UNIVERSITY OF OSLO
Department of Informatics

Comparison of Wireless Shielding Solutions

Pål Johnsen Blakstad

Network and System Administration

Oslo University College

May 24, 2011

Comparison of Wireless Shielding Solutions

Pål Johnsen Blakstad

Network and System Administration
Oslo University College

May 24, 2011

Abstract

Security and interfering networks are challenges in wireless networks today. A security technique concerning shielding wireless signal using signal reducing or canceling material can be used to solve some of these issues. This technique however, is regarded as expensive and hard to implement. To look into these claim, several types of shielding solution were tested and compared in regard to efficiency, cost and implementation. Testing of the solution was done using a test box with the solutions applied to the interior. As a result of the study it was found that affordable shielding solutions with decent attenuation and uncomplicated implementation exists. For higher attenuation performance more expensive materials, installed by professionals, are needed.

Acknowledgments

I would like to thank the following people for making this thesis possible:

- Hårek Haugerud for his advice and support during the writing and execution of this thesis, and his patient way of teaching and conveying knowledge.
- Kyrre Begnum for his useful thesis seminars, and his excellent and enthusiastic teaching.
- Tore Hassle for his help with ordering equipment and building materials.
- The other teachers of Oslo University College for all help and directions.
- My classmates for creating a friendly atmosphere and for educational discussions during the course of this master program.
- Ole Grøndalen and Per Hjalmar Lehne at Telenor for a interesting meeting and a rewarding discussion of the approach and testing methods.
- Sigbjørn Derås for providing a place for construction and testing
- Family and friends for giving support, solace and sanctuary through the duration of this thesis.

Contents

1 Introduction **5**
- 1.1 Motivation . . . 5
- 1.2 Problem statement . . . 7

2 Background material **9**
- 2.1 Wireless signals . . . 9
  - 2.1.1 Transmission media . . . 10
  - 2.1.2 Decibel . . . 13
  - 2.1.3 Near-field and far-field field regions . . . 13
  - 2.1.4 Transmission impairments . . . 14
  - 2.1.5 Wireless LAN . . . 15
  - 2.1.6 Security . . . 21
- 2.2 Equipment for sending and receiving signals . . . 26
  - 2.2.1 Wireless Network Analyzer . . . 26
  - 2.2.2 Software sending Wi-Fi . . . 26
  - 2.2.3 Signal generator . . . 27
  - 2.2.4 Spectrum analyzer . . . 28
  - 2.2.5 Software receiving Wi-Fi . . . 29
  - 2.2.6 Antennas . . . 30
- 2.3 Shielding solutions . . . 31
  - 2.3.1 Mu Faraday cage . . . 31
  - 2.3.2 Shielding paint . . . 31
  - 2.3.3 Shielding windows . . . 32
  - 2.3.4 Frequency Selective Surface (FFS) . . . 33
  - 2.3.5 Vegetation . . . 33
  - 2.3.6 Various shielding complimentations . . . 34

3 Experimental setup **35**
- 3.1 Efficiency . . . 41
- 3.2 Cost and Implementation . . . 45

4 Results **47**
- 4.1 Efficiency . . . 47
  - 4.1.1 REF . . . 48
  - 4.1.2 REF-BOX . . . 51
  - 4.1.3 REF-WIN . . . 54
  - 4.1.4 REF-W+P . . . 57

4.1.5 Analysis of the reference testing . . . 60
4.1.6 MU-CU . . . 61
4.1.7 PAINT . . . 64
4.1.8 MESH . . . 67
4.1.9 AL . . . 69
4.1.10 Analysis of the shielding efficiency . . . 72
4.2 Cost and implementation . . . 74
4.2.1 MU-CU . . . 74
4.2.2 PAINT . . . 74
4.2.3 MESH . . . 75
4.2.4 AL . . . 75
4.3 Result summary . . . 75

5 Discussion and conclusion **77**
5.1 Experimental setup and approach review . . . 77
5.2 Equipment used . . . 79
5.3 Review shielding solutions . . . 81
5.4 Future research . . . 83
5.5 Summary and conclusions . . . 84

Appendices **92**

A Firmware installation **93**

List of Figures

3.1 Simple overview of efficiency testing . . . 36
3.2 Technical drawing of the test box construction . . . 37
3.3 Pictures of a finished test box . . . 38
3.4 Pictures of the solutions applied to the test box . . . 40
3.5 Captured microwave interference during testing (at 2.412 GHz) . . . 43
3.6 Testing arrangement overview . . . 44

4.1 Accuracy of the REF result data (1m, 100mW) . . . 49
4.2 Graphs for testing results for REF . . . 50
4.3 Accuracy of the REF-BOX result data (1m, 100mW) . . . 52
4.4 Graphs for testing results for REF-BOX . . . 53
4.5 Accuracy of the REF-WIN result data (1m, 100mW) . . . 55
4.6 Graphs for testing results for REF-WIN . . . 56
4.7 Accuracy of the REF-W+P result data (1m, 100mW) . . . 58
4.8 Graphs for testing results for REF-W+P . . . 58
4.9 Accuracy of the MU-CU result data (1m, 100mW) . . . 62

4.10 Measurements on MU-CU with and without grounding (1m, 100mW) 62
4.11 Graphs for testing results for MU-CU 63
4.12 Accuracy of the PAINT result data (1m, 100mW) 65
4.13 Measurements on PAINT with and without grounding (1m, 100mW) . 65
4.14 Graphs for testing results for PAINT 66
4.15 Accuracy of the MESH result data (1m, 100mW) 68
4.16 Graphs for testing results for MESH 68
4.17 Accuracy of the AL result data (1m, 100mW) 70
4.18 Graphs for testing results for AL 71
4.19 Comparison of the different results 73
4.20 The materials compared 73

List of Tables

2.1 Frequency bands 11
2.2 Typical Digital Microwave Performance 12
2.3 Overview IEEE 802.11 standards 20
2.4 Physical layer standards 20

3.1 Test overview 41
3.2 9 scenarios (i.e. sets of measurements) for each solution 45

4.1 Median of the REF results in dB 49
4.2 Median of the REF-BOX results in dB 52
4.3 Median of the REF-WIN results in dB 55
4.4 Median of the REF-W+P results in dB 59
4.5 Comparison of the most stable measurements from the different types of test (1m, 100mW) 60
4.6 Median of the MU-CU results in dB 62
4.7 Median of the PAINT results in dB 65
4.8 Median of the MESH results in dB 67
4.9 Median of the AL results in dB 69
4.10 Attenuation calculated from only the stable results 72
4.11 Result overview 76

Chapter 1

Introduction

1.1 Motivation

Throughout this decade wireless communication has become more and more common. Due to several advantages over wired networks, like easy configuration, acessability and the drop in prices for wireless router and network cards, WLAN is commonly used in businesses, universities, public areas and recently in private homes. Wireless connections in WLAN offers a speed up to 54MB/s, although a bit slower than wired connections, it is nearly 1000 times faster than dial-up and a lot faster than cellular networks. Also more and more devices are delivered with possibility of Wi-Fi connection. Some examples of this is mobile phones, PDA, gaming consoles and tablet computers like the iPad. The global enterprise mobility solution marked was estimated, in 2008, to be 23.2 billion US dollars [1].

Because of the widespread use of wireless communication, security has become an ongoing challenge. Since wireless signals consists of radio waves and travel through air, signals from different WLAN can interfere or even be mistaken for each other. This means that all receivers within range can receive the wireless signals, opening for the possibility of eavesdropping and data theft by malicious users. Rogue access points can be introduced into a wireless network by a malicious user, making future eavesdropping, identity theft or man-in-the-middle attacks on the network easier. A malicious user may also conduct an attack known as a DoS (Denial of Service) attack, which includes jamming a wireless network by sending a massive amount of noise at a high signal strength in the same frequency as the targeted network.

Wireless security can be implemented both as a hardware and software solution. Wireless software security begins with securing the network with the common wired security measures. However, as the physical layer for wireless networks are more exposed, more wireless specific security should be introduced. Wireless specific security generally consists of encryption of the signal, authentication when connecting to the network and different signal hiding techniques. Although these measures might be enough for most wireless networks, more persistent malicious users may penetrate these barriers. Wireless DoS attacks and signal pollution are also issues not accounted for through wireless software security.

One of the few wireless network specific protection using hardware that exists, includes EMI site shielding. Electromagnetic Interference (EMI) shielding refers to the reflection and/or absorption of electromagnetic radiation by a material. This way signal transmitted at both the interior and the exterior of the shield is blocked, elimination the possibility of eavesdropping or performing DoS attacks on the network from the outside the shield. The material needs to be grounded so that the excess signal will travel to the ground. The effectiveness of the shield depends on the material it is made of, its thickness and the amount of openings or holes in the shield smaller than the wavelength of the signal to block. Another physical way to limit access to the network is the use of directional antennas or control of transmission power. However, limiting the access to the area or equipment could also be interpreted as hardware protection, and includes the use of locked doors, security guards etc.

There are several ways to shield a wireless area. As electromagnetic signals always will go through the material with the lowest electromagnetic resistance, EMI shields usually consists of highly conductive metal like copper, aluminum or nickel. As metal shields easily gets bulky, heavy and that the danger of electric shock is imminent without insulation, another solution includes the use plastic materials with metal fillers in the form of fibers, flakes or powder or conducting grade carbon black. As electromagnetic fields quality of blocking EMI signals, ferrites, usually magnetic materials (ceramic and iron(III) oxide) used as as permanent magnets, have been extensively used by the virtue of their property. Due to the range of different materials and forms they can be arranged, shielding comes in several shapes; from the classic copper Faraday cage, metal woven into a fabric and formed into a tent, a metal mesh to shield windows, ferrite powder mixed into a suitable binder forming a shielding paint, to frequency selective surface (FSS) materials that filters different frequencies. There has also been studies concerning documenting the shielding properties of vegetation, and looking into the performance of a vegetation shield [2].

Wireless shielding is a rather unstudied topic. There are just a handful relevant articles on the subject of shielding networks available, and few more on shielding electronic equipment. There are some more recent discoveries and development from 2000 to 2006, and some in 2009, mostly concerning either the shielding properties of certain materials or development and testing of new shielding solutions. Most articles regarding wireless security considers site shielding as expensive and hard to implement, though no real research has been done concerning how expensive or how difficult a shield is to implement.

1.2 Problem statement

Spurred by the motivation in chapter 1.1, this project investigates the different physical solutions for shielding wireless signals, well known and newer applications, looking into both the effectiveness of the shielding properties and the cost, time and difficulty of applying the product.

Currently physical site shielding in commercial businesses and most governmental organizations is uncommon, or limited to a small area. This is most likely caused by the limitation of the knowledge in the area along with expectancy of high expenses and extensive implementation. This project aims to explore the availability of easy and affordable solutions to shielding, opening up for the possibility of implementing shielding in small and medium businesses.

The hypothesis of the project is that even a moderately effective shield will add to the security, by increasing the demand of accuracy of the equipment for a potential eavesdrop or DoS attach. This will add to the expense of the equipment, and thus making the launching of such attacks less interesting for malicious users. Also containing the signals from networks to a specific area controls the amount of signal pollution leaked into the local environment, and decreases the chances of interference between neighboring WLAN.

The following problem statement gives a guide to direction and decision making regarding the experimental setup and testing done in this thesis. Answering these research questions, along with studying the theory behind them, is the goal of this thesis .
How do the different wireless signal shielding compare in the case of:

- *Effiecency*
- *Cost*
- *Implementation*

1. Build a small test environment, with possibility to send, receive and monitor wireless signal, and to apply the wireless shielding solutions.
2. Order several types of shielding solutions, from different companies, and apply them to the test environment.
3. Measure and compare the effiecency of the different shielding solutions.
4. Consider and compare the cost of applying the solution on the test environment.
5. Consider and compare the difficulty and time spent applying the solution on the test environment.
6. Based on the results, look for areas for further investigation and new ways to utilize the shielding solutions.

Chapter 2

Background material

The content of this chapter includes theory about the behavior and use of wireless signals in general, information about equipment for sending and receiving wireless signals, and information about wireless shielding solutions, both about published studies and existing products.

2.1 Wireless signals

Transmission of information over physical media touches on physics as it draws on ideas about electric current, light and other forms of electro-magnetic-radiation. Data communication also uses mathematics and different forms of analysis, since the information is digitalized and the digital data is transmitted. There are three main ideas that provides much of the background for data communication:

Sources of information can be arbitrary types - Information is not restricted to bits on computer, since it can be other media like audio and video. It is therefore important to understand that one form of information can be transformed into another.

Transmission uses physical system - Signal transmission need natural phenomenon, like electricity or electromagnetic radiation, to let information be transmitted. This makes it important to understand types and properties of media available, how information is transmitted over physical media, limits to physical systems, that problems that can arise during transmission and how to detect and solve such problems.

Multiple sources can share underlying medium - Most networks usually permits multiple entities to communicate over the same physical medium. It is therefore important to understand the possible ways underlying facilities can be shared, advantages and disadvantages of each and resulting modes of communication.

Data communication deal with two types of information: analog and digital. When an analog signal moves from on value to the next it move through all the intermediate values as well, while digital signals have fixed set of valid levels, and instantaneously move from one level to another. Signals are broadly classifies as periodic or aperiodic, depending of if they repeat or not. Much in data communication involves use

of sinusoidal trigonometric functions, and then especially sine. This is an important point since natural phenomena produce sine waves, as i.e. audible tone and electromagnetic radiation can be represented as sine waves as a function of time. There are four important characteristics of signals that are related to sine waves:

Frequency - number of oscillations per unit time (usually seconds). Frequency is usually measured in sine waves per second, Hertz or Hz, and a complete sine wave requires 2π radians. So if t is time in seconds and $\omega = 2\pi$, the function $\sin(\omega t)$ has the frequency of 1 Hz. Another way to calculate frequency is as the inverse of the time required for one cycle, or one period. This can be expressed as f=1/T, where f is frequency and T is the time for one period.

Amplitude - the difference between the maximum and minimum signal heights. As sin() produces values between -1 and +1 and has the amplitude of 1, the value can be multiplied with A to find that the amplitude of the resulting wave is A.

Phase - how far the start of the sine wave is shifted from reference time. In other words, phase is an offset that is added to t that shifts to the right or left along the x-axis.

Wavelength - length of a cycle as a signal propagates across a medium and is determined by the speed which the signal propagates. Finding the length of one wave can be expressed as c/f, where c is the speed of light and f the frequency.

Signals are either classified as simple or composite. Simple signals consists of a single sine wave and cannot be decomposed further, while composite signals can be decomposed into a set of simple sine waves. Composite signals are usually common in data communication, since they usually are the result of modulation, where the sender creates a composite signals and the receiver decompose the signal into the original components. As composite signals are fundamental there have been invented several methods to represent them. One is time domain, where the graph of a signal is represented as a function of time. Another alternative representation is known as frequency domain, which shows a set of sine waves that creates a composite function. The analog bandwidth of the signal is the difference between the highest and the lowest signal, and is trivial to compute if the signal is plotted in a frequency domain. [3, 4]

2.1.1 Transmission media

Transmission media is divided into type of path it takes and form of energy it uses. A signal can follow an exact path, as for cables, or no path at all, as for a radio transmission. A signal can also use electrical energy for cables, radio transition for wireless communication and light for optical fiber. The term guided or unguided transmission is used to distinguish between physical media that follows a specific path and radio transmission that travels through space in all directions. For unguided media transmission and reception is achieved by an antenna.

Electromagnetic communication uses electromagnetic energy in the Radio Frequency (RF) range as transmission media. RF energy has the ability to traverse long distances and penetrate items like walls and buildings, though the exact properties of

Band	Frequency range	Free-space wavelength range	Propagation characteristics	Typical use
ELF (extremely low frequency)	30 - 300 Hz	10,000 - 1000 km	GW	Power line frequencies; used by some home control system
VF (voice frequency)	300 - 3000Hz	1000 - 100 km	GW	Used by telephone system for analog subscriber lines
VLF (very low frequency)	3 - 30 kHz	100 - 10 km	GW; low attenuation day and night; high atmospheric noise level	Long-range navigation; submarine communication
LF	30 - 300 kHz (low frequency)	10 - 1 km	GW; slightly less reliable than VLF; absorption in daytime	Long-range navigation; marine communication radio bacons
MF	300 - 3000 kHz (medium frequency)	1,000 - 100 m	GW and night SW; attenuation low at night, high at day; atmospheric noise	Maritime radio; direction finding; AM broadcast
HF	3 - 30 MHz (high frequency)	100 - 10 m	SW; quality varies with time of day, season and frequency	Amateur radio; military communication
VHF	30 - 300 MHz (very high frequency)	10 - 1 m	LOS; scattering because of temperature inversion; cosmic noise	VHF television; FM broadcast and two-way radio; AM aircraft communication; aircraft navigational aids
UHF	300 - 3000 MHz (ultra high frequency)	100 - 10 cm	LOS; cosmic noise	UHF television; cellular telephone; radar; microwave links; personal communications system
SHF (super high frequency)	3 - 30 GHz	10 - 1 cm	LOS; rainfall attenuation above 10 GHz; atmospheric attenuation due to oxygen and water vapor	Satellite communication; radar; terrestrial microwave links; wireless local loop
EHF (extremely high frequency)	30 - 300 GHz	10 - 1 mm	LOS; atmospheric attenuation due to oxygen and water vapor	Experimental; wireless local loop; radio astronomy system for analog subscriber lines
Infrared	300 GHz - 400 THz	1 mm - 770 nm	LOS	Infrared LAN; consumer electronic applications
Visible light	400 - 900 THz	770 - 330 nm	LOS	Optical communication

Table 2.1: Frequency bands

a electromagnetic signal depends on its frequency. To refer to possible frequencies the term spectrum is often used, and the possible frequencies are usually allocated by government, and thus the spectrum are different from country to country. The spectrum of RF communication have the frequency range from approximately 3 kHz to 300 GHz, though the range from 30 GHz to 300 GHz is reserved for experimental testing. This spectrum may also be divided into two; the broadcast radio frequency and the microwave frequency. An more advance overview of the frequency bands are found in table 2.1.

Broadcast radio - The most principal difference between broadcast radio and microwave is that broadcast radio is omnidirectional, while microwave is directional. This mean that broadcast radio do not require dish-shaped antennas, and the antenna does not need to be rigidly mounted or precise aligned. The frequency range of broadcast radio is from 3 MHz to 1 GHz, and is often called radio range. This range covers FM radio, UHF and VHF television and number of data networking applications. Since the ionosphere is transparent to frequencies over 30 MHz transmission for broadcast radio is limited to line of sight (LOS), but distant transmitters will not interfere with each other since there are no reflection from the atmosphere. Broadcast radio is less sensitive to attenuation from distance than microwave, due to longer wavelength. The prime source of interference for broadcast radio is from multipath interference, where signals are reflected from land, water and other object.

Microwave frequency - Since microwave signals are directional the most common antenna is the parabolic dish, which has to be rigidly fixed and aligned to achieve a line of sight transmission to a receiving antenna. The antennas are usually located substantial height above ground level to be able to transmit above intervening obstacles. The most common frequencies are found in the range 1GHz to 40GHz, where a high frequency means higher potential bandwidth and therefor a higher potential data rate. A overview of the data rate performance compared to frequency is found in table 2.2. Microwave is commonly used for voice, television transmission, and increasingly for short point-to-point transmission between buildings. Other important uses for microwave includes cellular and satellite communication. The main source for microwave is attenuation, which increases with distance and rainfall. Another impairment, growing due to the popularity of microwave, is interference. Because of this the frequency bands for microwave is strictly regulated.

Band (GHz)	Bandwidth (MHz)	Data rate (Mbps)
2	7	12
6	30	90
11	40	135
18	220	274

Table 2.2: Typical Digital Microwave Performance

Another media for wireless communication is Infrared (IF) signals. Infrared signals uses the same communication technology as television remote which sends out a signal that behaves in the same way as visible light, but outside visible range of human eye. To successfully send and receive infrared signal line of sight is needed, either directly or through reflection, as the signal is reflected by smooth, hard surface, but opaque object and moisture blocks the signal. The infrared signal Covers arc of 30° and disperse quickly, but is Useful for point-to-point and multi point in confined area. The infrared frequency range is 300GHz to 400THz and has no frequency allocation, because no licensing is required. [3, 4]

2.1.2 Decibel

Decibel (dB) is used as an unit for expressing for the measurement of gain and loss for sound, electronic or mechanical power and voltage. Decibel is used by the telecomputing industry to express gain or loss in a medium, like copper, optical fiber or wireless, for transmission systems. In reality, the decibel is the relationship between a reference point and another point, either above or below the reference point. This base reference point is set to 0 dB, while all subsequent measurements are relevant to this reference point. To indicate the context of the measurement, decibel is often used along with a notation, such as:

dBi - antenna gain in dB relative to an isotopic source

dBm - power in dB relative to 1 milliwatt

dBW - power in dB relative to 1 watt

dBmV - reference to 1 millivolt, often used to as a measure of signal levels (or noise) on a network

The dBm is used in electronics to present sent power in a logarithmic scale, with 1 milliwatt as a reference point. If the actual power is represented as p milliwatt, then the dB m values equals to $10\log_{10}(p)$. Since the scale of dBm is based on a logarithmic scale the difference in 10 dBm represent a 10-fold change. A dB W scale, using a full watt reference point rather a milliwatt, for larger power levels. Since 1 watt equals 1000 milliwatt, 1dB W = 30 dBm [5, 6, 7].

