Remote Control of Smart Glass

An evaluation of possible remote protocols

Degree Project Report in Computer Engineering

VICKIE DAM
STEFFI DANIEL

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2015

A Control Panel for Smart Glass
A study of different remote protocols

VICKIE DAM
STEFFI DANIEL

Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone +46 (0)31 - 772 1000
Fax: +46-(0)31-772 3663

Department of Computer Science and Engineering
Gothenburg, 2015

Acknowledgement

First, we would like to thank Pierre Skönnegård from the company CGM for giving us this opportunity to work with this thesis. We would also like to extend our thanks to supervisors Magnus Almgren and Sakib Sistek from Chalmers University of Technology for their help and support during the thesis. Finally, we would also like to give our thanks to our fellow students Anton Ekberg and Daniel Svensson, who helped us with reviewing the report.

Vickie Dam & Steffi Daniel
Göteborg, 2015

Abstract

The aim of this thesis is to evaluate some of the design decisions that go into designing a control panel, namely appropriate wireless protocols to control the smart glass. The original request came from the company CGM which owns a prototype of a smart glass which has the ability to switch between having an opaque or transparent appearance. With this ability, it is possible to replace the regular glass with smart glass or use it to screen off areas. The project was initiated by overviewing the smart glass techniques and followed by a study and evaluation on different techniques for the wireless technologies available to control the glass. The range, security and maturity of the technique are factors that CGM considers important and these parameters formed the basis for our evaluation. Additional factors such as bandwidth, interference, cost, and suitability with the smart glass are also added in order to give a better evaluation result. With the consideration of the mentioned factors and the area of usage, Bluetooth LE was recommended as the technology to use for the wireless control panel.

Keywords
Smart glass, wireless technology, Bluetooth, Wi-Fi, ZigBee, Z-wave, NFC, Infrared

Sammanfattning

Syftet med detta examensarbete är att utvärdera några av besluten som genomförs för att utforma en kontrollpanel, nämligen passande trådlös teknik som styr det smarta glaset. Förslag till arbetet kom från företaget CGM där de äger en prototyp av ett smart glas som har förmågan att skifta mellan ett ogenomskinligt och transparent läge. Med en sådan förmåga är det möjligt att ersätta det vanliga glaset med det smarta glaset eller använda det för att skärma av delar av ett rum. Arbetet initierades med att få en överblick på hur det smarta glaset fungerar. Det övergick sedan till en undersökning av olika trådlösa tekniker som kan användas för fjärrstyrning. Resultatet evaluerades utifrån viktiga faktorer såsom räckvidd, säkerhet och mognad av teknik. Andra faktorer som också spelade in i evalueringen var bandbredd, störning, kostnad och hur passande tekniken är för det smarta glaset. Med avseende på faktorerna och användningssyftet, rekommenderas Bluetooth LE som teknologin för fjärrstyrning.

Table of Contents

Abbreviations/Acronyms

AES	Advanced Encryption Standard
AGC	Automatic Gain Control
AMP	Alternate MAC/PHY
AP	Access Point
BLE	Bluetooth Low Energy
DoS	Denial of Service attack
HS	High Speed
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Thing
IR	Infrared
IrDA	Infrared Data Association
LC	Liquid Crystal
LCD	Liquid Crystal Display
LE	Low Energy
NFC	Near Field Communication
NPD-LCD	Non-Linear Polymer Dispersed Liquid Crystal Display
P2P	Peer-to-peer
PDLC	Polymer Dispersed Liquid Crystal
RF	Radio Frequency
RFID	Radio Frequency Identification
SPD	Suspended particle device
UHF	Ultra High Frequency

1. Introduction

This chapter contains the background, purpose, goal, and delimitations of the project.

1.1 Background

The idea for this project originates from the company CGM where they had the desire to commodify [1] an item known as the “smart glass”. After taking part in discussions with the company, this project was initiated. The purpose, further expanded below, is to evaluate options and technologies for a suitable control panel for the smart glass.

This smart glass has the functionality to switch between two modes when electricity is applied to it. The glass can either be transparent, darkened or depending on the technology used, have a frost-like appearance. The ON/OFF mode will allow a user to switch between a clear transparent view and a shaded one that partially blocks out the sunlight, which can be beneficial in situations where offices are exposed to sunlight for a prolonged period during the day. It can also be used as a wall to separate rooms, hence to be a noiseless and more time-effective method to change the environment when desired. For some smart glass technologies, one can also control the levels of transparency.

The technology used for the company’s current smart glass is Polymer Dispersed Liquid Crystal (PDLC). The glass contains liquid crystals that align when voltage is applied and this will allow light to pass through the glass. With no voltage the crystals move freely, causing the glass to be translucent. This particular technology only allows the glass to be transparent or translucent with no intermediate settings. The function of the glass is further described in Section 3.

1.2 Purpose

A comfortable workplace is starting to play a bigger role for some companies [2] and one way to achieve this goal is by using technologies such as the smart glass. With the use of a smart glass, it will be possible to instantly change the environment without any difficulty. There are different ways to create a control panel for the smart glass. The purpose of our project is to evaluate different wireless solutions that can be used on a remote control panel for the smart glass.

1.3 Goals

The overall goal is to commodify the smart glass for the company to present it to a prospective customer. Our task is to evaluate possible wireless technologies, where the important factors to consider are the range, security, and stability. Additional but not as important factors to consider when evaluating the results are bandwidth, interference, cost, and suitability with the smart glass.

The goal of the current project is about design and feasibility of solutions. It is intended for the panel to later be implemented in the company’s system.

1.4 Delimitations

There will not be any design or production because of the current project time limit of 10 weeks. When evaluating solutions, we are not going to consider applications for phones, as it will not be convenient for some occasions, such as meetings where usage of a phone is prohibited. We will only investigate the technologies which are relevant when using smart glass as well as the additional factors mentioned in Section 1.3 and the factors which the company considers important. When evaluating the cost of each technology, only the bill of materials will be considered, there will not be any development or shipping cost included.

2. Method

To initiate the project, various studies of the smart glass will be made in order to have a deeper understanding of the glass. These studies are the base for the comparison of the suitability between the wireless technologies and smart glass. The focus will be on the most popular glasses that are currently in the market (please note that the plan and schedule has changed throughout the project, see the Discussion in Section 6 for further details).

The second stage is to study different wireless technologies that can be used as a remote control for the glass. Information will be gathered using several articles, reports, books, websites etc. from libraries and the databases recommended by Chalmers University of Technology. The information includes brief explanations about how the wireless technology works, its characteristics, area of usage, and some security problems. An overview of different network topologies and communication models used by the wireless technologies will also be mentioned to give the reader a better understanding on how the technology works.

After a discussion with the company and with preliminary studies made from different technical articles, the chosen technologies to study are:

- Bluetooth
- Z-wave
- ZigBee
- Wi-Fi
- NFC
- Infrared

The third phase is to compare the different products on the market to determine the optimal panel for the company with dependence of the outcome from the second phase. The decided control panel will be bought and tested at the company. If no such product exists, a prototype will be created if time allows. The components required will be provided by the company.

To find the optimized solution from the chosen wireless technologies, each parameter in the table (See Table 1, next page) will be evaluated in order to meet with the minimal requirements. The middle column contains the scale we use to evaluate the parameters while the last column is the requirements that has to be fulfilled to make a conclusion. The technologies were chosen based on the area of usage and suggestions made by the company.

Parameters	**Scale used to measure the technologies**	**Requirements/Qualifications**
Range	**Low**: Below 10 m **Medium**: Between 10 to 100m **High**: Above 100 m	The range needs to be at least 10 m for indoor use (**Medium**)
Security	**Low**: No protection at all **Medium**: There are protection methods but not hard to break **High**: Strong protection methods, harder to break	The protection methods should be strong in order to prevent intrusion (**High**)
Maturity/Stability	**Low**: Newly released in the market **Medium**: Still young with not so many improved version released **High**: Been in the market for a while with improved versions released through the years	The technology must be well established and stable (**High**)
Bandwidth/Data rate	**Low**: Below 1 Mbps **Medium**: Between 1 Mbps to 10 Mbps **High**: Above 10 Mbps	The bandwidth can be minimal for the remote control used for smart glass (**Low**)
Interference	**Low**: Does not interfere with other wireless signals **Medium**: Some interference but still stable **High**: High interference with other signals	The interference should be minimum when two or more devices are in close vicinity (**Medium**)
Cost	**Cheap**: Less than 200 SEK **Medium**: 200 to 400 SEK **Expensive**: More than 400 SEK	The price for the hardware components should not cost too much (**Medium**)
Suitability with the smart glass	**Low**: Not suitable with the glass **Medium**: Can be used but not the optimal choice **High**: The technology is optimal to use with the glass	The technology should be able to reach the receiver even if the signal goes through the smart glass (**Medium**)

Table 1 - Parameters to be evaluated with the scale to be used

2.1 Evaluation of each parameter

This chapter will describe each factor that will be used to evaluate the wireless solutions.

Range

The evaluation of the range will be based on when the technology is used indoors. The meter unit will be used to measure the range and low, medium, high will be the scale for the table in the evaluation section. The scale is defined in the table above (Table 1).

Security

The security level will be based on how easy it is to perform a network intrusion and how strong the security provided for the technology is.

Maturity

The level of maturity represents how long the technology has been in use, how many bugs and faults have been reduced by further development since initial release.

Bandwidth/Data rate

The bandwidth of each technology will be mentioned together with its data rate where the scale will be in low, medium, and high.

Interference

The signal interference will be measured in scale high, medium, and low where interference refers to coexistence with other wireless technologies.

