Master Thesis

Master's Programme in Network Forensics, 60 credits

Security Challenges of Communication Protocols in IoT

Comparing security features of ZigBee and Z-Wave communication protocols in IoT devices

Thesis in Digital Forensics, 15 credits

Halmstad, Sweden 2019-05-29

Hamed Shahidi

HALMSTAD UNIVERSITY

HALMSTAD UNIVERSITY

Information Technology Department

Security Challenges of Communication Protocols in IoT

Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Network Forensics

Supervisor:

Wojciech Mostowski, PhD

By:

Hamed Shahidi

May 2019

Acknowledgements

I should express my special thanks and gratitude to my supervisor, Wojciech Mostowski, who kindly helped me to prepare the present thesis.

I would also like to express my deep gratitude to the examiner, Stefan Axelsson, for his kind helps and very precise points he mentioned.

Abstract

This research studies the security challenges in IoT devices. At first, security challenges have been described and then specifically the security of communication protocols in the IoT has been addressed. Finally, among different communication protocols, ZigBee and Z-Wave protocols have been chosen for this study. The criterion for choosing these two protocols is the level of security they provide for IoT devices to protect them against unauthorized access and hacking. Security, frequency, power consumption and data rate are the characteristics that have been discussed in the review of these two protocols. In the end, a comparison of the various features of these two protocols clarified that the security of IoT devices in each of these protocols depends on the type of the IoT device, the required range and other requirements, however, in most cases the ZigBee protocol showed more security than Z-Wave.

Key Terms: Internet of Things, IoT, Security, Communication Protocols, ZigBee, Z-Wave, Protocol Analysis

Table of Contents

Title **Page**

Chapter One: Introduction

Chapter Two: Review of the Related Literature

Chapter Three: Design and Method

Chapter Four: Data Analysis and Discussion

Chapter Five: Conclusions and Implications

List of Tables

Table **Page**

List of Abbreviations

APL:	Application Layer
BLE:	Bluetooth Low Energy
CCTV:	Closed Circuit TV
ZDO:	ZigBee Device Object
DSK:	Device-Specific Key
ECDH:	Elliptic-Curve Diffie-Hellman
IoT:	Internet of Things
MAC:	Medium Access Control
NWK:	Network Layer
OOB:	Out-of-Band
PAN:	Personal Area Network
PHY:	Physical Layer
QR code:	Quick Response code
UI:	User Interface

Chapter One

Introduction

Chapter I

Introduction

This chapter introduces Internet of Thing (IoT) and the communication protocols in IoT devices, and then it briefly reviews the concept of security in communication protocols. After that the research question of the study will be introduced and finally the significance of the study will be presented.

1.1 Overview

The concept of Internet that we have in mind is a global network in which personal computers, cell phones, etc. are connected, and humans are communicating with each other using these connected devices everywhere. Now consider a world in which the Internet goes beyond its current concept and includes the objects/things around us. The Internet of Things is an emerging technology in which each “Thing” can send and receive data through various communication networks. Specifically, a “Thing” in IoT has the ability to collect data, control, or communicate remotely. A smart lock connected to your mobile phone, CCTV cameras which can be controlled remotely or a sprinkle in your garden that can be programmed are all examples of IoT devices. This technology will have a great impact on various aspects of human life and, therefore, it is necessary to select appropriate protocols and technologies for communication between different Things.

It can be said that the Internet of Things is a network of networks in which a large number of things, sensors and devices are connected through the communication and information infrastructure to provide value-added services through intelligent data processing and management for various applications (Parkodi, 2014).

Along with the tremendous benefits of the Internet of Things, this technology faces some challenges. One of the main challenges of the IoT is the security of these devices. Unauthorized access, data hijacking, data manipulation, network penetration, eavesdropping, etc. are among the IoT security challenges. Therefore, new standards and protocols are always required to solve sustainability, reliability, service quality, confidentiality and integrity. Smart home and smart cities are also in need of these updates.

In order to achieve this goal, it is very important to examine the protocols and standards of IoT. Actually, by using these surveys, we can provide better protocols and standards to address the challenges and limitations that currently exist.

Several communication protocols such as 802.11ah, Bluetooth Low Energy (BLE), DASH7, ZigBee, Z-Wave, LoRaWAN, SoAP, WirelessHART, etc. are available for connecting IoT devices. Among all of these communication protocols ZigBee and Z-Wave are the most commonly used protocols for connecting devices in Internet of Things. They are wireless radio frequency communication protocols designed for controlling, monitoring, and status-reading of connected devices

(Z-Wave and ZigBee, 2018). In this research, the introduction, examination and security of these protocols have been discussed.

1.2. Statement of the Problem

It is very important that IoT devices have adequate security. At the moment, given the fact that manufacturers are rushing to introduce new smart devices to the market, so the security of these devices is usually not the first priority for them. Consumers and businesses are often unaware of how their devices' security affects their lives or business. This will increase the risk of data breach or hacking these devices.

This research aims to investigate the security of ZigBee and Z-Wave protocols in communication between IoT devices.

1.3. Purpose of the Study

The main purpose of this study is to recognize challenges of using IoT smart devices and focusing on security challenges of using ZigBee and Z-Wave communication protocols in IoT devices.

1.4. Significance of the Study

Nowadays IoT is a fast growing new industry and almost all experts believe that in the coming years IoT will be used in many different aspects. However, this phenomenon, like many other IT-related phenomena, faces different challenges. Some studies have shown that the Internet of Things faces major challenges, which we briefly discuss in this study (IoT challenges, 2016). In Section 2.3, we will have a closer look at these challenges.