2.1.3 Near-field and far-field field regions

The area around a transmitting antenna, can essentially be divided into two regions, a near-field and a near-field region. For antennas with the maximum overall dimension considered small when compared to the wavelength, the near-field region is mostly reactive, and the electromagnetic components store energy while producing little radiation. The stored energy is periodically transfered between the antenna and the near-field. The reactive near-field extends from the antenna to the the distance R [8]

$$R = \lambda/2\pi \tag{2.1}$$

λ= the wavelength

For field strength in the near-field region for small antennas there are no general formula for estimation, and exact calculations can only be made for well-defined sources. Antennas considered large compared to the wavelength, the near-field consist of a reactive field followed by a radiation region. In the radiation near-field the field strength do not necessarily decrease with distance. The commonly used criterion for defining the distance from the source where the far-field begins is [8]

$$R = 2a^2/\lambda \tag{2.2}$$

a = the greatest dimension of the antenna

For paraboloidal circular antennas another criterion is used for finding the far-field [8, 9, 10, 11].

2.1.4 Transmission impairments

Within all communications systems, the transmitted signal may be changes by various transmission impairments, to differ from the receives signal. These impairments may be caused by attenuation in the media or noise and interference.

Attenuation - The strength of a signal falls with distance for any transmission media. For guided media attenuation generally is exponential, and is typically expressed as a constant fall per unit of distance. Attenuation in unguided media however, is a more complex function of distance and conditions in the atmosphere, and is also the main source for loss. Additionally, the attenuation is greater at higher frequencies and, in outdoor systems, with rainfall. Even if there are no other sources of attenuation impairments is assumed than distance, a transmitted signal attenuation because the signal is spread over a increasingly larger area. This type of attenuation is known as free space loss, and can be expresses as the ratio of the transmitted power P_t to the received power P_r by the antenna. To get this in dB, log_{10} can be taken of that ratio. For ideal isotopic antenna, free space loss is [4]

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi fd)^2}{c^2} \tag{2.3}$$

P_t = signal power at the transmitting antenna
P_r = signal power at the receiving antenna
λ = carrier wavelength
d = propagation distance between antennas
c = speed of light (3 x 108 m/s)
The unit of both d and λ is in meter.

This can be recast to find the loss in dB as [4]

$$L_{dB} = 10log_{10}\frac{P_t}{P_r} = log_{10}(\frac{4\pi d}{\lambda^2})^2 dB \tag{2.4}$$

L_{dB} = loss
d = distance
λ = wavelength
As loss can be compensated with antenna gain, antenna gain must be taken into account for non-isotopic antennas. This yields the following relationship between antenna gain and effective area [4]

$$\frac{P_t}{P_r} = \frac{(4\pi)^2(d)^2}{G_r G_t \lambda^2} = \frac{(\lambda d)^2}{A_r A_t} = \frac{(cd)^2}{f^2 A_r A_t}$$

G_t = gain of the transmitting antenna
G_r = gain of the receiving antenna
A_t = effective area of the transmitting antenna
A_r = effective area of the receiving antenna

A greater attenuation is found when a signal is traversing through other media than free space. Some examples of objects are 3dB for plasterboard walls, 4dB for cinder block and 6dB for Glass wall with metal frame [12]. Other studies have also been made regarding other building materials.

Multipath fading - described as the condition where transmitted radio signal are reflected by nearby physical object (i.e. buildings, bodies of water, vehicles, walls etc.), creating multiple signal path between the transmitting and receiving antenna. When these indirect signals arrive at the receiving antenna, they can either add to or subtract from the direct signal. If the indirect signal add or subtract, depends if it is in phase or out of phase with the direct signal. As indirect signals have been traveling through different path, there will be experienced random fluctuations in both amplitude and phase in received signal. If there is a random variation in the signal, typically encountered in a wireless environment, this is referred to as Rayleigh multipath fading. If there is a dominant signal or path, such as line of sight, between the transmitter and receiver, the multipath is referred to as Rician multipath fading [13, 14, 12].

Absorption - Some objects can absorb signals. Water is a prime signal absorber above the 2 GHz range. Therefore organic materials tend to absorb more wireless signals than inorganic materials. This is also why microwave ovens also use the 2.4 GHz frequency range. Because water cannot vibrate fast enough to keep up with the RF waves, the energy is absorbed in stead. Humans contain a large amount of water, and will therefore also absorb a large amount of a RF signal [15, 12, 13].

2.1.5 Wireless LAN

The article Trends in Local Wireless Networks by Kaveh Pahlavan and more [16], lines out four application areas for Wireless LAN (WLAN): LAN extension, cross building interconnect, nomadic access and ad hoc networks.

LAN extension - Wireless LAN was introduced as substitute for wired LAN in late 1980s, where it was marked to save the cost of installation, relocation and modification to the network structure. However when the awareness to LAN became greater, architects started designing building with prewiring and consideration to data applications. also, because of the advances in data transmission, there are an increased reliance of twisted pair cabling for LAN. Still there is a large role for wireless as alternative to wired LAN in i.e. large open areas such as warehouses and open office landscapes, historical buildings where drilling holes are prohibited and small offices where wiring is not economically. In all these examples wired connection is till needed for support servers and some stationary workstations.

Cross-building interconnect - The Use of wireless LAN technology to connect LAN in nearby buildings, i.e. point to point wireless link with microwave or infrared transmitter/receiver placed on rooftops of building with LOS. The connected devices are usually routers or bridges.

Nomadic access - Provides a wireless link between LAN hub and a mobile data terminal with an antenna. This is useful for data transfer from a portable computer to a server. An area of application for this could be in an extended environment like a campus or a business with clustered buildings. This will enable users with portable computers to move around and access servers and wired LAN from various locations within range of the wired network.

Ad hoc networking - with this type of networking a peer-to-peer network is set up temporarily for immediate need, without any real infrastructure. I.e. group of employees with convene in a conference room and links their computers into a temporary network for the duration of meeting. a peer collection of stations within range may also dynamically configure themselves into a temporary network.

WLAN is is most cases used as an adjunct to traditional wired LAN to satisfy requirements for mobility, relocation, ad hoc networking and coverage of location difficult to wire. The most prominent specification of WLAN was developed developed by IEEE 802.11, but has been little used until recently because of high prices, low data rates, safety and security concerns and licensing of frequencies. the IEEE 802 committee formed IEEE 802.11 in 1990 specifically devoted to wireless LAN. This committee issued a list of standards to keep pace with demand for WLAN at different frequencies and data rates. The 802.11b standard was first standard to gain broad industrial acceptance, because of its higher data rates. The Wireless Ethernet Compatibility Alliance (WECA), subsequently called WiFi Alliance, was formed 1999 to meet concern of products from different vendors interoperation. The WiFi Alliance's responsibility is to certify the interoperability for 802.11b products. They have also extended certification to 802.11g products and is working on the certification for 802.11a products.

Physical layer are issued in five layers in IEEE 802.11 (also shown in table 2.4)

- IEEE802.11: MAC layer, three physical layer specific; two 2.4 GHz band and one infrared operating at 1 and 2 Mbps

- IEEE802.11a operates in 5 GHz band at 11 Mbps
- IEEE802.11b operates in 2.4 GHz band at 5.5 and 11 Mbps
- IEEE802.11g operates in 2.4 GHz band at 54 Mbps
- IEEE802.11n operates either 2.4GHz or 5 GHz band at hundreds of Gbps

A full overview of the IEEE 803.11 standards are shown in table 2.3.

It is possible to use WLAN without licensing procedure, but the licensing regulation differ from country to country. In the US, FCC authorize two unlicensed application within ISM band: Spread spectrum system which operate up to 1 W and very low powered systems which operate up to 0.5 W. The spread spectrum got quite popular after opened for the public by FFC. In the US three microwave bands is set aside for unlicensed spread spectrum use: 902-928 MHz (915 MHz band), 2.4-2.4835 GHz (2.4 GHz band) and 5.725-5.825 GHz (5.8 GHz band). The 2.4 GHz band is used in same manner in Europe and Japan. Cordless telephones, wireless microphones, amateur radio etc. operate at the 900 MHz band, so the chance for inference from other devices are quite high. There are fewer devices operating at the 2.4 GHz band, but there are an exception with the microwave oven which has a greater radiation leakage with age. There are little competition at the 5.8 GHz band, but to access this band more expensive equipment is needed. For WLAN higher bandwidth means a higher potential bandwidth, but it also means a higher potential for interference.

Currently WLAN are generally categorized into three transmission technique categories:

Spread spectrum LAN - operates in ISM (industrial, scientific and medical) 2.4 GHz microwave band so no Federal Communication Commission (FCC) licensing is required in the US.

OFDM LAN - a technology called orthogonal frequency division multiplexing (OFDM) which is superior to spread spectrum for higher speeds. OFDM operates in the 2.4 GHz or 5 GHz band.

Infrared (IR) LAN - limited to single room, because infrared light do not penetrate walls. Infrared LAN are not much used though.

The three physical media described in the original 802.11 standard includes : Direct sequence spread spectrum (DSSS) that operates in 2.4 GHz ISM band at 1 and 2 Mbps. This spectrum require no licensing by the FCC. The channels available on the spectrum depends on various national regulatory agencies, but uses 13 channels in most of Europe. the Frequency-hopping spread spectrum (FHSS) operates in 2.4 GHz ISM band at 1 and 2 Mbps. The channels ranges from 23 in Japan to 70 in the US. Infrared sends at 1 and 2 Mbps, and operates at a wavelength between 850 and 950 nm. Additionally, according to the IEE 802.11 standard, the receiver sensitivity is defined have a bit rate of 1 Mbps at -80 dBm, or 2 Mbps at -75 dBm[17].

IEEE 802.11b is an extension of the IEEE 802.11 DSSS scheme, providing data at 5.5 and 11 Mbps at ISM band. This standard uses a modulation scheme known as complementary code keying (CCK) to achieve higher bit rate in same bandwidth and chipping rate. IEEE 802.11a was developed to compensate for 802.11b limited data, and uses the frequency band called Universal Networking Information Infrastructure (UNNI), which is divided into three parts:

- UNNI-1 band (5.15-5.25 GHz) for indoor use
- UNNI-2 band (5.25-5-35 GHz) for both indoor and outdoor
- UNNI-3 band (5.35-5.825 GHz) for outdoor

It also uses OFDM (orthogonal frequency spectrum) instead of the spread spectrum scheme. OFDM sends multiple carrier signals on different frequencies, but unlike FDM all the subchannels are dedicated to a single data source. IEEE 802.11g extends 802.11a to data rates above 20Mbps up to 54 Mbps, and as 802.11g and 802.11b both operates in the 2.4GHz range, the two are compatible.

The 802.11 committee have been looking for ways to increase data input and overall capacity, with the goal not only to increase the bit rate from the transmitting antennas but also increase the effective throughput of the network. the result is a package of improvements and enhancements embodied in a IEEE 802.11n standards. The changes is generally found in areas: MIMO, enhancements in radio transmission and MAC enhancements.

Multiple-input-multiple-output (MIMO) - the transmitter employs multiple antennas. The source stream divided into n substreams, one for each antenna. Individual substreams the input to multiple antennas. At the receiving end, m antennas receive transmission from the n source antennas via a combination of LOS and multipath. Outputs from the m antennas are combined with the signals from other received radios. The result is a much better received signal than achieved with single antenna or multiple frequency channels, but requires complex mathematics.

Radio transmission scheme - there are number of changes in this scheme, but the most significant technique, known as channel bonding, combines two of the 20 MHz channels to create a 40 MHz channel. When using OFDM this allows twice as many subchannels, doubling the transmission rate.

MAC enhancements - the most significant change is to aggregate multiple MAC frames into a single block for transmission. Station acquire the median from transmission and transmit long packets without significant delay between transmissions, and the receiver sends a single block ACK.

Security considerations in the IEEE 803.11 standard includes that stations need to be physically connected in wired LAN to be able to receive and transmit, Authentication where IEEE 802.11 supports several authentication schemes and allows expansion for their functionality and privacy to prevent content of messages to be read by others than

the recipient. The standard provides optional use of encryption to provide privacy. The security features for privacy and authentication for original 802.11 were quite weak, using the standard used Wired Equivalent Privacy (WEP) algorithm. To improve the encryption in the standard, WiFi Alliance promulgated WiFi Protected Access (WPA) as Wi-Fi standard as introduction of strong security into WLAN.

Wireless LAN must meet same requirement as any LAN with regard for high capacity, coverage of short distances, full connectivity and broadcast connectivity, but there are also specific requirement for wireless LAN in addition. The most important requirements specific for WLAN are the following:

- Throughput - MAC should make efficient use of wireless medium for maximize capacity
- Number of nodes - Wireless LAN may need to support hundreds of nodes
- Connection to backbone LAN - interconnection with station on wired backbone LAN is required in most cases. Accomplished with control modules. Accommodation for mobile users and ad hoc networks.
- Service area - typical coverage area; diameter of 100 to 300 m
- Battery power consumption - mobile users use battery-powered workstations that need long battery life. Typical WLAN implementation have features to reduce power consumption
- Transmission robustness and security - WLAN vulnerable to interference and eavesdropping if not properly designed. Design should permit reliable transmission and some level of security
- Collocated network operation - more WLAN operate in same area. May interfere with normal operation, allow unauthorized access
- License-free operation - users prefer WLAN products without securing license for frequency band
- Handoff/roaming - MAC should enable mobile station to move from one cell to another
- Dynamic configuration - MAC addressing and network management should permit dynamic and automated addition, deletion and relocation of end system without distribution to users

The architecture of WLAN are divided into three building blocks: access point (informally base station), interconnection mechanism (switch or router connected to access points) and a set of wireless hosts (also wireless nodes or wireless stations). WLAN can be arranged into multiple cells for larger networks, but adjacent cells should use different center frequencies to avoid interference. The topology for cells is either hub or peer-to-peer [18]

Standard	Scope
IEEE 802.11	Medium access control (MAC): One common MAC for WLAN applications Physical layer: Infrared at 1 Mbps and 2 Mbps Physical layer: 2.4 GHz FHSS at 1 Mbps and 2 Mbps Physical layer: 2.4 GHz DSSS at 1 Mbps and 2 Mbps
IEEE 802.11a	Physical layer: 5 GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4 GHz DSSS at 5.5 Mbps and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLAN to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	Recommended practices for multivendor access point interoperability
IEEE 802.11g	Physical layer: Extend 802.11b to data rates ¿20 Mbps
IEEE 802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Physical layer: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial correction
IEEE 802.11n	Physical/MAC: Enhancement to enable higher throughput
IEEE 802.11p	Physical/MAC: Wireless access for vehicular environments
IEEE 802.11r	Physical/MAC: Fast roaming (fast BSS transition)
IEEE 802.11s	Physical/MAC: ESS mesh networking
IEEE 802.11T	Recommended practice for the evaluation of 802.11 wireless performance
IEEE 802.11u	Physical/MAC: Interworking with external networks
IEEE 802.11w	MAC: data integrity, data origin authenticity, replay protection, and data confidentiality for MAC management frames
IEEE 802.11y	Physical layer: Extend 802.11a to include 3650-3700 MHz band
IEEE 802.11z	MAC: Amendment to define a new direct link setup (DLS) mechanism to allow operation with non-DLS capable access points
IEEE 802.11aa	MAC: Enhancement for robust audio video streaming
IEEE 802.11ad	Operation in the 60 GHz band
IEEE 802.11ae	Mechanisms for prioritizing IEEE 802.11 management frames
IEEE 802.11af	Modifications to allow 802.11 wireless networks to be used in the TV white space

Table 2.3: Overview IEEE 802.11 standards

	802.11a	802.11b	802.11g	802.11n
Peak Data Throughput	23 Mbps	6 Mbps	23 Mbps	60 Mbps (20 MHz channel) 90 Mbps (40 MHz channel)
Peak Signaling Rate	54 Mbps	11 Mbps	54 Mbps	124 Mbps (20 MHz channel) 248 Mbps (40 MHz channel)
RF Band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz or 5 GHz
Channel Width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Number of Spatial Streams	1	1	1	1, 2, 3 or 4

Table 2.4: Physical layer standards

2.1.6 Security

Because radio waves travel through air, signals from different senders can interfere with or even be mistaken for each other. The fact that all receivers within range with the right equipment can intercept the transmitted signals, and that nearby malicious users can launch attacks that bypass firewalls and IDS, creates threats and vulnerabilities unique to WLAN and makes security a major issue.

Most of the following threats and vulnerabilities describes in this report is listed in the article Wireless Network Security: Vulnerabilities, Threats and Countermeasures, written by M. Choi and group [19].

Accidental association - Users may gain unauthorized access to a network by any number of methods or intentions. Accidental association is described as when a user's computer latches on to a neighboring, overlapping network by accident. This might really become a problem if this creates a link between two companies network. Another problem is if the user uses the connection for bad behavior, like sending spam mail.

Malicious association - Malicious users can make wireless devices connect to a company's network through their cracking laptop instead of the company's access point. Since wireless networks work on layer 2, layer 3's authentication and Virtual Private Network (VPN) will not create any barrier against this type of attack. Wireless 802.1x do ask for authentication, but is still vulnerable to cracking. Once the malicious user got access to the network, it is open for attacks or theft of information. [20]

Identity theft - As the name implies, identity theft is when someone is taking another person's identity, or related to networks and computers, another persons user account. If an attacker gains access to a network in one way, this again gives access to new possibilities for access, and consequently more data and resources. Identity theft for WLAN, also called MAC spoofing, is when an attacker is able to listen in on network traffic and be able to identify the MAC address of a computer with network privileges. The attacker can then gain access to the network using this MAC address. [21, 22]

Man-in the-middle attacks - Man-in-the-middle attacks can come in two different forms: eavesdropping and manipulation. Eavesdropping is describes as more information leaking than an attack, where an eavesdropper can record and analyze data collected from a communication stream. A manipulation occurs when an attacker not just receive the data, but also retransmit it after changing it.

Eavesdropping on a wireless network is easy because the signals travel by air. A signal transmitted can easily be picked up without any substantial effort or equipment. If the interceptor is just passively listening, this can be done with an insignificant chance for detection. All frames or packages can then be examined in detail and then, if wanted, stored. Since the transmission range of WLAN is limited to hundreds of meters, the eavesdropper has to be relatively close to the

source of the signal.

The next step from eavesdropping is manipulation. The attacker can either masquerade as a client in the network or introduce a rogue access point by manipulating the data sent in a WLAN. Introducing a rogue access point is done through security faults in the protocols, and called a ”de-authorization attack”. This attack forces the clients of a network to disconnect from the network and connect to the malicious access point. These types of attacks are often done using software that automates certain steps in the process [23, 24, 25, 26, 22].

Denial of service (DoS attack) - DoS attacks are devastating to a network and difficult to protect against. A malicious user can block legitimate users or even crash the network by flooding false requests, premature connection success messages, failure messages and other commands.

DoS attacks can target different layers of the network. While a Dos attack on the application and transport layer has no fundamental difference from wired network, a DoS attack on the network, data-link and physical layer has critical differences. This thesis only deal with the layers which differ from wired networks.

A DoS attack at the network layer (OSI layer 3) happens if a malicious user is able to be associated in the network, and he/she either flood the access point with packets or transfer large files to it. This way the bandwidth of the access point will be saturated, and other clients will have a difficult time sending packets.

An attacker that uses malicious association and identity theft can do an DoS attack at the data-link layer (OSI layer 2) to make the access point disregard other clients. This is done by spoofing the Mac address of a client and simply sends frames with a stronger signal than this client. The access point will choose to send and receive the stronger signal and ignore traffic from the weaker source.

