UPC

telecom BCN

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

UNIVERSITAT POLITÈCNICA DE CATALUNYA

PROJECTE FINAL DE CARRERA

Security Issues in Internet of Things

Estudis: Enginyeria de Telecomunicació

Autor: Oriol Solà Campillo

Director/a: Ilker Demirkol

Any: 2017

Table of contents

Collaborations

Department of Network Engineering. Telecom BCN, UPC (Universitat Politècnica de Catalunya).

UPC
UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Acknowledgments

I would like to thank:

My wife for her endless patience and determination to encourage me to finish my studies despite having already been working for several years.

My parents for the education I have received from them and for the possibility they have given me to study the career I wanted.

Professor Ilker Demirkol for offering and supervising this study in spite of the situation and the short time available.

Director of studies Sandra Bermejo for her kind guidance in getting the opportunity to finish my studies and to the rector Enric Fossas Colet to allow me to do it.

Resum del Projecte

La idea principal darrera del concepte d'Internet de les coses (IoT) és connectar tot tipus d'objectes quotidians, per permetre comunicar-se entre sí i que les persones es comuniquin amb ells. IoT és un ampli concepte que engloba una extensa gamma de tecnologies i aplicacions. Aquest document dona una introducció al que és el IoT, les seves característiques fonamentals i les tecnologies que s'estan utilitzant actualment.

No obstant, les tecnologies utilitzades en el IoT encara estan evolucionant i madurant, donant lloc a grans reptes que s'han de resoldre per a un desplegament exitós del IoT. La seguretat és un dels reptes més significatius.

Els problemes de seguretat poden representar el major obstacle per l'acceptació general de l'IoT. Aquest document presenta una avaluació dels objectius de seguretat en el Iot, les seves amenaces i els requisits necessaris per assolir aquests objectius. Es realitza un estudi sobre un conjunt representatiu de tecnologies IoT en ús per avaluar el seu estat actual respecte a la seguretat. Per cada solució, es dona una descripció de la seva funcionalitat, les seves proteccions i els problemes trobats. Finalment, s'identifiquen els problemes comuns i es donen un conjunt de solucions futures.

Resumen del Proyecto

La idea principal detrás del concepto de Internet de las cosas (IoT) es conectar todo tipo de objetos cotidianos, para permitir comunicarse entre sí y que personas se comuniquen con ellos. IoT es un amplio concepto que abarca una extensa gama de tecnologías y aplicaciones. Este documento da una introducción a lo que es el IoT, sus características fundamentales y las tecnologías que se están utilizando actualmente.

Sin embargo, las tecnologías usadas en el IoT todavía están en evolución y madurando, dando lugar a grandes desafíos que deben resolverse para un despliegue exitoso del IoT. La seguridad es uno de las más significativos.

Los problemas de seguridad pueden representar el mayor obstáculo para la aceptación general del IoT. Este documento presenta una evaluación de los objetivos de seguridad en el IoT, sus amenazas y los requisitos necesarios para alcanzar dichos objetivos. Se realiza un estudio sobre un conjunto representativo de tecnologías IoT en uso para evaluar su estado actual respecto a la seguridad. Para cada solución, se da una descripción de su funcionalidad, sus protecciones y los problemas encontrados. Finalmente, se identifican los problemas comunes y se dan un conjunto de soluciones futuras.

Abstract

The main idea behind the concept of the Internet of Things (IoT) is to connect all kinds of everyday objects, thus enabling them to communicate to each other and enabling people to communicate to them. IoT is an extensive concept that encompasses a wide range of technologies and applications. This document gives an introduction to what the IoT is, its fundamental characteristics and the enabling technologies that are currently being used.

However, the technologies for the IoT are still evolving and maturing, leading to major challenges that need to be solved for a successful deployment of the IoT. Security is one of the most significant ones.

Security issues may represent the greatest obstacle to general acceptance of the IoT. This document presents an assessment of the IoT security goals, its threats and the security requirements to achieve the goals. A survey on a representative set of already deployed IoT technologies is done to assess the current state of the art with regards to security. For each solution, a description of its functionality, its security options and the issues found in the literature is given. Finally, the common issues are identified and a set of future solutions are given.

List of tables

List of figures

1. Introduction

1.1. Project context

IoT technologies and devices are being widely deployed. 500 billion devices are expected to be connected to the Internet by 2030 [1]. The number and variety of applications is increasing too: from environmental sensing to smart home control and autonomous cars.

The basic concept behind the IoT is to connect all kinds of everyday objects, thus enabling them to communicate to each other and enabling people to communicate to them. They will also be equipped with sensors or actuators in order to interact with the physical world.

However, the technologies for the IoT are still evolving and maturing. There are a plethora of specifications and standards. So, a lot of technical difficulties need to be solved for a successful deployment. One of the most significant challenge in IoT is security.

1.2. Objectives

During this project a general understanding of the Internet of Things concept is gained, describing its fundamental characteristics, the enabling technologies and the challenges and issues to its deployment. An assessment of the IoT security needs is devised and the security of a representative set of already deployed IoT networking solutions is performed.

The results of this study can be used as a starting point for anyone who wants to analyze the security aspects of different IoT networking solutions.

1.3. Document structure

This document is divided in the following chapters:

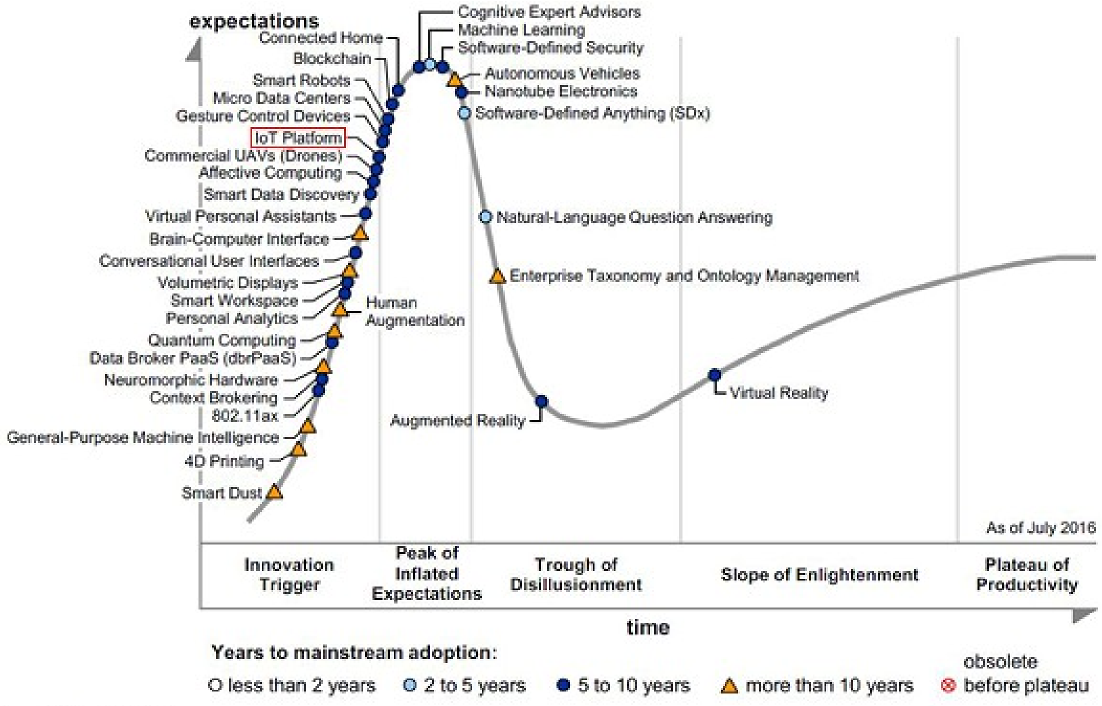
- Chapter 2 “Background“ gives a general view on what is the IoT, its fundamental characteristic and applications. Then, a description of the enabling technologies is given, especially focusing on the IoT networking solutions. Lastly, the challenges to a successful IoT deployment are introduced.
- Chapter 3 “Security for the IoT“ gives an introduction and discusses the security challenges to the IoT. It describes the security goals the IoT need to enforce, its related threats and the security requirements to achieve the goals.
- Chapter 4 “Security survey on networking technologies“ shows the results of a survey of the security options and found issues of the set of existing IoT networking technologies on the market today. For each solution, a description of its functionality, its security options and the issues found in the literature is given.
- Chapter 5 “Analysis of the survey results” presents an analysis of the results of the survey comparing all the solutions to each other. Then, a discussion on the issues that are common to all the surveyed technologies and some future solutions are presented.
- Chapter 6 “Conclusions” presents the conclusions of this study.

2. Background

This chapter presents the current state of the Internet of Things. Firstly, the term is introduced along with its fundamental characteristics, its applications, a general architecture and a set of its enabling technologies. Finally, an overview of the issues that the deployment of the IoT is facing is presented.

2.1. The Internet of Things

The term Internet of Things, from now on IoT, is seen as an emerging topic of technical, social and economic significance. Over the past few years, the IoT appeared across the world both in general and specialized magazines. There are lots of articles describing its potential to transform our daily lives by combining Internet connectivity with consumer product, cars, sensors and other everyday objects.



Source: Gartner (July 2016)

Figure 2.1: IoT as an emerging technology

In 2014 IoT ranked top in Gartner hype cycle [2] for emerging technologies and slightly below in 2016 [3]. With different available technologies, IoT developments may select different communication methodologies and architectures.

Projections for the impact of IoT on the Internet and economy are impressive, according to Cisco, 500 billion devices are expected to be connected to the Internet by 2030 [1].

The general idea of this trend is to interconnect everything that is able to embed a small computing and communication device that can offer valuable information or actuation to the physical world.

2.1.1. A definition for the IoT

The concept of the Internet of Things (IoT) was introduced in 1999, after the explosion of the wireless devices market, and the introduction of the Radio Frequency Identification (RFID) and the Wireless Sensor Networks (WSN) technologies. It was coined by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors.

Actually, there is no single, official or universally accepted definition of the IoT. Different groups have proposed different definitions of what IoT means and what are its most important attributes.

- The Internet Architecture Board (IAB) begins the RFC 7452, "Architectural Considerations in Smart Object Networking'' [4] saying that the term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called "smart objects,'' are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment.
- In the Internet Engineering Task Force (IETF), the term "smart object networking" is commonly used in reference to the Internet of Things. In this context, "smart objects" are devices that typically have significant constraints, such as limited power, memory, and processing resources, or bandwidth.
- The European Research Cluster on the Internet of Things (IERC) definition states that IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network." [5].
- The Internet Society, in "The Internet of Things: An Overview" [6], defines the term Internet of Things as generally referring to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.
- The Institute of Electrical and Electronics Engineers (IEEE) published the document "Towards a definition of the Internet of Things (IoT)" [7], which aims to give an all-inclusive definition of the IoT. To do so, it first compares the terms IoT and CPS. Then, compare it to the WSN and finally gives the following definition "An IoT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything.".
- The International Telegraph Union Telecommunication Standardization Sector (ITU-T), in the document "Y.2060 - Overview of the Internet of things" [8], defines the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)." and the term "thing" with regard to the IoT as "an object of the physical world (physical things) or

the information world (virtual things), which is capable of being identified and integrated into communication networks.”

2.1.2. Fundamental characteristics

From a security point of view, in the IoT every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. The fundamental characteristics of the IoT can be identified as follows:

- **Unequivocally identifiable**: IoT devices must be addressable in order to obtain data from them or to able to send commands to them. Authentication and authorization must be a key concept in the identification.
- **Interconnectivity**: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure. Security in this connectivity must be enforced.
- **Heterogeneity**: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks. Some of them may be resources constrained devices. The design of the security controls must take this fact into account.
- **Dynamic changes**: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically. Bootstrapping and device commissioning must be securely executed.
- **Enormous scale**: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. The impact of a security breach may be considerable.

2.1.3. Applications

The IoT includes a wide variety of devices and diverse applications, which call for different deployment scenarios. There are many market segments and verticals poised to drive IoT growth, some of them are:

- **Consumer goods**: Newer smartphones are including more and more sensors. Another successful vertical is smart homes with smart appliances, lighting and curtain controls, multimedia entertainment, security systems, etc. Smart cars with self-parking and voice commanding capabilities are becoming a reality.
- **Smart transportation**: It includes both public and private transport. Public transports activities include train control, electronically accessible timetables and ticketing. In the private transport domain, a major focus is vehicle automation including both vehicle control and system such as navigation and climate control. IoT applications can be the so called Car2X (car-to-car, car-to-infrastructure) or completely internal to the car. Another aspect of smart transportation is the appearance of services like car sharing for people who only need a car occasionally.

- **Energy distribution**: Smart grids are enabling the management of the energy distribution to make it more efficient and more resilient. It is using information and communications technology to gather and act on information.
- **Smart city**: It is a conceptual model that uses information and communication technologies to improve efficiency and development of all areas of urban life.
- **Distribution and logistics**: Stock accounting and tracking is saving time and money in the areas of inventory management, order fulfillment, warehousing, etc.
- **Industrial and manufacturing**: It helps increasing industrial automation and material flow traceability. Furthermore, remote and predictive maintenance are improving efficient factory operation.
- **Smart Home**: It uses the data to collect from environment sensors like temperature, humidity, lighting and noise levels to control air conditioning, lighting, heating, ventilation and security at home.
- **eHealth**: It is a broad segment that includes telemedicine, virtual healthcare and remote patient monitoring.

2.1.4. IoT architecture

A general architecture of the IoT can be described by defining three generic layers:

- **Physical or Perception layer**: Also known as the sensor layer, is implemented as the bottom layer in IoT architecture. The perception layer interacts with physical devices and components through smart devices (RFID, sensors, actuators, etc.). Its main objectives are to connect things into IoT network, and to measure, collect, and process the state information associated with these things via deployed smart devices, transmitting the processed information into upper layer via layer interfaces.
- **Network layer**: Also known as the transmission layer, is implemented as the middle layer in IoT architecture. The network layer is used to receive the processed information provided by perception layer and determine the routes to transmit the data and information to the IoT hub, devices, and applications via integrated networks. The network layer is the most important layer in IoT architecture, because various devices (hub, switching, gateway, cloud computing perform, etc.), and various communication technologies (Bluetooth, WiFi, Long-Term Evolution (LTE), etc.) are integrated in this layer. The network layer should transmit data to or from different things or applications, through interfaces or gateways among heterogeneous networks, and using various communication technologies and protocols.
- **Application layer**: Also known as the business layer, is implemented as the top layer in IoT architecture. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations. For instance, the application layer can provide the storage service to backup received data into a database, or provide the analysis service to evaluate the received data for predicting the future state of physical devices. A number of applications exist in this layer, each having different requirements. Examples include smart grid, smart transportation, smart cities, etc.

2.2. Enabling technologies

To allow all the expected billion of devices to communicate with each other, a communication technology is needed. Currently, there are plenty of wireless communication standards and specifications and each of them have strengths for certain applications. State of the art classic communication networks are being adapted to support IoT characteristics.

A set of networking technologies was compiled with the objective to have a representative set of technologies across the current state of the art. In that sense, technologies were evaluated based on their range and data rate, implemented layers, network type, network topology, frequency used, power consumption and the cost added to the application. Among the selected ones, it can be found classic and newer ones, coming from the WSN or from the cellular networks, ones that use licensed or unlicensed frequency bands and that are open or proprietary. The following table lists the set of representative technologies chosen for the survey and their characteristics:

	Layers	Network	Topology	Data rate	Range	Freq.	Power	Cost
Ethernet	PHY - MAC	LAN, WAN	star	1 Gbps	100 m	-	high	high
PLC	PHY - MAC	LAN, WAN	P2P	200 Mbps	200 m - 3 km	-	high	low
RFID	PHY	PAN	P2P	1kbps	up to 5 m	125 kHz - 915 Mhz	very low	very low
NFC	PHY	PAN	P2P	up to 400 kbps	10 cm	125 kHz - 915 Mhz	very low	very low
Bluetooth	PHY - APP	LAN	Star, mesh	1 Mbps	50 m - 100 m	2.4 GHz	moderate	moderate
WiFi	PHY - MAC	LAN	Star, ad-hoc	100 kbps, 1 Mbps - 6.7 Gbps	50 m 1 km	900 MHz 2.4 GHz 5 GHz	high	moderate
802.15.4	PHY - MAC	HAN	star, P2P	250 kbps	10 m - 100 m	915 MHz, 2.4 GHz	very low	low
ZigBee	NET - APP	HAN	star, mesh, tree	250 kbps	10 m - 100 m	915 MHz, 2.4 GHz	low	low
Thread	NET - TP	HAN	tree, mesh	250 kbps	10 m - 100 m	915 MHz, 2.4 GHz	low	low
Z-Wave	NET - APP	HAN	mesh	9.6, 40, 100 kbps	30 m	< 1GHz	low	low
SigFox	PHY - APP	WAN	star	100 bps	17 km	< 1GHz	very low	low
LoRaWAN	PHY - APP	WAN	star	10 kbps	5 - 15 km	< 1GHz	low	low
EC-GSM-IoT	PHY - NET	WAN	star	350 bps - 70 kbps	5 - 15 km	900 MHz 1800 MHz	moderate	moderate
LTE-M	PHY - NET	WAN	star	up to 1 Mbps	5 - 10 km	450MHz - 3.5 GHz	moderate	moderate
NB-IoT	PHY - NET	WAN	star	250 kbps	5 - 15 km	450MHz - 3.5 GHz	low	moderate

Table 2.1: Summary of networking technologies

In order to group the surveyed technologies, grouping criteria must be defined. Most of the technologies are based on wireless communications. So, a first group can be defined for the wired networking solutions in order to differentiate them.

For the wireless solutions, the following graphic show their range vs data rate:

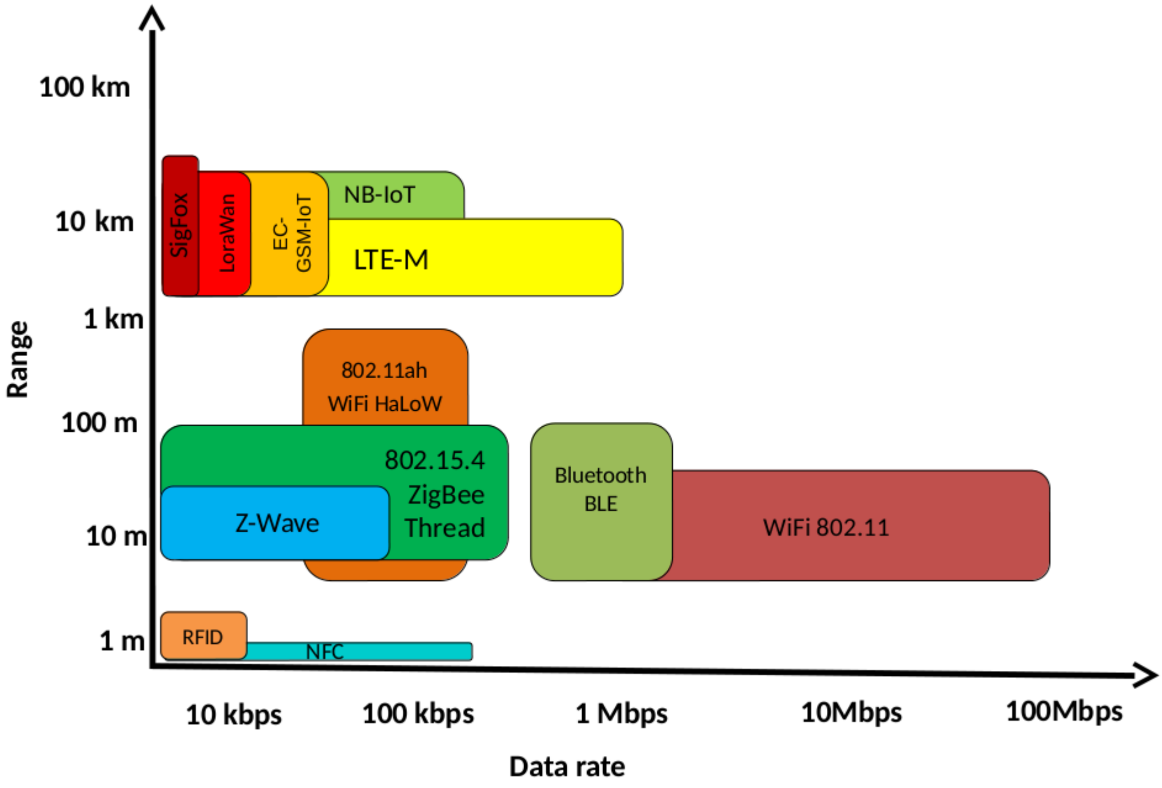


Figure 2.2: Wireless technologies range vs data rate

As can be seen in the figure, the wireless technologies can be basically grouped by its range. Three different range groups can be defined: Very short-range, Short-range and Long-range.

It was seen during the project that grouping them by its range is an adequate criteria. It was found that all the technologies in a certain range tend to implement similar solutions. And that these solutions are quite different than the implemented in other ranges. For instance, ZigBee (short-range) is quite different than technologies such RFID (very short-range) and NB-IoT (long-range) but have lots of similarities with technologies such as Z-Wave and Thread.

2.2.1. Wired networking technologies

Wired networks offer a great bandwidth at the expense of its cost and lack of flexibility. This was the first approach to connect sensor and actuators (e.g. surveillance cameras).

- **Ethernet**: It is the most used MAC protocol in the computer network. It is a known technology with wide manufacturer support. It is being deployed in some new buildings in a structured way along the electric wires. On the other hand, the need of a wire for every device connection makes the network to be static and costly to be modified.

- **Power Line Communications (PLC)**: It uses the building's existing electrical wiring for data transmission. It has an easy and low cost deployment because of exploitation of the existing wires. The most used existing standards for PLC is the HomePlug AV. A PLC adapter is connected to each of the devices, the adapters are then plugged into their wall sockets to form an Ethernet network between the devices over the electric wiring.

2.2.2. Very short-range networking technologies

Normally used for identification, tracking and application that requires direct human interaction with the device.

- **RFID**: Radio Frequency Identification, is a technology where information stored on a microchip can be read remotely, without physical contact using energy. In RF there are several frequency ranges used including Low Frequency (LF, 125 kHz), High Frequency (HF, 13.56 MHz), Ultra High Frequency (UHF, 433 MHz, 860-960 MHz) and Microwave (2.45 GHz, 5.8 GHz). These bands, in general, do not require a license if the transmitted power is limited. Some bands can be used globally (HF) while others are specific to certain regions (UHF in US, EU, and Japan).
- **NFC**: Near Field communication (NFC) is a short-range, high-frequency (13.56MHz) RF technology that allows user to exchange data and information between two NFC enabled devices. In future NFC can be one of the most used communication technology due to following reason. NFC provides easy network access and data sharing, without much lengthy process of handshaking. NFC can be configured with user intent and provide much better accessibility to device.

2.2.3. Short-range networking technologies

These technologies are normally used for Wireless Sensors Networks (WSN) and applications that requires several sensors/actuators spread in a short-range (e.g. home automation).

- **Bluetooth**: Bluetooth is based on the IEEE 802.15.1 standard. It is a low power, low cost wireless communication technology suitable for data transmission between mobile devices over a short range (5 - 150 m). The Bluetooth standard defines a personal area network (PAN) communication. It operates in 2.4 GHz band. The data rate in various versions of the Bluetooth ranges from 1 Mbps to 24 Mbps. The ultra-low power, low cost version of this standard is named as Bluetooth Low Energy (BLE or Bluetooth Smart). Earlier, in 2010 BLE was merged with Bluetooth standard v4.0. During the redaction of this report, Bluetooth Mesh was published to enable many-to-many communications.
- **Wi-Fi**: IEEE 802.11 is a collection of Wireless Local Area Network (WLAN) communication standards. For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60

GHz band. These standards provide data rates from 1 Mbps to 6.75 Gbps. WiFi provides communication range in the order of 20 m (indoor) to 100 m (outdoor).

802.11ah, and the corresponding WiFi HaLoW, was published in 2017. It uses 900 MHz band to provide extended range networks, albeit with lower data rates, and benefits from low power consumption.

- **802.15.4**: It defines a low-rate wireless personal area network. It specifies the Physical and datalink layers. It is the basis for Zigbee and Thread specifications. Alternatively, it can be used with 6LoWPAN to enable IPv6 as upper layer. 802.15.4 supports several radio bands and the last of its versions adopts channel hopping strategy to improve robustness against external interference. It is seen as the low layers of a standard IoT system.
- **ZigBee**: The ZigBee Alliance has developed a very low-cost, very low-power consumption, IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create, for instance, a PAN with small, low-power digital radios, such as for home automation or medical device data collection. The ZigBee network layer supports star, tree, and mesh topologies. Its low power consumption limits transmission distances to 10 - 100 meters line-of-sight, a defined rate of 250 kbps, which is best suited for intermittent data transmissions from a sensor or input device. IP addressable devices is introduced with the ZigBee IP specification.
- **Thread**: Thread is an IPv6 based networking protocol. It uses 6LoWPAN and 802.15.4 as a base for mesh communication. It is a protocol formed by a set of public standards and all of its nodes are IP-addressable.
- **Z-wave**: Z-Wave primarily allows reliable transmission of short messages from a control unit to one or more nodes in a network. Its architecture comprises five main layers: the physical, Medium Access Control, transfer, routing, and application layers. It uses two types of device controllers and slaves. Controllers poll or send commands to slaves, which either reply to or execute the controllers' commands.

2.2.4. Long-range networking technologies

The option to connect objects spread over the world is a challenge that has some similarities with the paradigm of cellular networks which aimed at connecting people. This similarity attracted the interest of mobile network providers to adapt its infrastructure to the IoT.

- **SigFox**: SigFox is an operated telecommunication network, dedicated to the Internet of Things. It utilizes ultra narrow-band signals and requires little energy. It was conceived for remote devices that don't have a lot to say, need to be very inexpensive, require very small power budgets and require very long range. It is an operated network that relays low-rate messages to distant devices over a range of up to 17 km.
- **EC-GSM-IoT**, **NB-IoT** and **LTE-M**: EC-GSM-IoT is based on eGPRS and designed as a high capacity, long range and low energy. NB-IoT is a narrow-band radio technology designed for the Internet of Things (IoT) and is one of a range of technologies standardized by the 3rd Generation Partnership Project (3GPP). It

operates in a licensed spectrum band. LTE Machine Type Communication Category M1 (LTE-M) reuses the already in place LTE infrastructure reducing its complexity and speed in order to enhance battery life time.