In this study different challenges of IoT will be discussed and then it will focus on the major and most important challenge of IoT which is IoT security. IoT security is very important because without an appropriate level of security nobody will trust using these devices.

The results of this study may be useful for IoT companies that produce IoT devices for the industry or home use. It may also be useful for students to get new ideas to study further.

1.5. Research Question

According to what was stated above, the research question of this study can be posed as:

Which of ZigBee and Z-Wave communication protocols is more secure to be used in IoT devices?

1.6. Definition of Key Terms

The following key terms are used in this study:

Internet of Things (IoT):

The Internet of Things (IoT) is a system of interrelated and connected devices, machines, things or people, and they are able to exchange data over a network without any human-to-human or human-to-computer interaction (IoT, 2019).

IoT Security:

Security challenges in IoT is applying security intelligence for detecting and solving issues as they occur, and also to predict and proactively protect against potential security threats (IoT security challenges, 2017). IoT security is a very widespread subject and includes many challenges such as data management, privacy, communication protocols, etc.

ZigBee Protocol:

ZigBee is an open global standard for wireless technology that uses low-power digital radio signals for personal area networks. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that require a low data transfer rate, energy efficiency and secure networking (ZigBee, 2019a).

Z-Wave Protocol:

Z-Wave is a wireless network which provides communication between devices in a home control network. Z-Wave can be used to control lights, heating and air conditioning, and appliances and home security, among other functions (Z-Wave, 2019a).

Protocol Analysis:

A detailed study of two or more communication protocols and the characteristics of each of them in terms of security, data rates, speed, frequency, power consumption, etc.

1.7. Limitations of the Study

This study concentrates on security aspects of ZigBee and Z-Wave protocols. There are many other aspects that needed to be studied. So this study, like many other studies, was developed under certain limitations.

The first limitation was lack of available similar devices in which both ZigBee and Z-Wave protocols have been implemented, therefore the researcher just concentrated on the current studies that could implement both protocols.

The second limitation was time limitation for the study which makes it impossible to study all different aspects of the two protocols in IoT devices.

Chapter Two

Review of the Related Literature

Chapter II

Review of the Related Literature

2.1. Overview

This chapter attempts to review the related literature in different parts. The first part discusses the definition of Internet of Things. Then it briefly explains different security challenges of IoT. Afterwards, some communication protocols which are used in IoT are reviewed. Finally this chapter reviews ZigBee and Z-Wave communication protocols. The most focus in these studies are on the security of IoT devices in different parts and different fields of IoT and they try to give a new perspective of new security challenges that IoT industry will face in future.

2.2. The Definition of IoT

It is essential to comprehend the concept and definition of IoT (Internet of Things) as specified by many scholars to obtain a whole picture of IoT devices. Having an easy and understandable definition for IoT that can state all of its features can help researchers and scholars to do more research and can help us to understand IoT concept much better. Some of these definitions are as follows:

Atzori et al. (2010, p. 3) states that one of the preliminary definitions of IoT is a ‘things oriented’ perspective in which the considered things are very simple items like RFID tags.

Minerva et al. (2015, p. 22) defines that IoT can be characterized as a set of things in an interworking network that can be made smart if they can be identified, named and addressed.

IoT is also defined as a “dynamic global network infrastructure with self-configuration and interoperable communication” (Ali et al., 2015, p. 37). It is also stated that the IoT means every device around us are supposed to be connected to the Internet in a way that it can behave intelligently and can pay attention to the existence of the kind of autonomy and privacy (Ali et al., 2015, p. 37).

IoT, Internet of things, is an interrelated network of devices such as mechanical and digital machines, objects, animals or people which can transfer data over a network without any need to human-to-human or human-to-computer interaction (IoT, 2019).

A general and simple definition is that IoT is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data (Internet of things, 2018).

2.3. Security Challenges

2.3.1. Basic Security: One of disputes about IoT devices is that "it is believed that IoT devices are being manufactured rapidly without giving much attention to security challenges and the requisite threats" (Makhdoom et al., 2018). Although security is one of the most important aspects of using IoT smart devices, it has not been paid much attention to.

2.3.2. Privacy: Privacy is another challenge in using IoT devices. By using IoT devices billions of devices across the globe are connected to each other and interact with each other and the privacy issue should be managed somehow. General privacy and security threats like internal and external attacks should also be covered in IoT studies (Makhdoom et al., 2018). And also "a lack of intrinsic security measures makes IoT vulnerable to privacy and security threats" (Panarello et al., 2018).

Schurgot et al., (2015) states that "well-known security and privacy problems have been shown across devices and networks, from pacemakers that can be made to deliver a fatal charge to networked light bulbs that can provide back doors into WiFi networks, to smart TVs that listen to conversations, to refrigerators that are enlisted into denial of service attacks."

According to Gartner (Connected Things, 2014) the number of connected IoT devices in use by 2020 will be nearly 25 billion, and by using such a big number of interconnected IoT devices there would be new types of security and privacy threats and hackers would use security gaps to use these devices for their personal benefits (Farooq, 2015).

Riahi (2013) categorizes privacy in IoT devices in three different aspects: data collection privacy, data sharing and management privacy and data security issues; He believes that more research should be done on each of these aspects to find their vulnerabilities in order to have a more secure network for IoT devices.

2.3.3. Data Management: Managing the huge amount of data produced by IoT devices is also another security challenge for spreading IoT. Recent studies show that many of the current methods of information management are ineffective in cloud computing because these methods are not able to manage and control the massive amounts of information generated by IoT smart devices (Gartner Survey, 2016).