Cost

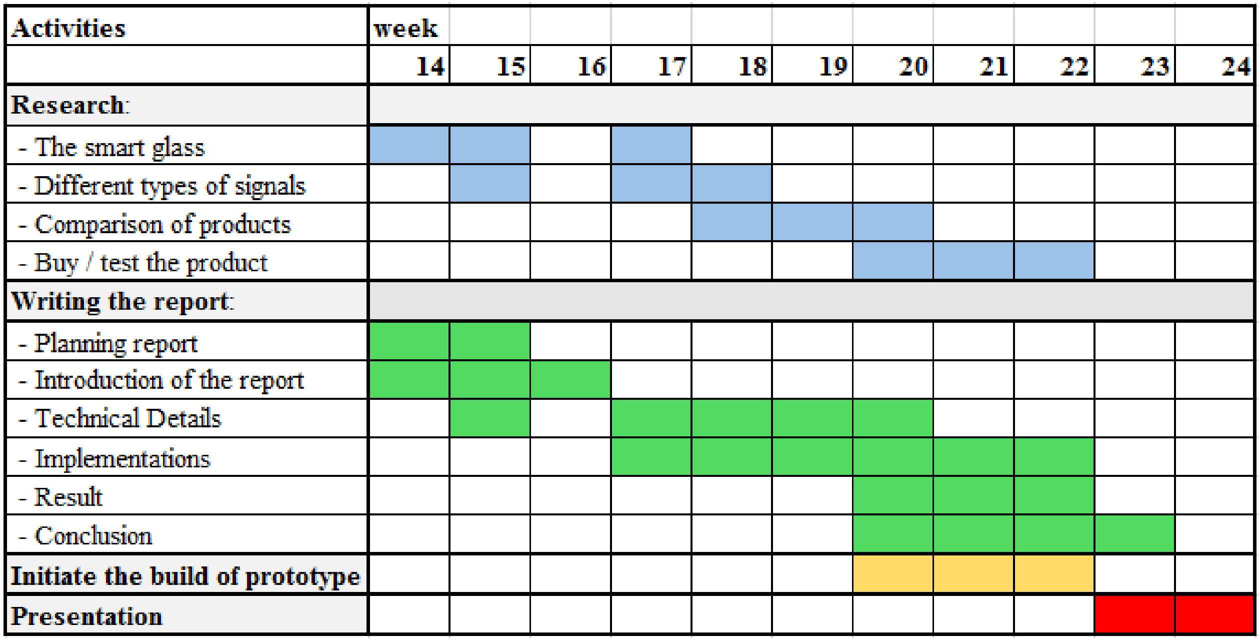
The prices will be very roughly estimated as to know exactly what components are necessary or which ones are unnecessary to build a remote control for all technologies is not possible within the time frame. The most mentioned component will be the module as it is the core of the hardware. Other materials such as power source and cable will not be mentioned since they are standard tools for developing hardware. The prices will vary depending on where the component is purchased. The price will only represent the bill of materials, other costs e.g. development, testing, shipping fee are not included.

Suitability with the smart glass

The suitability parameter represents an evaluation of how the signal itself is compatible with the smart glass. The signal will not be suitable for smart glass if it is unable to pass through the glass in order to reach the receiver. The smart glass contains many different layers and materials inside, making it hard to know the result without doing experiments. Because no experiment will be conducted to test this, the evaluation will be based on knowledge of which materials interfere with the signal and which do not.

2.2 Timeline

In order to complete the project, the schedule below should be followed (Section 2 must be read in order to comprehend the table):



Activities	week										
	14	15	16	17	18	19	20	21	22	23	24
Research:											
- The smart glass	🟦	🟦		🟦							
- Different types of signals		🟦		🟦	🟦						
- Comparison of products					🟦	🟦	🟦				
- Buy / test the product							🟦	🟦	🟦		
Writing the report:											
- Planning report	🟩	🟩									
- Introduction of the report	🟩	🟩	🟩								
- Technical Details		🟩		🟩	🟩	🟩	🟩				
- Implementations				🟩	🟩	🟩	🟩	🟩	🟩		
- Result							🟩	🟩	🟩		
- Conclusion							🟩	🟩	🟩	🟩	
Initiate the build of prototype							🟨	🟨	🟨		
Presentation										🟥	🟥

Table 2 - Timeline for the project

3. The Smart Glass

This chapter contains brief descriptions of different smart glass technologies currently used in the market.

3.1 Introduction of the smart glass

To satisfy humanity's daily usage of energy in today's society, the demand for natural resources has increased tremendously these past decades [3]. New energy efficient technologies are required if we want to reach a sustainable development. Smart glass or smart windows could be one of these technologies to help us reach such a goal. With smart windows, it would be possible to block light and thus preventing the room from heating up. This will allow the households and companies to save money, as they do not have to overuse any form of cooling system. By blocking UV radiation, many objects will be protected from damage, especially objects located near the window. Once turned on (or off depending on the type of smart glass), the smart glass/window will allow electricity to pass through it, causing a nearly instant change in opacity. There are many technologies for this type of glass, but this report will only mention Liquid Crystal, Electrochromic, and Suspended Particle Device (mentioned in the next sections) as they are the most common when it comes to smart glass/window. A common trait they share is the small energy consumption needed to keep the glass running.

3.2 Liquid Crystals

3.2.1 History of Liquid Crystal

The discovery of what we know today as Liquid Crystal (LC) began in the late 1800s by an Austrian named Friedrich Reinitzer [4]. He discovered the liquid crystalline nature of cholesterol extracted from carrots. This work has been studied and researched by different scientists and companies for over a century. In the late 1900s, the Liquid Crystal Display (LCD) was invented and is now used worldwide in monitors and smartphones [5].

Not only has this technology been used in electronics but also for glass applications. There are currently three generations of LC glass in the market where the generations are decided by the manufacturing technology.

3.2.2 First Generation - Nematic Curvilinear Aligned Phase

The first LC generation is using Emulsion Technology, also called Nematic Curvilinear Aligned Phase, where the technology uses water soluble polyvinyl alcohol to disperse liquid crystal droplets [6]. This technology is very sensitive to moisture, so laminated glass is required to make sure the smart glass will not be defective [6]. Since the patent expired, most manufacturers have joined the newer generations of LC technology.

3.2.3 Second Generation - Polymer Dispersed Liquid Crystals

Polymer dispersed liquid crystal (PDLC) is the second generation technology of LC. It consists of liquid crystals dispersed in a polymer matrix. The mixture is placed between two layers of glass or any kind of transparent material, with conductive coating to conduct electricity to the liquid crystals [7] (see Figure 1). The particles will instantly be aligned when voltage is applied, which will turn the glass transparent. Without voltage applied, the glass will have an opaque effect making it impossible to see through, which can be used to screen off areas when privacy is needed. However, with this technique the glass lacks the ability to control the level of transparency and can only switch between transparent or opaque.

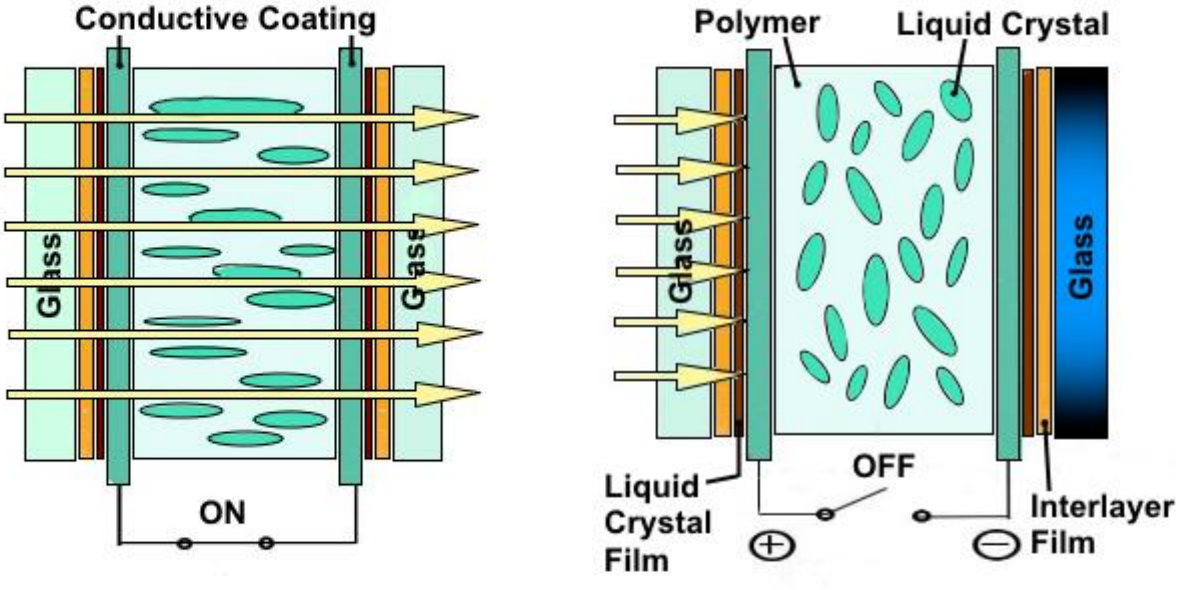


Figure 1 – Polymer Dispersed Liquid Crystal [8]

3.2.4 Third Generation - Non-Linear Polymer Dispersed Liquid Crystal

Non-Linear Polymer Dispersed Liquid Crystal Display (NPD-LCD) is the third generation of the liquid crystal technology with improved basic features of smart glass, such as lower driving voltage and higher UV resistance [6]. Unlike older generations which had to be protected using glass lamination from moisture that can harm the film, this new film has an improved moisture sensitivity [6]. The sensitivity is improved by using techniques involving silicon and fluorine that contain polymer which are commonly used in the fabrication of cookware. The change from being more moisture resistant allows the film to be directly put on the window like a regular tape using optical glue. Without the use of glass lamination which require costly industrial process development, the cost for this film is reduced [6].

3.3 Electrochromics

Electrochromics is based on the idea of substances getting electrified by charged electrodes, altering their color. The process is known as electrochromism and this technology is used to create electrochromic glass [9]. With a voltage applied, the glass will turn dark and while in absence of voltage the glass will turn transparent. Depending on the level of voltage added, the level of transparency can be controlled.

