MASTER'S THESIS | LUND UNIVERSITY 2015

The security of communication protocols used for Internet of Things

Farhad Johari

Department of Computer Science
Faculty of Engineering LTH

ISSN 1650-2884
LU-CS-EX 2015-42

The security of communication protocols used for Internet of Things

Farhad Johari
ada10fjo@student.lu.se

September 9, 2015

Master's thesis work carried out at
the Department of Computer Science, Lund University.

Supervisors: Jens Christensen, Jens.Christensen@cybercom.com
Jesper Holmén Notander, jesper.holmen_notander@cs.lth.se

Examiner: Flavius Gruian, flavius.gruian@cs.lth.se

Abstract

The thesis introduces a range of communication protocols used to implementing smart homes currently available on the market. Two protocols are chosen and theoretically analysed in depth. The analysis both describes how the protocols works and describes the measures taken in order to protect it against attacks from third parties. The theoretical evaluation analyses how susceptible the protocols are against the replay and eavesdropping attacks. The theoretical evaluation is followed by a case study where one of the communication protocols are analysed practically. During the case study a smart home using the chosen protocol is set up. The network is then attacked with the attacks described in the theoretical evaluation. The theoretical and practical outcomes are compared to see if they match. During this study the theoretical and practical outcome did not match due to faulty use of the protocol. The faulty use of the protocol prevented the equipment from differentiating authentic and inauthentic parties which made the equipment susceptible. However, the case study only represents a sample of the technology being used and the faulty use is caused by one manufacturer. Thus the protocol can not be deemed unsafe solely based on the outcome of the case study.

Keywords: MSc, Communications protocol, Integration Solutions, Internet of Things (IoT), Security, Protocol Analysis, Home Automation

Acknowledgements

I would like to extend a big thanks to my supervisor at Cybercom Sweden, Jens Christensen, for the opportunity and great support throughout the entire thesis.

Further, I would like to thank the examiner Flavius Gruian and the supervisor at LTH Jesper Holmén Notander for the guidance, comments and writing directions given.

Lastly, I would like to thank my brother, Hossein Johari, who spent several long evenings reading and providing writing directions in his free time.

Contents

Chapter 1
Introduction

The Internet of Things (IoT) has in recent years become a hot topic amongst technology enthusiasts and industry. It is a technological paradigm in which billions of heterogeneous devices are connected with each other forming a network of interconnected devices, e.g. The Internet of Things. Thus, enabling devices to communicate amongst each other as well as human beings. IoT is promised to have a profound impact on our lives, for instance as an enabler of smart homes where the connectivity of devices lets users remotely control, automate and monitor home appliances.

From a historical perspective, it has not been obvious that IoT could ever be realized. Reasons such as high cost of sensors, high energy consumption of wireless devices and the non existing Internet connectivity of appliances has been arguments amongst its critics.

However, due to developments in the last decade today's technology enables anyone to set up their own smart home. Along with the increased popularity, questions regarding the security of the technology and the integrity of the users have been raised.

There are studies showing how Internet of Things could improve different aspects of different industries such as, but not limited to, the manufacturing industry [1][2] or transportation industry [3]. Besides the previously mentioned industries Internet of Things is a paradigm relevant when developing smart homes. A smart home differs from an ordinary home by having its home appliances integrated with the Internet and allowing them to communicate with each other. The functionality of the appliances are then controlled remotely. Besides remote control it also allows the users to automate and monitor a lot of their home activity. An appliance can control elementary functionality such as turning on a light, regulating the heating, regulating the air conditioner or unlocking a door. However, to make an appliance support the smart home system the manufacturer has to integrate hardware and software supporting desired functionality. In other words, each appliance must be able to communicate with other appliances on the network. Each device that is a part of the smart home network makes use of an communications protocol, which can be seen as a standardised way to communicate amongst other participants in the network. Presently there is no a determined standard to use when integrating the hardware

and software in to a product.

Internet of Things, as previously mentioned, is a way to interconnect devices of any type to each other and to the Internet. In the past it has merely been a pipe dream to get two devices to surpass the machine-to-machine (**M2M**) communication, and to allow a unification between different appliances from different manufacturers. Imagine devices communicating with each other without a human being overseeing it.

Smart homes and home automation is becoming more common with every year that passes and is estimated to grow even bigger in the near future [4]. With the rise in popularity more users are concerned with questions revolving the security and the integrity of the user.

With the rapid evolving and rise in popularity of smart homes there are also a lot of questions emerging. Some of these surrounding the protection against an unauthorised unit or user gaining access to the appliances. Questions such as: what is done in order to protect the user from a potential home invasion? What is done in order to protect the integrity of the user when information is uploaded to the Internet? What makes each protocol unique, and keeps each home solution separate from each other? What ensures that the wireless communication is kept secure from third parties? These are just a fraction of what users are concerned about. The answers to these questions are dependent on the communication protocol the user is using.

This thesis will evaluate two of the existing standards from a security point of view. The question that we focus on is the non-authenticated access, in other words, denying third parties access to functions or information that makes the smart home vulnerable. Several essential points will be analysed on each communications protocol, and also two different scenarios of attacks will be simulated theoretically. The theoretical analysis will be followed by a practical case study (demonstration) where the same scenario will be evaluated.

1.1 Background

The availability of Internet and smart phones has in recent years become drastically improved, providing services to anyone at a low cost. The availability enables the existence of networks independent of size. Besides the availability more devices tend to support WiFi technology which enables them to connect to the Internet. These factors are the main causes to why Internet of Things is a hot topic in the current technology era.

When implementing a network that is using the Internet of Things paradigm several technical challenges and difficulties are encountered. An example of a previous major challenge is that the implementation of a home network required rewiring of electrical outputs and circuits in homes. The rewiring is not impossible, however, it requires a high budget. However, the rewiring issue can be avoided in recent protocols since most protocols use radio frequencies to communicate. Another example of a challenge and difficulty has been the security of a network. To be able to provide a secure solution where the users privacy and their network is protected against malicious activity. Some of the security challenges stem from not being able to hide the communication that is done over the radio frequencies, thus being available to anyone in the communications proximity.

When setting up a network there are several different techniques a user could use to get

the appliances to communicate amongst each other, such a technique is called an Integration platform or an Integration platform. All integration platforms consists of a communication protocol that describe communication related specifications, such as topologies used, routing, frequency band, et cetera. When implementing the communication protocol a combination of both hardware and software is used. The architecture is dependent on which integration platform that is studied. However, due to the rise in availability of wireless communication most integration platforms developed today has a similar ground layer specifying the physical communication form. Although they may be similar some of their specifications differ, such as the frequency band used.

A smart home is a home environment where the resident is able to remotely control functionalities provided by the home appliances and where the home appliances are able to communicate amongst each other. Thus the Internet of Things paradigm is connected to the smart home. One of the earliest reported concepts of a smart home was presented in 1975 with the use of an Integration platform called X10 [5]. The platform used power line wiring in order to signal and control home appliances. X10 has been updated some but still remains as an alternative when setting up a smart home.

An example of a scenario how a smart home could work is when the toaster and the smoke detector communicate. Imagine that bread gets stuck in the toaster, the smoke detector senses the smoke and tries to communicate with the home appliances in order to locate the smoke source. Another example of a smart home scenario could be when the resident is able to read and regulate the temperature in different parts of their home through their smart phone, since it forces a communication between the thermostat and air conditioning systems.

An example of what a smart home can consist of is demonstrated in the figure 1.1.

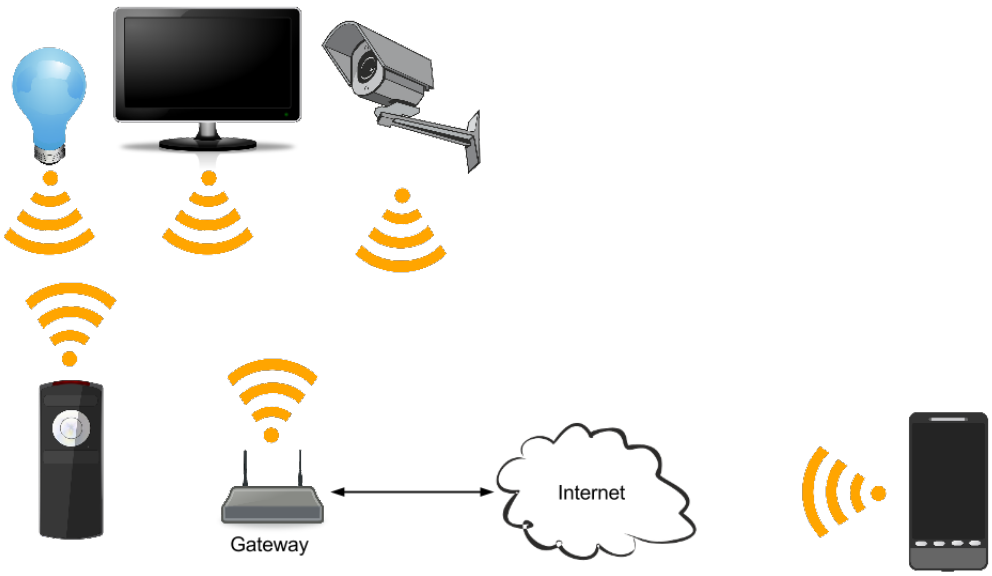

Figure 1.1: Demonstrates what a smart home can consist of. Phones use a different frequency when communicating therefore it sends messages through the Internet which are then relayed through a gateway.

With the growing market for smart homes more companies tend to produce devices that support the existing integration platforms [4]. However, when a company decides to develop products supporting the technology, they have to decide which integration platform to use. Currently there are a few different integration platforms available on the market and no standard is set.

The security of a smart home is considered to be one of the key questions when introducing a platform. With a non-secure platform, a smart home could be susceptible to a variety of different attacks, which could leave the resident unsafe in their own home. An attack performed by a unauthorised party outside the network is called a third party access attack.

A short list of different third party attacks and their causes when targeting smart homes follows:

- **Sniffing/Eavesdropping** - An eavesdropping attack is carried out by listening on a conversation between two other parties. This attack can be carried out if the platforms used communicate in clear text, since there is nothing stopping an attacker from using a receiver to pick up the communication between the participants when the communication is using a wireless solution.

- **Man-in-the-middle** - In a man-in-the-middle attack the attacker pretends to be a part of the targeted network, but in reality it stands in between two communicating units. As the man-in-the-middle it relays messages received on both ends to the believed destination, and therefore it is able to partake in the conversations. A man-in-the-middle attack can be performed if the platform uses an inadequate way to authenticate parties in the network.

- **Replay attack** - A replay attack is performed by eavesdropping and re-sending communication picked up. A smart home could be susceptible to a replay attack if the integration platform uses an inadequate way to authenticate parties or packets.

There are professional organisations that both develop and study security standards which are used when constructing communication protocols. The standards are used to ensure security for its users and to keep the protocols homogeneous. An example of such an organisation is the Institute of Electrical and Electric Engineers (IEEE), which consists of 426000 members. The organisations goal is to advance and innovate technology for the benefit of humanity [6]. IEEE has standardised partial layers of communication protocols which are commonly used in wireless communication, such as the IEEE 802.15.04. The 802.15.04 protocol uses the physical layer of the conceptual model described in the OSI model, where the data is transmitted in raw bit streams over a physical medium [7].

The communication in a smart home tend to become monotonous, and in order to enforce variation in the communication a randomised value is used. During each conversation between two parties a new randomised value is generated. The randomised value is called a nonce value, which is an acronym for Number used ONCE (NONCE). Without the use of nonce values parties communicating have a hard time proving the session authenticity and the originality of the communication. Thus some communication protocols tend to use nonce values.

1.2 Problem Statement

The growing market for smart homes will likely lead to the everyday person will encounter a smart home in the near future. However, the security may prevent the whole progress and growth of the market. It is not too far fetched to state that the consumers might find it daunting to live in a smart home if they lack trust in its security. Just imagine the consequences of a potential intruder, or a third party, gaining access to the functionality in a smart home, such as the security camera or the front door. It can concluded that a company has to consider the security risks and security precautions of a platform before choosing it.