- **LoRaWAN**: LoRaWAN is an open protocol designed to integrate billions of devices in the Internet of Things. It is maintained by the LoRa Alliance, an open, non-profit association of members. It provides low-rate, low-power, long-range communications between end-devices and Network and Application servers. It is put on top of the physical LoRa modulation that is based on spread-spectrum and a variation of chirp spread spectrum.

2.2.5. Communication protocols

These are the protocols that are used to transfer the data to and from internet and devices.

- **6LoWPAN**: The 6LoWPAN group has defined mechanisms for encapsulation and header compression that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. Since IPv6 requires support of packets sizes much larger than the largest IEEE 802.15.4 frame size, an adaptation layer is defined. It carries IPv6 datagrams over such constrained links, taking into account limited bandwidth, memory, or energy resources that are expected in applications such as wireless sensor networks.

2.3. Challenges of the IoT

The IoT raises significant technological challenges that could detriment its successful deployment. Three of the important ones are Interoperability and Standardization, Privacy and Security.

2.3.1. Interoperability and Standardization

State of the art IoT suffers from platform fragmentation and lack of established technical standards that describe how the different parts of the technology stack should interact. Instead, large players and industry organizations use their own solutions. Some segments, such as industrial, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years.

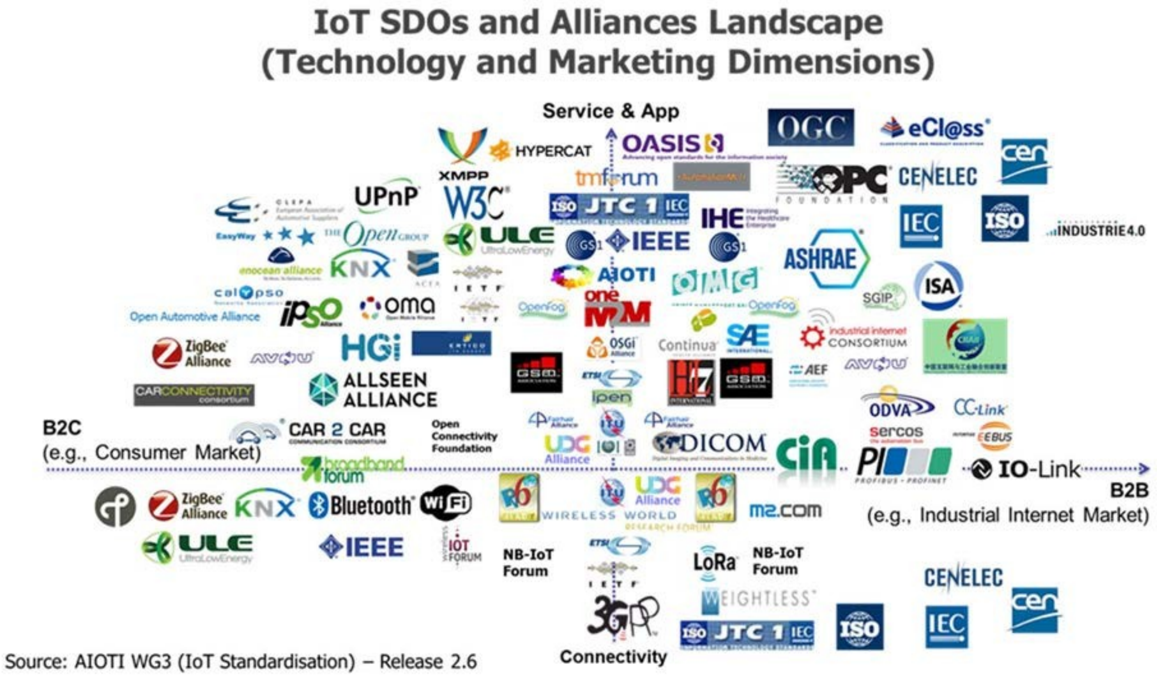
This lack of converged or interoperable standards may slow IoT adoption or discourage device manufacturers and others from developing new technological solutions, since they do not know whether their innovations will meet the guidelines that eventually become dominant. In addition, IoT players will have difficulty developing end-to-end security solutions without common standards.

2.3.1.1. Standard Developing Organizations (SDOs)

Multiple regional and international organizations are creating and proposing standards on how devices connect and communicate.

An effort to encourage the larger SDOs to strengthen collaboration and cooperation is being carried out by asking for regular progress report events to advertise the progress with the IoT standards, specifications in order to avoid reinventing similar but not compliant ones.

These organizations include standardization bodies or associations. Figure 2.3 shows a landscape of the SDO and alliances involved in the IoT.


IoT SDOs and Alliances Landscape
(Technology and Marketing Dimensions)
Service & App
B2C
(e.g., Consumer Market)
B2B
(e.g., Industrial Internet Market)
Connectivity

Source: AIOTI WG3 (IoT Standardisation) – Release 2.6

Figure 2.3: IoT SDOs and Alliances landscape

The major standardization bodies that are active in the IoT definition include the following:

- **IEEE**: It launched the P-2413 standardization projects [9], which aims to build an architectural framework for IoT, identify commonalities and relationships among various IoT verticals, define abstractions, provide a reference model, define building blocks and provide mechanism to develop multi-tier systems from these building blocks. The standard intends to supply a quadruple trust feature (protection, security, privacy, and safety). Its goals are to accelerate the growth of the IoT market by reducing the industry fragmentation.

  The IEEE claim that there are more than 350 standards that are applicable to the IoT, that 40 of them are being revised to better support the IoT and that there are more than 110 new IoT-related standards in development. For instance, the IEEE issued the IEEE-802.15.4 that is widely used as the physical and datalink layer of several of the already deployed IoT solutions.

- **ITU**: The ITU-Global Standards Initiative on the Internet of Things (IoT-GSI) [10] focuses on definitions, overviews, requirements, architecture and work plan for deploying the IoT. They published some recommendations like the Y.2060 - Overview of Internet of Things [8].

- **IETF**: It contributed to the IPv6 supporting by limited-energy devices in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [11]. Second, IEEE issued the Constrained Application Protocol (CoAP) [12] for resource-constrained devices to facilitate translation to HTTP for integration purpose with web application. Third, IETF developed IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) protocol [13]. Fourth, IETF proposed an integrated web services for M2M and IoT applications, called Constrained RESTful Environment (CoRE) [14].

- **IOT-A**: The Internet of Things - Architecture (IOT-A) [15] proposes an architectural reference model for IoT. They define suite of key building blocks. The main objective is to assist providers and researchers when they have to make their technical choices.
- **ETSI**: It has defined two main technical committees: ETSI Machine-to-Machine (M2M) [16] and ETSI Intelligent Transport Systems (ITS) [17]. ETSI M2M focuses on services, functional requirements, interfaces and architecture of M2M solutions, namely: smart grids, health, connected consumers, transportation, and smart cities. ETSI ITS debates all types of vehicular communications.
- **OneM2M**: The global standards initiative for M2M communications and IoT (OneM2M) [18]. Many standardization organizations are assembled to generate many specifications for a common M2M Service Layer. OneM2M is working to consolidate a lot of regional work that has already been done.

2.3.1.2. Industry alliances

IoT is growing fast and since standards organizations move relatively slow, many alliances or consortiums have been created to fill in the gap. Created from commercial vendors, they develop specifications and promote collaboration by partners but may compete against others. Many new industry coalitions have emerged alongside traditional SDOs. They have defined their own specification. The most important ones are the following:

- **ZigBee Alliance**: Established in 2002, the ZigBee Alliance [19] is an open, non-profit association of members dedicated to the development of the family of ZigBee specifications.
- **Thread Group**: Established in 2014, the Thread Group [20] is defining and promoting the use of the royalty-free Thread networking technology.
- **Z-Wave Alliance**: Established in 2005, the Z-Wave Alliance [21] is dedicated to the development and extension of Z-Wave technology.
- **SigFox**: Created in 2010, it is a private company that runs the SigFox network [22] since 2012.
- **LoRa Alliance**: Established in 2015, is an open, non-profit association [23] dedicated to maintain and develop the usage of the LoRa technology and LoRaWAN systems.
- **NFC Forum**: Established in 2005, is a non-profit industry association [24] dedicated to maintain and develop the use of NFC.

2.3.2. Privacy

Data privacy will play an important role in IoT deployments. Because IoT systems will produce and deal with personally identifiable information. An attacker can use these kinds of data which can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used.

Many of the IoT devices are designed to be embedded in the environment where a user does not notice the device nor its collected data. The user might not be aware that a sensor exists in her surroundings posing some privacy concerns. For instance, some regulation exists in the case of street monitoring cameras, where the user is alerted with a warning sign that the place is being monitored by surveillance cameras.

Legal issues also are arising related to the privacy in the IoT. It is in discussion who owns the data: if the sensed user or the device manufacturer. For example, in most of the vehicles since 2013 there is a device called Event Data Recorder (EDR) or “black box”. This device is storing information like vehicle’s speed, accelerator and brake pedals readings in order to perform accident reconstruction. Some vehicle manufacturer are even constantly monitoring the driver with an in-vehicle camera to implement driver drowsiness detection. All of these kinds of data are valuable for instance to insurance companies in order to define the liability in case of vehicle accident. On the other hand, the privacy of the end user is endangered by these practices.

2.3.3. Security

Security in the IoT has already captured headlines across the world. Security issues may represent the greatest obstacle to growth and deployment of the Internet of Things. So, security is a key requirement in the IoT. In the following chapter, the security risk and challenges to the IoT are described in more detail.

3. Security for the IoT

In this chapter, the security risk and challenges to a successful IoT deployment are introduced. Then, it is presented the security goals, its related threats and security requirement for the secure operation of an IoT system.

3.1. Security risks

IoT devices may present a variety of potential security risks that could be exploited to harm consumers by:

- **Enabling unauthorized access and misuse of personal information**: A lack of security can allow an adversary to have access to data stored or transmitted by a device. For example, a hacked baby monitoring doll cameras [25] or talking dolls acting as spies [26].
- **Facilitating attacks on other systems**: Vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems. For example, a horde of IoT devices infected with malware were used to attack the Internet infrastructure, causing shutdowns across Europe and North America [27].
- **Creating safety risks**: Everyday more systems are being controlled and monitored by computer-based algorithms, becoming Cyber-physical systems. A security flaw in one of these systems may have an impact on the safety of its user. For example, two security researchers that were able to remotely control a moving car [28] or a door lock that was remotely disabled by device manufacturer after customer's negative review on the product published online [29].

Although each of these risks exists with traditional computers and networks, they are aggravated in the context of the IoT systems due to its particular characteristics.

3.2. IoT Security challenges

The Internet of Things is facing security challenges that differ vastly from regular desktop computing, due to the unique constraints.

- **Massive scale**: End devices like sensors, actuators and consumer devices are designed to be deployed in a massive scale that will be orders of magnitude beyond the traditional connected devices. Therefore, existing tools, methods and strategies commonly used may need new considerations when used to the IoT. Furthermore, the impact of compromising an IoT system can be misused at scale, e.g. to perform a Distributed Denial of Service (DDoS) attack.
- **Constrained devices**: Many of the IoT devices, due to its size and power limitations, may not support the same level of security that the one expected from more traditional Internet connected device. Current IoT security technology is insufficiently sophisticated. Effective end-to-end security solutions that use leading-edge components are lacking. Processing capabilities are becoming less of an issue as time passes since increasingly faster chips are developed every year. Power

requirements are a big constraint for the current IoT affecting the processing speed, bandwidth, temperature and/or battery life. This restricts the choice of preventive techniques, such as cryptography, which can be applied as a first line of defense against attacks that are launched against individual nodes and the entire network.

- **Identical devices**: Many of the IoT deployments will consist in collections of identical or near identical devices. This fact magnifies the potential impact of a security vulnerability on one of the devices. Standardization and multiple interoperable devices manufactured by different vendors may minimize this challenge.
- **Long lifespan**: Many of the IoT devices will be deployed with an intended service life of several years (e.g. 10 years in the vehicles). This lifespan is longer than the typically associated to traditional connected devices. Security mechanisms at deployment time may not be adequate for the full lifespan as the security threats evolve. Long-term support and management is a challenge to the IoT.
- **Cyber-physical Systems: M**any of the IoT devices can affect the physical world, enabling potential attacks that may have greater impact than purely virtual attacks. A system malfunction may endanger the privacy and safety of the users, for instance in application areas such as health care or critical infrastructure.
- **Cross-device dependencies**: IoT devices can interact with other devices via explicit channels (e.g. a single app may use multiple IoT devices) or implicitly by affecting the physical world around them (e.g., an IoT heater may trigger an IoT temperature sensor). The result is that the security for an IoT deployment are likely to be complex and dynamic since they depend on both physical (e.g. environmental parameters) and computational (e.g., the state of other related devices) contexts.
- **Physically accessible**: Many of the IoT devices are deployed in places where physical security is difficult to achieve. An adversary with physical access to the device can apply more attack techniques than the one with only remote access to the device. Anti-tamper features may be considered for this kind of devices.
- **Wireless communications:** Most of the networking technologies used by the IoT are wireless communications on known and frequently used frequency bands. Due to the broadcast nature of wireless networks, an attacker armed with tools capable of capturing and injecting wireless information can inject forged packets into the network. Networking technologies must take this fact into account to mitigate them.
- **Not Managed**: Many of the IoT devices are designed without the ability to be reconfigured or upgraded. These mechanisms may be not practical to resource constrained devices. Furthermore, found vulnerabilities in one of these devices will perpetually remain if a costly recall is not performed. Many companies, particularly those developing low-end devices, may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.
- **Unattended devices**: Many of them are designed to work in an unattended way with no manner of user interaction. So, no direct user monitoring or configuration can be performed. In many cases the user does not have any insight that an exploited device is performing operations other than the intended ones. A security breach

might persist for a long time before being noticed and corrected if correction or mitigation is even possible or practical.

- **New connected devices**: Systems that may have been designed with the intention to be entirely isolated may, at a later stage, get connected to other systems. Connectivity comes with strong security requirements but it is not always that clear if it is not dealt during the design phase.

Several non-technical challenges that can affect the security design of an IoT system can also be identified:

- **New players:** Companies entering the IoT market may not have experience in dealing with security issues. They are traditional consumer-goods makers rather than computer hardware or software firms. For example, vehicle OEMs that are now including remote control capabilities to a car. The engineers involved may therefore be relatively inexperienced with data-security issues, and the firms involved may place insufficient priority on security concerns.
- **Security as a commodity**: Security is sometimes seen as a commodity or something that can be added afterwards (bolt-in). At a first sight, security does not have a direct value in return of investment. But taking security into account during the whole system design (built-in) does reduce the likelihood of future security issues at a lower cost than remediation after them.

For all of these reasons, it is not possible to simply use the same security features as are used in desktop computers to the Internet of Things.

3.3. Security life cycle

The life cycle of a device refers to the operational phases of the device in the context of a given application or use case. A generic life cycle applicable to very different IoT applications and scenarios can be defined, as shown in Figure 3.1.

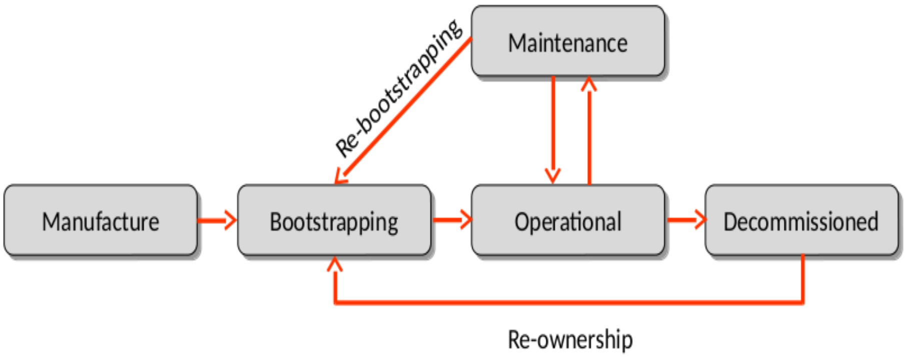


Figure 3.1: Security life cycle for an IoT device

The life cycle of an IoT device starts when it is manufactured. The device is later installed and commissioned within an IoT network during the bootstrapping phase. Specifically, the device identity and the secret keys used during normal operation are provided to the device during this phase. After being bootstrapped, the device and the IoT system are in operational mode and execute the functions they are intended to.

For devices that will operate during lifetimes spanning several years, they will eventually require maintenance cycles. During each maintenance, the software on the device can be upgraded or reconfigured. The maintenance tasks can be performed either locally or centralized from a backend system. Depending on the changes, it may be required to re-bootstrap at the end of a maintenance cycle.

It has to be noted that incorporating a mechanism to upgrade the software to fix vulnerabilities or to update configuration settings as well as adding new functionality is recommended but there are also security challenges when using software updates.

The device continues to loop through the operational phase until the device is decommissioned at the end of its life cycle. The end-of-life of a device does not necessarily mean that it is defective but rather denotes a need to replace the device by next-generation devices in order to provide additional functionality.

The device can be removed and re-commissioned to be used in a different IoT system and start the life cycle all over again. When decommissioned, some actions like to reset the device to factory settings or to update the security parameters of the left IoT system are carried out in order to maintain the level of security.

3.4. Adversary capabilities

Adversary capabilities can be categorized as technical and operational capabilities.

- **Technical capabilities**: It refers to the assumptions concerning what an adversary knows and his ability to analyze the target system. For example, it can be assumed that the adversary has an instance of the target system and the capability to reverse engineering it (or purchase this knowledge) and the appropriate tools to communicate to the system.
- **Operational capabilities**: It refers to the assumptions concerning what an adversary requires to deliver malicious input through a particular access interface in the field.

  It is roughly divided in three categories:

  - **Physical access**: Some of the devices used in the IoT may be physically accessible to a motivated adversary. Physical access to IoT devices introduces a wide range of additional attack possibilities. In some cases it may be possible to extract keys contained on chip. This can be accomplished using power analysis, or fault injection (glitching) attacks. Tools for physical attacks decrease in cost and become easier to use.
  - **Short-range access**: This adversary can take advantage of their spatial proximity to an IoT device to attack the device. An example can be an adversary in the range to be able to sniff a specific device’s bootstrapping communication. This category also includes an adversary connected to a LAN that is part of the IoT system. As the main purpose of the network in IoT is to transmit the collected data, most of the attacks focus on the impact of the

availability of network resources. Also, most devices in IoT are connected into IoT networks via wireless communication links.

- **Long-range access**: This adversary can take advantage of long-range communication network to interact with the IoT system (e.g. LoRaWAN, LTE). Long-range access also includes an adversary interacting with the IoT system through the Internet.

An attack can be performed from the network itself or from the Internet, and it might be applicable to a single device, some devices or all devices. For example, if an attack requires physical access to a specific device then it is deemed to affect only one device at a time. An attack to obtain a group key can affect multiple devices at one. Finally, an attack to obtain a master network key might affect the whole system.

An attack can be unnoticeable to the user or may result in an observable result (e.g., door opens or vehicle stops).

3.5. Security goals

For any system that deals with sensitive data, several security goals can be defined to model the security properties needed for the system. The classic goals for information security are Confidentiality, Integrity and Availability. The following additional goals will be considered for IoT: Authentication, Freshness and Authorization. It is interesting to know how a network cannot accept messages that are not authentic (e.g. coming from an authorized party), that are not fresh (e.g. replay attacks) and how is a device authorized to participate in the network.

For each considered security goal, its related threats and security recommendations are identified.

3.5.1. Confidentiality

Confidentiality is the property that data is not disclosed to entities unless they have been authorized to know the data.

Confidentiality is an important service for the IoT since some of its applications manage sensitive or critical information (e.g. Personal Identification Information, medical records or vehicle positioning). It becomes more relevant by the fact that most of the IoT networks have a wireless nature, where messages can be easily sniffed.

Confidentiality is commonly achieved by the use of cryptographic encryption where only the entities in possession of the cryptographic key are able to understand the protected data.

3.5.1.1. Threats

Several threats to data confidentiality can be defined:

- **Device capturing**: The adversary with physical access to the device may capture and control it by physically replacing the whole device or by tampering with the hardware of the device. If a deployed device is captured, some sensitive information (e.g. network key, firmware) may be obtained or altered by physical means.

- **Physical access**: An adversary may attempt to extract private information like firmware, keys, user data or manufacturer's IP by having physical access to the device's hardware. If there is available debugging ports (e.g., JTAG) or external memories, it enables him to dump the private data. Access to debugging ports enables the dynamic analysis of the firmware execution on the device dramatically increasing the chance to find vulnerabilities that can be exploited in other similar devices.
- **Eavesdropping**: Eavesdropping is the process of gathering information from a network by snooping on transmitted data. It consists in passive wiretapping done secretly (e.g., without the knowledge of the originator or the intended recipients of the communication). It is easier to perform on wireless networks since an adversary can passively listen to the communication frequency from a safe distance.

  Communication may be eavesdropped upon if the communication channel is not sufficiently protected or in the event of session key compromise due to a long period of usage without key renewal or updates.

  It is especially important during the commissioning of a device into a network, it may be susceptible to eavesdropping, especially if operational keying materials, security parameters, or configuration settings, are exchanged in clear using a wireless medium or if used cryptographic algorithms are not suitable for the envisioned lifetime of the device and the system.

  Advanced attacks like Man In The Middle (MitM) also apply to enable eavesdropping the network communication.
- **Sniffing / Traffic analysis**: Even if the protected data cannot be interpreted, the other non-protected fields in the communication exchange can be useful to an adversary. For example, the MAC header fields can be used to map all the devices in a network. Other factors, like time, power or direction of the transmission may be useful to track devices or to narrow down the position of every device in the network.
- **Bootstrapping attack**: The objective of this attack is to force a device to become unassociated from the network. The next time the device tries to rejoin the network, the adversary either passively eavesdrops on the association process in order to collect valuable bootstrapping information that it can use to perform its own association with the network, or the adversary can perform a man-in-the-middle attack in order to intervene with and thus prevent the association of the legitimate device.

3.5.1.2. Security requirements

In order to counter the threats to data confidentiality, the following security requirements can be defined:

- **Physical protections**: Device capturing detection can be accomplished by physical security or by incorporating motion detectors for static devices. Another option is to implement a keep-alive signal detection that will make the device to lock when the signal is not sensed.

- **Anti-dump**: There exist various ways of securing the physical layer such as epoxying the chips, disabling debugging interfaces for production versions, the usage of ball sockets (so the memory cannot be removed and dumped), and adding a tamper-sensor that triggers a secret erasure process. The degree of success is variable in providing resistance against an adversary.
- **Data Encryption**: Data should be encrypted in order that only authorized parties can access it. Especially before transmitting over a link and when stored. If the use of encryption is optional, it should be enabled by default. It is also recommended to apply several layers of security to avoid total confidentiality loss in case one of the layers is compromised. For example, encryption on the MAC and Application layers.
- **Key management**: Long-term keys usage should be avoided and the keys should be changed periodically. The compromise of a long-term key has a bigger impact on the confidentiality of the system than the usage of session keys.
- **Robust cryptography**: Robust and tested cryptographic algorithms should be used. For example, SHA2 as a hash algorithm, AES for symmetric cryptography and RSA or ECC for the asymmetric one. The cipher block chaining mode should be taken into account too. For instance, Electronic CodeBook (ECB) mode is not recommended since identical plaintext blocks (under the same key) result in identical ciphertext [30]. Furthermore, since ciphertext blocks are independent, malicious substitution of ECB blocks does not affect the decryption of adjacent blocks.
- **Key length**: Up-to-date key length recommendations should be met to make brute-force attack infeasible. For example, usage of 128-bits key for AES, 2048-bits keys for RSA and 256-bits key for ECC.
- **Secure bootstrapping**: The security material that will be used to participate in the network should be delivered in a secure way. For example, the use of asymmetric cryptography, secure key exchange protocols or out-of-band bootstrapping procedure.

3.5.2. Integrity

Data integrity is the property that data has not been changed, destroyed, or lost in an intended or unintended manner. Integrity is a ground base to trust data value. An integrity service ensures that changes to the data are detectable. There are integrity services that might also attempt to correct and recover from changes.

Integrity is an important service for the IoT since if IoT applications receive forged data or tampered data, erroneous operation status can be estimated and wrong feedback commands can be made, which could further disrupt the operation of IoT applications. For instance, applications that depends on the correct reception of a message to have an actuation in the physical world (e.g. vehicle braking, door unlock or increase insulin pumping).

Integrity is commonly achieved by the use of digest algorithms, error detection or correction codes. Normally, integrity is combined with authentication in order to provide verification that the data was not changed and was sent by an authorized entity by the use of Messages Authentication Codes.

3.5.2.1. Threats

Several threats to data integrity can be defined:

- **Message Manipulation**: Message manipulation are used to inject false data into the network by transforming a legitimate data frame into a modified frame containing information of the adversary’s choice. For instance, in the wireless communications, it can be based on emitting RF waves whose phase and amplitude are synchronized with those of the original at the correct time, which leads to a new signal containing the falsely injected data.

  Advanced attacks like Man in the Middle also applies to enable message manipulation.

  Message manipulation can also be used by an adversary to selectively modify some data on a legitimate message in order to be dropped by the integrity mechanism at the receiver, threatening the message availability.

- **Sinkhole**: In mesh networks or networks with redundant paths some kind of arbitration is enforced in order to choose the better path. Sinkhole attack (or black hole attack), is the attack where an attacker declares himself to have a high-quality route/path to the base station, thus allowing him to manipulate all packets passing through it.

3.5.2.2. Security requirements

In order to counter the threats to data integrity, the following security requirements can be defined:

- **Data Integrity mechanism**: The use of integrity checking mechanism like CRC, Message Integrity Codes (MIC) or digital signatures will enable the receiving entity to check if the integrity of the message is correct. It has to be noted that non-cryptographic mechanisms like CRC does not prevent data modification by an adversary able to modify the value of both the data and the CRC.

  The Key Management, Robust Cryptography and Key, and Key Length, presented in Section 3.5.1.2, also apply here in order to provide a robust data integrity checking mechanism

- **Secure routing protocol**: Dynamic routing must be designed in a way that a single device cannot make the network to send all the traffic to it. For example, there are routing protocols that uses neighborhood information of all the devices in the network to map the network devices, hence any inconsistency may be detected in this kind of protocol.

3.5.3. Authentication

Authentication is the process of verifying a claim that a system entity or data has a certain attribute value. Authenticated entities and data are legitimate. An authentication process consists in presenting the claimed attribute value (e.g. identity) and some evidence to prove the binding between the attribute and that for which it is claimed (e.g. value signed with a private key). It is used to verify the presence and identity of a person, device or service at the time and to verify the source of data.

