

Features of SMS:

- Power consumption: Very-low-power
- Standardization: 3GPP TS 23.040 Short Message Service, 3GPP TS 23.041 Short Message Service – Cell Broadcast (SMS-CB)
- Data size: max 160 7-bit characters or 140 8-bit bytes
- RF Bands: GSM and 3G mobile networks licensed bands
- SMS is cost-friendly
- Very reliable
- Range: Global coverage, all over the world where mobile phone works
- Market position: Over 3 billion devices, most of the mobile phones, can use SMS. New mobile chat applications (like WhatsApp) have reduced the use of SMS in smartphones.
- Typical use cases: Mobile phone text messaging, Product verification, Password confirmation, Appointments, Reminders, Alerts, and IoT device

[59], [69]

3.4.2 Sigfox

Sigfox is a wireless technology and a network service. The name comes from a French company Sigfox that offers its wireless technology as well as a local LPWAN for longer-range IoT applications. Sigfox was founded in 2009. Sigfox Foundation has registered the name “Sigfox for Action” and it develops the open source solutions based on Sigfox and IoT.

SIGFOX radios use ultra-narrowband (UNB) modulation and only transmit short messages at low data rates occasionally. Uplink messages can be up to 12 bytes long, and a node can send up to 140 messages per day. Downlink messages can be up to 8 bytes long, and a node can transmit up to 4 messages per day. Due to its narrow bandwidth and short messages, in addition to its 162-dB link budget, a long-distance of several kilometers is possible.

A Sigfox node device is not attached to a specific base station. The broadcasted messages are received by any base station in the range, typically three base stations. Sigfox network is available in 70 countries, covering most countries in Europe. 6.2 million devices are connected to the Sigfox network, and 13 million messages are collected every day. [28]

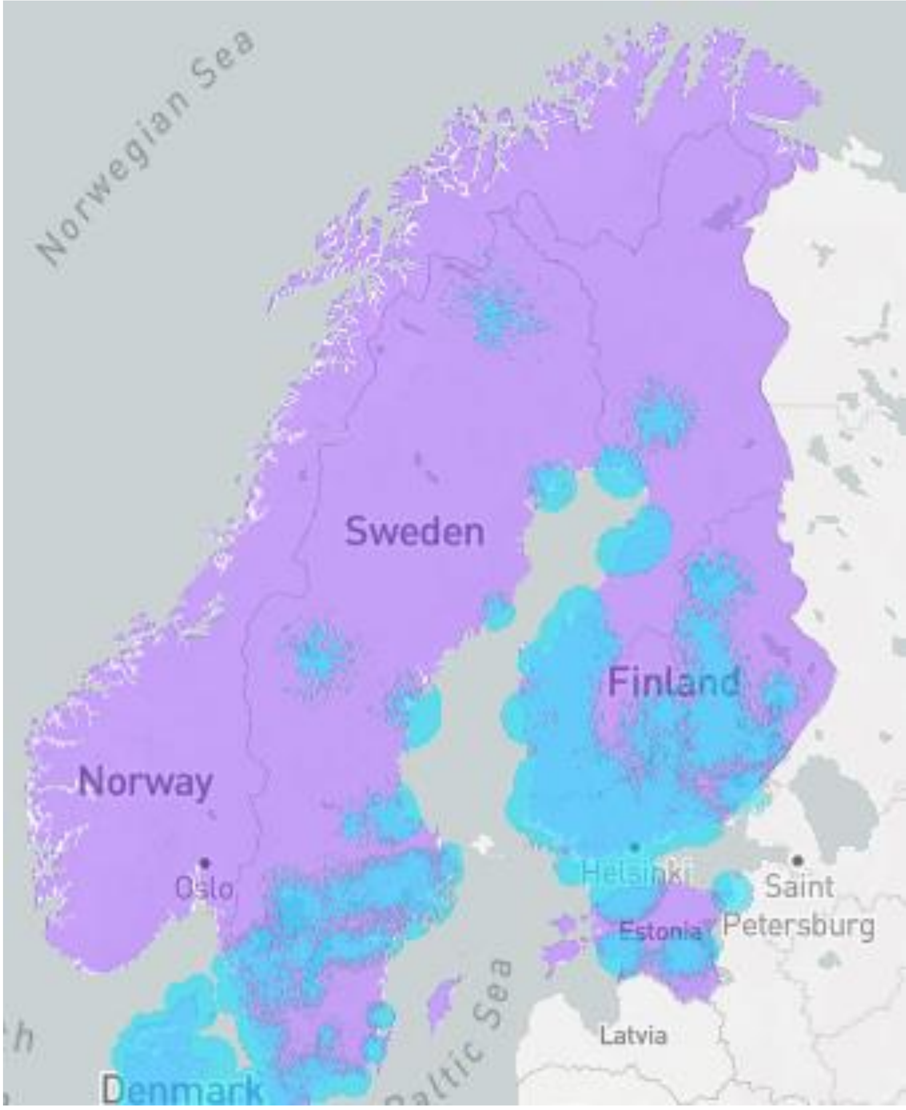


Figure 5 Sigfox network coverage in Finland (24.3.2019) [60]

Features of Sigfox:

- Power consumption: Very-low-power, long device battery life-cycle
- Standardization: Sigfox's proprietary standard
- Data size: Messages can be up to 12 bytes long, and a node can send up to 140 messages per day. Downlink messages can be up to 8 bytes long, and a node can transmit up to 4 messages per day.
- RF Bands: 868, 902, and 928 MHz unlicensed ISM bands
- Low connectivity fee

- Limited bidirectional, Half-duplex
- Network topology: Star
- Each Sigfox base station can handle millions of devices
- Range: 30-50 km
- Security: AES
- Connected Finland Oy is a Sigfox operator in Finland.
- Market position: 26 covered countries in Europe, the U.S., South America, Asia, and Africa and over 400 million end devices
- Typical use cases: Smart metering, Water monitoring, Energy management system, Electric monitoring, Smart waste management, Asset tracking, and Home security

[39], [53]

3.4.3 LoRaWAN

Semtech, founded in 2012, developed LoRa (Long Range) technology. LoRa Physical Layer (PHY) uses an FM chip spread spectrum with Error Correction (FEC). Chirp spread spectrum modulation has long been present in military and space communications due to long communication distances, but LoRa is the first low-cost commercial implementation.

LPWAN (Low Power Wide Area Network) has a multi-year battery lifetime. It is designed for sensors and applications needing to send small amounts of data over long distances a few times per hour from different environments. LoRaWAN is a wireless LPWAN (Low Power Wide Area Network) technology, developed by LoRa Alliance. LoRa is the physical layer enabling the long-range communication link, and LoRaWAN defines the network communication protocol and system architecture. The LoRa Alliance includes hundreds of companies and organizations such as Bosch, Cisco, Google, IBM, NEC, Schneider, Semtech, ZTE, and Digita. LoRaWAN is the right technology for IoT applications where remote locations, easy deployment, thousands of connections per gateway, and long battery life are needed.

The LoRaWAN nodes are asynchronous and communicate only when they have data ready to send, whether event-driven or scheduled. This method reduces power consumption and gives a long battery life. [35]

Features of LoRa:

- Power consumption: Very-low-power, long device battery life-cycle
- Standardization: LoRa’s proprietary open standard
- Data size: Only small packets, 19-250 bytes
- Data rate: Data rates are 0.3–50 kbps for Europe.

- RF Bands: LoRa uses frequencies of 902-928 MHz for the U.S. and 867-869 MHz for Europe unlicensed ISM bands
- Low connectivity fee
- Bidirectional, Halfduplex
- Network topology: Star, star-of-stars
- Digita is a LoRa operator in Finland and uses Digita's national transmission and broadcasting network
- Range: 10-40 km
- Security: LoRaWAN™ protects data and privacy with AES-128 encryption on multiple levels for all data from the sensor to the application server and back.
- Chip manufacturers: Semtech, Microchip
- Market position: 80 million LoRa enabled chips and nodes installed, and hundreds of thousands LoRa gateways installed the end of 2018. [53]
- Typical use cases: Smart metering, Smart Agriculture, Smart Buildings, Smart Cities, Smart Environment, Smart Healthcare, and Smart Home.

[36], [53]

