Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies (FEM)

Bachelor Thesis

Security of IoT: vulnerabilities and ways to prevent them

Tomiris Kassimova

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Tomiris Kassimova

Systems Engineering and Informatics
Informatics

Thesis title

Security of IoT: vulnerabilities and ways to prevent them

Objectives of thesis

The main objective of the thesis is to analyse IoT security and propose possible security solutions of selected sector.
Partial goals of the thesis are such as:
- characteristics of current IoT sectors.
- characteristics of current IoT devices of selected sector.
- analysis of the standard protocols defined for the Internet of Things.
- formulation of the future insight on improvement of the security in provided technology.

Methodology

Methodology of the thesis is based on study and analysis of information resources. The base of practical part is in analysis of IoT security and propose security solution of selected IoT sector. Based on the theoretical findings and results of the practical part, final conclusion and recommendation will be formulated.

The proposed extent of the thesis

40 pages of text.

Keywords

Internet of Things, IoT, security, protocols, vulnerabilities

---

Recommended information sources

Hassan, Qusay F., et al. Internet of Things: Challenges, Advances, and Applications. CRC Press/Taylor & Francis Group, 2018.

Serpanos, Dimitrios, and Marilyn Wolf. Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies. Springer International Publishing, 2018.

Simon, Michael. "Internet of Things Security Issues Bleed into 2018." Help Net Security, 17 Jan. 2018, www.helpnetsecurity.com/2018/01/16/internet-of-things-security-issues-2018/.

Writer, Guest. "The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History." IoT For All, 15 Feb. 2018, www.iotforall.com/5-worst-iot-hacking-vulnerabilities/.

Expected date of thesis defence

2019/20 SS – FEM

The Bachelor Thesis Supervisor

Ing. Pavel Šimek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 23. 03. 2020

Declaration

I declare that I have worked on my bachelor thesis titled "Security of IoT: vulnerabilities and ways to prevent them" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any person.

In Prague on 23.03.2020 _____

Acknowledgement

I would like to thank my supervisor Ing. Pavel Šimek, Ph. D for his help and time, also I am grateful to everybody who supported me during work on this paper.

Security of IoT: vulnerabilities and ways to prevent them

Abstract

For the past few years the Internet of Things became a very common concept and offers a potential of bringing many advantages into the world. It presents us with global network of computing devices embedded in everyday objects, which can interact with each other over the internet and thus, proposes quite many beneficial and convenient applications in daily life, business environments and many other spheres.

However, as more devices appear, deployed in complex and uncontrolled environments, security of IoT may present a few challenges. Lack of security and virtual protection of IoT technology presents the main problem.

Therefore, this paper will have two main approaches. Firstly, it will cover main challenges in IoT security, by analyzing current state of technology and secondly, propose and highlight possible solutions and advices on how to maintain IoT environment secure.

Keywords: Internet of things, IoT, Smart Home, security, protocols, vulnerabilities, Smart things, Z-Wave, Thread, ZigBee, KNX-RF, EnOcean

Table of content

List of figures

List of tables

List of abbreviations

AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Block Chaining
AES-CTR	Advanced Encryption Standard-Counter Mode
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter Mode with CBC-MAC
CMAC	Cipher-based Method Authentication Code
IPv6	Internet Protocol version 6

1 Introduction

Although Internet of Things (IoT) is relatively new technology and has not been used for very long, the very first concept of machines communicating with each other was born in the early 1800s (Dataversity, 2016) and the Internet of Things itself was first mentioned and coined by Kevin Ashton (Ashton, 2009) from Massachusetts Institute of technology's Auto-ID Labs (MIT) not a long after World Wide Web was first unleashed [1]. And throughout the time, when new technologies and advancements were introduced to the world, the idea of many devices capable of sensing, recording and communicating data wirelessly became possible and quite feasible.

Simply stated, the Internet of things presents us with the idea of giving physical objects used in daily lives a virtual presence, which makes this technology applicable and useful in many known fields and environments. This is simply happening by attachment of embedded computing devices to these objects, which consequently makes them so called smart objects / devices. These devices are uniquely identifiable, and they are capable of communicating with each other over the Internet [2].

The implementation of IoT technology is based on integration and deployment of existing technologies, to name a few significant: The Internet itself, sensors, radio frequency identification (RFID), near field communication (NFC) and others. Integration of those technologies into a system is what makes almost any device connected to the Internet with on/off switch to be part of IoT environment. This may include diverse variety of devices, the ones we use in our daily lives or almost anything we can think of, starting from powerful servers to the simplest constrained devices, such as RFID tags.

Keeping in mind that constrained devices are having limited processing capabilities, such as power, memory and bandwidth, it is more than possible that this kind of devices, may form insecure networks with low throughput, vulnerabilities and high probability of packet loss [3]. In this case, traditional security solutions used and designed for the Internet will not apply and function properly, mainly because they require a considerable amount of energy and resources, which, unfortunately, constrained IoT devices do not possess. Nonetheless, this issue was faced, and many research were done in order to enhance technology and develop applicable security solutions for constrained devices.

Bearing the fact, that IoT is used in large-scale environments and works with sensitive information, which is being constantly collected by the devices and

communicated throughout the network, security gains particular importance. Security concerns about confidentiality, integrity, availability of the data and information of the system, authentication, authorization and, thus, this paper will focus on how these crucial aspects of security are being maintained in IoT, specifically in Smart Home Systems. Also, it will cover security vulnerabilities of the system and advise possible solutions on how to maintain environment secure in all the mentioned aspects.

2 Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to analyze IoT security and propose possible security solutions of selected sector.

Partial goals of the thesis are:

- characteristics of current IoT sectors.
- characteristics of current IoT devices of selected sector.
- analysis of the standard protocols defined for the Internet of Things in selected sector.
- formulation of the future insight on improvement of the security in provided technology.

2.2 Methodology

Methodology of the thesis is based on study and analysis of information resources. The base of practical part is in analysis of IoT security and proposal of the security solutions of selected IoT sector. Based on the theoretical findings and results of the practical part, final conclusion and recommendation will be formulated.

3 Literature review

3.1 What is IoT? Definition of Internet of Things

Multiple international research centers and organizations have been involved in creation of common ground for the Internet of Things technology, which involved finding a general definition of the concept. The very first definitions of it were tightly connected to RFID – radio-frequency identification and as for Kevin Ashton, who first emerged the term, it generally meant “empowering computers with their own means of gathering information”, so that they would be capable of knowing everything there was to know, such as keeping track and counting everything around, sense the world around and analyze gathered data. (Ashton, 2009).

Throughout the time, as the term was becoming more universal and familiar to a greater audience, definitions started to evolve into more general concepts. For instance, later on The Study Group 20 (SG 20), which was established in 2005, published first ITU report on IoT with the support of the International Telecommunications Union Telecommunication Standardization Sector (ITU-T). In the published recommendation document Y.2060, the following definition of the IoT was proposed (ITU-T, 2012):

IoT as defined in ITU-T [ITU-T Y.2060]:
“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 [4].”

Following definition is explaining that Internet of Things is establishing so called new dimension, referred as well as “any thing” to the known digital connectivity, which already allows us to have communication “any time” and “any place”. “Thing” in this case would mean any kind of object that has virtual or physical identity and is capable of communicating with other things. Those objects as have mentioned before are capable of communicating with each other and can have attached sensors and actuators. Examples of physical objects would be any everyday object which was enhanced digitally, such as electrical appliances, machinery used for industrial purposes. Whereas virtual object is any

object that exists in the informational world, thus can be accessed, stored and processed. Example of those would be software.

There are many other definitions proposed by various research groups, some may have categorized definitions into two: those that think of an Internet of things as a concept and others as an infrastructure. However, even though the wording might be different, the main concept of the IoT would still remain similar: The Internet of things is made of virtual and physical objects, which have unique identity and are capable of capturing data and communicating with each other over the Internet.

3.2 Applications of IoT

IoT is promising to improve the quality of lives and societies as a whole. There are various fields in which IoT has been developed and implemented by now. Some sectors will be covered in this section; those will include health and fitness monitoring, environmental sector, smart cities and home automation [8].

(i) Smart cities

Smart cities are an urban territory that implements various technologies in order to improve the overall quality of the city and manage resources and assets more sufficiently. The main applications of IoT in smart cities are:

- Traffic management
- Safety on the roads (Accident detection applications)
- Intelligent parking
- Smart water systems

(ii) Health and Fitness

IoT has been proved very beneficial within health and fitness fields.
In the health industry IoT sensors are used for constant monitoring of patient's parameters with serious illnesses or those who are not able to operate by themselves. Such conditions as temperature, humidity, blood pressure, heartbeat rate and many others are being collected and then processed by the system, and later be used for future prescriptions.

In the Fitness IoT has already gathered good reputation. Many various wearable devices are used for recording fitness activities, different health parameters during activities.

(iii) Agriculture and Environment

IoT contributes to agriculture and environment sector by helping to enhance production, manage resources effectively and improve quality of products. Sensors are mainly used to measure various parameters, such as soil information, temperature, humidity in real time. The data is then processed, and the results are used to adjust those parameters and eventually improve quality of the grown plants.