A way to effectively take wireless devices offline and create an DoS attack at the physical layer (OSI layer 1), is to send enough Radio Frequency (RF) noise on the same frequency as the wireless network devices. The devices in the area will then not be able to distinguish the valid network signal from the random noise, and therefore will be unable to communicate. Creating a jamming device is quite easy, just removing the metal shielding of a normal microwave oven will give you a 1000W radio transmitter. [19, 23, 27, 24, 25, 20, 26].

Network injection - Access points exposed to non-filtered network traffic, especially broadcast networks (spanning tree, OSPF, RIP, HSRP), can be injected with bogus re-configuration commands. This can affect routers, switches and intelligent hubs in a way that the entire network goes down. To bring the network up again a reboot or even reprogramming of the intelligent network devices might be necessary.

Caffe latte attack - There is a way for an attacker to take advantage of the shared key authentication and the message modification flaws in 802.11 WEP. By targeting the Windows wireless stack and sending a flood of ARP requests an attacker can use the ARP responses to gain a WEP key in less than 6 minutes.

To counter the vulnerabilities and attacks unique to wireless communication, several security measures have been produced, like encryption and signal hiding. For some of the attacks the only defense is shielding the network entirely against external signals. Shielding though is regarded as expensive solution that is inconvenient to implement. Because of it attributes shielding will also block desired signals, like those from radio and cellular transmissions.

As with the threats, most of the countermeasures in this report are listed in the article Wireless Network Security: Vulnerabilities, Threats and Countermeasures, written by M. Choi and group [19].

Signal hiding techniques - To be able to intercept a wireless signal, an attacker must first be able to identify and locate the wireless network. There are several ways to make it more difficult to locate a wireless access point. One of them is to turn off the Service Set Identifier (SSID) broadcasting from access points. This will reverse the order of steps in the wireless router protocol, where a client sends a signal seeking an access point with a particular SSID, rather than the access point broadcasting it. This 'closed mode' does not prevent knowledge of the SSID though, as the initial exchange can be intercepted by anyone eavesdropping in communication range. Lowering the signal to the lowest level that still provides coverage of the building is another solution. The most effective, but also the most expensive, is to use directional antennas or using signal emanation-shielding techniques. Different shielding techniques will be described later in this thesis [23, 20, 22].

Encryption - One of the best way to protect the confidentiality of a wireless network is to encrypt all wireless traffic. Cryptography is rooted in higher mathematics, group and field theory, computational complexity and real analysis, probability and statistics. Although it is not necessary to understand the underlying mathematics to use encryption. If the data is well-disguised it cannot be read, modified or fabricated easily. Strong encryption can also significantly reduce the risk of man-in-the-middle attacks. Most wireless routers come with encryption built in, but they are often delivered with this feature turned off.

David Johansson and Alexander Sandström Krantz [27] have written a paper where they compare WEP with WPA. Halil Ibrahim Bulbul [28] also takes RSN in consideration. They write that the wireless encryption protocol WEP (Wireless Equivalent Privacy) is the initial security mechanism of WLAN. Though several serious weaknesses have been identified in WEP, it is still widely used. WEP was superseded by WPA (Wi-Fi Protected Access) in 2003, and then by the full 802.11i standard RSN (also known as WPA2) in 2004 [23, 28, 21, 25, 20].

The intension of WEP was to create a level of security equivalent to that of a wired network, but practice has shown this is hardly the truth. Some of the weaknesses in WEP is that it uses the master key directly, it has a small key size (40 or 104 bits), use of RC4 key cipher (considered to have weak keys), reuse and small sized IV (Initialization Vector), weakness of ICV algorithm (for detecting noise and common error in transmission) and easy to forge authentication messages. Brute force attack on a WEP 40-bit key will succeed quickly, and even the 104 bit version is easily defeated because of flaws in the RC4 algorithm. There are also several tools available that cracks a WEP encryptions in a few minutes, and even the FBI (at an conference in 2005) have demonstrated the ease of how a WEP secured wireless session can be broken [22].

WPA was designed to improve the security flaws in WEP. The main improvements over WEP are: Improved data encryption (scrambling the keys and adding an integrity-checking feature), user authentication and integrity using a mechanism MIC (Message Integrity Code) that detects errors in the data content. One alleged drawback with WPA is that keys generated from short passwords is subject to dictionary attack and a key generated from a pass phrase shorter than 20 characters are unlikely to deter attacks.

RSN (Robust Security Network) emerged in 2004 as a need for wireless devices to support additional capabilities. This standard uses the IEEE 802.1x standard for access control and AES (Advanced Encryption Standard) for encryption. It also uses a pair-wise key exchange for authentication and key management. The authentication scheme is based on 802.1x and EAP (Extensible Authentication Protocol).

Using EAP and AES, RSN is significantly stronger than WEP and WPA, however only the latest devices will have capability required to provide the performance expected of today's WLAN products.

Both L.J. Lee [21] and J. Hindström [20] describes another way to secure a WLAN, with using VPN (Virtual Private Network). While the previously mentioned protocols operates on layer 2 (data-link), VPN however, operates on layer 3.

VPN is primarily used for used for creating a secure channel between two private networks through a insecure public network, also called a tunnel or tunneling. The technology is intended for the Internet, but it is also possible to create a link in a insecure wireless network. Many firewalls can be used for VPN implementation, where users can request VPS sessions from the firewall. The users client and the firewall will then negotiate a session encryption key, and this key will then be used to encrypt the traffic between the user and firewall [22]. The two most common encryption algorithms used for VPN are IPsec and PPTP.

Since VPN uses 3DES or MPPE encryption this makes it much harder to crack than the WEP native standards. VPN also provides authentication for individual users, while WEP users shares one encryption key. The problem with VPN is that it requires a central server to handle authentication at data communication. VPN also only protect the integrity and security of data transmitted on the network, but will not secure the channel. With VPN an intruder can still access the wired network or potentially launch a DoS attack.

Authentication - using 802.1x on the network will authenticate all devices connected to the network, and prevent unauthorized devices (rogue access points) from connecting. It is important to change the default authentication setting to create strong authentication since these settings are well known. Authentication is traditionally achieved through the use of certified public-key or shared secret keys.

For private communication between two entities secret key establishment is fundamental. Suman Jana with group [29] write that the most common way of using secret key currently is using public key cryptography, but since this consumes computer resources they report that research is being done with e.g. using Quantum cryptography.

Audit - before setting up a wireless network a careful site survey should be done. That way the location of devices with signals with the possibility of causing unintentional DOS attacks will be identified. The result of this survey can also help with deciding where to locate wireless access points. Regular audits of the wireless networks should also be performed to find and remove offending devices (rogue access points) or increase the signal strength and coverage. The only solution to completely secure a WLAN against all external DoS attacks is setting up an EMI shield [19, 23, 27, 24, 25, 20].

WiFi Protected Access (WPA) as a standard was promulgated by the Wi-Fi alliance to introduce strong security to WLAN. WPA is a set of security mechanisms that eliminates most of 802.11 security issues and is based on current state of the 802.11i standard. IEEE 802.11 addresses three main security areas: authentication, key management and data transfer privacy.

IEEE 802.11i require the use of a authentication server (AS) for more robust authentication protocol, where the AS plays role in the key distribution. For security 802.11i provides three different encryption schemes. The scheme for long time solutions is Advances Encryption Standard (AES) with a 128-bit key, but this require extensive upgrade to existing equipment. Alternative schemes based one 104-bit RC4 is also defined in the standard.

802.11i architecture consists of three ingredients:

Authentication - protocol to define exchange between user and AS that provides authentication and generates temporary keys to be used.

Access control - enforces authentication functions, routes message properly, facilitates key exchange.

Privacy and message integrity - MAC-level data encryption, message integrity code to ensure that data not been altered.

Authentication that operates in the level above LLC and MAC protocols are considered beyond the scope of 802.11, also there is other popular authentication, like EAP and RADIUS, that will not be covered in this rapport [22].

2.2 Equipment for sending and receiving signals

This section includes information about equipment for sending, receiving and testing in general and for specific products.

2.2.1 Wireless Network Analyzer

Network analyzers comes in two categories; vector analyzers which can measure complex reflections (magnitude and phase) and transmission of a signal, while scalar analyzers only measure magnitude. Network analyzers in general can measure impedance, VSWR (Voltage Standing Wave Ratio, the voltage ratio of the amplitude of a standing wave), loss or gain in signal amplitude, isolation and group delay (measure of time distortion) of any two ports of multi-port network. The two mayor manufacturer of network analyzers are Agilent and Anritsu

The key features for antenna measurements are high sensitivity to reduce measurement uncertainties, increase speed to decrease test time and cost, flexibility that makes the equipment upgradeable for future testing, security to enable multiple users. There are two methods for testing, near-field and far-field, to chose from for antenna measurements [30].

2.2.2 Software sending Wi-Fi

A simple wireless router can be used for sending wireless signals on the IEEE 802.11 standard frequency bands. Most routers have implemented firmware with options to change certain settings for the router, though these are usually limited in the included firmware. Especially options for signal strength are usually lacking in the included firmware, a feature that is useful when experimenting with signal range and the attenuation ability of the environment. To apply more features to the router, it is possible to install new firmware on the router. There are several free firmware available, but the two perhaps best known are DD-WRT and Tomato.

DD-WRT (DD is the car number plate code in Dresden) is a third-party firmware developed in the term of GPL for a variety of IEEE 802.11a/b/g/h/n wireless router based on Broadcom or Atheros chip reference design. DD-WRT is Linux based and open source, and the first versions were based on Alchemy firmware by Sveacorp Inc, but is now maintained by Sebastian Gottschall (aka BrainSlayer).

Download is available for free for private use, but commercial purposes require a paid license. The main emphasis is focused on providing easy handling while supporting great number of functionalities within hardware platform used, though speed and stability also is important. The GUI is logical structured and operated through web browser, where the functionalities can be configured. Some of the functionalities are 802.1* Extensible Access Protocol (EAP), Access restrictions, Ad hoc mode, DMZ settings, QOS Bandwidth management, syslog, SSH/Telnet server and client and several wireless client modes. DD-WRT has a huge user community that gives help both to the developers and other users. Help and support and most of the documentation can be found in forums and wiki, both managed by the users themselves, are available on the DD-WRT website. [31, 32]

Tomato is a small open-sources, Linux bases replacement firmware made for Broadcom-based routers based on Linksys' source code. Tomato was created with emphasis on stability, speed and efficiency by Polarcloud. Tomato has a web-based user interface in a GUI fashion made in Ajax, where the available features can be reached. Some of these features are realtime broadband-usage monitor, QOS with 10 unique QOS classes defined, access restriction and several wireless client modes. Tomato has also raised the limit for the maximum connection for P2P and allow custom script or SSH/Telnet in. [33, 34]

2.2.3 Signal generator

A radio frequency (RF) signal generator is essential to any RF design or test laboratory. a RF signal generator will enable signals to be generated, that will be to be fed into RF circuits so that their operation can be viewed when operating under various signal conditions. A number of specification are associated with any RF signal generator. Some of them are fairly common to all applications, so it is necessary to ensure that all requirements for a signal generator is captured and noted. The following list contains some of the more common parameters for a RF signal generator:

- Frequency range - the range of the frequencies to cover.
- Harmonics and spurious signals - all signal generators generate some level of spurious signals, but harmonics are generally much higher as a considerable effort is used to reduce intermodulation and other non-harmonic spurious signals.
- Power output - for most signal generators the power output is defined in dBm, although different signal generator have different output levels. The most common is +13dBm, although the maximum level is normally in the range of 10 to 20dBm (10 to 100 mW).
- Power accuracy - for many test scenarios it is necessary for the output to be accurately known, as the response of the unit might vary according to signal generator level. A result of the way the output level is controlled, there are two elements to the output level accuracy: An attenuator that gives the ability to vary

the output level, and a amplifier (with a feedback loop) which is used to maintain a fixed level. The accuracy of the attenuator provides the relative accuracy while the maintained level of the amplifier provides the absolute level accuracy.

- Phase noise - many signal generators fall into the category synthesized signal generators. While these signal generators offers many advantages from exact frequency selection to stability and high levels of programmability, issue of phase noise can be a problem in some of the generators. This makes it necessary to also carefully consider the phase noise spec of a signal generator.

- Accuracy - for RF signal generators using frequency synthesizers, the frequency accuracy is determined by the frequency standard used by the signal generator. The frequency standards define the accuracy with a number of specification which, if combined in the correct manner, gives the overall accuracy. Though also elements like including temperature stability, line voltage stability, aging, etc. need to be added statistically for a more correct overall accuracy.

- Modulation formats - most signal generators have the ability to modulate signals in a variety of ways, but some provides more flexibility than others. Originally many signal generators only had the capability to have amplitude and frequency modulation applied, but radio and wireless systems uses far more advanced forms of modulation [35].

2.2.4 Spectrum analyzer

A spectrum analyzer is a wide band, very sensitive receiver and an invaluable item of electronic test equipment. It is used in design, test and maintenance of radio frequency circuitry and equipment, and ranges from handheld equipment to high performance benchtop instruments. Like an oscilloscope, a spectrum analyzer is a basic tool for observing signals, but while an oscilloscope look at signals in a time domain spectrum, a spectrum analyzer display look at signals in a frequency domain. It converts the higher frequencies (normally ranging up to several 10s of GHz) to a measurable quantities. the received frequency spectrum slowly swept through range of pre-selected frequencies, converting to measurable DC level (usually logarithmic scale), and displayed it on a CRT. The display of a spectrum analyzer will show the amplitude of the signal at a vertical scale and the frequency at the horizontal scale. The received signal strength is normally measured in decibels (dBm). The primary reason for measuring power in dBm rather than voltage are the low signal strength, and the frequency range of measurement. A spectrum analyzer is capable of measuring frequency response of devices as low as -120dBm [36, 37].

In view of the way of the display output, spectrum analyzers are widely used looking at a spectrum generated by a source. Spurious signals including harmonics, intermodulation products, noise and other signals can this way be monitored to discover if it conforms to the required levels. With a spectrum analyzer it is also possible to make measurements of bandwidth of modulated signals to be checked if within required mask. Another use is checking and testing response of filters and networks. Some of the key features of spectrum analyzers are:

- Resolution bandwidth - an important parameter as the sensitivity directly dependent of the resolution bandwidth (RBM). For wide band 3kHz RBM is sufficient. For very narrow band measurement 300Hz or 10Hz RBM should be considered.
- Frequency range - the range of frequencies to take measurements. The frequency range for available for spectrum analyzers ranges from 100 Hz to 50 GHz.
- Frequency stability - the ability to maintain frequencies within specified accuracy. This depends on the local oscillator stability. This is very important for narrow band measurements.
- Input power range - the range of input power fed to spectrum analyzer input connector. this normally ranges from -100 dBm to +10 dBm. Signals beyond the lower limit the spectrum analyzer may not identify the signal from background noise.
- Harmonics - the measure of accuracy. This is normally greater than 30dB below desired signal. Since the harmonics adds to the measurement uncertainty, it should be kept to a minimum.

Spectrum analyzers also comes in a USB form. An example is the Fluke Network AirMagnet Spectrum XT.

Fluke Network Airmagnet Spectrum XT - Comes in an universal USB form for WLAN troubleshooting that combines RF spectrum analysis and WLAN traffic analysis. It can automatically detect interference sources based on signatures stored in a database, and it is also possible to create custom signatures. Some of the build-in types of graphs available includes real-time RF Spectrum and Wi-Fi, which can be recorded and replayed. Recorded data can also be sored in a .csv file [38]

2.2.5 Software receiving Wi-Fi

Most computers equipped with a wireless network card can, with software, be used to monitor the wireless signals from nearby wireless network access points (AP). Due to limitation in the most network network cards the frequency of the monitored wireless signals are restricted to the IEEE 802.11 frequencies. Some network card are better suited to for network monitoring than others, also proper drivers and directional antennas with high gain can enhance the performance of the audit. Some of the software available are WirelessMon, NetStumbler, Kismet and InSSIDer and some of them also have options for packet sniffing and intrusion detection if properly configured. As monitoring or auditing networks or system owned by others are illegal in some countries, it is advised to review relevant legislation and legal ramification before starting any monitoring activity on network without authority.

WirelessMon is a software tool created to monitor the status of wireless WiFi adapters and gathers information from nearby wireless AP hot spots in real time log. WirelessMon is created by PassMark Software and is available for Windows XP, 2003, 2008, Vista and Windows 7 32bit and 64bit and all various IEEE 802.11

is supported. Some of the features of WirelessMon is that it can verify 802.11 network configuration, test if WiFi hardware or device drivers functioning correctly, check signal strength levels of local WiFi networks and locate nearby interference sources. The current connection information including SSID, MAC address, signal strength, Tx Power, Authentication type, channel in use and frequency in use are some of the WLAN information displayed by WirelessMon (depends on network adapter). With this information it is possible to verify security settings, measure network speed and throughput or check WiFi network coverage and range. The information can be logged and saved to file, or be draw in comprehensive graphs with signal level, real time IP or 802.11 statistics. The information about gathered about the nearby AP can be used to create signal strength maps of the area. WirelessMon also has GPS support for this kind of logging and mapping of signal strength. WirelessMon cost $24 for standard edition and $49 for professional edition, but offer a 30 day free evaluation. The function for generating coverage maps based on signal strength of AP is only available for the professional edition. [39]

NetStumbler is a Windows wireless network tool, to map networks. NetStumbler is developed by Marius Milner, is a beggarware (free download, but the developer asks for donations) and works on all Windows version, but not well with Windows Vista. The mapping is done by active search as NetStumbler not only listen to traffic, but sends network packages that other networks will answer to. This way also networks with hidden SSID will be found. The GUI in NetStumbler will show information about which networks that are encrypted (WEP, WPA) which channels they use and the strength of their signal among other things. The primary function of NetStumbler is detecting AP using the WLAN IEEE 802.11a/b/g standard, but NetStumbler is also able to detect detect rogue AP, AP overlapping in range and do interfering networks noise readings. With a GPS receiver attached to the Computer with NetSumbler, it is possible to track the location of AP. NetStumbler can be extended and supports active scripting under Windows, including VBScript, JScript, and ActiveState's PerlScript and Python. [40, 41]

2.2.6 Antennas

An antenna is defined as electrical conductor or a system of conductors for radiating or collecting an EM signal. When an antenna is transmitting it will convert RF electrical energy into EM energy and radiate into the environment. When receiving a signal, the antenna will convert the received EM signal into electrical energy and fed into the receiver. Antennas however are often used for both the transmission and reception of signals. When transmitting, antennas will send in all directions, but typically not equally well in all direction. However, an idealized antenna, known as an isotopic antenna, will produce the simplest radiation pattern with equal radiation power in all directions.

As an antenna is a passive device, it cannot create actual gain or loss. It is possible however, to produce gain by propagate more energy in a limited scope of directionality. The antenna gain specification depends on the type, vendor and materials [4, 15, 42].

2.3 Shielding solutions

This section includes information about the articles testing or product concerning wireless shielding. Some of the studies found also regarded testing of the shielding ability of a type of material. These studies include ”Electromagnetic interference shielding effectiveness of carbon materials” by D.D.L. Chung [43] and ”Fluorination effects of carbon black additives for electrical properties and EMI shielding efficiency by improved dispersion and adhesion” by Ji Sun Im and group [44].

2.3.1 Mu Faraday cage

A Faraday cage is a special enclosure of metal that effectively screen the interior from radio waves.

Mu-Copper foil Wall Covering System - foil made of copper that can be applied to walls, ceilings and floors with a special adhesive. The standard width is 1000 mm, delivered as rolls of 100 meters or as prefabricated sheets. The parts can be linked together either using a 50mm overlap of the sheets, or a seaming or copper tape with a conductive self-adhesive. However the best performance is gained from soldering the sheets together. The copper foil has a very hight attenuation with respect to electrical fields and magnetic fields, with an attenuation of up to 120 dB, even at low frequencies according to the documentation [45].

2.3.2 Shielding paint

Extensive studies have been made by M.R. Meshram and group on design, development and characterization of ferrite powder, mixed with in epoxy resin to form a microwave-absorbing paint. The experiments ranges from observing the difference in absorption of different ferrites, to comparing the absorption of coating thickness and amounts of layers. The frequency for testing are between 8 and 12 dB, and therefore done with though of military applications, like radio communication, camouflage and prevention of EMI [46, 47].