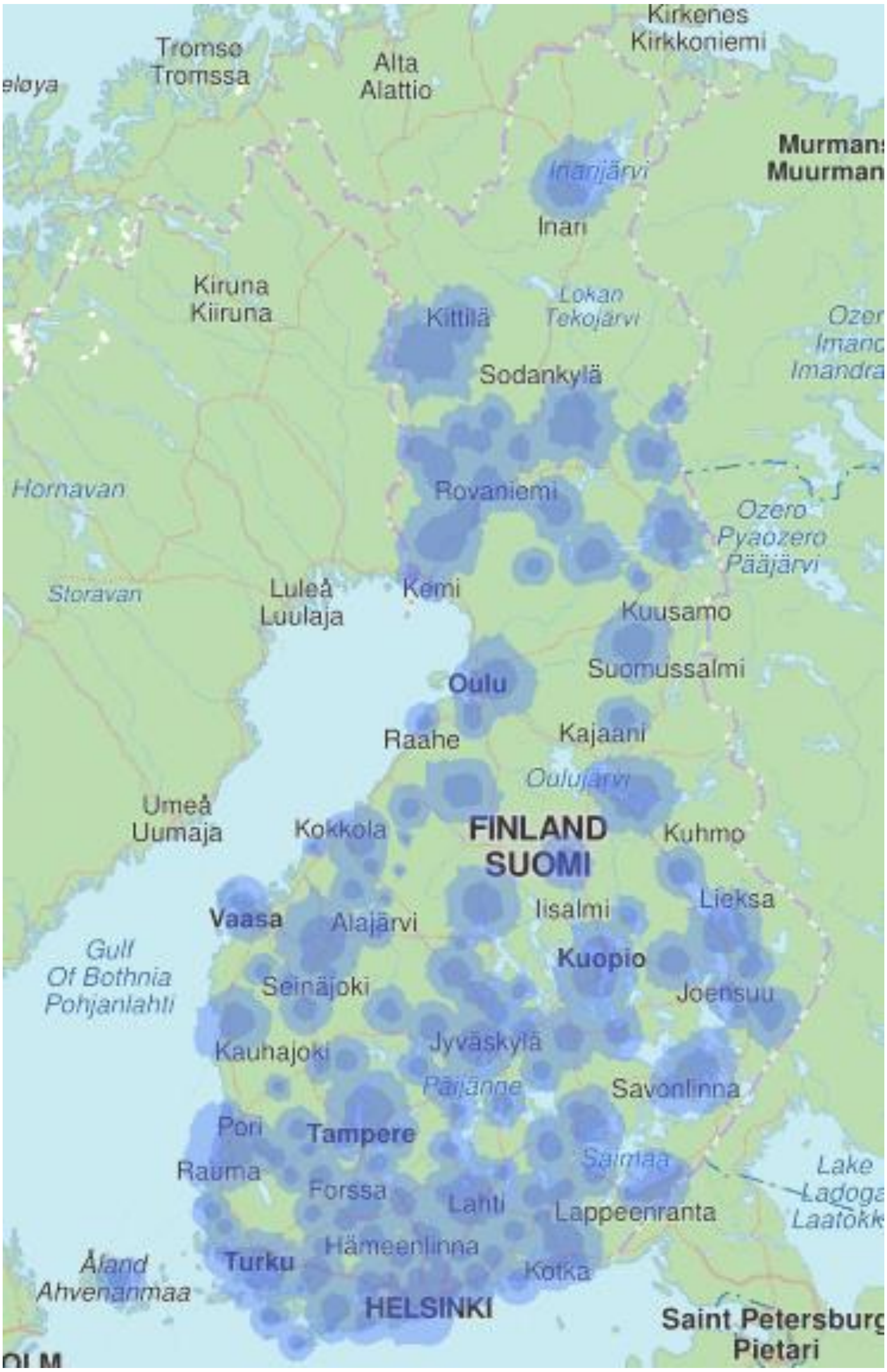
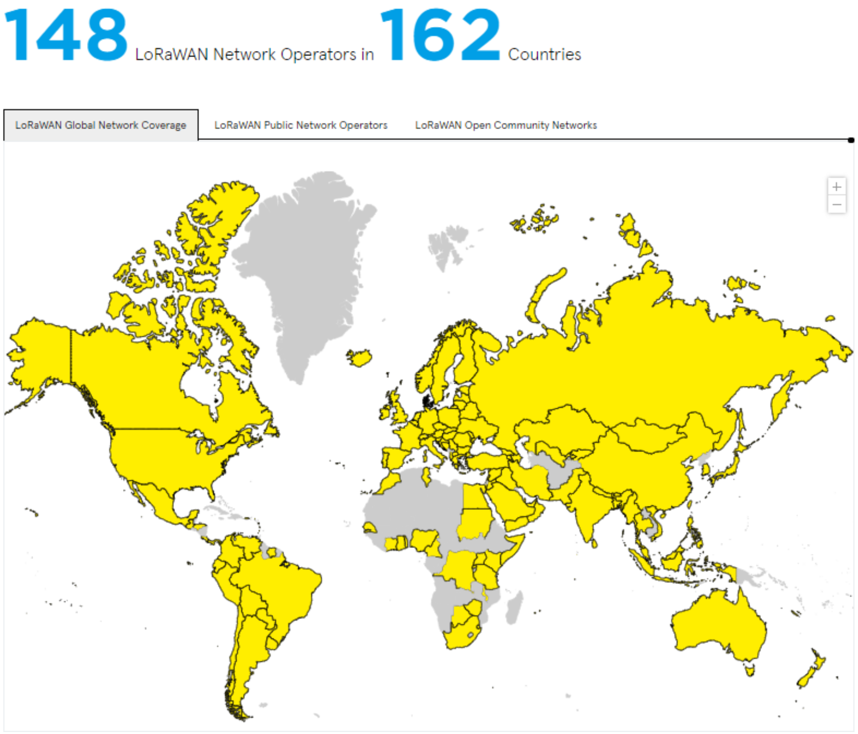


Figure 6 LoRaWAN network coverage in Finland (24.3.2019) [37]

The figure shows the LoRaWAN network coverage in Finland. The technology is comprehensively available throughout Finland in the city areas.



148 LoRaWAN Network Operators in 162 Countries

LoRaWAN Global Network Coverage
LoRaWAN Public Network Operators
LoRaWAN Open Community Networks
+
–

Figure 7 LoRaWAN Global Network Coverage (6.2.2021) [61]

LoRa technology is widely used around the world in urban areas, with the exception of many African countries.

3.4.4 4G (LTE)

4G is a fourth-generation data transmission network provided by mobile operators designed to use Internet connections. 4G is several times faster than the previous 3G network; in Finland, the normal range is 5-100 Mbps, and thus, it replaces fixed DSL-based broadband networks in many places. 4G networks already cover almost 100% of the Finnish population.

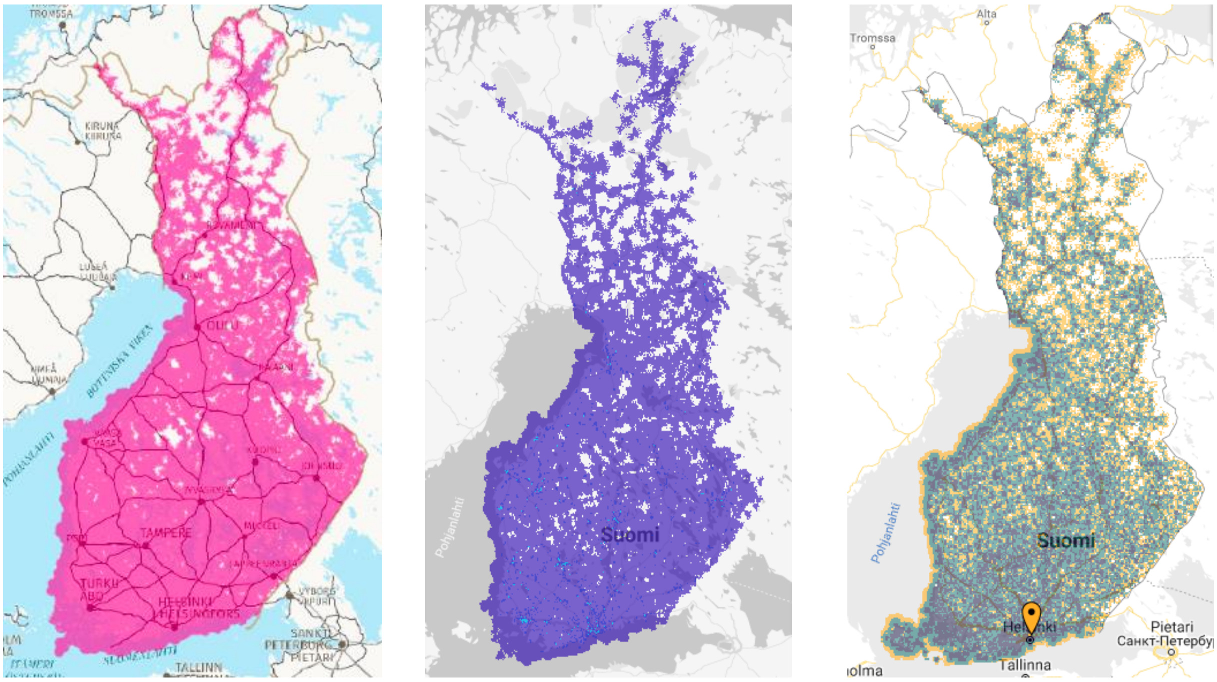


Figure 8 DNA, Elisa and Telia 4G (LTE) networks in Finland (14.4.2019) [44, 43, 42]

There are three 4G operators in Finland, and the 4G networks of all of them cover population centers well. Only sparsely populated areas in the north are out of the coverage network.

Features of 4G:

- Power consumption: Medium
- Standardization: 3GPP Long Term Evolution (LTE) Rel-9 2009, 3GPP LTE Advanced Rel-12 2014
- Data rate: Normal rate 5-100 Mbps
- Latency: less than 10 ms
- RF Bands: 3GPP licensed mobile bands, in Finland 700, 800, 900, 1800, and 2600 MHz bands
- Multiplexing: OFDMA downlink and SC-FDMA uplink
- Modulation: QAM
- Bidirectional, Half-duplex mode
- Network topology: Star
- DNA, Elisa, and Telia are 4G operators in Finland
- Range: up to 10 km
- Security: LTE Encryption

- Typical use cases: Mobile phone/Tablet/PC Internet connections, 4G Internet routers, Remote locations, Digital signage, Industrial sites, and IoT connectivity.

[70]

3.4.5 NB-IoT

Narrowband IoT (NB-IoT) is a low power wide-area network (LPWAN), which enables to connect devices needing low bandwidth, a small amount of data, and long battery life. NB-IoT is a relatively recent variation of using LTE for IoT. NB-IoT uses a 180-kHz-wide resource block, instead of full LTE 10 or 20 MHz bandwidth. Data rates will be in the up to 60 kbps.

NB-IoT provides very low power consumption for connected devices. NB-IoT offers a competitive long-range solution. NB-IoT is supported in Finland, Sweden, Norway, Denmark, most of the other European countries, the US, Turkey, Australia, Brazil, Thailand, South Africa, and Japan.

Features of NB-IoT:

- Power consumption: Low-power, LTE PSM (Power Saving Mode)
- Standardization: 3GPP LTE Cat NB1 Release 13 in 2017
- Data rate: Up to 100 kbps
- Latency: 1.5-10 s
- RF Bands: 3GPP licensed mobile Ultra Narrow Band 800 MHz
- Multiplexing: OFDMA downlink and SC-FDMA uplink
- Modulation: QAM
- NB-IoT is compatible with most of the existing LTE networks (requires software upgrade)
- Bidirectional, Half-duplex mode
- Network topology: Star
- DNA, Elisa, and Telia are NB-IoT operators in Finland.
- Range: up to 10 km
- Security: LTE Encryption
- Chip manufacturers: Qualcomm, Samsung, Intel, HiSilicon, Nordic Semiconductor, Sierra Wireless, and U-Blox.
- Market position: Global NB-IoT device shipments: 53 million in 2018, 142 million in 2019. NB-IoT started from Europe.
- Typical use cases: Smart Parking, Smart metering, Smart Fire Protection, Smart Buildings, and Smart Cities.