In IoT devices, data management should be as a layer between the devices that generate data and the applications that have access to this data. The data that is provided by IoT devices should be available to the network of IoT devices, depending on the level of privacy desired by the owners; Thus, communication, storage and process are the key factors in the design of data management solutions for IoT devices (Abu-Elkheir, 2013). Besides, data which is collected from all IoT devices in a smart city must be securely protected to decrease the risk of data theft that can make other significant problems such as identity fraud or financial damage (Bohli et al., 2015).

2.3.4. Communication Protocols: Current communication protocols can also be a challenge for IoT devices. Experts believe that there are many barriers to establishing secure connections between IoT device elements and sensors and a Wi-Fi network (WiFi Standards, 2016).

Moreover, there are vulnerabilities in current WiFi technology that can increase the security risk of using WiFi technology in sensitive IoT devices such as those that are used in military places. These vulnerabilities can allow attackers to intercept network traffic and steal data transmitted over a WiFi network (Wi-Fi network vulnerability, 2018). Since billions of devices will connect to each other by IoT devices in near future the current WiFi technology weaknesses must be resolved. In addition, some new characteristics of IoT devices cannot be implemented securely by current security protocols that are used on the Internet because most of these protocols are designed to work with desktop and laptop computers not IoT devices (Al-Fuqaha et al., 2015).

Z-Wave and ZigBee are the different “languages” that IoT smart devices can use to talk with each other. Each of these protocols has weaknesses and strengths that will be referred to in this research, but the main focus in on weaknesses and strengths in terms of security issues of these protocols.

2.4. ZigBee and Z-Wave Communication Protocols

2.4.1. ZigBee Communication Protocol:

ZigBee is a standard for Personal Area Networks and it was developed by the ZigBee Alliance (including companies like Samsung, Philips, Motorola, Texas Instruments and many others) with the aim of providing low-cost, low-power consumption, two-way, reliable, wireless communications standard for short range applications (ZigBee Alliance, 2018). The standard is completely open and gained ratification by the Institute of Electrical and Electronics Engineer (IEEE) in 2003. The protocol stack of ZigBee is based on IEEE 802.15.4. Advantages of choosing ZigBee are the provision of long battery lifetime, the support of a large number of nodes (up-to 65000) in a network, the easy deployment, the low costs and global usage. (Zillner & Strobl, 2015)

The ZigBee stack consists of four layers: (ZigBee Alliance, 2018)

- Physical Layer (PHY)
- Medium Access Control Layer (MAC)
- Network Layer (NWK)
- Application Layer (APL)

The IEEE 802.15.4-2003 standard is used for the two lowest layers, the physical layer (PHY) and the medium access control layer (MAC). The other two layers are defined by the ZigBee Protocol Stack. From a security perspective, the network and the application layer are of highest relevance (Zillner & Strobl, 2015).

The ZigBee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device. Within star networks, the coordinator must be the central node. Both tree and mesh networks allow the use of ZigBee routers to extend communication at the network level. Another defining feature of ZigBee is that it facilities carrying out secure communications, protecting establishment and transport of cryptographic keys, ciphering frames, and controlling device. It builds on the basic security framework defined in IEEE 802.15.4 (ZigBee, 2019b)

ZigBee networks have different uses depending on design, function, and price, but they have become more widely used in some markets, based on market requirements as well as producer interest (ZigBee Alliance, 2018):

- Industry
- Home automation
- Commercial building automation
- Automation of system sales in large retail stores
- Smart houses
- Intelligent lighting control system
- Smart energy
- Telecommunication services
- Health care
- Remote control

2.4.2. Z-Wave Communication Protocol:

Z-Wave is a wireless communications protocol for home automation. This technology is designed to help customers to control and monitor their home automation devices remotely (Z-Wave, 2019b). It is a mesh network using low-energy radio waves to communicate from appliance to appliance, allowing for wireless control of residential appliances and other devices (Smart Home, 2017). Like other protocols and systems aimed at the home and office automation market, a Z-Wave system can be controlled via the Internet from a smart phone, tablet or computer, and locally through a wall-mounted panel with a Z-Wave gateway or central control device serving as both the hub controller and portal to the outside (Z-Wave automation, 2013).

The Z-Wave hub acts as a home network controller and allows wireless devices to communicate. The more modules or sensors are connected to the device, the longer the signal can travel. Z-Wave, like the ZigBee mesh system, can transmit signals sent through the hub (central controller) through internal modules to other modules that are farther away (Z-Wave, 2019b). Z-Wave is user-friendly and provides a simple system that customers can set up. It is the best choice for someone who has a basic knowledge of technology and wants to have a safe, efficient, and easy-controlling home automation system (Z-Wave setup, 2017). Z-Wave works with popular brands and homemade smart devices, so customers should not experience any difficulties in installing the devices.

Z-Wave applications (Z-Wave Applications, 2018):

- Smart hubs
- Smart lighting
- Smart locks
- Smart sensors
- Smart home automation
- Security and alarm
- Voice controlled application
- Water management

2.5. Summary

As it was stated in earlier parts of this study, using IoT devices is very common and is constantly expanding. Although using these devices have many benefits but it has many challenges as well. One of these challenges is the security challenges of using these devices. In this chapter, we listed some of these security challenges in studies from different scholars. Security of IoT communication protocols is one of these challenges.

Chapter Three

Design and Method

Chapter III

Design and Method

3.1. Overview

This chapter describes the design of the present study, papers that were utilized in this study, the procedures and the data collection.

3.2. Design and Method of the Study

This study is a descriptive research; it concentrates on an individual subject and attempts to describe data and features of the subject being studied. Besides, this study employs description to categorize the data into different arrangements in order to analyze them.