Some of the microwave-absorbing paint products available on the commercial marked, include Y-SHIELD and CUPro-cote Paint:

Y-Shield - a water based high frequency shielding paint for walls, ceilings, doors and other interior, that can be applied on the interior as well as the exterior. It is effective for cell phone, CB, TV, AM, FM signals, radio frequency radiation, microwaves, typically 40 dB attenuation per layer and with ~10 Ohm resistivity per square according to the documentation. Tested up to 18 GHz. Will have consistent attenuation regardless of the direction of the signals polarization due

to holohedral carbon structure, without fibers and meshes. As a bonus about 10% of the Y-Shield effictiveness is due to absorbsion, which helps reduce reflection and minimize the risk from RF sources being trapped inside the shielded area. Require grounding like any other RF shielding material. The paint has a black color, but can be covered with latex paint, wallpaper, etc. for estetics. Manufactored by YSHIELD EMR-Protection [48, 49].

CuPro-cote Paint - a copper particle water based paint. it is sprayable, brushable, rollable and made out of a conductible coating of specially formulated copper as conductive agent. The paint was developed initially for RF/EMI shield for plastic electronic equipment, and can therefore be directly applied onto acrylic. It has more than 75 dB attenuation from 30 MHz to 1.5 GHz. and a resistivity of <1 Ohm/sq. As the paint is not a absorbent in itself, the paint needs to be combined with a microwave absorber sheet to extract RF reflections inside the shielded area [49].

2.3.3 Shielding windows

An article by Jonichi Hirai and Isaya Yokota with the title ”Electromagnetic Shielding Glass of Frequency Selective Surfaces”, describe testing of a developed frequency selective surface (FSS) window [50]. The study was conducted as a result of the need to prevent leakage of radio waves in and out of rooms caused by PHS (Personal Handyphone) devices. The FSS Glass used for the window, consists of cluster of thin antennas printed in it. As the antennas needed to be both of a highly conductive material and thin enough not give an optical disadvantage to the window glass, a 0.5mm diameter silver antenna was chosen. The FSS Glass material has an attenuation peak of 35 dB at 1.9 GHz, and has a 35 MHz band around 1.9 GHZ where it attenuates more than 30 dB. The shielding glass is intended and tested at the PHS band, but it is claimed in the article that it can be applied to other bands, or several band at a time, as well. It is also mentioned that other materials can be used for shielding as well, as long as the silver element can be printed on it.

In additions to the shielding glass described in this article, several products shielding films for application to a smooth surface is available for purchase.

EMI/RFI transparent shielding foil (Meshfoil) - a shielding foil to apply on standard displays, glass, acrylic, polycarbonate, plexus glass. The material consist of a very fine mesh laminated between two layers of transparent. The foil is so fine as it appear transparent, but both strong and bendable. The forms of mesh available are: stainless steel, blackened copper and phosphor bronze. The foil can be delivered with a self-adhesive layer, for easier application. The frequency covered by the foil is between 10kHZ and 30GHz, where finer mesh is more effective against higher frequencies. The attenuation for 10 - 1000kHz will be between 20 and 61 dB, for 1 to 100 MHz it will be between 68 and 120 dB, for 1 to 10GHz it will be between 33 and 87 dB depending on the type of wire and the wire material according to the documentation [51]. Manufactured by Holland Shielding Systems.

HF Window Films - consists of precious-metal coated with a self-adhesive film for shielding windows and application on glass-surfaces. The film comes in several variations with different attenuation, light transmission abilities, and film width, and is exclusively for indoor application and for non heat-absorbing glass. The price varies with the abilities, where the cheapest possesses a 22 dB attenuation and a 62% light transmission and the most expecive possesses a 32 dB attenuation and a 72% light transmission. Manufactured by YSHIELD EMR-Protection [48].

2.3.4 Frequency Selective Surface (FFS)

A Ph.D. thesis done by Hui-Hsia Sung in Electrical an Electronic Engineering done at the University of Auckland [52], describes the development and testing of an technique of interference control with the use of FFS in indoor wireless environments. This testing was done to find a solution to external interference. The FSS created was in the form of a prototype wallpaper with frequency filtering patterns. The pattern in the wallpaper consisted of square loop elements, and testing were done with different dimensions of this pattern. The material used for the wallpaper included polyester tape, polyester film, aluminum foil tape. The testing included several setups, like the wallpaper suspended in air, surrounded by microwave absorbers, on plasterboard and on plasterboard with spacing. The frequency range tested was from 2 to 8 GHz, 30 different distances tests with maximum distance at 3 meters and various test of angles, from 0° to 56°. The results from the testing showed that the prototype wallpaper could attenuate 5.3 - 5.8 GHz transmissions by 15 dB, while other frequencies experienced only little attenuation. The attenuation was also consistent in all the angles. The 15 dB reduction was found to be sufficient to isolate a wireless system from external interference. The testing also showed that the wallpaper could be applied directly to the wall. An article is also publishes by Hui-Hsia Sung and group testing the wallpaper with a frequency selective (FS) wall [53]. With this setup a 30 dB attenuation was reached.

The article ”An Experimental Study of a $\lambda/4$ Wave Absorber Using a Frequency-Selective Surface” by Akihiko Ito and group studies the performance of a FSS applied to a $\lambda/4$ wave absorber [54]. The test was performed to fin a way to better improve the electromagnetic environment for the use of personal digital cellular (PDC), personal handy-phone system (PHS) and wireless LAN. The wave absorber consisted of an indume-tin-oxide (ITO) film on a absorption PET film with the absorber set to 19 GHz, while the FSS consisted of a foam polystyrene and aluminum patterns. As a result the shielding characteristics were obtained at about 30 dB at 9.7 GHz for the FSS, and 40 dB also at 9.7 GHz with the absorber using the FFS.

2.3.5 Vegetation

A study made by Iñigo Cuiñas and group called ”Using Vegetation Barriers to Improving Wireless Network Isolation and Security”, includes testing shielding abilities of vegetation [2]. The article is based the problem of the increasing number of WLAN using the same spectrum and security issues in WLAN. The proposal is to use bushes and trees as a barrier to attenuate signals from other networks, and protect from other

interference. Interior plans are considered to cut the line of sight of adjacent networks, or exterior trees to reduce outdoor coverage and limit external users. Both common outdoor and indoor vegetation species were analyzed in the study. The measurements was performed at the 2.4 and 5.8 GHZ frequency band, with a result of attenuation up to 10.7 and 21.2 dB respectively. The minimum security distance results using QPSK, 16-QAM and 64-QAM modulation represents a 73% reduction in distance at which two network could be operated.

2.3.6 Various shielding complimentations

In addition to the shielding solutions mention above, shielding can also come in the form of shielding fleeces, nettings, tiles and fabric. Several solutions like conductive foil or tapes, shielding for doors and ventilation shafts also exist to compliment the surrounding shielding solution [55].

Chapter 3

Experimental setup

To solve the problem statement for this thesis, a setup including a test box, a transmitter and a receiver will be used. the transmitter will be placed inside the test box with the solution applied to the inside. The transmitter will then send out a signal, and a receiver, placed on the outside of the test box, will be monitoring any signals traversing from the inside of the test box from the outside. A simple overview of the model is shown in figure 3.1. As the experiments needed to be in a environment relatively free from interfering signals, the experiments were performed in the basement floor of the p35 building of HiO.

The test box was originally meant to be made in a 1 x 1 x 1 meter scale, but due to consideration of cost, building time and the practical handling the scale was changed to 0.5 x 0.5 x 0.5 meter. The building materials of the test box consisted of steel profiles, creating a skeleton for the box, and plasterboard, creating walls on the inside of the box where the shielding solutions was applied. An exception from this is the test box for intended testing the wired mesh, which must be applied to an smooth surface. One of the walls of this test box was made of either of a acrylic plastic material to accomplish this requirement. These materials was chosen because they are easy to work with, relatively lightweight and appears in most home and office environments. A weakness in the approach is that there will be no shielding applied to the floor of the box. An approach regarding shielding tiles or a plaster board with one of the shielding solution applied were considered, but these approaches would either be costly, impractical or hard to successfully integrate in the shielding in the test box. Additionally the floor of the testing area was made out of concrete, which contain some shielding abilities, and resides at the bottom level of the building, making it unlikely for any signal to enter from below when the test box resting on the floor. An opening in the shield in the floor would also reflect the situation from the real world, since there seems to be few practical solutions for shielding floors available, and the existing products would be comprehensive to apply to an existing office area.

The technical drawing of the construction of the test box with dimensions is shown in figure 3.2, where figure 3.2(a) shows the bottom part of the box, figure 3.2(b) the top and figure 3.2(c) the side. Pictures of the finished test box is shown at figure 3.3, where figure 3.3(a) shows the test box with the right side up and figure 3.3(b) shows

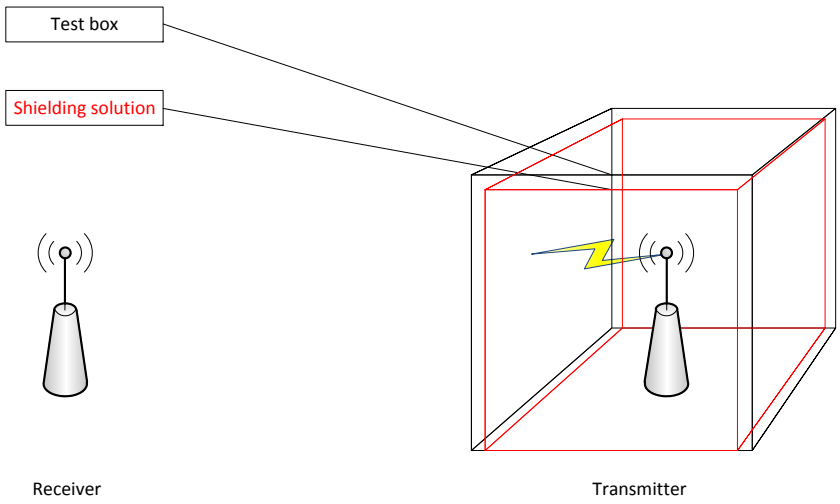


Figure 3.1: Simple overview of efficiency testing

the test box toppled over to the side to show the inside.

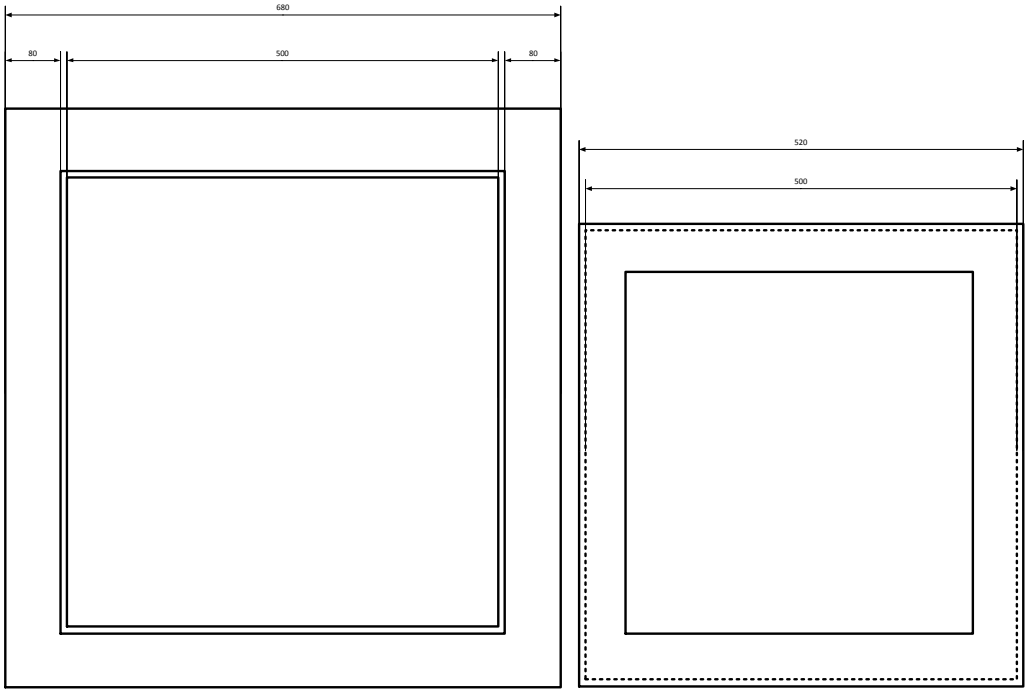
The following list shows the products tested and compared in this theses. Originally a stealth wallpaper was included in this list, but as there were no response to any inquiries to the producers of the product, it was later excluded.

- Mu-copper Faraday cage
- Y-Shield paint
- Mesh foil
- Self-applied aluminum foil

These products are chosen for their ability for realistic application for an office environment. The aluminum foil is included to see the efficiency of the most affordable and available solution. How the solutions are applied depended in the type of solutions and will be explained for each of them, but common to all of them is that they all needed to be grounded to be able to shield properly. How the grounding is applied also depended on the shielding solution, but the grounding wire used was a green/yellow PN 2x1.5mm^2 with a alligator clip on the end to connect to any grounded system in the vicinity.

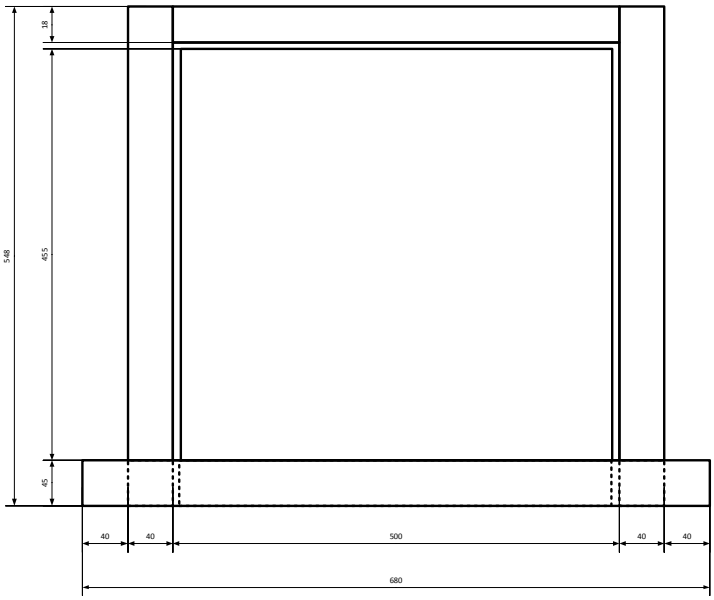
Mu-copper Faraday cage - Chosen to compare the original and more classic type of Faraday cage with the more modern versions.

A glue gun was used to attach the copper sheets to the test box. 50mm overlap were used one the sheets with Y-SHIELD paint used as connector (silver paint was offered by the manufacturer, but the price for it was quite steep) to block any



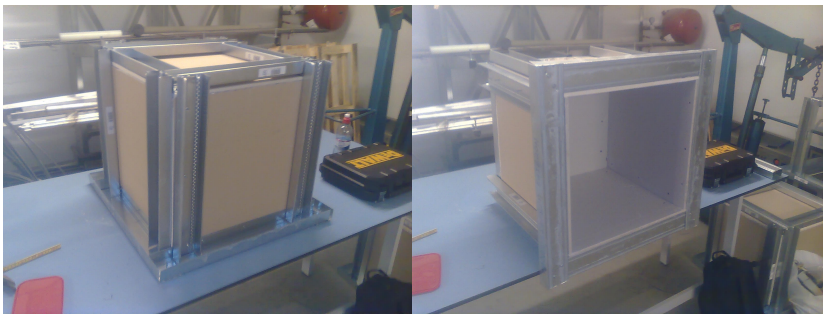
(a) The test box from below

(b) The test box from above



(c) The test box from the side

Figure 3.2: Technical drawing of the test box construction



(a) Test box (b) Test box on the side

Figure 3.3: Pictures of a finished test box

possible signal leakage. For higher performance soldering the sheets together is recommended, but this was opted out because of the fire hazard. The grounding, however, was soldered to the copper sheet, as it was possible to do this in a safe way. Y-SHIELD paint (in stead of the silver paint) was used to cover any possible weak spots in the shielding. As the Mu-copper foil came with no instructions of how to apply and ground it, the procedure of application and grounding was found through e-mail correspondence with the manufacturers. A picture of the test box with the MU-copper foil applied can be found in figure 3.4(a).

Y-Shield paint - The Y-Shield paint was chosen over the CuPro-cote paint because of its ability to block frequencies of higher levels. Another contributory factor was the Y-Shield paint's ability to absorb signal rather than reflect them.

To properly ground the shield, a Y-Shield ground kit was purchased along with the paint. The kit included a roll of conducting tape to connect the shielding on the different walls and on the ceiling, and a grounding plate for connecting the shield to ground. The conducting tape was applied, before painting the test box, to all walls and the ceiling in the test box, creating a cross where the tape for the wall intersected the tape for the ceiling at the space where the grounding plate would later be mounted. Holes, with plugs, for the grounding plate was also drilled before applying the paint. One layer of paint was applied to the whole inside of the test box with an roller. A second layer was applied to the area where the grounding plate would be mounted, along with any areas where gaps could be expected. These procedure of applying and grounding the paint was done according to the instructions that followed the paint and grounding kit. A picture that shows the test box with the paint and the ground plate applied can be found in figure 3.4(b).

Mesh foil - Selected to cover materials for shielding windows. This was delivered as a laminated wire with adhesive on one side, for a probably easy application.

A decision to only apply the mesh foil of the test box, since the material proved to be quite expensive per square inch. For the side were the mesh foil would be

applied, a pane of acrylic was attached, while the rest of the box was covered in Y-SHIELD paint (since this was the cheapest solution). The mesh foil was then applied to the acrylic pane on the test box like a sticker, by the adhesive applied to the mesh foil. To connect the mesh foil shield to the shielding in the rest of the box, some of the wiring on one side of the foil was delivered uncovered. The uncovered wire part was placed to cover a painted area by the window, and made to stick by applying more Y-SHIELD paint. As the Mu-copper foil came with no instructions of how to apply and ground it, the procedure of application and grounding was found through e-mail correspondence with the manufacturers. A picture of the mesh foil applied to the test box can be found in figure 3.4(c).

Self-applied aluminum foil - This material was included to see the effectiveness of a cheap and highly available material. There have been a study of the radio signal shielding effectiveness of aluminum hats, performed at MIT, where the result shows that this material have little attenuation ability [56]. However, this study concerned a tests where the material was not grounded, also the frequency specter ranged from 10 kHz to 3 GHz.

The aluminum foil chosen was a type for use with microwave ovens, commonly available in most grocery stores, which was both more likely to have an effect on EMI signal and also more robust than the more basic types. The sheets was folded for a dual layer of material to increase the thickness of the shield, and conductive grease was used to increase the connectivity between the layers. To connect the different walls and the ceiling, each sheet had an extended length of 50mm on each side. The extended length of immediate sheets was folded together several times for better connection and a larger connection surface. For easy application (and removal if necessary) the material was attached to the test box using TaicIt, and the shield was grounded using a termination part. A picture showing the aluminum foil applied to the test box is found in figure 3.4(d).

To further answer the bullet point in the problem statement the rest of this chapter is divided into the following parts:

Shielding efficiency - The testing of the shielding efficiency, what tools that will be used to send, receive and monitor the signals and an overview of how the testing and measurements will be organized.

Cost and Implementation - The cost for applying of each solutions to the test box, and an estimate the cost of each solution scaled for imagined, but realistic environment. The time and effort used to apply the solutions to the test box, an estimate of the time scaled to an imagined, but realistic environment, and comments on the experience in applying the solutions.

(a) MU-copper foil (b) Y-Shield paint

(c) Mesh foil (d) Self-applied aluminum foil

Figure 3.4: Pictures of the solutions applied to the test box

Test name	Description
REF	Reference measurements without test box
REF-BOX	Reference measurements with test box
REF-WIN	Reference measurements with windowed test box
REF-W+P	Reference measurements with windowed test box and Y-SHIELD paint
MU-CU	Mu-copper Faraday cage
PAINT	Y-Shield paint
MESH	Mesh foil for windows
AL	Aluminum foil

Table 3.1: Test overview

3.1 Efficiency

To find the efficiency of the different shielding solutions, testing was done on each solution along with reference test with and without the test box, and with the test box with a window. Also a reference test with the windowed test box with the other walls covered in Y-SHIELD paint was included, as paint was used to cover the non-windowed walls in the mesh foil test. A list of the names and type of the different test is found in table 3.1.

The equipment for transmitting and receiving/monitoring signals for this thesis is a Linksys WRT54GL wireless router type G and a Airmagnet Spectrum XT B4070 USB-based spectrum analyzer. The choice of equipment is entirely based on the cost and availability, as this was the major contributor in limiting the selection of equipment. The draw-back with this solution is that the frequency spectrum is limited to the WLAN frequencies, and there are little flexibility in the antenna arrangement. Because of the manual way the test had to be executed the frequency range was limited to the 2.4 GHz specter, which is the most used specter for WLAN today.
ting the selection of equipment. The draw-back with this solution is that the frequency spectrum is limited to the WLAN frequencies, and there are little flexibility in the antenna arrangement. Because of the manual way the test had to be executed the frequency range was limited to the 2.4 GHz specter, which is the most used specter for WLAN today.