[18], [53],

3.4.6 LTE-M

LTE-M (Long Term Evolution-Machine) is a simplified industry term for LTE-MTC (Long Term Evolution-Machine Type Communication) Low Power Broadband (LPWA) technology standard published by 3GPP in Publication 13 specification. It refers explicitly to LTE CatM1, which is suitable for Internet applications. LTE-M is a low-power, wide-area technology that supports the Internet network through reduced device complexity and provides expanded coverage while allowing LTE's installed base to be reused. LPWA allows a battery life of up to ten years in a wide range of applications.

LTE-M is supported nationwide on DNA's and Telia’s mobile networks in Finland. Elisa is upgrading its mobile network to LTE-M in 2020, covering all of Finland’s base stations. The LTE-M is suitable for more real-time applications requiring intermittent higher capacity and long battery life. Such applications typically include remote reading, logistics and healthcare services, and security solutions. LTE-M provides higher throughput rates (<1 Mbps), supports the same power-saving features as the NB-IoT, and provides 5-10 years of battery life for the devices. LTE-M, like NB-IoT, is a technology dedicated to IoT devices in both 4G and 5G standards.

The standard LTE network is overkill for essential monitoring and control cases. LTE-M is a simplified version that can provide solutions for M2M applications with maximum data rates of 1 Mb/s.. LTE-M uses the existing LTE bandwidths with orthogonal frequency-division multiple-access (OFDMA) modulation. This long-range solution is capable of kilometres of distance.

Features of LTE-M:

- Power consumption: Low-power, LTE PSM (Power Saving Mode)
- Standardization: 3GPP LTE-MTC low power wide area, Release 13
- Data rate: Data rates are up to 1 Mbps uplink
- Latency: 50-100 ms
- RF Bands: 3GPP licensed mobile bands B3 (1800 MHz), B8 (900 MHz), and B20 (800 MHz)
- Multiplexing: OFDMA downlink and SC-FDMA uplink
- Modulation: QAM
- Bidirectional, Half Duplex
- Network topology: Star
- LTE-M is supported nationwide on DNA's and Telia’s mobile networks in Finland. Elisa is upgrading its mobile network in Finland to LTE-M in 2020.
- Mobility: Yes
- Voice: Yes, LTE-M also supports voice over 4G network (VoLTE, Voice over LTE).
- Range: up to 10 km
- Security: LTE Encryption
- Chip manufacturers: Qualcomm, Intel, Altair, and Nordic Semiconductor.

- Typical use cases: Logistics, Smart Healthcare, and Automotive.

[33], [53], [55],

3.4.7 5G

5G (5th Generation) is a 3GPP definition for a new digital cellular network. It supersedes 2G, 3G, and 4G technologies. 5G is a new generation mobile network that revolutionizes how we use and utilize mobile networks and mobile devices. 5G is up to 10 times faster than 4G, so transferring videos, movies, and other massive files is fast.

At 5G, the delay is minimal, making it a completely new experience, for example, playing on a 5G network. The use of remote-controlled devices is also comfortable and at all possible. The reliability of the 5G network is better than the existing networks, where the use of services and applications is uninterrupted. 5G enables many times lower costs per gigabyte than 4G. 5G Release 15 also specifies further enhancements on Critical Communications (including Ultra-Reliable Low Latency Communication and Highly Reliable Low Latency Communication), Machine-Type of Communications (MTC) and Internet of Things (IoT), Vehicle-related Communications (V2X), and Mission Critical (MC).

Finland entered the 5G in January 2019, when the licenses were granted to operators: DNA, Elisa, and Telia.

DNA opened the 5G network in Helsinki in January 2019. DNA's 5G services are currently available in Helsinki, Vantaa, Tampere, Turku, and Hyvinkää. DNA's 5G network will be public in more than 20 locations during the first half of 2020.

Elisa has already opened 5G networks in Tampere, Helsinki, Jyväskylä, Turku, Pori, Seinäjoki, Vaasa, Kuopio, Oulu, and Kuusamo.

Telia was the first operator to open the 5G network in Helsinki, Oulu, and Vantaa in autumn 2018. The 5G was launched on 5th September 2018 in Helsinki in cooperation with Nokia at the Telia 5G Arena, which used the 5G network for real-time multi-video broadcasting. In November 2018, Telia opened a 5G network in Oulu, which supports the industry and logistics operator’s ecosystem in the region in developing digital operating models and innovations.

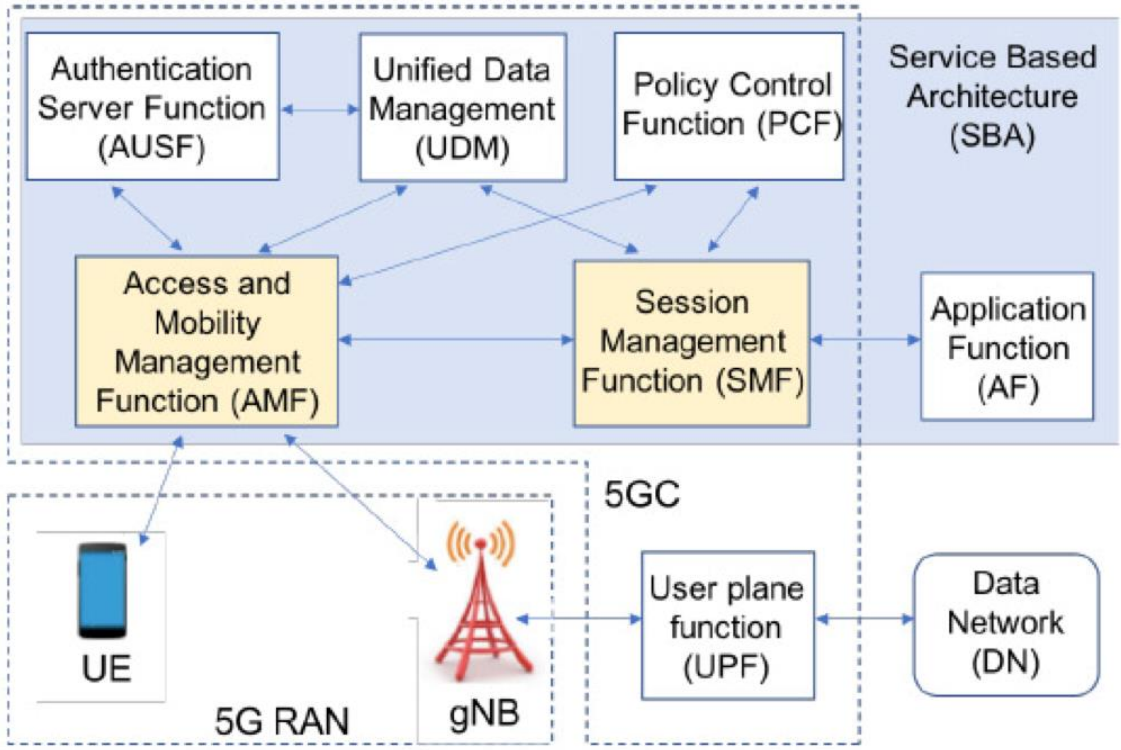

Authentication Server Function (AUSF)
Unified Data Management (UDM)
Policy Control Function (PCF)
Service Based Architecture (SBA)
Access and Mobility Management Function (AMF)
Session Management Function (SMF)
Application Function (AF)
5GC
UE
5G RAN
gNB
User plane function (UPF)
Data Network (DN)

Figure 10. Simplified 5G reference network architecture [4G and 5G networks security techniques and algorithms, page 37]

Features of 5G:

- Power consumption: Small to Medium
- Standardization: 3GPP standard for 5G New Radio (NR) Non-standalone 2017
- Data rate: Over 100 Mbps
- Latency: 1 - 10 ms
- RF Bands: 3GPP licensed mobile bands, in Finland 1.9-2.1 GHz, 2.5-2.6 GHz, 3.4-3.8 GHz bands
- Multiplexing: OFDMA
- Modulation: QAM
- Bidirectional, Full-duplex or Half-duplex mode
- SMS support
- Network topology: Star
- DNA, Elisa, and Telia are 5G operators in Finland
- Range: up to 1 km
- Security: LTE Encryption, 5G security enhancements

Typical use cases are Automotive, Transport, Logistics, IoT, Public Safety, Health and wellness, Smart cities, and Media and entertainment.

[46], [47], [48]

3.4.8 Satellite

A communications satellite is placed in Earth’s orbit. It creates a communication channel source between transmitter and receiver at various locations worldwide to transmit and receive data. Television, telephone, radio, Internet, and military applications use satellites to communicate. There are over 2000 communications satellites in Earth’s orbit, used by both private and government organizations. [49]

Low Earth Orbit (LEO) is a circular orbit from 200 to 2000 km above Earth. SpaceX’s Starlink and Swarm Technologies operate in this area, and these satellites orbit the Earth in about 90 minutes.

Medium Earth Orbit (MEO) is a circular orbit from 2000 to 35786 km above Earth. Examples are GPS (24 satellites, orbit Earth every 12 hours at 20200 km), Glonass (20 satellites, orbit Earth every 12 hours at 19100 km), Galileo (22 satellites, orbit Earth every 14 hours at 23222 km).

Geosynchronous Orbit is a circular orbit 35768 km above Earth. The satellite orbits the Earth at the same speed as Earth’s rotational speed; the satellite seems to stay in place according to Earth. There are over 400 satellites in Geosynchronous Orbit.

High Earth Orbit (HEO) is a circular orbit above geosynchronous orbit (35786 km). Examples of satellites are Vela 1A and IBEX. Their rotational speed is lower than Earth’s rotational speed.

The high-frequency radio waves used for telecommunications links travel by line of sight and are thus obstructed by the curve of the Earth. The purpose of communications satellites is to allow communication between widely separated geographical points. International organizations have regulations for which frequency ranges or "bands" specific satellite organizations can use, which minimizes the risk of signal interference.