ZigBee and Z-Wave protocols are commonly used in IoT devices to connect these devices together. This study tries to find out which of them are more secure in order to be used in IoT devices. The researcher gathered over 30 articles and books focusing on the security features of IoT devices, and tried to compare different aspects of these protocols in order to understand which of them has the most potential capability to save user’s security and privacy.

3.3. Procedures and Data Collection

At first a literature study had been done in order to choose which communication protocols should be selected. The Google Scholar was used to find articles and books about different communication protocols which are used in IoT devices. After studying many of them and focusing on the level of security and privacy they provide, ZigBee and Z-Wave protocols were selected to be studied in more details as they are considered to be the most commonly used protocols in IoT devices (Al-Sarawi et al., 2017). Focusing on security was one of the most important criteria for choosing these two protocols. After the protocols were selected the researcher tried to collect articles and books that scrutinized the features of the two protocols and carefully examined them.

In this study, the following characteristics of ZigBee and Z-Wave protocols have been investigated:

- **Security:** the level of security ZigBee and Z-Wave protocols provide for IoT devices in order to protect them against unauthorized access and hacking.
- **Frequency:** the frequency, in which each protocol operates on, and the advantages and disadvantages of low and high frequencies on the protocol's security aspects.
- **Power Consumption:** how much power the devices consume when these protocols are operating and if they support battery-powered devices or not.
- **Data Rate:** the transmission speed, it is actually the maximum ability of the channel to transmit bits in a second.

3.4. Summary

To sum up, this research is a descriptive study which focuses on an individual subject and attempts to describe features of the subject being studied. This research studies the two communication protocols, ZigBee and Z-Wave, used in IoT devices to determine which one provides more security features in order to save user’s security and privacy and protect them against unauthorized access and hacking.

Chapter Four

Data Analysis and Discussion

Chapter IV

Data Analysis and Discussion

4.1. Overview

This study tries to find out which of ZigBee and Z-Wave communication protocols provide more security in IoT devices. ZigBee and Z-Wave are the most common used protocol in IoT devices and it is important to investigate which one has the more capability in saving user's privacy and protecting devices against unauthorized access and hacking.

4.2. Data Analysis

The chronological steps that were mentioned in chapter three are reported here:

In the first step, all gathered articles and books about this topic were studied. Then, those data that were related to the security of ZigBee and Z-Wave protocols in IoT devices were collected. After that the information about different aspects of each protocol were compared in order to determine which of these protocols can provide more security in IoT devices.

4.2.1. Security Features

4.2.1.1. ZigBee Protocol:

ZigBee protocol uses Advanced Encryption Standard, AES-128 algorithm, to encrypt data transmission in the network, freshness counter to prevent replay attacks, message integrity check to prevent message modification and also supports authentication in order to confirm identities (Nguyen & Rong, 2007). In other words, communication between devices on a ZigBee network is encrypted with a network key, messages between two devices are authenticated with a different key and replay attacks, that repeat already-verified communications, are impossible (ZigBee devices, 2019).

ZigBee claims that it can provide advanced security tools to allow its users to have secure IoT wireless devices. Its security is based on symmetric-key cryptography and it means that both sides of the communication must share the same keys to communicate. ZigBee uses 128-bit AES-based encryption system which is considered a highly secure standard (ZigBee Alliance, 2018). The wireless standard of ZigBee protocol is IEEE 802.15.4, which has two layers, the physical layer (PHY) and the medium access control layer (MAC). ZigBee builds the network layer (NWK) and the application layer (APL) on top of PHY and MAC (Fan et al., 2017).

Cryptographic protection in ZigBee only exists between devices and not between different layers in a device because ZigBee assumes an ‘open trust’ model where the protocol stack layers trust each other; therefore layers of the same device are allowed to reuse keys. ZigBee also uses the same security level for all devices in order to simplify information exchange between devices. In addition, it demonstrates this principle that the layer that originates a frame is responsible for initially securing it (ZigBee Specification, 2014).

Besides, ZigBee also uses a frame counter to stop replay attacks (in which an attacker could record and replay a command message). The receiving endpoint always checks the frame counter and ignores duplicate messages (Fan et al., 2017).

As it was previously mentioned, ZigBee uses 128-bit keys to enforce its security mechanisms. A key may belong to a network and in that case, it can be used both by the ZigBee layers and MAC sub-layer, or it can be related to a link that is obtained through the pre-installation, agreement or transfer steps. The creation of security keys for links is based on a key master that controls the match of the link key. In the worst scenario, at least the original master key must be obtained through a secure medium (transmission or pre-installation), because the security of the entire network depends on it. Links and Keys are visible only for application layer. Different services use one-way link changes (using a one-way function) to prevent data leaks and security risks (Baronti et al., 2007).

Key distribution is one of the most important network security measures. A secure network defines a special device that other devices on the network rely on to distribute security keys that are called trust center. Ideally, the devices know the address of the trusted center, and the master key is pre-loaded. Typical applications use a network key that is provided by the trust center (through a channel that is initially unsafe) to communicate without a specific security measure (Bennett & Highfill, 2008).

As a result, the trust center maintains both the network key and the point-to-point security. Devices, except for the primary key master, only accept communications that come from a key provided by the trust center. The security architecture is distributed among network layers as follows:

- The MAC layer has the ability to establish reliable communications. As a rule, the security level that this layer is required to use is determined by the upper layers.
- The network layer manages routing, processing of received messages and broadcasting requests.
- The outputs, if possible, use the appropriate link key that is determined by routing; otherwise the network key is used to maintain the security of information against external devices.
- The application layer provides the creation of key and transfer services to ZDO (ZigBee Device Object) and various applications.