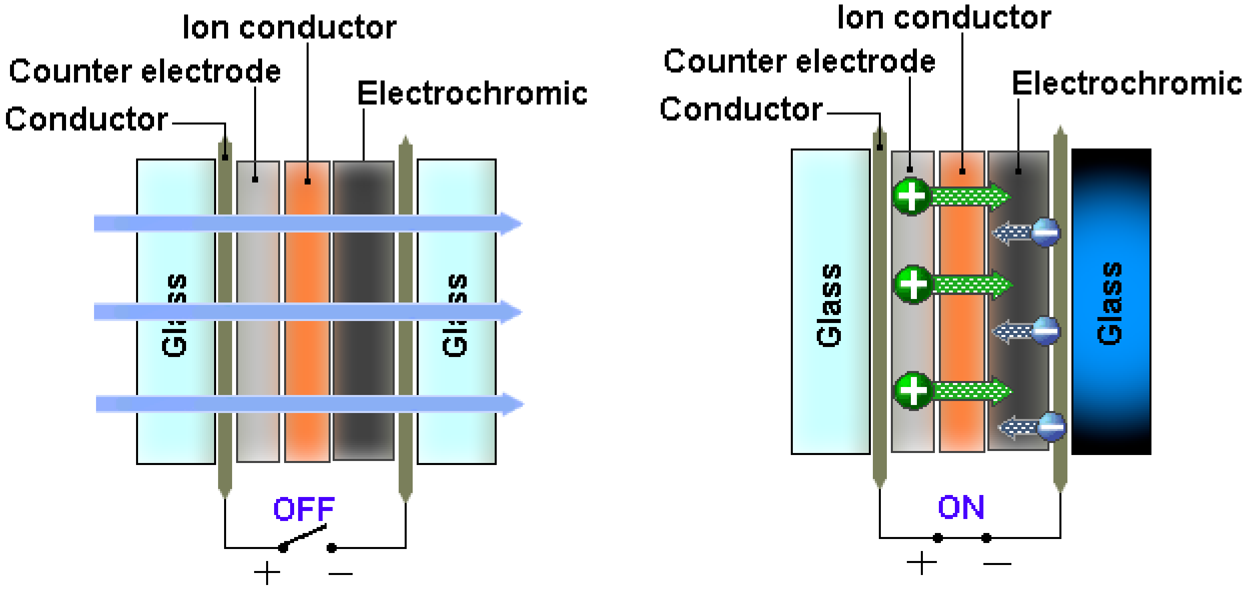


Figure 2 – Electrochromic glass [10]

The electrochromic window consists of 5 thin layers of materials. An ion conductor in the middle followed by an electrochromic layer of the outer part of the window. On the inner side of the window there is the counter electrode layer, and the window ends up with a transparent conductive layer on each side (see Figure 2 above). Positive charged lithium atoms, also known as ions, move back and forth between the electrodes through the ion conductor [11]. When voltage is applied, the ions move to the side facing the sun, blocking the sunlight. It works the opposite way when no voltage is applied. The ions will then move to the other side causing the window to be transparent. The change of color (usually blue) can take several minutes to complete depending on the size of the window. The change of color starts from the corner of the glass and moves towards the middle [12]. Once the glass has darkened, it will have the ability to absorb UV radiation [13]. The glass is not intended for privacy, since the glass can be seen through even in its darkened state. This makes the glass more suitable as a window or wall in the outer part of the building.

3.4 Suspended Particle Devices (SPDs)

SPD, Suspended Particle Device, is one of the technologies used in the smart-window application. A SPD glass is made of two panes of glass, coated with conductive material [14]. Between the panes, there is liquid suspension which allows millions of rod-like particles to float freely (see Figure 3). These particles are known as suspended particle devices. When voltage is applied with the help of the conductive material the SPD will align and an effect of a transparent window will occur. When no voltage is applied, the particles will float randomly and work as an obstacle to block light with a dark blue shade appearance. The change between the transparent and tint appearance is instant once the voltage is applied or turned off. It is also possible to control the level of transparency if desired by simply applying less or more voltage into the SPD glass.

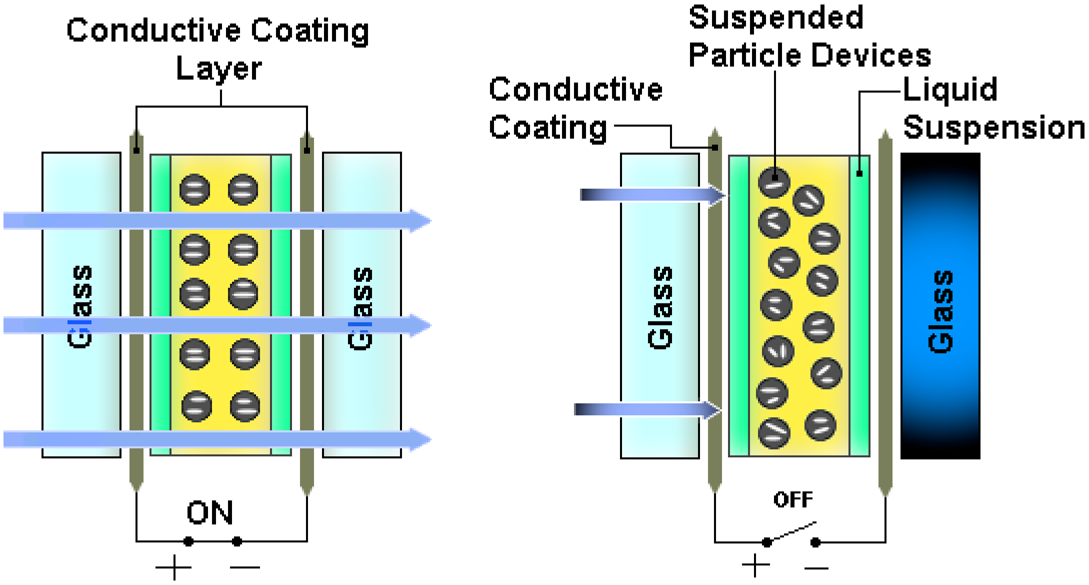


Figure 3 – Suspended Particle Devices [15]

4. Overview of Networks

In this chapter, both the background information of different transmission protocols and the network topologies and models that are used in the technologies will be elaborated.

4.1 Network Topologies

4.1.1 Mesh Network

A mesh network topology contains nodes where each node distributes or is distributing data for the network by relaying data to one another. Each node contains information about the accessible nodes in its close vicinity. These can be read as a list by the start node in order to determine the shortest route towards the destination [16]. To have a full mesh topology, all nodes in the network must have a connection to each other (see Figure 4). This allows the network to be more stable as there are more paths to take even if some nodes malfunction. Another alternative is a partially connected mesh topology where at least two nodes must have a connection to multiple nodes in the network.

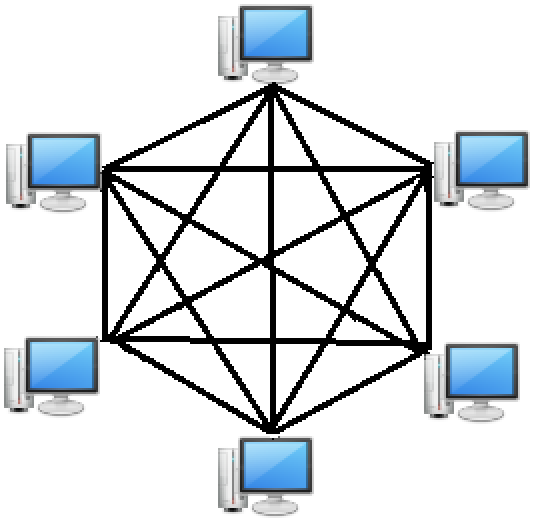


Figure 4 - Full Mesh Topology [17]

4.1.2 Star Network

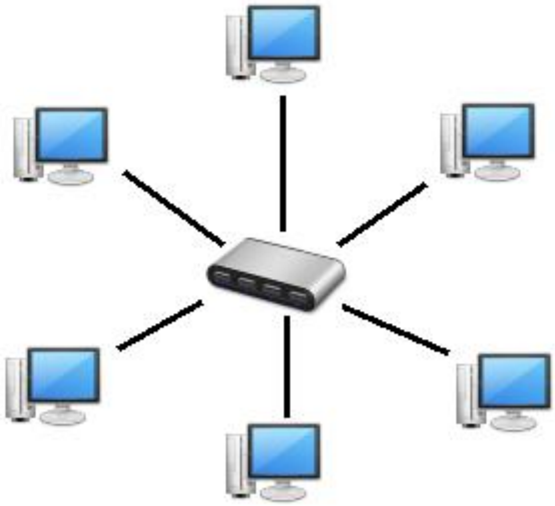


Figure 5 - Star Topology [20]

In a star network topology, every node is connected to a central node like a hub or switch (see Figure 5) [18]. The central node acts like a server while the rest are connected to the node as clients. A sending node transmits the data signal to the central node, which retransmits the signal to all other nodes. Each node checks the destination address of the signal and if the address does not match with its own, the signal will be dropped [19]. With a star topology it is easy to monitor each node in the network but if the central node fails the network will be down.

4.1.3 Tree Network

The tree topology consists of one central node (root of the tree) connected to more star networks [21]. This allows the star networks to communicate with each other, hence expanding the network. If the root node fails, the connection between the star networks will be lost but the nodes within its own network will still be able to communicate as long as the central node in the network is still functioning [22].

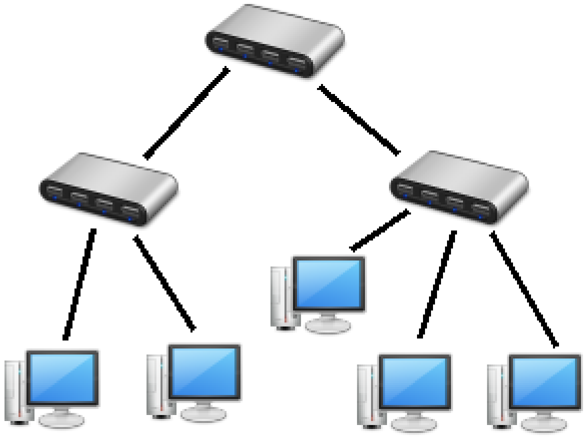


Figure 6 - Tree Topology [22]

4.2 Network communication models

4.2.1 Master/slave Network

In a master/slave topology, the device that initiates and commands the data transmission is the master and the devices responding and following orders are the slaves. A master is allowed to have many slaves and can request data transmission from and to their slaves [23]. On the other side, the slaves can only belong to one master, meaning they are prohibited to communicate with other nodes apart from their master. This includes communicating with other slaves in the network.

4.2.2 Peer to Peer Network

Peer-to-peer (P2P) is a topology where each node (or peer) in the network has the capability to initiate a communication session. Each node can request and transmit without a centralized administrative system like the client/server model, thus allowing each node to have the function of a client and server. P2P software is mostly used for file sharing between users. Due to the easy and convenient sharing system, many software piracy and illegal sharing has occurred using P2P [24].

4.3 Wireless Technologies

4.3.1 Bluetooth

This wireless technology uses the short-wavelength Ultra High Frequency (UHF) radio waves for exchanging data over short distances from one device to another. It was first developed by the telecom company Ericsson in the 1990s with the purpose of replacing the RS-232 [25] data cables used for serial communication [26]. Bluetooth can connect to several devices using the master/slave network (explained in Section 4.2.1) to control the transmission of data. Bluetooth operates between 2.4 GHz and 2.485 GHz. The technology uses the spread-spectrum frequency-hopping technique which allows it to hop between the randomly chosen frequencies within the range. With this technique, it is possible to avoid interference with devices using the same band [27]. Because Wi-Fi (described in Section 4.3.4) and ZigBee (described in Section 4.3.3) also operate in that band, interference might occur when transmitting data. The data rate varies from 1-24 Mbps depending on the Bluetooth technology [28]. The range for Bluetooth can vary depending on the use case and class of radio used in the implementation. The manufacturer can also tune the implementation to suit his/her own use case [27]. Class 3 radios have a range of 1 m and class 2 radios have a range of 10 m, which is used for mobile phones and remotes. For industrial purposes the range is up to 100 m where class 1 radio is used.