(iv) Smart Homes

Home automation is becoming very popular due to a couple of reasons. Sensors, actuators and wireless sensor network technologies are becoming more mature and therefore allow more space for development. Moreover, nowadays people are more openminded to allow various systems to improve the quality of their lives.
In home automation various sensors are used to provide smart solutions for the people who seek to automate some daily tasks and maintain some of the routine rituals. Smart homes also include such applications as security, energy conservation and entertainment.

3.3 Enabling technology

The Internet of Things is a developing area, which means that many new technologies are being implemented as the years pass. International organization ISO WG 10 prepared mind map which includes 6 IoT related areas [5], such as technologies, application areas, requirements, stakeholders and standards. Technology itself has a separate mind map, mainly because a great number of still developing and existing technologies that are aiming to be a key enabling technologies of the internet of things. However, in this paper only a few of them would be mentioned.

3.3.1 Identification

As we got to know from the above chapter, all of the things within the distributed network has to be uniquely identifiable, thus they require certain technologies. And when we say things, we mean any physical or virtual object, an event or even a person. There is no one particular technology used for all of these objects and they may differ depending on purpose [6].

Alliance for internet of things innovation (AIOTI) has presented an executive overview of the identifiers in Internet of things in which they were classified into multiple groups.

Briefly, it includes (Identifiers in IoT, version 1.0 2018):

i. Thing identifier – used to identify the things of an Internet of Things application. It could be for instance any physical or digital object, others would include applications, services, users and etc. (e.g. barcodes, RFID tags)

ii. Application and service identifier – used to identify different SW applications and services (e.g. API)

iii. Communication identifier – as name implies, used to identify various communications points, such as source and destinations, as well as sessions. (e.g. MAC addresses, IP addresses)

iv. User identifier – identifies users of Internet of Things services and applications. Users would include humans, any parties and SW applications that interact and access with the IoT system (e.g. for humans - username, fingerprints, for SW applications – unique keys)

v. Data identifier – is used to identify both data types and some specific data instances (e.g. meta data)

vi. Location and protocol identifier – used to identify location in a geographic region (e.g. coordinates and postal addresses)

vii. Protocol identifier – used to inform and ensure which protocols have to be used in order to establish particular communication interchange

3.3.2 Smart object communication patterns

Internet of Things world is all about communications between various devices, gateways and cloud. Data is being interchanged between all of the mentioned parties, with the main aim of comprehensive end-to-end communication. This section will describe basic communication patterns utilized in IoT environment, including available communication technologies and protocols used.

RFC 7452 [7] described four communication patterns in smart object communication (Architectural Considerations in Smart Object Networking, 2015), which are:

- Device-to-device pattern

This type of communication applies when two devices interoperate and communicate directly, usually using a wireless network. Depending on usage scenario, there are several protocol bundles that could be used to carry out this particular type of communication. Those may include Bluetooth, IPv6, User Datagram Protocol (UDP), and Constrained Application Protocol (CoAP)

- Device-to-cloud

This pattern is used when device uploads data captured from certain environment on application service provider. In this pattern communication is based on Internet Protocol (IP). However, the integration of other devices may occur to be difficult when manufacturer of the device and the Application service provider are the same. To terminate this problem, protocols that could be used to communicate with the server have to become available.

- Device-to-gateway

This pattern can be used when there are non-IP devices being the part of the system, as well as when there is a need of legacy devices and in case when some additional security functionality needs to be implemented. Gateways in this case can be mobile (Mobile phones for instance), which means they will provide only temporary connections to the Internet.

- Back-end data sharing

Bank end data sharing pattern is needed when there is a necessity to analyze combined data from various sources. This pattern may also be used to move data from one IoT service to another (Rose at al., 2015).

It is worth mentioning that including well known communication technologies, such as Bluetooth, GSM, Wi-Fi, there are many other technologies and communication standards developing right now specifically for IoT scenarios. Good example would be Low power wide area networks (LPWAN), which are dedicated specifically for systems which are composed of devices with constrained capabilities.

3.3.3 IoT communication protocols

This section will provide comprehensive overview of communication protocols that are being used in IoT systems. However, this section will only overview protocols used in IoT, and in the practical part of the thesis, Smart Home wireless protocols will be analyzed separately.

The IoT has a wide range of applications, those will include healthcare, industry, transportation, logistics and many others. Connection between things may be wireless or wired. Since a wireless connection tends to be a main focus of the IoT technology, many wireless communication protocols can be used. Some examples are: Internet Protocol Version 6 (IPv6), ZigBee, Near Field Communication (NFC) over Low power Wireless Personal Area Networks (6LoWPAN), Bluetooth Low Energy (BLE) and etc.

Communication protocols used in IoT may be categorized into Low Power Wide Area Network (LPWAN) and Short-Range Network [9]. See figure 1.

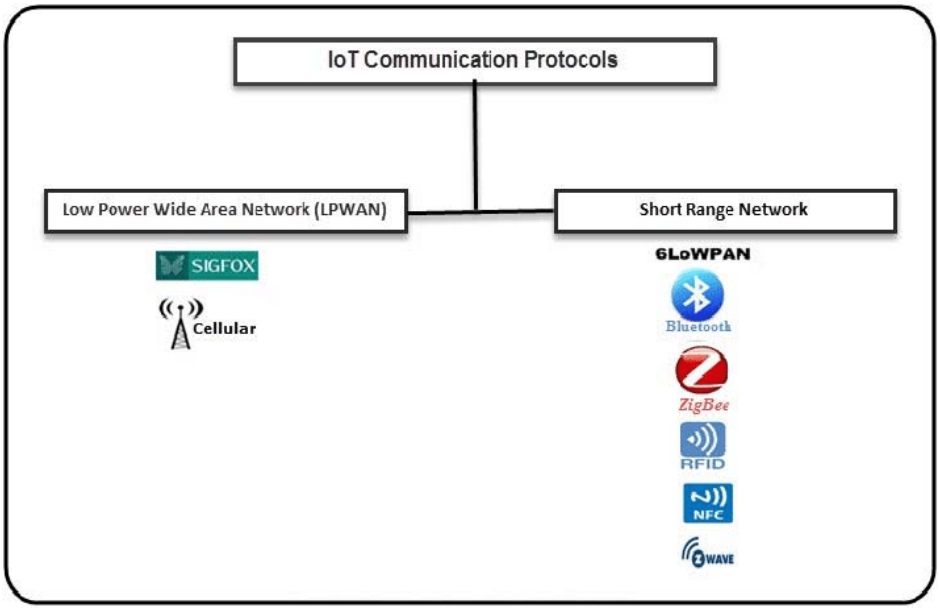

Figure 1: Internet of Things Communication Protocols (Source: Internet of Things (IoT) Communication Protocols: Review, 2017)

(i) Low Power Wide Area Network (LPWAN)

- SigFox

SigFox is a technology which connects great and diverse range of low-power energy devices, which include M2M applications and sensors. Used for transmission of small amount of data with the range up to 50 km and uses Ultra Narrow Band (UNB) technology, which only requires small battery and was designed to manage low data transfer speed (10 ~ 1000 bits/second). Near field communication (NFC) is usually used in such devices as patient monitors, security and agriculture devices, environmental sensors, smart meters and etc. SigFox network topology is star [9].

- Cellular

This technology allows high throughput data over long distances and reliable connection to internet but requires high power consumption. Thus, it won't be suitable for local networks and M2M communications. Cellular technology can be used for many applications, especially those which deploy mobile devices.

(ii) Short Range Network

- 6LoWPAN

6LoWPAN was created by the IETF – Internet Engineering Task Force and it is most common standard on the Internet of Things communication protocols. It is a low-cost variant with low bandwidth energy consumption.

6LoWPAN is an IP based protocol and can allow direct connection to another IP network with no intermediate translation gateways and proxies. It utilizes Internet Protocol (IP) over low-power wireless IEEE802.15.4 networks using Internet Protocol Version 6 (IPv6). 6LoWPAN can support various topologies such as star or mesh.

- BLE

Bluetooth Smart protocol plays an important role for IoT application. Designed for short-range, low latency and low bandwidth and has lower power consumption.

- RFID

RFID system is consisting of RF tag – small radio frequency transponder with programmed unique information, which contains distance reading characteristics and Reading Device called Reader. IoT applications include health care, smart shopping and etc.

- NFC

Near field communication is a short-range technology, which transmits data between devices by bringing them together or distant no more than a couple of inches. NFC used similar to RFID technology principals, but it could be used not only for identification, but also more established two-way communication. This technology is being used for contactless payments, by mobile phones and in various industrial applications.

3.4 IoT Architecture

IoT devices are equipped with various sensors, actuators and embedded transceivers along with processors. It cannot be referred as one single technology, but rather a tandem of technologies working together.
To connect all the various devices within IoT network a lot of standardization is needed, which is still one of the greatest issues of the technology. Thus, there is no universally agreed architecture for Internet of Things. In this section two most common proposed architecture will be discussed: Three-Layer and Five-Layer Architectures. [8]

Three-Layer Architecture is one of the most basic proposed architectures. As shown in the figure 2 it is made of three layers, which go as following: the perception layer, the network layer and application layer.