Skylogic has 24 satellites that provide coverage to over 150 countries, reaching 90% of the world’s population. Skylogic offers bi-directional satellite connections that allow companies worldwide to solve the communications problem in areas with no other possibilities. [50]

As of 1 March 2020, SpaceX has launched 302 Starlink satellites, with a target of 12 000 total. The idea of a global Internet satellite network to an altitude of 550 km. Satellites are communicating with each other using lasers. One satellite can handle an area of 500 km diameter range.

Swarm Technologies, founded in 2016, is creating a low-cost satellite network for IoT use, like Agriculture, Energy, Transportation, Shipping and Maritime, and Connected Cars. They already have seven satellites in orbit, and they have the plan to deploy 150 in total. Satellite’s altitudes are 450-550 km.

Satellite navigation is a system that makes use of artificial satellites for providing autonomous geospatial positioning. Global Navigation Satellite System (GNSS) refers to a combination of satellites that offer space signals that send positioning and timing information to GNSS receivers.

The receivers then use this data to determine location. By definition, GNSS provides global coverage. Examples of GNSS include Europe’s Galileo, the USA’s NAVSTAR Global Positioning System (GPS), Russia’s Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), and China’s BeiDou Navigation Satellite System.

4 Home Automation Project

This chapter describes the implementation of a home automation system and what was learned from it. The Home Automation Project’s focus was to find out the support of home devices for various wireless technologies and how a home automation system can utilize and control their information.

4.1 Tested Devices and Wireless Techniques

The table lists home environment devices and their wireless and wired network interfaces. NFC is used for contactless payments. Zigbee is the wireless technique for the IKEA Trådfri system. Bluetooth is used for the Jabra Evolve 75 headphones connected to the iPhone, iPad, and MacBook. Bluetooth is also used for the Toyota Auris car connection to the iPhone. Wi-Fi is used for iPhone, iPad, MacBook, Lenovo PC, Sony Bravia 55" TV, Elisa Viihde Digibox N7950, and Arlo Pro2 Camera connections to the Asus ZenWi-Fi AC router. Ethernet is used for Arlo Base Station, IKEA Trådfri Gateway, and Raspberry Pi 3 Model B connections to the Asus ZenWi-Fi AC router. The Asus ZenWi-Fi AC router is connected to the Internet using a 100 Mbps fiber Ethernet connection.

Table 3: Devices and connections in the home environment

Device / Connections	NFC	Bluetooth	ZigBee	Wi-Fi	GSM/3G	4G	GNSS	Ethernet RJ-45
Apple iPhone 8	NFC	Bluetooth 5.0	-	802.11ac, 802.11n	GSM/EDGE	LTE Advanced	GPS/GNSS	-
Apple iPad 3rd generation	-	Bluetooth 5.0	-	802.11ac, 802.11n	-	-	GPS/GNSS	-
AppleTV 4K	-	Bluetooth 5.0	-	802.11ac, 802.11n	-	-	-	Gigabit Ethernet RJ-45
Apple Macbook Air 2017	-	Bluetooth 4.0	-	802.11ac, 802.11n	-	-	-	-
Lenovo ThinkPad	-	-	-	802.11ac, 802.11n	-	-	-	10/100 Mbps Ethernet RJ-45
Sony Bravia 55" TV	-	-	-	802.11n	-	-	-	10/100 Mbps Ethernet RJ-45
Elisa Viihde digibox N7950	-	-	-	802.11ac, 802.11n			-	10/100 Mbps Ethernet RJ-45
Asus ZenWi-Fi AC router	-	-	-	802.11ac, 802.11n			-	Gigabit Ethernet RJ-45

Arlo Base Station	-	-	-	802.11ac, 802.11n			-	10/100 Mbps Ethernet RJ-45
Arlo Pro2 Camera	-	-	-	802.11ac, 802.11n			-	-
IKEA Trådfri Gateway	-	-	ZigBee	-	-	-	-	10/100 Mbps Ethernet RJ-45
IKEA Trådfri lamp	-	-	ZigBee	-	-	-	-	-
IKEA Trådfri socket	-	-	ZigBee	-	-	-	-	-
Toyota Auris	-		-	802.11n	-	-	GPS/GNSS	
Raspberry Pi 3 Model B	-	Bluetooth 4.1	-	802.11n	-	-	-	10/100 Mbps Ethernet RJ-45
Jabra Evolve 75 head-phones	-	Bluetooth 4.0	-	-	-	-	-	-
Credit and payment cards with contact-less payment	NFC	-	-	-	-	-	-	-

4.2 Home Automation Systems

The study looked at four different home automation systems: IKEA Smart Home, Apple HomeKit, Arlo Surveillance Camera System, and Home Assistant software solution.

4.2.1 IKEA Smart Home

IKEA Smart Home consists of Trådfri-Gateway device, Trådfri Remote controller and ZigBee wireless network remotely controlled devices: Trådfri lamps (monochrome, color), Trådfri socket, Trådfri motion detector, Float led light panels, and Fyrtur blackout curtains. The test configuration included one Trådfri Gateway (connected with an Ethernet cable to WLAN access point and there to the Internet), one Trådfri Remote controller, two pcs Trådfri Led lamps 600 lm (color/white spektrum, dimmable), one Trådfri Led-lamp 250 lm (warm glow spectrum, dimmable) and one Trådfri socket. The IKEA Home Smart app works on Apple IOS (at least iOS 9) and Android devices (at least Android 4.4). The Trådfri Remote controller is used for remote controlling lamps and also pair new smart devices (light, socket, etc.) to the Trådfri Gateway and IKEA Home Smart app. IKEA Trådfri also works with Apple HomeKit.

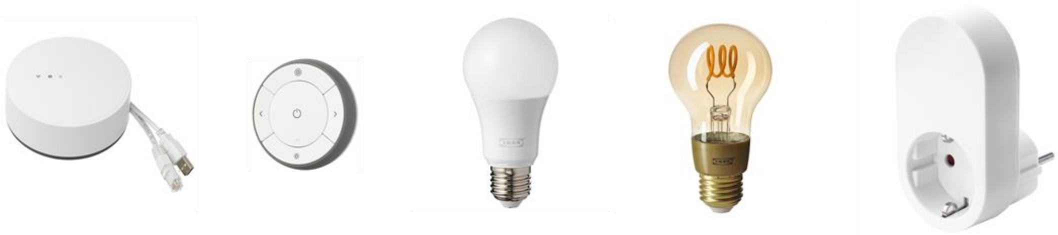


Figure 11 Trådfri Gateway, Remote controller, lamps, and socket

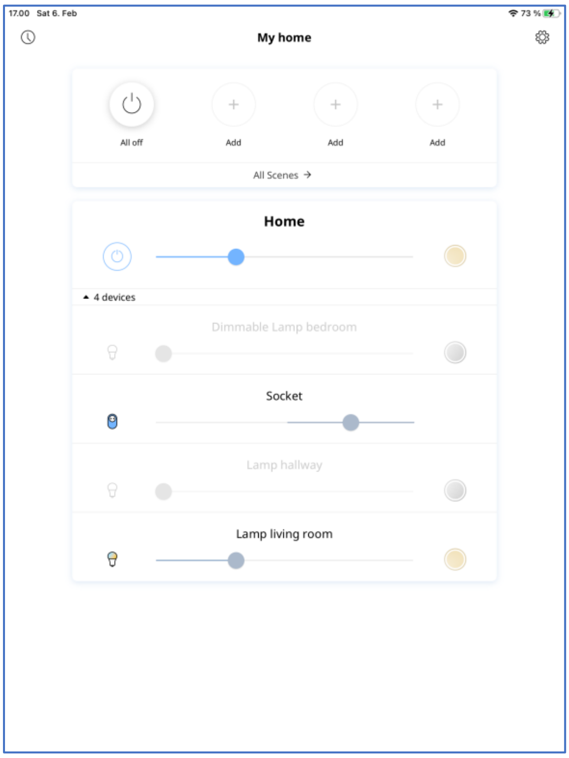


Figure 12 IKEA Home Smart App

With the IKEA Home Smart app (both Android and iOS versions), it is possible to manually control devices or create automatic setups. There are three different automatic setups: Wake-up (sets devices to wake up to a new day, the lights start to brighten slowly 30 minutes before the set time), Light & Dark (select the desired start and end times to increase or decrease the home lighting), and Away from home (sets the lights and the blackout curtains to rise and fall as if you were at home). With Light & Dark, it is possible to automate the car's engine heater on and off at the desired time by commanding the Trådfri socket. IKEA Trådfri Gateway uses WLAN to connect to the IKEA Home Smart App and other App like Apple Home Kit. Wireless connections between Gateway and lamps and sockets are based on ZigBee Light Link.

The following automations can be performed with the IKEA Home Smart App:

1. Warm the car at the mornings using the socket and Schedule a Timer function:
    - What time?
        - Start the timer at: 07:00

        - Stop the timer at: 8:00
    - Which day?
        - Mo, Tu, We, Th, Fr
    - Which devices?
        - Socket
2. Wake-up lighting at the mornings using the lamp and Rise and shine function:
    - What time?
        - Start at: 07:15
    - Which day?
        - Mo, Tu, We, Th, Fr
    - Which devices?
        - Bedroom’s lamp
        - Brightness: 40%

[62]

4.2.2 Arlo Security Camera System

Figure 13 Arlo Base Station and two Arlo Pro2 cameras

The Arlo Pro 2 system is a truly wireless and easy-to-use surveillance system with a Base station and two Full HD (1920 x 1080) cameras. The Arlo base station is connected with an Ethernet RJ-45 cable to a network device connected to the Internet and via a WLAN connection to the Arlo Pro 2 cameras. Arlo Pro 2 cameras can be used with either batteries or AC power. The cameras are suitable for both indoor and outdoor use.