With the Bluetooth technology it is possible to share data with another connected device. Voice, music, and other files are sharable as long as the devices are paired with each other. Depending on which Bluetooth technology is implemented on the device, the technology can be used in cars, headset, mobile phones, computers etc. [29] (different Bluetooth versions will be mentioned in the next sections).

Bluetooth offers fast and easy connections between devices but it does not come without risks. There are several known threats and security issues, such as DoS, eavesdropping, message modification, and resource misappropriation [30]. These are general threats for wireless networks while bluesnarfing, bluejacking, bluebugging, car whisperer etc. are Bluetooth-specific attacks [30]. Depending on what the Bluetooth will be used for, countermeasures should be applied using the recommendations by NIST when creating the device [30]. These threats are more towards devices with the risk of getting information stolen, such as mobile phones.

4.3.1.1 Bluetooth Classic

The features in the classic version of Bluetooth provide a stable connection between devices. To keep it stable for long range communication, the latency must be low. The technology has an ability to continuously stream data with high transmission speed, which can make it consume more power than other versions of Bluetooth. This version is more used for cars, headsets, and industrial controllers because of its ability to continuously stream data [31]. If the version is used for industrial purposes, the range can be up to 100 m. The usual data rate for Bluetooth Classic varies from 1-3 Mbps.

4.3.1.2 Bluetooth Low Energy

Bluetooth Low Energy (Bluetooth LE or BLE) is a technology designed to consume little energy by implementing an idle mode [32]. BLE was introduced in Bluetooth version 4.0 with the Internet of Things (IoTs) in mind [33]. This version has many features implemented from Bluetooth Classic and in order not to use much power, it only supports small data packets with a transfer speed of 1 Mbps [32]. The range of BLE is not bound to the specification which allows the manufacturer to optimize the range to over 100 m [32]. The devices using this technology commonly use a coin cell battery which can last for many years without the need to change it [34]. Compared with the ordinary master/slave communication, this version can have a larger number of slaves depending on the available memory of the device [31]. This technology is useful for small data transfer that needs to be transferred in intervals. In cases when the devices are required to be further away from each other, this might not be the ideal technology. BLE is used for smartphones and tablets that have to communicate with for example, coin cell battery-operated sensors in fitness applications.

4.3.1.3 Bluetooth 3.0 + High Speed

Bluetooth High Speed (HS) technology was released in 2009 with the completed Bluetooth Core Specification 3.0 + HS. Alternate MAC/PHY (AMP) is the official name of the transport link which allows devices to use well-known Bluetooth protocols while having a high throughput of 24 Mbps with the use of a secondary radio [35]. AMP will enable the Bluetooth radio to discover other high speed devices when transferring data. The transceiver has higher security compared to older versions. The use of this technology does not consume much energy because it is only activated when file transfer is requested. The speed of the transfer is very high making the transfer time shorter, thus lowers the energy consumption [35]. When sending packages of data at high speed, the latency can be lowered and the data transmission will not be delayed. Bluetooth High Speed designed with focus on speed rather than range and thus the standard range for this version is around 10 m.

4.3.1.4 Bluetooth version 4.2

On December 2014, a new Bluetooth version was released with improved features specified for Internet of Things (IoTs) improving the previous versions of 4.0 and 4.1 [36]. The key features include the ability to extend the reach of power-efficient devices to Internet which allows a sensor to access the Internet through a gateway device [36]. It also has improved the LE privacy, preventing Bluetooth devices from being tracked. Another improvement made is better energy efficiency [36]. The upgrade for faster data transfer has been done by a feature called LE Data

Length Extension [36]. Bluetooth 4.2 is not supposed to replace the previous version for BLE but to extend its functionalities.

4.3.2 Z-wave

The Z-wave protocol, a proprietary technology from Sigma Designs, is designed for home automation [37] [38]. Depending on where the Z-wave product is used the frequency varies [39]. It uses a mesh network to transfer and receive data between the starting point and endpoint. The use of mesh networks allows the range to be up to 100 m [40].

Unlike other protocols, Z-wave does not interfere with other wireless technologies because the protocol operates in the 1 GHz sub-band instead of the 2.4 GHz band [41]. Since this technology is energy efficient and wireless, it is easy to install and use. Devices using Z-wave work on batteries and last for at least a year because of its low data rate of 100 kbps [40] [41]. After each command there will be a notification requesting a confirmation to apply the action in order to let the user know the command is acknowledged.

With the use of home automation, one or more computers can automatically or remotely control the basic home functions. Home automation can include controlling the lights, heating, and alarm system. The purpose for automated homes is to make the house more comfortable and convenient for its inhabitants. Z-wave is a licensed technology used in home automation and in order to develop a product, the developer’s kit must be purchased [42]. Some of the devices using Z-wave are locks and sensors mechanisms for the door [43].

In a computer security conference Black Hat 2013, and an annual hacker convention DEF CON 21, several topics about attacking home automated houses were mentioned [44]. During the DEF CON 21, it was pointed out that the capture of Z-wave’s Advanced Encryption Standard (AES) key was possible [45]. There have not been many practical researches made on this technology, making it harder to understand the level of security.

4.3.3 ZigBee

Over these past years, ZigBee has grown rapidly in the market and can be found in many devices, such as remote controls [38]. This protocol is a wireless communication standard, standardized by the Institute of Electrical and Electronics Engineers (IEEE) using the 802.15.4 standard and operating in the 2.4 GHz frequency band globally (not country specific) with the transmission range of 50 m [46]. For outdoor industry use case, ZigBee can reach the range of 1000 m and if the device is amplified, the range can go up to 4000 m. ZigBee supports three different network topologies which are star, tree and mesh network topology. Each of them have their own advantages and can be used in different situations. This protocol is implemented with a power saving application and, together with its low data rate of 250 kbps, allows ZigBee devices to have low energy consumption [47] [48]. ZigBee is capable of supporting more than 64 000 nodes in the network [48]. However, the downside of using ZigBee is that some devices have difficulties communicating with other devices made by a different manufacturer [37]. ZigBee has also problems coexisting with other wireless technologies, especially Wi-Fi [49]. There is a study made by Microsoft on how to avoid the interference [49].

ZigBee can be used in various areas, such as home automation, wireless sensor networks, industrial control etc. [50]. Unlike Z-wave (described in Section 4.3.2), this protocol is not licensed but it is widely spread among people. In order to use ZigBee for commercial purposes, the ZigBee Alliance standard must be fulfilled [51].

There are some of attacks that can be used on the ZigBee technology, and they can generally be split into three categories: physical attacks, key attacks, and replay & injection attacks. A physical attack means the hacker can physically interact with the device and access the encryption key using the fact that the hard-coded key is flashed in the ZigBee device and later transferred to the RAM during the power up [52]. The hacker can also create a device that mimics a node on the network to capture packets during the transmission. The captured packets can be decrypted or analyzed, and this type of attack is categorized as key attack [52]. The last category, Replay & Injection Attack, is when the hacker replays or injects fake packets to the ZigBee device and tricks it into doing unauthorized actions [52]. The Replay & Injection Attack is possible when it is combined with the key attack. Improvements have been made through the years but a full prevention method to stop the hackers from attacking the network has yet to be found. Most ZigBee devices require some security solutions designed into the device [53]. For home automation, the owner of the house can install a sensor to detect when some unauthorized intruder has entered. The owner will be notified about the intrusion and can contact the police if needed.

4.3.4 Wi-Fi

Wi-Fi is a networking technology that allows users to have access to Internet without any physical wired connection to the device. With a Wi-Fi antenna, it uses radio signals to send and receive data between users. To be able to send data using radio signal, the end device must have a Wi-Fi card or adapter to convert the data into radio signals. Access points (APs) act like central transmitters and receivers for the signals. In wireless home networks, most routers have an AP included.

Two frequency bands of 2.4 GHz or 5 GHz are used to be able to carry more data for the transmission. The data rate of Wi-Fi varies depending on which IEEE standard it uses. Older standards of Wi-Fi could go up to a data rate of 11 Mbps, while a transmission speed over 100 Mbps can be reached with newer standards [54]. Wi- Fi has a mechanism to reduce its data rates when other wireless technologies are detected in order to avoid interference [34]. The use of this technology also consumes more power because its high throughput [38], which might not be ideal for battery-based devices that do not have enough power to support it.

Wi-Fi is one of the most-used internet connection technologies for both commercial and non-commercial purposes [55]. Except for connecting to the Internet, Wi-Fi can also be used for connecting smartphones and tablets with for example lamps and printers. When the devices are connected to Wi-Fi, it will be possible for them to communicate with each other. The range of Wi-Fi varies depending on the manufacturer and area of usage. An example of range for GoPro is approximately 150 m [56].

A wireless network does not require physical connections, thus making it easier for a third party to hack inside the network, making it more vulnerable to attacks [57]. If the network does not have any security features, the intrusion can remain undetected. One common type of attack is the sniffer attack, which is an application that can capture packets on the network. With a sniffer it is possible to analyze the network and obtain information to cause the network to crash or be corrupted [58]. Another type of attack is the Denial-of-Service (DoS) where the hacker can overload the network with data traffic, causing the network to shut down [58]. These attacks are more common for Internet networks where packets contain more information useful to the hacker. That makes Wi-Fi without any security measures a vulnerable target. There are more common network attacks and solutions to prevent them, but as the technology keeps progressing, there will be new vulnerabilities or holes for hackers to exploit [58].

4.3.5 NFC

Near Field Communication (NFC) was first used in Star Wars character toys in 1997 and was later implemented in 2010 to Android phones. NFC transfers data within a very close range which allows the devices to establish P2P communication (described in Section 4.2.2) and exchange information without the need of pairing like Bluetooth. NFC operates in the frequency band 13.56 MHz with the transmission speed of either 106, 212 or 424 kbps [59].

NFC is the newer version of Radio Frequency Identification (RFID) communication. The biggest difference between them is the range where RFID has a wide range which makes it easier to attack [59]. With NFC the range is around approximately 5 cm, making it harder for attackers to hack because of the short range.

For NFC to be able to communicate, it needs a NFC card. This card is an integrated smart card that has a secure microcontroller and an integrated memory to increase the security. The smart card must have power supply from the device where it is inserted. There are three types of smart cards but the most used for NFC is the wireless smart card. This wireless smart card communicates only when the devices are close to each other, which lowers the probability for interception. The reasons for using the smart card is to increase the security as well as enabling higher energy transfer [59].