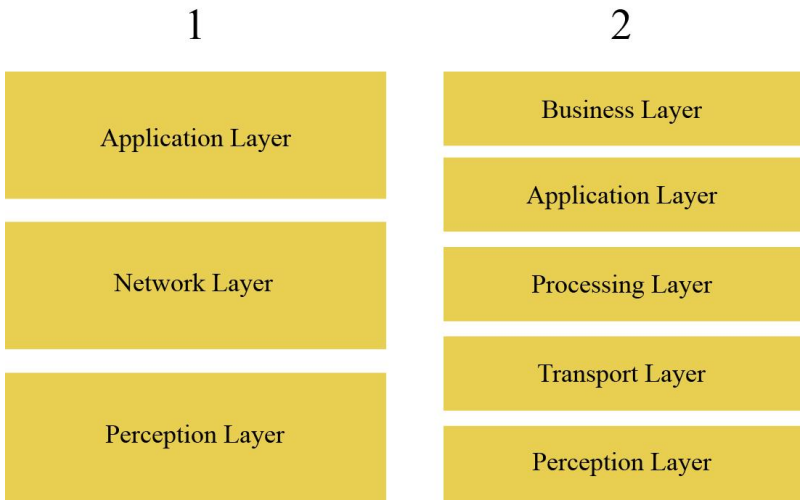

Figure 2: Architecture of IoT (1) Three-Layer and (2) Five-Layer (Source: Author)

(i) The perception layer - physical layer consisting of all the sensors, which are responsible for sensing and collecting data from its physical environment. It is also responsible for sensing physical parameters and identification of other smart devices within the network.

(ii) The network layer – is a layer, which is responsible for connection of smart things, networking devices and servers. It is also where transmission and processing of sensor data is happening. This layer consists of physical components and network communication software primarily responsible for transferring information captured by the perception layer sensors to other layers without intervention.

(iii) The application layer – is a layer responsible when it comes to delivery of application services to the user. In other words, this layer provides the services to the user as per his requirement. It basically defines how and in which specific applications IoT can be deployed. Those include smart environments, such as smart homes, cities, health etc.

Three layered architecture is describing main concept of IoT, defining basic layers and their idea. However, for a deeper research, which focus on detailed aspects of the Internet of Things this architecture might be insufficient. Thus, the other, more

detailed architecture was introduced. In comparison with Three-Layer Architecture, Five-Layer Architecture contains two additional layers, namely, the processing and business layers. Which makes it this structure: the perception, transport, processing, application and business layers. The perception and application layers have the same definition as in previous architecture, thus other three layers will be described below.

(i) The transport layer - is a layer, responsible for transferring sensor data through networks (e.g. 3G, Bluetooth, wireless, RFID, NFC) from the perception layer to the next – the processing layer and in the opposite direction.

(ii) The processing layer – middleware layer, whose main functions is to store, analyze and process huge amounts of upcoming data from the transport layer. This layer can also provide various services for the lower layers. The processing layer is employing diverse set of technologies, to name a few, cloud computing, big data, databases.

(iii) The business layer – layer for managing of the whole IoT system, which includes applications, privacy of the users, business models.

It is also important to mention Open Systems Interconnection (OSI) layer and TCP/IP models, see figure 3, which give a better understanding of how protocols are being implemented generally.

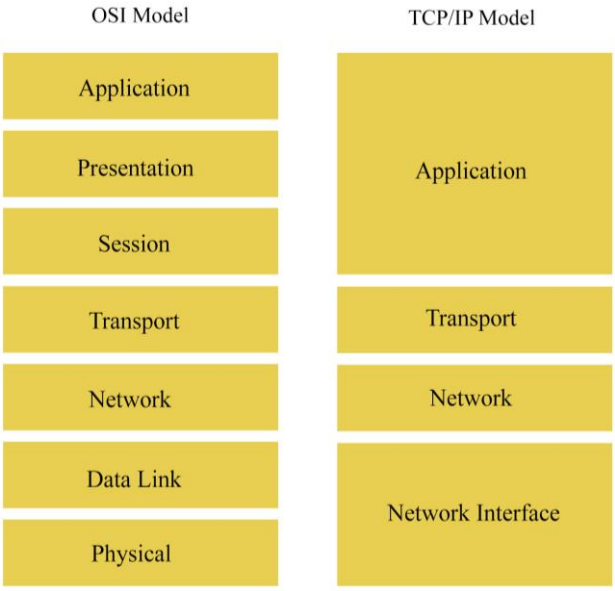

Figure 3: OSI and TCP/IP models overview (Source: Author)

3.5 Topologies

Another key element, which should be covered is the way devices in the network are connected to one another via wireless domain. Even though, there are various topologies to cover, following topologies can be determined as main types:

(i) Centralized / Star:

Centralized or star topology has a central node (hub), which takes responsibility of managing communications between all nodes within the network, as well as outside of it. All the messages are passing through the central node and are redirected accordingly.

(ii) Decentralized / Fully connected:

In this type, nodes are interconnected with other nodes within the network. Decentralized topology might not be efficient when talking about bigger networks, because increasement of number of nodes causes communication effort exponentially.

And other types include following topologies:

(iii) Mesh:

This type of topologies presents multiple ways for a message to reach its end destination. One node in the network can be connected to one or multiple nodes. Routing algorithm is used to determine the way messages will take in order to reach the destination.

(iv) Ring:

Each node in the following topology is connected to two nodes, which creates a closed loop or ring. Messages are transmitted along the loop in one direction until they reach their final destination.

(v) Bus:

In the bus topology, nodes are connected to the transmission medium / backbone, where all the messages and communications are going through. Each node will receive every message sent, however only intendent node will accept it.

(vi) Line:

Simplest topology, which presents connection between two endpoints.

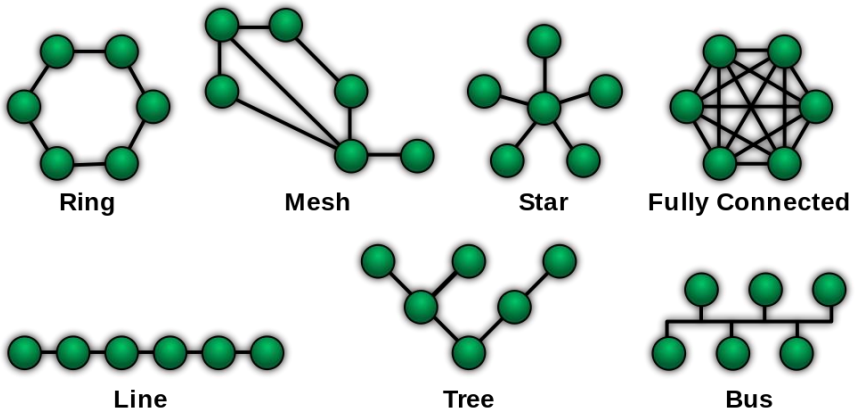

Figure 4: Visualization of network topologies (Source: https://commons.wikimedia.org/w/index.php?curid=15006915)

3.6 Main challenges

As it was mentioned before IoT is a driving power of technological development and promises to make great transformations not only in technological area, but also society and economy. Thus, all of the involved stakeholders starting from manufacturers, ending with users may face challenges related to IoT. This chapter will cover some of the main ones, including interoperability, openness, security, scalability and how IoT systems handles failures. The main focus would be security aspects of the IoT.

(i) Interoperability

IoT systems are composed of various things, machines, devices and groups of them, which require communication and full cooperation between each other. For this system to work, every single element should be uniquely identifiable as well as discoverable to others. Interoperability is a crucial aspect in IoT and requires further development and constant revision as much more new technologies appear and as more things are appearing [9].

(ii) Openness

Openness of a system is important in IoT. It is defined as the amount or degree in which a system can be expanded or reimplemented in different and new ways. When building an IoT system, it is necessary for the devices that compose such a system to be able to interact and exchange data between other systems in order to create a robust IoT system.

(iii) Scalability

With the number of users and resources growing rapidly each year, systems must be able to retain their effectiveness in working under such growth and this is where scalability comes into play. a large number of this growth is due to the increase of mobile users. When discussing scalability, 2 levels of are proposed or thought of in the area of IoT. first being network scalability and second is data scalability. it explains that when the number of objects or devices in a network increase, openness of a system must be ensured as well as privacy and safety of the data.

3.6.1 Security

Security is being a great concern when implementing IoT systems. For sure we mean the degree of defense or protection of the IoT infrastructure and applications. Most of these devices are easy pickings because they rely on a few external resources and often remain unprotected. Predictions state that the amount of IoT devices will increase to 20 billion things by 2020. And the main challenge is to make a common and secure framework that will apply to all of them.

This section will provide overview of the key types of security challenges that are presented on the Internet of Things systems. Those will include Authentication, Authorization, Confidentiality, Integrity and Privacy.