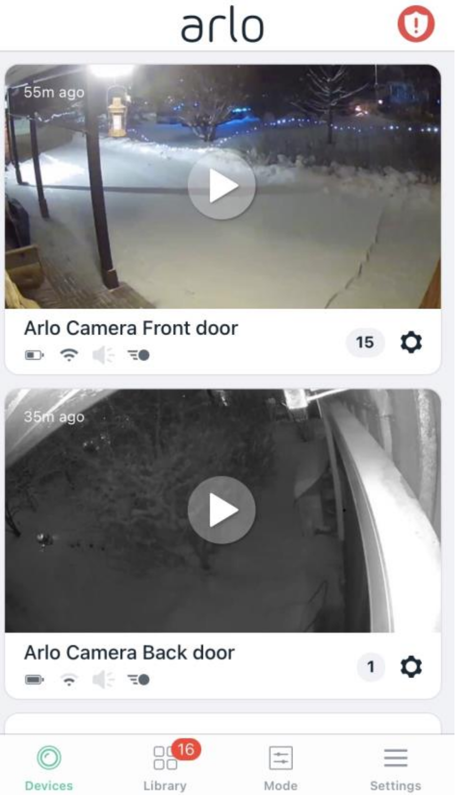


Figure 14 Arlo mobile application

The cameras have motion detection and voice detection, and the home station supports both local and manufacturer cloud recording. A separate mobile application (Android / iOS) can manage the system. Thanks to the camera's built-in motion sensor and sound sensor, it is possible to set automatic warnings, notifications, or e-mails when the camera detects movement or sound. Arlo Pro 2 supports several other commonly used protocols and services, including IFTTT, Apple HomeKit, and Amazon Alexa.
[63]

4.2.3 Apple HomeKit

HomeKit is Apple's home automation solution that allows access and connecting different smart devices through Apple's Home app. HomeKit devices can be used and managed on Macs and iOS devices. It is possible to automate the functions of different devices, control devices with Siri, and create different rules and automation. The Apple HomeKit device selection includes sensors, sockets, lamps, thermostats, and cameras from various well-known equipment manufacturers. [64]

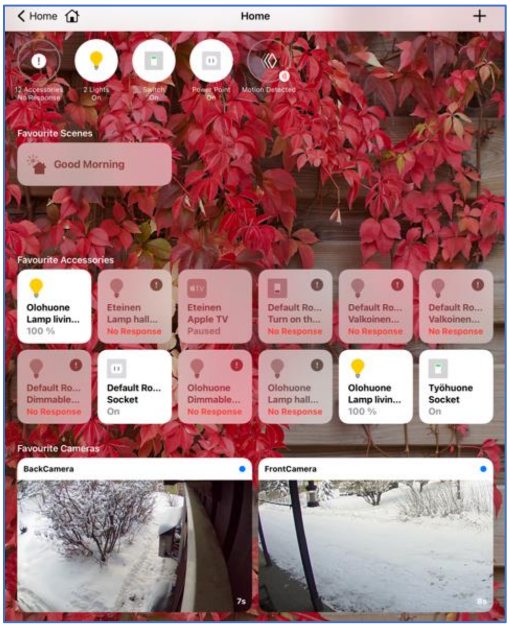

Home
Home
+
12 Accessories No Response
2 Lights On
Switch On
Power Point On
Motion Detected
Favourite Scenes
Good Morning
Favourite Accessories
Olohuone Lamp livin... 100 %
Eteinen Lamp hall... No Response
Eteinen Apple TV Paused
Default Ro... Turn on th... No Response
Default Ro... Valkoinen... No Response
Default Ro... Valkoinen... No Response
Default Ro... Dimmable... No Response
Default Ro... Socket On
Olohuone Dimmable... No Response
Olohuone Lamp hall... No Response
Olohuone Lamp livin... 100 %
Työhuone Socket On
Favourite Cameras
BackCamera
FrontCamera
7s

Figure 15 Apple Home app

It is possible to add IKEA Trådfri Gateway to the Apple Home app and then use the Apple Home app to control IKEA Trådfri devices like lamps and sockets. It is also possible to add the Arlo camera system to the Apple Home app to use the camera’s motion detection as a trigger for automation and use cameras.

There are five different automation types for own automation creations:

1 **People Arrives (someone from the family arrives to empty house)**

Action: Anyone comes (can use the location information of family member’s smartphones and tablets)
Location: Home
Time: Any
Action: Can select Scenes like “We Are at Home” or directly control IKEA lamps, sockets, etc.

2 **People Leaves (Everyone has left home)**

Action: Everyone leaves (can use the location information of family member’s smartphones and tablets)
Location: Home
Time: Any
Action: Can select Scenes like “We Are Left Home” or directly control IKEA lamps, sockets, etc.

3 **Time Automation**

When: Sunrise, Sunset, or exact Time of Day, Repeat (Mo, Tu, We, Th, Fr, Sa, Su)

Action: Can select Scenes like “Good Morning” or directly control IKEA lamps, sockets (Car warming), etc.

4 **Accessory Automation**

Trigger: Choose the accessory (turn on/off the lamp, socket, etc.) that will start this automation

Time: Any time, During the day, At night, or Specific times

People: Off, When I am home, When I am not home

Action: Can select Scenes like “Home” or directly control IKEA lamps, sockets, etc.

5 **Sensor Automation**

Trigger: Choose the sensor that will start this automation (Arlo camera’s motion detection etc)

When: Detects motion, Stops Detecting Motion

Time: Any time, During the day, At night, or Specific times

People: Off, When I am home, When I am not home

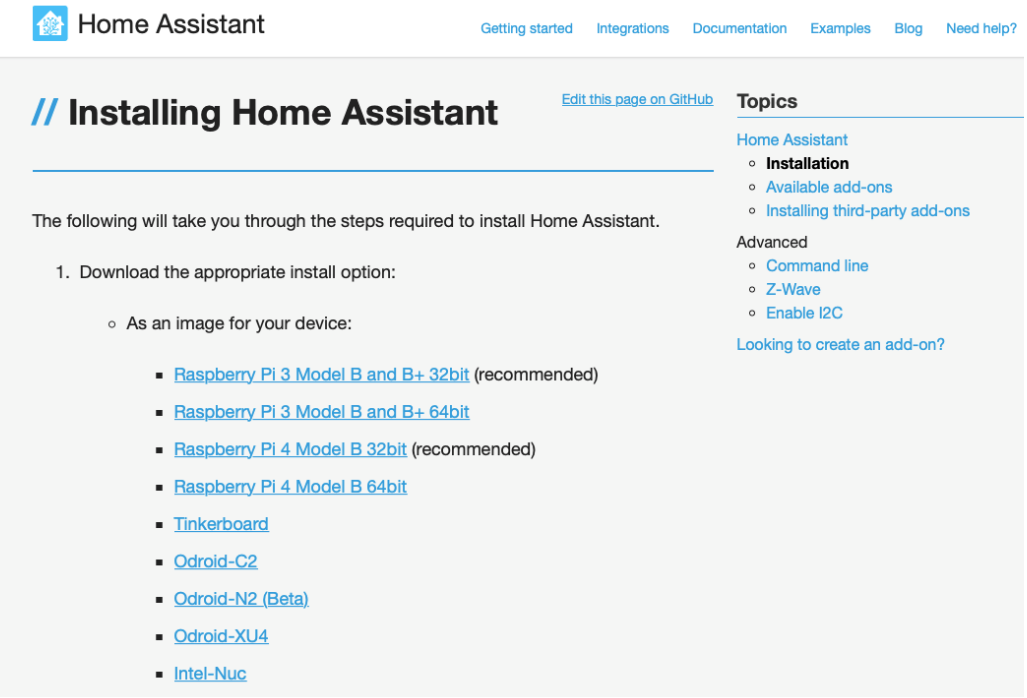
Action: Can select Scenes like “Surprise” or directly control IKEA lamps, sockets, etc.

4.2.4 Home Assistant

The Home Assistant (https://www.home-assistant.io) software was chosen as Home Automation Software because it is an open system, it supports a variety of hardware brands. It can be controlled and programmed in many ways. The Raspberry Pi 3 Model B was chosen as the hardware platform because it can be used for different Linux based systems. It is inexpensive and widely used and available. For the installation, the needed system was the Raspberry Pi 3 Model B, 32 GB Micro SD memory card, MacBook Air (PC is another option), and the Internet connection.

Figure 16 Raspberry Pi 3 Model B [54]

The Home Assistant HassOS Image (Raspberry Pi 3 Model B and B+ 32bit) was downloaded from <home-assistant.io>.



Home Assistant

Getting started · Integrations · Documentation · Examples · Blog · Need help?

// Installing Home Assistant

Edit this page on GitHub

The following will take you through the steps required to install Home Assistant.

1. Download the appropriate install option:
   - As an image for your device:
     - Raspberry Pi 3 Model B and B+ 32bit (recommended)
     - Raspberry Pi 3 Model B and B+ 64bit
     - Raspberry Pi 4 Model B 32bit (recommended)
     - Raspberry Pi 4 Model B 64bit
     - Tinkerboard
     - Odroid-C2
     - Odroid-N2 (Beta)
     - Odroid-XU4
     - Intel-Nuc

Topics

Home Assistant
- Installation
- Available add-ons
- Installing third-party add-ons

Advanced
- Command line
- Z-Wave
- Enable I2C

Looking to create an add-on?

Figure 17 Home Assistant

The downloaded image was flashed to a 32 GB SD card using balenaEtcher software.