In order to restrict the study to a subgroup of platforms we only consider the platforms which are not directly connected to the power line. Another attribute that is highly valued for selecting a platform is that the products should be from today's market. This is determined by how relevant the platform is today, in other words how widely the platform is spread and used, and also the platforms potential to grow even further in the market.

To narrow the range of available platforms we set a few requirements on the platforms. One of the requirements we set on our platforms is that it should be completely wireless, between the controller and the devices. The requirement allowed us to exclude platforms where there are partial wiring to the electrical sockets or similar stationary platforms, which made the case study easier.

The thesis will try to give answers to the following questions:

RQ1 How is security handled by contemporary IoT communication protocols with regard to unauthorised third party access attacks?

RQ2 Which of the studied IoT communication protocols provides better security with regard to how they handle unauthorised third party access attacks?

RQ3 What are the challenges of implementing a smart home appliance using an existing IoT integration platform with regard to how they handle unauthorised third party access attacks?

1.3 Method

We conducted a literature study in order to choose which communication protocols to evaluate. The study was performed by identifying different communication protocols, focusing on integration platforms, for smart homes using primarily Google Scholar. We included only those platforms that were mentioned by the top 10 number of articles when searching with the keywords wireless home automation networks, smart home wireless protocols, etc. Among the protocols identified, we selected two for a more thorough analysis.

In order to get some more background before choosing which communication protocols to evaluate, a literature study is carried out. The study consisted of analysing the protocols found when searching for smart homes and integration platforms on the search engine, Google Scholar. A brief introduction of the top results is presented and two protocols are selected for further analysis.

This study's revolves around the security measures used to protect against third party attacks giving the third parties unauthorised access to the data and functionality. Even though some of the protocols might have other security problems, such as physical attacks, e.g. breaking a lock on a door, these kind of attacks will not be considered in this evaluation.

The chosen protocols are thoroughly introduced and their protocols are dissected in order to gain some deeper understanding of the communication between the different layers and what is accompanied with the actual data when a packet is sent.

After gaining a thorough understanding of the protocol structure, it's layers and their functions, and the measures taken to secure the communication are presented. Anything that is considered to be a part of the security is included in the evaluation and are presented with a brief explanation of their functionality.

Any third party developed feature, such as encryption algorithms or encoding, are also to some extent introduced and explained since it is considered a part of the system even though it is not developed by the manufacturers. If there are any known security liabilities in the third party features they are also presented.

After explaining the selected protocols from a security perspective a subsection follows in which attack scenarios are outlined and the outcome of running the scenarios are reasoned about based on the available information. Due to restriction on both resources and time, the only two attacks chosen for the scenarios in this thesis are Replay attack and Eavesdropping attack. However, the outcome of these two attacks will demonstrate how secure the authentication and the encryption process is.

The following two scenarios will be used:

Replay Attack

1. Connect Unit-A so it controls a lamp/light bulb (receiver).
2. Unit-B sniffs the traffic.
3. Unit-A sends a request to switch the lamp/light bulb on.
4. Confirm that the receiver changes state.
5. Unit-A sends a new request to switch the lamp/light bulb off.
6. Confirm that the receiver changes state.
7. Unit-B does a replay attack by resending the first packet, trying to turn on the lamp/light bulb.
8. The attack is successful if the receiver changes state.

Unit-A is the unit which should have access to the functionality, also referred to as transceiver. The receiving component is connected to the lamp/light bulb. Unit-B is the unit which should not have access to the functionality and should be excluded from the network.

Eavesdropping and deciphering status attack

1. Connect Unit-A so it controls a lamp/light bulb (receiver).
2. Unit-B tries to communicate with the lamp/light bulb.

3. The attack is successful if unit-A responds with its current state/condition (on/off).

Unit-A is the unit which should have access to the functionality, also referred to as transceiver. The receiving component is connected to the lamp/light bulb. Unit-B is the unit which should not have access to the functionality and should be excluded from the network.

The theoretical evaluation is then concluded with a review on how vulnerable the protocol might be. To determine the vulnerability the review consists of analysing the protocol from the following four different aspects:

- Authentication process - When communicating with another party in the network it is important to use a proper authentication process. The authentication process ensures that the parties indeed are whom the claim to be, and identifies each party in the network. An inadequate authentication process can result in the fact that outside parties gain access to functionality within the network.
- Protocol - Each platform implements, or uses a predefined, protocol when constructing the messages transmitted between the parties in a network. If the protocol has known vulnerabilities, or security flaws, the whole platform becomes vulnerable. A vulnerability in a protocol could literately be caused by a wrongful definition or a bug defined in the protocol. We use Google Scholar in order to discover existing vulnerabilities.
- Functionality exposure - Most platforms require that each component, using their technology, provide a group of basic platform-related functionality, such as relaying messages and broadcasting messages. The components should provide some functionality for external use while some should remain private. Is it ensured that the public functionality is separated from the private functionality.
- Denial of service attacks - Does the platform protect itself from high stress attacks? A typical way to stress a system is to perform a denial of service attack, where the attacker overloads the system with too many requests causing it to eventually crash.

The theoretical evaluation is followed by a chapter describing a case study. One of the evaluated protocols are physically tested. The scenarios used in the case study are the same scenarios used in the theoretical evaluation. The results of both the theoretical evaluation and the case study are presented in the chapter concluding the thesis.

1.4 Related Work

This thesis is based on the security aspect of integration platforms, and will focus on specific platforms that already exist. The idea of a smart home has been coined by the American Association of Housebuilders in 1984 [8], and there is plenty of work describing possibilities as well as the current problems.

In their paper [9] Fischerström et. al. present a security analysis of the potential software issues encountered when using a wireless smart home. The thesis introduces three

different integration platforms briefly along with several different known attacks such as Man in the middle, ARP spoofing, Replay attack and Denial of service. The risk analysis and implementation of the attacks, Replay attack and Cross-Site Request Forgery, are both presented. The replay attack was unsuccessful when using their platform. However, in this thesis other integration platforms and other equipment is used to preform a similar attack and other attacks. The use of different equipment and a different platform may result in a differentiating outcome.

In [10], Liu et. al. presents some of the security, privacy and key issues when discussing Internet of Things. The paper stands as a research presenting what challenges that have been solved and some challenges that still remain unsolved. Both security features and security requirements of the different protocol layers are presented to separate the different key mechanisms, such as key agreements, encryption, authentications and anti-ddos functions. The layer instructions presents what mechanisms should be used on which layer, and the reasoning behind their placement. Whilst the goal and aim of the paper may hugely differ from this thesis, it is related in the sense that the directions given in the paper are easily traceable in this thesis. However, the attacks considered in this thesis are mainly directed at the application layer and the network layer, which are two of the four introduced in the paper.

In their paper [11], Babar et. al. present the objectives of Internet of Things so the reader understands what the motives and purposes of Internet of Things is. The objectives is then followed with security requirements surrounding the privacy, trust and authentication of the data along with their related security threats. The importance of using a thorough security model when implementing a network is argued. In their argument they state that the popularity and availability of Internet of Things is highly dependent on the privacy and security provided in the platform. Implying that if security measures are taken lightly or are overseen it can decrease the adoption among the Internet of Things users. To conclude their paper they provide a new security model where they use a cube model to depict the security. The three dimensions consist of Security, privacy and trust. The paper uses good arguments to why the security is of grave importance to both the user as well as the growth and realisation of Internet of Things.

In their paper [12], Olawumi et. al. reports how a platform handles a variety of unauthorised third party access attacks. The paper presents a security overview of the platform used where information about how the communication is set up and handled. The paper demonstrates how the laboratory environment used is set up. After documenting the environment the unauthorised third party access attacks are simulated, and both the replay attack and eavesdropping attack is among the performed attacks. The outcome of the attacks is successful, and the security is deemed to be unsatisfactory. The author then concludes the paper with possible platforms in order to prevent the unauthorised third party access attacks from being successful. One of the measures suggested in order to prevent replay attacks from being successful is to include timestamps in the packets sent. Thus in case a packet is reused the timestamp would differentiate from an original packet. The approach of presenting an overview on the platform security and then performing several attacks on the network is the exact approach used in this thesis.

This thesis will give insight on what integration platforms currently are available for the manufacturer, and what two of the integration platforms do in order to keep the communication secure. The thesis also gives insight of what consequences a faulty use of a

integration platform can lead to. In the conclusion of this thesis one of the evaluated platforms will be recommended and the recommendation will be based on both information gained during the theoretical analysis and information gained during the case study.

Chapter 2
Review of Communication protocols

This chapter consists of an introduction to several different integration platforms on the market. After briefly introducing a few integration platforms, Z-Wave and ZigBee are chosen to be described thoroughly and evaluated. The method used to evaluate is described in the first chapter (1.3). After the evaluation one of the platforms is chosen for the case study.

2.1 Overview

When developing a smart home appliance there are plenty of different communication protocols to chose from. The wide range of integration platforms is a result of the fact that no exclusive standard has yet been set. Some companies see this as an opportunity to set their own standard, in other words implement their own integration platform.

When choosing which protocols to evaluate in this thesis, the availability and popularity are considered. The integration platforms presented below were the top results when searching for newly published scholar papers on Google Scholar:

- Z-Wave - One of the biggest and most common platforms in toady's market is the integration platform Z-Wave developed by Sigma Design. Sigma Design claim that of all smart home communications used today approximately 80% of it utilises Z-wave technology [13]. There are more than 300 companies that produce products supporting Z-wave technology and all these companies are in a consortium called Z-wave Alliance. All these companies produce wireless products that are interoperable with each other[14]. International Telegraph Union Telecommunication Standardization Sector (ITU-T), a sector of the specialised agency of the United nations, has described the lower layers of the protocol used by Z-Wave.

- Enocean - The platform is developed by the German company Enocean GmbH. This platform is mostly used in Europe. During the platform's early years the re-

leased products lacked the use of an encryption algorithm when constructing data packets. This allowed various types of attacks. However, the company has recently announced that they soon will upgrade their security and include an AES-128 encryption on their data packets [15]. Compared to the other platforms the amount of research and scholar papers found surrounding this technology is rather few. Enocean provides a solution that can solely run on green energy which can be regarded as a environmentally friendly alternative. Green energy, which is energy that is received from environmental friendly platforms, such as solar panels or kinetic energy [16]. The energy harvesters are also released by Enocean.

- ZigBee - ZigBee is a communications protocol developed by the company ZigBee Alliance. The protocol is categorised as a WiFi protocol and is commonly used in smart home networks. The protocol is based on the IEEE 802.15.04 standard that is well known and which describes the physical and media access control layers. The higher levels are however developed solely by ZigBee Alliance. There are some regular differences between ZigBee and the competitors, such as frequency bands, maximum amount of devices and the maximum range between two communicating devices. However, what really sets ZigBee apart from its competitors is its use of an open source protocol stack. The use of an open source stack gives the user the option to characterise the platform based on own preferences.

- Insteon - Insteon is a integration platform registered trademark of Smartlabs Inc. This platform was very popular about ten years ago and was reported having 40% of the market share by that time [17]. However, related papers and technical documentation surrounding its technology is extremely limited when searching on engines such as Google Scholar, which would restrict the depth of the security evaluation.

The items listed above are some of the top results found when searching for integration platforms on Google Scholar. However, being realistic and having certain restrictions on time and resources only a few platforms could be evaluated in this report. In order to determine which protocols to evaluate we set a few requirements. One of the requirements is that the technology uses a wireless platform which all platforms presented above support. Only solutions that are obtainable by the public user are considered, which excludes some platforms that are currently in development and platforms that are expensive.

Another property valued highly is the popularity of the platform. However, it is difficult to measure the popularity since we could not find a recent estimate of the market share for the currently used communication protocols. Instead we studied the amount of third party manufacturers and resellers which could be found at some of the solutions homepages [18] [19] [20]. It is assumed that the availability, supply and demand is increased with the popularity of a platform. It is also assumed that the market for the third party device manufacturers is bigger if a technology is widely used. An exception to the popularity requirement is if the platform deem to have a revolutionary property. Due to the popularity amongst manufacturers[14] it should be perceived as a good candidate for the evaluation.