3.6.1.1 Authentication

Authentication is an important process which identifies whether something is what it claims to be. This applies to everything that is pretending to be something else in order to access the system.

The identification in IoT plays an important role and has to be aware of not only the users and electronic devices, but what it is communicating to. And since most of the communications in IoT occur without human interaction, it is crucial to ensure that only correct and authorized devices and users can access the system [11].

3.6.1.2 Authorization

Authorization mechanism is used to determine the privileges that every device has, which is practically what actions device can and allowed to perform. For instance, device can have limited access to the data or full access to resources. Thus, authorization mechanisms are playing an important role in controlling the actions and operations each device is able to perform.

IoT environments are usually large scale and there is always a possibility that some devices within the network can be compromised. Therefore, authorization mechanisms can make sure that there are restrictions to device, which is being compromised by the attacker.

One of the examples of the authorization mechanisms is the user account, which is used to access computer. The initial log in will be a part of authentication process, however after user got an access to the system, the access control mechanism is going to define which actions user can perform under this specific username.

3.6.1.3 Confidentiality

Confidentiality is one of the crucial aspects in modern world. Confidentiality ensures that only those who have a rightful access to the information, should have access to that particular information.

In IoT environments confidentiality has even a bigger importance since majority of the time IoT devices gather and transmit very sensitive information. And, thus, IoT users would not want their personal information to be public.

A good example of confidentiality within IoT is all the data that devices can collect about you and your schedule within smart home IoT network. The information is not only private and sensitive in nature but can also be beneficial in hands of wrong people, such as intruders.

3.6.1.4 Integrity

Integrity is used to ensure if the information or data is correct and wasn't changed or modified in any way by malicious or unauthorized entities. This is crucial when we are talking about transmission of information from one IoT device to another, since this is one of the weak spots of the network.

Integrity in IoT is of key importance, mainly due to the fact that IoT system will not function properly without collection of accurate data by sensors. That is why system should not allow side modifications of data and in case it happened, system should identify it.

Importance of integrity within IoT can be seen in health-care sector. If the data collected by sensors is being modified by third-party

3.6.1.5 Privacy

Privacy itself is a very broad field, which has a wide range of research and therefore is not going to be in the scope of this paper.

IoT systems tend to gather a lot of data from the surrounding environment, which includes information about individuals involved. Therefore, privacy becomes an important security concern.

Privacy is best described as the individual's right to decide what kind of information of himself should be communicated, how it should be communicated and to which extent it should be communicated. Even though, privacy may involve such aspects as prevention of information being read during transmission or potentially when being stored, privacy involves a deeper concern, because information is still being available for the central server where all the procession and storage happens. And as such, such means as anonymity and digital forgetting are important in ensuring privacy.

Anonymity's idea behind is to remove or decouple the connection between certain user and the gathered data. Digital forgetting implies complete removal of the data from the digital environment.

3.7 Vulnerabilities

The Internet of Things communications and devices are vulnerable to various threats, same as normal networks and devices are. Therefore, it is important to understand what kind of vulnerabilities IoT devices and network can face. This section will provide a brief overview of main threats which face IoT. Those will be categorized according to Three-Layered Architecture: Physical (Perception), Network and Application layer [14].

And even though, the main focus of the following paper is analysis of security on Network layer, all layers have to maintain security in order to provide security to the IoT environments.

Threats appearing on physical level include all the attacks, which directly target physical part of devices. Network section will include threats that appear during transmission of the data between nodes. And at last, attacks targeting application layer will be discussed.

IoT layer	Security issue
Application layer	Information availability, user authentication, information privacy, data integrity, IoT platform stability, middleware security, management platform
Transport layer	DOS/DDOS attacks, forgery/middle attack, heterogeneous network attacks, WLAN application conflicts, capacity and connectivity issues etc.
Sensing layer	Interruption, interception, modification, fabrication, uniform coding for RFID, conflict collision for RFID etc.

Table 1: Summary of security vulnerabilities in the IoT architecture (Source: Security in Internet of Things: A Survey, 2017)

3.7.1 Physical (Perception)

(i) Accessing device physically. This can only happen if the intruder gets into the same place, where the IoT system is being implemented. Attacker can remove parts of IoT devices or the whole device.

Another type of attack that can be applied when intruder has physical access to the IoT devices is differential power analysis [12]. It is based on analysis and

finding patterns of the power consumption of an IoT device, and which later can be used to find cryptographic keys.

(ii) Outdated firmware may be one of the problems that occur with many devices and routers [31]. Ubuntu presented a survey which shows that many users don't update firmware, when its needed. Updating firmware in IoT is important; as long as many devices are expected to function for a long time with no human interference, failure to apply updates may give attackers a breach from known issues.

(iii) One of the problems that may occur can be caused by pre-computed cryptographic keys [31]. These keys are usually already implemented to the firmware and are commonly same or not sufficiently random. This can be a weak spot as long as attacker may guess or know the cryptographic key used in device.

3.7.2 Network

It is important to mention that many IoT devices may still have an unsecured communication.

(i) Man in The Middle Attack (MITM) – attack based on interception of communication between two nodes in a network. A common example of the MITM attack would be client – server communication. An attacker is pretending to be a server to which client is connecting to. When the request from the client has been received, the attacker sends it to the server and the other way around. This is allowing attacker not only to see what is being transferred, but also make changes and modifications [15].

(ii) DDoS attack is a denial-of-service attack; It aims to make a computer or network resource inaccessible to its intended users by momentarily or permanently disabling a host's internet-connected services. In the case of a

distributed denial-of-service attack (DDoS), incoming traffic flooding to a target derives from multiple sources, making it nearly impossible to avoid the cyber-attack simply by blocking a single source. DDoS attacks are actually rising rapidly, primarily because of the lack of security in IoT Devices. [22]

The ultimate objective of a DDoS hacker who is hacking into an IoT device is not to interfere with consumer heating systems or disrupt their morning coffee routine, but rather to manipulate thousands of devices and turn them into a "zombie army". A DDoS attack can be large enough to bring even a supposedly "secure" corporate network down, or it can be minor— nearly invisible that escapes human detection but infiltrates and maps networks very quickly. All are dangerous.

One of the biggest DDoS attacks on IoT networks happened in 2016, when Botnet Attack utilized around 400,000 IoT Devices. At one point, the researchers claim the botnet generated more than 292,000 requests per minute. When researchers looked closer at the IP addresses involved in the incident, it found that most of them were linked to the internet of things. [23]

(iii) Sybil attacks are conducted over a network using false identities or devices. One or more malicious nodes operate as multiple nodes, influencing, manipulating or spying on other legitimate nodes [17].

(iv) Hijacking device. The intruder hijacks a device and ultimately takes control. These attacks are very hard to detect as the attacker does not change the device's basic functionality. In addition, re-infecting all smart devices in the home theoretically requires only one device. For example, an intruder who initially compromised a thermostat might potentially gain access to a whole network and open a door remotely or change the PIN code of the keypad to restrict entry.

3.7.3 Application

The study of a newer, programmable smart home device illustrates IoT device layer vulnerabilities [24]. Multiple design vulnerabilities were discovered in smart home applications, and then used to execute attacks to obtain lock pin codes, disable vacation mode and trigger false alarm in smart home security systems. Many of the found vulnerabilities involve Over-privileging. A common issue with IoT systems appears to be over-privileged default users. Applications can get more functionality than they need, because of the SmartThings system which was used in this case.

4 Analysis of Security in Smart Home

Keeping in mind that IoT is a very broad and vague field and that it is covering wide range of different devices which have completely different uses and ways of operating, it would be hard to focus on everything at once. Therefore, practical part of this paper will be focusing on one specific and common field of IoT application, which was mentioned before – Smart Home domain.

As it's been discussed in the theoretical part of the paper, currently there are many security challenges and vulnerabilities which appear in IoT implemented systems. Smart Home systems are not an exception and therefore, it is important to understand what the current state of security is and what can be done to improve it.

According to the main objectives of the thesis, following research question were chosen for the practical part:

(i) What security mechanisms are used in the most common communication protocols in the domain of smart homes?

(ii) Are there any vulnerabilities present in the chosen protocols?

(iii) Which protocol/protocols is/are the most effective in terms of security?

Wireless communication means are more popular in the modern systems, including smart homes. Wired connection is harder to implement and organize, thus it is usually unsuitable for many users. Therefore, as the main focus of the analysis in the practical part, following Smart Home wireless communication protocols were chosen: KNX – RF, EnOcean, Thread, ZigBee and Z-Wave.

Starting with a brief introduction into smart homes and characteristics of IoT devices within that domain, this section will include overview of chosen wireless protocols, followed by analysis of the security mechanisms used in each.

4.1 Smart Home System

In simple words, smart homes can be defined as a connection of everyday used objects in order to form the common network with the main aim of improving efficiency, functionality and convenience of life within the house. In modern world, this kind of systems are used to control and maintain the house automatically.