The technology uses tags which are microchips that store a small amount of information to be later read by a NFC device [60]. These tags are for example wristbands or stickers containing small microchips with antennas. If a person has a NFC-tag, he can use it for commercial and non-commercial purposes. NFC is used when people wish to pay with their commuting cards for services such as public transportation. Some hotels also use a NFC card to open the rooms. Nowadays this technology has been implemented in some smartphones and tablets [61].

There are various attacks that can affect the NFC technology [62]. These attacks are not specially aimed for hacking NFC but are common attacks in the general network security. One type of attack is eavesdropping where the attacker can record communication between the devices and thus steal or corrupt the transmitted information. Data corruption is a form of DoS attack where the attacker can block or disturb the data flow by fluctuating radio signals to reduce the signal into random noises. Because NFC is used for transmitting sensitive data, it is of highest priority to make sure it is secure even if close proximity is required for the attacks.

4.3.6 Infrared - IrDA

William Herschel was a German astronomer who discovered a type of invisible electromagnetic radiation in the beginning of 1800s [63]. He conducted an experiment by placing thermometers within each color of the visible spectrum and measured the temperature difference. The temperature increased from blue to red but he noticed an even warmer temperature beyond the color red in the visible spectrum [63]. The discovery came to be known as infrared (IR).

Ordinary remote controls using IR have a transmitter but no receiver. The remote control generates particular digits into a sequence which are then transmitted as multiple IR signals. These signals are rapid ON and OFF pulses, which will be detected by an IR receiver. The receiver, attached to another device, will reconstitute the cycle to the original sequence. The frequency of the on/off cycle differs among manufacturers. The lowest frequency used is 32.75 kHz and highest is 56.8 kHz with 38 kHz being the most common carrier frequency [64]. In order for IR receivers to distinguish which signal to accept due to different kind of lights, the receivers have an optical filter to let the infrared pass while rejecting lights in the visible spectrum. Signals sent from a greater distance will lose strength as they approach the receiver. In order for the signal to be stabilized, the receiver module contains an Automatic Gain Control (AGC) which increases or decreases the signal amplification. When the signal pass through the ACG, the incoming carrier signal is bandpass filtered to reduce interference from other light sources. High frequency lightning devices, such as fluorescent lamp can cause stronger interference on the IR remote control [65]. The bandpass filter compares the carrier frequency with the receiver frequency [64].

Infrared Data Association (IrDA) is using the infrared spectrum to send data. This technique is commonly used in telecommunications and mobile phones. While using IrDA provides a low energy consumption and good security when used correctly, it has downsides of having short range of approximately 1 m and the connection can only be established if the two devices are in direct line-of-sight [66] [67].

For IrDA which has the direct line-of-sight requirement between the transmitter and receiver, there is no security provided at the link layer but instead it relies on the upper level protocols and applications [68]. The encryption and authorization are managed by the application layer. It is possible to eavesdrop a communication between the transmitter and receiver by detecting reflecting light and filter out the ambient noise assuming that the line-of-sight and range requirements are fulfilled.

5. Evaluation argument

This chapter contains arguments for each parameter found in the requirement table (Table 1, mentioned in Section 2). On each parameter, the technologies mentioned in this report will be evaluated according to the table located at Section 5.8 (Table 3).

5.1 Range

Bluetooth

As mentioned in the previous chapter (Section 4.3.1), the range for Bluetooth technologies vary depending on the use case, manufacturer, and class of radio used in the implementation. When the classic version of Bluetooth is used for industrial purposes, class 1 radio will be implemented which allows the range to be up to 100 m. In other areas of usage, for example a headset connected to the phone, a class 2 radio is used which have a range of 10 m. Bluetooth High speed has a standard range of 10 m which gives the scale medium (described in Section 4.3.1.3) while BLE normally has a range of 10 m but it can also have a range of over 100 m depending on how the manufacturers optimized the device.

Z-wave

Z-waves uses mesh network, which allows the technology to extend its range if needed by adding nodes in the network. The average range for Z-wave is 100 meters (see Section 4.3.2) which makes it medium in the range measurement, but it depends mostly on the use case. Devices designed for indoor use has a shorter range while for outdoor the range is considerably longer.

ZigBee

ZigBee can be used in many areas therefore the range can have a big variation, especially if the technology is used outdoors. For indoor use, the range is around 10 m while for outdoor use the range can be up to 4000 m with an amplifier (mentioned in Section 4.3.3). Otherwise the range of ZigBee is roughly 50 m without considering the environment, giving it medium in the range measurement.

Wi-Fi

Wi-Fi can be used in many areas thus the range varies like many of the other technologies (described in Section 4.3.4). Depending on type of antenna, transmission power, and the environment, the range can be limited for an indoor wireless router but still be big enough to support for example a campus. The range for outdoor arrangements can be extended with many kilometers between the AP stations.

NFC

As mentioned in Section 4.3.5, NFC has the shortest range of 10 cm which gives it a low measurement for range. With this range, the device must be really close to the receiver to function.

Infrared - IrDA

The infrared technology has a range of with 1 m with IrDA (see Section 4.3.6). While the distance between the transmitter and receiver is acceptable, the problem with IrDA lies in the line-of-sight requirement when transferring data. This could cause signal losses and inconvenience for the ones using the remote.

5.2 Security

Bluetooth

There have been network attacks reported on the Bluetooth technology but because the technology is used differently depending on the area of usage, there are recommendations to prevent them (mentioned in Section 4.3.1). Some devices are stronger against one kind of attack while being weaker to another, which is why the application area is important for adjusting what kind of prevention should be focused on. This makes the level of security relatively high for Bluetooth.

Z-wave

Mentioned in the previous chapter (Section 4.3.2) there have not been many researches made on Z-wave technology, mainly because it is a proprietary standard. However, the possibility of attacking the network has been mentioned in a security conference (See Section 4.3.2). Because of the possibility to capture the AES key (described in Section 4.3.2), thus giving an outsider the power to control the transmission, the security of Z-wave is considered as medium. Despite the fact that the AES key can be captured, the technology still comes with a certain level of security

ZigBee

Flaws have been discovered for the home automation technology ZigBee where the attackers can easily perform a sniffing attack on the system with a software available on the Internet network [69]. It is also possible for a hacker to access the encryption key by doing physical attacks (see Section 4.3.3). The security level for ZigBee can be considered as high but not as high as Wi-Fi and Bluetooth. The level also depends on the application area where different functionalities are focused on e.g. a smart lighting system does not require as high security as a burglar alarm system would.

Wi-Fi

Wi-Fi can be easily exploited if the range is too large, thus allowing unwelcome intrusions especially when there is no protection available e.g. an antivirus software and firewall. Despite that, the security of Wi-Fi is still considered high because it is widely associated with the Internet where there are high risks for encountering unwanted intrusions and malware (mentioned in Section 4.3.4). The security for Wi-Fi is constantly going through improvements where many studies and researches are being made in order to update the database with more recent protection methods against possible threats. Even so, new threats are always being discovered as new holes in the network appear together with the improvements.

NFC

One of the strong points in the security of NFC is the short range, making it harder for a hacker to sniff data (described in Section 4.3.5). In order to sniff data the hacker must be relatively close to the device in order to intercept signals. Besides the close range requirement there are other protection methods implemented for NFC. Because this technology can be used for handling payment purposes such as storing credit card information, the security concern is far most the highest priority for this technology, making the security level pretty high.

Infrared - IrDA

The security of Infrared is considered high because of the line-of-sight requirement. The signal can be stopped by an obstacle or wall, causing the signal to be lost, which makes it hard to intercept. Protocols and applications on devices using IrDA should provide secure authentication and encryption implementations as the link layer has no security provided (mentioned in Section 4.3.6).

5.3 Maturity of the technology

Bluetooth

The high maturity of Bluetooth can be proven by the fact it has been widely used for over a decade (see Section 4.3.1). Many versions have been released through the years, covering many usage areas and improvements since its initial release. The latest release is the Bluetooth 4.2, which came out on December 2014.

Z-wave

The Z-wave protocol is relatively new compared to Bluetooth and because it is a proprietary standard, the specifications are only available within the alliance of Z-wave. Unlike ZigBee where the specifications are open to the public and where tests are performed by many, Z-wave is more restricted within its manufacturers. Z-wave is still making efforts to improve the IoTs and has yet to reach its peak as there are more improvements to make, such as the security problem.

ZigBee

ZigBee is a known technology for home automation where for non-commercial purposes, the specification is open to the public. Because it is open to the public, more tests and studies have been made by different developers, leading to fast improvements. ZigBee is used in various areas with many versions released to match different usage and environments, which gives the technology a high maturity level.

Wi-Fi

Wi-Fi is one of the most used technology around the world and it has been in use for a long time since the wireless Internet technique was introduced. Many improvements have been made in order to make Wi-Fi more efficient, which include improved security, data rate etc. Different studies and discussions can be found about the Wi-Fi technology around the world. The fact that Wi-Fi has gone through several improvements since its breakthrough makes the maturity of Wi-Fi high.

NFC

The use of NFC is still continuing to spread across Europe, Asia, and the United States. As it is relatively new compared to Bluetooth and Wi-Fi, the technology is not considered to be well established in the market yet as improvements and innovations can still be made before it hits its peak. The technology may be fresh but it is still stable for its current area of usages, which makes this technology medium in matters of maturity.

Infrared - IrDA

Infrared is one of the oldest wireless technology and used in a very big area scale, from simple remote controls to military purposes like heat detector for guided missiles. Infrared itself cannot be improved because it is an invisible electromagnetic radiation. However the different techniques using the radiation can and have been improved to maximize the utilization of infrared, making the maturity of the technology high. The infrared television remote control technology has existed for over a half century and it is still being used in many use cases.

5.4 Bandwidth/Data rate

Bluetooth

The Bluetooth technology operates in an unlicensed band at 2.4-2.48 GHz. The data rate can vary between 1 to 24 Mbps depending on the design of the Bluetooth technology, the version with the lowest data rate is BLE with 1 Mbps while Bluetooth High Speed being the highest with 24 Mbps. Bluetooth Classic can vary between 1-3 Mbps.

Z-wave

The technology operates in the 1 GHz sub-band instead of the 2.4 GHz band like most wireless technologies. With a data rate up to 100 kbps, the technology does not require much power to transmit data packets.

ZigBee

ZigBee operates in the band 2.4 GHz band like most wireless technologies do, causing chances for interference. The data rate for ZigBee is 250 kbps which is lower than Bluetooth and NFC but it is designed for lower power consumption rather than high data rate.

Wi-Fi

The technology can operate in the 2.4 GHz or 5 GHz which can carry more data if the device is close to the AP. It also has more bandwidth compared to the 2.4 GHz frequency. The data rate of Wi-Fi depends on which IEEE standard is used and can be adjusted to suit the use case. In the newer standards, the transmission speed can reach more than 100 Mbps.