The Airmagnet spectrum analyzer came with a spectrum USB adapter with an attachable antenna, which both needed to be connected to an USB-port on a computer (preferably a laptop) and mounted on a appropriate location (on the rear of the screen when mounting to a laptop). Also included was a software with a user interface, and possibility of recording to either a amt-file (internal file type for signal replay) or a .csv-file. The use interface includes several presentation of the measured signal. However, the default presentation includes real time FFT (showing the maximum hold, maximum and average) and spectrum density of the frequency spectrum, AP channel strength, and a summary of the current, average and maximum signal strength for each channel.

The data file from the spectrum analyzer, consisted of one line per second of testing (or per 1 - 2 second, because of the way Windows handles time). Each of these

lines consisted of 590 point of measured signal strengths from the 2.4 GHz band, and 590 point the 5 GHz band, along with an epoch time, start and end frequency. Each of these 590 point represented a 590th of the end frequency subtracted from the start frequency, which equals to approximately 156 kHz per point for the 2.4 GHz band. Through some testing it was found that 2 minutes testing per test one channel and frequency would collect 87 samples, which give a fairly accurate result considering the stable values from the test data. This also limited the time used on each test to an endurable amount.

To observe if the solutions efficiently shield a range of frequencies, a selection of frequencies will be included in the testing. To investigate the possibility of penetrating a shield by simply increasing the signal strength, a selection of signal strength will be included. The range and selection of frequencies and signal power used for the test greatly depended on the equipment used in the testing for sending and receiving. Although the ideal range of frequency would be from 560 MHz to 6 GHz to also include the mobile telephone frequencies and the higher frequencies of the new IEEE 802.11n standard, but due to the manual way the test had to be executed, the frequency range was limited to the 2.4 GHz specter, which is the most used specter for WLAN today. The selection of frequencies also depends on if the tests are possible to automate, as i.e. doing tests per 100 or 500 MHz may take extensive amount of time done manually. Using a router for sending also limits the frequencies to the channels available in the frequency band. Since using a complete range of signal strength for testing would be excessive and unnecessary for this project a selection of a low, a middle and a high signal strength will be sufficient. The actual values setting for the router was a range between 1 and 255 mW, but as it is recommended not to exceed 100mw because of possibilities of overheating the router, the signal strengths for testing was set to 1, 50 and 100 mW.

To avoid interfering signals from surrounding electromagnetic sources, the testing was done in the basement of HiO. However this location was not entirely without interference, as a microwave oven resided on the floor above. This interference spanned over all the testing frequencies and had maximum signal strength of between -70 and -80 dB, enough to affect the result of the testing. For this reason, all testing ceased when the microwave interference were detected. A sample from microwave oven interference can be found in figure 3.5.

To observe and experiment with how EMI signals behave both in general and to the shielding solutions, the testing included several distances and angles in the positioning of the receiver versus position of the transmitter. This way any weaknesses in the shielding solution due to distance or angle will be found and documented. Some of the solutions were also tested with and without connection to ground, to document the possibilities of turning the shielding on and off by connecting and disconnecting the grounding. To simplify the measurements and analysis if the data the receiver should be placed in the far-field of the transmitting antenna. To find the far-field in equation (2.2). The frequency 2.4 GHz will be used as the frequency in the calculation, as the frequency with the largest wavelength (λ). Additionally the greatest dimension of the

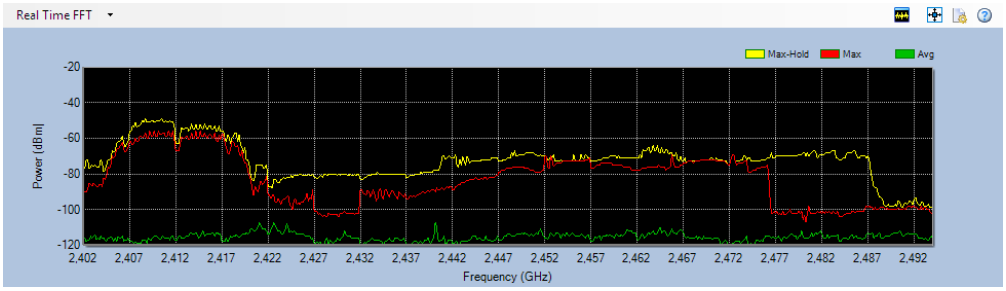


Figure 3.5: Captured microwave interference during testing (at 2.412 GHz)

antenna (a) was measured to be 3.5 cm.

$$\begin{aligned} R &= \frac{2a^2}{\lambda} \\ &= \frac{(2x0.035)^2}{3x10^8/2.4x10^9} \\ &= 0,0392 \end{aligned}$$

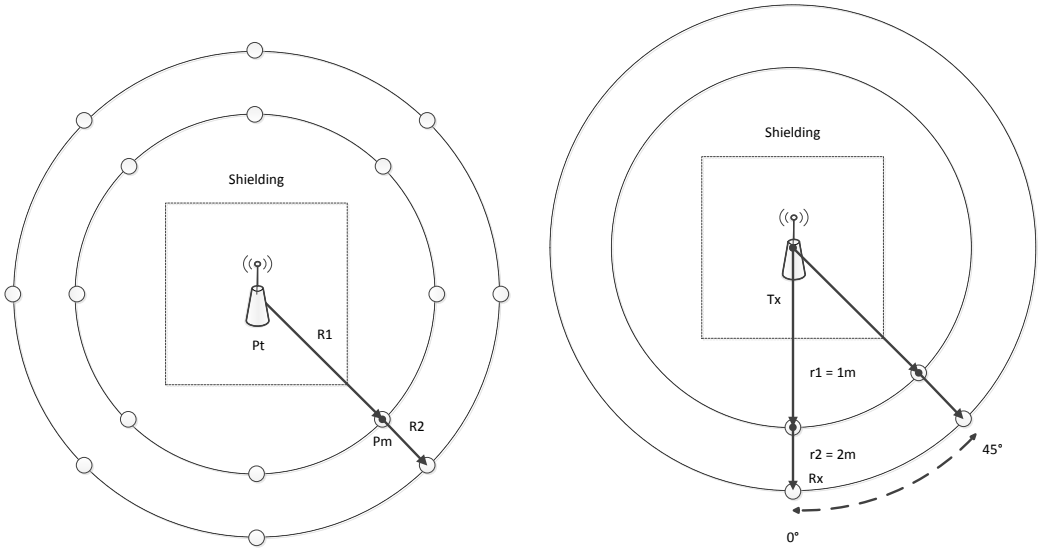
According to this calculation the far field starts 3,92 cm from the transmitter. The arrangement of positioning the receiver is therefore 1 m and 2 m from the sender, as this will place it in the far field of the transmitter and additionally be easy numbers to use in further calculations. To find an estimate was done on the the expected difference between the two distances. The free space equation (2.4) was used as only the difference in attenuation for the two distances is interesting. This also simplifies the calculation a bit.

$$\begin{aligned} L_{1m} &= 10log_{10}(\frac{4\pi d}{\lambda})^2 dB \\ &= log_{10}(\frac{4\pi 1}{3x10^8/2.4x10^9})^2 dB \\ &\approx 58.10dB \end{aligned}$$

$$\begin{aligned} L_{2m} &= 10log_{10}(\frac{4\pi d}{\lambda})^2 dB \\ &= log_{10}(\frac{4\pi 2}{3x10^8/2.4x10^9})^2 dB \\ &\approx 64.12dB \end{aligned}$$

According to this calculation there should be approximately a 6 dB difference in received signal between the two distances.

The first draft of the testing arrangement included several angles at several sides of the test box (figure 3.6(a)). This initial approach was later revised as it would demand a relatively large area for testing, along with extending the testing time radically with each angle. Also any difference in the measurements from one side to another would only show the quality of the handiwork put into applying the solution rather than the



(a) First draft of testing arrangement

(b) Second draft of testing arrangement

Figure 3.6: Testing arrangement overview

quality of the solution. To find out more about the value of distances and angles would have on the result, some pre-tests were done with several distances and angles on the shielding solutions. Through these pre-tests it was found that change in angles had little effect on the attenuation, also it was found that tests on different distances on each angle would be redundant for the initial 0° test. This resulted in a second draft, where the testing would be performed at on one side of the test box at a 0° and 45° degree angle.

Additionally, a simple test were performed to investigate the minimum signal strength for data transfer and connection to the receiver, and compliment the description of receiver sensitivity in the IEEE 802.11 standard [17]. The experimental setup included connecting a laptop to an AP, run a data stream and monitor with WirelessMon. The distance between the laptop and the connected AP was then increased until the connection was lost. The minimum signal strength for connection would be equal to the last entry found in the data file generated by WirelessMon.

Much of the testing approach was borrowed from a PhD. thesis based on tests on the stealth wallpaper [52], but simplified as this thesis was based on very extensive testing. and an overview of the test scenarios used in this project can be found in table 3.2.

Set	Frequency (GHz)	Tx signal power (mW)	Distance (m)	Azimuth angle (θ°)
1	2.4	1	1	0
2	2.4	50	1	0
3	2.4	100	1	0
4	2.4	1	2	0
5	2.4	50	2	0
6	2.4	100	2	0
7	2.4	1	1	45
8	2.4	50	1	45
9	2.4	100	1	45

Table 3.2: 9 scenarios (i.e. sets of measurements) for each solution

3.2 Cost and Implementation

The cost results was based on the prices for purchasing the shielding material, how much of the material used in applying it on the test box.

The implementation results is based on the time, effort and experiences in applying the shielding solution to the test box. Additionally all experiences regarding applying the shielding solution are added as comments for each product.

Chapter 4

Results

The results of the testing described in this chapter include a comparison of the efficiency in attenuation of the shielding solutions, a comparison of the total cost of acquiring them and the time and effort put into applying them. The chapter concludes with a summary of the comparison of the shielding solutions.

4.1 Efficiency

The results from the efficiency testing includes the results from the signal measurements from each shielding solution, along with the measurements from the reference tests. The section starts by looking at the results from the reference tests, giving an analysis of these results. Then results from the test of the different shielding solutions are studied, and later analyzed and compared regarding to their attenuation efficiency.

The results are both presented in form of tables and in graphs. The tables include the median of the dB data for each test. The median was taken of both the specter of each channel, and of the 87 sets of data per second. The graphs made from each set of tests first show the reliability of the data with median, 10% and 90% percentiles, then compares the result from different signal strength, distance and angle. The measured dB unit uses logarithmic scale of log_{10} of the corresponding mW value. Therefore graphs where the values is converted to mW was added to give more insight into the actual impact of growth or fall in values. A comparison of the different results and of the attenuation of the different shielding solutions is also shown in a graph. Tables of the mW data were not includes as these were difficult to interpret in the form of tables. As the purpose ot the tesing was aimed at finding the maximum attenuation in the shielding solutions, the strongest signal (1m, 100mW) was selected when there was a choice in data sets.

The 2 meter distance tests were at some point found to be somewhat redundant for the 1 meter test, and measurements at this distance was excluded from the succeeding tests. Test on the other hand was added, testing shielding solutions where this seemed useful.

An issue noticeable in all the results, was fluctuations and instability in the signal

transmitted from the wireless router. These fluctuation is most likely caused by low harmonics in the transmitter and/or difference in the reflection in the testing environment (due to movement etc.). The signals however, are more stable at some instances than in other, so the stable data sets are used as often as possible. These more stable data sets are found through looking at the data accuracy graphs, the mW converted data and by using measurements in other signal strength, distances and angles as reference points.

4.1.1 REF

The REF abbreviation refers to the reference testing without any shielding nor a test box. According to the graphs showing the data accuracy of the results in dB (figure 4.1(a)) and in mW (figure 4.1(b)), the signal from this test seem quite stable. This is indicated by the steady gap between the percentiles that stays at approximately 8 dB or ~0.01 - 0.012 mW with the median located more or less in the middle for most the frequencies. The median of the signal is found to range from -51 to -55 dB, with perhaps the most stable signal at 2.442 and 2.457 GHz, due to a more centered median.

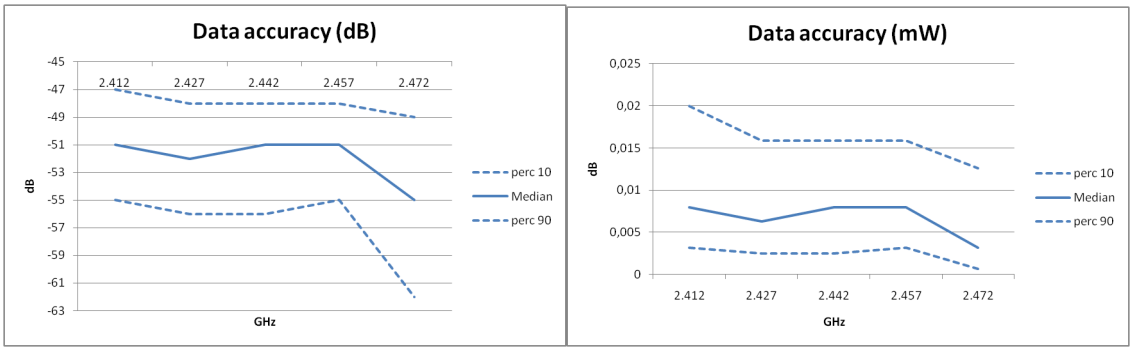
The results of the difference in the transmitted signal strengths, are found in table 4.1, figure 4.2(a) in dB and figure 4.2(b) in mW. Only considering one of the more stable frequencies, 2.442 GHz, the signal received is shown to increase from -61 to -55 dB (or ~0.001 - 0.003 mW) from 1mW to 50mW transmitted signal and -55 to -51 dB (or ~0.003 - 0.008 mW) from 50mW to 100mW. The results in mW shows that the receives signal when the 50 mW transmitted signal is more than three times the signal strength of the 1 mW transmitted signal. Equally the received signal at 100 mW is more than 2.5 times in signal strength than form the 50 mW signal. These result in measured in the received signal strength is clearly irregular to the increase in the transmitted signal, however the signal may also have been affected by reflections in the environment combined with instability in the harmonics in the transmitter.
Table 4.1 and the graph comparing distances (figure 4.2(c)) in dB, shows a 2 - 5 dB (~0.004 - 0.008 mW, figure 4.2(d)), higher received signal from the 2 meter distance than 1 meter distance. These differences in signal strength was rather low considering the 6 dB estimated difference, but might be more evidence of fluctuations.

The result found in table 4.1 and the graph comparing the result from different angles (figure 4.2(e)), shows that the signal from the two angles have a more or less equal signal strength at all frequencies, except at 2.472 GHz where the measurement from the 45° angle is rather hight, -45 dB (>0.03 mW), compared to the other frequencies, -55 to -49 dB (<0.015 mW). This result however, can be disregarded as a difference in fluctuation when doing the two measurements, since there are no other logical reason for this difference in signal strength at this frequency.

The results from both table 4.1 and from the graphs in 4.2 shows a fall, -51 to -55 dB(0.008 to 0.003 mW) for 1m 100mW, in the received signal on 2.472 GHz for all the test except the test for the 45°, where there is a greater received signal at 2.472 GHz, -45 dB (>0.03 mW) at 1m 100mW. However, the data accuracy results indicates that the measurements on this frequency was a bit more unstable than the other frequencies.

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-61	-62	-61	-63	-64
	50mW	-55	-55	-55	-55	-59
	100mW	-51	-52	-51	-51	-55
2m, 0º	1mW	-60	-61	-61	-61	-57
	50mW	-58	-56	-59	-52	-57
	100mW	-49	-50	-48	-48	-50
1m, 45º	1mW	-65	-61	-62	-61	-58
	50mW	-59	-58	-56,5	-53	-51
	100mW	-55	-51	-51	-49	-45

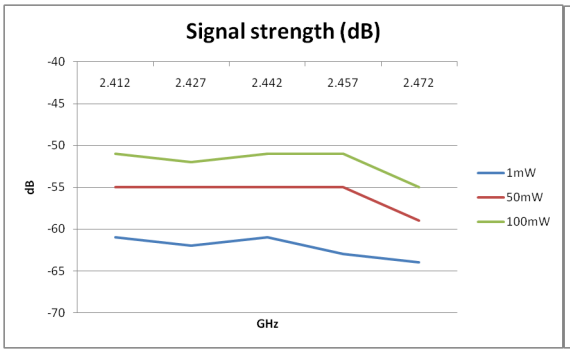
Table 4.1: Median of the REF results in dB



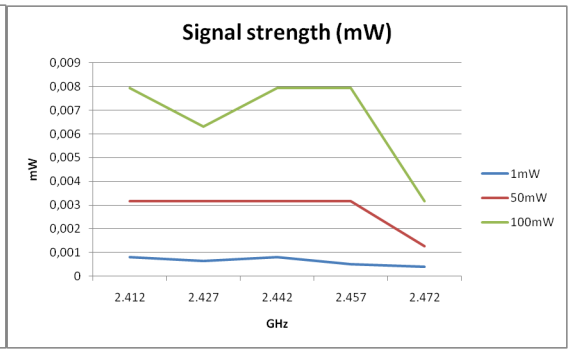
(a) Median, 10% and 90% persentiles in dB

(b) Median, 10% and 90% persentiles in mW

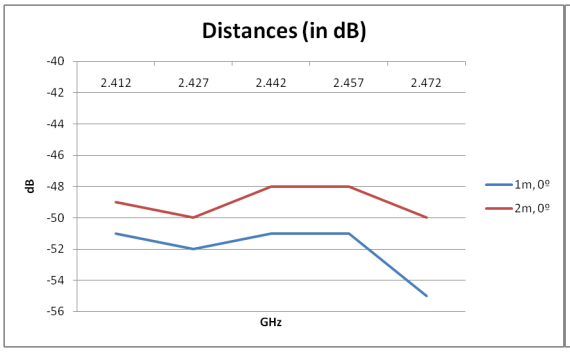
Figure 4.1: Accuracy of the REF result data (1m, 100mW)



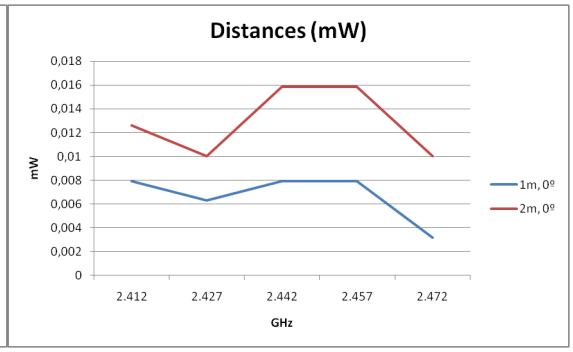
(a) Different signal strength measurements in dB



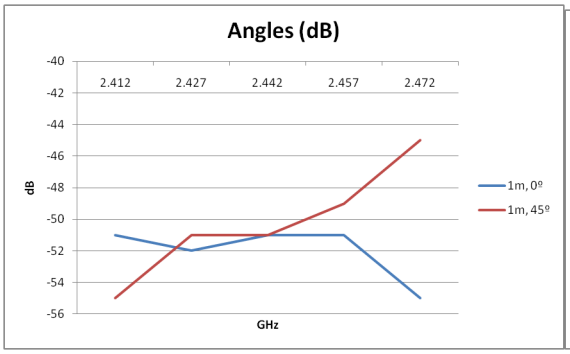
(b) Different signal strength measurements in mW



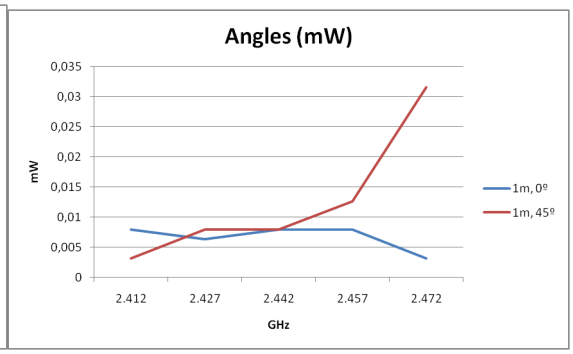
(c) Different distances measurements in dB



(d) Different distances measurements in mW



(e) Different angles measurements in dB



(f) Different angles measurements in mW

Figure 4.2: Graphs for testing results for REF

4.1.2 REF-BOX

The REF-BOX abbreviation refers to the reference testing of the test box, without any applied shielding materials. According to the graphs showing the data accuracy of the results in dB (figure 4.3(a)) and in mW (figure 4.3(b)), the gap between the percentiles ranges between 10 and 13 dB (or less than 0.01 mW) for all frequencies with the median more or centered. The exception is for 2.412 GHz, where this gap ranges as hight as 25 dB or over 0.14mW. This indicates quite a quite stable signal on all frequencies, except at 2.412 GHz. At this frequency, there were measured a number noticeably strong signals compared with the other frequencies, indication instability in the measurement. The measurements at 2.427 GHz has also the same tendencies, but not as prominent. The median of the signal ranges from -51 to -58, with some significantly stronger signals at 2.412 GHz and perhaps 2.427, affecting the result.