Authentication is important to the IoT to ensure that non-authenticated devices or applications cannot connect to the IoT network and to ensure that the devices and data delivered in an IoT are legitimate. Since the IoT is formed by a large number of diverse objects and that most of them are operated without human interaction, authentication is a challenging process.

This aspect, which requires to identify the communication endpoints, is particularly relevant in those scenarios where it is necessary to ensure that private data cannot be accessed by unknown or unauthorized parties.

Authorizing a device within IoT have some challenges that does not exist in desktop computing, where the concept of a user with different user-names and passwords will be entered into the service a user wishes to use. In IoT, the user is not actively using the device through an advanced user interface.

3.5.3.1. Threats

Several threats to authentication can be defined:

- **Message injection**: Message injection are used to inject data into the network. An adversary may try to inject illegitimate messages to the network in order to execute non-authenticated actions.
- **Spoofing**: Spoofing is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet. Spoofing may be used to hide the original source of an attack or to work around network Access Control Lists (ACLs) that are in place to limit host access based on source address rules.
- **Sybil attack**: Sybil attack, whereby an attacker presents multiple identities to other devices in the network is similar to Spoofing but tries to exploit the fact that normally a single identity is associated to each device in the network.

3.5.3.2. Security requirements

In order to counter the threat to authentication, the following security requirements can be defined:

- **Authentication mechanism**: An authentication mechanisms like Message Authentication Codes or digital signatures should be used. For the Message Authentication Code case, it is recommended that the symmetric key is unique per device to avoid authenticating different devices with the same credentials.

3.5.4. Freshness

Freshness or data liveness is a property of a communication association or a feature of a communication protocol that provides assurance to the recipient of data that the data is being freshly transmitted by its originator (e.g., that the data is not being replayed, by either the originator or a third party, from a previous transmission).

Data liveness is typically achieved by the inclusion of a random nonce or a non-repeating value in the data exchanged by the protocol.

3.5.4.1. Threats

The main threat to freshness can be defined as:

- **Replay attack**: An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and re-transmits it. Replay attacks may be used to bypass and authentication control by repeating the messages of a previous legitimate authentication. It can be used to induce a previous observed state change or action within the network.

3.5.4.2. Security requirements

In order to counter the threat to freshness, the following security requirement can be defined:

- **Use of nonces**: A nonce is a random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks.

3.5.5. Availability

Availability is the property of a system or data being accessible, or usable or operational upon demand by an authorized entity. It is especially important in critical systems which requires to timely receive messages in order to operate in a safely manner.

3.5.5.1. Threats

There is a main threat to the availability that can be identified:

- **Denial of Service**: This attack focuses on rendering a device as not available by exhausting its resources or blocking access to physical resources such as wireless medium. An adversary can continuously send requests to be processed by specific things so as to deplete their resources. This is especially dangerous in the IoT since typically the devices tend to have tight memory and limited computation resources.

  Several techniques have been used to achieve this result:

  - **Radio Jamming**: Radio jamming is a physical layer attack with the intend of creating a DoS on the network links. It consists in the emission of high transmission power radio signals in order to disrupt the reception of messages at network devices.

    The jamming can be over all the channels of the frequency band or targeting only a single channel rather than all the channels. It can be continuously transmitted or started when it senses ongoing network activity.

    Jamming can also be performed on upper network layers. It consists in emitting packets of useless content at specific or random moments. Its objective is to affect the correct execution of protocols. Jamming attack can be used as a step for further attacks like delayed message or man-in-the-middle attacks.

  - **Device-specific flooding**: Flooding attempts to cause a failure in a system by providing more input than the system can process properly. A simple PC may be able to flood some of the IoT devices since they are resource-constrained devices.
  - **Channel reservation abuse**: Data link layer that uses channel reservation mechanisms like CSMA-CA may be abused by an adversary to hijack the channel access or to jam it without needing to transmit at a high duty cycle. For example, CSMA-CA short back-off time used by an adversary will make the legitimate devices to increase its own back-off time and power consumption during the reception of the adversary's data. Another example may be transmitting a frame with empty payload but with a big frame duration value.
  - **Wormhole**: Wormhole attack, where an attacker may record packets at one location in the network and tunnel them to another distant location. This creates the perception that two distant nodes are very close to each other, greatly impacting the functionality of routing. The tunnel is either a wired link or a high frequency link. The effects of the attack may serve an adversary to routing disruption or selectively drop data packets.
  - **Sleep deprivation attack**: One of the solutions to enable an extended lifetime for battery powered devices is to remain most of the time asleep and only wake up when necessary. In these situation, the so-called Sleep deprivation attacks applies. It tries to break the sleep routines and keep the device awake all the time until they are shut down.

3.5.5.2. Security requirements

In order to counter the threat to availability, the following security requirements can be defined:

- **DoS detection**: DoS attacks are difficult to defend, especially in a system with resource-constrained devices. On the other hand, they are normally easy to detect, for instance, jamming attacks can be detected by sensing the channel with a radio monitoring equipment and a policy that detects not normal communications. Once the attack is detected several actions can be performed, like route the messages through a different network path or even try to physically locate the jamming source.
- **Use of Multiple channels**: The usage of multiple channels make the potential jamming to be costlier since it has to cover more frequency channels. The channel can be proactively changed after a certain duration of time (e.g., with channel hopping) or upon the attack detection.
- **Flooding resistance**: A device should be designed to gracefully tolerate excessive numbers of unauthenticated messages. It means to have spare resources for communications functionality or a degraded mode of operation that maintains the system in an operative state.
- **Multi-path / Mesh networks**: Sending the same message through several different paths may diminish the impact of DoS attack. Mesh networks may implement redundant paths to the same destination and use one or the other or both at the same time.

3.5.6. Authorization

Authorization is an approval that is granted to an entity to access a system resource. An authenticated user may be authorized to access some resources (e.g. service user vs, service administrator).

This aspect, which requires to identify the communication endpoints, is particularly relevant in those scenarios where it is necessary to ensure that private data cannot be accessed by unknown or unauthorized parties.

Authorizing a device within IoT have some challenges that does not exist in desktop computing, where the concept of a user with different user-names and passwords will be entered into the service a user wishes to use. In IoT, the user is not actively using the device through an advanced user interface.

Only authorized devices should be able to access the IoT network. Unauthorized devices should not be able to route their messages over the IoT network, because it may access sensitive data or exhaust resources needed for correct network operation.

3.5.6.1. Threats

Several threats to authorization can be defined:

- **Unauthorized commands**: Some systems may accept a set of commands without authorization. A malicious use of these commands may be exploited to get access to the network resources. It especially happens before a trust relationship have been established (e.g. before device commissioning).
- **Misplaced trust**: Some systems trust a device if they are, for instance, in the same network (e.g. LAN, WiFi AP) or if its data link layer address lays in a certain range.
- **Attacks on no/weak device commissioning**: Default or weak credentials used during device commissioning to the network may be exploited to gain access to the network by unauthorized devices. Weak credentials, not carefully chosen (e.g. randomly), are vulnerable to be compromised by brute forcing all its possible values.

3.5.6.2. Security requirements

In order to counter the threat to authorization, the following security requirements can be defined:

- **Reduced set of unauthorized commands**: It is recommended that the only unauthorized commands are the ones dedicated to trust establishment (e.g. device commissioning, key exchange handshake).
- **Per-device unique authentication credentials**: It is recommended to not use default passwords shared between devices, or weak out of the box passwords. All passwords should be randomly created using high quality random number generators.
- **Resistance to brute force attacks**: Authentication mechanism should be designed to make attacks like brute-force authentication attacks, dictionary attacks infeasible,

as well as other attacks that involve exhaustive searching of the device’s key or password space.

- **Secure device commissioning**: Device commissioning procedure is the first step on network access control. It is where a trust relationship between the network and the joining device is established. It is recommended that each device that requires authentication should be instantiated either prior to shipping, or on initial configuration by the user, with credentials unique to that device.

4. Security survey on networking technologies

This chapter surveys the security of the state of the art networking technologies enabling the Internet of Things. A set of representative networking technologies have been surveyed describing their security options and listing the issues found in research studies and security conferences. The analysis is purely theoretical, based on published information.

4.1. Ethernet

Ethernet is the most used MAC layer protocol in the computer networks. Originally conceived as a simple, inexpensive local-area network (LAN) technology, it's now used throughout most of the wide-area networks (WANs) for carrying the Internet traffic.

It is a family of computer networking technologies. It was standardized in 1983 as IEEE 802.3. The most common used physical medium by Ethernet is a copper twisted pair or fiber optic links.

There are several refinements to the standard supporting higher bit rates and longer distances. There exist commercial repeaters or switches to enhance the distance range.

The need of a wire for every device connection makes the network static and costly to be modified. The cost of a wire to connect every device can be considered high compared to wireless solutions.

Ethernet only manages until the MAC layer, but it is able to carry a payload of 1500 bytes. It can play a role on the LAN and WAN part of the IoT systems and for critical systems that have strict requirements on latency and bandwidth.

4.1.1. Security options

Security Goal	Ethernet (802.3)	802.1X + 802.1AE
Confidentiality	No	AES-128 GCM
Integrity	CRC	
Authentication	No	
Freshness	No	Packet Number in the MIC
Availability	Wired media	
Authorization	By physical connection	EAP-TLS with TLS v1.2
Key type	Not applicable	Session key MACSec key
Key management	Not applicable	Periodic re-authentication
Required power	moderate	high

Table 4.1: Ethernet security options summary

Ethernet does not offer any specific security mechanism. On the other hand, its big payload is able to carry any of the full-fledged IP-based security network and transport protocols.

Mechanisms such as MAC filtering to implement access control using the MAC source addresses or the Virtual LAN (VLAN) to divide the broadcasting domains are easily bypassed using spoofing techniques.

Note that while the CRC provides some integrity protection, it is not considered to provide cryptographic integrity as it can be easily forged.

802.1X

The IEEE 802.1X standard [31] defines the port-based network access control that is used to provide authenticated wired access to Ethernet networks. It specifies an architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and secure communication between the ports. Access to the port can be denied if the authentication process fails.

It defines two basic components:

- **Supplicant**: An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.
- **Authenticator**: The Authenticator is a network device, normally a managed switch featuring access control whereby a port will remain in an “unauthorized” state (not allowing access) prior to authentication occurring, and the port will be changed to an “authorized” state (allowing access) after successful authentication occurs. Network connections can also be configured to time out and then force re-authentication for any new connections.

And a third optional component:

- **Authentication Server**: The authentication server (typically a RADIUS server) validates the credentials of the supplicant requesting access. Credentials might include username/password, digital certificate or other methods.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) [32] which is known as "EAP over LAN" or EAPOL. It allows a number of different authentication methods to be used including the use of Public Key Encryption and One Time Passwords. 802.1X mandates the use of EAP-TLS [33]. At the end of a successful EAP-TLS handshake, a Master Session Key (MSK) is derived in both ends.

Periodic re-authentication can be configured, being 1 hour the default value.

It defines applications of port-based network access that use IEEE 802.1AE. It supports the derivation of key material from the EAP MSK and key distribution to enable the 802.1AE operation.

802.1AE

The IEEE 802.1AE standard [34] defines a Layer 2 security protocol called Medium Access Control Security (MACsec) that provides point-to-point security on Ethernet links between nodes for securing a wired LAN. Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is secured through the use of data integrity checks and, if configured, encryption.

MACsec uses AES-128 in Galois Counter Mode (GCM) as the authenticated encryption algorithm.

It adds a security field to the Ethernet frame with information needed for MACsec operation including a 4 bytes Packet Number for replay protection. This field, along with the encrypted payload, will be included in the integrity checking that is added at the end of the Ethernet frame.

4.1.2. Issues

The primary weakness with Ethernet is that it is a broadcast system. Every message sent out by any computer on a segment of Ethernet wiring reaches all parts of that segment and potentially could be read by any computer on the segment.

It is a great advantage to be able to install and expand a LAN just by connecting switches and computers together with cabling and have it work automatically. However, the features that enable this, like MAC table learning and ARP together with the underlying broadcasting mechanism, are also key vulnerabilities.

- **Unauthorized joins**: The basis for attacks is gaining access to the target Ethernet segment. The attacker may, for example, be an insider with full access rights, may have found an Ethernet connection in a public space, or may have taken control of a workstation in the LAN. Then, it is easy to eavesdrop all the traffic in the link.
- **Switch control**: An adversary can use the MAC learning table and ARP mechanisms to make the target switch forward frames destined for a remote host to the network adversary. It can be achieved by repeatedly sending frames spoofing the MAC address of the remote host.
- **MAC learning table exhaustion**: An adversary render the switch inoperable by sending lots of frames with random MAC addresses to fill the MAC learning dynamic table. It is possible that from that point the switch work in hub mode repeating all the received frames to all the ports.
- **VLAN Tagging and Hopping**: An attacker can create Ethernet frames that have a VLAN tag and thus inject frames to VLANs to which they are not supposed to have access.

4.2. Power Line Communication (PLC)

Power line communication, that is, using the electricity infrastructure for data transmission, is experiencing a renaissance in the context of Smart Grid. It is used for remote meter reading.

The basic principle in transmitting data through Power Line Communication (PLC) consists in superimposing a high frequency signal that is message signal (1.6 to 30 MHz) at low energy levels over the 50 Hz electrical signal like the one usually found at home. It is able to carry from 500kbps to 135Mbps, depending on the quality of the wires.

It has an easy and low cost deployment because of exploitation of the existing wires. The devices have an Ethernet MAC address and can be connected to a computer or Ethernet compatible network device like a switch or router.

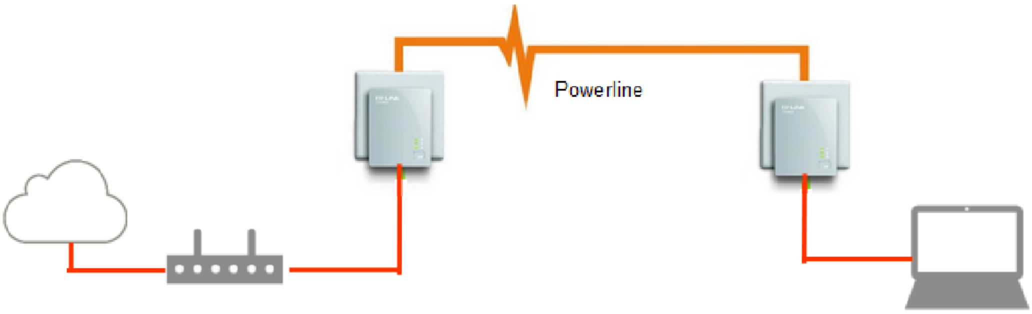


Figure 4.1: PLC topology

The most used existing standards for PLC is the HomePlug AV. This standard has been produced by HomePlug Powerline Alliance [35]. It offers a peak data rate of 200 Mbps at the physical layer, and about 80 Mbps at the MAC layer.

4.2.1. Security options

Security Goal	PLC
Confidentiality	AES-128 CBC
Integrity	CRC-32 in the encrypted payload
Authentication	
Freshness	Nonces
Availability	Wired media
Authorization	By physical connection, custom key agreement or user provided credentials
Key type	Network membership, encryption, device access and temporary encryption keys
Key management	Key is changed and securely distributed periodically
Required power	low

Table 4.2: PLC security options summary

HomePlug AV security was studied in [36]. It includes key distribution techniques and the use of AES-128 encryption. Older HomePlug AV versions use the less secure DES protocols.

Four types of keys are used in HomePlug AV:

- **Network Membership Keys**: which enable a device to authenticate to the network. It can be pre-installed, obtained protected with the Device Access key or by the key exchange protocol.
- **Network Encryption Keys**: which enable a device to perform the cryptographic processing needed to exchange data with another device within the same network.

- **Device Access Keys**: which are unique to a device and allow other devices to pass it the Network Membership keys securely. It is derived from a password chosen at random by the manufacturer and usually printed on the back of the device.
- **Temporary Encryption Keys**: which are generated and used in the key distribution protocols.

To form a network, the Network Membership key is distributed to all the devices. Using this key, the coordinator distributes a periodically changing Network Encryption Key to each device in the network. Nonces are used to prevent replay attacks. There are four ways to join a new device to the network:

- The user plugs devices into the outlets and they connect by themselves.
- The user enters a network password to get a device to join a network (devices with rich user interfaces).
- The user enters a device password to add another device to its network (at least one device with rich user interface).
- The user pushes a button on each of two devices to get them to connect to each other.

4.2.2. Issues

- **Emissions**: Twisted and protected cables are not used for power lines. For this reason, the electromagnetic emissions produced by power lines can be received by radio receivers and may be used on an eavesdropping attack.
- **Default password**: Encryption key is normally based on a default password defined by the manufacturer. Most of the user won't change that value.
- **Low entropy keys**: Keys are derived from passwords or even the device's MAC address.
- **Non-controlled range**: The assumption that the perimeter of the house is a barrier. Power line may cross the perimeter of a house if, for instance, a plug is available on the outside or it is a building with a shared power feed. The signal can travel quite far down wires, and despite fuse boxes offering some resistance to signals, it is usually found that the signal is retrievable in the neighbor's house.

4.3. Radio-Frequency Identification (RFID)

A basic Radio-Frequency Identification (RFID) system consists of an RFID reader and RFID tags. It's main role in the IoT is to provide identification services. RFID uses wireless technologies such as ISO/IEC 14443.

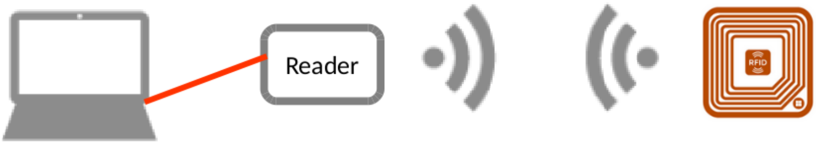


Figure 4.2: RFID topology

An RFID system consists of two components: a transponder and a reader:

- **The transponder**: Also known as a tag, acts as the actual data carrier. It is applied to an object (e.g. on a good or package) or integrated into an object (e.g. in a smart card) and can be read without making contact, and rewritten depending on the technology used. Basically, the transponder consists of an integrated circuit and a radio-frequency module. An identification number is stored along with other data on the transponder and the object with which it is connected. Two types of tags can be defined:
  - **Active tags**: Requires a power source like powered infrastructure or battery. One example is the transponder attached to an aircraft that identifies its national origin.
  - **Passive tags**: Does not require batteries or maintenance. They are powered by the reader's RF field and are small enough to fit into an adhesive label.
- **The reading unit**: it consists of a reading, in some cases a write/read, unit and an antenna. The reader reads data from the transponder and in some cases, it instructs the transponder to store further data.

4.3.1. Security options

Security Goal	RFID
Confidentiality	No
Integrity	CRC-16
Authentication	No
Freshness	No
Availability	No
Authorization	By physical proximity
Key type	Not applicable
Key management	Not applicable
Required power	low

Table 4.3: RFID security options summary

RFID does not offer any specific security mechanism other than the CRC for integrity checking. Note that it is not considered to provide cryptographic integrity as it can be easily forged.

Some sort of confidentiality and Authentication can be provided if the stored data is encrypted and includes an authentication mechanism like MAC or digital signature. Newer tags have security functionality built into the chip but are not a part of the specification.

In a second generation, a Kill command was included. Tags can be “killed” or permanently rendered inoperable by command under the Generation 2 protocol.

4.3.2. Issues

RFID tags are considered simple devices that can only listen and respond, no matter who sends the request signal. This brings up risks of unauthorized access and modification of tag data. In other words, unprotected tags may be vulnerable to eavesdropping, spoofing or denial of service attacks [37].

- **Eavesdropping**: Radio signals transmitted from the tag, and the reader, can be detected several meters away by other radio receivers. It is possible therefore for an unauthorized user to gain access to the data contained in RFID tags if legitimate transmissions are not properly protected.
- **Spoofing**: By spoofing valid tags, the intruder could fool an RFID system, and change the identity of tags to gain an unauthorized or undetected advantage.
- **Denial of Service**: DoS is possible using radio Jamming techniques, by the use of a “blocker tag” that simulates many tags simultaneously flooding the legitimate RFID reads or by corrupting a large batch of tags. Or by killing the tag with Kill command.
- **Unauthorized Access to Tags**: A rogue reader can read a tag, recording information that may be confidential. It can also write new, potentially damaging information to the tag. Or it can kill the tag. In each of these cases, the tags respond as if the RFID reader was authorized, since the rogue reader appears like any other RFID reader.
- **Unauthorized tracking**: Even if tag data is protected, it is possible to use traffic analysis tools to track predictable tag responses over time. Correlating and analyzing the data could build a picture of movement, social interactions and financial transactions.

4.4. Near Field Communication (NFC)

Near Field Communication (NFC) is a set of short-range communication technologies, operating over electromagnetic fields at a frequency of 13.56MHz over distances of about 10 cm. NFC specifications are developed by the NFC Forum, an association composed of companies with interest in NFC. NFC was approved as the ISO/IEC 18092 [38].

NFC operation is described in standards ISO/IEC 14443 and ISO/IEC 18092. NFC is used to read and write information stored in tags. For example, Temperature and humidity sensors readings on transported consumer goods.

As can be seen in Figure 4.3, the main characteristic of NFC is that it is a wireless communication interface with a working distance limited to about 10 cm. It is intended to create a close proximity communication between two devices.

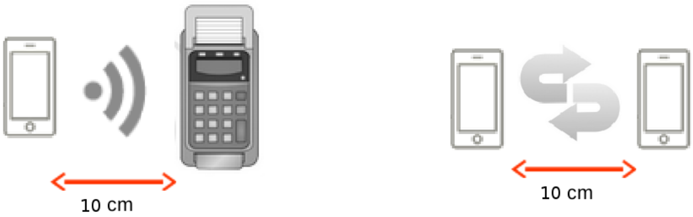


Figure 4.3: NFC topology

NFC devices communicate by generating electromagnetic fields. In an active communication, both devices generate their own fields. In a passive communication, one device transmits data by modulating the field generated by the active device.

It was also chosen as the principal communications protocol for mobile payments since most of the mobile devices were NFC enabled devices. ISO/IEC 14443 is the same standard used for contactless payment cards.

4.4.1. Security options

Security Goal	NFC	NFC-SEC
Confidentiality	No	AES-128 CTR
Integrity	CRC-16	AES-XCBC-MAC-96 or AES-128 GCM
Authentication	No	
Freshness	No	Sequence number in the MIC
Availability	No	No
Authorization	By physical proximity	ECDH 192-bits
Key type	Not applicable	Exchanged key Confidentiality key Integrity key
Key management	Not applicable	New key agreed on each connection
Required power	low	low

Table 4.4: NFC security options summary

Physical features of the NFC radio signal offer some security like short-range and direction of signals. In other words, it is assumed that user is able to notice if the attacker participates to the communication. Note that CRC integrity checking is not considered to provide cryptographic integrity as it can be easily forged.

Just like RFID, some sort of confidentiality and Authentication can be provided if the stored data is encrypted and includes an authentication mechanism like MAC or digital signature.

Newer tags have security functionality built into the chip but are not a part of the specification. If applications require security, it needs to be implemented at higher levels.

NFC-SEC

ECMA-385 NFC-SEC [39] specifies two security services and protocols over the NFC:

- Shared Secret Services: It establishes a shared secret key between the two peers, which the application will use at its discretion.
- Secure Channel Service: It provides the establishment of a link key by derivation of a shared secret key established by key agreement mechanism. Subsequent communication will be protected by the link keys in either direction across the channel.

The services will use a NFC-SEC cryptography part that defines the cryptographic algorithm to be used during security services.

ECMA-386 NFC-SEC-01 [40] is a security part that specifies the use of ECDH with a 192-bit key for the key agreement and the AES-128 for the secure channel. From the exchanged key, a key for encryption and a key for integrity are derived. AES-128 in CTR mode is used for confidentiality and AES-XCBC-MAC-96 for the integrity. AES-XCBC-MAC-96 is the AES-XCBC-PRF-128 [41] truncated to 12 bytes. A sequence number is protected by the integrity mechanism.

ECMA-409 NFC-SEC-02 [42] specifies similar security protections but using ECDH with 256-bits key for key agreement and AES-128 in GCM mode as authenticated encryption algorithm.

4.4.2. Issues

Older NFC standards did not include any notion of communication security. This made NFC exchanges vulnerable to eavesdropping, data modification, and data insertion [43]:

- **Eavesdropping**: It is possible since NFC is a wireless communication interface. The adversary needs knowledge on how to decode the sniffed RF signal. 10 cm is typically the maximum range, but it is possible to eavesdrop the communication from 1m to 10m (depending on the mode of operation) away from the target.
- **Data corruption**: It is possible by transmitting at the same time as a legitimate node. On the other hand, it does not allow an attacker to manipulate the actual data rendering this attack as a Denial of Service attack.
- **Data manipulation**: In data manipulation, the attacker wants the receiving node to receive some valid but manipulated data. The feasibility of this attack highly depends on the applied strength of the amplitude modulation. Furthermore, the attack is only possible for some bits due to the values used on the encoding of the data. Short operating distance and RF characteristics of NFC (“load modulation”) help keeping risk low.
- **Relay attacks:** It can be used two transponders in order to relay over a large distance the information that a reader and a node exchange. A proxy-node is placed near the reader and a proxy-reader is placed near the legitimate node.

4.5. Bluetooth Low Energy (BLE)

Also known as Bluetooth Smart, it reduces energy consumption and device costs when compared with classic Bluetooth. BLE is a technology introduced by the Bluetooth Special Interest Group (SIG) in the 4.0 version of the Bluetooth protocol specification [44]. The last version is the Bluetooth 4.2 [45].

Bluetooth®

The Bluetooth specification defines a complete communication stack for BLE composed of the physical layer, the link layer, the Logical Link Control and Adaptation Protocol (L2CAP) (not all of the L2CAP capabilities are available), which multiplexes the upper layer protocols, the Attribute Protocol (ATT), which defines a way of discovering and transporting attributes (values) and the Generic Attribute Profile (GATT), which defines a framework based on ATT for defining services. The stack is split between the Controller, which implements the physical and link layers, and the Host, which implements the upper layers. These two components communicate with each other using the standardized Host Controller Interface (HCI).