There are many fields of application in such setup, such as security, energy consumption, entertainment and hassle-free lifestyle, see figure 5 [8]:

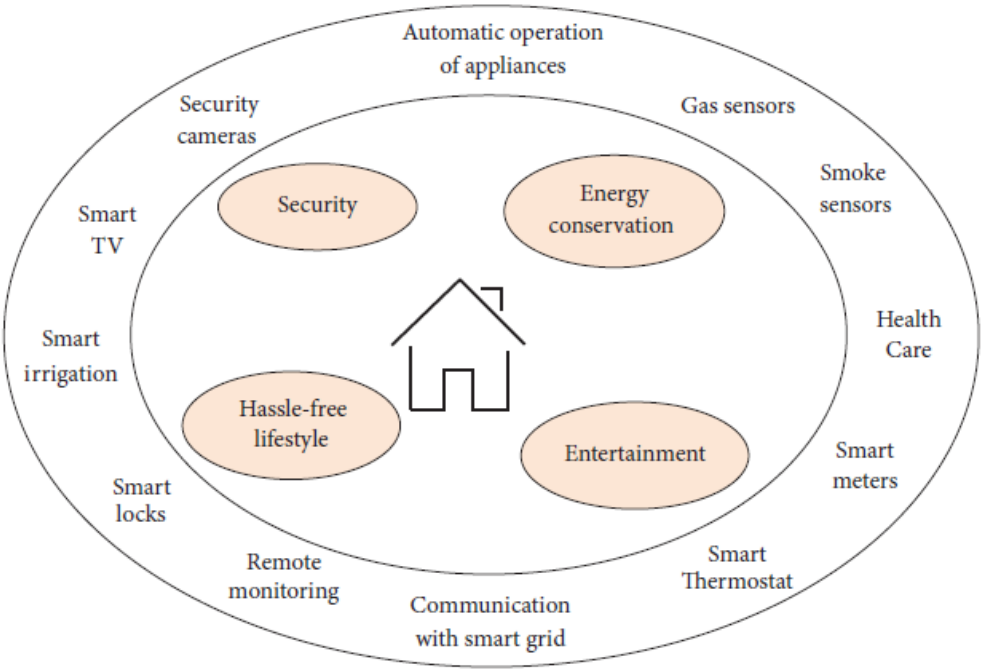

Figure 5: Smart Home block diagram (Source: Journal of Electrical and Computer Engineering, 2017)

4.1.1 Characteristics of IoT devices in Smart Homes

As it was mentioned before IoT is a collection of all kind of devices, which differ in the way they operate, function and communicate. Home automation system is not an exception and may include all kind of varieties of devices connected to it. Devices in such setup are interconnected between each other through the internet, allowing people to maintain and control such functions as access to the home, temperature in the whole house, lighting, as well as many other functions remotely.

Figure 5 shows various devices in different fields of application in Smart Home systems. Those include smart locks, smart bulbs, gas sensors, thermostats, refrigerators, smart TVs and many others.

4.2 Wireless Smart Home protocols

(i) KNX-RF

KNX was developed in 1991 [21] and is one of the most popular protocols for implementing automation, as well as in the HVAC: Heating, Ventilation and Air Conditioning. There are various compatible devices available for the purchase, and as a matter of fact KNX was accepted as an open standard in 2006. KNX is based on standard OSI model and covers following layers in it: data link, network, and transport.

Following chosen research criteria, this work will be focusing on KNX- RF (Radio-Frequency), however this protocol is not limited only to this communication medium, but other transmission ways, e.g. wired: twisted pair, ethernet and power line.

Band for the wireless transmission is at 868 MHz and 2.4 GHz and maximum range can reach up to 150 meters. Data rate transmission at maximum can reach up to 16.385 kbps. The nodes can be connected through three topologies, which are star, line and tree. KNX is a peer-to-peer system and can address up to 65k devices, which, in their turn can communicate between each other with no master device.

Specification	KNX-RF Value
Transmission Band	868 MHz
Frequency Band	2.4 GHz
Range	< 150 m
Data Rate	< 16.385 kbps
Number of Nodes	< 65000
Network Topology	Star, Line, Tree

Table 2: KNX-RF specifications

(ii) EnOcean

Though patented in 2001, it became an international standard in 2012 (ISO / IEC 14543-3-10). The key feature is the wireless power supply that allows devices to operate independently of a battery, since they derive their energy from the wireless signal. The standard EnOcean covers the three lowest layers: physical, data, network of the OSI model.

The EnOcean alliance offers the EnOcean Equipment Profiles (EEP) layer located in the application layer to achieve interoperability with this standard between various types of products and suppliers, to ensure better integration. It uses the transmitting frequency of the ISM bands; 868 MHz, 315 MHz, and 2.4 GHz via Easyfit5 as of May 2017.

EnOcean is using a mesh topology where all nodes interact among themselves. The signal range in free field is up to 300 meters and inside a building is 30 meters; the highest data rate is 125 kpbs.

Specification	EnOcean Value
Transmission Band	868 MHz, 315 MHz
Frequency Band	2.4 GHz
Range	30 - 300 m
Data Rate	< 125 kbps
Network Topology	Mesh

Table 3: EnOcean Specifications

(iii) Zigbee

The ZigBee Alliance developed ZigBee protocol, which was first adopted in 2014. The IEEE 802.15.4 standard is a base of ZigBee protocol; [27] ZigBee can be defined as a specification of series of high-level communication protocols commonly used for personal area networks, e.g. smart homes. It is indeed low-power and low-cost technology, which was designed to be less costly and simpler than other WPANs, such as Wi-Fi or Bluetooth.

It's also a standard to suite high-level low-cost communication protocols, which enables to build PANs with low-power and longer distances from small size.

In a perfect setting, ZigBee can have line-of-sight transmission range equal to 100 meters, 915 MHz frequency and 40-250 kbps data rate. Zigbee supports three topologies, which include tree, star and mesh, allowing a maximum of 65k nodes. The IEEE 802.15.4 standard is used as a data link and physical layer.

Specification	ZigBee Value
Transmission Band	915 MHz
Frequency Band	2.4 GHz
Range	10-100 m
Number of nodes	< 65000
Data Rate	40-250 kbps
Network Topology	Star, Tree, Mesh

Table 4: ZigBee specifications

(iv) Z-Wave

Z-Wave was developed in 2001 and focuses primarily on lightweight wireless and low-latency transmission of data. [26] The protocol's newest upgrade, called Z-Wave Plus, was launched in 2013 and introduces some enhancements, such as enhanced battery life and wireless range. Unlike EnOcean or ZigBee, Z-Wave is not a standard and its advancement is regulated by the Z-Wave Alliance7 which includes more than 600 companies, as well as major IoT players like Siemens and Huawei. Z-Wave utilizes a mesh network with the number of linked devices in a network restricted to 232 nodes. Z-Wave uses four lower layers of OSI models, physical, data link, network and transport.

It can operate on a common industrial frequency of 828 MHz (EU markets) and 908 MHz as part of ISM bands with a 30 meters maximum range. At last, the maximum data rate provided is 100 kbps.

Specification	Z-Wave Value
Transmission Band	828, 908 MHz
Frequency Band	2.4 GHz
Range	< 30 m
Number of nodes	232
Data Rate	< 100 kbps
Network Topology	Mesh

Table 5: Z-Wave specifications

(v) Thread

Thread is a protocol specifically developed for wireless device-to-device communication. It can be used together with low-power devices on small and large networks. One of the most powerful advantages of the stack is that there is no single point of failure. If a slave device depends on a master device that is not available, the child will be able to choose another master device independently. That's possible since it utilizes a mesh network topology together with 6LoWPAN, where each node can act as a master node and there is no limit to connected nodes due to the use of IPv6.

6LowWPAN is also being used in version 4.2 of Bluetooth Low Energy (BLE) via the Internet Protocol Support Profile, which allows Bluetooth Smart sensors to access the Internet directly through 6LoWPAN connectivity. The Thread Protocol implementation is specified in layers 3 and 4 of the OSI layer model and uses the IEEE 802.15.4 standard in layers 1 and 2, which allows a data rate of 250 kbps.