Since ZigBee security infrastructure is based on CCM* mode of the AES cipher for encryption and message authentication (ZigBee CCM, 2019), the protocol uses emergency keys for cryptographic exchanges. These keys are known and cannot be changed. This feature makes this cryptographic system highly vulnerable.

4.2.1.2. Z-Wave Protocol:

Z-Wave protocol provides packet encryption, integrity protection and device authentication services. Z-Wave also supports AES-128 encryption system (Fouladi & Ghanoun, 2013).

Z-Wave authentication mechanism lets an including controller to verify that a node that is joining to the network is the real physical device that it is claiming. Depending on the UI, an including controller may allow the installer to enter a Device-Specific Key (DSK) string of decimal digits that can be read visually or scanned as a QR code. The DSK is the first 16 bytes of the 32-byte long ECDH public key of the joining node. Z-Wave nodes are added to the Z-Wave network (PAN) with Out-of-Band (OOB) authentication to ensure that they can be trusted. A strong temporary key is used to assign keys for one or more security classes (Smart Home Security, 2016).

Z-Wave uses a mesh network technology to securely connect hundreds of smart devices. In this framework, each non-battery device in the network becomes a repeater, which means the network becomes stronger as more devices are added. In addition to strengthening the network, this infrastructure also protects every connected device from malicious hacking. Z-Wave also supports device interoperability to reserve electricity and minimize any lags or interference on your broadband connection (Z-Wave Technology, 2018).

Although Z-Wave claims that it can offer the same strength and sophistication as that used by banks to protect online accounts and user access (Z-Wave Technology, 2018), and using it has some benefits such as low cost, no need for additional cabling, simple installation, remote or local control, affordability, etc (Z-Wave advantages, 2012), but some other experts argue that Z-Wave is not a suitable protocol for IoT devices (Z-Wave Myths, 2017) since:

- It is vulnerable to man-in-the-middle attacks
- It is a dated technology
- It is hard to integrate Z-Wave into products
- It can’t be added to an existing product
- It has a high cost barrier to entry for developers

It can be concluded that selecting each of these two protocols is based on the usage of the IoT device. Z-wave will be used where simplicity and user-friendliness are most important factors, and ZigBee can be used when security is more important.

4.2.2. Frequency

The ZigBee protocol uses 2.4 GHz frequency band, while the Z-Wave uses 915 GHz band in the US and 868 MHz in Europe. Despite its high frequency, ZigBee still has a higher data transfer speed (40 kbps to 250 kbps) (ZigBee Specification, 2014) than the Z-Wave (9.6 kbps to 100 kbps) (ZigBee & Z-Wave, 2012).

The ZigBee protocol uses a higher frequency compared to the Z-Wave frequency of 908 MHz. The higher frequency allows ZigBee to transmit more data and information, but reduces the signal level. The lower range can even be further reduced when it is in blind spots. A high frequency signal can have less effect than a low frequency signal when passing through the walls (Z-Wave vs ZigBee, 2019).

A Z-Wave signal with an unconstrained setting can pass between two network nodes up to 100 meters in an outer space. However, this amount is clearly reduced at indoor places. Walls and obstacles, with other interferences from different sources, reduce the effective distance. A very precise instruction for installing at home is 30 meters for open areas and 15 meters with walls between them. The free space at home for ZigBee is about 12 meters (Z-Wave vs ZigBee, 2019).

The ZigBee protocol is used more in industrial, scientific and medical radio bands. Although the 2.4 GHz frequency is the most common frequency in the global standard but its operating frequency may change in different areas. The frequency in China is 784 MHz, in Europe it is 858 MHz, and in the USA and Australia it is 915 MHz (ZigBee, 2019b).

In 2009, the RF4CE and the ZigBee Alliance consortium agreed to jointly develop a standard for radio frequency radio control. ZigBee RF4CE was also designed for a wide range of consumer electronic products such as TVs and digital receivers and promised much more benefits than the current controls in the market. These benefits included stronger connectivity, increased reliability, flexibility and improved features, versatility and functionality behind the barriers (Zigbee RF4CE, 2012).

Since Z-Wave is a wireless communication protocol designed for home automation, home and smart buildings, the information in this protocol is sent with low frequency radio waves. Unlike WiFi or Bluetooth, which were designed to transfer large volumes of information at high rates, Z-Wave was designed to transmit low volume data with low power consumption. The distance between Z-Wave communication nodes is between 30 to 50 meters, which can be amplified by the middle nodes up to 4 times. This means that the distance between nodes can be increased between 120 to 200 meters. It shows that Z-Wave protocol is more ideal for home applications (Z-Wave, 2019b).

Since ZigBee protocol uses a higher frequency than Z-Wave protocol, and therefore it has more ability to transfer data and information, ZigBee can have higher security than the Z-Wave protocol. Each of these two protocols can be used in different locations for different applications. The Z-Wave protocol should be used more commonly for home and office applications and the ZigBee protocol for industrial, scientific, and medical applications which require higher security.

4.2.3. Power Consumption

ZigBee protocol is designed for applications with low power and low transmission rates. The network running through this protocol only uses a very small amount of energy (Dementyev et al., 2013). Devices that use this protocol must have a lifetime of at least two years to receive a special ZigBee certificate. In ZigBee technology, low-power digital radio signals are distributed in short-range Personal Area Networks (PAN). Low cost and very low power consumption is achieved by the loss of transmission bandwidth and coverage (ZigBee, 2019b).

ZigBee Green Power is designed as a low power standard to support low power devices. This protocol ensures that the least amount of power is consumed by managing the network in such a way that it can be turned off for a long time (Alliance, 2012).