The last requirement is that only platforms that has some recent updates and studies are considered. In order to evaluate a platform the technical documentation or published papers for the integration platform should be available on the Internet and on the search engine Google Scholar. When searching with the query Insteon or Enocean, there is a lack

	Z-Wave	Enocean	ZigBee	Insteon
Wireless platform	Yes	Yes	Yes	Yes
Mesh topology supported	Yes	Yes	Yes	No
Encryption used	AES-128	None	AES-128	AES-256
Information availability	Plenty	Scarce	Plenty	Scarce

Table 2.1: Demonstrates the main factors making a platform eligible for the thesis. The last row, Information availability, represents the availability of scholar articles on Google Scholar.

of recent papers. Because of the lack of information, the other integration platforms were prioritised over Insteon and Enocean.

ZigBee has gotten a lot of attention recently because it is based on an open standard. The technology is not directed to any specific group of users, which makes it suitable for any type of user or company. Due to its cheap retail price and free licenses, any company could use the technology in their products. The vast availability makes the forum for questions bigger and more diverse, which is beneficial from an information point of view. The broad community might be an argument to why a user chooses this type of technology.

The table 2.1 is constructed to demonstrate and summarise the requirements and comparing the eligible platforms and communication protocols with each other. The two chosen platforms are ZigBee and Z-Wave.

2.2 Z-wave

The requirement for setting up a smart home using Z-Wave technology is that the network at least consists of one gateway, one controller and one smart home device, such as a lamp, surveillance camera, etc. If a mobile device is to be used instead of a controller, the whole network needs to be connected to the Internet. The gateway translates the commands sent from the mobile devices to packets that are used for communicating between the devices on the home network. The reason why mobile devices are unable to send packets directly to the smart home devices is because communication is done on different frequency bands.

When communicating through radio frequencies, protocols define what a message is complemented with. Information such as the source address, the destination and the message are all used to construct a packet that is sent. Therefore the protocol will also determine the security process each packet has to go through in order to ensure that third parties are unable to intercept or eavesdrop on the communication.

A protocol can often be split into several different layers where each layer has its own properties. Each packet can be split into different headers that carry information about what properties are set. All layers provide own headers to a packet.

The protocol used in Z-wave has the following four layers:

1. Physical Layer
2. Transport Layer
3. Network Routing Layer

4. Application Layer

Even though there are different Z-wave modules the protocol layers remain the same, and most of the layers provide the same features independent of module version [21]. Each layer will be explained independently in their own subsection.

2.2.1 The physical layer

The Physical layer, which in some cases is referred to as the radio layer, is closest to the hardware. This layer describes how the communication between a transceiver (a controller) and a receiver (device being controlled) is done. As previously mentioned, Z-wave uses radio waves for communication. When using radio waves for communication, the user needs to consider signal properties of a transceiver such as attenuation, frequency, encoding, interference, etc.

The maximum distance between two communicating devices is highly dependent on the environment and the equipment used. However, there is a source stating that in an indoor and perfectly open environment the maximum range is 75 feet, which translates to roughly 22 meters [22]. Some of the radio specifications are dependent on what region the Z-Wave chipsets are manufactured for [23] and some examples of the specifications are listed in table 2.2.

	Europe	USA
Center frequency	868.42 MHz	868.40 MHz
Modulation Scheme	FSK	FSK
Encoding	Manchester	Non-Return-to-Zero (**NRZ**)

Table 2.2: Displays some of the specification differences between the devices manufactured for different regions. The presented specifications contain some of the needed specifications when setting up and constructing hardware that is able to eavesdrop on the communication.

Each packet sent on the physical layer contain a payload, which in turn has a variable size. The maximum allowed size of the payload data is 64 bytes [24].

The physical layer also provide communication features, such as the collision avoidance and back off algorithms. These features are not visually detectable by the end user. However, the communication features are of grave importance in order to get the home network working properly.

Collision avoidance ensures that a device is communicating with one device at a time, in other words it ensures that the communication throughout the whole conversation is in between the same devices. This is done by setting the receiving device into a receiving state, which then makes the unit unreachable to other devices. The device will only be able to receive packets from one device at a time. Besides avoiding collisions inside a network this feature will block an attack where a third party tries to jumble the original packet with other packets.

2.2.2 The transport layer

The packets sent on the transport layer contains information revolving the devices (senders/recipients) and the home network information. The figure 2.1 displays the organisation of a packet at the transport layer [23]. If the frame format of the packet sent is set to multicast, the destination field is split in to two fields and carries a destination bit map.

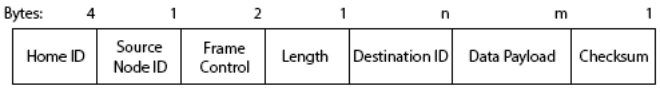

Figure 2.1: The frame structure of the transport layer.

The following list is used in order to understand what the packets consist of and how the information is presented:

- Home ID - This ID is unique for each individual network. As seen in figure 2.1 the ID is described by 4 bytes which in turn restricts the amount of available home networks to around 4 million unique addresses (2^{32}). The primary node of a network sets the Home ID which then is inherited by all the nodes connected to the same network.
- Source Node ID - This is the node ID of the sending device. The ID is 1 byte long and unique for each node in the same network. The length of the ID would restrict the network to 256 nodes per network, however, there some addresses that are allocated and thus restrict the highest amount of connected devices in a single network to 232 [22] [23].
- Frame Control - This field consists of 2 bytes describing how the packet is to be sent. One of the configurations of the frame control is the frame formats. There are three different frame formats; singlecast, multicast and broadcast.
- Destination ID - This field's size and content is dependent on what type of frame format is used. In the scenario when a controller is communicating directly with the node that is to be controlled, it will contain the ID of the destination. In the case when the frame format is set to multicast there will not be a single destination but instead a destination bit map [25]. The multicast format is used to transmit a single packet to several receivers. The maximum amount of receivers is the same as the maximum amount of devices in a network, i.e. 232 devices [23]. The broadcast format will broadcast a packet to all the devices in a network.
- Data Payload - This field consists of the application layer which will be described later in this section (2.2.4).
- Checksum - The algorithm used to calculate the checksum is presented in the ITU standard ITU-T G.9959 [26]. The code for generating the checksum is presented in the following code block:

```
BYTE GenCheckSum(BYTE *Data,BYTE Length){
 BYTE CheckSum = 0xFF;
 for (; Length > 0; Length--){
 CheckSum ^= *Data++;}
return CheckSum;}
```

2.2.3 The network routing layer

The purpose of the network routing layer is scanning the network topology and maintaining an updated routing table. Every device included into a network carries its own network topology which contains information about other devices in the same network. Depending on the type of device used, the network routing layer can resend packets if needed.

The network topology used in the network routing layer is mesh networking. Mesh networking allows devices to find a route between devices even if no direct connection is available. An example of a mesh network is shown in figure 2.2, in this example all six devices are in range of each other which enables direct communication. A mesh network can also be partially connected whereas some devices are out of each others reach and have no direct connection, but are able to establish a connection through other devices.

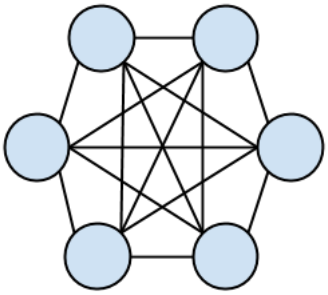

Figure 2.2: A mesh network consisting of 6 devices. All devices are within range of each other and thus able to directly communicate.

2.2.4 The application layer

The application layer handles the parsing of packet payload and the decoding of commands. The first application header sets the frame format in its first byte and the remaining bytes contain command information and associated command parameters.

The Z-Wave commands can be divided in two categories, the first being protocol-related commands and the others being application-specific commands. All devices using Z-Wave technology provide the most basic protocol-related functionality, such as assigning Home ID and Source Node ID (both described in 2.2.2) to a device. The application-

specific commands vary depending on what type of device used. An example of an application-specific commands is when locking or unlocking a door.

Static positioned controllers, often called static controllers, provide a functionality called Static Update Controller. The purpose of the Static Update Controller is to keep an updated routing table between all the controllers in a network. The static controller receives an updated routing table from the primary controller, which is the controller that includes other devices in the network. The static controller then sends out the updated routing table to all the non-primary controllers in the network. If the primary controller is damaged or lost the static controller is able to assign another controller to become the new primary controller.

Static ID Server acts as a register or a depot keeping track of Source Node IDs that can be signed to controllers. If this feature is used with the static update controller it gives the end user access to some of the primary controller options in more than one single controller. An example of an option is including new devices.

With lacking security measures both the Static ID Server and the Static positioned controllers can be targeted by third party attackers, and the outcome could be that unauthorised parties are able to include their own controllers and devices into the network.

2.2.5 Security Overview

The use of radio frequencies makes the communication accessible by any party in the communications proximity and the developers have to take measures to secure the communication. Some examples of the measures taken are encryption, authentication methods and secure keys.

There is a risk when using the combination of a static update controller and a static id server. If the authentication process is faulty, or no authentication process exists, it could allow the outsider to include devices into the network. Including new devices, such as remote controllers, could in turn allow the attacker to remove existing devices or communicate with the existing devices. This possibility appears because of the functionality to physically add new devices when using a static id server.

When including a new device in a network the initial communication between the controller and the new device consists of a key exchange. The key exchange is done by the new device generating a key which is used to encrypt the packets that are sent in between the controller and new device. The key exchange protocol used for Z-Wave is demonstrated in the figure 2.3.

The initial key is generated by the new device and it is constructed with the use of a pseudo random number generator (**PRNG**). The pseudo random number generator used is integrated on the Z-Wave chip of the device. The key is encrypted with a default value which is set on the Z-Wave chip's firmware. If a third party is eavesdropping during the initial key exchange it will only be able to pick up an encrypted version the key. If the default value, which is used to encrypt the generated key, is discovered the key used for communication can be decrypted and the third party will be able to eavesdrop on the communication. In order to perform this kind of attack successfully the attacker needs to be present at the exact moment when an initial setup or re-installation of the device is done. This limits the time frame of when the attack can be performed.

A measure that a user can take in order to secure the key exchange is to switch the radio

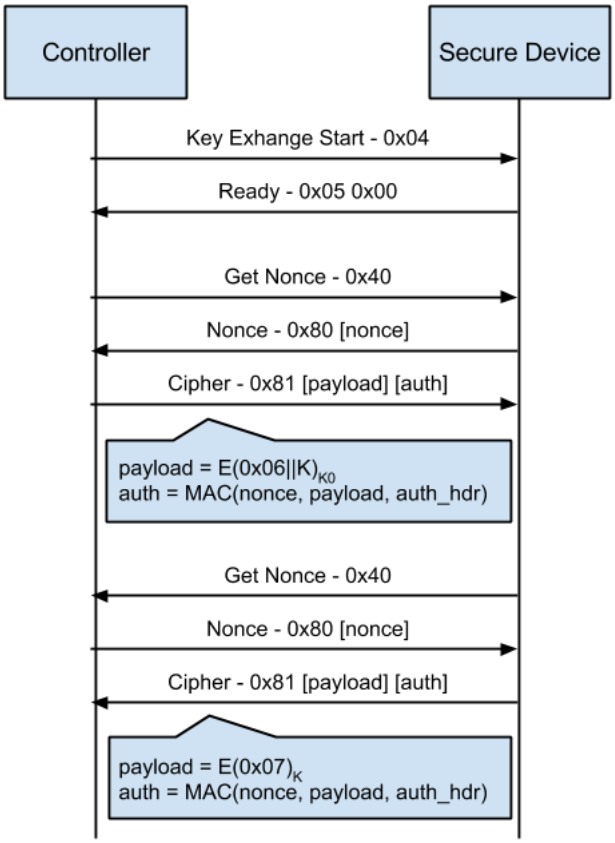

Figure 2.3: A key exchange between a controller and a secure device. The sizes of each packet is written in hexadecimal, hence the 0x before the size-values. The first step of the communication consists of ensuring that the device is available and ready, when a response is sent the controller requests a nonce in order to prove that it is a original packet. The controller uses the received nonce accompanied with an authentication header and the encrypted network key to calculate a MAC, which is sent to the device. Accompanied with the MAC, the encrypted network key is also sent in the same cipher packet. The device uses the same nonce technique to ensure that it is original and sends a encrypted message with the received key to confirm that the new key is set.

transmission signals to a low power mode. The low power mode shortens the range between the controller and the device being included, which also shortens the range between the potential eavesdropper and the device. This forces the attacker to move closer to the devices in order to be in the communications proximity. However, the third party will still need access to the default value set on the product which makes the third party dependent on the manufacturer of the device.