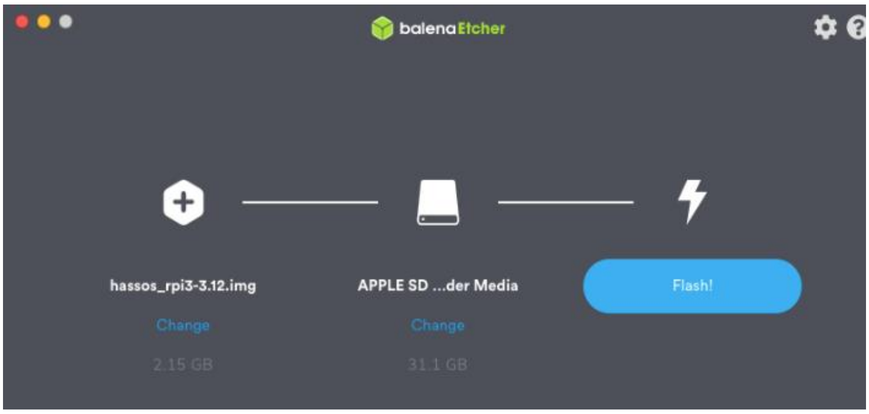
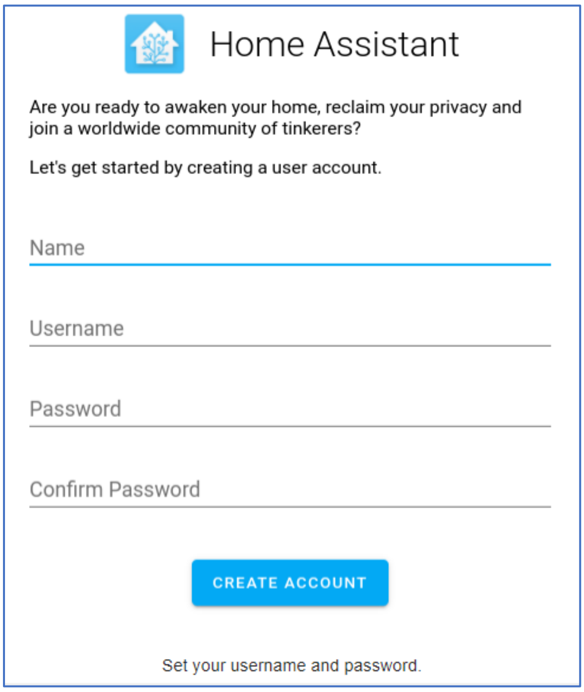


Figure 18 Flash the image to an SD card using balenaEtcher.

Then SD card was installed to Raspberry Pi 3, which was connected to the Internet (Ethernet connection to the Asus Zen Wi-Fi AC Router, which was connected to the Internet). Then the power supply was connected to the Raspberry Pi 3 with a USB cable. Raspberry Pi 3 boots up, connects to the Internet and downloads the latest version of Home Assistant. This phase takes about 20 minutes. After that, it is possible to configure Home Assistant using a web browser, it is available at address http://homeassistant.local:8123 or http://x.x.x.x:8123 (use Raspberry Pi's real IP address instead of x.x.x.x).



Home Assistant

Are you ready to awaken your home, reclaim your privacy and join a worldwide community of tinkerers?

Let's get started by creating a user account.

Name

Username

Password

Confirm Password

Set your username and password.

Figure 19 Home Assistant

At the first connection, a user account is created. After login, it is possible to add the integrations to the system. The Home Assistant community provides over 1700 different integrations.

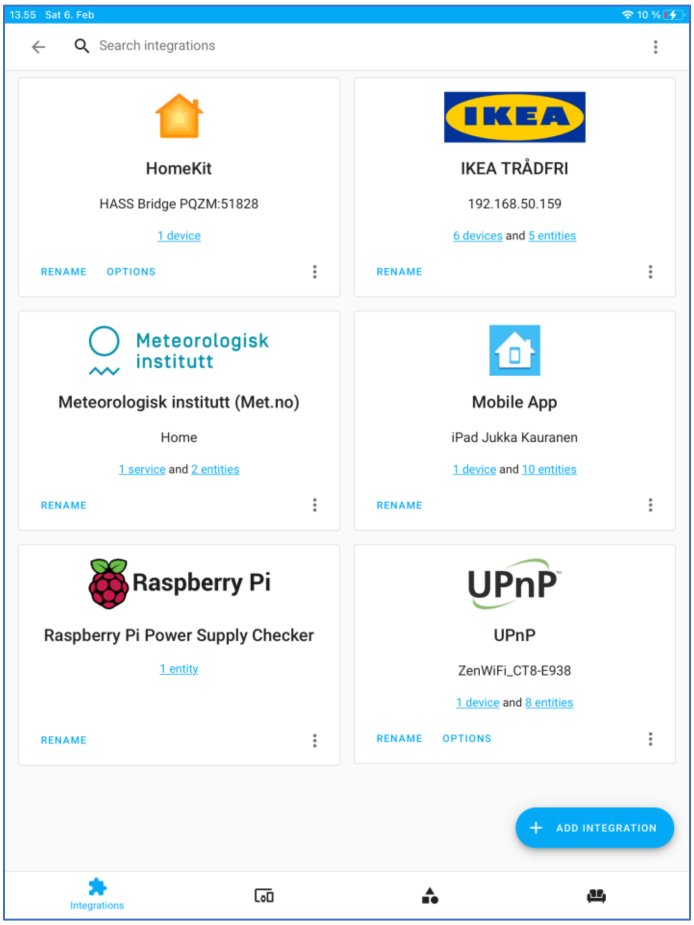
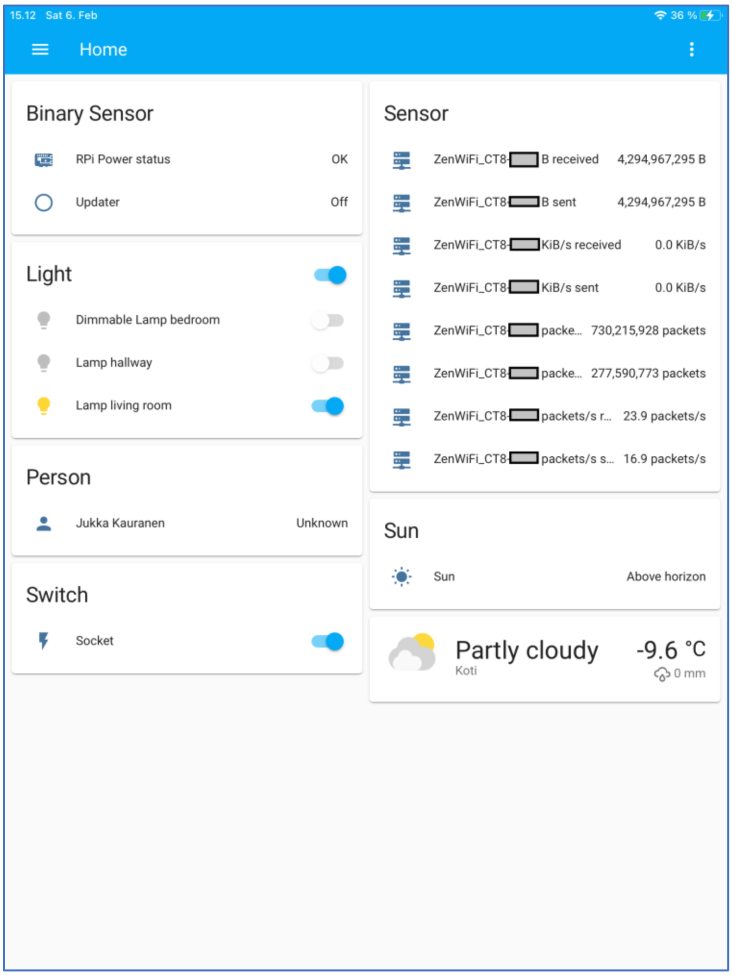


Figure 20 Home Assistant Integrations

The Home Assistant App was installed on iPhone and iPad. The Home Assistant found the following integrations: Apple HomeKit, Ikea Trådfri, Raspberry Pi, Asus ZenWi-Fi, Meteorologist institute, and Home Assistant Mobile App in iPad. After integrations, it is possible to manage Home Assistant either using the web application or using Mobile App.

The Home Assistant structure is three-level:

1) Integrations to the different systems, like IKEA Trådfri
2) Devices, like IKEA Trådfri Gateway, lamp, and socket
3) States, like light.lamp_living_room = on



15.12 Sat 6. Feb

36 %

Home

Binary Sensor

RPi Power status OK

Updater Off

Light

Dimmable Lamp bedroom

Lamp hallway

Lamp living room

Person

Jukka Kauranen Unknown

Switch

Socket

Sensor

ZenWiFi_CT8-[redacted]B received 4,294,967,295 B

ZenWiFi_CT8-[redacted]B sent 4,294,967,295 B

ZenWiFi_CT8-[redacted]KiB/s received 0.0 KiB/s

ZenWiFi_CT8-[redacted]KiB/s sent 0.0 KiB/s

ZenWiFi_CT8-[redacted]packe... 730,215,928 packets

ZenWiFi_CT8-[redacted]packe... 277,590,773 packets

ZenWiFi_CT8-[redacted]packets/s r... 23.9 packets/s

ZenWiFi_CT8-[redacted]packets/s s... 16.9 packets/s

Sun

Sun Above horizon

Partly cloudy -9.6 °C

Koti 0 mm

Figure 21 Home Assistant Mobile App

The Home Assistant interface shows all the integrated devices, and it is possible to command devices directly from the home page. The automation rules can be made from the user interface Configuration => Automation, where it is possible to create a new automation. It is relatively easy to develop new automation, which can be edited. Home Assistant uses the YAML syntax for configurations. YAML (YAML Ain't Markup Language) is a human-friendly data serialization standard for all programming languages. [66].

Three different automation created: Lights on in the evening, Lights on in the workday morning, and Warm car in the cold mornings.