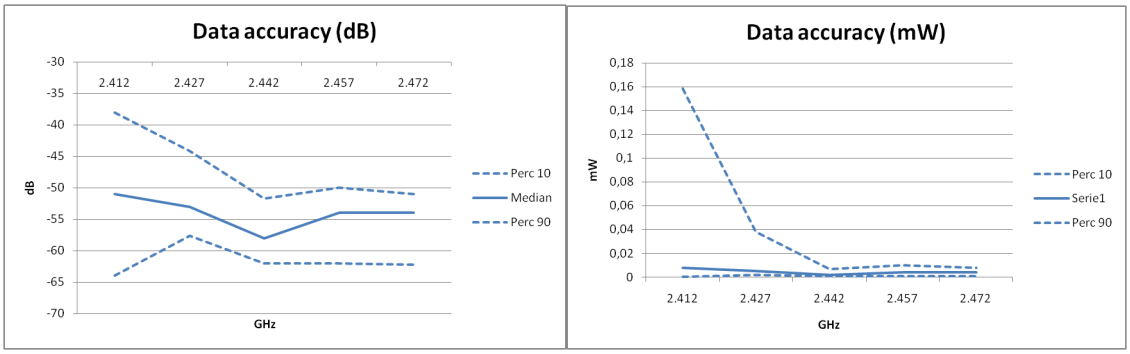
The results of the different signal strengths transmitted, are found table 4.2, figure 4.4(a) in dB and figure 4.4(b) in mW. Only considering the result from 2.457 GHz, one of the more stable frequencies, the signal received is shown to increase from -64 to -57 dB (or ~0.0005 to 0.002 mW) when the transmitted signal is increased from 1 to 50 mW, and -57 to 54 dB (or ~0.002 to 0.004 mW) from 50 to 100 mW. Here the received signal seems to be multiplied with 4 when increasing the transmitted signal from 1 to 50 mW , and double from 50 to 100 mW. These results, along with the previous test, indicate that the received signal do not follow the same pattern as the transmitted signal.

The results found table 4.2 and the graph comparing the results from a 1 and 2 meter distance (figure 4.4(c)) and in mW, figure 4.4(d)), shows at one point a 5dB greater received signal strength from the 2 meter result than the 1 meter result. This unexpected result is found at the 2.442 measurement, which is lowest from the 1 meter distance test, -58 dB, and the highest from the 2 meter distance test, -54 dB (0.0015 and 0.004 mW). The results at 2.472 GHz for the 2 meter test are also rather low, -64 dB ($<$0.001mW), comparing with the measurements from the other frequencies, -58 to -54 dB (0.0015 - 0.004 mW). Furthermore, the result at 2.412 GHz for the 1 meter test is rather hight, -51 (0.008 mW), compared to the measurements at the frequencies, -53 to -58 dB (0.005 - 0.0015 mW). As there are no logical reason for the received signal from a 2 meter distance to be larger than from 1 meter at 2.442 GHZ, nor the large differences at 2.412 and 2.472 GHz, these results is probably cause by the fluctuation in the transmitter or environmental reflections. This however, means that the only source for a reliable result from both distances is at 2.457 GHz, which makes the comparison of signal strength difficult. The distance result at 2.457 of 2 dB also low compared with the 6 dB estimated difference.

The results from the angles, shown in table 4.2 and the graph comparing angles (figure 4.4(e), shows that the results from the two test more or less follow each other, except a fall in signal strength at 2.442 for the 0° measurement, and at 2.457 GHz for the 45° measurement. These falls in signal strength is probably cause by the fluctuation in the transmitter or by reflections in the environment and can be disregarded.

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-58	-59	-68	-64	-65
	50mW	-54,5	-57	-61	-57	-59
	100mW	-51	-53	-58	-54	-54
2m, 0º	1mW	-68	-68,5	-66	-65	-74
	50mW	-62	-61	-60	-59	-67
	100mW	-58	-56	-54	-56	-64
1m, 45º	1mW	-63	-62	-64	-69	-66
	50mW	-55	-56	-56,5	-64	-57
	100mW	-52	-53	-54	-57	-54

Table 4.2: Median of the REF-BOX results in dB

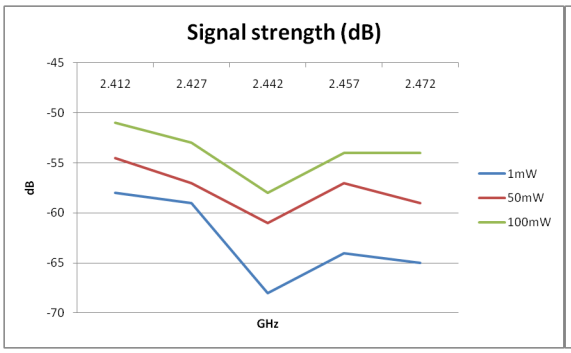


(a) Median, 10% and 90% persentiles in dB

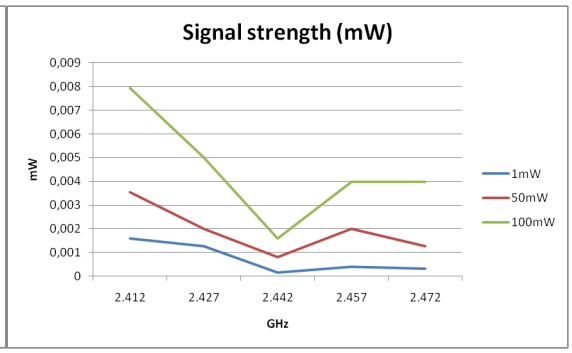
(b) Median, 10% and 90% persentiles in mW

Figure 4.3: Accuracy of the REF-BOX result data (1m, 100mW)

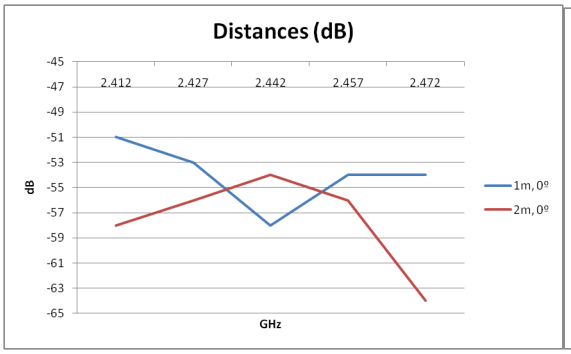
In this test it is revealed by the graphs in figure 4.2 and 4.4, that the measurements at 2.412 GHz was quite unstable and was found to be rather high compared with the measurement for the other frequencies. The results from the distance measurements was found to be difficult to compare, as the readings showed that for several frequencies, while the 1 meter measurements had low readings when the 2 meter measurements had high readings and visa versa.



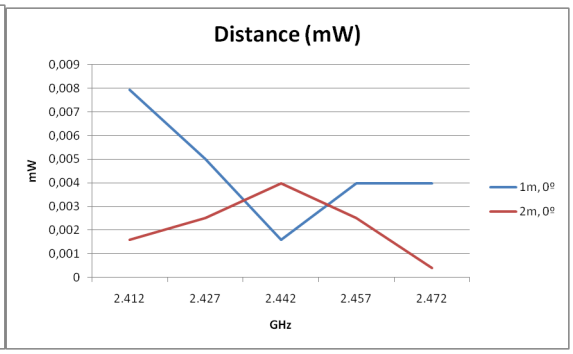
(a) Different signal strength measurements in dB



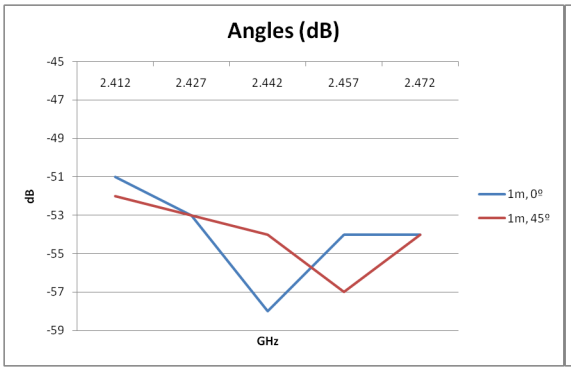
(b) Different signal strength measurements in mW



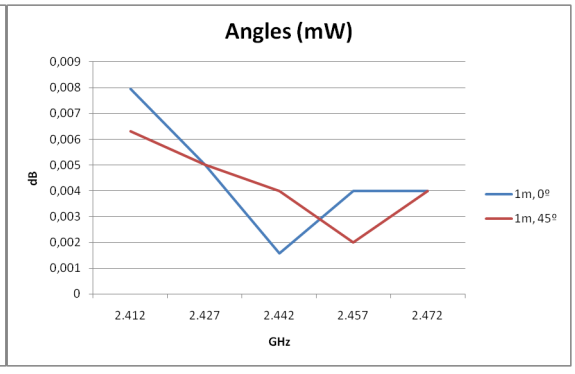
(c) Different distances measurements in dB



(d) Different distances measurements in mW



(e) Different angles measurements in dB



(f) Different angles measurements in mW

Figure 4.4: Graphs for testing results for REF-BOX

4.1.3 REF-WIN

The REF-WIN abbreviation refers to the reference testing of the test box with a acrylic window, without any shielding applied. According to the graph showing the data accuracy of the results in dB (figure 4.5(a)) and in mW (figure 4.5(b)), the gap in most of the values between the 10% and 90% percentile is between 10 and 13 dB (or ~0.002 - 0.004 mW), with an approximatly centered median. An excepton however is found at at 2.457 and 2.472 GHz, where the gap increases to 32 and 20 dB. The mW convertion however, shows that the unstable signal resides at 2.442 and 2.457 GHz rather than at 2.457 and 2.472 GHz. The median ranges from -48 to -59, with some significantly more unstable signals found at 2.442 and 2.457 GHz affecting the result.

The results of the different transmitted signal strengths, are found in table 4.3, figure 4.6(a) in dB and 4.6(b) in mW. Only considering the results from 2.472 GHz, one of the more stable frequencies, an increase is shown in the received signal from -54 to -45 dB (or ~0.0001 to 0.0005 mW) when the transmitted signal is changed from 1 to 50 mW, and -45 to -42 dB (or ~0.0005 to 0.008 mW) from 50 to 100 mW. These quite random results adds to the assumptions of an unpredictable result in signal strength.

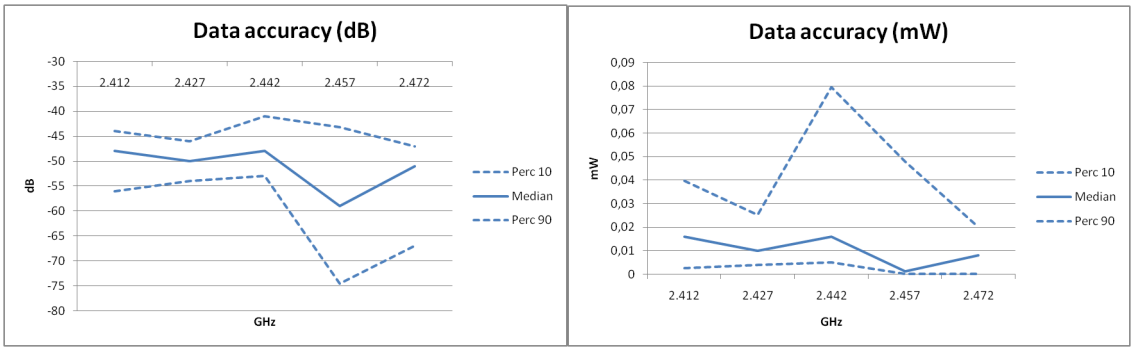
According to table 4.3 and the graph comparing the 1 and 2 meter distance results (figure 4.6(c), the signal at 2.412 to 2.442 GHz, from a distance of 1 meter is 2 - 6 dB (~0.004 - 0.012 mW, in figure 4.6(d)) greater than than the one from a 2 meter distance. However, at 2.457 and 2.472 GHz, the signal from 1 meter is 2 - 7 dB (~0.004 - 0.005 mW) lower than from 2 meter. The 1 meter measurements which are lower than the 2 meter measurement, are clearly caused by an unstable received signal, confirmed by the result in data accuracy graph figure 4.5. At the remaining two frequencies, 2.412 and 2.427 GHz, the signal strength (4 and 2 dB) are a bit low compared to the 6 dB estimate.

The results from table 4.3, graph of comparing angles in dB (figure 4.6(e)) and especially the graph comparing the angles in mW (figure 4.6(f)), show that the received signals are mostly similar, except for at 2.412 and 2.472 GHz. Here there is a larger gap between the measured signal strength of 8 and 5 dB (or $>$0.01 and $>$0.015 mW). Considering the results found in the data accuracy graph (figure 4.5), this is clearly the result of instability in the received signal and can therefore be disregarded.

In this test table 4.3 and the graphs in figure 4.6 indicates that the results found at 2.472 GHz in the 2m distance test and the 45° angle test are too high. Similarly the result seem low at 2.457 GHz in the 1m,0° test and at 2.412 GHz in the 45° test. Considering this, the results found at 2.427 and 2.442 will give the best impression when comparing the different distances and angles.

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-60	-61	-58	-69	-71
	50mW	-54	-54	-52	-64	-60
	100mW	-48	-50	-48	-59	-51
2m, 0º	1mW	-64	-63	-63	-64	-60
	50mW	-60	-58	-59	-58	-57
	100mW	-52	-52	-54	-52	-49
1m, 45º	1mW	-66	-60	-61	-59	-57
	50mW	-59	-54	-53	-61	-52
	100mW	-56	-50	-50	-53	-46

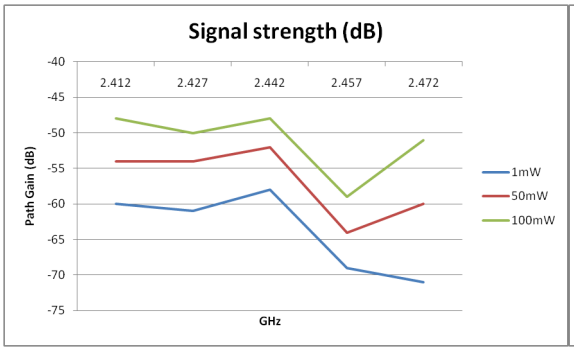
Table 4.3: Median of the REF-WIN results in dB



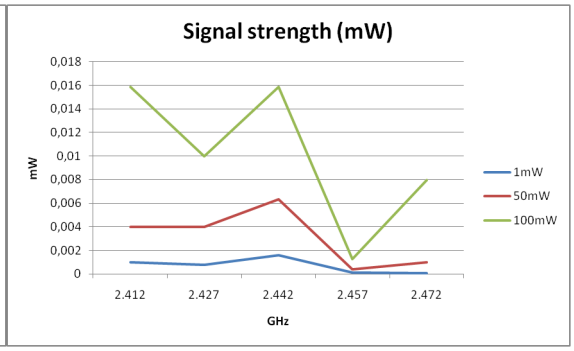
(a) Median, 10% and 90% persentiles in dB

(b) Median, 10% and 90% persentiles in mW

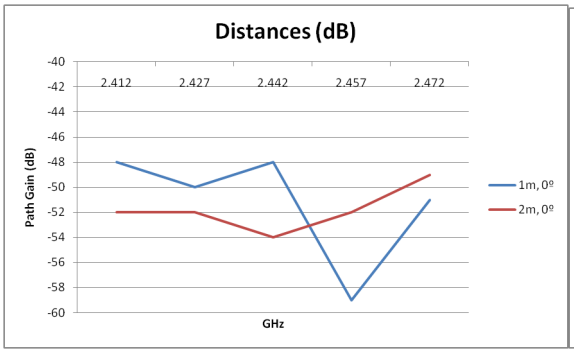
Figure 4.5: Accuracy of the REF-WIN result data (1m, 100mW)



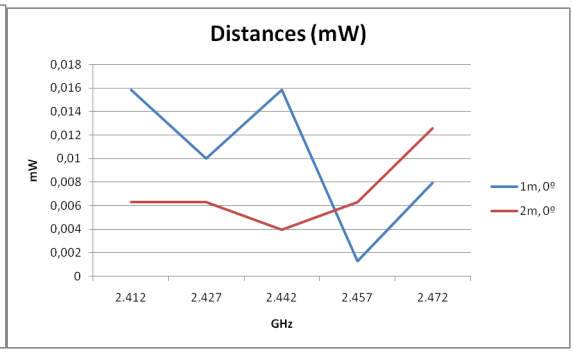
(a) Different signal strength measurements in dB



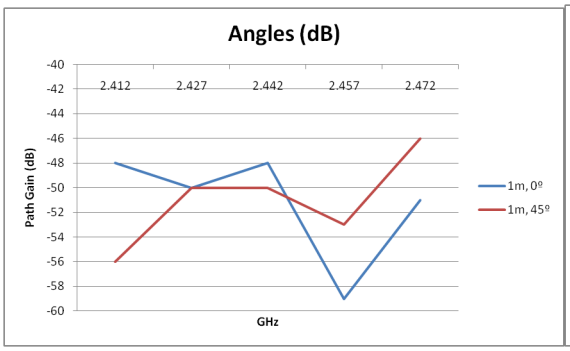
(b) Different signal strength measurements in mW



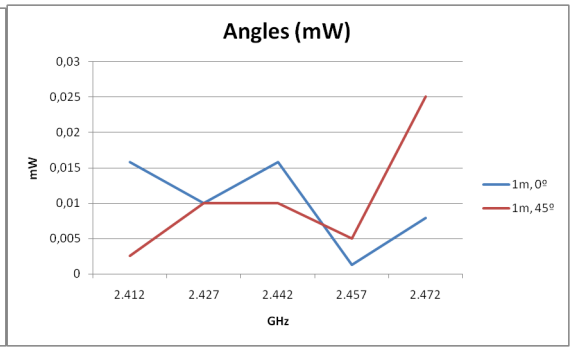
(c) Different distances measurements in dB



(d) Different distances measurements in mW



(e) Different angles measurements in dB



(f) Different angles measurements in mW

Figure 4.6: Graphs for testing results for REF-WIN

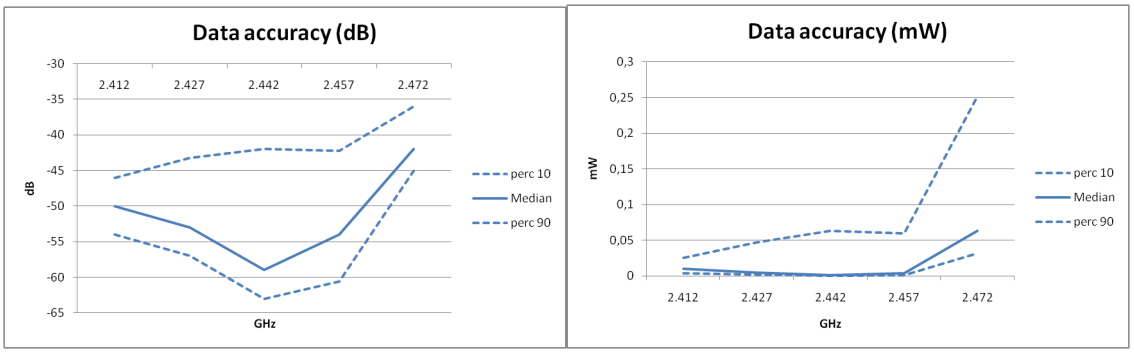
4.1.4 REF-W+P

The abbreviation REF-W+P refers to the reference testing of the test box with an acrylic window and Grounded Y-SHIELD paint applied to the interior. According to the graph the data accuracy of the result in dB (figure 4.7(a)) and in mW (figure 4.7(b)), the gap in received signal strength between the 10% and 90% percentile ranges from 8 - 21 dB (or <0.5mW to >0.20mW). The median is only found as the middle value at 2.412 GHz, for the rest of the frequencies the gap in values between the median and the 90% percentiles are insignificant to the gap between the median and the 10% percentiles. Furthermore, at 2.472 GHz the median is measured to be greater than the 10% percentile of the other frequencies, and the 10% percentile is measured to be almost 5 times greater than at the other frequencies. The results of the measurements for this test seem to be higly unstable, and seemingly increasing with frequency. Considering the method used when the testing were performed, reviewing the frequencies from the lowest to the highest, the increase can also be regarded to be caused by time. The latter is perhaps the most likely, considering the partial reflecting abilities the shielding material applied to most of the test box. Also considering that the only opening in the shielding is toward the receiver, this can be a possible cause of the steadily increasing signal strength. The result of this effect however, whatever the cause, that the median ranges from -42 to -59 dB, with the only stable signal at 2.412 GHz.