If the key exchange is successful, both parties will have a network key (K_N). Through

the network key both parties calculate two new keys, each of length of 16 bytes (128 bits). One of the keys is used to authenticate the origin of a packet (K_{origin}). The other key is used to encrypt the frames before they are sent ($K_{encrypt}$).

When using encryption in the communication, the options of an attacker are limited. The attacker has two possibilities, the first is figuring out the key used in the encryption algorithm in order to eavesdrop on the communication. The other possibility is tricking the network into believing that their device is a part of the same network in order to communicate with the other devices in the network.

In order to calculate the two keys, the Z-Wave chips use Advanced Encryption Standard (**AES**) on a block cipher mode called Electronic CodeBook (ECB). The calculations can be simplified into the two equations displayed in the list below [23]. ECB is a block cipher mode where a packet is split into separate blocks and each block is encrypted separately from each other. If there are identical blocks when the packet is split, the encrypted blocks will also become identical. For a third party that eavesdrop on the communication might detect patterns when the packets lack any type of verity. Depending on the amount of text encrypted, it is better to use a mode that scrambles the block's content in order to hide patterns. If a solution is found to the encryption method, the use of this mode will make the protocol susceptible to a lot of attacks, one type being replay attacks [23].

$K_{encrypt}$ = AES - $ECB_{K_N}(Password_{encrypt})$

K_{origin} = AES - $ECB_{K_N}(Password_{origin})$

Both $Password_{origin}$ and $Password_{encrypt}$ are hardcoded values set on the Z-Wave firmware.

As previously mentioned Z-Wave uses the encryption algorithm AES which is a widely used standardised cryptographic algorithm. AES is a symmetric key algorithm where both the encryption and the decryption key are the same. According to NIST, a federal agency, AES-128 will remain secure to at least 2030 based on the current cryptanalytic progress and the growth rate in computer power in order to successfully execute a buteforce attack [27]. This ensures that the packets that are encrypted will not be decrypted without access to the encryption key ($K_{encrypt}$).

To ensure that the packets are not manipulated and that the packets origin is genuine, Z-Wave also makes use of cipher block chaining message authentication code technique (**CBC-MAC**). This is used during the data origin authentication. The CBC-MAC technique uses a block cipher to construct a message authentication code (**MAC**). The CBC mode makes sure the encryption of each block is dependent on the correct encryption of the previous block (similar to the calculation of the CBC-MAC, seen in figure 2.4). The difference between these is that each block will form its own output in CBC mode. This form of interdependence ensures that if one of the blocks are altered or manipulated it affects the encryption of the following blocks.

When using CBC-MAC on variable length messages, security threats appear. The threat appears if an attacker knows two correct pairs in sequence, which is consisting of plain text and their CBC-MAC [28]. How this is done is briefly shown in the example 2.1 and 2.2.

The attacker has access to two of the frames sent in sequence. To calculate the MAC of these messages Z-Wave uses the plain text for the message (M1/M2) and the CBC-MAC (t).

$$f(M1, t) = MAC1, f(M2, t) = MAC2 \tag{2.1}$$

The device is susceptible to an attack where the attackers XOR:s the last block an extra time, which nullifies the first XOR. This is demonstrated in the following equation:

$$f(M1, t) = MAC1, f(MAC1 \oplus M2, t) = MAC2 \tag{2.2}$$

There are several measures available in order to make the cipher secure when using CBC-MAC with variable length messages. Examples of measures are input-length key separation, length prepending or encrypting the last block. These methods are common and will not be explained in this report [29]. Although there is no source to prove that Z-Waves makes use of one of these, it is very likely that they do in order to heighten their security.

Before a device can send commands to another device it needs to alert it (if it is in a sleeping mode), or prepare it for communication. In the first packet the initiator asks the receiver for a nonce value. The receiver then uses a pseudo random number generator to generate a nonce value which is returned. The initiator will then insert this nonce in its frames during this exchange. This works both ways, meaning that if the receiver wants to send information to the initiator it will also ask for a nonce value before sending its own frame. This is done in hope to prevent unauthenticated parties from performing a replay attack.

The 64 bit nonce value is generated during the MAC calculation and a in depth description of how it is generated can be read in the security evaluation paper [23]. The equation proves that the nonce values generated are completely random through the use of a pseudo random number generator used.

Since some companies develop products that support the Z-wave protocol through the chip it is important that they use it correctly. In one case [23], it was found that the improper use of the protocol lead to third party access to a closed off functionality.

2.3 ZigBee

The protocol provided by ZigBee is open source which means that any developer or company is allowed to use the technology for free. To ensure that their reputation remains untainted ZigBee Alliance certifing the products they believe hold the security standards. Only products can be certified, not companies, since ZigBee Alliance analyse the security of a specific product. Each product that is certified is listed on their website [30].

The ZigBee protocol is built on IEEE 802.15.04 which is a standardised protocol that defines two of the lower layers. To be more specific ZigBee uses the Physical layer and the Media Access layer of IEEE 802.15.04. On top of these two layers ZigBee applies its own two layers that together create an integration platform suited for smart home networks. The two layers are the Network layer and the Application layer [31].

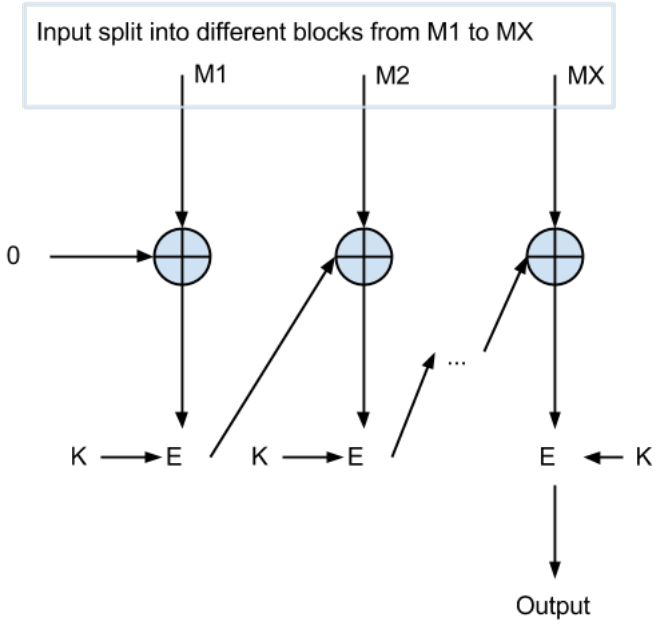

Figure 2.4: The calculation of the CBC-MAC. The frame is split into several different blocks, the first block is XOR;ed with a predefined value (0 in this scenario). The result of which is encrypted with a key. The result of the first block is XOR;ed with the next block and this is repeated until meeting the last block. Once the last block is met the output will form the CBC-MAC value. The initial seed used (0) can be replaced with a initial vector, which can be a sequence of randomly generated numbers or a static vector of numbers.

2.3.1 The physical layer

The physical layer is not a layer that ZigBee has developed themselves instead they use a well known standard called IEEE 802.15.04. Radio frequencies are used by ZigBee in order to communicate. As mentioned in 2.2.1 the use of RF media as communication will force the manufacturers to consider the existence of attenuation, interference, frequency, etc.

The distance between a receiver and a controller for the modules ZigBee IP and ZigBee 920IP is between 50-200 meters [32].

The IEEE 802.15.04 standard defines two different physical layers, which operate on two different frequency ranges. The two physical layers represent three different non licensed frequency bands. The 2.4 GHz band is used on the worldwide devices. The lower frequency range operates on 868/915 MHz, the lower band (868 MHz) is used in Europe and the upper band (915 MHz) is used in a few countries such as United States, Australia, and more [31].

The radio specifications are obtainable in the protocols specifications document [31] and vary dependent on what region the technology is developed for [33].

The packet structure on the physical layer contains the Physical Service Data Unit, which also is known as the media access frame. The maximum length of this field is 127 bytes [34]. The frame has several different formats, dependent on what the frame is used for a certain format is used. As an example the fields in a acknowledge frame differs from the fields in a data frame. There are four different MAC frames, all with different purposes.

2.3.2 The media access layer

The media access layer in IEEE 802.15.04 provides features such as data transmission service, acknowledged frame delivery, association and disassociation, channel access mechanism, frame validation, guaranteed time slot management and beacon management. There are four different types of packet frames each serving different purposes. Explinations of the features and the different packet structures can be read in the specification [33].

2.3.3 The network layer

The network layer serves several purposes and provide different functionality, such as starting up networks, organising the joining and leaving of a device, routing between the devices, searching for devices within range and storing information regarding neighbour devices. There are three different types of ZigBee devices in a network [31].

- ZigBee Coordinator - The main device in a home network is the coordinator and each network always contains one. The coordinator is used as a storage and a trust center [31], storing information about the network and their security keys. The trust center is used by all devices in a network to obtain secure keys. When two devices want to communicate the coordinator establishes a common master key which will represent a link between the two parties.

- ZigBee End devices - An end device is not able to communicate with other end devices. They only communicate with Routers and Coordinators. End devices provide minimal functionality related to the network, and instead they provide functionality seen by the user such as a light sensor or a light switch.

- ZigBee Router - An intermediate router that passes on data between devices. However, some routers also run application functions.

The network layer provides a property list called the network information base, and the properties are used to alter the behaviour and specifications of the network. Two examples of properties changing the behaviour of the network are nwkAllFresh and nwkSecureAllFrames. The attribute called nwkAllFresh indicates whether the received network packets should be analysed for their originality. The attribute nwkSecureAllFrames indicates whether certain security measures are taken on the data frames that are sent and received.

When establishing connection between devices in a network different topologies can be used. The topologies supported by ZigBee are star, tree and mesh topologies. The range of topology alternatives allow the user to use the network topology suited for their purpose.

A network using mesh topology is demonstrated in the figure 2.2.

The star topology works similarly to a local area network where each computer is directly connected to a switch, or a hub. The switch directs the packets sent to its intended destination, or destinations. The figure 2.5 demonstrates a network consisting of 6 devices using star topology.

The tree topology is a combination of two or more star networks which are all connected to each other through a buss topology. A network using tree topology is demonstrated in the figure 2.6. In networks using tree topology routers use a hierarchical routing strategy to route control messages and data to other parties.

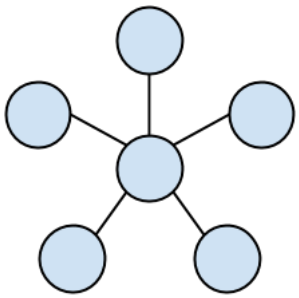

Figure 2.5: A star topology consisting of 6 nodes.

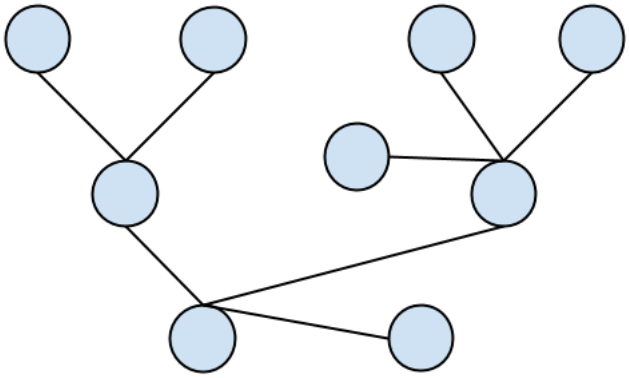

Figure 2.6: A tree topology consisting of 9 nodes.