Lights on every evening in YAML code. Automation uses the sunset as a trigger condition, which is retrieved from the Norwegian Meteorological Institute. When the sunset happens, the living room lamp is turned on.

```
- id: '1612213xxxxxx'
alias: Turn on the lights every evening when the sun is set
  description: ''
  trigger:
  - platform: sun
    event: sunset
  condition:
  - condition: time
    weekday:
    - mon
    - tue
    - wed
    - thu
    - fri
    - sat
    - sun
  action:
  - domain: light
    entity_id: light.lamp_living_room
    device_id: a364a1dff5c1d85a601d336a94xxxxxx
    type: turn_on
    brightness_pct: 30
  mode: single
```

Lights on in the workday mornings in YAML code. Automation uses time and day of the week as the trigger condition. When the trigger condition happens, then the bedroom lamp is turned on.

```
- id: '161224312'
alias: Lights on in the workday mornings
  description: ''
  trigger:
  - platform: time
    at: 07:00
  condition:
  - condition: time
    weekday:
    - mon
    - tue
    - wed
    - thu
    - fri
  action:
  - domain: switch
    entity_id: dimmable_lamp_bedroom
    device_id: a364a1dff5c1d85a601d336a96xxxxxx
    type: turn_on
  mode: single
```

Car warming in the cold workday mornings. Automation uses the time (07:00), outdoor temperature (below 0 ºC), and day of the week (only workdays) as the trigger condition. When the trigger condition happens, then the socket is turned on. The car's heating cord is plugged into the socket. The car has an engine heater. Car warming is turned off at the triggered time (08:00). **Warning: this IKEA socket is only for indoor use and max 3840W power.**

```
- id: '1612330xxxxxx'
  alias: Car warming on in the cold workday mornings
  description: ''
  trigger:
  - platform: numeric_state
    entity_id: weather.koti
    attribute: temperature
    below: '0'
  condition:
  - condition: time
    after: 07:00
    weekday:
    - mon
    - tue
    - wed
    - thu
    - fri
  action:
  - type: turn_on
    device_id: 0d8dc5d435921c1fb275083402xxxxxx
    entity_id: switch.socket
    domain: switch
  mode: single

- id: '1612621xxxxxx'
  alias: Car warming off
  description: ''
  trigger:
  - platform: time
    at: 08:00
  condition:
```

```
- condition: time
  weekday:
  - mon
  - tue
  - wed
  - thu
  - fri
action:
- type: turn_off
  device_id: 0d8dc5d435921c1fb275083402xxxxxx
  entity_id: switch.socket
  domain: switch
mode: single
```

[65]

4.3 Conclusion from Project

The project found that many of electrical devices used in homes already have some form of wireless communication available. There are many alternative solutions for implementing home automation, and many of them also support different brands of devices. The necessary environment used in the project (IKEA Trådfri Gateway/lamps/socket, Raspberry Pi 3 Model B & Home Assistant software) can be bought for less than 200 Euros. Thus almost anyone interested in IoT Automation can start studying and applying with them. A positive surprise in the project was how well different brands of devices are supported in these Automation systems and how easy it is to implement basic functionality. Implementing more versatile and complex automation requires more imagination, construction, and programming. The system used in the project enables the connection of a wide variety of devices and useful automation implementation.

5 Results and Analysis

As a result, the study concluded that there are various needs and requirements in the IoT environment. Several different wireless solutions are needed to solve these. The commonly used techniques below can address over 80% of different needs and requirements.

The following criteria were used to select wireless solutions to the list:

- The answer should be an open standard with multiple manufacturers and suppliers
- The solution must have features that other solutions on the list cannot implement
- The solution must be available and widely used in a wide geographical area
- The answer must be usable now and will continue to evolve in the future

Table 4: Recommendations

Standard	Typical use cases
NFC	Near Field Communication (NFC) is a newer, more finely modified version of RFID. NFC can be categorized into two classes: 1) Passive NFC – which has not a power source and 2) Active NFC – devices that can send as well receive data. NFC devices can be used in commerce for contactless payments and electronic tickets, for electronic identity documents and keycards, for smart NFC tags and gaming. Range up to 10 cm.
RFID	Radio Frequency Identification (RFID) is used mostly for tags or labels attached to the objects. RFID tags can be passive, active (has a battery), or battery-assisted passive. RFID devices can be used for item identification in manufacturing, logistics, stores, and sports. Different ranges for passive RFID tags: close-range 1 cm, remote range from 1 cm to 1 m, long-range more than 1 m. The range of active RFID tags from few meters to 100 m.
Bluetooth	Bluetooth comes in two radios: Classic and Low Energy. Bluetooth Classic enables wireless printers, wireless headsets, and wireless speakers. The range of Bluetooth Classic is from few meters to 10 m. Bluetooth Low Energy (BLE) uses less power and enables areas such as health care, heart rate monitoring, smartphones, beacons, and IoT devices. The typical range of BLE is from 10 m to 100 m. Security: 128-bit AES.
802.15.4	802.15.4 standard-based wireless networks are ZigBee, Thread, WirelessHART, and Wi-SUN. ZigBee is currently the most common of these. ZigBee is a high-level communication protocol used to create personal area networks with small, low-power digital radios. ZigBee is an open wireless standard from the ZigBee Alliance and was established in 2004. Typical use cases: Home automation, Smart lighting, Smart energy, building automation, health care, and status reading applications. The range is up to 100 m. Security: AES-128. For outdoor and commercial use, it is worth exploring other options: Thread, WirelessHART, and Wi-SUN.
Wi-Fi	Wi-Fi Alliance (from 2000) is the worldwide network of companies that drives global Wi-Fi adoption and evolution and ensures interoperability, security, and reliability. Wi-Fi is one of the greatest successes, with billions of devices shipped each year. Typical use cases: Office WLAN and Home WLAN, Wireless Display, Outdoor campus/auditorium, and Manufacturing floor automation. There are many versions of Wi-Fi that are compatible downwards. Wi-Fi 4 / IEEE 802.1n, typical speed 300 Mbps, range up to 70 m. Wi-Fi 5 / IEEE 802.1ac, typical speed 870 Mbps, range up to 70 m. Wi-Fi 6 / IEEE 802.1ax, typical speed 1 Gbps, range up to 70 m. Security: AES-128.

SMS	The Short Message Service (SMS) provides a method for sending messages of limited size (max 160 7-bit characters or 140 8-bit bytes) to and from GSM/UMTS/EPS SMS mobile devices. Typical use cases: Mobile phone text messaging, Product verification, Password confirmation, Appointments, Reminders, Alerts, and IoT device. IoT devices can use SMS can for asset tracking, as well as environmental and agricultural sensors. SMS works almost anywhere in the world where there is a mobile network and in every mobile phone.
4G	4G is a fourth-generation data transmission network provided by mobile operators designed to use Internet connections. 4G is several times faster than the previous 3G network; in Finland, the normal range is 5-100 Mbps, and thus, it replaces fixed DSL-based broadband networks in many places. 4G networks already cover almost 100% of the Finnish population. Range: up to 10 km. Security: LTE Encryption
NB-IoT	Narrowband IoT (NB-IoT) is a low power wide-area network (LPWAN), enabling connected devices needing low bandwidth, a small amount of data, and long battery life. NB-IoT is a variation of using LTE for IoT. Typical use cases: Smart Parking, Smart metering, Smart Fire Protection, Smart Buildings, and Smart Cities.Data rate: Up to 100 kbps. Range: up to 10 km. Power consumption: Low-power, LTE PSM (Power Saving Mode). Security: LTE Encryption.
5G	5G (5th Generation) is a 3GPP definition for a new digital cellular network. It supersedes 2G, 3G, and 4G technologies. 5G is a new generation mobile network that revolutionizes how we use and utilize mobile networks and mobile devices. Typical use cases: Automotive, Transport, Logistics, IoT, Public Safety, Health and wellness, Smart cities, and Media and entertainment. Data rate: Over 100 Mbps. Latency: 1 - 10 ms. Range: up to 1 km. Security: LTE Encryption, 5G security enhancements
GNSS	Satellite navigation is a system that makes use of artificial satellites for providing autonomous geospatial positioning. Global Navigation Satellite System (GNSS) refers to a combination of satellites that offer space signals that send positioning and timing information to GNSS receivers. By definition, GNSS provides global coverage. Examples of GNSS include Europe’s Galileo, the USA’s NAVSTAR Global Positioning System (GPS), Russia’s Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), and China’s BeiDou Navigation Satellite System.

However, not all technical and commercial needs can be addressed with these, and it is worth exploring other alternative solutions. The technology is also continually evolving, and thus there will also be new solutions in the future.

6 Discussions, Conclusion, and Further Improvements

Electronics and circuit technology have evolved. It is possible to build a chip made with 5 nm technology and in one circuit up to more than 11 billion transistors (like the new Apple iPad Air A14 Bionic chip). This allows for more versatile features, better performance, and better perfordemance/power consumption. The wireless network can already be found on many different devices: alarm system, automation, camera, car, climate system, device automation, doorbell, energy, fan, geolocation, health device, heating, headphone, humidifier, light, lock, mobile phone, notepad, sensor, tablet, TV, watch, etc.

Energy consumption is one of the essential requirements for the design and implementation from the IoT application. Message sending and idle power consumption is the most critical factor in battery life. Battery technology is continuously evolving due to electric cars, and also energy harvesting is an excellent opportunity for IoT devices. The energy harvesting circuit could be incorporated into the chip to produce clean, unrestricted, low-voltage current for small devices or sensors. The energy harvesting sources can be thermal, solar, motion, wind, radiofrequency, and sound. [66], [67]

Using licensed mobile networks have to pay fees based on usage or traffic volumes, some of which are returned to the community as operator’s license fees. The society also benefits from the use of mobile networks for individuals, businesses, and organizations.

In the future, the frequencies released after the 2G and 3G networks’ shutdown can be used to expand the 4G and 5G networks. The new satellite networks will enable good telecommunications connections even outside populated areas. Likewise, many of today’s wireless technologies (Bluetooth, Wi-Fi, 5G) will evolve.

Technical solutions for implementing IoT-based commercial solutions exist. Likewise, applications for building using both edge computing and cloud technology are readily available at a reasonable cost. All that is needed now is courage and imagination to carry out both technically and commercially practical projects.

System security must be involved in design, implementation, and production. Disable unused networks & ports, change the default passwords to long passwords, and use two-factor authentication (2FA) when possible. Remember what Sgt. Philip Freemason Esterhaus on the 1981-1987 police drama Hill Street Blues said: **“Let's be careful out there.”**

References

1 Dhillon H. S., Huang H., Viswanathan H.: Wide-area Wireless Communication Challenges for the Internet of Things. IEEE Communications Magazine 10.1109/MCOM.2017.1500269CM. February 2017

2 Wade Trappe: Security for Low-End IoT Devices: When Energy is Not Enough, What is One to Do? WiSec 2015 keynote. <http://www.sigsac.org/wisec/WiSec2015/cfp/WiSec2015_keynote_Dr.Trappe.pdf> Accessed 27.11.2017.