BLE like the classic Bluetooth operates in the unlicensed 2.4 GHz ISM band but it is designed for use cases and applications with lower data rates and has lower duty cycle. It employs a frequency hopping transceiver to combat interference and fading. Two multiple access schemes are defined: Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA). 40 physical channels, separated by 2 MHz, are used in the FDMA scheme. 3 are used as advertising channels and 37 are used as data channels. A TDMA based polling scheme is used in which one device transmits a packet at a predetermined time and a corresponding device responds with a packet after a predetermined interval.

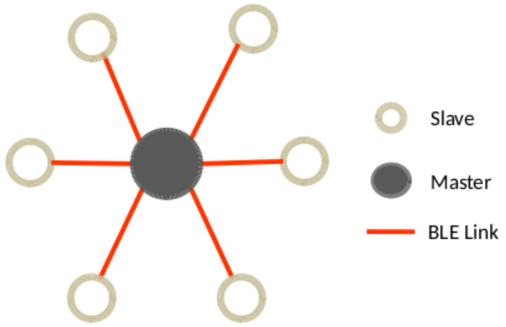


Figure 4.4: BLE topology

Only one device is the network master; all others being network slaves. All communication is between the master and slave devices. There is no direct communication between slave devices on the network.

IPv6 over BLE

It is specified in the RFC 7668 [46]. It describes how IPv6 is transported over Bluetooth low energy using 6LoWPAN techniques.

In BLE, direct wireless communication only takes place between a master and a slave. Nevertheless, two slaves may communicate through the master by using IP routing functionality per the RFC 7668 specification. Using the 6LoWPAN terminology, the BLE master have the role of a 6LowPAN Border Router (6LBR) and the slaves have the role of 6LowPAN Node (6LN).

In a typical scenario, the BLE network is connected to the Internet through the 6LBR router. In this scenario, the BLE star is deployed as one sub-net, using one /64 IPv6 prefix, with each spoke representing an individual link. The 6LBR is acting as router and forwarding packets between 6LNs and to and from Internet.

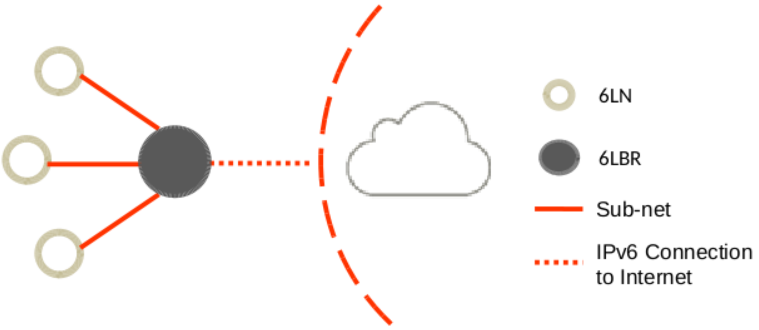


Figure 4.5: IP over BLE topology

Bluetooth Mesh

During the redaction of this report, a new specification was published, Bluetooth Mesh [47]. Mesh networking improves reliability, redundancy, security, speed, and overall performance. It uses a wireless ad-hoc architecture to connect servers and devices without requiring the input of a centralized hub or router. The points creating the architecture, called nodes, dynamically interact and reconfigure themselves based on available bandwidth, storage, and network pathways.

4.5.1. Security options

BLE offers various security services for protecting the information exchange between two connected devices. Most of the supported security services can be expressed in terms of two mutually-exclusive security modes called LE Security Mode 1 and LE Security Mode 2. These two modes provide security functionality at the Link Layer and at the ATT layer, respectively.

BLE uses AES-128 with CCM encryption and Message Integrity Check (MIC). When encryption and authentication are used in a connection, a 4-byte Message Integrity Check (MIC) is appended to the payload of the data channel PDU. Encryption is then applied to the PDU payload and MIC fields. It is also possible to transmit authenticated data over a non encrypted Link Layer connection. In this case, a 12-byte signature is placed after the data payload at the ATT layer.

Security Goal	BLE 4.0 / 4.1	BLE 4.2	Bluetooth Mesh
Confidentiality	AES-128 CCM (4-byte MIC)		AES-128 CCM (4 or 8 byte MIC)
Integrity			
Authentication			
Freshness	Counter incremented on every signed PDU		24-bit sequence number
Availability	Frequency hopping		Frequency hopping Mesh network
Authorization	Custom key exchange based on AES-128	P-256 ECDH HMAC-SHA-256	
Key type	Temporary key Short term key Long term key	Temporary key Long term key	Device key Network key Application key
Key management	Encryption key can be changed on application request		
Required power	very low	low	low

Table 4.5: Bluetooth security options summary

Each security mode accounts with different levels, which express requirements as to the type of pairing that has to be used.

		Pairing mode	Encryption	Integrity	Layer
Security Mode 1	Level 1	No	No	No	Link layer
	Level 2	Unauthenticated	Yes	Yes	
	Level 3	Authenticated	Yes	Yes	
Security Mode 2	Level 1	Unauthenticated	No	Yes	ATT layer
	Level 2	Authenticated	No	Yes	

Table 4.6: BLE security Modes and Levels

BLE version 4.0 and 4.1 uses a custom key exchange protocol unique to the BLE standard. In this setup, the devices exchange a Temporary Key (TK) and use it to create a Short Term Key (STK) which is used to encrypt the connection. How secure this process is depends greatly on the pairing method used to exchange the TK.

BLE version 4.2 upgraded BLE pairing to utilize P-256 elliptic curve cryptography in what are known as LE Secure Connections. Instead of using a TK and STK, LE Secure Connections use a single Long Term Key (LTK) to encrypt the connection. This LTK is exchanged/generated using Elliptic Curve Diffie-Hellman (ECDH) public key cryptography which offers significantly stronger security compared to the original BLE key exchange protocol. It has to be noted that the ECDH is not offering protection against MitM attacks since no party is authenticated. Numeric comparison, Out-of-Band and Passkey pairing models gives a protection against this kind of attack.

The value of the TK used for the key exchange is selected depending on the pairing model used. BLE uses four pairing models:

- **Just Works**: The Just Works association model is primarily designed for scenarios where at least one of the devices does not have a display capable of displaying a six-digit number nor does it have a keyboard capable of entering six decimal digits. The application may simply ask the user to accept the connection.
- **Passkey Entry**: The Passkey Entry association model is primarily designed for the scenario where one device has input capability but does not have the capability to display six digits and the other device has output capabilities. The user is shown a six-digit number (from "000000" to "999999") on the device with a display, and is then asked to enter the number on the other device. If the value entered on the second device is correct, the pairing is successful.
- **Out-of-Band**: The Out-of-Band (OOB) association model is primarily designed for scenarios where an Out-of-band mechanism is used to both discover the devices as well as to exchange or transfer cryptographic numbers used in the pairing process. It can be implemented with an out-of-band channel such as an NFC connection. The main advantage to this method is that a very large TK can be used, up to 128 bits, greatly enhancing the security of the connection.
- **Numeric Comparison**: Introduced in the BLE version 4.2, the Numeric Comparison association model is designed for scenarios where both devices are capable of displaying a six-digit number and both are capable of having the user enter "yes" or "no". The user is shown a six-digit number (from "000000" to "999999") on both displays and then asked whether the numbers are the same on both devices. If "yes" is entered on both devices, the pairing is successful.

Bluetooth Mesh

All messages are encrypted and authenticated using two types of keys. One key type is for the network layer communication, such that all communication within a mesh network would use the same network key. The other key type is for application data. Separating the keys for networking and applications allows sensitive access messages (e.g., for access control to a building) to be separated from non-sensitive access messages (e.g., for lighting). There are no non-encrypted or unauthenticated messages within a mesh network.

Three types of keys are defined:

- **Device key**: it facilitates confidentiality and authentication of key material between a Provisioner and a single node.
- **Application key**: it facilitates confidentiality and authentication of application data sent between intended nodes.
- **Network key**: it facilitates confidentiality, and authenticity of network messages. Shared among all of the network nodes.

A node may have knowledge of a single device key, multiple application keys, and multiple network keys.

To create a mesh network, a Provisioner is required. A Provisioner shall generate a network key using a random number generator. The Provisioner can then provision these devices to become nodes within the mesh network. Provisioning of the network key is based on the use of the ECDH key exchange mechanism.

4.5.2. Issues

- **Optional No security mode:** The end user can choose to configure the security mode to No security or to use non-authenticated pairing modes.
- **Legacy non-secure pairing modes**: In versions prior to the 4.2, Just Works and Passkey modes are susceptible to be attacked by eavesdropping attacks.
- **Legacy Passkey pairing method**: In versions prior to the 4.2, there is at least one theoretical Man in the Middle attack that is able to succeed without advanced knowledge of the passkey as detailed in the article [48].
- **Offline brute force on legacy pairing modes**: In versions prior to the 4.2, it is possible to perform an offline brute force of the confirm value for every possible Temporary Key between 0 and 999.999. If the master and slave used Just Works or 6-digit PIN, it is possible to quickly find the proper TK whose confirm matches the value exchanged over the air [49].
- **Just Works does not offer device authentication**: This method offers no way of verifying the devices taking part in the connection and thus it offers no Man in the Middle attack protection. This model is the most probably used by low-resources devices since the other models require an user interface or an extra method to perform Out-of-band key exchange.

4.6. Wireless Fidelity (WiFi)

Wireless Fidelity (WiFi) is a widely used wireless local area network technology defined by IEEE. It is defined by the IEEE 802.11 family of standards [50], with the first one introduced in 1997. Most devices support the newer standards IEEE 802.11n and IEEE 802.11ac.

WiFi communications use frequency bands around 2.4 GHz and 5 GHz; devices operate on frequency ranges centered on preset channels located within those bands. If two WiFi network channels overlap, interference can lead to lower throughput or even loss of connectivity. Wireless devices often support dynamic selection of channels. The IEEE 802.11 wireless networks operate in two basic modes: infrastructure and ad-hoc.

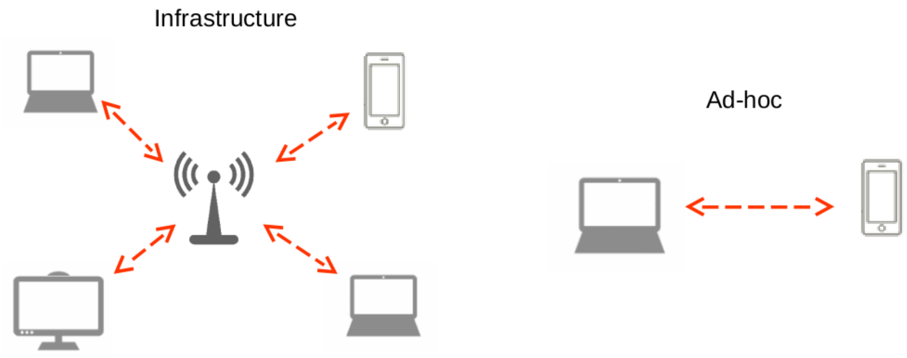


Figure 4.6: WiFi topologies

Infrastructure mode is the most common operation mode in which we could find wireless networks. In this operation mode, each wireless client connects directly to a central device called Access Point. This device is also the main responsible for handling the clients' authentication, authorization and link-level data security.

Ad-hoc mode is the less common operation mode in where each wireless client connects directly with each other. There is no central device managing the connections, meaning that each wireless client talks to each other freely. Security in this type of network is harder to implement because there is no central device that could authenticate and authorize the wireless clients.

WiFi HaLoW (802.11ah)

WiFi interfaces use more power compared to other communication technologies; this makes it undesirable for remote sensors with limited battery power. A new amendment was published targeting the low-resources devices.

The IEEE 802.11ah [51] operates in 900 MHz band, which helps to cut down power consumption, extend transmission range, improve propagation (the ability to transmit in the presence of many interferences) and penetration (the ability to transmit through various barriers, such as walls or floors). It is expected that the radius of a WiFi HaLoW device will be twice that of modern WiFi standards and up to one kilometer, which can be further extended using relay. Actual data-rates supported by the IEEE 802.11ah will not be too high with up to 26 channels that provide up to 100 Kbps throughput.

4.6.1. Security options

WiFi networks support both plain text communication and encrypted communication. Possible security protocols include Wireless Equivalent Privacy (WEP) and WiFi Protected Access version 1 or 2 (WPA or WPA2).

In the WiFi protocol stack, the security mechanisms locate between the medium access control layer and the physical layer. Both unicast and multicast communication can be secured using pairwise and group keys, respectively. Key establishment on smaller networks is based, typically, on pre-shared secrets. Additionally, alternative mechanisms, which have been specified in WiFi Protected Setup (WPS), include: 8-digit PIN entry, 'push button' model, and out-of-band channels such as NFC.

Security Goal	WEP	WAP	WAP2
Confidentiality	RC4		CCMP: AES-128/256 CCM or GCMP: AES-128/256 GCM
Integrity	CRC32	Custom keyed hashing function (20 bits security)	
Authentication	Encrypted CRC32		
Freshness	24 bits IV	48 bits IV	48-bit packet number
Availability	Dynamic selection of channels		
Authorization	Pre-shared key	Pre-shared key or EAP	Pre-shared key or EAP
Key type	40-128 bits pre-shared key	128 bits pre-shared key Session keys	Pairwise key Group key Session keys
Key management	Key is the combination of pre-shared key with the IV	Per packet key (TKIP)	Changed periodically and sent using specific key-wrapping key
Required power	low	medium	medium

Table 4.7: WiFi security options summary

The details of every security protocol is as follows:

- **WEP** was the default encryption protocol introduced in the first IEEE 802.11. t is based on the RC4 encryption algorithm, with a secret key of 40 bits or 104 bits being combined with 24-bit Initialization Vector (IV) to encrypt the plaintext message M and its checksum (CRC32).
- **WPA** is based on the 802.11i and consists of three main components: TKIP, 802.1x, and MIC. Important security improvements were implemented, such as key hierarchy that protects the exposure of the WPA main key from attacks and implementing 802.1x protocol for access control to the network. Using key hierarchy means that WPA does not directly use the main key to encrypt, instead the main key (Pairwise Master Key) is used to generate other temporal keys such as session keys, group keys, etc.; and recursively the session key is used to generate the per-packet encryption key. The IV is also expanded from 24 bits to 48 bits long and assigning it another role as a sequence counter for avoiding replay attacks. Improvement in packet integrity protection is made by implementing a especially designed cryptographically protected hashing function instead of using the CRC32 linear function. Temporal Key Integrity Protocol (TKIP) was introduced for this purpose.
- **WPA2** supports Counter Mode CBC-MAC Protocol (CCMP) or Temporal Key Integrity Protocol (TKIP). CCMP uses AES-128/256 (128/256-bit keys and 128-bit blocks) in Counter Mode with CBC-MAC (CCM) mode of operation. Setting WPA2 with CCMP is the recommended method for securing WiFi. It also supports GCMP based on the Galois Counter Mode (GCM) of the AES encryption algorithm.

  Two authentication methods are supported by WPA2: personal, which uses pre-shared keys, and enterprise, which requires an additional RADIUS authentication server and can use multiple underlying authentication mechanisms through Extensible Authentication Protocols (EAP). For pre-shared keys, the overall security of the wireless network relies on choosing a secret key that is hard to guess.

From the key exchanged, several temporal and static keys are derived (e.g. session keys, key-wrapping key). Temporal keys are changed periodically.

The AES-CCMP cipher suite uses a 128/256-bit key for encryption and decryption. An AES-CCMP key can be one of the following: Pairwise key to protect unicast traffic and Group key to protect multicast and broadcast traffic.

When a client initially connects to an access point, a secure challenge-based handshake to test whether both devices have the same pre-shared key. The handshake never reveals the pre-shared key. The purpose of the handshake is to derive a temporary secret key for encryption and integrity.

4.6.2. Issues

Some vulnerabilities have been found on the security of the WiFi standards:

- **WEP design flaws**: Efficient attacks exist for WEP [52]. WEP uses a RC4 stream cipher for data protection with a pre-shared secret key from 40 to 104 bits of length. RC4 has some weaknesses that were used in order to attack WEP in the first place. Next attack makes use of flaws in the WEP protocol itself, like the integrity mechanism based on CRC32 only and the lack of replay protection. Furthermore, some access points never change their WEP key, which once known the whole system is in jeopardy. In addition to that, WEP does not support mutual authentication. It only authenticates the client, making it open to rouge AP attacks. More complex and efficient attacks were devised exploiting the fact that IV is eventually repeated. The use of WEP for confidentiality and authentication is deprecated. The WEP algorithm is unsuitable for the purposes of the 802.11 specification but it is still widely used in practice.
- **WPA design flaws**: Vulnerabilities have also been identified in WPA [52]. WPA TKIP is also based on RC4 stream cipher. Traffic injection, man in the middle and key recovery attacks were devised. TKIP algorithm is unsuitable for the purposes of the 802.11 specification but it is still widely used in practice.
- **WPS design flaws**: Brute-force attack is possible against some WPS implementations [53]. Several design flows reduce the number of trials to be brute-forced before recovering the secret (e.g. WPS PIN.). Some implementation flaws were also found on commercial devices.
- **Default passwords**: Some default passwords or password based on the SSID and MAC address of the WiFi access point were used by some manufacturers and Internet Service Providers.

4.7. IEEE 802.15.4

The IEEE defined the IEEE 802.15.4 standard was designed as a basis for a protocol stack oriented towards short range, low data-rate and energy efficient communication.

It was originally introduced in 2003 [54], with several revisions and additions over the years 2006 [55], 2011 [56] and defines the physical (PHY) and Medium Access Control (MAC) layers for short range communications at 250Kbps.

In 2006, the standard was revised and added two more PHY options. The MAC remained backward compatible, but the revision added MAC frames with an increased version number and a variety of MAC enhancements, including the following:

- Support for a shared time base with a data time stamping mechanism.
- Support for beacon scheduling.
- Synchronization of broadcast messages in beacon-enabled personal area networks (PANs).
- Improved MAC layer security.

In 2011, the standard was revised to include the three amendments approved subsequent to the 2006 revision. This effort added four more PHY options along with the MAC capability to support ranging.

The latest version of the standard was released in 2015 [57] and includes previously released amendments that add additional PHY layers and modifications to the MAC layer which better support industrial markets. An enhanced acknowledgment frame that can carry data and can be secured. A variety of new PHY modulation, coding, and band options to support a wide variety of application needs. It introduces changes to the security text to correct errors and clarify the text and removal of the encrypt only mode.

There are three different types of devices that can exist in a network:

- **Full Function Device (FFD)**: a node that has full levels of functionality. It can be used for sending and receiving data, but it can also route data from other nodes.
- **Reduced Function Device (RFD)**: a device that has a reduced level of functionality. Typically, it is an end node which may be typically a sensor or switch. RFDs can only talk to FFDs as they contain no routing functionality. These devices can be very low power devices because they do not need to route other traffic and they can be put into a sleep mode when they are not in use. These RFDs are often known as child devices as they need other parent devices with which to communicate.
- **Coordinator***:* This is the node that controls the IEEE 802.15.4 network. This is a special form of FFD. In addition to the normal FFD functions it also sets the IEEE 802.15.4 network up and acts as the coordinator or manager of the network.

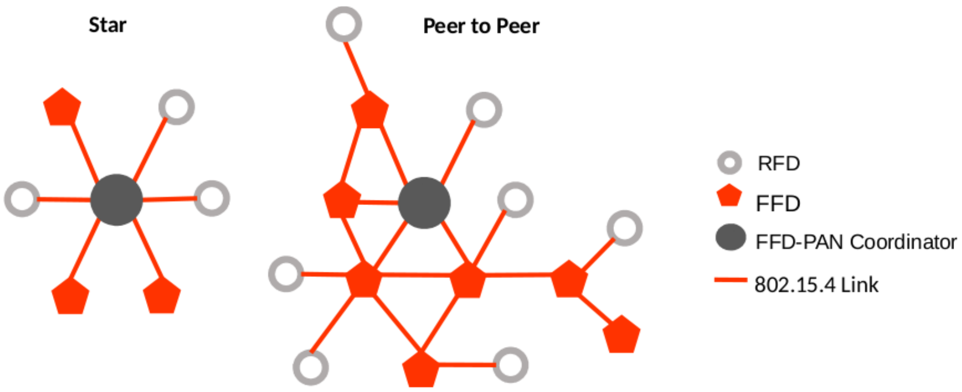


Figure 4.7: 802.15.4 topologies

4.7.1. Security options

Security Goal	802.15.4	
Confidentiality	AES-128 CCM*	AES-128, CTR mode
Integrity		AES-128, CBC-MAC (32, 64, 128 bits MIC)
Authentication		
Freshness	Frame counter per key included in the MIC computation	
Availability	Last version supports frequency hopping techniques	
Authorization	Not specified	
Key type	Network, group, link	
Key management	Not specified	
Required power	Very low	

Table 4.8: 802.15.4 security options summary

While in IEEE 802.15.4 the PHY layer does not offer any security, the MAC layer provides multiple security levels:

- Level 0 – No security
- Level 1 – MIC-32: Data authenticity (4-bytes MIC)
- Level 2 – MIC-64: Data authenticity (8-bytes MIC)
- Level 3 – MIC-128: Data authenticity (16-bytes MIC)
- Level 4 – Reserved
- Level 5 – ENC-MIC-32: Data confidentiality and data authenticity (4-bytes MIC)
- Level 6 – ENC-MIC-64: Data confidentiality and data authenticity (8-bytes MIC)
- Level 7 – ENC-MIC-128: Data confidentiality and data authenticity (16-bytes MIC)

The 802.15.4 specification refers to the message authentication code as a message integrity check (MIC) to differentiate it from media access control. An auxiliary security header is defined to include the security parameters and the MIC.

Octets: 1	0/4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Table 4.9: Format of the 802.15.4 Auxiliary Security Header

All security services are based on the AES-128 block cipher [58] coupled with the CCM* mode of operation [59]. Broadly, it first applies integrity protection over the header and data payload using CBC-MAC and then encrypts the data payload and MAC using AES-CTR mode.

Bits: 0 – 2	3 – 4	5	6	6 – 7
Security Level	Key Identifier Mode	Frame Counter Suppression	ASN in nonce	Reserved

Table 4.10: 802.15.4 Security Control field format

The CCM* mode is a slightly modified version of CCM, which gives more flexibility than the standard CCM: CCM* enables to use either authentication or encryption, while both are always required in CCM.

Although the standard specifies security as optional, the effect of having AES-128 in the specification is that most IEEE 802.15.4 compatible hardware platforms implement some form of hardware acceleration for AES-128. This ensures that the energy cost of enabling security on these platforms is minimal.

The cryptographic mechanism provides particular combinations of the following security services:

- **Data confidentiality**: Assurance that transmitted information is only disclosed to parties for which it is intended. Levels 5 to 7.
- **Data authenticity**: Assurance of the source of transmitted information (and, hereby, that information was not modified in transit). All levels but Level 0 (no security) and 4 (not supported).
- **Replay protection**: Assurance that duplicate information is detected by the use of a frame counter. Always enabled.

Cryptographic frame protection uses either a key shared between two peer devices (link key) or a key shared among a group of devices (group key), thus allowing some flexibility and application-specific trade-offs between key storage and key maintenance costs versus the cryptographic protection provided. If a group key is used for peer-to-peer communication, protection is provided only against outsider devices and not against potential malicious devices in the key-sharing group.

The IEEE 802.15.4 specification does not define how to do key management. The AES-128 block cipher uses 128 bit symmetric keys, but the generation, distribution and replacement of those keys is left for the upper layers. The standard does however include a key storing system inside the MAC PAN Information Base (PIB) and a way of implementing a form of access control at the MAC layer, with pair-wise keys or group keys, through the use of the MAC PIB and the Key Source field inside the Auxiliary Security Header.

4.7.2. Issues

IEEE 802.15.4 security has been considered in several researches. Since 802.15.4 is a wireless communication using known frequency bands it is susceptible to all the classic physical wireless attacks like jamming, frame injection, sinkholes, etc.

The following is a list of reported issues (it has to be noted that most of them are fixed on the 2015 version of the specification or can be fixed in upper layers):

- **Same-nonce attacks**: In previous versions of the 2015 standard, security level 4 was a level which provided only data confidentiality but without data authenticity. This security level is deprecated and shall not be used in implementation compliant with this standard. But if these versions are used, the same-nonce attacks are possible if, at least, two frames are encrypted with identical key and nonce (with AES-CTR, data is XORed with a key stream based on a nonce and a pre-shared key). If a nonce is used repeatedly, key streams remain identical and if two such frames are captured, it may be possible to decrypt them [60].

  To illustrate this, let’s consider that P and P’ are two payloads, C and C’ the two corresponding encrypted payloads and K, the key stream for both payloads. We thus have *C+C’ = (P+K) + (P’+K) = P+P’*. From here, mutually XORed plaintext payloads can be recovered using statistics or if parts of any of the two payloads are guessable. With the IEEE 802.15.4 standard, this can only be due to frame counters being identical.

- **Malleability attacks** rise from the combination of the two previous vulnerabilities: if a plain text can be retrieved using a same-nonce attack, then a simple XOR operation will reveal the corresponding keystream. From there, if a previously-used frame counter is accepted upon reception, instead of replaying a captured frame, an attacker could forge a new one based on the retrieved keystream and the corresponding counter.

- A 802.15.4-specific way to induce **DoS** is to increase the frame counter while replaying packets (it is not encrypted even in secured mode). Indeed, if an attacker replays captured frames with a counter higher than expected, targeted devices may update their counter accordingly. Consequently, future legitimate frames could be rejected as the counter they provide would now be invalid [60]. It is unfortunate as the purpose of this mechanism is the prevention of replay attacks.

- Another kind of **DoS** is achieved by sending fake conflict notifications to coordinators, thus forcing multiple conflict resolution procedures in the called **PANId conflict attack** [61]. This can be considered as a Rogue AP attack.

  PANId conflict is the situation when there is more than one PAN coordinator in the same personal operating space with the same PANId. When that happens, PAN coordinators can detect the conflict by receiving beacons or notifications from devices. Then, the conflict resolution procedure is executed: a new PANId is chosen and the affected coordinator broadcasts it to all its devices and, after re-synchronization with beacons, the network is operational again.