Specification	Thread Value
Transmission Band	828, 908 MHz
Frequency Band	2.4 GHz
Range	20-30 m
Number of nodes	250
Data Rate	250 kbps
Network Topology	Mesh

Table 6: Thread specifications

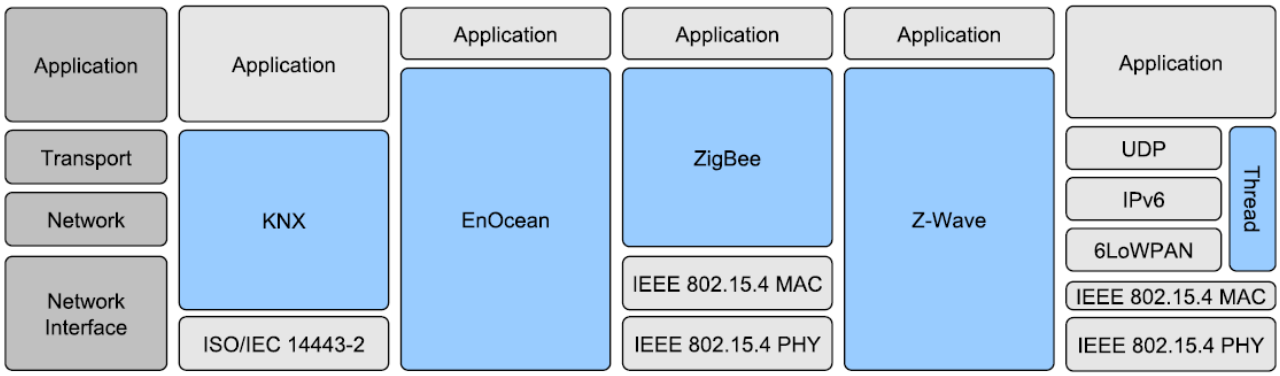

Figure 6: Stack of KNX, EnOcean, ZigBee, Z-Wave, Thread as per TCP/IP Model (Source: An Overview of Wireless IoT Protocol Security in the Smart Home Domain, 2017)[19]

4.3 Security in protocols

Security is the level of risk protection, intrusion defence and interference whether unintentional or malicious, that can compromise privacy and security. In IoT protection is indistinguishable from safety.

This section will include an analysis of the security mechanisms and measures taken by chosen protocols from the section above. In regard to such security issues as authenticity, confidentiality, integrity and replay protection, this section will cover cryptography methods taken by each of protocols.

What are the key security features in security of the protocol?
As it is been discussed in the theoretical part of the thesis, following security elements are important to consider, when implementing security in protocols:

- **Confidentiality** means that data in packets can't be decrypted without a known key and only designated node will be able to access it.
- **Authenticity** and **Data Integrity** mean that the data has not been tampered with.
- **Data Freshness** means that message was sent recently.

4.3.1 KNX-RF security

For quite a long time, the KNX had failed to develop security measures and mechanisms for the protocol. Nonetheless, KNX has introduced the KNX Data Secure for partly encryption, and KNX IP Secure for entire encryption (but only upon KNX IP medium).

As of updated information on KNX security from KNX Association (2020), KNX Secure can be activated or deactivated (on application level). In the KNX Data Secure, pre-shared secret is used for key exchange: secure devices have a Tool Key and unique FDSK, or Factory Device Setup Key (can't be modified or deleted), which is the pre-shared key. For replay protection, timestamps (consecutive sequential number) are given to packets, as well as authentication code (HMAC). To ensure the authentication and integrity AES 128 CBC MAC is used, whereas AES 128 CTR is used for encryption. [25]

Even though, the technology was in use for quite some time, there is no available detailed security analysis of the KNX-RF Security.

	Authentication/ Data Integrity Algorithm	Encryption Algorithm	Replay Protection	Key Exchange
KNX-RF	AES-128 CBC-MAC	AES-128 CTR	Timestamp	PSK

Table 7: Summary of KNX-RF security mechanisms

4.3.2 EnOcean security

EnOcean protocol offers protection towards authentication, integrity checks, encryption and replay. The protocol uses VAES (Variable AES) to secure telegram (packet) content. It is the combination of the 128-bit AES algorithm with RLC – rolling code, which varies generated encrypted code.

The CMAC algorithm is being used for message authentication and integrity checking. In the scenario, where RLC counter checking has been bypassed, to prevent replay

attacks, Nonce is used as a challenge in challenge and response authentication, which in its turn is only valid for limited amount of time.

Consequently, it is suggested to use a Nonce-starting RLC for replay protection inside the packet, VAES for encryption and CMAC for authentication and integrity checking when using EnOcean. All of this security information (such as encryption method, key, RLC) are shared in a teach-in mode. In the newest update of the System Specification (Security of EnOcean Radio Networks V2.5, 2019), it was stated that this kind of exchange of secure information over the radio interface might be omitted. [28]

	Authentication/Data Integrity Algorithm	Encryption Algorithm	Replay Protection	Key Exchange
EnOcean	AES-128 CMAC with counter	VAES-128	Counter	PSK

Table 8: Summary of EnOcean security mechanisms

4.3.3 ZigBee security

As it was mentioned before, Zigbee is based on IEEE 802.15.4 and is therefore exposed to security concerns relevant to that protocol, however this is not going to be discussed in this work.

ZigBee maintains two different security levels, which are Commercial security for a higher security measures and Residential Security for a standard protection. They mainly distinguish in the way they distribute and maintain keys.[10]

ZigBee security is based on AES 128-bit algorithm, which offers security services, such as key establishment, transport, frame protection. There are a few built-in provided security services, which maintain secure transmission between nodes. For instance, ZigBee implements AES with CCM - Cryptographic block Ciphers Mode encryption (CTR + CBC-MAC). [27] This ensures authentication and confidentiality during data transmission. However, the process is simplified as the same key is reused on each level of ZigBee Architectural Stack. CCM is only suitable for 128-bit

cryptographic cipher blocks. ZigBee supports a modified CCM version also known as CCM *; CCM* requires either authentication or encryption, whereas both are required in the standard version of CCM.

To ensure data integrity, ZigBee uses MIC – message integrity check, which can also check that the data came from a proper node with cryptographic key.
In order to ensure replay protection a sequential freshness counter is used. Counter, therefore, will reset anytime a new frame is sent or received.

Authentication in ZigBee is maintained on the network (NWK) and application (APS) layers with help of network and link keys.

One of the ZigBee's important built-in security features is the trust center. This handles new devices that are incorporated into the network, and also periodically updates the shared network key. The coordinator node is typically the trust center and therefore should be known by all other network nodes. Trust center functions can be summed as follows: distribution of authenticity shared keys to new devices and allowing end-to-end protection between nodes.

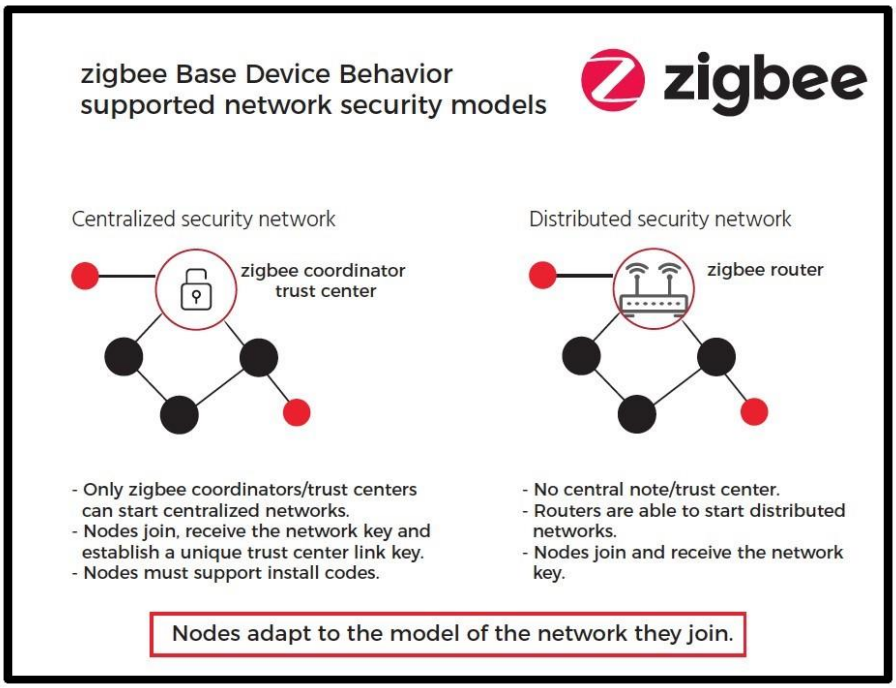

Figure 7 : ZigBee security models (Source: https://research.kudelskisecurity.com/2017/11/08/zigbee-security-basics-part-2/)

Zigbee can run in a centralized or distributed way. The first uses a trust center to control security (in particular, to authorize new devices and manage key distributions, as it was mentioned before).

In distributed networks, nodes form a mesh topology, where each router may operate as a parent to the new devices, while there is no extra authorization needed if the network key was pre-distributed in some form. Moreover, the application link keys used to secure the application layer data are not set in the Zigbee, conveying that task to a higher-level protocol. This lack of specification leaves room for insecurity. [19]

	Authentication/Data Integrity Algorithm	Encryption Algorithm	Replay Protection	Key Exchange
ZigBee	AES-128 CCM*	AES-128 CCM*	Counter	PSK

Table 9: Summary of ZigBee security mechanisms

4.3.4 Z-Wave security

Z-Wave protocol ensures authentication, confidentiality and replay protection by using so called Security Layer in its Security Command Classes.
There are two classes that ZigBee implements: first is Security 0 for lightweight (S0) and Security 2 for strong (S2), which in its turn has more subclasses: S2 Authenticated, S2 Unauthenticated and S2 Access control. All of the above-mentioned use AES-128 encryption algorithm. [19]

As a key exchange mechanism, Z-Wave S2 uses Elliptic Curve Diffie Hellman (ECDH) and has to support Curve25519, with help of which a public key can be calculated from private key with the length of 256 bits. Every S2 node is having an ECDH key pair, which is used to create secure channel for the further Network Key exchange.