Only a selection of the supported topologies enable beacon oriented communication. For networks using the tree topology routing the beacon oriented communication is available, while mesh topology use a full peer-to-peer type communication, where no regular beacons are emitted [31].

2.3.4 The application layer

The top layer of the protocol is called the application layer, and is the layer where the manufacturers and developers apply their own products that use ZigBee technology. The layer itself consists of several sub-layers. The Application Support sublayer, which maintains

tables of device pairs that use each others functionality and pairs that need each other in order to work properly. The binding is used to forward messages between the two devices.

Another sublayer in the application layer is called ZigBee Device Object. This sublayer has several responsibilities such as defining device roles in the network (router, coordinator or end device), the initiating and/or responding to the binding requests.

The last sublayer is called the Application Frame work. This sublayer represents the environment where the application object is hosted. The manufacturer of a product using ZigBee technology will implement their own functionality on this sublayer. The functionality differs dependent on the product, and can literally be anything form a light switch to a locking mechanism for a door.

2.3.5 Security Overview

As previously mentioned the ZigBee technology is based on IEEE 802.15.04, which means that the security measures taken in the standardised IEEE protocol are relevant when evaluating the security of the ZigBee protocol. The security evaluation will be separated in two different subsections, separating the IEEE 802.15.04 measures from the ZigBee applied measures.

Security of IEEE 802.15.04

There are several different precautions taken by the standardised protocol in order to ensure reliable security. One precaution includes enforcing the use of message authentication code's (MAC). The use of MAC ensures access control, which means that unauthorised parties are prohibited from joining the communication. Using MAC also ensures that the message integrity is kept secure, in other words received packets are guaranteed to be unaltered by any unauthorised third party. Authenticated devices are able to differentiate between packets sent by legitimate parties and non legitimate parties.

The message authentication code can be seen as a cryptographic checksum for a packet, it is calculated both when sending and receiving a packet. In order to compute the code both parties (sender and receiver) need to share a mutual secret key. The key is a parameter in the algorithm used when calculating the message authentication code, thus the key needs to be kept unknown to the unauthorised users. The sender constructs the packet it wants to send and then calculates a message authentication code for that specific packet. The MAC is dependent on each field in the packet. After calculating the MAC, the code is added to the packet in its own field. When the packet is received by the device on desired destination, the content is once again used to calculate the MAC. The result of the calculation is then compared to the value in the MAC field (code calculated by the transmitter). If the packet has been tampered with, it becomes detectable because of the differentiating MAC value, and if there is a difference between the values the packet is ignored.

Another precaution taken is encryption, which is used to ensure that the communication maintains its confidentiality. In other words encryption ensures that the information transferred between the parties are kept secret from unauthorised parties. The encryption algorithm used has a semantic security property, which ensures that if the same values is encrypted twice it will most likely give two different ciphertexts (results). In order to achieve this property, the encryption algorithm uses a nonce value. The nonce is used to

introduce variation into the packets. This will in turn force the receiver to use the nonce when decrypting the packet.

The encryption algorithm used is the AES with block size 128 bits. The standardised IEEE 802.15.04 protocol supports several different mode of operations and all modes offer different properties. The supported modes are Counter mode (CTR), cipher block chaining message authentication code mode (CBC-MAC) and two different Counter with CBC-MAC modes (CCM and CMM*). However, the mode used by ZigBee is CCM* and will therefore be the only one that is evaluated.

CCM* is a combination of two other block ciphers, one being the counter mode and the other being CBC-MAC (explained in 2.4). There is, however, a modification to the regular CBC-MAC mode in CCM* mode. The modification allows for the calculated CBC-MAC value (the result) to have a reduced length. The CTR mode is demonstrated in the figure 2.7. It combines a plain text header with an encrypted payload, in order to protect the integrity of both the header and the payload. Another property that separates CCM* from ordinary CCM is the fact that CCM* only allow encryption and authentication. The CCM* demonstrated with the help of the figure 2.8.

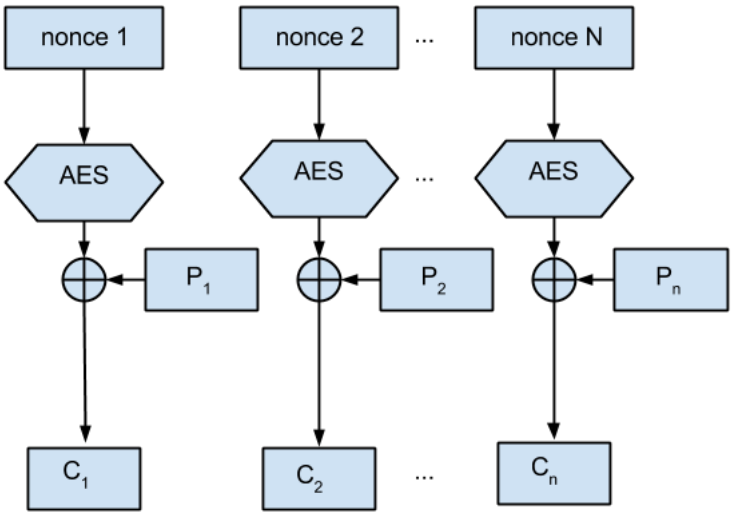

Figure 2.7: The CTR mode uses a counter to construct a stream cipher from a block cipher. The counter is concatenated with the nonce value. The differences in the input becomes the counter value since the nonce is identical in each input. The counter can be generated by any type of function with the requirement that the number used in the sequence is not reused for a long time.

The packets sent and received on the network layer have the option of being secured. One way to use security on the network layer is by setting an attribute called *nwkSecure-AllFrames* in the network information base to true. There are several ways to enforce the network security and if one of the requirements are fulfilled ZigBee uses a frame protection mechanism. The frame protection mechanism is both used when sending and receiving packets, and can be read in detail in the specification [35].

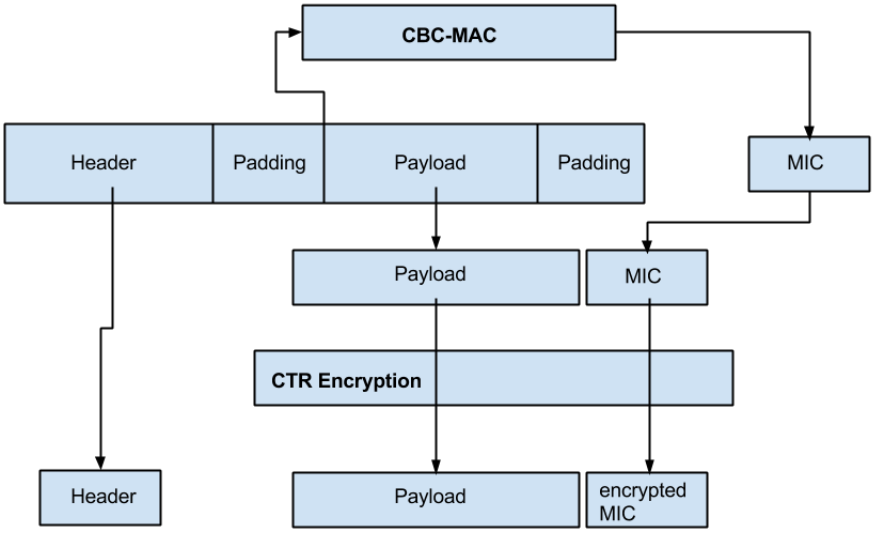

Figure 2.8: In CCM* the constructed packet is padded with null bytes (padding). The packet is then used with an initialisation vector to calculate a CBC-MAC value (MIC). The nonce is constructed through packet specific properties, and is used to encrypt the payload and the MIC (during the CTR encryption). Lastly, the length of the MIC is checked and reduced if needed. The possible length of the MIC is 0, 32, 64 or 128 bits. The 0 bit length implies that the packet lacks authentication.

Security of ZigBee

To secure the communication between different devices, ZigBee uses a network key and several different link keys. Link keys are used when two devices are communicating directly using the frame format unicast. The network key is used when the frame format is set to broadcast. Both keys consists of 128 bits, and all the devices in a network share a common network key.

Both the network key and link keys can be set through either key-transport and pre-installation. Supplementary to these mechanisms link keys can also be set through key-establishment.

Setting a key through pre-installation implies setting the key during the factory installation.

Setting a key through key-transport implies setting the key through communication from one device to another. There are two different commands used when transporting keys, one is labelled as a secure command while the other is labelled insecure. When using the secure transport-key command both the key and the key source (similar to Trust Center) is sent. The insecure transport key command is used when constructing initial keys,

and does not provide any cryptographic protection. Thus the initial key is sent in cleartext. The insecure command type is mainly meant for situations where the key-transport can be realised without any risk of third party eavesdroppers. An example of such a scenario is when the communication is done on a out-of-band channel where the secrecy and authenticity can be guaranteed, however the responsibility of secrecy and authenticity is set on the user.

The key-establishment mechanism used for link keys have certain requirements, such as network size of at least two devices (an end device and a coordinator). Another requirement is that the establishment is prefaced with a trustprovisioning step. The trustprovisioning can consist of simply exchanging trust information between the communicating parties. An example of trust information that can be exchanged is a master key. When the trustprovisioning is fulfilled the establishment of the actual key consists of three steps, these are listed below.

- Short-lived data is exchanged.
- The short-lived data is used to derive the link key.
- Another calculation is done in order to confirm that the derivation of key was successful.

The application support layer located on the application layer establishes and manages keys. Beside the key related processes it also handles the security process when receiving and sending packets on the application layer [35]. The security process differs from the security process followed when sending and receiving packets on the network layer. An explanation of security process on the application layer can be read in detail in the specification [35].

ZigBee provides a configurable security process, where the user is allowed to skip authenticity processes or encryption processes for individual devices and a network as a whole. However, configuring a network to skip a authentication processes or an encryption processes might result in a non secure network.

2.4 Evaluation

In this section the scenarios introduced earlier (see section 1.3) will be theoretically evaluated and and their outcome will be hypothesised. Following the hypothesis, the platform is analysed from four aspects described earlier in Method (see the section 1.3). All of the conclusions and outcomes of the platform are based on the platforms security overview.

Lastly, a comparison between the platforms will conclude this chapter.

2.4.1 Z-Wave

Theoretical evaluation of attacks

Replay attack - After considering the tools being available, it is possible to state that this attack should not be possible since the nonce-value makes use of a generated

nonce and a received nonce. Considering how the nonce is generated (described in detail [23]), the device will recognise that the nonce value is invalid, thus making it impossible to perform a replay attack.

1. Connect Unit-A so it controls a lamp/light bulb (receiver) - Possible by setting up a simple home network.
2. Unit-B sniffs the traffic - Theoretically possible by developing a sniffer that listens to the frequency that is used for communication. Alternatively simply buying Z-Wave's own released sniffer [36].
3. Unit-A sends a request to switch the lamp/light bulb on - Use a controller to change the state.
4. The receiver should change state - It should receive the packets without any complications.
5. Unit-A sends a new request to switch the lamp/light bulb off - Use a controller to change the state.
6. The receiver should change state - It should receive the packets without any complications.
7. Unit-B does a replay attack by resending the first packet trying to turn on the lamp/light bulb - With the use of the sniffer the first sent packet should be picked up and then in this stage transmitted.
8. The receiver should change state - The attack should fail and the lamp should remain turned off, and the device should not be affected to the packet because of its non-valid nonce value. The nonce should be invalid since each conversation should generate its own unique nonce value, thus the resending of a previously used nonce should count as a non-valid nonce value.

Eavesdropping and deciphering status attack - It is fully possible to sniff the packets but it is complicated to decipher the packets sent. Since the encryption is done by the AES 128 algorithm, which as earlier mentioned is believed to be unbreakable until at least 2030 [27], and if the device is following the Z-Wave protocol it should not send any plain text. Theoretically the third party device will not have the same Home ID which means that all the communication from the third party device will not affect the home network.