3 Faisal Fayyaz Qureshia, Rahat Iqbalb Muhammad, Nabeel Asgharc: Energy efficient wireless communication technique based on Cognitive Radio for Internet of Things. Journal of Network and Computer Applications, Volume 89, Pages 14-25. July 2017. <https://www-sciencedirect-com.ezproxy.metropolia.fi/science/article/pii/S10848045173000481> Accessed 27.11.2017.

4 Rob van der Meulen: Gartner News, Feb 2017. <https://www.gartner.com/newsroom/id/3598917>. Accessed 27.11.2017

5 Keith D. Foote: A Brief History of the Internet of Things, August 16, 2016. <https://www.dataversity.net/brief-history-internet-things/> Accessed 3.3.2018.

6 Weldon M.: The future X network a Bell Labs perspective. CRC press. Version Date: 20160127

7 Azamuddin: Survey on IoT Security. <https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec2.pdf>. Accessed 18.1.2020

8 Tarmo Anttalainen, Ville Jääskeläinen: Introduction to communication networks, 2015.

9 Steve Ranger: The future of telecommunications is open.<https://www.mwrf.com/community/article/21849065/are-there-too-many-shortrange-wireless-standards> Accessed 16.2.2020

10 Lou Frenzel: Are There Too Many Short-Range Wireless Standards? <https://www.electronicdesign.com/technologies/iot/article/21801725/12-wireless-options-for-iotm2m-diversity-or-dilemma> Accessed 16.2.2020

11 Welcome to Ant+. <www.thisisant.com> Accessed 16.2.2020

12 RFID4U, <https://rfid4u.com/rfid-basics-resources/basics-rfid-regulations/> Accessed 28.12.2018

13 Draft ETSI EN 302 208 v3.1.0 (2016-02). <https://www.etsi.org/deliver/etsi_en/302200_302299/302208/03.01.00_20/en_302208v030100a.pdf> Accessed 16.2.2020.

14 RFIDWorld, RFID Market Projected to Double to $22 Billion USD by 2020. <https://www.rfidworld.ca/new-report-rfid-market-projected-to-double-to-22-billion-usd-by-2020/2493> Accessed 16.2.2020.

15 Martin Woolley, Bluetooth 5 / Go Faster. Go Further. <https://3pl46c46ctx02p7rzdsvsg21-wpengine.netdna-ssl.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf> Accessed 22.02.2020

16 LED driven: ZigBee versus Z-Wave. <http://www.leddriven.nl/de/ledwiki/16-zigbee-versus-z-wave> Accessed 22.02.2020

17 IEEE Standards Association, IEEE Standard for Low-Rate Wireless Networks, IEEE Std 802.15.4-2015

18 How Wi-SUN® Compares with LoRaWAN® and NB-IoT <https://www.wi-sun.org/wp-content/uploads/Wi-SUN-Comparing-IoT-Networks.pdf>. Accessed 22.2.2020

19 Wi-SUN Alliance <https://www.wi-sun.org>. Accessed 22.2.2020

20 Wireless Industrial Networking Alliance, Choosing the right wireless technology for industrial applications. <https://www.pharmamanufacturing.com/assets/wp_downloads/pdf/WINAWebinarWireless.pdf>. Accessed 22.2.2020

21 Renesas, Sub-GHz Wireless Communications Solutions <https://www.renesas.com/eu/en/img/misc/catalogs/pdf/r30pf0141ej0100-sub-ghz.pdf> Accessed 22.2.2020

22 Yehan Ma, Cyper-Physical Systmes Laboratory, Intorduction of WirelessHART. <https://www.cse.wustl.edu/~lu/cse521s/Slides/wirelesshart.pdf>. Accessed 22.2.2020

23 HART – Digital transformation for analog instruments. <https://fieldcommgroup.org/technologies/hart> Accessed 22.2.2020

24 Sesia S., Toufik I., Baker M., LTE: The UMTS Long Term Evolution: From Theory to Practice, Second Edition. John Wiley & Sons. 2009.

25 ETSI. Mobile-edge Computing, White paper. <https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf>. Accessed 17 Dec 2015.

26 Mark Weiser, The Computer in the 21st Century, Sep 1991. <http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf>. Accessed 3.3. 2018

27 Friedermann Mattern, Christian Floekemeier, From the Internet of Computers to the Internet of Things. <http://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf>

28 10.23919/ICACT.2017.7890183, Authors: Mangal Sain, Young Jin Kang, Hoon Jae Lee, Survey on Security in Internet of things: state of the art and challenges, February 2017. Pages 699 – 704

29 Bluetooth SIG, Bluetooth market update 2018

30 Bluetooth SIG, Bluetooth 5, Go Faster, Go Further. December 2016

31 802.15.4-2015, <https://ieeexplore-ieee-org.ezproxy.metropolia.fi/stamp/stamp.jsp?tp=&arnumber=7460875> Accessed 30.12.2018.

32 What’s The Difference Between ZigBee And Z-Wave? Electronic Design, Lou Frenzel, Thu, 2012-03-29 10:35

33 Long Term Evolution for Machines: LTE-M. <https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/> Accessed 13.1.2019

34 Mobile IoT Deployments, <https://www.gsma.com/iot/deployment-map/>, Accessed 13.1.2019

35 About LoRa Alliance <https://lora-alliance.org/about-lora-alliance> Accessed 24.3.2019

36 What is LoRaWAN <https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf> Accessed 24.3.2019

37 Digita IoT LoRaWAN <https://www.digita.fi/yrityksille/iot/iot_lorawan-verkon_peittokartta> Accessed 24.3.2019

38 Connected Finland <http://www.connectedfinland.fi> Accessed 24.3.2019

39 Sigfox 0G network on track to establishing a standard <https://www.sigfox.com/en/news/sigfox-0g-network-track-establishing-standard> Accessed 24.3.2019

40 What is Thread. <https://www.threadgroup.org> Accessed 24.3.2019

41 Global 802.15.4 IoT Markets Report 2018. <https://www.prnewswire.com/news-releases/global-802-15-4-iot-markets-report-2018--300648621.html> Accessed 24.3.2019

42 Telia kuuluvuuskartta <https://www.telia.fi/asiakastuki/verkko/verkko/verkkokartta> Accessed 14.4.2019

43 Elisa kuuluvuuskartta. <https://elisa.fi/kuuluvuus/<https://elisa.fi/kuuluvuus/> Accessed 14.4.2019

44 DNA peittokartta. <https://www.dna.fi/peittokartta> Accessed 14.4.2019

45 Joonas Järvinen: IoT-verkkoteknologioiden vertailu. <https://www.theseus.fi/bitstream/handle/10024/128159/Jarvinen_Joonas.pdf>

46 Nokia: 5G technologies will transform your network. <https://networks.nokia.com/5g>

47 DNA: 5G – entistäkin nopeampi ja viiveetön verkko.<https://www.dna.fi/5g-verkko>

48 Elisan 5G-verkko. <https://elisa.fi/5g/>

49 What is GNSS? <https://www.gsa.europa.eu/european-gnss/what-gnss> Accessed 22.2.2020

50 Skylogic a Eutelsat company <http://www.skylogic.it> 22.2.2020

51 Wi-Fi Alliance: Who We Are. <https://www.wi-fi.org/who-we-are>

52 Lou Frenzel: What's the Difference Between IEEE 802.11ah and 802.11af in the IoT?, Jul 17 2017, <https://www.electronicdesign.com/industrial-automation/article/21805297/whats-the-difference-between-ieee-80211ah-and-80211af-in-the-iot>.

53 NB-IoT / LTE-M Issues Boost LoRa / Sigfox Market Share for IoT Networks. <https://www.everythingrf.com/News/details/8443-NB-IoT-LTE-M-Issues-Boost-LoRa-Sigfox-Market-Share-for-IoT-Networks> Accessed 29.2.2020

54 Raspberry Pi 3 Model B <https://www.raspberrypi.org/products/raspberry-pi-3-model-b/ > Accessed 6.2.2021

55 GSM Assocation: LTE-M Deployment Guide to Basic Feature Set Requirements. <https://www.gsma.com/iot/wp-content/uploads/2018/04/LTE-M_Deployment_Guide_v2_5Apr2018.pdf> Accessed 29.2.2020

56 IEEE 802.11n WLAN Standard <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11n.php> Accessed 29.2.2020

57 IEEE 802.11ac Gigabit Wi-Fi <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ac.php> Accessed 29.2.2020

58 IEEE 802.11ax Wi-Fi 6 <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ax.php> Accessed 29.2.2020

59 Telia Kontakti SMS Service Description, 2019-10-10

60 Sigfox network coverage <https://www.sigfox.com/en/coverage> Accessed 24.3.2020

61 LoRaWAN Global Network Coverage <https://lora-alliance.org/> Accessed 6.2.2021

62 IKEA Home smart app & TRÅDFRI gateway support. <https://www.ikea.com/gb/en/customer-service/product-support/app-gateway/> Accessed 6.2.2021

63 Arlo Pro2 Wireless Camera. <https://www.arlo.com/en-us/products/arlo-pro-2/default.aspx> Accessed 6.2.2021

64 Apple Your home at your command. <https://www.apple.com/uk/ios/home/> Accessed 6.2.2021

65 Home Assistant <https://www.home-assistant.io> Accessed 6.2.2021

66 YAML: YAML Ain't Markup Language <https://yaml.org/ > Accessed 6.2.2021

67 University of Arkansas: Physicists Build Circuit That Generates Clean, Limitless Power From Graphene. <https://news.uark.edu/articles/54830/physicists-build-circuit-that-generates-clean-limitless-power-from-graphene> Accessed 30.1.2021

68 Hassan Elahi, Khushboo Munir, Marco Eugeni, Sofiane Atek, and Paolo Gaudenzi: Energy Harvesting towards Self-Powered IoT Devices, 22 Oct 2020

69 3GPP: Technical realization of the Short Message Service (SMS), release 16, 2020-07

70 ETSI: Long Term Evolution (LTE). <https://www.etsi.org/technologies/mobile/4g> Accessed 6.2.2021