NFC

NFC operates in the frequency band 13.56 MHz with the transmission speed of 106 kbps, 212 kbps or 424 kbps, which is slower than Bluetooth but faster than Z-wave and ZigBee. Unlike Bluetooth, NFC does not require pairing and the connection between the devices are almost instantaneous.

Infrared -IrDA

IrDA has a big variation of the frequency band of 32.75 - 56.8 kHz and with a data rate of 4 Mbps, this technology does not consume a lot of energy (mentioned in Section 4.3.6). The transmission speed of IrDA is slightly higher than BLE but lower than Bluetooth HS.

5.5 Interference

Bluetooth

The Bluetooth technology operates in an unlicensed band at 2.4-2.48 GHz. With many Bluetooth devices close to each other, interference might occur and in order to avoid that, the spread spectrum frequency-hopping technique is implemented (mentioned in Section 4.3.1). The avoidance of interference does not only apply to the Bluetooth devices in close proximity but to all wireless technologies using the same 2.4 GHz band.

Z-wave

The technology operates in the 1 GHz sub-band instead of the 2.4 GHz band like most wireless technologies. Operating in the sub-band allows the technology to avoid interference with other technologies, making it more coexisting friendly.

ZigBee

ZigBee operates in the band 2.4 GHz band like most wireless technologies do, causing chances for interference. Studies have been made to prove that ZigBee have problems coexisting with other devices made by different manufacturers (mentioned in Section 4.3.3) and especially interference with Wi-Fi. However, ZigBee is still going through iterative improvements which in the future might decrease the interference level and improve the coexistence with other wireless technologies.

Wi-Fi

The technology can operate in the 2.4 GHz or 5 GHz band which has more bandwidth compared to the 2.4 GHz frequency. The lower frequency can communicate at a bigger distance away from the AP but might have bigger chances of interference with other devices in the same room or as far the range reaches.

NFC

NFC operates in the frequency band 13.56 MHz which usually is used for bandwidth experiments to avoid interference from other RF devices. Since it operates in another band, it has no problem coexisting with other wireless technologies.

Infrared - IrDA

IrDA has a big variation of the frequency band of 32.75 - 56.8 kHz, where 38 kHz is normally used. High frequency fluorescent lightning devices can cause interference problems when used together with an IR wireless remote control (mentioned in Section 4.3.6). With its limited range and line-of-sight requirement, the user can adjust the angle and range to make sure less interference will occur during the performance.

5.6 Cost of initial development

Bluetooth

The cost for the Bluetooth components is roughly 400 SEK when building a device where the module costs approximately 300 SEK, antenna 50 SEK, and other components e.g. transceiver 30 SEK [70] [71]. The sum of the cost is for development purposes while components bought in bulk are considerably cheaper per unit. The price varies depending on manufacturer and the specifications of the hardware. The more powerful specification the more a component will cost.

Z-wave

Z-wave is designed in such a way that it should be easy to implement a Z-wave end-device. A Z-wave development kit which is a platform consisting of all software and hardware utilities needed to develop Z-wave products, making it easier and faster to setup the product [72]. The kit can be purchased for around 24000 SEK and a license agreement has to be signed [73]. A component needed to develop a Z-wave product is a module that cost roughly around 100 SEK or more [74]. What kind of module to purchase depends a lot on the usage purpose.

ZigBee

The price for a ZigBee remote control module is roughly 200 SEK and an antenna is around 30 SEK [75] [76]. There are many types of modules available for ZigBee where most depend on the application area. For industrial control the price tag for a module is higher and for a more powerful component the price is significantly greater. A module has many other smaller components included, such as transceiver. It is also possible to purchase a simple chip and the other smaller components separately, but the development cost will be higher as more testing will be required [77]. To get into the development with the ZigBee technology easier and quicker, there are some starter kits that can be purchased for under 3200 SEK if desired [78].

Wi-Fi

Wi-Fi has a wide assortment of components for different application areas which makes it harder to the specify prices, but a rough estimation of a module is around 300 SEK and antenna for it is 60 SEK [79]. The price on a module varies on how powerful the specifications are and what smaller components are implemented in it. There are many extra accessories to add for a Wi-Fi device, such as amplifiers and more completed units for development that cost around 700 SEK. [80].

NFC

A NFC reader module costs around 800 SEK and for a NFC tag price is 10 SEK. NFC is a new version of RFID and the components used for NFC are about the same as long they are compatible with the NFC technology [81]. A development kit containing a complete set of components and software tools needed to develop a NFC device is available and can cost up to 8000 SEK.

Infrared - IrDA

An IrDA board costs 200 SEK while other smaller components like transmitter, microcontrollers cost around 20 SEK each [82] [83]. The components required to build an IrDA remote control are not as expensive as the other technologies and it does not have a development kit. Infrared is used in many applications and depending on where the technology is used, the components required can be very different.

5.7 Suitability with smart glass

Obstacles such as walls, furniture, and other physical objects can cause the signal to drop. Tinted glass can cause signal loss but it also depends on thickness and the materials inside the glass. Smart glass can contain small amount of metal which has a big impact for interference where it weakens the signal. Unless the signal is lost due to the obstacle, there are chances for the signal to reach the receiver if the material used for the glass is more interference friendly.

Bluetooth & Wi-Fi

Bluetooth and Wi-Fi signals have the ability to pass through drywalls and other kind of materials like clear glass but there are also materials that have high chances of completely blocking the signals, especially metals [84]. Depending on the material used for the smart glass apart from the necessary layers to have an opaque and clear effect, the signal strength can be weakened when passing through the whole glass [85]. There are more interference friendly materials to use such as ceramic window film which does not block for the radio signal. Using more interference friendly materials will allow the signal to reach the receiver easily, even if the user is standing on the other side of the glass.

Z-wave & ZigBee

As Z-wave and ZigBee signals work the similarly to the Bluetooth and Wi-Fi signals, they can suffer some power loss by passing through obstacles such as water and metals [86] [87]. For the suitability with the glass, there are interference friendly materials to use on the glass to prevent the signal to be lost when the signal has to pass through the smart glass.

NFC

NFC signal can pass through regular glass and plastic materials (used as tags) but it still has problems going through metal objects. Considering the short range of NFC, the signal might not be able to reach the receiver when placed on the other side of a thick smart glass, due to the different materials it contains.

Infrared - IrDA

Infrared is a technology that has the line-of-sight requirement for transmitting signals. The signal is a form of light invisible to human eyes and cannot pass through walls. Infrared used on remote controls can pass through normal clear glass but might have trouble on tinted glass. An experiment is needed to be able to confirm whether the infrared signal can pass through a smart glass, as it contains different materials inside (this report does not include the experiment).

5.8 Evaluation table

This table contains the summary results of the parameters mentioned above.

Technology	Range	Security	Maturity /Stability	Bandwidth (GHz) /Data rate	Inter-ference	Cost	Suitability
Bluetooth HS	Medium	High	High	2.4-2.48/ High	Medium	Medium	Medium
Bluetooth Classic	High	High	High	2.4-2.48/ Medium	Medium	Medium	Medium
BLE	High	High	High	2.4-2.48/ Medium	Medium	Medium	Medium
Wi-Fi	High	High	High	2.4 or 5/ High	Medium	Medium	Medium
Z-wave	Medium	Medium	Medium	1/ Low	Low	Cheap	Medium
ZigBee	Medium	High	High	2.4/ Low	High	Cheap	Medium
NFC	Low	High	Medium	13.56/ Low	Low	Expensive	Low
IrDA	Low	High	High	$(3.3\text{-}5.7)*10^{-5}$/ Medium	Low	Cheap	Low

Table 3 – Summarizations of the parameters on each mentioned technology

6. Discussion & Result

This chapter contains discussion of the work method used for this project and the evaluation result based on the previous chapter.

6.1 Method discussion

As described in the section describing the methodology, the plan consisted of three phases where the first phase was to get an overview of the smart glass. Some issues occurred in the first phase which hindered us to proceed with the project. It took longer than expected to search for the necessary information, which made the project lag behind the time schedule (see Table 2, Section 2.2). This could have been avoided by raising research questions which could guide us when screening the useful data. By doing this, we could have had more time to polish the other phases.

The second stage was to study the different wireless technologies and conclude whether they meet the requirements or not (mentioned in Section 2). The study of the different technologies were conducted while focusing on the parameters for each of them. However, the realization of not being able to keep up with the planned schedule had made us to take another turn as more time was needed for the report. To accomplish this project within the time limit, we discussed the problem with our supervisors and together came up with the decision to limit the scope of this project to two phases instead of three as initially planned. The idea of buying and testing a prototype was dismissed. Although this solution set aside more time to study the required knowledge, it could have been avoided if the time schedule was better planned in the beginning of the project.

6.2 Evaluation result

The main purpose of the project was to find a suitable protocol for a remote panel to control the smart glass. Many factors have to be taken into consideration when deciding the most optimal protocol for the wireless remote. After a discussion with the company, it was decided that the important factors to be kept in mind in this case are the security, range, and maturity of the technique. Additional parameters was also added in order to get a better overview of each technology which includes bandwidth, interference, cost, and suitability with the smart glass. Below are the discussions based on the parameters mentioned on the first table together with the requirements (Table 1, see Section 2). The result is based on comparison of the evaluation table (Table 3, see Section 5.8) and the requirements of the first table (Table 1, see Section 2).

6.2.1 Range

Range is an important factor that must be taken into consideration when evaluating the results. The required range for the technology is medium (see Table 1, Section 2) and according to the evaluation table (Table 3), NFC and Infrared fails to fulfill the range requirement. Other technologies have at least the scale medium or above which is sufficient to satisfy the requirement.

6.2.2 Security

In terms of wireless network, there is no such thing as perfect security but there are methods of preventing certain attacks. According to the requirements for the security parameter of the table (see Table 1), the level should be high. Bluetooth, Wi-Fi, ZigBee, NFC, and Infrared are considered to have high security among the technologies according to Table 3 (see Section 5.8) and thus fulfill the acquisition. However, Z-wave fall below the requirement with medium level.

6.2.3 Maturity/Stability

The maturity and stability of a technology is important because the more tests conducted and improved version released, the more stable the technology becomes. The required maturity and stability for each technology is high (see Table 1, Section 2) and technologies fulfilling the requirement are Infrared, Bluetooth, ZigBee, and Wi-Fi according to the evaluation table (Table 3, Section 5.8). Other technologies are still young and not stable enough to meet the acquisition which make them unsuitable for this project.