The result of the different transmitted signal strengths, are found in table 4.4, figure 4.8(a) in dB and figure 4.8(b) in mW. Only considering the stable result from 2.412 GHz, an increase is shown in the received signal strength from -61 to -53 dB (or ~0.001 to 0.005mW) when the transmitted signal is changed from 1 to 50 mW, and -53 to -50 dB (or ~0.005 to 0.01mW) from 50 to 100 mW. These results further increase the suspicions of an unpredictable increase in the received signal strength. In this test, the signals behave according to the logical assumption, where the received signal doubles when the transmitted signal is doubled. This however, is the only test where this behavior has been observed, and is therefore most likely a coincident.

In the results found in table 4.4 and the graph comparing the different angles in dB (figure 4.8(c)), the measurements from two angles have to same result of -59 dB at 2.442 GHz. At the other frequencies the difference in received signal strength for the two angles ranges between 3 and 18 dB. However, the graph with the results translated into mW (figure 4.8(d)), the difference in received signal strength between the angles at 2.472 GHz is measured to be more than 6 times greater than the strongest difference in signal strength found at any of the other frequencies. This result is most probably caused by the partly coverage by one of the shielded walls in the test box.

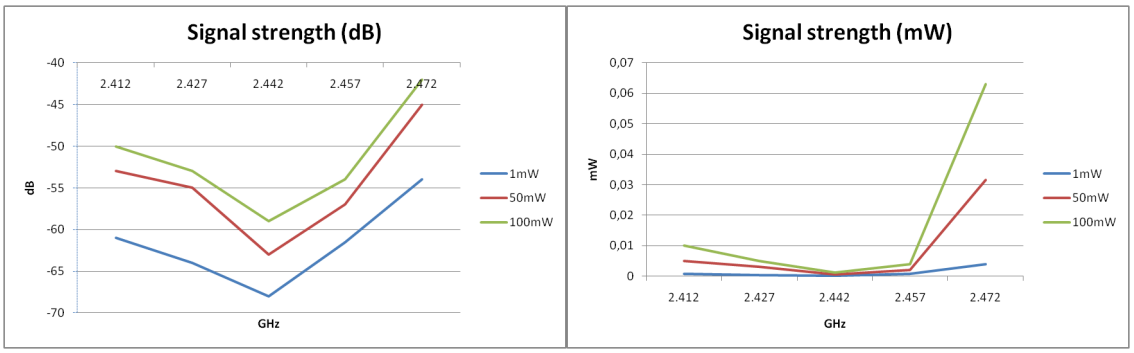
The unstable nature of the results found in table 4.4 and the graphs in figure 4.8 was not entirely unexpected, as the shielding in the paint was assumed to have some influence in the measurements. However, the extremely high signal strength found at 2.472 GHz in result found in the 0° test was on the other hand entirely unexpected. For this result not to overshadow any other results, this value will be excluded when comparing future results.



(a) Median, 10% and 90% persentiles in dB

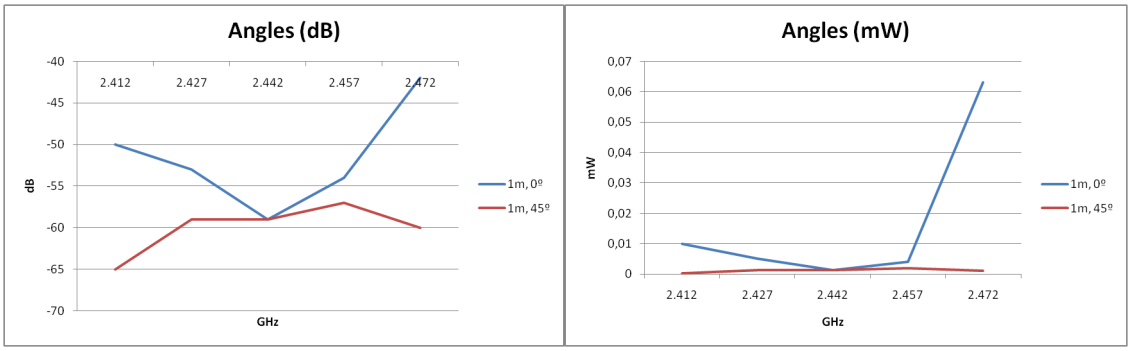
(b) Median, 10% and 90% persentiles in mW

Figure 4.7: Accuracy of the REF-W+P result data (1m, 100mW)



(a) Different signal strength measurements in dB

(b) Different signal strength measurements in mW



(c) Different angles measurements in dB

(d) Different angles measurements in mW

Figure 4.8: Graphs for testing results for REF-W+P

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-61	-64	-68	-61,5	-54
	50mW	-53	-55	-63	-57	-45
	100mW	-50	-53	-59	-54	-42
1m, 45º	1mW	-66	-70	-67	-65	-71
	50mW	-64	-62	-62	-60	-63
	100mW	-65	-59	-59	-57	-60

Table 4.4: Median of the REF-W+P results in dB

Name	dB	mW
REF	-51 to -52	0.0065 to 0.008
REF-BOX	-54 to -58	0.004 to 0.0015
REF-WIN	-48 to -51	0.016 to 0.008
REF-W+P	-50 to -54	0.01 to 0.004

Table 4.5: Comparison of the most stable measurements from the different types of test (1m, 100mW)

4.1.5 Analysis of the reference testing

All the measurements in the reference test had some fluctuation in values between the 10% and 90% percentiles. For most of the results this was around 10 in dB, or between less than 0.001 and 0.003 in mW. A smaller gap and centered median between the two percentiles meant a more stabile and accurate measurement. Also the result translated into mW gave a more accurate representation of the data than in dB. No real pattern was found data considering accuracy and signal strenght to the different frequencies. However, the results from 2.472 GHz seem to be unstable more often than the other frequencies.

According to table 4.5, showing the most stable measurements, the test REF-BOX had a 3 - 6 dB weaker received signal than the test REF, REF-WIN is 1 - 3 dB stronger and REF-W+P is 1 db stronger to 2 db weaker. The results of the difference between the REF and REF-BOX signal strength is caused by the material in the test box, indication a 3 - 6 dB attenuation. The stronger signal strength in REF-WIN and REF-W+P compared to REF may be caused by random fluctuation in the signal strength, but might also indicate that the shielding in the paint applied to the interior of the test box influenced the result. The weaker signal from REF-W+P to REF is probably also caused by the shielding paint in the test box.

The results of the received signal strength measured from the different signal strength seems to be completely random and unpredictable. However, when comparing the result in the more stable result from all the tests translated into mW some resemblance of a pattern was discovered. The received signal strength from the 1 mW transmitted signal, seemed to be approximately one tenth of the received signal strength from the 100 mW transmitted signal for all the tests. The distance of one meter in the distance measurements seemed to be too close to distinguish the difference caused by distance from the natural fluctuation in the transmitted signal. However, the most stable results from the 1 meter distance was measured to be between 2 - 3 dB, or 0.002 - 0.008 mW, stronger than the results from a 2 meter distance. This less than the 6 dB estimated difference, indicating either that the signal strength is affected by reflections in the environment, or the estimate is incorrect. Considering the results from other tests, the former seems to be the most likely.

There was a maximum 2 dB (0.005mW), difference in signal strength when comparing the more stable result from the test from a 0° and 45° angle. However, an exception of this when testing the angles in the REF-W+P test. The most stable result here gave a 15 dB, or 0.01 mW, lower signal from an 45° angle. This is probably

caused by the shielding in the box, partly covering the line of sight between the transmitter and receiver.

4.1.6 MU-CU

The MU-CU abbreviation refers to the testing of the Mu-copper foil. According to the graph showing the data accuracy of the results in dB (figure 4.9(a)) and mW (figure 4.9(b)), the gap between the 10% and 90% percentiles ranges from about 9 and 17 dB (or ~0.0005 - 0.0007 mW). The measuremnt at 2.457 and 2.472 GHz is found to be a bit more accurate, with a smaller gap between the percentiles and a more centered median. However, the difference measured signals are at such a low signal strenght that the result seem to be rather stable. The range of the median in this test was found to be between -90 and -102.

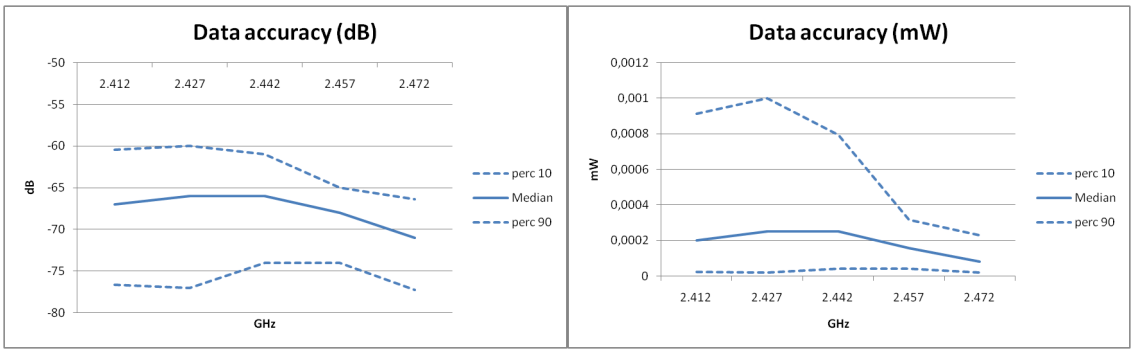
The most stable 1 meter, 0° signal from the MU-CU test, -68 to -71 dB, compared to the correspondent signal in the REF-BOX test, -54 to -58 dB, show a 13 to 14 dB attenuation in the applied shielding. In the graph comparing the result of the shielding with and without grounding (figure 4.10), the signal strength have similar strength in some frequencies. However, at 2.412 and 2.427 GHz the result from the ungrounded shield is 6 - 8 dB (~0.00015 - 0.0002mW) stronger than the grounded shield. These extremely low measured attenuation results compared to the attenuation promised in the documentation (110 dB at 1 GHz) raise the suspicion of leakage in the shielding. Equal to better attenuation of an ungrounded shield, also indicate the possibility of a weakness in the connection to ground.

The results from the different signal transmitted signal strengths are found in table 4.6, figure 4.11(a)) in dB and figure 4.11(b) in MW. Only considering the result from one of the most stable frequencies, 2.472, an increase is shown of the received signal strength from -85.5 to -77 dB (or ~0.01 to 0.02 μW) in received signal strength when the transmitted signal is changed from 1 to 50 mW, and from -77 to -71 dB (or ~0.02 to 0.08 μW) from 50 to 100 mW. This results compliments the results in the reference tests, and shows the Mu-copper have no effecting the difference in effects between the signal strength. This indicates that there is still potential for more attenuation.

Table 4.6 and the graphs comparing angles (figure 4.11), shows that while the measurements from both angles at 2.412 GHz starts at 67 dB (0.2 μW). However, when the values from the 0° results decrease with the increase in frequency, the values from the 45° increase. At 2.472 GHz the difference in value between the two angles has reached 13 dB (>0.0014 mW). This result might be caused by a leakage in the shielding, with a gradually increase in the leaked signal, as the bandwidth in the frequency gets smaller.

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-84	-86	-82	-81	-85,5
	50mW	-75	-76	-75	-72	-77
	100mW	-67	-66	-66	-68	-71
1m, 45º	1mW	-79	-83	-73	-72	-72
	50mW	-69,5	-75	-65	-64	-63
	100mW	-67	-65	-61	-59	-58

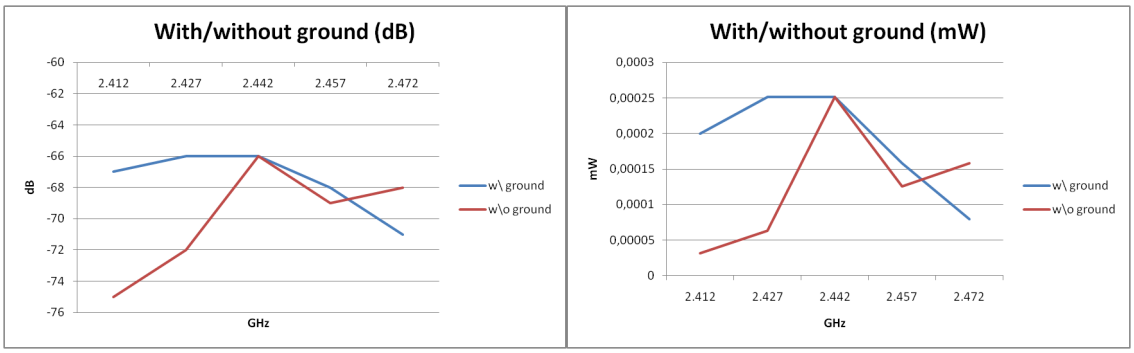
Table 4.6: Median of the MU-CU results in dB



(a) Median, 10% and 90% persentiles in dB

(b) Median, 10% and 90% persentiles in mW

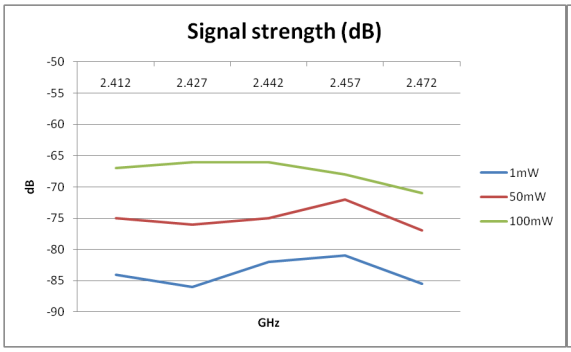
Figure 4.9: Accuracy of the MU-CU result data (1m, 100mW)



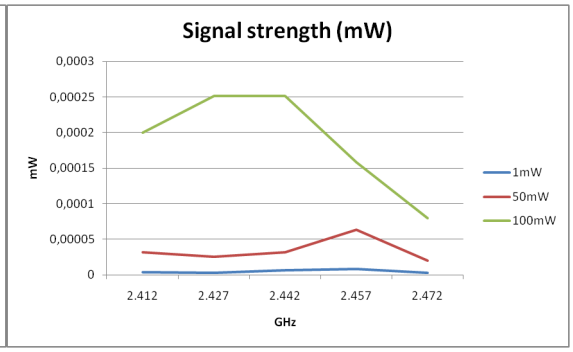
(a) With and without grounding in dB

(b) With and without grounding in mW

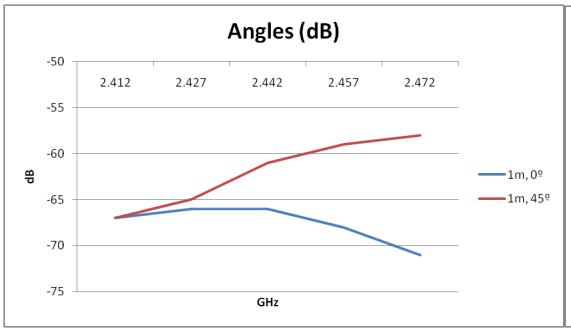
Figure 4.10: Measurements on MU-CU with and without grounding (1m, 100mW)



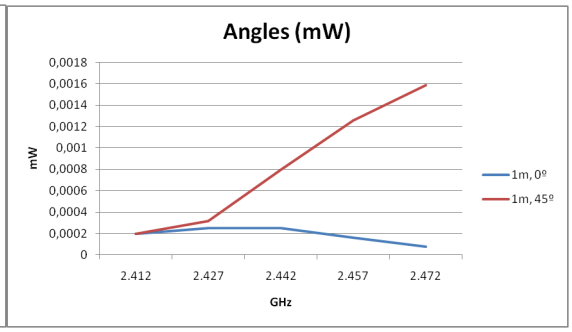
(a) Different signal strength measurements in dB



(b) Different signal strength measurements in mW



(c) Different angles measurements in dB



(d) Different angles measurements in mW

Figure 4.11: Graphs for testing results for MU-CU

4.1.7 PAINT

The abbreviation PAINT refers to the testing of Y-SHIELD paint. According the graph showing the data accuracy of the results in dB (figure 4.12(a)) and in mW (figure 4.12(b)), the gap in values between the 10% and the 90% percentiles are insignificantly small an stable for all frequencies. The gap in percentiles at 2.442 GHz however, is particularly small, less than 0.25 nW. In this test the median is measured to range from -90 to -102 dB.

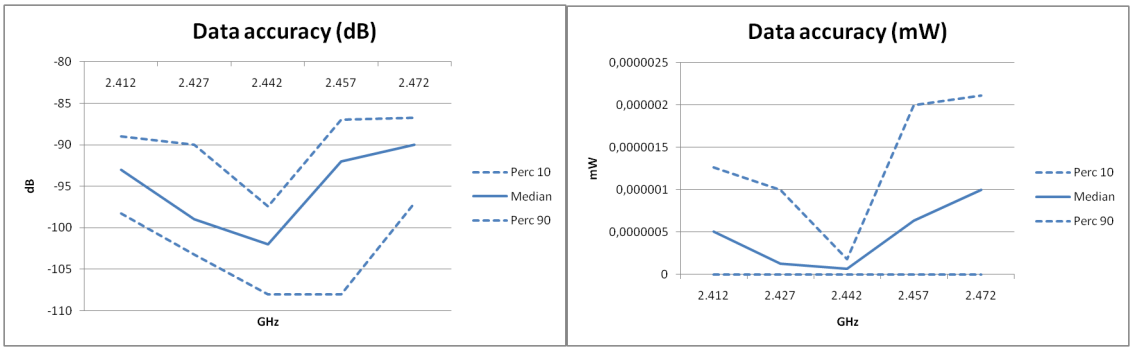
Comparing the most stable 1 meter, 0° results from the Paint test, -99 to -107 dB, with the correspondent results from the REF-BOX test, -54 to -58 dB, the attenuation is found to be between 44 and 49 dB. The graph comparing the result of the shielding with and without grounding in dB (figure 4.13(a)), reveals a more than 25 dB decrease in attenuation when the shield is left ungrounded. This large decrease in attenuation is confirmed in the graph showing the result in mW (figure 4.13(b)), although there is a large decline in signal strength at 2.442 GHz. Considering that the measured attenuation was equal or better than described in the documentation, and the much stronger signal with a ungrounded shield, the paint seem to be properly applied and grounded.

The result from the different transmitted signal strengths are found in table 4.7, figure 4.14(a) in dB and figure 4.14(b) in mW. Only considering the results from one of the most stable frequencies, 2.442 GHz, no increase is found in the received signal when the transmitted signal is changed from 1 to 50 mW. This lack of difference when the transmitted signal is increased, indicates that the maximum attenuation is reached at 50 mW, and the transmitted signal cannot be distinguished from the random noise in the testing environment. When the transmitted signal strength is increased from 50 to 100 dB however, the received signal increases from -107 to -102 (or ~0.05 - 0.25 nW), giving potential for more attenuation.

Table 4.14(c) and the graphs comparing the received signal from 1 and 2 meter in dB(4.14(c)) and in mW (figure 4.14(d)), shows a difference in received signal strength between the two distances of 3 - 10 dB ($<$1 nW). This is both more and less than the estimated 6 dB difference, further indication fluctuations in the received signal. Table 4.7 and the graph comparing the angles in dB, show little difference in signal strength between the two angles, with a maximum of 6 dB. This is also concurred in the graph with the result translated into mW (figure 4.14(f)) where the maximum is less than 1 nW. This is an indication that the angle of the transmitted signal has little effect on the attenuation.