1. Connect Unit-A so it controls a lamp/light bulb(receiver) - Possible by setting up a simple home network.
2. Unit-B tries to communicate with the lamp/light bulb - The attacker (unit-B) tries to communicate with unit-A through a constructed packet. Without knowing the Home ID it is impossible to get the receiver to respond. However, if the attacker has eavesdropped on Unit-A's previous conversations, and the packets are sent in clear text, the attacker is able to read the Home ID.
3. The receiver responds with its current state/condition(on/off) - The eavesdropping attack should fail and the packet sent should be ignored. No response should be sent since the receiver should not respond to any device that has a

different Home ID. If the Home ID and the device ID is known by the attacker and the attacker has access to a tool altering the content of the packets sent they may be able to get Unit-A to receive the packets sent.

Possible vulnerabilities

This section will discuss if and how the platform handles some common measures taken. An important and recurring fact is that the device manufacturers and developers (third party developers that use Z-Wave technology) are responsible for using the technology right. A recommendation is to only buy products that are verified by Z-Wave Alliance, thus recommended and tested by Z-Wave to confirm that the device is using Z-Wave properly.

- **Authentication process** - Based on the information and security introduced in the security evaluation (see 2.2.5) the authentication process provided is safe, both when communicating between devices and setting up a network. Each key exchange and communication is using proper authentication processes. However, the authentication also relies on the manufacturers of the device. Devices come with a default key and if this key is the same for each copy of that device, it is easy for a third party to obtain the key.

  Some devices require physical interaction when including them into the network, an example of such a device is the wall plug used in the case study (see 3) [37]. This can be seen as another precaution taken when authenticating the user. However, this is not the case for all devices, thus can not be a concluding factor.

- **Protocols vulnerability** - When searching for articles or papers presenting vulnerabilities in the Z-Wave protocol on Google Scholar only papers presenting faulty usage of the protocol were found. Thus we conclude that no protocol vulnerabilities has been found as of yet.

- **Access through devices** - An example of how access through devices is possible, is given in one of the previous subsections (see the section 2.2.4). In the example the home network uses a combination of a static ID server and a static update controller since these two are able to assign a new primary controller or a new device. This would, however, require physical interaction where the third party user would need to gain to the fixed devices.

  Each device will need to be included in a network before being able to communicate with the other devices in the system, thus no foreign devices are able to access or communicate with the other devices in the home network.

- **Vulnerability towards Denial of service attacks** - A denial of service (DOS) attack is in most scenarios possible via jamming when dealing with wireless communications independent of the integration platform used. The jamming is accomplished by transmitting high continuous streams of noise on the frequency used in the network, causing interference. The problem derives from the communicating devices inability to differentiate between relevant and non-relevant packets. Thus the use of a publicly known frequency enables the attacker to jam the network. The equipment

required to jam a network is easily obtained by the public and users can even develop their own transmitters to operate on the same frequency.

Besides jamming the network, an attacker is able to perform an denial of service attack directed at the Internet used by the network. A DOS attack directed at the Internet can lead to a non-functioning network, the network being unable to retrieve requests deriving from controllers connected through the Internet. The user is able to keep their smart home local, in other words not connecting the functionality to the Internet, which will prevent the attacker from being able to attack the system gateway. However, disabling the Internet connection means that the smart home will not be available for external controllers such as smart phones or laptops.

Due to the use of mesh topology in Z-Wave, attackers performing the denial of service attacks are able target specific units in order to keep the unit in a receiving state (explained earlier in 2.2.1) or drain the units battery.

2.4.2 ZigBee

Theoretical evaluation of attacks

Replay attack - After considering the security analysis, it is apparent that a replay attack should not be possible. One reason to why it will fail is because of the use of CBC MAC values. Each time a packets CBC MAC is calculated, output will be different since it is partially dependent on the generated nonce. CCM* also ensure that each packet will have a slight different output, since CCM* uses a counter accumulated with the nonce which will generate originality.

1. Connect Unit-A so it controls a lamp/light bulb(receiver) - Possible by setting up a simple home network.
2. Unit-B sniffs the traffic - Theoretically possible by developing a sniffer that listens to the frequency that is used for communication
3. Unit-A sends a request to switch the lamp/light bulb on - Use a controller to change the state.
4. The receiver should change state - It should receive the packets without any complications.
5. Unit-A sends a new request to switch the lamp/light bulb off - Use a controller to change the state.
6. The receiver should change state - It should receive the packets without any complications.
7. Unit-B does a replay attack by resending the first packet, trying to turn on the lamp/light bulb - With the use of the sniffer the first sent packet should be picked up and then in this stage transmitted.
8. The receiver should change state - The attack should fail and the lamp should remain turned off, and the device should pay not attention to the packet because of its non-valid nonce and CBC-MAC values.

Eavesdropping and deciphering status attack - It is fully possible to sniff packets, however the challenging part is to decipher the packets sent. Since the encryption is done by the AES 128 algorithm, which is believed to be unbreakable until at least 2030 [27], and if the device is following the ZigBee protocol it should not send any plain text (if not instructed to do so). Theoretically the third party device will not be included in the trust center or the route map, which means that packets sent from these devices will be ignored (explained earlier in 2.3.5 and 2.3.5).

1. Connect Unit-A so it controls a lamp/light bulb(receiver) - Possible by setting up a simple home network.
2. Unit-B tries to communicate with the lamp/light bulb - With the information gained construct a packet manually and transmit it.
3. The receiver responds with its current state/condition(on/off) - The attack should fail and the packet sent should be ignored. No response should be sent since the receiver should not pick up or respond to any device that is not included in their map. This was explained in the receiving of packets on the application layer (explained in 2.3.5).

Possible vulnerabilities

This section will discuss if, or how, the platform handles some common measures taken. An important and recurring fact is that the device manufacturers and developers (third party developers that use ZigBee technology) are responsible for using the technology right. A recommendation is to only buy products that are verified by ZigBee Alliance, thus recommended and tested by ZigBee to confirm that the device is using ZigBee properly.

- **Authentication process** - Based on the information and security introduced in the Security Evaluation (see section 2.3.5) the authentication process provided is safe, both when communicating between devices and setting up a network. There are different ways to set up a home network and with the use of the proper security levels both the establishments of keys and the communication between devices will theoretically remain secure.

  The authentication process in ZigBee is dependent on the trust center, which in turn becomes the target for third party attackers trying to falsely authenticate themselves. Without access to the master key, which is used when encrypting link keys between two parties, the third party is theoretically unable to authenticate as a trusted device. The only way to gain access to the master key is through pre-installation, which requires manufacturer access. The other way to obtain the master key is through a secure key-transport which requires that the party is included in the trust center (both pre-installation and key-transport are explained earlier in 2.3.5). Thus one could conclude that the platform provides a secure authentication process.

- **Protocols vulnerability** - During our survey we found no present vulnerability in either protocols (IEEE 802.15.04 or ZigBee). However, since the ZigBee protocol is dependent on a external protocol it has spread dependencies, meaning that a vulnerability in the external protocol becomes a vulnerability in their own protocol.

- **Access through devices** - If an unauthorised user is able to access the coordinator they may be able to include their own devices, and through their devices they are able control other devices in the network. Another possibility appears when using binding (explained earlier in 2.3.4) which should not have binding since it might let an attacker control one device through another, however this would require the two devices to be included in the same network.

- **Vulnerability towards Denial of service attacks** - The issues with denial of service (DOS) attacks in ZigBee are similar to the ones described in Z-Wave (explained earlier in 2.4.1) since the physical layers of both platforms share a lot specifications. However, each packet received from an unknown source starts an authentication process which involves the trust center. Thus a DOS attack can be directed at more than one specific unit.

2.4.3 Comparison

The two solutions share the same hypothesis in the scenarios and have similarities in their protocol structures, such as encryption algorithm and mesh topology. However, the protocol also have several differences. The security differences that we consider important when imagining our scenarios will be introduced in this section.

In the case of the replay attack both of the platforms rely on the use of nonce values. However, generating the nonce values differ and the nonce values are used in different parts of the communication. In Z-Wave the nonce value is generated by using a PRNG number generated on the hardware combined with other parameters (explained earlier in the section 2.2.5). In ZigBee however, the nonce generated for the CCM* decryption/encryption is generated through parameters that are independently obtainable by both parties (explained earlier in the figure 2.8).

Another difference between the two platforms are the block cipher mode of operation used. In ZigBee the CCM* mode is used, which consists of two consecutive modes and in Z-Wave the CBC-MAC mode is used. While the CCM* partially consists of the CBC-MAC mode it is noteworthy that the process used in Z-Wave would be easier to follow when dissecting packets, based on the fact that it consists of a shorter process. In terms of security CCM* use the same block cipher (CBC-MAC) with an extension which could be argued to be more secure.

Another difference that is relevant when considering the attacks performed is the authentication process that is used. In ZigBee packet received from unknown sources are authenticated through the trust center, which means that all devices in a network completely trusts the trust center. In Z-Wave, however, the devices are mainly authenticated through the used Home ID in the packet.

The protocol used for ZigBee allows for more customisation's which sets the platform apart from the other platforms. The user is allowed to turn off different security measures, such as encryption, in the network information base (introduced earlier in the section 2.3.3). In Z-Wave, however, the usage is more static in the way that most features are essential for the communication to work, which restricts the user from altering the behaviour. From this we conclude that for the inexperienced user who have little interest and knowledge about the protocol it might be preferred to use Z-Wave in order to avoid exploit-

ing security processes. However, for the more technically interested and knowledgeable user it might be a good alternative to use Zigbee in order to achieve the results desired.

Chapter 3
Case Study

This chapter describes the case study performed to get a first hand experience of attacking a integration platform. The chapter begins by choosing one of the integration platforms that were theoretically evaluated. After choosing a platform a description of the smart home and the attacking equipment is briefly presented. The chapter is concluded with a evaluation of the scenarios presenting the results of the attacks.

3.1 Platform Selection

Based on the comparison presented in section 2.4.3 it is hard to claim that one of the platform is more secure than the other. Both platforms remain secure even if they tend to take different measures. However, due to the popularity and the restricted way of use (also explained in 2.4.3), Z-Wave was chosen for the case study.

3.2 Design

To ensure that the Z-Wave Technology is used fairly only equipment tested and supported by Z-Wave Alliance were chosen. To be able to simulate the smart home used in the scenarios (see section 1.3) several different Z-Wave components are required. The components required consists of a system gateway, a wall plug and a remote controller. Supplementary to the appliances used to construct the smart home several tools are required when both receiving and transmitting packets.

- Hardware tools:
  - System gateway - The system gateway used in this case study is Fibaro Home Center 2 Gateway. The purpose of the system gateway is to act as the central hub of the network. Each device in the network is connected to the gateway

which in turn is connected to the Internet. Thus all information surrounding the appliances are obtainable through the system gateway.

- Wall plug - The wall plug used in this case study is Fibaro Wall Plug. The wall plug acts as a switch turning on and off depending on the signal received. Due to the work environment we believe that the wall plug is an easier alternative when implementing this scenario.
- Remote controller - The primary controller used in this case study is Aeon Labs Minimote EU. A controller is needed in order to both control the home appliances without accessing the Internet and in order to be able to include new equipment in to the network.
- Two transceivers - The two transceivers used is Texas instruments CC1110. These transceivers are used to transmit falsely constructed packets and to receive the communication sent in the home network.
- USB to UART - The USB to UART adaptor used is Future Technology Devices International Ltd C232HD. In order to connect the transceivers to a computer a USB to UART adaptor is needed. These adaptors provide power and raw bit streams from the transceivers to the computer, and vice versa.

• Software tools:

- SmartRF Flash Programmer - used to flash program the transceivers [1].
- SRecord 1.63 - used to convert the transceiver specifications to HEX-format [2].
- Z-Force - used to both transmit and receive the sent packets [3].

Accessing functionality and checking status of the appliances through a computer requires the system gateway to be connected to the same network router as the computer. All the Z-appliances using Z-Wave technology are used to construct a home network by following the instructions received with the equipment.

The CC1110 transceivers are flash programmed; one is flash as the receiver whilst the other is flashed as the transmitter. In order to flash the CC1110's the SmartRF flash programmer is used and the radio specifications are converted to HEX-format through SRecord.