6.2.4 Bandwidth

The bandwidth does not have to be big to use for a remote control for a smart glass. For this purpose the technologies are required to have at least a low level bandwidth (stated in Table 1, see Section 2). This means that all technologies are suitable for this requirement. However technologies with large data rate consume more power than technologies with lower data rate, which makes them not suitable to use for a remote control based on a coin sized battery.

6.2.5 Interference

Interference can easily occur when devices are using the same frequency band, thus makes it important to have a minimal interference for each technology. The acquisition is to have at most medium of interference (see Table 1, Section 2). According to the evaluation table (Table 3, Section 5.8), only ZigBee that does not fit in the requirement, while all other technologies meet the acquisition.

6.2.6 Cost

For the hardware cost it cannot cost too much as companies need to gain profit thus the requirement for the hardware can at most be at a medium price (See Table 1, Section 2). All technologies except NFC have cost of medium or low (see Table 3, Section 5.8), which meet the requirements.

6.2.7 Suitability with the smart glass

The signals of technologies should reach the receiver even if the signal has to go through the smart glass. For this purpose, the acquisition for suitability should at least be medium (see Table 1, Section 2). Infrared and NFC have a low suitability as mentioned in the evaluation table (see Table 3, Section 5.8). Other technologies have a medium suitability with a smart glass and meet minimum requirement.

6.2.8 Result table

This section shows the result table after the discussion of each parameter mentioned in Section 6.2.

Technology	Range	Security	Maturity /Stability	Bandwidth (GHz) /Data rate	Inter-ference	Cost	Suitability
Bluetooth HS	Medium	High	High	2.4-2.48/ High	Medium	Medium	Medium
Bluetooth Classic	High	High	High	2.4-2.48/ Medium	Medium	Medium	Medium
BLE	High	High	High	2.4-2.48/ Medium	Medium	Medium	Medium
Wi-Fi	High	High	High	2.4 or 5/ High	Medium	Medium	Medium

Table 4 – The technologies that passed all the requirements

7. Conclusion

The aim of this thesis was to evaluate some of the design decisions that go into designing a wireless control panel that is appropriate to control the smart glass. The work was initiated with studies of different technologies that are used to create a smart glass. The main focus of this thesis was the study of different wireless techniques and the evaluation of which one is more suitable to use as a control panel for the smart glass. The important factors that were considered when evaluating the result were the range, security, and maturity of the technology. Other factors bandwidth, interference, cost, and suitability with the smart glass were also added to give a better overview of the result (the result is mentioned in Section 6).

To summarize the result, NFC and IrDA are not recommended technologies for the panel because of the range and line-of-sight requirement. Neither is Z-wave because of the security level is not high enough. Wi-Fi is a good choice if the protection has been appropriately handled by an expert, but its downside can be seen when too many devices are connected and therefore slowing the network down. ZigBee is not a suitable technology because it cannot properly coexist with other wireless technologies due to its high interference level. The Bluetooth technologies High Speed and Classic are more recommended for larger data transmission, which is not required for a remote panel designed for a smart glass. To conclude, the recommended technique would be BLE because of its range, security level, and the fact that Bluetooth is a well-established technique. The interference level is also acceptable and the price for the hardware components are reasonable. In 2014, the new Bluetooth version 4.2 was released with updated functionalities and improvements for the BLE, which enhanced the security and range.

References

[1] "Commoditization," Investopedia, 2015. [Online]. Available: http://www.investopedia.com/terms/c/commoditization.asp. [Accessed 5 May 2015].

[2] "Ergonomics & Human Factors," Chartered Institute of Ergonomics & Human Factors, 2015. [Online]. Available: http://www.ergonomics.org.uk/learning/what-ergonomics/. [Accessed 31 March 2015].

[3] H. Staff, "Energy Crisis (1970s)," A+E Networks, 2010. [Online]. Available: http://www.history.com/topics/energy-crisis. [Accessed 30 March 2015].

[4] "History and Properties of Liquid Crystal," Nobelprize.org, 9 September 2003. [Online]. Available: http://www.nobelprize.org/educational/physics/liquid_crystals/history/. [Accessed 30 March 2015].

[5] "The Early History of the Liquid Crystal Display," IEEE Spectrum, 2015. [Online]. Available: http://spectrum.ieee.org/static/timeline-the-early-history-of-the-liquid-crystal-display. [Accessed 30 March 2015].

[6] "How to Evaluate Smart Glass and Liquid Crystal," Scienstry Inc, 2014. [Online]. Available: http://www.scienstry.us/How%20to%20evaluate%20smart%20glass%20and%20liquid%20crystal%20switchable%20film.pdf. [Accessed 4 May 2015].

[7] "Smart Glass Applications with Polymer Dispersed Liquid Crystal," Continuing Education Center, May 2014. [Online]. Available: http://continuingeducation.construction.com/article.php?L=395&C=1199&P=3. [Accessed 15 May 2015].

[8] K. Bonsor, "How Smart Windows Work," HowStuffWorks.com, 29 March 2001. [Online]. Available: http://home.howstuffworks.com/home-improvement/construction/green/smart-window3.htm. [Accessed 20 May 2015].

[9] C. Woodford, ""Smart" windows (electrochromic glass)," Explainthatstuff!, 17 September 2014. [Online]. Available: http://www.explainthatstuff.com/electrochromic-windows.html. [Accessed 14 May 2015].

[10] K. Bonsor, "How Smart Windows Work," HowStuffWorks.com, 29 March 2001. [Online]. Available: http://home.howstuffworks.com/home-improvement/construction/green/smart-window4.htm. [Accessed 20 May 2015].

[11] "How Dynamic Glass Works," Sage Glass, 2015. [Online]. Available: http://sageglass.com/technology/how-it-works/. [Accessed 4 May 2015].

[12] M. Beevor, "Smart Building Envelopes," June 2010. [Online]. Available: http://www.smartglassinternational.com/wp-content/uploads/2011/01/Cambridge-University-SPD-SmartGlass-Report.pdf. [Accessed 10 April 2015].

[13] "Switchable Technology," Sage Glass, 2015. [Online]. Available: http://sageglass.com/technology/switchable-technology/. [Accessed 4 May 2015].

[14] "SPD Smart Glass," SPD Control System Corporation, 2010. [Online]. Available: http://www.spdcontrolsystems.com/spdglass.htm. [Accessed 13 May 2015].

[15] K. Bonsor, "How Smart Windows Work," HowStuffWorks.com, 29 March 2001. [Online]. Available: http://home.howstuffworks.com/home-improvement/construction/green/smart-window2.htm. [Accessed 20 May 2015].

[16] B.A.Forouzan, Data Communication and Networking, 3rd ed., McGraw-Hill, 2003, p. 10.

[17] "Mesh topology," Computer Hope, 2015. [Online]. Available: http://www.computerhope.com/jargon/m/mesh.htm. [Accessed 10 May 2015].

[18] M. Rouse, "Star Network," TechTargets, 2015. [Online]. Available: http://searchnetworking.techtarget.com/definition/star-network#. [Accessed 8 May 2015].

[19] "Communication Network Topologies," WikiBooks, 14 April 2015. [Online]. Available: http://en.wikibooks.org/wiki/Communication_Networks/Network_Topologies. [Accessed 8 May 2015].

[20] "Star Topology," Computer Hope, 2015. [Online]. Available: http://www.computerhope.com/jargon/s/startopo.htm. [Accessed 10 May 2015].

[21] C. Janssen, "Tree Topology," Techopedia, 2015. [Online]. Available: http://www.techopedia.com/definition/24206/tree-topology. [Accessed 8 May 2015].

[22] "Tree Topology," Computer Hope, 2015. [Online]. Available: http://www.computerhope.com/jargon/t/treetopo.htm. [Accessed 8 May 2015].

[23] M. Rouse, "Master/Slave Definition," TechTarget, 2015. [Online]. Available: http://searchnetworking.techtarget.com/definition/master-slave. [Accessed 18 May 2015].

[24] "P2P," TechTerms, 2015. [Online]. Available: http://techterms.com/definition/p2p. [Accessed 16 May 2015].

[25] "Introduction to Serial Communication," TalTech, 2015. [Online]. Available: http://www.taltech.com/datacollection/articles/serial_intro. [Accessed 5 May 2015].

[26] "Bluetooth inventor nominated for top European honor," Ericsson, 12 June 2012. [Online]. Available: http://www.ericsson.com/news/120612_bluetooth_inventor_nominated_for_top_european_honor_244159019_c. [Accessed 10 May 2015].

[27] "A Look at the Basics of Bluetooth," Bluetooth, 2015. [Online]. Available: http://www.bluetooth.com/Pages/Basics.aspx. [Accessed 14 May 2015].

[28] "Bluetooth," Wikipedia, 16 June 2015. [Online]. Available: https://en.wikipedia.org/?title=Bluetooth. [Accessed 20 June 2015].

[29] "Welcome to Bluetooth Technology 101 - A brief tutorial on Bluetooth wireless technology," Bluetooth, 2015. [Online]. Available: http://www.bluetooth.com/Pages/Fast-Facts.aspx. [Accessed 27 May 2015].

[30] J. Padgette, K. Scarfone and L. Chen, "Guide to Bluetooth Security," National Institute of Standards and Technology, June 2012. [Online]. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911133. [Accessed 11 May 2015].

[31] R. Nilsson and B. Saltzstein, "Bluetooth Low Energy vs. Classic Bluetooth: Choose the Best Wireless Technology For Your Application," Medical Electronic Design, 8 June 2012. [Online]. Available: http://www.medicalelectronicsdesign.com/article/bluetooth-low-energy-vs-classic-bluetooth-choose-best-wireless-technology-your-application. [Accessed 27 April 2015].

[32] "The Low Energi Technology Behind Bluetooth Smart," Bluetooth, 2015. [Online]. Available: http://www.bluetooth.com/Pages/low-energy-tech-info.aspx. [Accessed 24 May 2015].

[33] "Bluetooth Smart," Bluetooth, 2015. [Online]. Available: http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx. [Accessed 17 May 2015].

[34] P. Smith, "Comparing Low-Power Wireless Technology," Digikey, 8 August 2011. [Online]. Available: http://www.digikey.com/en/articles/techzone/2011/aug/comparing-low-power-wireless-technologies. [Accessed 23 May 2015].

[35] "Bluetooth High Speed," Bluetooth, 2015. [Online]. Available: http://www.bluetooth.com/Pages/High-Speed.aspx. [Accessed 16 May 2015].

[36] "Bluetooth Core Specification 4.2 Frequently Asked Question," Bluetooth, December 2014. [Online]. Available: https://www.bluetooth.org/en-us/Documents/Bluetooth4-2FAQ.pdf. [Accessed 11 May 2015].