- **Spoofed ACK** frames can be forged easily as they are not encrypted, even in secured mode. If a malicious individual can carry out radio-jamming activities during a transmission before sending a spoofed ACK frame right after, hence deceiving the emitter about the proper reception [60]. Lost frames will not be re-emitted: this is again a form of **DoS**. In the last version of the specification, it is possible to protect the ACK frames solving this issue if configured.
- **GTS attacks** rely on the fact that portions of the superframe allocated by a coordinator are dedicated to particular devices and thus are supposed to ensure collision-free communications. Start and length of a GTS periods are given by GTS descriptors embedded within beacons, which are not encrypted, even in secured mode [61]. Therefore, a malicious individual could extract this information and then disrupt communications at the right time for a given device thus, yet again, a kind of **DoS**.
- **Specification implementation errors** is a potential source of security issues. There is one example of this situation that we are able to disclose because faulty components are publicly available: Digi XBee S1 IEEE 802.15.4 RF modules [62]. The nonce, it was supposed to be a concatenation of the 8-octet source address of the transmitting device, the 4-octet frame counter and the 1-octet key sequence counter. However, this last parameter was not correct. In fact, its value never increased and was always set to the value 4, which happens to be the security level of CCM* in encryption-only mode. Coincidentally, between the 2003 and the 2006 standards, the key sequence counter is replaced by the security level when creating the nonce. These modules were using IEEE 802.15.4-2006 for the security suites but IEEE 802.15.4-2003 for the MAC frame format.

4.8. ZigBee

ZigBee is a technology for short range wireless data transfer especially designed for wireless low-power devices. It is based on 802.15.4-2006 adding the network and application layers on top of the physical and MAC layers defined by the 802.15.4. It also provides enhanced security and support for mesh networks.

ZigBee is formed by a group of protocols maintained by the ZigBee Alliance, these protocols may be not compatible with one another. They share the same basis for their physical layers, but ZigBee, ZigBee Pro [63] and ZigBee IP [64] are otherwise incompatible with each other. On top of that several application profiles were published.

The first version of ZigBee specification, was released in 2004 (nowadays this version can be considered obsolete and thus it is not supported anymore in new ZigBee devices). The second version of ZigBee specification, also called as ZigBee was released in 2006. Then in 2007, ZigBee Pro was released, this version is used when the size of the ZigBee network is very large and enhanced security features are needed to protect the network.

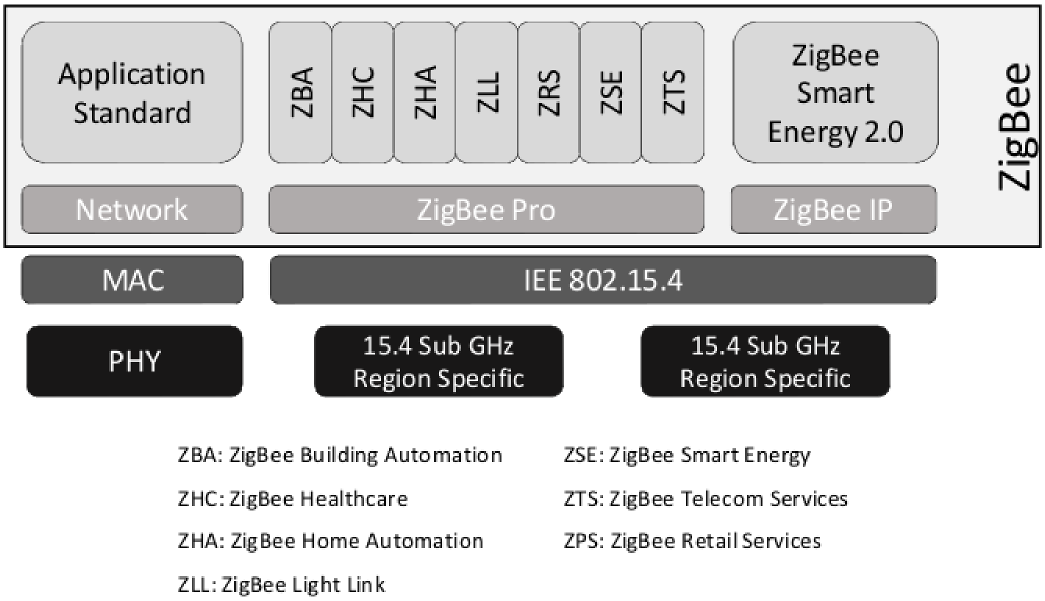


Figure 4.8: ZigBee architecture

There are two types of devices based on their resources:

- **Full-function device (FFD)** – It has full-function calculation capabilities, processing and memory is powerful enough to support complex computations. They are normally supplied by a battery. They are able to play any ZigBee logical role.
- **Reduced-function device (RFD)** – It has limited calculation capabilities. It operates at the low power situation, most of the time the device is asleep to save the power consumption. They are able to act as End devices.

Then, four types of logical devices are defined in a ZigBee network:

- **Coordinator** – It is a FFD device responsible for the whole network. It chooses the channel to be used by the network, starts the network by assigning how addresses are allocated on the other nodes, managing devices to join or leave the network and holding a list of nodes and routers.
- **Router** – It is a FFD device used to form and extend the ZigBee network topology. It is also in charge of choosing the optimal route path to transmit the data.
- **End device** – It can be either a FFD or a RFD. It is used to model the low power and low cost devices. It is only able to talk to a FFD that act as a parent (router or coordinator).

- **Trust Center** – It is in charge of ZigBee network security management. It can be combined with the device that has the role of Coordinator since security management is needed during the Coordinator responsibilities.

Several topologies are supported by the ZigBee devices:

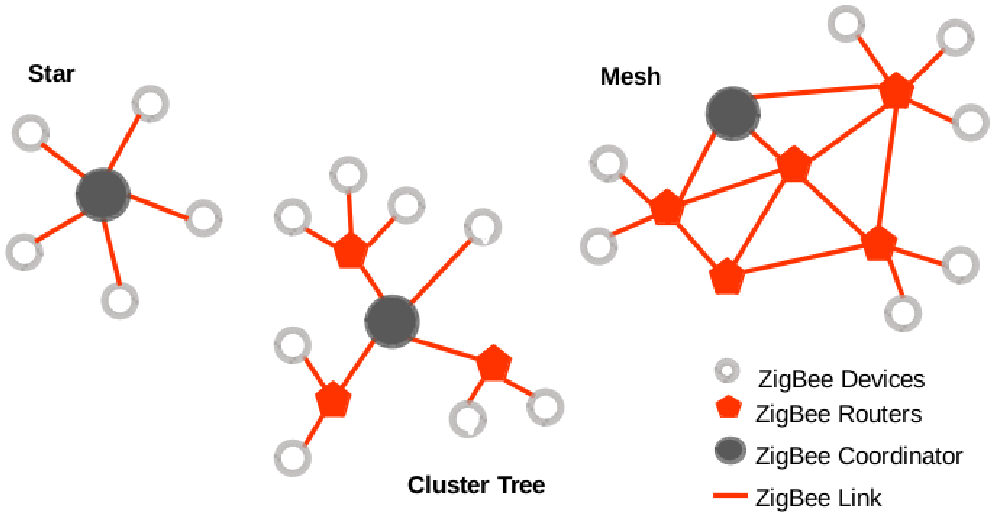


Figure 4.9: ZigBee topologies

Battery lifetimes up to several years are possible in ZigBee enabled systems due to power-saving modes and battery-optimized network parameters, such as a selection of beacon intervals, guaranteed time slots, and various enable/disable options.

End devices rely on a parent (a router or a coordinator) to remain awake and receive data packets. When an End device wakes up from a sleep mode, it sends a message (poll request) to its parent asking if there is any data available: upon receipt of the poll request, the parent sends a response to the poll request as well as the buffered data (if any) of the corresponding End device. In case there is no buffered data, the End device can return to a sleep mode.

ZigBee IP

ZigBee IP is a version of the ZigBee standard for mesh networking for remote control and sensing. It is based on the ZigBee smart Energy 2.0 profile. As the name indicates, the ZigBee IP standard provides for Internet operation using IPv6-based full wireless mesh networks.

It specifies a set of other standard specifications: 6LoWPAN adaptation layer, IPv6 network layer, TCP/UDP transport layer, ROLL RPL routing and PANA/EAP/EAP-TLS security.

It maps IPv6 addresses to link layer addresses and there is no need for application gateway. The system compresses the IPv6 headers using the techniques used in 6LoWPAN to reduce the transmission overhead, increase efficiency and use RPL routing protocol.

Each node on a network can be individually addressed using IPv6 routing and addressing protocol.

4.8.1. Security options

Security Goal	ZigBee	ZigBee IP
Confidentiality	AES-128 CCM (32, 64, 128 bits MIC)	
Integrity		
Authentication		
Freshness	Frame counter per key	
Availability	Mesh topology	
Authorization	Pre-shared key Trust Center link key Install codes	PANA/EAP-TLS PSK or ECDH with AES-128-CCM (64-bit MIC)
Key type	Master, Network, group, link	
Key management	New key from the Trust Center Multicast with old network key Unicast with link key	New key from the Trust Center Unicast with over PANA session
Required power	very low	low

Table 4.11: ZigBee security options summary

The present security architecture consists of the ZigBee coordinator which performs network joining and key distribution duties, here the Thrust Center concept was introduced, which plays three roles:

- **Trust Center** – forms a centralized network and allows routers and end devices to join the network if they have a proper credentials. Only the Trust Center can issue encryption keys. It also establishes a unique Trust Center Link key for each device as they join and link keys for each pair of devices as requested.
- **Network manager** – Maintenance and distribution of the network keys.
- **Configuration manager** – Provision of end-to-end security between devices.

ZigBee implements two extra security layers on top of the 802.15.4. First one is the network layer and second one is the application security layer.

- **Master key** – They are pre-installed in the device. Their function is to keep the link keys exchange confidential in the Key Establishment procedure.
- **Link keys** – These are unique between each pair of nodes and are managed by the application layer. More memory resources are required because there is a need for encrypting the information shared between two devices.
- **Network Key** – It's a key that is shared among all the nodes in the network. It is randomly generated at different intervals by the Trust Center. Only if the node has the network key they can join the network. The new network key is shared using the old network key (broadcast) or the link keys (unicast).

ZigBee uses AES-128 with CCM* for data confidentiality and authentication. There are two policies that the Trust Center (the one which generates the network key) follows:

- **Commercial mode** (High security): Shares the master key and a different link key for each device in the network.
- **Residential mode** (Standard security): Share only the Network key (this is done in order to cope with low memory resources). Unsecured key-transport of Network Key for every new device that joins the network or network key update procedure.

The Trust Center periodically creates, distributes and then switches to a new network key. Updated keys are sent to each device encrypted. It can be protected using the soon-to-be-old network key or using the each of the Link keys per each node.

Application layer encryption is supported by creating an application level Link Key between two devices' applications.

Joining a centralized network with a Trust Center requires to provide credentials that have been previously entered into the Trust Center out-of-band (Trust center Link key):

- There is a default Trust Center Link key defined in the specification.
- From ZigBee 3.0, the option to add a Link Key per each joining device is derived from an install code. The install code shall be manually entered to the Trust Center via some kind of out-of-band method.

ZigBee IP

Zigbee IP provides end-to-end security using TLS 1.2 protocol, link layer frame security based on AES-128-CCM algorithm and support for public key infrastructure using standard X.509 v3 certificates and ECC-256 cipher suite.

Protocol for Carrying Authentication for Network Access (PANA) is a network-layer protocol with which a node can authenticate itself to gain access to the network. PANA does not define a new authentication protocol and rather uses EAP over User Datagram Protocol (UDP). It is used to authenticate joining nodes and to transport the network security material from the Coordinator to each authenticated node in the ZigBee IP network. It is used as the EAP transport for carrying authentication data between a joining Node and the Authentication Server.

Extensible Authentication Protocol (EAP) is an authentication frame work that supports multiple authentication methods. EAP runs directly over the link layer and supports duplicate detection with re-transmission but does not allow fragmentation of packets.

It used TLS 1.2 handshake to provide mutual authentication between the node and the coordinator. Two mandatory cipher suites are specified: TLS_PSK_WITH_AES_128_CCM_8 and TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8. The PANA session remains open for the purposes of network key update and maintenance.

4.8.2. Issues

Since ZigBee is based on versions of the 802.15.4 prior of the 2015 version, it inherits all of the 802.15.4 issues for the physical and MAC layers (see section 4.7.2). Several issues directly related to the ZigBee were identified in [65]:

- **Residential mode**: When the Residential mode (Standard Security) policy is used, the network key is transmitted unsecured over-the-air and thus this is a serious vulnerability for the security of the ZigBee enabled networks leading to the conclusion that the Standard Security level cannot be recommended for safety critical systems.

  However, it is possible to manually pre-install network keys onto each legitimate device of the ZigBee network, but this is clearly a trade-off between usability and security, at least when the size of the network is large: therefore, the network administrator is likely to opt for less secure but more usable options.

  Some profiles like ZigBee Smart Energy does not allow this. These use public key ECC certificates, which are bound to the device, to protect the key exchange.
- **Default keys**: On the other hand, other application profiles like Home Automation and the Light Link profiles specify that the default Trust Center Link Key is “ZigBeeAlliance09”. It introduces a high risk to the secrecy of the network key if an attacker is sniffing while device commissioning.
- Another security concern lies in the shared network key. By compromising one of the nodes of a ZigBee network, an attacker could dump the node’s internal memory and retrieve this network key, giving them access to the network. Such a scenario may be particularly dangerous in certain configurations used for home networks that have sensors deployed outside of the house, such as an external lamp. On the other hand, to obtain the current Network key is not useful to be able to decrypt past messages protected by older Network keys.
- **ZigBee End-Device Sabotage Attack**: An attacker impersonates a ZigBee router or coordinator in order to abuse the End device poll requests. It sends broadcast or multi-cast replies to all poll request of legitimate End devices thus making them to constantly waking up, dramatically increasing the power consumption and eventually leading to battery exhaustion. It is a kind of DoS attack.

4.9. Thread

The Thread is an open standard for reliable low power wireless device-to-device communication.

It is based on 802.15.4 adding the network and transport layers on top of the physical and MAC layers defined by the 802.15.4. The IEEE 802.15.4 2006 version of the specification is used for the Thread version 1.1.1, 2017 [66]. Spread spectrum technology is used at the physical layer to provide good immunity to interference.

Upper layers are based on adaptation layer 6LoWPAN to be able to route IPv6 communications. All devices have IPv6 addresses plus a short Thread address. Devices use RPL routing to forward packets. A routing table is populated with network addresses and the appropriate next hop.

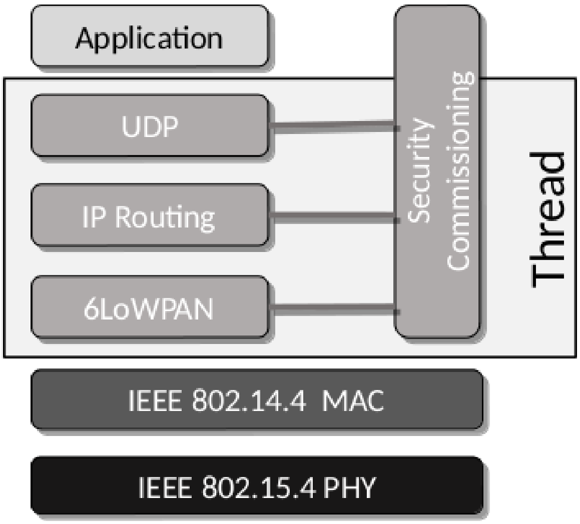


Figure 4.10: Thread architecture

The stack is designed to provide secure and reliable operations even with the failure or loss of individual devices. While there are a number of devices in the system that perform special functions, the Thread design is such that they can be replaced without impacting the ongoing communication. For example, a Sleepy End Device Child requires a Parent router for communications so this Parent represents a single point of failure for its communications. However, the Sleepy End Device can and will select another Parent Router if its Parent Router is unavailable. Four device types are defined:

- **Border routers**: A Border Router is a specific type of router that provides connectivity from the 802.15.4 network to adjacent networks on other physical layers (Wi-Fi, Ethernet, etc.) acting as a gateway. It offers routing services for off network operations. A Thread Network typically contains one or more Border Routers.
- **Routers**: Routers provide routing services to network devices. They maintain neighbor, child and routing tables and connect with each other to maintain the mesh network. Routers also provide joining and security services for devices trying to join the thread Network. Routers are not designed to sleep. Routers can downgrade their functionality and become Router-Eligible End Devices (REEDs).
- **Router-Eligible End devices**: REEDs can become routers but due to the network topology or conditions these devices are not acting as routers. As such, a REED is not a specific device type but a state of a routing-capable device when in the Thread Network. These devices do not forward messages or provide joining or security services for other devices in the network but listens to routing information messages. If necessary, the network manages the transition of a device from REED to router without user interaction.

- **Sleepy End devices**: Sleepy End Devices (SEDs) are host devices. They communicate only through their parent router and cannot forward messages for other devices.
- **Leader**: A leader manages a registry of assigned router identifications and accepts requests from REEDs to become routers. All information contained in the Leader is present in the other Thread Routers. So, if the Leader fails or loses connectivity with the Thread network, another Thread Router is elected, and takes over as Leader without user intervention.

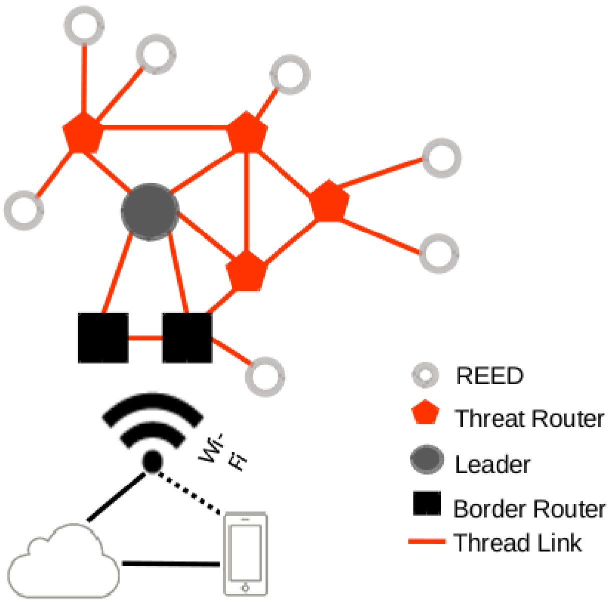


Figure 4.11: Thread topology

Devices join a network as either a sleepy end device or a REED. A REED can learn the network configuration, then it potentially requests to become a Thread Router.

All routers exchange with other routers their cost of routing to other routers in the network in a compressed format using MLE (Mesh Link Establishment). MLE operates below the routing layer and uses one hop link local unicasts and multicasts between routers.

MLE messages are used to identify, configure, and secure links to neighboring devices as the topology and physical environment change. MLE is also used to distribute configuration values that are shared across the network such as the channel and PAN.

4.9.1. Security options

The Thread Network is designed to provide a high level of security during the process of adding devices to the network and during normal network operation. During the joining process, devices must be specifically authenticated and authorized, and required to complete a key agreement mechanism.

Security Goal	Thread
Confidentiality	AES-128 CCM (32, 64, 128 bits MIC)
Integrity	
Authentication	
Freshness	Frame counter per key
Availability	Self-healing Mesh topology
Authorization	DTLS handshake with Commissioning credentials DTLS handshake with Joining credentials
Key type	Network key, MAC key, MLE Link keys
Key management	Key rotation based on synchronized key generation on every device
Required power	Very low

Table 4.12: Thread security options summary

Once on the network, all communications are secured with a MAC key based on the 802.15.4 MAC security. ENC-MIC-32 is the default security level for Thread MAC security.

The Thread network is protected with a network-wide key (Network key) from which two keys are derived, one for the underlying MAC layer and another one for the MLE messages. HMAC-SHA256, where the key is the Network Key and the message is a sequence counter, is used to produce both keys.

MAC security is used for all the messages. Security is enabled by default and mandatory for all devices. ENC-MIC-32 is the default value for Thread MAC security. The same happens for the MLE messages.

Commissioning must be able to take place in a system where a Joiner that wishes to participate in the Thread Network is authenticated using a device known as a Commissioner. The Commissioner have some sort of user interface.

Adding a new device to a Thread Network is the process of a human administrator authenticating it to the network as eligible for joining, followed by the commissioning of the device with the master key for the network over a secured channel. Only after completing this process, the new device is qualified to attach and participate on the secured Thread Network.

Thread defines a protocol for securely authenticating, commissioning and joining new, non-trusted devices to a mesh network [67]. Two steps are defined:

1. Commissioner candidate is authorized. There are two types of commissioners:
   - **External commissioner**: It resides in the exterior of the Thread network and it is commonly an application on a smartphone or computer. The commissioning application must authenticate itself to the Border Router by means of a successful DTLS session using out-of-band pre-shared commissioning credentials (6 to 255 bytes passphrase). Then, the Border Router arbitrates with the Leader on behalf of the external commissioner to be authorized as the network commissioner.

   - **Native commissioner**: It resides in the Thread network and it is commonly a Router that acts also as the commissioner. An authorization petition is directly sent to the Leader.

2. The joiner device is commissioned. The joiner device is attached to a Joiner Router (will be the parent router of the device once authorized) that will forward the DTLS handshake messages between the joiner device and the commissioner. Once the joiner device is authenticated with a successful DTLS session using out-of-band pre-shared joining credentials (6 to 32 bytes passphrase), a pair-wise key will be established.

3. The Network key is sent to the joiner device protected with the pair-wise key.

The fundamental security used during the joining for authentication and key agreement is an elliptic curve variant of J-PAKE (EC-JPAKE), using the NIST P-256 elliptic curve. J-PAKE is a PAKE (Password Authenticated Key Exchange) with “juggling” (hence the “J”). It essentially uses elliptic curve Diffie-Hellman for key agreement and Schnorr signatures as a Non-Interactive Zero-Knowledge proof mechanism to authenticate two peers and to establish a shared secret between them based on the passphrase.

The first device in a network, typically the initial Leader, should be out-of-band commissioned to inject the correct user generated Commissioning Credentials into the Thread Network, or provide a known default Commissioning Credential to be changed later.

Thread defines key rotation mechanism that is synchronized with the neighboring devices by the use the Key Index field present in the 802.15.4 MAC layer’s security header. Key switching is performed when the current key rotation time of use is expired or the node receives and successfully processes an incoming message with Key Index equal to the next key index on the key rotation pool of keys.

4.9.2. Issues

Since Thread is based on versions of the 802.15.4 prior of the 2015 version, it inherits all of the 802.15.4 issues for the physical and MAC layers (see section 4.7.2). It has to be noted that no security analysis was found about the security of the Thread technology.

- A first security concern lies in the shared Network key. By compromising one of the nodes of a Thread network, an attacker could dump the node’s internal memory and retrieve this Network key, giving them access to the network.
- Furthermore, since the key rotation is changing the MAC and MLE keys but the Network key is always the same and that the diversification factor is a monotonic counter, compromising the Network key may enable the attacker to compute previous and future MAC and MLE keys being able to decipher past and future communications.

4.10. Z-Wave

Z-Wave is a low-power wireless communication protocol. It was designed for remote control applications in residential and small-size commercial environments. It has an architecture similar to ZigBee. Z-Wave is a complete protocol stack that covers all layers, from physical to application layer.

All Z-Wave devices uses sub-gigahertz radio frequencies as per the ITU-T G.9959 specification [68] for MAC and PHY layers. It uses a sub-1GHz frequency range, this way, it avoids interference with other wireless technologies used in domestic context at the 2.4 GHz range (Wi-Fi, Bluetooth, ZigBee, etc.). Z-Wave provides a range of 30 meters for point-to-point communications and allows a transmission rate of up to 100 kbps.

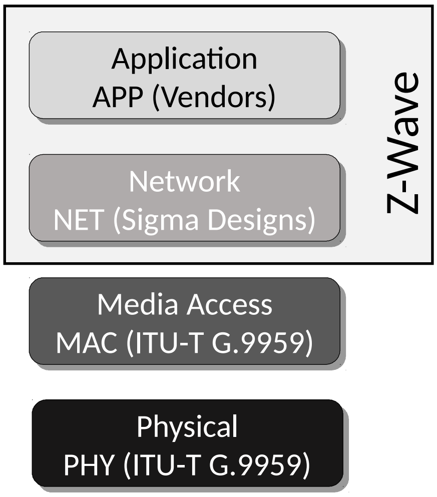


Figure 4.12: Z-Wave architecture

The simplest network is a single controllable device and a Primary Controller. Additional devices can be added at any time, as can secondary controllers. A Z-Wave mesh network consists in a controller device and up to 232 nodes. Each Z-Wave network is identified by a Network ID, and each device is further identified by a Node ID. The Network ID (also called Home ID) is the common identification of all nodes belonging to one logical Z-Wave network. The Network ID has a length of 4 bytes (32 bits) and is assigned to each device, by the primary controller, when the device is "included" into the Network.

During bootstrapping, the Primary Controller asks the new node to discover its neighbors. Thanks to the neighbor nodes information, the Primary Controller builds a network map and knows the different possible routes to reach a node.

In order to determine the best route to a destination node, each device in the Z-Wave network maintains a network topology that indicates all other devices in proximity.

Z/IP Clients and Gateway

The Z/IP Gateway bridges the low-power Z-Wave wireless communications protocol with the Internet of Things (IoT) by assigning a unique private IP address to each device within a Z-Wave network.

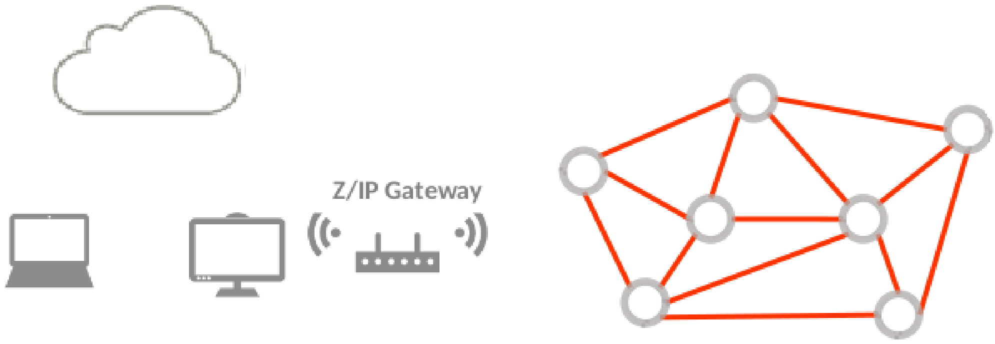


Figure 4.13: Z-Wave Z/IP topology

The Z/IP Gateway is putting Z-Wave command classes' payload on a UDP packet when sending data from the Z-Wave network to the LAN of consumer devices and the other way around.

Z/IP is a Z-Wave Command Class encapsulation datagram for sending Z-Wave datagrams (Command Class messages) to Z/IP enabled devices. This makes Z/IP communication independent of the Link Layer. All that matters is that the receiving device supports IP, UDP port 4123, Z/IP and Z/IP Command Classes.