In S0, all secure nodes throughout the network are using the same Network Key. Network key distribution utilizes a temporary key to secure the key exchange.

Network key exchange occurs immediately after new node inclusion. This isn't the same in S2, in which each subclass does have its own network to avoid compromising those of a higher-security class with a compromised low-security class system. Practically, the S2 access control and S2 authentication can be considered equivalent, whereas S2 unauthenticated lacks the ability to authenticate the client.

Authentication and Encryption in S2 are supported by AES-128 encryption algorithm in CCM mode, while AES-128-CMAC and Pre-Agreed Nonces (PAN) with next-nonce derivation functions are used to verify integrity and replay protection.

Overall, the protocol itself has no established security flaws. On the other hand, there are reports of positive examples of attacks against individual implementations. For instance, a most know case of how door lock was compromised, because of lack of validation check on an important status. [29]

	Authentication/Integrity Algorithm	Encryption Algorithm	Replay Protection	Key Exchange
Z-Wave	AES-128 CMAC, AES-128 CCM	AES-128 CCM	Nonce-based	ECDH Curve25519

Table 10: Summary of Z-Wave security mechanisms

4.3.5 Thread security

Same as Zigbee (4.4.3), Thread uses a network-wide key for security at network- level [30]. Network-wide key is used to encrypt the MAC data frames in the MAC (Media Access Control) layer. This is a basic type of security used to avoid casual eavesdropping and targeted interruption of the Thread Network from outside. Since it is a network-wide key, any compromised Thread Device may potentially expose the key; thus, it is not usually used as the only form of security inside the Thread Network. The possession of the network key is used to distinguish between an authenticated and authorized device and the connecting device, when talking about joining of new devices into a network. The network-wide key is transmitted safely to a joining device along with other network variables, using a KEK (Key

Encryption Key) to secure it. That way, on a wireless connection, the network key is never revealed in the open.
To provide further security Transport Layer Security (TLS) and Datagram Transport Layer Security (RFC6347) are used to cover the vulnerability with a network-wide key. However, combined security might have an effect on overall performance and can be hard to implement with constrained embedded devices. [19]

In order to secure packets, AES-128 CCM is used and key is exchanged via a J-PAKE – a juggling Password-Authenticated Key Exchange, which is based on the so-called EC-JPAKE - P-256 elliptic curve Diffie-Hellman key exchange. As all devices know this key, the protocol further recommends security on the application layer.

	Authentication/Integrity Algorithm	Encryption Algorithm	Replay Protection	Key Exchange
Thread	AES-128 CCM	AES-128 CCM	Counter	mod. ECDH P-256

Table 11: Summary of Thread security mechanisms

4.4 Vulnerabilities

In this section let us look at existing and possible vulnerabilities that reviewed protocols have. Smart Homes often use constrained devices with a very limited memory, communication capabilities and energy usage. This all makes it harder to come up with a security measures, which will suite all devices. Thus, for instance such measures as Public Key Cryptography or TLS based security might be challenging for such cases.

To highlight common vulnerabilities that chosen technologies might face are key attacks - which is for instance, an attempt to retrieve an encryption key of the encryption flow, replay attacks – e.g. network attack in which data is replicated illegitimately or being delayed, unauthorized transmission, unauthorized interception of any data flow between devices.[32]

As it could be seen from the previous section, all of the protocols use AES 128 bit standard for the authentication, integrity checks and general encryption. They differ in supported modes; From the security point of view, AES encryption algorithm is considered to be secure and stable, considering the restriction of constrained devices and limitation on computational power in Smart Home / IoT environments. As per study [13], the AES has proven to be generally secure against the attacks. Experts at AES Protection claim that AES is safe when properly implemented. However, you always need to secure AES encryption keys [11].

KNX-RF is relatively new technology and as it was said, the security mechanisms for the protocol were missing for quite a long time. Since KNX Data Secure was introduced, there were no conducted analysis of security vulnerabilities published.

As it was mentioned, EnOcean protocol is using teach-in mode to transmit encryption method, RLC and key. To establish mode, pre-shared key is advised to use, because otherwise exchange of such secure information will take place unencrypted [19]. However, it was suggested that this method of exchange can be omitted [28].

As per ZigBee, a study [27] highlighted threats and possible vulnerabilities to the ZigBee protocol. Those included physical attacks, interception attacks and others. Even though, it is one of the leading technologies available, the limitations in the protocol, such as limited number of nodes, memory and energy doesn't allow it to use higher security measures. Restrictions as such can grow into security implications or failures [10].

Z-Wave hasn't been explored a lot; however it has a very advanced security measures used to secure data transmissions. Z-Wave, as well as Thread establish key exchange based on the ECDH or Elliptic Curve Diffie–Hellman Key Exchange, which is an anonymous key agreement scheme which enables two sides to establish a shared secret via an insecure channel, each having an elliptic-curve public–private key pair. The main benefits about using cryptographic algorithms based on elliptic curves instead of cryptographic algorithms based on finite fields include a smaller key size for security equivalence and will perform better [33]. From the other hand, threats towards Z-

Wave include for instance, Black Hole attack, when router discards packets instead of passing them [32]. There was a known case of successful attack on Z-Wave implementation, such as when door locks were compromised because of lack of important validation [34].

Thread technology utilizes network-wide key, which doesn’t provide optimal protection [30], because it is known to all network devices. Thus, additional security is required, which in case of Thread is TLS, but the problem is that constrained devices might not have capabilities to haft this security combination. As Thread Group states the technology is secure and there is no known vulnerability to make use of. [30]

Results and Discussion

As a result of the research on the security mechanisms in most popular communication protocols used in Smart Home domains, which are KNX-RF, EnOcean, ZigBee, Z-Wave and Thread, following table 12 summarizes measures taken by each.

	Authentication/Data Integrity Algorithm	**Encryption Algorithm**	**Replay Protection**	**Key Exchange**
KNX-RF	AES-128 CBC-MAC	AES-128 CTR	Timestamp	PSK
EnOcean	AES-128 CMAC with counter	VAES-128	Counter	PSK
ZigBee	AES-128 CCM	AES-128 CCM	Counter	PSK
Z-Wave	AES-128 CMAC, AES-128 CCM	AES-128 CCM	Nonce-Based	ECDH Curve25519
Thread	AES-128 CCM	AES-128 CCM	Counter	mod. ECDH P-256

Table 12: Overview of security features in chosen protocols

From 5 chosen technologies, all use the Advanced Encryption Standard (AES) with 128-bit in different modes for encryption and/or authentication and integrity check, as can be seen in the table 12. ZigBee, Z-Wave and thread support CCM mode, while KNX-RF and EnOcean implement CBC-MAC and CMAC variant.

For a secure key exchange Z-Wave and Thread are implementing ECDH - elliptic curve Diffie-Hellman, on different curves, while others rely on pre shared key, which is less secure and less practical. As for replay protection many adopt Counter, whereas Z-Wave is implementing Nonce-Based counter and KNX-RF timestamps.

Summarizing collected information, it can be seen that all the protocols provide security to some extent in terms of confidentiality, authenticity, data integrity and freshness, which were set as a security goal. Chosen protocols differ in the way they are implemented, architectures, number of nodes supported and etc.; All of them are utilizing different security mechanisms to provide protection as to their own capabilities / features. However, as to decide which protocol provides the most effective security based on what was found, it can be summarized that as a combination of all the security mechanisms together, Z-Wave offers strong security. It offers high protection through different levels: S0 and S2 and its sub-classes. By usage of nonce-based counter it ensures replay protection and ECDH for a secure key exchange.

Regarding vulnerabilities in smart home protocols, as it was seen, all are vulnerable to threats of different kind. Several security issues were defined for the Smart Homes based on the used sources, and due to restricted nature of the smart devices it is harder to implement advanced security solutions.

Future Insight

IoT and security go along together. If the security is not provided, private data of one can be misused or revealed. Thus, it is essential to keep IoT safe. After analyzing security mechanisms of common wireless protocols in the Smart Home domain, it can be said that all of them have room for growth. The current state of technology is still very vulnerable and that's why has to go through a long way of improvement.

Security is not standing on one place; it is always in the process of development and advancement. There are many new technologies emerging the world, and soon limitation of constrained devices will not be a problem in order to have a secure communication between devices.

However, as for now, following recommendations can be used to maintain IoT environment secure, following recommendation can be used:

- First is incorporating safety during the construction/implementation process.

Protection should be evaluated as an integral part of any networked system. It is still very often that protection is ignored when the company releases products or when the system is implemented.

- Advance software maintenance and vulnerability management

The protection can be high even in the design process by patching, software fixes and vulnerability managing strategies. It includes, e.g., replacing the default password and scheduling the updates, updating firmware.

- Prioritizing security measures with regard to their implications

It is important to know where particular security measures will be implemented in the network, by focusing on the results of disturbances or malicious activity.