[37] "Z-wave vs. ZigBee," LinkLabs, 1 March 2015. [Online]. Available: http://www.link-labs.com/z-wave-vs-zigbee/. [Accessed 11 May 2015].

[38] D. Prindle, "What the heck are ZigBee, Z-Wave, and Insteon? Home automation standards explained," Digital Trends, 31 Januari 2014. [Online]. Available: http://www.digitaltrends.com/home/zigbee-vs-zwave-vs-insteon-home-automation-protocols-explained/. [Accessed 20 April 2015].

[39] "Z-wave Frequency Coverage," 2015. [Online]. Available: http://z-wave.sigmadesigns.com/docs/Z-Wave_Frequency_Coverage.pdf. [Accessed 20 April 2015].

[40] "Frequently asked Questions," Z-Wave, 2015. [Online]. Available: http://www.z-wave.com/questions. [Accessed 16 May 2015].

[41] "About Z-Wave Technology," Z-Wave Alliance, 2015. [Online]. Available: http://z-wavealliance.org/about_z-wave_technology/. [Accessed 20 April 2015].

[42] "Z-Wave For OEMs & Developers," Z-Wave Alliance, 2015. [Online]. Available: http://z-wavealliance.org/z-wave-oems-developers/. [Accessed 26 May 2015].

[43] "Z-Wave Security," UK Automation, 2015. [Online]. Available: http://www.uk-automation.co.uk/categories/Z%252dWave-Automation/Z%252dWave-Security/. [Accessed 27 May 2015].

[44] M. Smith, "Hacking and attacking automated homes," Microsoft Subnet, 25 June 2013. [Online]. Available: http://www.networkworld.com/article/2224849/microsoft-subnet/hacking-and-attacking-automated-homes.html. [Accessed 28 May 2015].

[45] "HONEY, I’M HOME!! - HACKING Z-WAVE HOME AUTOMATION SYSTEMS," Black Hat, 2013. [Online]. Available: http://www.blackhat.com/us-13/briefings.html#Fouladi. [Accessed 28 May 2015].

[46] "ZigBee Technology," SMK Electronics Corporation, 2015. [Online]. Available: https://www.smkusa.com/usa/technologies/zb/ (. [Accessed 17 May 2015].

[47] "Low-power, low-cost, low-complexity networking for the Internet of Things," ZigBee Alliance, 2015. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/. [Accessed 25 May 2015].

[48] "ZigBee PRO with Green Power," ZigBee Alliance, 2015. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/. [Accessed 24 May 2015].

[49] C.-J. . M. Liang, N. B. Priyantha, J. Liu and A. Terzis, "Surviving Wi-Fi Interference in Low Power ZigBee Networks," in *Proceedings of the 8th ACM Conference on embedded networked sensor systems,* Zurich, Switzerland, 2010.

[50] "ZigBee Home Automation Smarter, more energy-efficient and secure homes.," ZigBee Alliance, 2015. [Online]. Available: http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbeehomeautomation/. [Accessed 27 May 2015].

[51] "Open Standards Development," ZigBee Alliance, 2015. [Online]. Available: http://www.zigbee.org/zigbeealliance/developing-standards/. [Accessed 26 May 2015].

[52] B. Bowers, "ZigBee Wireless Security: A New Age Penetration Tester's Toolkit," Cisco, 9 January 2012. [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4. [Accessed 28 May 2015].

[53] V. Tech, "VVDN ZigBee Wireless Gateway and Device Platform," VVDN Technologies, 25 February 2014. [Online]. Available: http://vvdntech.com/blog/vvdn-zigbee-wireless-gateway-and-device-platform/. [Accessed 28 June 2015].

[54] J. Andrew, "WiFi Transfer Rates & Types," Demand Media, 2015. [Online]. Available: http://everydaylife.globalpost.com/wifi-transfer-rates-types-21881.html. [Accessed 21 June 2015].

[55] "Wireless Local Area Networks (WLAN/WiFi) Usage Regulations," Comminucations and Information Technology Commission, 2015. [Online]. Available: http://www.citc.gov.sa/English/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/PL-PM-002-E-WiFi%20Regulations.pdf. [Accessed 11 May 2015].

[56] "Wi-Fi Range," GoPro, 2015. [Online]. Available: https://gopro.com/support/articles/wi-fi-range. [Accessed 28 May 2015].

[57] P. Thangaraj, N. Geethanjali, K. Kathiresan and R. Madhumathi, "Wifi Infrastructure Security System from Vulnerable Attacks," *International Journal of Computer Science and Network Security (IJCSNS),* vol. 13, no. 12, p. 104, 2013.

[58] "Common Types of Network Attacks," Microsoft, 2015. [Online]. Available: https://technet.microsoft.com/en-us/library/cc959354.aspx. [Accessed 28 May 2015].

[59] K. Ok, V. Coskun and B. Ozdenizci, Near Field Communication From Theory To Practice, 2nd, Ed., John Wiley & Sons, 2011, pp. 1-10.

[60] "NFC Tags Explained," KimTag, 2013. [Online]. Available: http://kimtag.com/s/nfc_tags. [Accessed 19 May 2015].

[61] "Närfältskommunikation," Kjell & Company, 29 September 2014. [Online]. Available: http://www.kjell.com/fraga-kjell/hur-funkar-det/mobilt/anslutningsmojligheterna/narfaltskommunikation. [Accessed 26 May 2015].

[62] P. Paganini, "Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema," InfoSec Institute, 18 June 2013. [Online]. Available: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/. [Accessed 28 May 2015].

[63] R. Netting, "INFRARED ENERGY," NASA's Science Mission Directorate, 13 August 2014. [Online]. Available: http://missionscience.nasa.gov/ems/07_infraredwaves.html. [Accessed 9 April 2015].

[64] J. R. Smith, Programming the PIC Microcontroller with MBASIC, Amsterdam: Elsevier/Newnes, 2005, pp. 517-541.

[65] S. Kataoka and K. Atagi, "Prevention of IR interference from high frequency fluorescent lighting to IR remote-control systems," in *Proceedings of 1995 IEEE Applied Power Electronics Conference and Exposition - APEC'95, 1995*, 1995.

[66] "Security information for infrared communication," Microsoft, 21 January 2005. [Online]. Available: https://technet.microsoft.com/en-us/library/cc775941(v=ws.10).aspx. [Accessed 12 May 2015].

[67] J. Earley, "Infrared meets speed and security needs," TechTarget, 26 May 2005. [Online]. Available: http://www.computerweekly.com/opinion/Infrared-meets-speed-and-security-needs. [Accessed 10 May 2015].

[68] D. Suvak, "IrDA and Bluetooth: A Complementary Comparison," Extended Systems, Inc., 2000. [Online]. Available: http://alumni.cs.ucr.edu/~csyiazti/courses/cs260/downloads/IrDA_vs_Bluetooth.pdf. [Accessed 28 May 2015].

[69] J. Wright, R. Speers and R. Melgares, "This is KillerBee - Framework and Tools for Attacking ZigBee and IEEE 802.15.4 networks.," 2015. [Online]. Available: https://github.com/riverloopsec/killerbee. [Accessed 18 June 2015].

[70] "RF Transceivers - Bluetooth," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rf-transceivers/3539948?k=bluetooth. [Accessed 18 June 2015].

[71] "RF Antennas - Bluetooth," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rf-antennas/3540022?k=bluetooth. [Accessed 21 June 2015].

[72] "Development Kit for Z-wave End-Devices," 2014. [Online]. Available: http://z-wave.sigmadesigns.com/docs/brochures/Z-Wave_Dev_Kit_br.pdf. [Accessed 20 June 2015].

[73] "Z-wave Get Started," Sigma Designs Inc, 2015. [Online]. Available: http://z-wave.sigmadesigns.com/dev_kits#z-wave_get_started. [Accessed 18 June 2015].

[74] "Sigma Designs Inc ZM4101AJ-CME3," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-detail/en/ZM4101AJ-CME3/703-1058-ND/2416275. [Accessed 21 June 2015].

[75] "RF Transceivers - ZigBee," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en?FV=fff40036%2Cfff803ec&k=zigbee&mnonly=0&newproducts=0&ColumnSort=-405&page=1&stock=0&pbfree=0&rohs=0&quantity=&ptm=0&fid=0&pageSize=500. [Accessed 19 June 2015].

[76] "RF Antennas - ZigBee," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rf-antennas/3540022?k=zigbee. [Accessed 20 June 2015].

[77] Ø. Nottveit, "ZigBee® - Make or Buy? The life cycle cost of a ZigBee HW solution," 2007. [Online]. Available: http://www.radiocrafts.com/uploads/radiocrafts_euzdc_2007_paper.pdf. [Accessed 22 June 2015].

[78] R. Maley, "4 Under $400: Get Started with ZigBee Today," ZigBee, 19 February 2015. [Online]. Available: http://www.zigbee.org/4-400-get-started-zigbee-today/. [Accessed 21 June 2015].

[79] "RF Transceivers - Wifi," Dig-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rf-transceivers/3539948?k=wi-fi. [Accessed 20 June 2015].

[80] "RF Evaluation and Development Kits, Boards," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rf-evaluation-and-development-kits-boards/3539644?k=wi-fi. [Accessed 20 June 2015].

[81] "RFID Reader Modules," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/rf-if-and-rfid/rfid-reader-modules/3539638?k=NFC. [Accessed 20 June 2015].

[82] "Microchip Technology AC164124," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-detail/en/AC164124/AC164124-ND/1616602. [Accessed 20 June 2015].

[83] "Interface - Drivers, Receivers, Transceivers," Digi-Key Electronics, 22 June 2015. [Online]. Available: http://www.digikey.com/product-search/en/integrated-circuits-ics/interface-drivers-receivers-transceivers/2556324?k=irda. [Accessed 20 June 2015].

[84] D. Weedmark, "What Will Block a Bluetooth Signal?," Synomum, 2015. [Online]. Available: http://classroom.synonym.com/block-bluetooth-signal-17777.html. [Accessed 19 June 2015].

[85] M. Harwood, CompTIA Network+ N10-004 Exam Cram, 3rd Edition, 3rd ed., Pearson IT Certification, 2009.

[86] "User Guides," Vera Control, Ltd., 07 October 2014. [Online]. Available: http://support.getvera.com/customer/portal/articles/1719040-q-what-is-the-range-of-my-vera-controller-and-can-i-extend-it-. [Accessed 19 June 2015].

[87] A. Sterian, "A Guide to Wireless Range & Repeaters," SmartThings, 13 Auguest 2014. [Online]. Available: http://blog.smartthings.com/iot101/a-guide-to-wireless-range-repeaters/. [Accessed 19 June 2015].