Z/IP Gateway's capabilities include:

- IPv6-compliant, Z-Wave acts as Link Layer to IP.
- Internet Protocol routing: Transmitting Z-Wave UDP/IP datagrams between Z-Wave devices and IP address.
- Translating IP address to Z-Wave HomeID+NodeID.
- DHCP Client (assigning NodeIDs to PAN device and assigning IP address to those devices).
- Full support for Internet Control Message Protocol (ICMP) ping of devices.
- Caching of device capabilities, allowing IP devices to discover and identify all Z-Wave devices, including sleeping devices.

4.10.1. Security options

Wireless security was enabled on the Z-Wave Plus in 2013 [69]. When secure transmission mode is enabled, the frame payload is encrypted and an 8-byte authentication header is added.

It has to be noted that there is the option of devices using commands from a supported command class that is not required by the device to use the security layer.

Security Goal	Z-Wave Plus	Z-Wave S2
Confidentiality	AES-128 - OFB	AES-128 – CCM (64-bits MAC)
Integrity	AES-128 – CBC-MAC (64-bits MAC)	
Authentication		
Freshness	64-bit nonce (PRNG)	Pre-agreed nonce and CTR_DRBG (13-bytes)
Availability	Mesh topology	
Authorization	Custom protocol with known pre-shared Master key	ECDH-256 with user interaction
Key type	Network	Network and Group
Key management	Protected by known pre-shared Master key	Out-of-band authenticated ECDH with temporary keys
Required power	Very low	Medium

Table 4.13: Z-Wave security options summary

The secured commands encryption and authentication services are provided by three AES-128 keys: Network key, and then the encryption (ENC) and authentication (MAC) keys (both of them derived from the network key).

The Network key is generated by the network controller by Pseudo Random Number Generator (PRNG) and sent to all the devices requiring cryptographic services. The key exchange is performed encrypted using a default key hard-coded in firmware.

The encryption and authentication keys are obtained by encrypting two 16-byte seed values, also hard-coded in firmware, using AES in ECB operation mode and the network key.

Z-Wave computes a Message Authentication Code (MAC) using CBC-MAC with AES, the 8 bytes authentication header, in order to ensure data origin authentication and data integrity. It also uses 64-bit nonce values (generated using PRNG) when computing the MAC in order to provide anti-replay protection (freshness).

The frame payload is encrypted using AES in OFB operation mode, in order to provide data confidentiality.

S2 commands

In 2016, the Z-Wave Alliance announced stronger security standards for devices known as Security 2 (S2) [70]. It improves the used encryption standard and mandates new pairing procedures for each device, with unique PIN or QR codes on each device. S2 separates the devices into different groups with different keys.

The S2 authentication process allows an including controller to verify that a joining node is indeed the physical device that it claims to be. Depending on the user interface, an including controller may allow the installer to enter a device specific key that can be read visually or scanned as a QR code. This step ensures which devices are included into the network. This key is the first 16 bytes of the 32-byte long ECDH public key of the joining node. The rest of the key is sent during the joining protocol. With ECDH, a temporary link key. The link key allows an including controller to transfer the network key securely to a joining node.

The nonces required by CCM as input are generated by a CTR_ DRBG algorithm, which allows the two parties to stay synchronized and not have to exchange nonces before each communication. Should decryption fail on the receiver side, it will request a fresh nonce from the sender and sync back up.

Z/IP Clients and Gateway

The Z/IP Gateway [71] controls access to the Z-Wave network by only forwarding commands from trusted LAN clients or from a trusted Internet host.

LAN hosts and Z-Wave nodes communicate via a Z/IP Gateway which terminates the DTLS encryption and strips Z/IP and IP headers before forwarding Z-Wave commands securely in the Z-Wave network. DTLS 1.0 with PSK-AES128-CBC-SHA or PSK-AES256-CBC-SHA may be used.

The Pre-shared key used to perform the key exchange is provided by the Gateway. It is printed on the device or shown by a display upon physical interaction with it. It is the same for all the devices in the LAN network.

Connection to an Internet portal is protected by TLS based tunnel. The portal may be configured to only accept trusted gateways and the gateway to only accept trusted internet hosts. Z-Wave gateway monitors periodical heartbeat signals from all nodes in the Z-Wave network so that jamming can be detected within minutes after the attack is initiated.

4.10.2. Issues

- The first public vulnerability research was published in 2013 [69]. It was discovered **an implementation error** on a commercial door lock that allows an attacker to reset the established network key to a known value (remote re-keying). Then, the injection of unauthorized commands to the Z-Wave device was possible opening the door lock without using the controller.

  It is also discovered that the initial network key exchange was protected by a **hard-coded temporary default key** in the chip's firmware with **all its bytes equal to zero**.

- In [72] a hardware key extraction vulnerability was identified. It was found that the network key was stored in an external persistent memory without any protection against physical memory dump.

  It is also discovered that the authentication and the encryption key on the device that are derived from the network key with some seeds with values of all 5s and all As respectively.

- In [73] some vulnerabilities were found on the Z-Wave gateway. They were related to the absence of authentication on the management web console of the gateways and several classic web vulnerabilities like path traversal, Server side request forgery and Cross-site request forgery. Communications between the gateway and the Internet server were also non-protected. During BlackHat 2013 several commercial Z-Wave devices were shown to be under-protected with these kinds of vulnerabilities.

4.11. SigFox

SigFox technology is a good fit for any application that needs to send small, not very frequent bursts of data. Examples such as basic alarm systems, location monitoring, and simple metering are one-way systems that might make use of such network infrastructure.

The SigFox network is designed for small messages sent every now and then. It is not appropriate for high-bandwidth usages. It is designed for devices that don’t have a lot to say, need to be very inexpensive, require very small power budgets and require very long range.

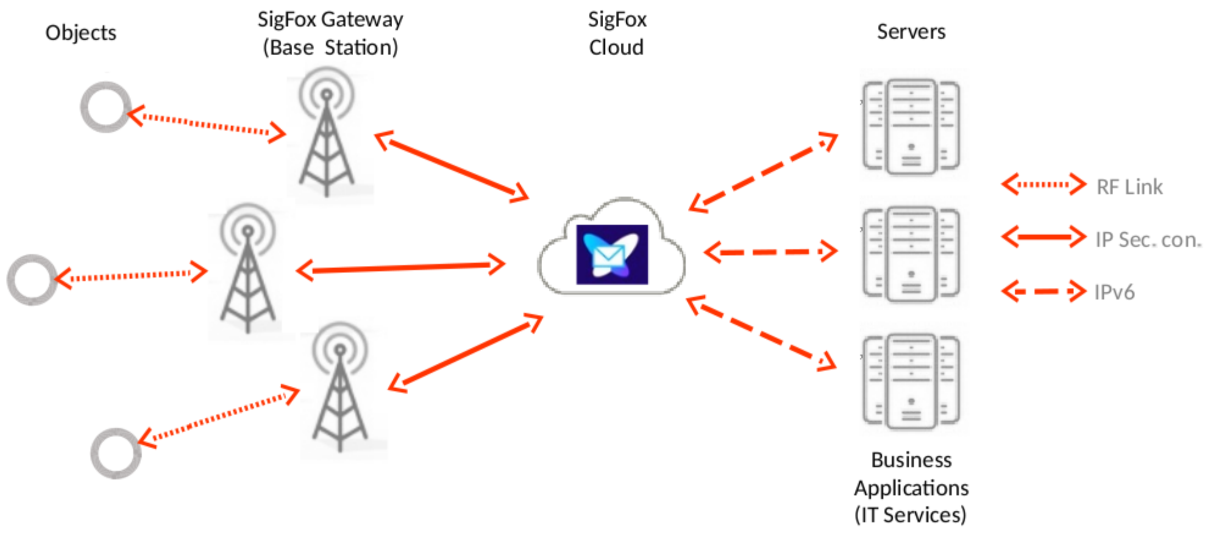

Objects
SigFox Gateway (Base Station)
SigFox Cloud
Servers
RF Link
IP Sec. con.
IPv6
Business Applications (IT Services)

Figure 4.14: SigFox topology

SigFox wireless systems send very small amounts of data which is 12 bytes for the uplink (maximum 140 per day) and 8 bytes for the downlink (maximum 4 per day). The downlink usage is intended for configuration and data requests.

It has a very slow rate from 100 bps to 600 bps using standard radio transmission methods namely phase-shift keying (D-BPSK) for uplink and frequency-shift keying (GFSK) for downlink.

It runs in ultra-narrow band (UNB) and is able to send lots of simultaneous, small frames (in time) achieving a high capacity of the network. This allows the receiver to only listen in a tiny slice of spectrum which mitigates the effect of noise. It requires an inexpensive endpoint radio and a more sophisticated base station to manage the network.

In the SigFox network the devices are always initiating the communication exchanges to save battery and provide certain security since an adversary will have smaller windows of opportunity.

4.11.1. Security options

Security Goal	SigFox
Confidentiality	AES-128 based encryption (optional)
Integrity	Authentication token based on AES-128 (2 - 5 bytes MIC)
Authentication	
Freshness	Sequence counter inside the authenticated payload
Availability	Same message sent several times at random moments and different frequencies
Authorization	Personalized during manufacturing
Key type	Authentication key Encryption key
Key management	None
Required power	Very low

Table 4.14: SigFox security options summary

SigFox is a proprietary solution and it is difficult to find information about the actual security mechanisms that implements. The following is information gathered from SigFox white papers [74] and [75], a presentation about SigFox in IETF 96 [76] and a ST Microelectronics' data sheet of a micro-controller intended to be used for SigFox connection [77].

In a SigFox network, each device stores a unique ID, a Network Authentication Key, and an Encryption Key, the last two being secret, and based on AES-128. The keys are provisioned during manufacturing.

Each message sent or received by a device contains a cryptographic token generated using the Authentication Key. This token authenticates the sender. The token is based on AES-128 computations and the result is truncated to 2 - 5 bytes.

To make sure there are no copies or duplication possible, the system inserts a sequence counter. Furthermore, the protocol sends each message at three random times and on three different frequencies. As a result, some resistance against Denial of Service attacks is achieved.

By default, data is conveyed over the air without any encryption. However, depending on the application, this data may be very sensitive and its privacy must be guaranteed. SigFox gives customers the option to either implement their own end-to-end encryption solutions or to rely on an encryption solution provided by the SigFox protocol.

The communications between the Base Stations and the Cloud services and Business Applications are sent through a VPN. Cloud on and Business Applications servers are secured and distributed physically. Connection to Business application is through HTTPS.

4.11.2. Issues

No security analysis was found about the SigFox security but some issues can be identified:

- **No key management**: The keys used for data protection are never changed. If one of these keys is compromised future and past communications can be eavesdropped. In such a case, message injection is also possible.
- **Truncated MIC**: It seems that the MIC is based on a AES-128 computation (16 bytes block size) and then truncated to 2-5 bytes to create the authentication token. Reducing the size of a cryptographic MIC should be done carefully since it reduces the space for brute forcing all the possible values.
- **Replay attack**: It is not clear what happens when the sequence counter value reaches its maximum value. If the counter is reset, then it enables replay attacks since the same sequence number will be used with the same key. An adversary can wait to the counter to overflow to be able to replay messages.
- **Optional encryption**: The fact that the encryption is optional will make that most of the messages are not protecting its confidentiality.

4.12. EC-GSM-IoT, LTE-M and NB-IoT

Through the modification of their cellular networks, the 3GPP have standardized three low power wide area network solutions operating in licensed spectrum bands.

- **Extended Coverage GSM IoT (EC-GSM-IoT)**: is a 3GPP Release 13 feature based on eGPRS and designed as a high capacity, long range, low energy and low complexity cellular system for IoT communications. The optimizations made in EC-GSM-IoT are designed to allow the technology to be introduced into existing GSM enabling extensive coverage. It introduces a security framework comparable with 4G standards.
- **LTE Machine Type Communication Category M1 (LTE-M)**: It is a 3GPP Release 13 feature with three main objectives: reduce complexity to the LTE, increase coverage and improve battery life, while allowing reuse of the LTE installed base. It still provides many similar features to legacy LTE, opening the possibility for a LTE-M to integrate voice in IoT applications.
- **Narrow-band IoT (NB-IoT)**: It is a 3GPP Release 13 feature that reuses various principles and building blocks of the LTE physical layer and higher protocol layers to enable rapid standardization and product development. NB-IoT has been designed to offer extended coverage compared to the traditional GSM networks.

Several functions were designed to support IoT services and also for devices that are potentially constrained by their battery technologies:

- **Power saving mode**: This capability is focused on reducing the power consumption enabling the devices to enter a new deep sleep mode. It is designed for infrequent data transmission and that can accept a corresponding latency in the mobile terminating communication.
- **Extended idle-mode discontinuous reception**: It allows the device to turn part of its circuitry off during this period to save power. The device is not listening for paging or downlink control channels, so the network should not try to contact the device.
- **Enhancements for cellular IoT applications**: Optimizations suited for applications involving lower data volumes transfer and for applications where the possible range of data volume transmission is unpredictable and can vary quite significantly in frequency and volume and introducing the concept of connection suspending and resuming.

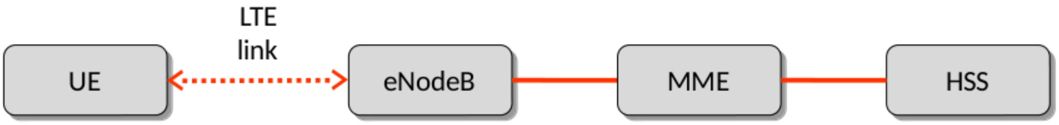


Figure 4.15: LTE access network architecture

The entities that appear in this case are the User Equipment (UE), the eNodeB (the antenna), the Mobility Management Entity (MME) and the Home Subscriber Server (HSS) who will authenticate the UE.

4.12.1. Security options

Security Goal	EC-GSM-IoT / NB-IoT / LTE-M
Confidentiality	AES-128 CTR mode or SNOW 3G
Integrity	(4 byte MIC) AES-128 CMAC or SNOW 3G
Authentication	
Freshness	Sequence counter
Availability	Frequency hopping techniques
Authorization	EPS AKA procedure based on a pre-shared secret.
Key type	Pre-shared key Session Ciphering key Session Integrity key
Key management	Each time the UE access the network a new set of session keys is derived. Key derived with keyed HMAC-SHA256.
Required power	moderate

Table 4.15: 3GPP IoT security options summary

All three technologies share similar network architectures and provide similar transport layer security mechanisms and constraints. Several security mechanisms are available [78].

They are mostly the ones used in the standard LTE networks:

- **LTE authentication**: Performs mutual authentication between the UE and the network. It is based on a pre-shared key and a cryptographic computation over a nonce generated by the HSS. The MME sends the nonce (RAND), a key derivation index (K_{ASME}) and an authentication token (AUTN) computed using the shared key. The UE can verify the authenticity of the HSS and compute its authentication token (RES) that will be verified by the MME.
- **Securing of communication channels**: Once the UE and the HSS are authenticated, Ciphering and Integrity keys are derived from the combination of the pre-shared key and the RAND that will be used to protect further communications.
- **Secure provisioning and storage of device identity and credentials**: It is required the use of a UICC to store the UE identification and secret keys. This type of device is designed to be resistant to physical attacks.
- **Ability to support "end-to-end security" at the application level**: 3GPP security mechanisms can be used by the application layer for application authentication and data confidentiality, but encryption would not be used, if not needed.

The cryptographic algorithms supported are SNOW 3G (stream cipher designed by Lund University) and AES-128. Confidentiality is protected by the use of CTR mode and Message Authentication Codes are computed with a CMAC algorithm.

4.12.2. Issues

Several issues were identified in the document [79], mainly due to the first unprotected messages before mutual authentication is performed:

- **Eavesdropping, Man in the middle attack (MitM)**: An adversary can take advantage of a known weakness in LTE wherein the user identity transference occurs non-encrypted, in clear text between the UE and the eNodeB, during the initial attach procedure. This allows an eavesdropper to track the user cell-location or launch a Man in the Middle attack by user IMSI impersonation and relay of user messages using IMSI catchers.
- **Temporary blocking mobile devices**: Since the Tracking Area Update (TAU) reject messages are not protected, an adversary can spoof such a message to block the access to the network to a target device provoking a denial of service attack.
- **Soft downgrade to GSM**: An adversary can trigger a soft downgrade of the connection to GSM, known for being more insecure. The same TAU Reject and Attach Reject messages, a rogue base station can indicate a victim mobile device that it is not allowed to access 3G and LTE services on that given operator. The target device will then only attempt to connect to GSM base stations. An attacker could combine this with a rogue GSM base station, which would open the doors to a full Man in the Middle attack, fully eavesdropping all mobile network traffic. The attack is not possible with devices not supporting GSM.

4.13. LoRaWAN

LoRaWAN is an open protocol designed to integrate billions of devices in the Internet of Things. It is maintained by the LoRa Alliance, an open, non-profit association of members. The last version of the LoRaWAN specification is 1.0.2 [80].

It supports low-cost, mobile, and secure bi-directional communication. It is normally deployed in a star of stars topology in which gateways are transparent bridge relaying messages between end-devices and a central network server in the backend. Gateways and backend server are connected via a standard IP connection. End-devices use single-hop wireless communications to one or many gateways. Gateways support multicast communications enabling services like software upgrade over the air.

Communications are spread out on different frequency channels and data rates ranging from 300bps to 50kbps. It is designed to communicate over large ranges from 5km to 15 Km.

It uses the LoRa modulation technique that is based on spread-spectrum and a variation of chirp spread spectrum.

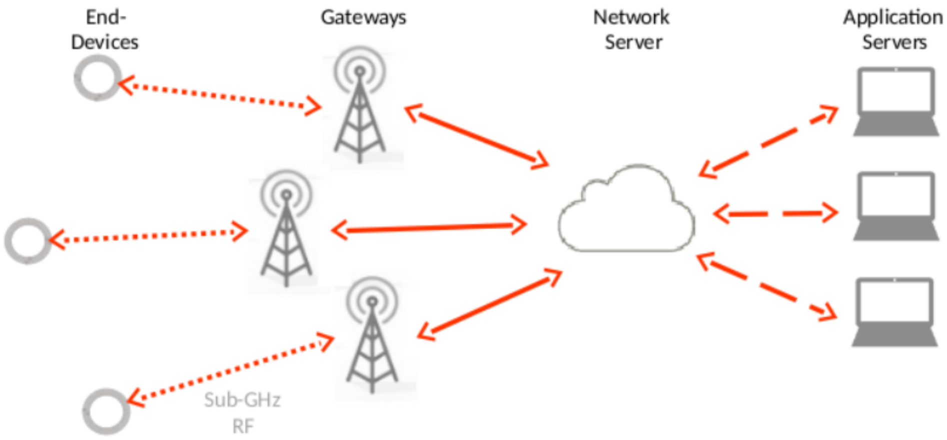


Figure 4.16: LoRaWAN topology

It supports three classes of end-devices:

- **Class A** (baseline): the most energy efficient to maximize battery lifetime. This kind of nodes initiates data transfers followed by two short listening windows to receive commands from the server. The transmission slot scheduled by the end-device is based on its own communication needs (ALOHA-type of protocol).
- **Class B** (beacon): similar to class A nodes but with an extra listening window allowing the server to send data to the node in a predefined time marked using a beacon. The server also receives the beacon knowing when the node is listening.

- **Class C** (continuous): always listening nodes. Suitable for the most data-intensive applications or for the ones that requires high responsiveness.

4.13.1. Security options

Security Goal	LoRaWAN
Confidentiality	AES-128 CCM (4-byte MIC)
Integrity	
Authentication	
Freshness	Frame counter
Availability	Several antennas may be at range
Authorization	Over-the-air activation using Application key or Personalization
Key type	Application key per device Session Network key per device Session Application key per device
Key management	Over-the-air activation: keys changed on every reset or Personalization: None
Required power	Low

Table 4.16: LoRaWAN security options summary

LoRaWAN standard includes two security layers: one for the network and one for the application. Network-layer security ensures device authentication for network messages and Application-layer security ensures the protection of the application data (confidentiality, integrity).

Network security is based on the 802.15.4 security. So, it uses AES-128 keys in CCM mode to both encrypt the message payload and to produce a MIC to verify the integrity and authentication.

Secure communications are based on the use of two different keys:

- **Network Session key**: It is an AES-128 key specific for an end-device. This is used by the end-device and the Network server to compute and verify the message integrity code (MIC). It is also used for encryption and decryption of the payload of the Network messages.
- **Application Session key**: It is an AES-128 key specific for an end-device. It is used by the end-device and the Application server to encrypt and decrypt the payload of application-specific data messages. It may also be used for computing and verifying an application-level MIC (which may be included in the payload of application-specific data messages).

Each device should have a unique set of Network and Application session keys. So, compromising the keys of one device shouldn't compromise the security of the communications of other devices.

When an end-device is added to the LoRaWAN network, it needs to be personalized and activated. Key exchange is performed by two available methods:

- **Over-the-Air Activation**: Based on a globally unique identifier and a handshake communication. End-device requests to be joined to the Application server by sending its globally unique device identifier, application identifier and a nonce. All authenticated with the Application key.

  The Application key is an AES-128 application key specific for the end-device that is assigned by the application owner to the end-device and most likely derived from an application-specific root key exclusively known to and under the control of the application provider.

  Application server answers with encrypted and authenticated Device address and a nonce from where the Network and Application session keys are derived.
- **Activation by personalization**: The Device address and the two session keys are directly stored at production time.

4.13.2. Issues

Several vulnerabilities in the LoRaWAN specification and attacks were devised in the document [81]:

- **No key management in Personalization mode**: The keys used for data protection are never changed. If one of these keys is compromised future and past communications can be eavesdropped.
- **Replay attack in Personalization mode**: The Frame counter is reset when an end-device joins the network. If the Personalization mode is used, after a device reset, the Frame counter will be also reset with the same keys as a previous session enabling replay attacks.
- **Replay attack in over-the-air mode**: The Frame counter is also reset when it reaches its maximum value, thus enabling replay attacks. An adversary can wait to the counter to overflow to be able to replay messages.
- **Eavesdropping**: Since the same counter value and the same key can be used for more than one message, the payload of a protected message can be eavesdropped using the Same-nonce attacks issue seen in 802.15.4 (see section 4.7.2).
- **Denial of Service**: In [82], it is identified that if multiple LoRaWAN networks are present in the area, since LoRaWAN channels are shared, additional interference will increase packet-error-rate. Since LoRa has a low co-channel dynamic range, without a closed-loop power control scheme, any nodes close to the gateway will drown out nodes far away. These issues can be exploited to perform a DoS attack.
- **Key ownership conflict**: In [83], it is identified that since the two session keys are derived from the Application key (owned by the Application provider), the Application provider can derive itself the Network Session key and thus clone devices.

4.14. 6LoWPAN

6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks [84].

6LoWPAN acts as an adaptation layer between the IPv6 networking layer and the IEEE 802.15.4 link layer.

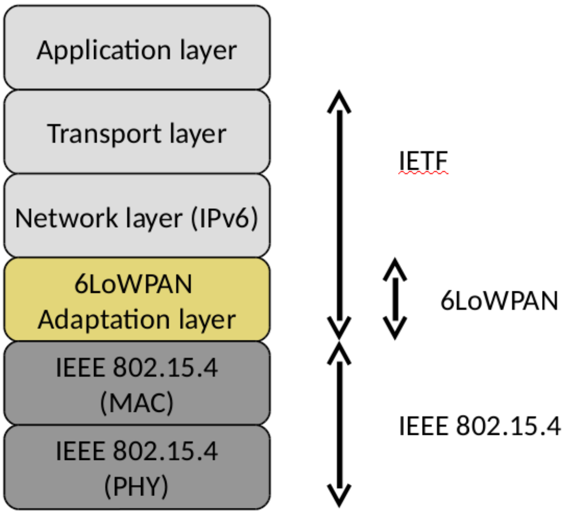


Figure 4.17: 6LoWPAN architecture

It provides the following features:

- **IPv6 packet encapsulation**: The 6LoWPAN layer takes the IPv6 packets, wraps them using encapsulation headers, and then subsequently sends them over-the-air using the IEEE 802.15.4 MAC and PHY layers.
- **IPv6 packet fragmentation and reassembly**: To meet the IPv6-required MTU of at least 1280 bytes with the IEEE 802.15.4 layer offering at most 102 bytes of payload per frame, a fragmentation mechanism below the IP layer is specified using an optional Fragmentation Header before the actual IPv6 header. A fragmented packet is carried in frames containing the fragmentation header.
- **IPv6 header compression**: To minimize the overhead of sending IPv6 messages in IEEE 802.15.4 frames, 6LoWPAN provides stateless compression mechanisms for both IPv6 and transport headers that take advantage of cross-layer redundancies between protocols such as source and destination addressing, payload length, traffic class and flow labels.

Another important feature of the 6LoWPAN layer is the ability to provide link layer packet forwarding. It provides a very efficient and low overhead mechanism for forwarding multi hop packets in a mesh network.

4.14.1. Security options

This adaptation layer does not directly offer any security mechanism. On the other hand, it is placed over the 802.15.4 that offer security mechanisms at the data link layer. Furthermore, since it enables IPv6 at the network layer, 6LoWPAN enable the use of security mechanisms like IPsec, DTLS or any other IP-based upper later security mechanism.

5. Analysis of the survey results

In this chapter, a comparison of the security options of all the surveyed networking technologies is presented, comparing them to one another.

	Confidentiality	Integrity	Authentication	Freshness	Availability	Authorization
Ethernet	◒	◒	◒	◒	◒	◒
PLC	●	◒	◒	●	◒	◒
RFID	○	○	○	○	○	○
NFC	◒	◒	◒	◒	◒	◒
Bluetooth	◒	●	●	●	◒	◒
Wi-Fi	◒	◒	◒	●	◒	◒
802.15.4	◒	◒	◒	●	◒	○
ZigBee	●	●	●	●	◒	◒
Thread	●	●	●	●	◒	●
Z-Wave	●	●	●	●	◒	◒
SigFox	◒	◒	◒	●	◒	●
EC-GSM-IoT LTE-M NB-IoT	●	◒	◒	●	◒	●
LoRaWAN	●	◒	◒	◒	○	●

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.1: Security options comparison

Most of the surveyed technologies, but RFID, offers a good level of security services, at least on the latest version of their specifications. On the other hand, some of them maintain backward-compatibility to older version(s) leaving the option of exploit for known flaws on new systems.