A schematic of the set up is demonstrated in the figure 3.1.

To be able to understand the packets contents the mac frame is studied (explained and demonstrated in figure 2.1). An example of a packet sent when turning on a binary switch is "F8 48 90 3A 01 41 0B 0D 02 20 01 00 81". According to the frame structure the initial 4 bytes represents the home ID, "F8 48 90 3A". The home ID is followed by the source ID "01", the frame control "41 0B", length "0D", the destination ID "02", the data payload "20 01 00" and, lastly, the checksum "81".

[1] http://www.ti.com/tool/flash-programmer
[2] http://srecord.sourceforge.net/download.html
[3] https://code.google.com/p/z-force/

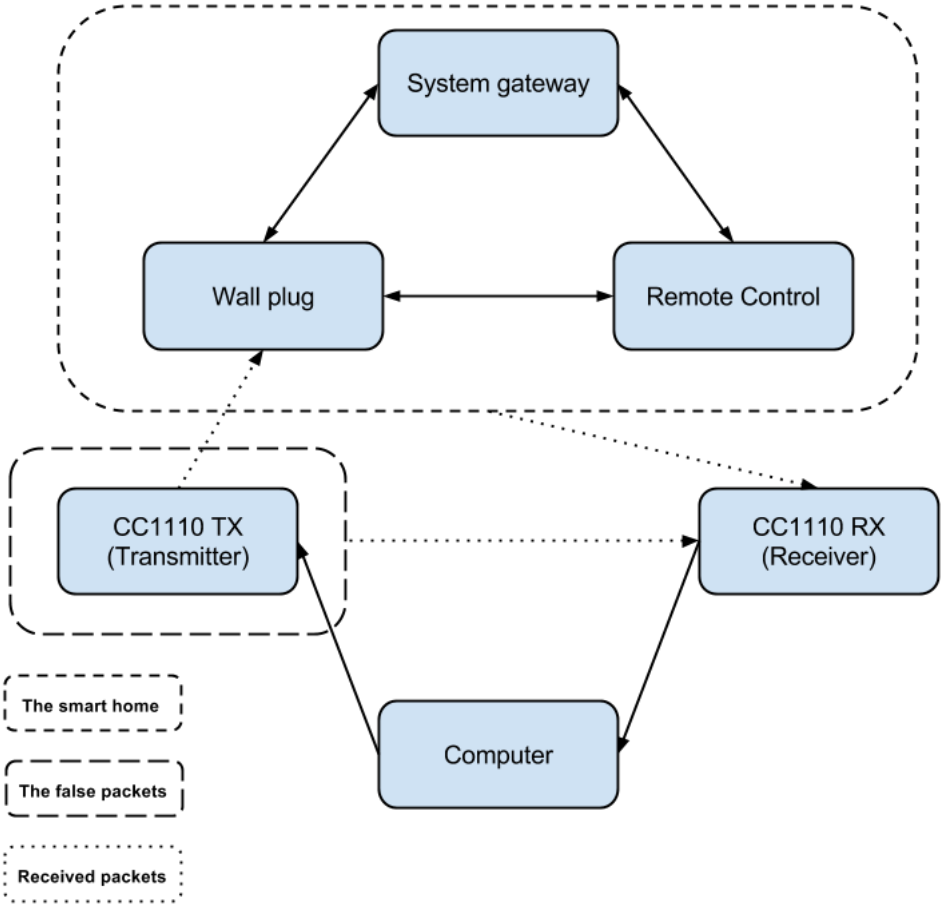

Figure 3.1: Demonstrates how the case study was set up. The CC1110 RX (Receiver) received all communication on the used frequency, both the communication on the home network and the constructed packets sent by the CC1110 Tx (transmitter). The computer is used to construct the packets sent by the CC1110 TX (transmitter) and to display the received packets by the CC1110 RX (Receiver).

3.3 Evaluation

Replay attack - According to the theoretical evaluation the replay attack should be unsuccessful 2.4.1.

1. Connect Unit-A so it controls a lamp/light bulb(receiver) - The system gateway is plugged in and the controller is connected by using the inclusion button. After including the controller into the home, it is automatically set as the primary controller and can be used to include the wall plug into the smart home. A desk lamp is connected to the wall plug and is set to on.
2. Unit-B sniffs the traffic - The receiving chip plugged in to the computer through the USB to UART adapter and the computer runs the program ZForce to display the sniffed packets. All of the packets sent in the range of the transceiver is picked up and displayed on the computer.
3. Unit-A sends a request to switch the lamp/light bulb on - Press the controllers on button that is connected to the wall plug.
4. The receiver should change state - The wall plug turns on and the lamp is on. The computer now displays the packet content as "F8 48 90 3A 01 41 09 0D 02 20 01 FF 7D".
5. Unit-A sends a new request to switch the lamp/light bulb off - Press the controllers off button that is connected to the wall plug.
6. The receiver should change state - The wall plug turns off and the lamp is off.
7. Unit-B does a replay attack by resending the first packet, trying to turn on the lamp/light bulb - The packet sniffed is used to construct a identical packet. The constructed packet is transmitted by the CC1110 chip flashed with the TX program.
8. The receiver should change state - The lamp changes state, and the attack is successful. The result of the attack is seen both physically (lamp is turned on) and through the status on the gateway.

Eavesdropping and deciphering status attack - According to the theoretical evaluation the eavesdropping and deciphering status attack should be unsuccessful 2.4.1.

1. Connect Unit-A so it controls a lamp/light bulb(receiver) - The system gateway is plugged in and the controller is connected by using the inclusion button. After including the controller into the home, it is automatically set as the primary controller and can be used to include the wall plug into the smart home. A desk lamp is connected to the wall plug and is set to on.
2. Unit-B tries to communicate with the lamp/light bulb - Without prior knowledge and just following the patterns seen when dissecting the packets, a new packet is constructed in ZForce. The constructed packet is then transmitted through the USB to UART adaptor which in turn converts the packet into raw bit streams sent on the transmitting C1110 chip.

3. The receiver responds with its current state/condition(on/off) - The attack was unsuccessful in getting it Unit-A respond, however, eavesdropping is still possible since the appliances transmit packets in clear text and sniffing is possible. The only requirement is that the attacker understands the coding of the data payload. The only way to get Unit-A to respond to Unit-B's requests is to use a identical Home ID. This can be set when the attacker is using tools such as ZForce.

Chapter 4
Discussion

4.1 RQ1

It is safe to assume that both of the studied protocols consider that security against third party attacks is important even if they take different measures to prevent attacks. The combination of handshakes and key exchanges differ and are dependent on which protocol is used. Discussion about the differences, strengths, weaknesses and challenges with the different platforms follow.

One of the properties differentiating the protocols is the openness of ZigBee. A technical documentation describing details of all processes such as the construction of a packet or a establishment of a connection between two devices are obtainable by any user. The concept of releasing all technical details to the public is a way for the manufacturer to convey confidence in the platform. The openness allows the end user, as well as companies, to try out the technology and gives them opportunity to discover security vulnerabilities. However, the ability to change the packet structure also allow users to use tweak the technology in order to serve the user's purpose, which may seem flexible and good but actually may result in a security vulnerability. Certain steps in the communication are configurable whereas the user is allowed turn off certain authentication steps or the construction related steps when receiving and transmitting a packet. The ability to manipulate the behaviour increases the risk of an erroneous usage of the technology [35].

Z-Wave is not as adjustable as ZigBee and may seem more restricted in usage when comparing the two. This does not imply that Z-Wave is static in its usage since the user is only given directions to follow. A user is able to ignore the directions and implement as they prefer. An example of directions given is the use of the PRNG generator (explained in 2.2.5) included on the Z-Wave chip, however, there is nothing preventing the user from using a static predefined set of numbers instead of the generated input.

There are obtainable specifications describing the packet structure for both ZigBee and Z-Wave, which allows for the attacker to understand the content of a packet. However,

during the case study we found it a bit difficult to understand certain headers and the content of the payload used in Z-Wave. This could be considered as the most challenging when attacking such a system. If the packet content is encrypted, or if the user has no access to the structure and coding of commands, it is nearly impossible to understand the contents of the packets sniffed.

The use of a trust center in ZigBee forces all devices during their first interaction to rely on a third unit. Involving more parties when establishing a communication medium is reliable in the sense that they share a common trusted unit that confirms the validity of other parties. The use the trust center also hinders third parties from attacking individual devices in a network. However, involving more parties can be considered unreliable in the sense that if the trust center is infiltrated the whole network becomes vulnerable. The coordinator in a network acts as the trust center, once a device is included into the network the trust center adds link keys and a network key to the included device. It is safe to assume that no external device is able to pose as the trust center since all devices in a network have traded keys with the trust center.

Theoretically both platforms provide secure protocols for setting up a smart home. Z-Wave relies on good authentication processes when establishing a connection between devices and CBC MAC when masking the communication. To assure originality and authenticity of packets Z-Wave uses nonce values. ZigBee relies on proper key establishments, secure key-transports and its trust center to assure authenticity. To assure packet security ZigBee uses CCM*, which also uses nonce values to ensure originality. In both platforms the block ciphers provided the use the AES 128 cryptographic algorithm for encryption. The user is given the option to turn off the encryption in ZigBee. Since CCM* combines the CTR mode and the CBC MAC mode it is hard to compare the block ciphers with each other. Z-Wave's platform relies on CBC-MAC only, and it is only used when setting up a communication medium for the key exchange. When the key exchange is successfully finished, the keys are used for the communication.

The companies behind ZigBee and Z-Wave both have other companies analysing products using their technology to confirm that the technology is used correctly. It may be comforting for a user to know that experienced protocol testers confirm the products security when a manufacturer of a product only uses other companies technology.

4.2 RQ2

Considering a scenario where both platforms are implemented correctly the smart home would be secure in both cases. However, due to the well tested security of IEEE 802.15.04 and the consistent authentication and encryption processes, ZigBee would be a more likely to be the safe alternative between the two platforms.

ZigBee supports a lot of configuring, including altering how packets are received and sent. However, altering the authentication process or the encryption processes might result in a non secure smart home network. Thus we conclude that a smart home that uses the initial non configured ZigBee protocol is a secure alternative, while a smart home using a configured ZigBee protocol might result in a non secure network.

4.3 RQ3

A challenge encountered when implementing a network that uses wireless communication is to prevent unauthorised parties to gain access to the communication sent. The challenge arise when there is no physical connection between two parties and the communication can not be directed specifically at a party. All parties using the same platform are awaken when a device is within the sending proximity and thus causes all devices awaken to waste energy. Besides wastefulness the communication also become available by unauthorised third parties if they obtain the radio specifications used for communication.

Due to the far reach of the radio waves, the attacking distance do not pose as a challenge for the attacker. As mentioned earlier, one measure that the user can take in order to restrict the range of attacks is to set the communication into a smaller range mode.

In this thesis the case study needed equipment that used the same frequency as Z-Wave in order to receive and transmit packets. Luckily, the equipment is easily obtained, inexpensive and obtainable by the public. This, regretfully, means that users with technical knowledge or interest are able to obtain the right equipment for sniffing and transmitting packets. The specifications of the radio settings are also obtainable by the public, some of which are presented earlier in this thesis (seen in the table 2.2). Thus there were no real challenge when sniffing up Z-Wave packets. All the software used is easily obtainable and legally free of charge, which allows for the user to find something suited for their purpose.

During the case study there was a difference between the theoretical hypothesis and physical outcome of the replay attack. The outcome of the theoretical evaluation was that the attack would be unsuccessful whilst the case study proved the replay attack to be successful. The attack was successful due to the fact that the equipment lacked the use of a valid nonce value, instead the equipment used a static value which caused the construction of unvaried packets. With the use of a proper nonce value the replay attack would become unsuccessful. If the appliances would use nonce values the values would have been unpredictable since they are generated with the use of a PRNG generator (explained in 2.2.5). Thus an attacker would be unable to perform replay attacks.