The current ZigBee protocol support Beacon or non-Beacon networks. Beacon frame is one of the management frames in WLANs which are based on IEEE 802.11 standard. It contains all the information about the network. Beacon frames are transmitted periodically; they serve to announce the presence of a wireless LAN and to synchronize the members of the service set (Beacon frame, 2019). In Beacon networks, certain network nodes known as ZigBee Routers periodically generate signals to signal their presence to other nodes on the network. The nodes may be deactivated between these signals. This will reduce the cycle time and increase battery life (Galeev, 2004).

In general, ZigBee protocol is minimized when the radio transmitter is activated, thus reducing the power consumption of the system. In Beacon networks, nodes must only be active when the signal is being transmitted. In non-Beacon networks, power consumption is asymmetric. Some devices are always active, while others are most often disabled (ZigBee, 2019b).

The Z-wave protocol also has very low power consumption, using this protocol makes battery-powered equipments (such as sensors) experience more than two years of battery life. Z-Wave devices can work with 0.1% Cycle Duty, which can dramatically reduce energy consumption and, consequently, increase battery life (Z-Wave, 2010).

Generally both protocols are very low power consuming. They use less energy than Wi-Fi. This advantage makes them suitable to be used in IoT devices. There are various applications that do not have access to electricity for different devices and should be activated by battery. A number of devices that use these two protocols can work with a cellular battery for several years while if the same device is kept active with Wi-Fi, it will usually be deactivated within a few days.

Therefore, selecting each of these two protocols depends on the usage of the device. When simplicity and being user friendly is important then Z-Wave is the best option; and when power consumption, several number of supported sensors and, of course, higher security is important then ZigBee protocol should be used.

4.2.4. Data Rate

Data rate is the speed of transferring data within a computer or between computers and other devices. Data rate is measured in bytes per second (B/s) or bits per second (bit/s) (Data rate, 2019).

Today, many wireless systems do not require a high rate of data transmission, but low cost and low power consumption are the requirements. The ZigBee protocol is commonly used in applications that require low data rates, long battery life, and secure networks. The ZigBee data transfer rate is 250 Kb/s, which is very suitable for data transfer from a sensor or an input device (ZigBee, 2019b).

For internal applications with a frequency of 2.4 GHz, the transmission distance can range from 10 meters to 20 meters (IoT Connection, 2014), its exact distance depends on the materials that are used in the building, number of walls to pass through and the output power in that geographic area. The output power of the radio signals is usually between 0 and 20 dB (1-100 mW). ZigBee protocol is specifically used for low-rate applications and which need long-life batteries (ZigBee, 2019b).

Z-Wave is designed to provide reliable, low-latency transmission of small data packets at data rates up to 100 kbit/s (About Z-Wave, 2013). The throughput is 40 kbit/s (9.6 kbit/s using old chips) and suitable for control and sensor applications (Galeev, 2006).

Despite its high frequency, ZigBee still has a higher data transfer speed (40 Kb/s to 250 Kb/s) than the Z-Wave (9.6 Kb/s to 100 Kb/s) and the protocol which has higher data transfer speed, here ZigBee, is more secure than the others since it can send and receive messages more quickly.

In Table 4.1 a summary of features of both protocols has been shown.

	Standard	**Security**		**Frequency (Hertz)**	**Power Consumption**	**Data Rate (Kb/s)**
		Encryption	**Data Protection**			
ZigBee	IEEE 802.15.4	128-bit AES	16 bit CRC	2.4G/915M	15 mW	20-250
Z-Wave	Zensys Corp	128-bit AES	N/A	908M/860M	1 mW	9.6-100

Table 4.1. ZigBee and Z-Wave Features

4.3. Summary of the Results

In this chapter different aspects of ZigBee and Z-Wave protocol have been studied. These aspects were security, frequency, energy consumption, and data rates. The results of these studies were described in each section and then compared with each other. The results showed that the ZigBee protocol was more secure than the Z-Wave protocol in the various aspects examined in this study. Therefore, according to the results, ZigBee protocol can be a better option for applications with higher security requirements, such as industrial, scientific or medical applications.

Table 4.2 shows a summary of different aspects of ZigBee and Z-Wave.

		ZigBee	Z-Wave
Security	**Encryption:**	AES 128-bit	AES 128-bit
	Data Protection:	16 bit CRC	N/A
Frequency		2.4 GHz	906 MHz
Data Rate		20-250 Kb/s	9.6-100 Kb/s
Power Consumption		15 mW	1 mW
Operative Range		10-20 m	30-36 m
Cost of Building Device		Low	High
Work in All Countries		Yes	No
No. of Nodes		50-65000	10-232
Max No. of Hops		30	4
Network Type		Mesh	Mesh
Applications		– Industry/Home Automation – Low Power Networks	Home Automation

Table 4.2. Different aspects of ZigBee and Z-Wave protocols

Chapter Five

Conclusions and Implications

Chapter V

Conclusions and Implications

5.1. Overview

In order to provide an acceptable answer to the research question, some analyses were done to distinguish which of the two ZigBee and Z-Wave protocols provide higher security to be used in IoT devices. The results of these analyses in relation to the research question have been provided in the previous chapter. Nevertheless, this chapter attempts to provide a conclusion, pedagogical implications of the research, and in the end, gives some recommendations for further study.

5.2. Conclusion

This study was an attempt to inspect the security of using ZigBee and Z-Wave protocols in IoT devices.

In order to summarize this study it can be said that firstly both ZigBee and Z-Wave protocols were explained in details. Then different aspects of each protocol such as security features, frequency, power consumption and data rate were compared with each other in order to find out which of these two protocols are able to provide more security in IoT devices.