Most of them base their security services on symmetric cryptography, specifically on AES-128 which is considered a robust cryptographic algorithm.

Confidentiality, Integrity, Authentication and Freshness can be achieved with a good security level in most of the technologies, if the devices are properly configured and deployed.

Availability is difficult to achieve for technologies based on wireless communications, but techniques like frequency hopping and mesh network topology may help to mitigate the impact of a DoS attack.

The use of symmetric cryptography force them to perform secure key management. This is what some of the technologies failed to achieve in their earlier versions. Most of the technologies tend to use some kind of out-of-band method. Last versions started to use asymmetric cryptography in trust establishment procedure between new device and network.

5.1. Confidentiality

Most of the surveyed technologies offers confidentiality services for the data sent through the network. The following table summarizes and compares these services for each of the technologies.

	Confidentiality	Description
Ethernet	◒	Not offered by the 802.3. AES-128 GCM if 802.1AE is implemented.
PLC	●	AES-128 CBC. Key used for encryption is periodically changed and securely distributed using a different key for that purpose.
RFID	○	Not offered.
NFC	◒	NFC-SEC uses AES-128 in CTR mode.
Bluetooth	◒	AES-128 in CCM mode. On the other hand, there exists some configurable security levels that does not perform data encryption and some issues are known on the pairing procedure from where the key is derived. Bluetooth Mesh encrypts all the messages within the mesh network.
Wi-Fi	◒	WEP and WAP uses vulnerable stream cipher RC4 and several design flaws are known that make its use not recommended. WPA2 uses AES-128/256 in CCM or GCM modes.
802.15.4	◒	AES-128 in CCM mode. On the other hand, older versions of the specification have the option of only ciphering the data without authentication and since the Counter mode is used it suffers from the same nonce attacks. Furthermore, there is a No-security security level.
ZigBee	●	AES-128 in CCM mode.
Thread	●	AES-128 in CCM mode.
Z-Wave	●	Z-Wave Plus uses AES-128 in OFB mode. Z-Wave with S2 commands uses AES-128 in CCM mode.
SigFox	◒	Custom AES-128 based encryption. On the other hand, its usage is optional.
EC-GSM-IoT LTE-M NB-IoT	●	AES-128 CTR mode or SNOW 3G.
LoRaWAN	●	AES-128 in CCM mode.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.2: Confidentiality mechanisms comparison

As can be seen, most of the surveyed technologies uses the AES cryptographic primitive. AES is a robust primitive to use at the time of writing this report. It is used in CCM authenticated encryption mode with a key of 128 bits of size. The size of the AES key is considered enough for near term future system use according to Algorithms, Key Size and Parameters recommendations from the European Union Agency for Network and Information Security (ENISA) [85]. SNOW 3G isa stream cipher and it is considered robust.

The CCM mode implies the use of block cipher Counter (CTR) mode. The security of CTR mode is robust but it strongly depends on that the counter value is not repeated. The 802.15.4 specification correctly defines that when the counter associated to a key is exhausted, the key in no more usable. The technologies based on the 802.15.4 are correctly implementing this fact too.

802.1AE is using AES-128 in GCM mode. GCM mode is considered robust too and it is more computationally efficient since only an AES computation is needed.

WAP2 is specifying as one of the possible ciphers to use the AES-256, thus enhancing the security by using a bigger key size.

SigFox is using a custom algorithm based on AES-128. Since it is proprietary solution, no information on the actual algorithm was found. Due to the size of the SigFox messages' payload (12 bytes at most), the standard usage of AES does not apply (AES block size is 16 bytes). So, some kind of cipher-text truncation may be applied.

5.1.1. Found issues

Some of the surveyed technologies have the option to disable the confidentiality services (802.15.4, Bluetooth, SigFox) and may have it disabled by default. If the final application is managing sensitive data, it may be clearly recommended to enable confidentiality services on system deployment.

For the case of Bluetooth, low entropy keys are derived from the non-secure pairing modes enabling brute force attack to be practical. The last BLE version (4.2) fixed that problem by the use of Diffie-Hellman key exchange in order to get high entropy keys after pairing.

The WiFi security protocols WEP and WPA uses the RC4 for data confidentiality. It has several known problems that makes this cryptographic primitive to be not recommended anymore. The key sizes used in this protocols (40 to 104 bits) are also considered not enough.

ZigBee bootstrapping suffers from several problems that affect the confidentiality of the system like the Network key sent in to a joining device in clear text if Residential mode is configured or the usage of a default known key for protecting the Network key distribution. So, it is recommended to not configure the Residential mode and to change the default key to a new value before the system is operational.

LoRaWAN is partially using the 802.15.4 security scheme. It wrongly resets the frame counter when a device joins the network or when the frame counter is exhausted. It impacts the security of the CTR mode. On the other hand, the former method can be fixed by using over-the-air joining mode and the last one is partially impractical because of the low number of messages intended in this kind of networks. Nevertheless, it is recommended to fix this fact.

5.2. Integrity

Most of the surveyed technologies are providing mechanisms to verify the integrity of the data sent through the network. The following table summarizes them.

	Integrity	Description
Ethernet	◒	CRC-32 over the frame header and payload. Note that while the CRC provides some integrity protection, it is not considered to provide cryptographic integrity as it can be easily forged. 802.1AE uses AES-128 in GCM mode including 8 bytes MIC.
PLC	◒	CRC-32 over the frame header and payload included in the encrypted payload.
RFID	○	CRC-16 over the frame header and payload. Note that while the CRC provides some integrity protection, it is not considered to provide cryptographic integrity as it can be easily forged.
NFC	◒	CRC-16 over the frame header and payload. Note that while the CRC provides some integrity protection, it is not considered to provide cryptographic integrity as it can be easily forged. NFC-SEC uses AES-128 based 12 bytes MIC computation.
Bluetooth	●	AES-128 in CCM mode including 4 bytes MIC. 8 bytes MIC can be used in the Bluetooth Mesh.
Wi-Fi	◒	WEP uses CRC-32. WAP uses a custom keyed hashing function (20 bits security) TKIP. WPA2 uses AES-128/256 in CCM or GCM modes.
802.15.4	◒	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC. On the other hand, older versions of the specification have the option of only ciphering the data without integrity checking. Furthermore, there is a No-security security level.
ZigBee	●	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC.
Thread	●	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC.
Z-Wave	●	Z-Wave Plus uses AES-128 CMAC with 8 bytes MIC. Z-Wave with S2 commands uses AES-128 in CCM mode including 8 bytes MIC.
SigFox	◒	Authentication token based on AES-128 with 2 - 5 bytes MIC.
EC-GSM-IoT LTE-M NB-IoT	◒	AES-128 CMAC with 4 bytes MIC or SNOW 3G.
LoRaWAN	◒	AES-128 in CCM mode including 4 bytes MIC.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.3: Integrity mechanisms comparison

Most of the surveyed technologies opted for combining the integrity checking and the authentication mechanisms in a single Message Integrity Code. Most of them use the included MIC in the AES-218 CCM and others use the AES CMAC one. The security of the

CMAC Message Authentication Code is robust if the cryptographic primitive is strong enough (AES in this case) and if the final MIC value is not truncated in excess.

ECMA-386 NFC-SEC-01 uses AES-XCBC-MAC-96 for the integrity and authentication checking. So, 12 bytes MIC is used. This is one of the options supported by IPsec.

802.1AE uses AES-128 in GCM mode including an 8 bytes MIC.

SigFox is using a custom algorithm based on AES-128. The size of the used MIC is 2 to 5 bytes. Since it is proprietary solution, no information on the actual algorithm was found.

5.2.1. Found issues

Some of the surveyed technologies use a CRC checksum to provide some integrity protection, but CRC is not considered to provide cryptographic integrity as it can be easily forged after data manipulation. An adversary with the capability to intercept a message and change its content can manipulate the data, compute the new CRC value and update the CRC value in the message.

The PLC is also using a CRC for data integrity protection. But, since it is including the CRC in the encrypted payload, an adversary does not have a practical way of modifying the protected message in a way that after decryption the CRC will be valid. The adversary can modify the message but at the receiving side the modification can be detected and the message can be dropped.

WiFi security protocols WEP and WAP does not provide robust integrity checking mechanism. The former one is based on CRC and the last is based on TKIP that have several known problems and its security is put on the same level of a 20-bits key.

802.15.4 have the option to not protect neither the confidentiality nor the integrity / authenticity of the messages selecting the “No security” security level. It is recommended not to use this security level for security relevant applications.

Some of the surveyed technologies are truncating the output of a CMAC. A MAC function with security 2^s should have an output size of at least *s* bits. If we truncate the MAC output by *e* percent, then the security drops to $2^{e \cdot s}$, as stated in section 4.2 of the document [85]. The size of the AES CMAC is 16 bytes and some technologies are truncating it to its half (8 bytes) or even a quarter of it (4 bytes). The NIST SP 800-38B [86] recommends that at least 8 bytes MAC should be used as protection against guessing attacks. Some of the technologies allows to configure the size of the MIC, it is recommended to use the full size or at least a size of 8 bytes.

SigFox is truncating an authentication token based on AES to 2-5 bytes in size. This fact is dramatically reducing its security. But since no more information was found about the actual mechanism and the actual size of the protected payload is small, no more conclusion can be devised.

5.3. Authentication

Most of the surveyed technologies are providing mechanisms to verify the authenticity of the data sent through the network. The following table summarizes them.

	Authentication	Description
Ethernet	◒	802.1AE uses AES-128 in GCM mode including 8 bytes MIC.
PLC	◒	CRC-32 over the frame header and payload included in the encrypted payload.
RFID	○	Not offered.
NFC	◒	NFC-SEC uses AES-128 based 12 bytes MIC computation.
Bluetooth	●	AES-128 in CCM mode including 4 bytes MIC. 8 bytes MIC can be used in the Bluetooth Mesh.
Wi-Fi	◒	WEP uses encrypted CRC-32. WAP uses a custom keyed hashing function TKIP. WPA2 uses AES-128/256 in CCM or GCM modes.
802.15.4	◒	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC. On the other hand, older versions of the specification have the option of only ciphering the data without integrity checking. Furthermore, there is a No-security security level.
ZigBee	●	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC.
Thread	●	AES-128 in CCM mode including 4 / 8 / 16 bytes MIC.
Z-Wave	●	Z-Wave Plus uses AES-128 CMAC with 8 bytes MIC. Z-Wave with S2 commands uses AES-128 in CCM mode including 8 bytes MIC.
SigFox	◒	Authentication token based on AES-128 with 2 - 5 bytes MIC.
EC-GSM-IoT LTE-M NB-IoT	◒	AES-128 CMAC with 4 bytes MIC or SNOW 3G.
LoRaWAN	◒	AES-128 in CCM mode including 4 bytes MIC.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.4: Authentication mechanisms comparison

Since most of the surveyed technologies opted for combining the integrity checking and the authentication mechanisms in a single MIC, the Table 5.4 becomes exactly the same to the shown in the Integrity mechanisms.

5.3.1. Found issues

MAC truncation should be considered. It is recommended to use at least 8 bytes MAC.

5.4. Freshness

Most of the surveyed technologies are providing mechanisms to verify the freshness of the data sent through the network to avoid replay attacks. The following table summarizes them.

	Freshness	Description
Ethernet	◒	802.1AE includes a Packet Number included in the MIC computation.
PLC	●	Nonces are used to prevent replay attacks.
RFID	○	Not offered.
NFC	◒	Not offered. NFC-SEC includes a Sequence Number in the MIC computation.
Bluetooth	●	BLE have a counter that is incremented on every signed message. Bluetooth Mesh is adding a 24-bits sequence number to the messages.
Wi-Fi	●	WEP is adding a 24-bits IV. WAP is adding a 48-bits IV. WAP2 is adding a 48-bits packet number.
802.15.4	●	Frame counter per key included in the MIC computation. Always included in the frame header.
ZigBee	●	Frame counter per key included in the MIC computation. Always included in the frame header.
Thread	●	Frame counter per key included in the MIC computation. Always included in the frame header.
Z-Wave	●	Z-Wave plus is using a 64 bits nonces generated using PRNG when computing the MIC. Z-Wave S2 commands implements a mechanism to agree a nonce between the parties to be used as the initial value of the counter of the CCM mode.
SigFox	●	Sequence counter inside the authenticated payload.
EC-GSM-IoT LTE-M NB-IoT	●	Sequence counter.
LoRaWAN	◒	Frame counter.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.5: Freshness mechanisms comparison

Most of the surveyed technologies includes a frame or sequence counter in the message header and in the MIC computation that enables to identify replayed messages.

5.4.1. Found issues

As explained above LoRaWAN wrongly resets the frame counter when a device joins the network or when the frame counter is exhausted enabling replay attacks.

5.5. Availability

Since most of the surveyed technologies are based on wireless communications, availability is difficult to enforce because radio jamming can be achieved with off-the-shelf equipment.

	Availability	Description
Ethernet	◒	Wired media. On the other hand, some DoS attacks are possible misusing its control mechanisms like MAC dynamic table and ARP.
PLC	◒	Wired media. On the other hand, since its range is not controlled, it may be accessible from outside of the building where jamming signal can be inserted from a safe distance.
RFID	○	No protection. Radio jamming and the use of a “blocker tag” is possible.
NFC	◒	No protection but its 10 cm range can help in avoiding jamming impact.
Bluetooth	◒	Frequency hopping and Mesh topology.
Wi-Fi	◒	Wireless devices often support dynamic selection of channels. But crowded unlicensed frequency band.
802.15.4	◒	Last version supports frequency hopping techniques. On the other hand, several identified DoS techniques based on media access control frame counter exhaustion.
ZigBee	◒	Mesh topology.
Thread	◒	Self-healing Mesh topology.
Z-Wave	◒	Mesh topology.
SigFox	◒	The same message is sent several times at random moments using different frequencies.
EC-GSM-IoT LTE-M NB-IoT	◒	Frequency hopping techniques. Multiple antennas can service the same geographically position.
LoRaWAN	○	No protection offered.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.6: Availability mechanisms comparison

Wireless jamming based Denial of Service is difficult to defend but several techniques can be used to diminish its impact or to reduce the practicality of the attack by the need more complex adversary’s method.

Wired technologies (Ethernet, PLC) present some protection inherent from its physical nature, normally deployed over copper twisted pair or fiber optic wires. Physical access needed, easy to detect and normally deployed with redundant paths.

NFC very short range (10 cm) can help on diminishing the effects of a jamming interference, since a little increase of the reader’s power makes the jamming signal to increase its power considerably to be able to maintain the same level of interference. Furthermore, since both devices are one in front of the other, the devices can be used as a shield to the external interferences.

BLE employs a frequency hopping transceiver to combat interference and fading.

Mesh topologies (Bluetooth Mesh, ZigBee, Thread, Z-Wave) can be deployed in a way that if some of the nodes of the mesh network is affected by a denial of service, the rest of the network can be dynamically configured to route the messages through a different path.

SigFox protocol sends each message at three random times and on three different frequencies. As a result, some resistance against Denial of Service attacks is achieved.

Most of the surveyed have some kind of frequency hopping technique that helps on mitigating the impact of such attack.

5.5.1. Found issues

Ethernet control mechanisms can be misused in order to render a network switch inoperable. Dynamic MAC learning tables can be modified by sending lots of frames with a target MAC address to make the switch do not send its frames to the correct port. The same effect can be achieved with mechanisms like ARP.

PLC may cross the perimeter of a house if, for instance, a plug is available on the outside or it is a building with a shared power feed. The signal can travel quite far down wires, and despite fuse boxes offering some resistance to signals, it is usually found that the signal is retrievable from the far off of the intended range.

RFID systems can be attacked by the so called “blocker tag” that simulates many tags simultaneously flooding the legitimate RFID reads. In a second generation, a 32-bit password protected Kill command was introduced in order to deactivate the tags that can be used to Denial of Service attacks.

CSMA-CA misuse, PANId conflict or spoofed acknowledge attacks can be used in 802.15.4 to implement DoS attacks.

In the 3GPP cellular technologies, the first non-authenticated messages can be used to temporarily block the access to a target device by the use of spoofed network access reject messages.

5.6. Authorization

Most of the surveyed technologies base its access control on the possession of credentials that are provided during the device commissioning. Device joining procedure have to be protected to avoid unauthorized devices to access the network.

	Authorization	**Description**
Ethernet	◒	802.1X uses EAP-TLS with TLS 1.2 in order to authenticate new devices connected to an Ethernet switch.
PLC	◒	By physical connection, custom key agreement or user provided credentials
RFID	○	No protection. By physical proximity and field generation.
NFC	◒	NFC-SEC agrees a new key on each connection using ECDH with a 192-bits key.
Bluetooth	◒	Based on pairing modes. Some of them uses low-entropy secrets. Just Works mode does not offer authentication at all. BLE versions prior to 4.2 used a AES-128 based custom key exchange with these low-entropy secrets. BLE version 4.2 and Mesh is using ECDH in order to provide high entropy key agreement to the pairing modes.
Wi-Fi	◒	Based on a pre-shared key. Several pairing modes (some of them non-secure). WPA and WPA2 uses EAP supporting standard authentication mechanisms.
802.15.4	○	Not specified.
ZigBee	◒	Based on pre-shared key or install codes. ZigBee IP introduces the use of PANA/EAP-TLS with pre-shared key or certification based ECDH with ECDSA authentication.
Thread	●	Based on a DTLS handshake with Commissioning credentials to manage the device joining. Another DTLS handshake with Joining credentials to obtain the Network key. Requires user interaction.
Z-Wave	◒	Z-Wave Plus is based on a custom protocol with pre-shared key. Z-Wave S2 is based on ECDH-256 with required user interaction.
SigFox	●	Different key per device personalized during manufacturing. No commissioning is performed.
EC-GSM-IoT LTE-M NB-IoT	●	Based on pre-shared keys. EPS AKA procedure to allow a device to connect to the network.
LoRaWAN	●	Over-the-air activation mode uses a per device pre-shared key to authenticate the joining device. Personalization mode uses keys stored during manufacturing an no commissioning is performed.

● Fulfilled, ○ Not fulfilled, ◒ Partially

Table 5.7: Device commissioning mechanisms comparison

All of the surveyed technologies are based on the possession of a pre-shared key or credentials. Most of them use a master secret installed in the device during manufacturing or by an out-of-band method prior device deployment. These credentials will be used as the secret for a key agreement protocol between the joining device and the network in order to derive final keys to be used to implement the other security services. Other systems install the final keys directly to the device (SigFox, LoRaWAN, 3GPP).

802.1X implements access to the Ethernet network by the use of standard EAP-TLS. 802.1X offers periodic re-authentication with key exchange.

PLC HomePlug AV is changing the key used to protect the data periodically and securely distributing it with a different key intended only for that use.

NFC-SEC is using ECDH with a 192-bits key to exchange a new key on every connection. It has to be noted that Diffie-Hellman key exchange is not protected against Man in the Middle attacks. On the other hand, NFC very short range (10 cm) can help on diminishing the effects since the transmission party can be monitoring the field while transmitting in order to detect the attack.

WiFi WPA2 uses EAP supporting standard authentication mechanisms. Furthermore, they are changing the key periodically and distributing the new key using specific key-wrapping key.

Bluetooth Low Energy v4.2 and Mesh introduced a ECDH key exchange in the pairing process in order to provide high entropy key material for the channel protection.

ZigBee IP is using PSK or ECDH EAP-TLS for device joining. It maintains the PANA session in order to securely perform Network key distribution.

Thread is using an elliptic curve variant of J-PAKE (EC-JPAKE) for key agreement while providing Non-interactive Zero-Knowledge proof two authenticate both peers based on a passphrase. It offers key rotation based on synchronized key generation on every device.

Z-Wave S2 is using ECDH with a 256-bits key. To provide peer authentication, part of the joining device’s public key used in the key agreement is not sent over-the-air but provided by some other out-of-band method.

3GPP IoT technologies are using EPS AKA procedure to perform mutual authentication and exchange a key from where keys for protecting the communication channel are derived.

LoRaWAN over-the-air commissioning is based on a per device pre-shared key used to perform key agreement and derive the keys for channel protection.

5.6.1. Found Issues

Some of the surveyed technologies base its access control on the knowledge of a pre-shared credentials. Some manufacturers tend to set this credentials to a default value publicly available in the devices’ documentation.

Several ways to join a device in a PLC HomePlug AV network imply the use of a low entropy password, sometimes a default password equal for all the devices of a same manufacturer.

In version of BLE prior to v4.2, it is offered non-secure pairing modes like Just Works that does not offer authentication, or Passkey mode that uses a low-entropy secret in order to exchange a key. Just Works and Passkey modes are susceptible to be attacked by eavesdropping and secret brute force attacks.

Some WiFi offer WPS which has design flaws that allows brute force attack to recover the secret (e.g. WPS PIN.). Some implementation flaws were also found on commercial devices. Some manufacturers configure default password based on public data like the SSID or the MAC address of the WiFi access point. WEP and WAP does not change the key once is established.

ZigBee specify a Residential mode in which the network key is transmitted unsecured over-the-air and thus this is a serious vulnerability for the security of the ZigBee enabled networks. In non-Residential mode, device commissioning is based on a pre-shared key between the Trust Center and the joining device. A default Trust Center link key is provided in the specification that all the compliant devices may use introducing a risk to the network key secrecy. ZigBee is distributing a new network key protected with the old key using multicast.

Z-Wave Plus suffered from implementation errors on commercial devices that enabled the attacker to reset the established key to a known value. It is also discovered that a default pre-shared key was used in these devices.

5.7. Common issues

The following common issues can be defined to affect most of the surveyed technologies:

- **Unique network-wide shared key:** Most the technologies are based on symmetric key and uses a unique symmetric key shared among all the network participants. The main issue with this fact is that the impact of compromising the key in one device will affect the security of the whole network. An attacker that compromises this key will be able to eavesdrop all the future data going through the network and to inject new data to the network.

  The fact that this shared key may be stored in a low-cost, low-resources and physically accessible unattended device makes the chances of key compromising to be high.

  Some of the systems adequately change this key periodically but if the method to protect the new key distribution is based on using the compromised one, the attacker will be able to obtain the value of the new key.

  In the particular case of the Thread, key management uses a key rotation algorithm based on the use of the shared key and a monotonic counter. So, if the attacker is in possession of the key, she will be able to compute all the future and past keys by applying the algorithm on future and past values of the counter. In the Thread documentation, it is noted that this shared key is not typically used as the only form of protection within the Thread network.

- **Custom cryptographic mechanisms**: Some of the technologies in its earlier versions designed its own cryptographic mechanisms.

  For instance, WiFi’s WEP and WAP security mechanism, BLE in its versions prior to the version 4.2 and the Z-Wave Plus. They all end having design vulnerabilities.

  A cryptographic scheme isn't secure until it has been extensively attacked. So, it is recommended to use already existing well-studied ones. Defining a new one along the application that will be deployed in the wild is not recommended. Note that design flaws are more difficult to solve than implementation or configuration issues.

- **Cryptographic support**: Most of the surveyed technologies make use of the AES cryptographic algorithm. It is a good choice for its security characteristics, but for some of the technologies its 16-bytes block size may be excessive. Some of them are truncating Message Integrity Codes based on AES to a size that dramatically reduces its security.

- **Usability first**: Most of the surveyed technologies were not designed with security from the beginning. First versions of the specifications to cover only functional aspects like usability, performance and data rate.

  For instance, ZigBee Residential mode designed the first network key distribution to a joining node to be sent in the clear prioritizing usability over security, assuming the exploitation window is short. BLE prior to v4.2 offers the non-secure pairing mode Just Works that does not offer authentication since it was designed for devices that do not have the capability to show or input any credentials.

  On the other hand, it is also understood that a security that cannot be used is not a good security.

- **Default credentials**: Another consequence of the previous issue is the use of default credentials. On pre-shared key scenarios where a new device has to share a secret with an already in the network device, it is easier if the pre-shared key is the same on all the manufactured devices. But this kind of decision may break the security of the whole system. It is even worse if the default credentials are defined in the specification since all manufacturers may choose to use the same.

- **Denial of Service**: Some of the surveyed technologies do not provide any mechanism against DoS. Other offer frequency hopping, mesh topologies and self-healing mechanisms, which may help in preventing such attacks.

- **Security as an option**: Some of the specifications does not mandate security or give the option to not provide one of the security services (e.g. confidentiality). Some of them have security disabled by default. Although security may be enabled in such a system, since security has an inevitable penalty on system's performance or networking capabilities, some of the manufacturers or end users may tend to disable security to get the better performance.

- **Deployed old specification versions**: The time between a new version of a specification and its deployment on actual devices is always considerable. This fact was evident during the survey.

  For instance, most of the technologies based on the 802.15.4 standard were still using the 802.15.4-2006 version even though several security fixes were published in the 2011 and 2015 versions.

  Known flaws or vulnerabilities from the old specification may be inherited by the new system. Some of the specifications solve this issue by putting its own security on top, or by limiting the use of the base technology to the parts that are known to be secure. On the other hand, others maintain backward-compatibility to older version(s) for practical reasons leaving the option of exploiting known flaws on new systems.

For instance, you can still configure WEP security in a WiFi access point although it has been a long time after it was known to be vulnerable and the existence of multiple exploiting tools.

Some of the industry alliances manage this situation by timely marking as deprecated the old specifications and the new version as mandatory for the certification of new devices.

For instance, the Z-Wave Alliance mandated that all devices submitted for certification after November 2016 should include the new security S2 protocol.

- **Software update capability**: Some of the surveyed technologies does not have enough downlink data rate (e.g. SigFox, LoRaWAN) to enable a practical software update mechanism. Others lack the provision of credentials to protect the mechanism.

5.8. Security Solutions

After the results of this study, the first solution will be to apply the general recommendation to use the latest versions of a network technology and to carefully configure its security services to offer the desired security level. Depending on the final application one technology or another may be more suited to be used.

- **Hardware security**: To defend a device against physical attacks that may compromise a secret, several hardware solutions have been devised. Hardware Security Module (HSM) or Trusted Platform Module (TPM) are normally implemented in a micro-controller by adding a processing unit and memories that are only dedicated to security related functionality. These modules are protected against physical attacks. They can be used to store secret data and avoid its compromise.

  Another hardware alternative is Physical Unclonable Function (PUF), it is a physical entity that is embodied in a physical structure that is easy to evaluate but hard to predict. Furthermore, an individual PUF device must be easy to make but practically impossible to duplicate. PUFs evaluate manufacturing variations to generate unique secrets inside a micro-controller, avoiding storing the key in a non-secure general purpose memory or in more expensive alternatives like HSM or TPM modules.