Chapter 5
Summary

This thesis has presented several different communication protocols used when implementing smart home networks. Two scenarios are introduced where two different third party attacks are performed, one being a Replay attack and the other being an eavesdropping attack. An in depth analysis of two communication protocols, Z-Wave and ZigBee, is presented along with a overview on their security against third party unauthorised attacks. The main purpose of the security overview was to prove if the protocols take measures against third party unauthorised attacks and if one protocol is more secure than the other. Theoretically both protocols proves to be secure against the two attacks due to various reasons.

A case study is performed where a smart home network using the Z-Wave technology is set up, and the scenarios used in the theoretical analysis is performed practically. The outcome of the case study proved to be different from the theoretical hypothesis because the manufacturer used a static value as a nonce, which created unvaried packets. Thus the network could not differentiate original from falsely constructed packets. The practical outcome however, did not conclude that the protocol had a security vulnerability instead it demonstrated that false use of the technology can have grave impact on the security of a network.

5.1 Conclusions

The security of both platforms is deemed secure against unauthorised third party access attacks if the equipment follow the technical description of the protocol. In our case study we encountered a device with flawed security, which was result of false implementation from the manufacturer. There are cases where products that are supported by the testing companies still fail to follow the protocol, such as the set up used in this thesis case study or a door lock presented in the paper Security Evaluation of the Z-Wave Wireless Protocol [23]. A rule of thumb is to only include products supported by the platform security test-

ing companies (Z-Wave Alliance or ZigBee Alliance depending on the platform), which supposedly follow the protocol as it was theoretically intended.

The recommended platform differs depending on the home network desired, and partially on the user setting up the network. If a lot of configurations are to be done, and the user desires consistent authentication and encryption processes, we would recommend using ZigBee. If the user is interested in setting up a home network and know for a fact that they will not perform any sorts of configurations, we would recommend using Z-Wave because of the fact that the platform has no configurability which will ensure that no security processes are skipped.

The implementation of a smart home using Z-Wave technology is rather easy and does not consist of many challenges with regard to the unauthorised third party access attacks. One challenge is that the communication will remain obtainable by any party since it communicates over radio frequencies, and are sent to all devices in range. Another challenge is choosing products that provide secure platforms. To determine if a platform is secure the user could either manually attack their product or trust the review done by the platform security testing companies.

5.2 Future work

To further analyse the security of the technology more smart home setups should be tested, since only one smart home network (3 devices) is analysed during this thesis. If more equipment using Z-Wave technology were bought and tested and all equipment prove to be susceptible to the replay attack, there could be a error with the platform and not the equipment.

In order to strengthen the conclusion in the thesis several equipment that fulfils all the recommended security properties should be analysed. Equipment where nonce values and AES-128 cryptography is used properly.

Bibliography

[1] Lopez Research LLC. Building smarter manufacturing with the internet of things (iot) - part 2. of "the iot series". http://www.cisco.com/web/solutions/trends/iot/iot_in_manufacturing_january.pdf, 2014. Accessed: 2015-08-11.

[2] Oracle. Java and the internet of things: Automating the industrial economy. http://www.oracle.com/us/solutions/internetofthings/java-iot-industrial-automation-2430562.pdf, 2015. Accessed: 2015-08-11.

[3] Intel. Building an intelligent transportation system with the internet of things (iot). http://www.intel.com/content/dam/www/program/embedded/internet-of-things/blueprints/iot-building-intelligent-transport-system-blueprint.pdf, 2014. Accessed: 2015-08-11.

[4] Tony Danova. The connected-home report: Forecasts and growth trends for the leading 'internet of things' market. 2014.

[5] Dave Rye. My life at x10. Accessed: 2015-08-22.

[6] IEEE. Ieee at a glance. http://www.ieee.org/about/today/at_a_glance.html#sect1. Accessed: 2015-08-22.

[7] Microsoft. The osi model's seven layers defined and functions explained. https://support.microsoft.com/sv-se/kb/103884. Accessed: 2015-08-22.

[8] Richard Harper. Inside the smart home: Ideas, possibilities and methods. In *Inside the smart home*, pages 1–13. Springer, 2003.

[9] Niclas Hansson, Alexander Lantz, and Ludvig Fischerström. A security analysis of wireless smart home technologies. 2015.

[10] Hui Suoa, Jiafu Wana, Caifeng Zoua, and Jianqi Liua. Security in the internet of things: A review.

[11] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the internet of things (iot). In *Recent Trends in Network Security and Applications*, pages 420–429. Springer, 2010.

[12] Olayemi Olawumi, Keijo Haataja, Mikko Asikainen, Niko Vidgren, and Pekka Toivanen. Three practical attacks against zigbee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned. In *Hybrid Intelligent Systems (HIS), 2014 14th International Conference on*, pages 199–206. IEEE, 2014.

[13] Sigma Designs. The internet of things starts at home. `http://www.sigmadesigns.com/internet-things-starts-home/`. Accessed: 2015-08-11.

[14] Z-Wave Alliance. Member companies of the z-wave alliance. `http://z-wavealliance.org/z-wave_alliance_member_companies/`.

[15] Enocean GmbH. Enocean expands enhanced data encryption to its complete 868 mhz batteryless wireless portfolio. `https://www.enocean.com/en/enocean-expands-enhanced-data-encryption-to-its-complete-868-mhz-batteryless-wireless-portfolio/`. Accessed: 2015-08-11.

[16] Enocean GmbH. Enocean energy harvesting products. `https://www.enocean.com/en/energy-harvesting/`, 2015. Accessed: 2015-08-11.

[17] West Technology Research. Insteon has 40% market share of the emerging home control marketplace. 2007. Accessed: 2015-08-11.

[18] Insteon. Insteon - where to buy. `http://www.insteon.com/where-to-buy`, 2015. Accessed: 2015-08-11.

[19] Z-Wave Alliance. Z-wave - member companies. `http://z-wavealliance.org/z-wave_alliance_member_companies/`, 2015. Accessed: 2015-09-07.

[20] ZigBee Alliance. Zigbee - member companies. `http://www.zigbee.org/zigbeealliance/our-members/`, 2015. Accessed: 2015-09-07.

[21] Sigma Designs. Z-wave zm5304 brochure. `http://z-wave.sigmadesigns.com/docs/brochures/ZM5304_br.pdf`. Accessed: 2015-08-11.

[22] Honeywell. Introductory guide to z-wave technology. `https://library.ademconet.com/MWT/fs2/VAM/Introductory-Guide-to-Z-Wave-Technology.pdf`. Accessed: 2015-08-11.

[23] Behrang Fouladi and Sahand Ghanoun. Security evaluation of the z-wave wireless protocol. *Black hat USA*, 24, 2013.

[24] Mikhail T Galeev. Catching the z-wave. *Embedded Systems Design*, 19(10):28, 2006.

[25] Thorbjørn Borup, Alexander Larsen, Kim Mørk, Ebbe Nielsen, and Sigurd Villumsen. A generic software framework for distributed coordination and control in multiagent systems. 2008.

[26] Eeherald. Itu-t g.9959 standard is close to z-wave tech. http://www.eeherald.com/section/newss/nwss201201173.html. Accessed: 2015-08-11.

[27] BlueKrypt. Cryptographic key length. http://www.keylength.com/en/4/. Accessed: 2015-08-11.

[28] Ron Rivest. Computer and network security, lecture 5. http://web.mit.edu/6.857/OldStuff/Fall97/lectures/lecture5.pdf. Accessed: 2015-08-11.

[29] Jonathan Katz. Introduction to cryptography - cmsc 456, chapter 4. http://www.cs.umd.edu/~jkatz/crypto/f12/chap4.pdf. Accessed: 2015-09-08.

[30] ZigBee Alliance. Zigbee certified. http://www.zigbee.org/zigbee-for-developers/zigbeecertified/, 2105. Accessed: 2015-08-11.

[31] ZigBee Alliance. Zigbee specification, 2006.

[32] ZigBee Alliance. Zigbee ip and 920ip. http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/, 2015. Accessed: 2015-08-11.

[33] William C Craig. Zigbee: Wireless control that simply works. *Program Manager Wireless Communications ZMD America, Inc*, 2004.

[34] Lamia Chaari and Lotfi Kamoun. Performance analysis of ieee802. 15. 4/zigbee standard under real time constraints. *International Journal of Computer Networks & Communications (IJCNC) Vol*, 3, 2011.

[35] ZigBee Specification. Zigbee document 053474r06 version 1.0. *Zigbee Alliance Std*, 2004.

[36] Sigma Designs. Sigma dev kit. http://z-wave.sigmadesigns.com/dev_kits, 2015. Accessed: 2015-08-11.

[37] Fibaro. Fibaro wall plug. http://www.fibaro.com/en/the-fibaro-system/wall-plug, 2015. Accessed: 2015-09-09.

INSTITUTIONEN FÖR DATAVETENSKAP | LUNDS TEKNISKA HÖGSKOLA | PRESENTATIONSDAG 2015-08-28

EXAMENSARBETE The security of communication protocols used for Internet of Things
STUDENT Farhad Johari
HANDLEDARE Jesper Holmén Notander (LTH), Jens Christensen (Cybercom Sweden)
EXAMINATOR Flavius Gruian

Hur säkert är ”smarta hem”?

POPULÄRVETENSKAPLIG SAMMANFATTNING **Farhad Johari**

I takt med att “smarta hem” har blivit ett allt mer populärt koncept har säkerheten blivit en väldigt viktig fråga. Under detta examensarbete undersöks det hur felaktigt användande av en integrationslösning för smart hem kan göra hemmet känsligt för attacker.

Under de senaste åren har paradigmet Internet of Things varit ett mycket omtalat ämne i den teknologiska världen. Paradigmet har introducerats i industrier som exempelvis transport, sjukvård och hemnätverk. Smarta hem, som bygger på hemnätverk, är något som blivit mycket populärt och skälet till detta är att tillgängligheten av utrustning och det ökade intresset av att göra egna smarta lösningar i hemmet. Vid uppsättning av ett smart hem kan flera olika lösningar implementeras och det som skiljer lösningarna ifrån varandra är den struktur och process som används vid trådlös kommunikation. Med den växande trenden har säkerheten i smarta hem ifrågasatts då en bristfällig teknik kan möjliggöra intrång från obehöriga. Den trådlösa kommunikationen kan inte riktas till en enskild mottagare utan finns tillgänglig för alla inom räckhåll från den sändande enheten. Detta examensarbete har som målsättning att undersöka säkerheten i ett par olika lösningar och försöka besvara några av de säkerhetsfrågor som finns. Vidare fastställs vilken lösning som är bäst anpassad för smarta hem från en säkerhetssynvinkel.

Under arbetet har kommunikations protokollen som utnyttjats av ZigBee och Z-Wave analyserats på djupet ur en säkerhetssynvinkel. Potentiella brister i säkerheten betraktas och riskerna som dessa kan utgöra presenteras. Vidare sätts ett scenario upp för en Replay attack där en utomstående part fångar och skickar ut paket, och ett scenario för en Eavesdropping attack där fångad kommunikation försöker att tolkas. Resultaten av dessa scenario analyseras teoretiskt. Båda integrationslösningar jämförs med varandra och bevisar på olika sätt att de teoretiskt har tagit åtgärder för att förebygga dessa attacker.

Baserat på Z-Waves strikta protokoll och deras popularitet på marknaden väljes den för en praktisk undersökning. Ett smart hem konstrueras med den utvalda teknologin och de två scenarion som beskrivits utförs i praktiken. Resultatet av de praktiska attackerna visar att det teoretiska resultatet inte sammanfaller med det praktiska resultatet. Skillnaden beror på att den produkt som undersökts i det praktiska experimentet använde sig av ett statiskt värde istället för ett genererat slumpvärde. Detta leder till att det inte blir någon variation i kommunikations paketen vilket leder till att paket som innehåller samma kommando blir identiska. Slutsatsen som dras är att varje produkt som används i ett smart hem bör kontrolleras så att de följer riktlinjerna för hur protokollet ska användas. Om man inte har kunskap eller utrustning för att själv testa produkter kan man använda befintliga säkerhetskontroller som företag i samarbete med tillverkaren av integrationslösningen tagit fram, Z-Wave Alliance i Z-Waves fall.