ZigBee protocol could show more security in comparison with Z-Wave. From the aspect of security features it was found that both protocols support authentication, encryption for communications, etc. but ZigBee protocol can provide more security when security is a priority in IoT devices while Z-wave can be used where simplicity and user-friendliness are the most important factors.

ZigBee protocol uses a higher frequency than Z-Wave protocol and as a result it has more ability to transfer data and information, thus it can provide more security than the Z-Wave protocol in critical situations.

While Z-Wave protocol can be used more commonly for home and office applications, the ZigBee protocol can be used for industrial, scientific, and medical applications which require higher security.

At the power consumption aspect generally both protocols are very low power consuming. This advantage makes them suitable to be used in IoT devices but it should be considered that selecting each of these two protocols depends on the usage of the IoT device. Therefore when low power consumption along with several numbers of supported sensors and higher security is important then ZigBee protocol should be used.

At data rate aspect, although ZigBee has higher frequency but it still has a higher data transfer speed than Z-Wave and since it can send and receive messages more quickly, it can provide more security in critical situations, like military or medical devices, where transfer speed is a key point.

The final analysis of the results of the comparison of two protocols clarified that the ZigBee protocol is more secure to be used in IoT devices.

In summary, the results of the various aspects that were examined in this study showed that ZigBee protocol can provide more security than Z-Wave protocol in IoT devices. Therefore, according to the results, ZigBee protocol can be used in applications which require higher security, such as industrial, scientific or medical applications.

5.3. Implications of the Study

The result of this study can be helpful to improve the probable future studies in comparing different communication protocols in order to find the best one for a specific application.

5.4. Suggestions for Further Research

Due to the limitations of this research, the results of this research can contribute to other researches and investigations in this field.

One possibility may be repeating the same research by choosing more aspects of the two protocols such as modulation, hardware requirements, etc. Since ZigBee and Z-Wave protocols have many aspects and just some of them were studied in this study, therefore other aspects can be examined in further studies in order to have a more complete vision of the subject.

5.5. Summary

As it was mentioned earlier, using IoT devices has become widespread and is increasing every year; providing security for these devices has always been one of the serious concerns in this area. In the current study, different aspects of two communication protocols in IoT devices have been compared in order to find out which one provides more security to be used in IoT devices.

In this chapter, based on the data collected, the conclusion was drawn and it was confirmed that according to the results of the study the ZigBee protocol can provide more security that Z-Wave protocol and thus ZigBee protocol is more secure to be used in IoT devices.

References

About Z-Wave. (2013). In *https://z-wavealliance.org*. Retrieved April 3, 2019, from https://z-w avealliance.org/about_z-wave_technology/

Abu-Elkheir, M., Hayajneh, M., & Ali, N. (2013). Data management for the internet of things: Design primitives and solution. *Sensors, 13*(11), 15582-15612.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications.*IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International Conference on Information Technology (ICIT)*(pp. 685-690). IEEE.

Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): Definitions, Challenges and Recent Research Directions. *International Journal of Computer Applications (0975--8887) Volume*.

Alliance, Z. (2012). New Zig Bee PRO Feature: Green Power Connecting Battery-Free Devices. *(2012-12)[2014-12-25]*.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Baronti, P., Pillai, P., Chook, V. W., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. *Computer communications*, *30*(7), 1655-1695.

Beacon frame. (March, 2019). In *https://en.wikipedia.org*. Retrieved March 27, 2019, from https://en.wikipedia.org/wiki/Beacon_frame

Bennett, C., & Highfill, D. (2008, November). Networking AMI smart meters. In *2008 IEEE Energy 2030 Conference* (pp. 1-8). IEEE.

Bohli, J. M., Skarmeta, A., Moreno, M. V., García, D., & Langendörfer, P. (2015, April).SMARTIE project: Secure IoT data management for smart cities. In *Recent Advances inInternet of Things (RIoT), 2015 International Conference on* (pp. 1-6). IEEE.

Connected Things. (11 Nov, 2014). In *https://www.gartner.com*. Retrieved December18, 2018, from https://www.gartner.com/newsroom/id/2905717

Data rate. (2019). In *https://www.pcmag.com*. Retrieved April 2, 2019, from https://www.pcmag.com/encyclopedia/term/40833/data-rate

Dementyev, A., Hodges, S., Taylor, S., & Smith, J. (2013, April). Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario. In *2013 IEEE International Wireless Symposium (IWS)* (pp. 1-4). IEEE.*scenario*.

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7).

Fan, X., Susan, F., Long, W., & Li, S. (2017). Security analysis of zigbee.

Fouladi, B., & Ghanoun, S. (2013). Security evaluation of the Z-Wave wireless protocol. *Black hat USA*, *24*, 1-2.

Galeev, M. (2004). Home networking with Zigbee. *Embedded Systems Programming*, *17*(5), 26-31.

Galeev, M. T. (2006). Catching the z-wave. *Embedded Systems Design*, *19*(10), 28.

Gartner Survey. (March 3, 2016). In *www.gartner.com website*. Retrieved November 11, 2018, from https://www.gartner.com/newsroom/id/3236718

Internet of Things. (17 Dec, 2018). In *https://en.wikipedia.org*. Retrieved December 18, 2018, from https://en.wikipedia.org/wiki/Internet_of_things

IoT. (February, 2019). In https*://internetofthingsagenda.techtarget.com*. Retrieved February 7, 2019, from https://internetofthingsagenda.techtarget.com/ definition/Internet-of-Things-IoT

IoT Challenges. (February 2, 2016). In *www.cbronline.com website*. Retrieved November11, 2018, from https://www.cbronline.com/news/verticals/cio-agenda/privacy-liability-patents-4-major-iot-legal-challenges-every-cio-is-facing-4799717

IoT Security Challenges. (17 Nov, 2017). In *https://developer.ibm.com*. Retrieved February 10, 2019, from https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of Threatsto The Internet of Things. *IEEE Communications Surveys & Tutorials*.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative, 1*, 1-86.