  Hardware Random Number Generators play also an important role on the security of the systems since most of the cryptographic system depends on the quality of random numbers.

- **Firmware update Over The Air (FOTA)**: The ability to securely update firmware of deployed embedded devices over networks is one of essential features nowadays. Vendors use the remote firmware update to provide new functionalities and also to patch vulnerabilities on the embedded devices. For securing the remote firmware update, asymmetric cryptographic algorithms such as ECC or RSA are normally used. For instance, to provide integrity and authentication of the firmware.

  Firmware updates may open the doors to attacks exploiting the update mechanism itself. So, this kind of mechanism must be very well-studied before being deployed.

The document [87] describes the development of a design for such an update process focusing on flexibility and feasibility - without neglecting security.

In [88], a lightweight protocol is presented to update each device in a secure way. The cryptographic keys employed are fresh and are not stored but reconstructed by exploiting the Physical Unclonable Functions (PUFs) of the device hardware.

In [89], a new firmware update scheme that utilizes a Blockchain technology is proposed to securely check a firmware version, validate the correctness of firmware, and download the latest firmware for an IoT device.

- **IP-based security mechanism adaptation**: A general trend that can be observed is the adaptation of the security mechanisms used in the traditional Internet. They are being adapted to the specific characteristics of the devices and networks involved in the IoT.

  In [90], an adaptation of the IPsec Authenticated Header (AH) and Encapsulating Security Payload (ESP) protocols is defined. In [91], a collaboration of DTLS and CoAP is proposed for IoT. It also proposed DTLS header compression scheme that helps to reduce packet size, energy consumption and avoids fragmentation by complying the 6LoWPAN standards. In [92], a 6LoWPAN compression for Internet Key Exchange (IKE) version 2 is proposed. In the RFC 7925 [93], a profile for TLS and DTLS version 1.2 is defined that offers communications security for resource-constrained nodes.

- **Lightweight cryptography**: In resource-constrained environments, conventional cryptography primitives may be infeasible. Numerous research activities were accomplished and led to plenty of block ciphers primitives for IoT. Recently the NIST started a lightweight cryptography project to investigate the issues and then develop a strategy for the standardization of lightweight cryptographic algorithms [94].

  For the symmetric key cryptography, some of the ciphers were designed by simplifying conventional, well-analyzed block ciphers to improve their efficiency. Alternatively, some of the algorithms are dedicated block ciphers that were designed from scratch. PRESENT [95] is one of the first lightweight block cipher designs that was proposed for constrained hardware environments. SIMON and SPECK [96] are families of lightweight block ciphers that were designed to be simple, flexible, and perform well in hardware and software. There are also algorithms from the 1990s such as RC5 [97], TEA [98] and XTEA [99], which consist of simple round structures that make them suitable for constrained software environments. They present smaller block sizes, smaller key sizes and simpler rounds and key schedules. M. Cazorla et al. [100] presented a comprehensive survey of lightweight algorithms and the results of comparing them to each other in terms of operation and performance.

  For the public key cryptography, alternative public-key cryptographic schemes with shorter keys may be used like ECC, Hyper-Elliptic Curve Cryptography (HECC) [101], NTRU [102] and BlueJay [103].

- **Confidentiality with no cryptographic computations**: For the technologies that does not provide security like RFID or the NFC without the NFC-SEC, several workarounds have been presented to offer security services without the use of cryptography. To protect confidentiality, solutions controlling eavesdroppers' signal-to-noise ratio with artificial noise have emerged [104]. It proposes the reader to emit a controlled noise while receiving the node’s answer, since the reader knows the noise value, it can subtract it and recover the node data.

Haselsteiner et al. [43] proposed a key extraction solution, which is based on eavesdropper inability to determine direction of NFC transmissions. The idea is that both devices, say Device A and Device B, send random data at the same time. While sending random bits of 0 or 1, each device also listens to the RF field. When both devices send a zero, the sum signal is zero and an attacker, who is listening, would know that both devices sent a zero. This does not help. The same thing happens when both, A and B, send a one. The sum is the double RF signal and an attacker knows that both devices sent a one. It gets interesting once A sends a zero and B sends a one or vice versa. In this case both devices know what the other device has sent, because the devices know what they themselves have sent. However, an attacker only sees the sum RF signal and he cannot figure out which device sent the zero and which device sent the one.

Active attacks have been addressed in [105] with distance bounding protocol. Distance bounding is based on detecting round-trip delays caused by active man-in-the-middle attackers.

- **Robust key management**: RFC 4107 [106] discusses the trade-off between manual and automatic key management and recommends the use of automatic key management if the number of devices is considerable and any stream cipher such as AES-CTR or AES-CCM is used.

  Eschenauer and Gligor [107] propose a key pre-distribution scheme that relies on probabilistic key sharing among nodes within the sensor network. They try to avoid the sharing of a single key that if compromised will compromise the whole network. Their system works by distributing a key ring to each participating node in the sensor network before deployment. Each key ring should consist of a number randomly chosen keys from a much larger pool of keys generated offline. The authors show that, while not perfect, it is probabilistically likely that large sensor networks will enjoy shared-key connectivity.

  Adrian Perrig et al. [108] propose a key-chain distribution system for their μTESLA secure broadcast protocol. The basic idea of the μTESLA system is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys. In this case a sender will broadcast a message generated with a secret key. After a certain period of time, the sender will disclose the secret key. The receiver is responsible for buffering the packet until the secret key has been disclosed. After disclosure, the receiver can authenticate the packet, provided that the packet was received before the key was disclosed. One limitation of μTESLA is that some initial information must be unicast to each sensor node before authentication of broadcast messages can begin.

- **Intrusion Detection system (IDS)**: An Intrusion Detection system (IDS) is a device or application that monitors a network for malicious activity. Two types of IDS can be identified: Signature-based (recognizing malicious patters) and Anomaly-based (recognizing deviations from a model of “normal traffic”). An IDS system can be used to detect an attack in the network and react to it.

In [109], a survey on IDS system in the WSN can be found. It categorizes the types of IDS depending on the intrusion type, detection methodology, source of data and its place in the network. There may be value if it were possible to single out a device, which shows faulty behavior or has been compromised, and to shut that down in some sense.

- **Threat analysis**: The design for a device should study the potential security threats considered in its design, and the specific security controls applied (if any) to remedy or limit the impact of each threat. This analysis encourages making deliberate, explicit choices about security controls at design time rather than leaving security as an afterthought. The results of this analysis are also useful later in the life cycle of a device if it becomes necessary to enhance security. For instance, it can help to identify whether the original design choices fulfilled their intended function or failed to do so, or whether a newly discovered threat was not anticipated in the original design.
- **Standardization activities in IoT security**: Regulators and interoperability bodies should develop security standards. In [110], the major actors of standardization efforts for IoT security and their relevant activities are presented. ITU-T published recommendations that are directly related to IoT and its security in [8] and [111]. 3GPP is defining LTE security, it issued two technical specifications series, namely 33series (Security aspects) [112] and 35series (Security algorithms) [113]. BroadBand Forum (BBF) released a set of technical reports and defines its own TR-069 [114] protocol suite and data models for home network management. OneM2M has publications related to authorization, access control, confidentiality, authentication, identification, trust and integrity verification, for instance in oneM2M-TS-0003 [115] (Security Solutions) and oneM2M-TR-0008 [116] (Security Analysis). Finally, the ETSI M2M technical committee debates security aspects related to authentication, integrity, confidentiality, trust management and access control.

6. Conclusions

This chapter contains the conclusions drawn from the results of this study together with future work that suggests the security analysis of an actual implementation of the surveyed technologies.

6.1. Conclusions

In the last years, a huge amount of IoT systems are being deployed. However, the technologies for the IoT are still evolving and maturing. The idea behind the IoT to interconnect everything is so broad that a big number of different applications and technologies are involved. Since the development of standards is relatively slow to the fast rate of IoT growth, several industrial alliances and consortiums have been created to fill in the gap. They develop specifications and promote collaboration by partners but may compete against others. The IoT ecosystem ended up being formed by a plethora of different specifications and standards.

Regarding to the security of these technologies, as seen through this study, many threats and security challenges have to be solved to a successful IoT deployment. Some of the challenges presented are common in information security, but they pose new challenges since most of the participants in an IoT system may be resources constrained devices without enough processing power, memory or battery to implement the security mechanisms that are usually handled by libraries like OpenSSL and TLS in the desktop computers. Deciding on an encryption, authentication and signature algorithm requires a thought process to both efficiently and effectively secure a device.

Security should be a consideration through the whole system life cycle. Key decisions on security should have been decided long before deployment. These include how keys should be distributed to each device, if hardware-acceleration should be used, how updates can be handled, if asymmetric cryptography is a viable solution for the device, what type of cryptographic algorithms should be used, etc.

This study presented a comparative evaluation of IoT networking technologies with regard to communication security requirements. IoT systems include technologies designed especially for low-power devices, such as IEEE 802.15.4, LoRaWAN, Z-Wave while other technologies used in the traditional Internet or the mobile systems are being adapted to the specific characteristics of the IoT. Some of them cover the physical and media access layers (IEEE 802.15.4, Wi-Fi, NFC and LoRaWAN) while others cover the entire networking stack (BLE, Z-Wave, Thread). A selection of representative set of IoT networking technologies was made with the objective to try to cover the whole spectrum of the already deployed IoT networking solutions.

A total of thirteen IoT technologies were analyzed, describing their functionality, security options and found issues. Many different systems architectures, involved layers and security solutions have been adopted by the different technologies and there is a lot of research in many different areas involving IoT. Many different kinds of adaptations to protocols and authentication methods for IoT have been proposed which makes it very difficult to identify the best solution. Therefore, there is the need of standardization in order to interconnect all kinds of devices, protocols and security solutions.

The general conclusion is that the current level of security in the IoT networking solutions is quite good if the latest specifications are used, they are correctly implemented and their secure configuration is used. Most of the found issues were related to early versions of the technology where naive trust assumptions were taken.

The personal outcomes of this work are the understanding of the IoT's magnitude, the acquired knowledge of a new set of wireless technologies and the insight on how the security mechanisms are used in actual systems.

Several open research questions should be addressed in the future for a successful IoT deployment like efficient FOTA mechanisms that can be securely used on IoT devices, the adaptation to the IoT of traditional Internet's security mechanisms, the definition and security proof of lightweight cryptographic algorithms and the standardization of the IoT security.

6.2. Limitations

What limited our efforts the most was the amount of available time for this study. IoT is such an extensive concept that working with it is both difficult and time consuming.

The amount of surveyed technologies and the lack of previous knowledge about most of them required additional work in order to understand its concept and how the security services were devised.

Another limitation comes from the fact that some of the surveyed technologies are proprietary (e.g. SigFox) or just publicly released its specifications (e.g. Z-Wave). This makes the research of information more difficult or even not possible.

6.3. Future work

Another interesting area of research would be to investigate how the security properties of the various technologies' specifications transfer to practical implementations, given the limitations of IoT devices and the possible variations inherent in a complete stack. In the last years, several ready-to-use tools have been released making the security analysis of this kind of technology affordable. For instance, the Ubertooth [117] device for Bluetooth and the KillerBee [118] for the ZigBee.

Bibliography and references

[1] http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

[2] http://www.gartner.com/newsroom/id/2819918

[3] http://www.gartner.com/newsroom/id/3412017

[4] IETF, RFC7452 - Architectural Considerations in Smart Object Networking, 2015

[5] Ovidiu Vermesan, Peter Friess. "Internet of Things – From Research and Innovation to Market Deployment", 2014.

[6] Internet Society, The Internet Of Things: An Overview, Oct 2015

[7] IEEE Internet Initiative, Towards a definition of the Internet of Things (IoT), May 2015

[8] ITU-T. "Y.2060 - Overview of the Internet of things", 2012.

[9] https://standards.ieee.org/develop/project/2413.html

[10] ITU. "Internet of Things Global Standards Initiative", .

[11] https://www.rfc-editor.org/rfc/rfc4944.txt

[12] https://tools.ietf.org/html/rfc7252

[13] https://tools.ietf.org/html/rfc6550

[14] https://tools.ietf.org/html/rfc6690

[15] http://www.meet-iot.eu/iot-a-deliverables.html

[16] http://www.etsi.org/technologies-clusters/technologies/internet-of-things

[17] http://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport

[18] http://www.onem2m.org/

[19] http://www.zigbee.org/

[20] https://threadgroup.org/

[21] https://z-wavealliance.org/

[22] https://www.sigfox.com/

[23] https://www.lora-alliance.org/

[24] https://nfc-forum.org/

[25] http://www.fox19.com/story/25310628/hacked-baby-monitor

[26] https://www.nytimes.com/2017/02/17/technology/cayla-talking-doll-hackers.html

[27] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[28] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[29] http://www.telegraph.co.uk/cars/news/customer-leaves-bad-review-door-app-gets-banned-garage/

[30] https://blog.filippo.io/the-ecb-penguin/

[31] IEEE. "802.1X-2010 - Port-based Network Access Control", 2010.

[32] IETF. "RFC 3748 - Extensible Authentication Protocol (EAP)", 2004.

[33] IETF. "RFC 2716 - The EAP-TLS Authentication Protocol", 2008.

[34] IEEE. "802.1AE-2006 - Media Access Control (MAC) Security", 2006.

[35] HomePlug Powerline Alliance. "HomePlug AV Specification, Version 2.1", 2014.

[36] Richard Newman, Larry Yonge, Sherman Gavette, Ross Anderson, "HomePlug AV Security Mechanisms", 2007 IEEE International Symposium on Power Line Communications and Its Applications, 2007, pp. 366-371.

[37] Bundesamt für Sicherheit in der Informationstechnik. "Security Aspects and Prospective Applications of RFID Systems", 2005.

[38] ISO. "ISO18092 - Near Field Communication - Interface and Protocol (NFCIP-1)", 2013.

[39] ECMA. "NFC-SEC - NFCIP-1 Security Services and Protocol", 2015.

[40] ECMA. "NFC-SEC - Cryptography Standard using ECDH and AES", 2015.

[41] IETF. "RFC 4434 - The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", 2006.

[42] ECMA. "NFC-SEC - Cryptography Standard using ECDH-256 and AES-GCM", 2015.

[43] Ernst Haselsteiner, Klemens Breitfuß, "Security in Near Field Communication (NFC), Strengths and Weaknesses", in Proceedings of the RFIDSec’06 on RFID security, 2006.

[44] Bluetooth SIG. "Bluetooth Specification Version 4.0", 2010.

[45] Bluetooth SIG. "Bluetooth Specification Version 4.2", 2015.

[46] IETF. "RFC 7668 - IPv6 over BLUETOOTH(R) Low Energy", 2015.

[47] Bluetooth SIG. "Bluetooth Specification, Mesh profile v1.0", 2017.

[48] Tomáš Rosa, "Bypassing Passkey Authentication in Bluetooth Low Energy", Cryptology ePrint Archive: Report 2013/309, 2013.

[49] Mike Ryan, "Bluetooth: With Low Energy comes Low Security", Presented as part of the 7th USENIX Workshop on Offensive Technologies, 2013.

[50] IEEE. "802.11 - Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications", 2016.

[51] IEEE. "802.11ah - 802.11 Amendment 2: Sub 1 GHz License Exempt Operation", 2016.

[52] Matthieu Caneill, Jean-Loup Gilis. "Attacks against the WiFi protocols WEP and WPA", 2010.

[53] Stefan Viehbiick. "Brute forcing Wi-Fi Protected Setup", 2012.

[54] IEEE, 802.15.4:2003 - IEEE Standard for Low-Rate Wireless Networks, 2003

[55] IEEE. "802.15.4:2006 - IEEE Standard for Low-Rate Wireless Networks", 2006.

[56] IEEE. "802.15.4:2011 - IEEE Standard for Low-Rate Wireless Networks", 2011.

[57] IEEE, 802.15.4:2015 IEEE Standard for Low--RateW ireless Networks, 2015

[58] NIST. "FIPS 197 - Advanced Encryption Standard (AES)", 2001.

[59] IETF, RFC3610 - Counter with CBC-MAC (CCM),

[60] Naveen Sastry, David Wagner, "Security Considerations for IEEE 802.15.4 Networks", Proceedings of the 3rd ACM Workshop on Wireless Security, 2004, pp. 32-42.

[61] Radosveta Sokullu, Ilker Korkmaz, Orhan Dagdeviren, Anelia Mitseva, Neeli R.Prasad, "An Investigation on IEEE 802.15.4 MAC Layer Attacks", in Procedings of The 10th InternationalSymposium on Wireless Personal MultimediaCommunications (WPMC), 2007.

[62] Jean-Michel PICOD, Arnaud LEBRUN, Jonathan-Christofer DEMAY, "Bringing Software Defined Radio to the penetration testing community", Black Hat Conference, 2014.

[63] ZigBee Alliance. "ZigBee Specification", 2015.

[64] ZigBee Alliance. "ZigBee IP Specification, rev 34", 2014.

[65] Niko Vidgren, Keijo Haataja, José Luis Patiño-Andres, Juan José Ramírez-Sanchis, Pekka Toivanen, "Security threats in zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned", 2013 46th Hawaii International Conference on System Sciences, 2013, pp. 5132-5138.

[66] Thread Group. "Thread Specification, v1.1.1", 2017.

[67] Thread Group. "Thread Commissioning, v2", 2015.

[68] ITU-T, G.9959 - Short range narrow-band digital radiocommunication transceivers – PHY, MAC, SAR and LLC layer specifications, 2015

[69] Behrang Fouladi, Sahand Ghanoun. "Security Evaluation of the Z-Wave Wireless Protocol", 2013.

[70] Sigma Design. "Security 2 Command Class, version 0.9", 2016.

[71] Sigma Design. "Z/IP LAN Security", 2016.

[72] Chris Badenhop, Ben Ramsey, "Carols of the Z-Wave Security Layer; or, Robbing Keys from Peter to Unlock Paul", published on PoC or GTFO 12, 2016.

[73] Jonathan D. Fuller, Benjamin W. Ramsey, "Rogue Z-Wave Controllers: A Persistent Attack Channel", 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), 2015, pp. 734-741.

[74] SigFox. "Sigfox Technical Overview", 2017.

[75] SigFox. "Sigfox Security White paper, rev 34", 2017.

[76] https://www.ietf.org/proceedings/96/slides/slides-96-lpwan-10.pdf

[77] ST Microelectronics. "STSAFE-A1SX data sheet", 2017.

[78] 3GPP. "3GPP TS 33.401, version 10.3.0, Release 10", 2012.

[79] Roger Piqueras Jover. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio", 2016.

[80] LoRA Alliance. "LoRaWAN Specification, v1.0.2", 2016.

[81] Xueying Yang. "LoRaWAN: Vulnerability Analysis and Practical Exploitation", 2017.

[82] Simone Zulian. "Security threat analysis and countermeasures for LoRaWAN join procedure", 2015.

[83] Gemalto. "Low Power Wide Area Networks security", 2015.

[84] IETF. "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", 2007.

[85] ENISA. "Algorithms, key size and parameters report – 2014", 2014.

[86] NIST. "SP 800-38B, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication"", 2005.

[87] Silvie Schmidt, Mathias Tausig, Matthias Hudler, Georg Simhandl. "Secure Firmware Update Over the Air in the Internet of Things Focusing on Flexibility and Feasibility", 2015.

[88] M. A. Prada-Delgado, A. Vázquez-Reyes, I. Baturone, "Trustworthy Firmware Update for Internet-of-Thing Devices Using Physical Unclonable Functions", 2017 Global Internet of Things Summit (GIoTS), 2017, pp. 1-5.

[89] Boohyung Lee, Jong-Hyouk Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment", J. Supercomput., 2017, pp. 1152--1167.

[90] Shahid Raza, Tony Chung, Simon Duquennoy, Dogan Yazar, Thiemo Voigt, Utz Roedig. "Securing Internet of Things with Lightweight IPsec", 2011.

[91] Ajit A.Chavan, Mininath K. Nighot. "Secure CoAP Using Enhanced DTLS for Internet of Things", 2014.

[92] Shahid Raza, Thiemo Voigt, Vilhelm Jutvik, "Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15.4 Security", IETF Workshop on Smart Objects Security , 2012.

[93] IETF. "RFC 7925 - Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) - Profiles for the Internet of Things", 2016.

[94] NIST. "NISTIR 8114 - Report on Lightweight Cryptography", 2017.

[95] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe. "PRESENT: An Ultra-Lightweight Block Cipher", 2007.

[96] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louis Wingers. "Simon and Speck: Block Ciphers for the Internet of Things *", 2015.

[97] Ronald L. Rivest. "The RC5 Encryption Algorithm", 1997.

[98] David J. Wheeler, Roger M. Needham. "TEA, a Tiny Encryption Algorithm", 1994.

[99] David J. Wheeler, Roger M. Needham. "Tea extensions", 1997.

[100] Mickaël Cazorla, Kevin Marquet, Marine Minier, "Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks", 2013 International Conference on Security and Cryptography (SECRYPT), 2013, pp. 1-6.

[101] Junfeng Fan, Lejla Batina, Ingrid Verbauwhede, "HECC Goes Embedded: An Area-Efficient Implementation of HECC", Part of the Lecture Notes in Computer Science book series (LNCS, volume 5381), 2009, pp. 387-400.

[102] Jeff Hoffstein, Daniel Lieman, Jill Pipher, Joseph H. Silverman. "NTRU: A public key cryptosystem", 1996.

[103] Markku-Juhani O. Saarinen. "The BlueJay - Ultra-Lightweight Hybrid Cryptosystem", 2012.

[104] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy, "RFID Noisy Reader, How to Prevent from Eavesdropping on the Communication?", Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, , pp. 334-345.

[105] Gerhard P. Hancke, Markus G. Kuhn, "An RFID Distance Bounding Protocol", First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), 2005, pp. 67-73.

[106] IETF. "RFC 4107 - Guidelines for Cryptographic Key Management", 2005.

[107] Laurent Eschenauer, Virgil D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 41-47.

[108] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. "SPINS: Security Protocols for Sensor Networks", 2001.

[109] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, 2014, pp. 266-282.

[110] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A Roadmap for Security Challenges in Internet of Things", Digital Communications and Networks, 2017.

[111] ITU-T. "Y.2061 - Requirements for the support of machine-oriented communication applications in the next generation network environment", 2012.

[112] http://www.3gpp.org/DynaReport/33-series.htm

[113] http://www.3gpp.org/DynaReport/35-series.htm

[114] Broadband Forum. "TR-069 - CPE WAN Management Protocol", 2013.

[115] oneM2M. "oneM2M-TS-0003 - oneM2M Security Solutions", 2014.

[116] oneM2M. "oneM2M-TR-0008 - Analysis of Security Solutions for the oneM2M System", 2013.

[117] http://ubertooth.sourceforge.net/

[118] https://github.com/riverloopsec/killerbee

Glossary

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
3GPP	3rd Generation Partnership Project
6LBR	6LoWPAN Border Route
6LN	6LowPAN Node
ACL	Access Control Lists
AES	Advanced Encryption System
AIOTI	Alliance for IoT Innovation
AP	Access Point
APP	Application layer
ARP	Address resolution Protocol
ATT	Attribute Protocol layer
BLE	Bluetooth Low Energy
CBC	Cipher Block Chaining mode
CCM	Counter with CBC-MAC mode
CCMP	Counter Mode CBC-MAC Protocol
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environment
CPS	Cyber-physical System
CRC	Cyclic Redundancy Check
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CTR	Counter mode
D-BPSK	Differential Binary Phase Shift Keying
DdoS	Distributed Denial of Service
DES	Data Encryption Algorithm
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EC-GSM-IoT	Extended Coverage GSM for the Internet of Things
ECB	Electronic Code Book mode
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EDR	Event Data Recorder
eGPRS	Enhanced General Packet Radio Service

ETSI	European Telecommunications Standards Institute
EU	Europe Union
FDMA	Frequency Division Multiple Access
FFD	Full-Function Device
GATT	Generic Attribute Profile layer
GCM	Galois Counter Mode
GCMP	Galois counter Mode CBC-MAC Protocol
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile Communications
GTS	Guaranteed Time Slot
HAN	Home Area Network
HCI	Host Controller Interface
HF	High Frequency
HMAC	Hash-based Message Authentication Code
HSS	Home Subscriber Server
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster on the Internet of Things
IETF	Internet Engineering Task Force
IoT	Internet of Things
IOT-A	Internet of Things - Architecture
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISM	Industrial, Scientific and Medical band
ITS	Intelligent Transport Systems
ITU-T	International Telegraph Union Telecommunication Standardization Sector
JTAG	Joint Test Action Group
L2CAP	Logical Link Control and Adaptation Protocol layer
LAN	Local Area Network
LF	Low Frequency
LTE	Long-Term Evolution
LTK	Long Term Key
M2M	Machine to Machine
MAC	Medium Access Control layer
MACsec	Medium Access Control Security
MIC	Message Integrity Code

MitM	Man In The Middle
MLE	Mesh Link Establishment
MME	Mobility Management Entity
MSK	Master Session Key
NB	Narrow-band
NB-IoT	Narrow-band IoT
NET	Network layer
NFC	Near Field communication
OEM	Original Equipment Manufacturer
OFB	Output FeedBack mode
OOB	Out-of-Band
P2P	Peer to peer
PAKE	Password Authenticated Key Exchange
PAN	Personal Area Network
PANA	Protocol for Carrying Authentication for Network Access
PC	Personal Computer
PDU	Protocol Data Unit
PHY	Physical layer
PIB	PAN Information Base
PIN	Personal Identification Number
PLC	Power Line Communications
PRF	Pseudo-Random Function
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
RC4	Rivest Cipher 4
REED	Router-Eligible End Device
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request For Comment
RFD	Reduced Function Device
RFID	Radio Frequency Identification
ROLL	Routing Over Low power and Lossy networks
RPL	Pv6 Routing Protocol for Low-Power and Lossy Networks
RSA	Rivest, Shamir y Adleman
SDO	Standards Developing Organizations
SED	Sleepy End Device
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SIM	Subscriber Identity Module (an application running on a UICC)

SSID	Service Set Identifier
STK	Short Term Key
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TK	Temporary Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TP	Transport layer
UDP	User Datagram Protocol
UE	User Equipment
UHF	Ultra High Frequency
UICC	Universal Integrated Circuit Card (sometimes known as the SIM card)
UNB	Ultra-narrow Band
US	United States
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wireless Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	WiFi Protected Setup
WSN	Wireless Sensor Networks
XOR	eXclusive OR
Z/IP	ZigBee IP