- Connect thoughtfully and stay always aware

Smart Home users should follow guidelines on how to use IoT and keep it safe, they should always advice on what has to be done from their side in order to protect the network.

Conclusion

As it could be seen from the literature review and practical part, security is an essential element of every and each smart environment. Smart Homes rely on security even more, because they deal with a very private information coming from our personal lives. IoT devices are becoming inevitable part of our lives and, thus, have to be protected.

Cryptographic measures are the answer to achieving most of the security targets, such as confidentiality, integrity, authentication and non-reputability. Cryptographic algorithms are used for the safe data storage and secure transmission. This thesis identified the wireless Smart Home protocols generally and more precisely from a security standpoint for smart home systems. From the chosen five protocols (Zigbee, EnOcean, Z-Wave, KNX-RF and Thread), all have specified security services, and all provide security to some extent. In addition to that, vulnerabilities in the following protocols were underlined and discussed.

As it was discovered, the general state of the Smart Home is still vulnerable from security standpoint of the analyzed protocols. When deciding a communication technology for an IoT, it is important to understand what is used in network devices, what is required and what you want from the network. Communication technology features are distinct, and therefore they can be good choices for different environments.

References

[1] FOOTE, Keith D. A Brief History of the Internet of Things. DATAVERSITY [online]. 6 August 2016. [Accessed 23 December 2019]. Available from: https://www.dataversity.net/brief-history-internet-things/

[2] HASSAN, Qusay F., KHAN, Atta ur Rehman and MADANI, Sajjad A. Internet of Things: challenges, advances, and applications. Boca Raton: Taylor & Francis Group, CRC Press, 2018.

[3] The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020. ABI Research: for visionaries [online]. [Accessed 23 January 2019]. Available from: http://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/

[4] CARUGI. ITU-T SG20 Work Progress on IoT and Smart Sustainable Cities and Communities. ITU [online]. [Accessed 1 December 2019]. Available from: www.itu.int/en/ITU-T/Workshops-and-Seminars/201707/Documents/003-Marco-Carugi-ITU-T SG20 work progress on IoT and Smart Sustainable Cities and Communities.pdf.

[5] Internet of Things (IoT) Preliminary Report 2014. ISO [online]. 2014 [Accessed 1 January 2020]. Available from: www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf.

[6] EU Agenda Team. Identifiers in Internet of Things 2 (IoT). EU Agenda [online]. February 2018 [Accessed 1 January 2020]. Available from: https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf

[7] Architectural Considerations in Smart Object Networking. IETF Tools [online]. March 2015. [Accessed 23 March 2019]. Available from: https://tools.ietf.org/html/rfc7452

[8] SETHI, Pallavi and SARANGI, Smruti R. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*. 2017. Vol. 2017. DOI 10.1155/2017/9324035.

[9] AL-SARAWI, Shadi, ANBAR, Mohammed, ALIEYAN, Kamal and ALZUBAIDI, Mahmood. Internet of Things (IoT) communication protocols: Review. *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*. 2017. No. October, p. 685–690. DOI 10.1109/ICITECH.2017.8079928.

[10] RAZOUK, Wissam. Zigbee Security within the Framework of IoT. In : . 2014.

[11] ROUSE, Margaret. What is AES Encryption and How Does it Work? SearchSecurity [online]. 20 February 2020. [Accessed 20 March 2019]. Available from: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[12] XU, Jiaming, FAN, Ao, LU, Minyi and SHAN, Weiwei. Differential Power Analysis of 8-Bit Datapath AES for IoT Applications. In: *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*. 2018. ISBN 9781538643877.

[13] Secure MQTT using AES for Smart Homes in IoT Network. International Journal of Innovative Technology and Exploring Engineering (IJITEE) [online]. 2019. [Accessed 13 December 2019]. Available from: https://www.ijitee.org/wp-content/uploads/papers/v8i5s/ES3468018319.pdf

[14] ORACEVIC, Alma, DILEK, Selma and OZDEMIR, Suat. Security in internet of things: A survey. *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*. 2017. No. May. DOI 10.1109/ISNCC.2017.8072001.

[15] AZIZ, Tariq and HAQ, Ehsan-ul. Security Challenges Facing IoT Layers and its Protective Measures. *International Journal of Computer Applications*. 2018. Vol. 179, no. 27, p. 31–35. DOI 10.5120/ijca2018916607.

[16] LOPEZ, Nicole Angelyn T, PASAOA, John Ryan B, PARADO, Justin A. and MORALES, Joshua O. A Comparative Study of Thread Against ZigBee, Z-Wave, Bluetooth, and Wi-Fi as a Home-Automation Networking Protocol. . 2016. No. November. DOI 10.13140/RG.2.2.36693.22249.

[17] WITHANAGE, Chathura, ASHOK, Rahul, YUEN, Chau and OTTO, Kevin. A comparison of the popular home automation technologies. In: *2014 IEEE Innovative Smart Grid Technologies - Asia, ISGT ASIA 2014*. 2014. ISBN 9781479913008.

[18] JONAS, Karl, VOGL, Bastian and RADEMACHER, Michael. Security Mechanisms of wireless Building Automation Systems. *Tech. Rep. / Hochschule Bonn-Rhein-Sieg - Univ. Appl. Sci. Dep. Comput. Sci.* [online]. 2017. No. March. DOI 10.18418/978-3-96043-044-5.

[19] MARKSTEINER, Stefan, JIMENEZ, Victor Juan Exposito, VALIANT, Heribert and ZEINER, Herwig. An overview of wireless IoT protocol security in the smart home domain. *Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks*. 2017. Vol. 2018-Janua, p. 1–8. DOI 10.1109/CTTE.2017.8260940.

[20] CYRIL JOSE, Arun and MALEKIAN, Reza. Smart Home Automation Security: A Literature Review. *The Smart Computing Review*. 2015. Vol. 5, no. 4, p. 269–285. DOI 10.6029/smartcr.2015.04.004.

[21] KNX RF KNX Association [Official website] [online]. [Accessed 23 March 2019]. Available from: https://www.knx.org/knx-en/for-manufacturers/development/radio-frequency/index.php

[22] Smart Home: Threats and Countermeasures. Rambus [online]. [Accessed 1 March 2020]. Available from: https://www.rambus.com/iot/smart-home/

[23] ASOKAN, Akshaya and ROSS, Ron. Massive Botnet Attack Used More Than 400,000 IoT Devices. Bank Information Security [online]. [Accessed 1 March 2020]. Available from: https://www.bankinfosecurity.com/massive-botnet-attack-used-more-than-400000-iot-devices-a-12841

[24] FERNANDES, Earlence, JUNG, Jaeyeon and PRAKASH, Atul. Security Analysis of Emerging Smart Home Applications. In: *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*. 2016. ISBN 9781509008247

[25] LOURDAS, Vassilios. KNX Data Secure. KNX Association [online]. [Accessed 23 March 2020]. Available from: https://support.knx.org/hc/en-us/articles/360012689639

[26] Safer, Smarter Homes Start with Z-Wave. Z [online]. [Accessed 23 January 2020]. Available from: https://www.z-wave.com/

[27] KHANJI, Salam, IQBAL, Farkhund and HUNG, Patrick. ZigBee Security Vulnerabilities: Exploration and Evaluating. *2019 10th International Conference on Information and Communication Systems, ICICS 2019*. 2019. No. July, p. 52–57. DOI 10.1109/IACS.2019.8809115.

[28] aSecurity of EnOcean Radio Networks V2.5 [online]. EnOcean Alliance, [no date]. Available from: https://www.enocean-alliance.org/wp-content/uploads/2019/04/Security-of-EnOcean-Radio-Networks-v2_5.pdf

[29] GUPTA, Pamela. Mitigating Risks From A to Z-Wave. Security Industry Association [online]. 30 September 2019. [Accessed 3 March 2019]. Available from: https://www.securityindustry.org/2019/04/23/mitigating-risks-from-a-to-z-wave/

[30] GROUP, Thread. Thread in Commercial White Paper [online] 2018. [Accessed 13 February 2020]. Available from: https://www.threadgroup.org/Portals/0/documents/support/ThreadInCommercialWhitePaper_2542_1.pdf

[31] House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide. *SEC Consult* [online]. [Accessed 24 2019]. Available from: https://sec-consult.com/en/blog/2015/11/house-of-keys-industry-wide-https/

[32] RAY, Abhay Kumar and BAGWARI, Ashish. Study of smart home communication protocol's and security & privacy aspects. In: *Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017*. 2018. ISBN 9781538618608.

[33] GEMALTO. Benefits of Elliptic Curve Cryptography. [online]. 2012. No. March. Available from: http://www.securitydocumentworld.com/creo_files/upload/client_files/gov_wp_ecc1.pdf

[34] AL-SARAWI, Shadi, ANBAR, Mohammed, ALIEYAN, Kamal and ALZUBAIDI, Mahmood. Internet of Things (IoT) communication protocols: Review. *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*. 2017. No. October, p. 685–690. DOI 10.1109/ICITECH.2017.8079928.