Nguyen, S. T., & Rong, C. (2007, July). ZigBee security using identity-based cryptography. In *International Conference on Autonomic and Trusted Computing* (pp. 3-12). Springer, Berlin, Heidelberg.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoTIntegration: A Systematic Survey. *Sensors, 18*(8), 2575.

Porkodi, R., & Bhuvaneswari, V. (2014, March). The internet of things (IOT) applications and communication enabling technology standards: An overview. In *2014 International Conference on Intelligent Computing Applications* (pp. 324-329). IEEE.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013, May). A systemic approach for IoT security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on* (pp. 351-355). IEEE.

Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015, June). Experiments with security and privacy in IoT networks. *In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*(pp. 1-6). IEEE.

Smart Home. (2017). In *https://www.forbes.com*. Retrieved January, 21, 2019, from https://www.forbes.com/sites/haroldstark/2017/05/22/the-ultimate-guide-to-building-your-own-smart-home-in-2017/#475a52c13afb

Smart Home Security (2016). *Introduction to the Z-Wave Security Ecosystem* [PDF file]. Retrieved from https://www.vesternet.com/mwdownloads/download/link/id/2072

Wi-Fi network vulnerability. (2018). In *https://us.norton.com*. Retrieved December 22, 2018, from https://us.norton.com/internetsecurity-emerging-threats-what-to-do-about-krack-vulnerability.html

Wi-Fi Standards. (24 Mar, 2016). In *https://readwrite.com website*. Retrieved November 10,2018, from https://readwrite.com/2016/03/24/wi-fi-industry-standards-needed-sm4/

Z-Wave. (2010). In *http://wiki.micasaverde.com*. Retrieved April 4, 2019, from http://wiki.micasaverde.com/index.php/Z-Wave

Z-Wave. (2019a). In *https://www.techopedia.com*. Retrieved 8, February, 2019, from https://www.techopedia.com/definition/27782/z-wave

Z-Wave. (2019b). In *https://en.wikipedia.org*. Retrieved April 5, 2019, from https://en.wikipedia.org/wiki/Z-Wave

Z-Wave and ZigBee. (2018). In *https://support.smartthings.com*. Retrieved 9, February, 2019, from https://support.smartthings.com/hc/en-us/articles/208672926-Z-Wave-and-ZigBee-FAQ

Z-Wave Applications. (2018). In *https://www.rfpage.com*. Retrieved January, 23, 2019, from https://www.rfpage.com/applications-of-z-wave-technology/

Z-Wave automation. (2013). In *https://www.digitaltrends.com*. Retrieved January, 22, 2019, from https://www.digitaltrends.com/home/smarten-dumb-house-z-wave-automation/

Z-Wave Myths (2017). In *https://www.electronicdesign.com*. Retrieved Feb 26, 2019, from https://www.electronicdesign.com/industrial-automation/11-myths-about-z-wave-technology

Z-Wave Technology (2018). In *https://www.z-wave.com*. Retrieved Feb 21, 2019, from https://www.z-wave.com/blog/why-z-wave-is-the-safest-technology-for-your-smart-home-b90d7399-3180-4a67-a31c-dbdd5bb6a93e

Z-Wave setup. (2017). In *www.z-wave.com*. Retrieved January, 23, 2019, from https://www.z-wave.com/blog/a-diy-smart-home-setup-how-one-customer-uses-z-wave-to-make-life-at-home-safe-and-simple

Z-Wave vs ZigBee (2019). In *https://thesmartcave.com*. Retrieved March 10, 2019, from https://thesmartcave.com/z-wave-vs-zigbee-home-automation/

ZigBee. (2019a). In *https://www.techopedia.com*. Retrieved February 8, 2019, from https://www.techopedia.com/definition/4390/zigbee

ZigBee. (2019b). In *https://en.wikipedia.org*. Retrieved April 6, 2019, from https://en.wikipedia.org/wiki/Zigbee

ZigBee & Z-Wave. (March, 2012). In *https://www.electronicdesign.com*. Retrieved Feb 26, 2019, from https://www.electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave

ZigBee Alliance (2018). *ZigBee 3.0 Stack User Guide JN-UG-3113 v1.5* [PDF file]. Retrieved from https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf

ZigBee CCM (2019). In *http://www.ipcores.com*. Retrieved Feb 28, 2019, from http://www.ipcores.com/zigbee_802.15.4_aes_ccm.htm

ZigBee devices. (2019). In *https://www.csmonitor.com*. Retrieved Feb 27, 2019, from https://www.csmonitor.com/Technology/2015/0819/ZigBee-smart-home-devices-use-absolute-minimum-security?kbid=62750

Zigbee RF4CE. (2012). In *http://www.rfwireless-world.com*. Retrieved March 30, 2019, from http://www.rfwireless-world.com/Terminology/what-is-zigbee-RF4CE.html

ZigBee Specification (2014). In *https://www.zigbee.org*. Retrieved Feb 29, 2019, from https://www.zigbee.org/download/standards-zigbee-specification/

Zillner, T., & Strobl, S. (2015). Zigbee exploited—the good, the bad and the ugly. *Black Hat–2015 [Электронный ресурс].–Режим доступа: https://www. blackhat. com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly. pdf (дата обращения: 21.03. 2018)*.

HALMSTAD
UNIVERSITY

PO Box 823, SE-301 18 Halmstad
Phone: +35 46 16 71 00
E-mail: registrator@hh.se
www.hh.se