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-102	-103	-107	-104	-101
	50mW	-99	-102	-107	-100	-96
	100mW	-93	-99	-102	-92	-90
2m, 0º	1mW	-107	-107	-108	-107	-107
	50mW	-104	-107	-108	-107	-107
	100mW	-97	-102	-107	-104	-104
1m, 45º	1mW	-105	-106	-107	-103	-100
	50mW	-102,5	-103	-107	-98,5	-96
	100mW	-99	-97	-102	-92	-92

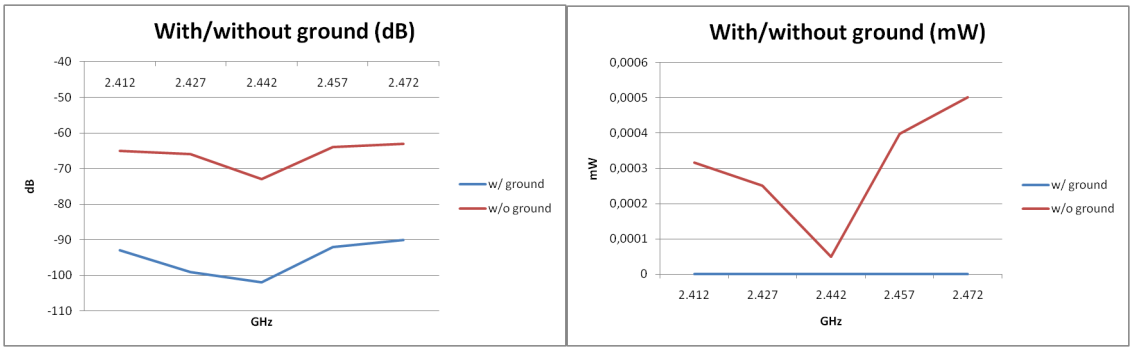
Table 4.7: Median of the PAINT results in dB



(a) Median, 10% and 90% persentiles in dB

(b) Median, 10% and 90% persentiles in mW

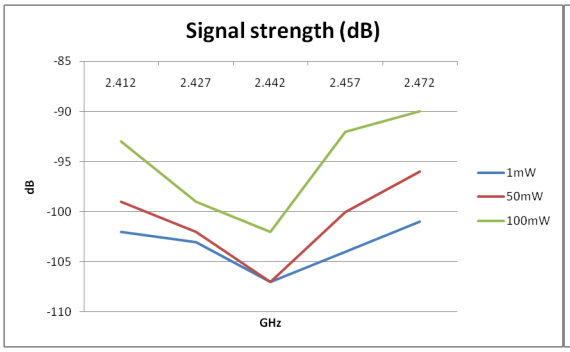
Figure 4.12: Accuracy of the PAINT result data (1m, 100mW)



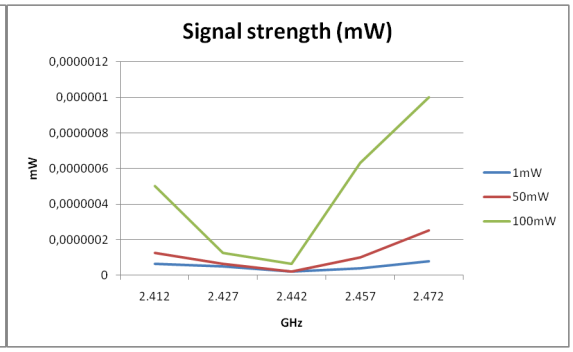
(a) With and without grounding in dB

(b) With and without grounding in mW

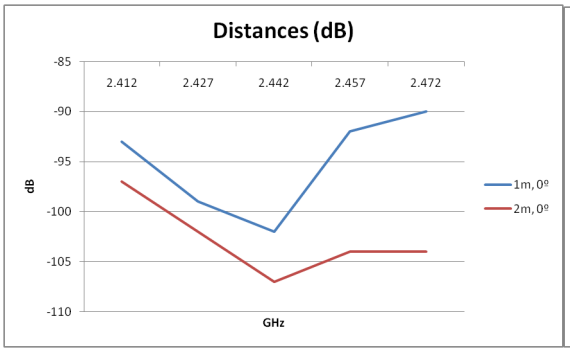
Figure 4.13: Measurements on PAINT with and without grounding (1m, 100mW)



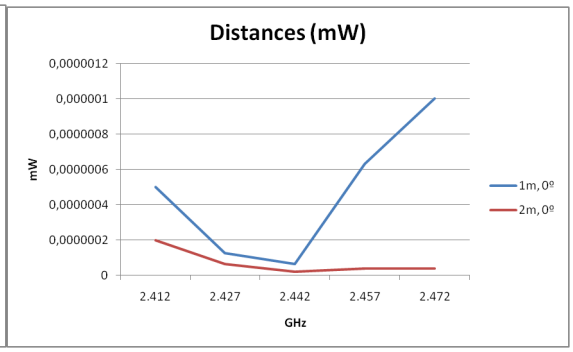
(a) Different signal strength measurements in dB



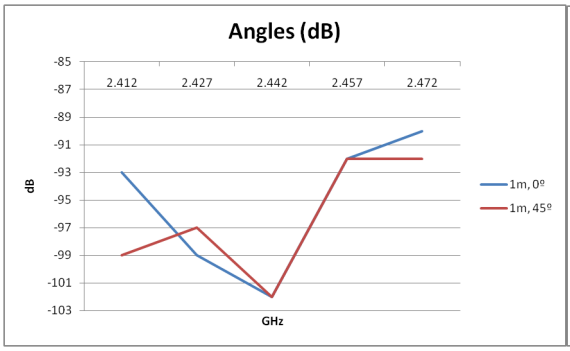
(b) Different signal strength measurements in mW



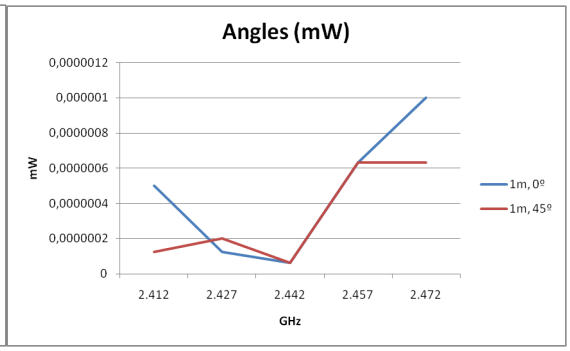
(c) Different distances measurements in dB



(d) Different distances measurements in mW



(e) Different angles measurements in dB



(f) Different angles measurements in mW

Figure 4.14: Graphs for testing results for PAINT

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-71	-72	-72	-73	-74
	50mW	-62	-67	-63	-74	-66
	100mW	-59	-61	-61	-61	-62
1m, 45º	1mW	-78	-77	-76	-76	-73
	50mW	-74	-69	-70	-69	-64,5
	100mW	-66	-67	-65	-65	-60

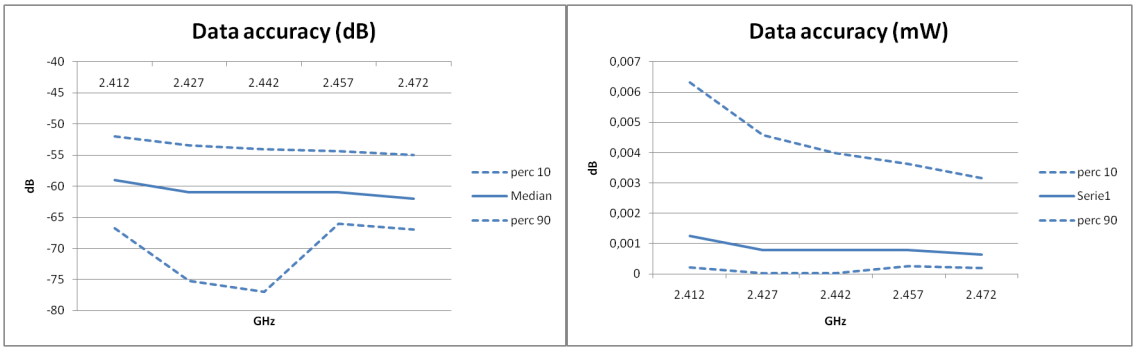
Table 4.8: Median of the MESH results in dB

4.1.8 MESH

The abbreviation MESH refers to the testing of the mesh foil for windows. According to the graph showing the data accuracy of the results in dB (figure 4.15(a)) and in mW (figure 4.15(b)), the gap between the 10% and 90% percentiles ranges from 12 - 25 dB (or ~0.003 - 0.006 mW). The graph showing the results in mmW, shows that the median is closer to the 90% percenitle, an indication of more of the higher signal strengths than the low. The median from the result of this test ranges from -59 to -62 dB.

The most stable 1 meter, 0° results from the MESH test, -61 to -62 dB, compared with the corresponding results in RED-W+P, -50 to -53 dB, indicates an attenuation of between 9 to 11 dB. This result was quite low according to the attenuation promised in the documentation (66 dB at 1 GHz), and indicated a leakage in the shielding. No test without grounding was done in this test, since the shielding in the mesh foil was connected to the shielding in the paint, which might effect the result.

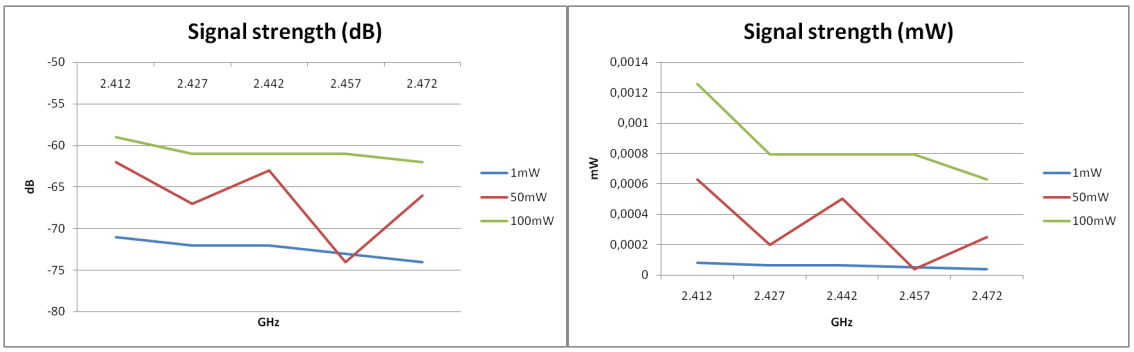
The results from the different transmitted signal strength are found in table 4.8, figure 4.16(a) in dB and figure 4.16(b) in MW. It was decided to disregard the results gathered with a 50 mW transmitted signal because of its unstable nature compared with the results from the other signal strengths. Only considering the more stable frequency, 2.472 GHz, changing the transmitted signal from 1 to 50 mW the received signal increases from -74 to -66 dB (or ~0.02 to 0.2 μW) and -66 to -62 (~0.2 to 0.6 μW) from 50 to 100 mW. This difference in received signal strength indicates that there still is potential for more attenuation. In table 4.8 and the graphs comparing angles (figure 4.16(c) and figure 4.16(d)), the received signal from a 0° angles is 4 - 7 dB (~0.005 - 0.010 mW) greater than the received signal from a 45° angle. The exception is at 2.472 GHz, where the received signal at 45° angle is 2 dB (~0.004 mW) greater than at an 0° angle. This strengthen the suspicion of a leakage in the shielding



(a) Median, 10% and 90% persentiles in dB

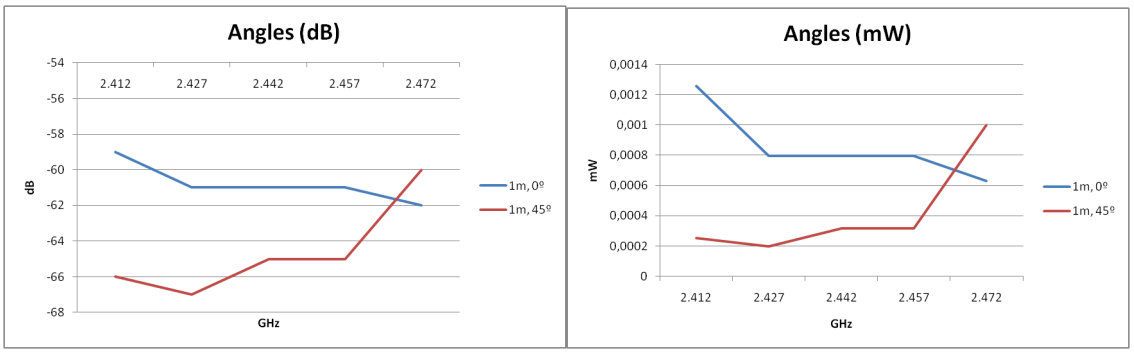
(b) Median, 10% and 90% persentiles in mW

Figure 4.15: Accuracy of the MESH result data (1m, 100mW)



(a) Different signal strength measurements in dB

(b) Different signal strength measurements in mW



(c) Different angles measurements in dB

(d) Different angles measurements in mW

Figure 4.16: Graphs for testing results for MESH

		Channel 1 2.412	Channel 4 2.427	Channel 7 2.442	Channel 10 2.457	Channel 13 2.472
1m, 0º	1mW	-84	-72	-77	-77	-72
	50mW	-73	-69	-68	-69	-64
	100mW	-65	-61	-65	-66	-60
2m, 0º	1mW	-93	-82	-80	-85	-79
	50mW	-86	-73	-72	-74	-72
	100mW	-81	-72	-68	-73	-66
1m, 45º	1mW	-78	-78	-79	-83	-78
	50mW	-69	-73	-69	-73	-69
	100mW	-66	-66	-68	-70	-65

Table 4.9: Median of the AL results in dB

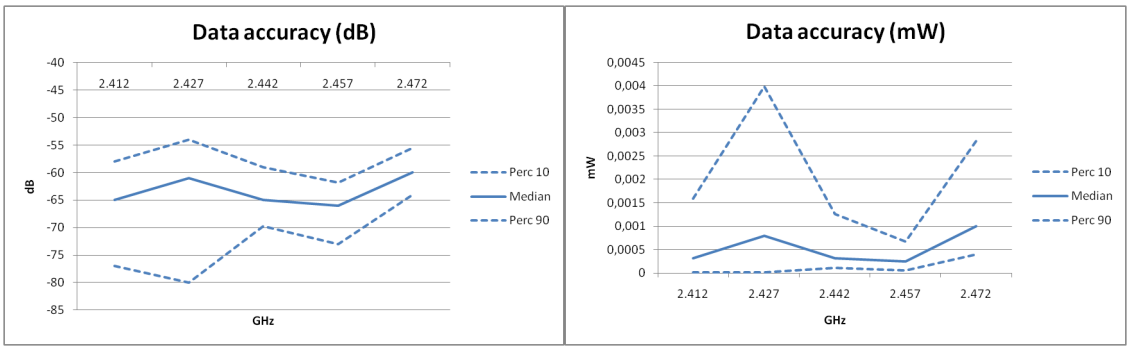
4.1.9 AL

The AL abbreviation refers to the testing of the aluminum foil. According to the graph showing the data accuracy of the results in dB (4.15(a)) and in mW (figure 4.9), the gap in the values between the 10% and 90% percentiles ranges from 8 to 19 dB (or ~0.7 to 4 μW), with the median more or less centered. The graph with the results in mW however, shows that the result are a bit more unstabel than indicated in the db graph. The most stable signal is found to be at 2.457 GHz. The median of the result in this test ranges from -60 to -66 dB.

Comparing the stable 1 meter, 0° result from the AL test, -65 to -66 dB, to the correspondent result in the REF-BOX test, -54 to -58 dB, the attenuation in the shielding is found to be between 8 and 11 dB. This result is surprisingly good, when considering the result in [56], where the aluminum foil was found to amplify the signal by 30 dB at some frequencies (although ungrounded in this test).

The results from the different transmitted signal strengths is found in table 4.9, figure 4.17(a) in dB and figure 4.17(b) in mW. Only considering the most stable frequency, 2,457 GHz, an increase is shown in the received signal strength from -77 to -69 dB (or 0.02 to 0.15 μW)when the transmitted signal strength is changed from 1 to 50 mW, and -69 to -60 dB (~0.15 to 0.25 μW) from 50 - 100 mW. This indicates a potential in further attenuation.

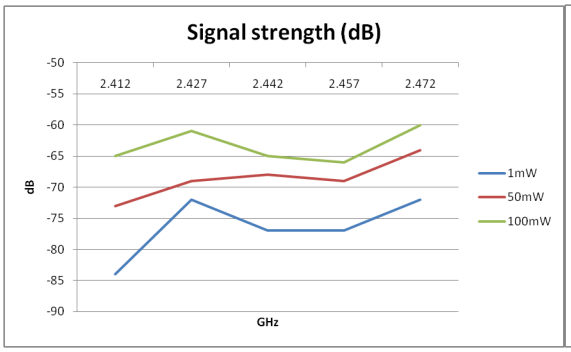
Table 4.9 and the graph comparing the received signal from 1 and 2 meter (figure 4.18(c) and 4.18(d)), shows a increased signal strength of 3 to 16 dB (<0.0002 to 0.0008 mW). This i both lower and a lot higher than the estimated 6 dB difference, further indicating fluctuation in the received signal. In table 4.9 and the graph of the result from received signal from different angles (figure 4.18(e)), the signals from the two angles seem close in strength. However, in the graph showing the results in mW (figure 4.18(f)), the signal at 2.427 and 2.472 is noticeable greater at the results from the 0° angle than at an 45° angle, compared with the difference at the other frequencies.



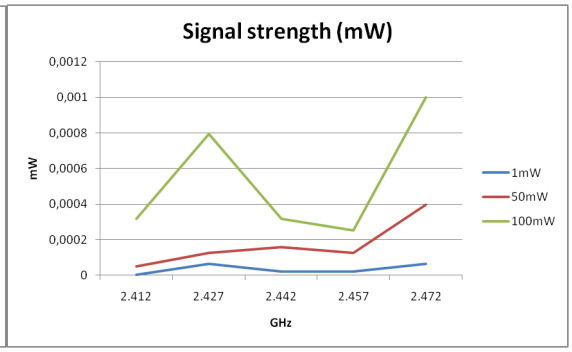
(a) Median, 10% and 90% persentiles in dB

(b) Median, 10% and 90% persentiles in mW

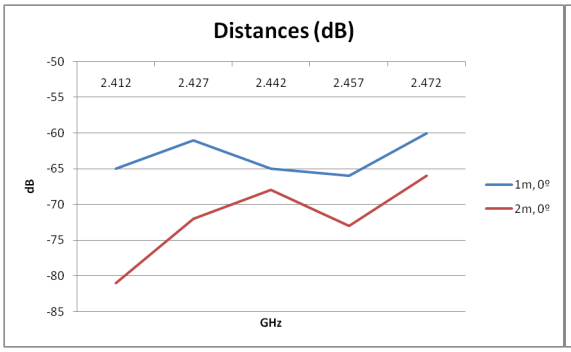
Figure 4.17: Accuracy of the AL result data (1m, 100mW)



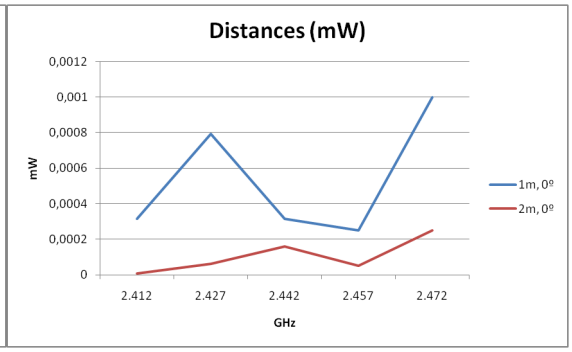
(a) Different signal strength measurements in dB



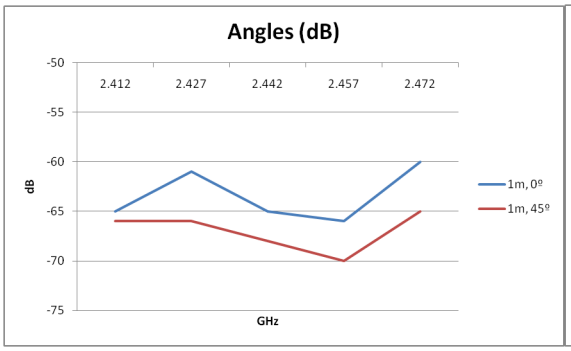
(b) Different signal strength measurements in mW



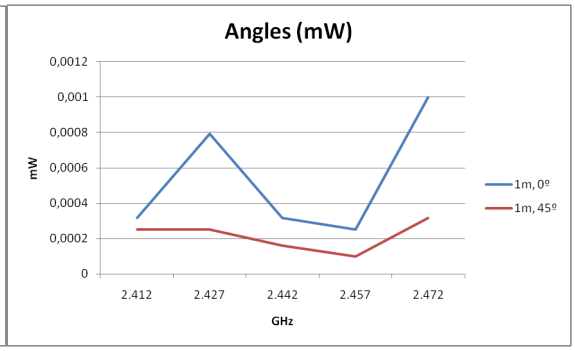
(c) Different distances measurements in dB



(d) Different distances measurements in mW



(e) Different angles measurements in dB



(f) Different angles measurements in mW

Figure 4.18: Graphs for testing results for AL

Name	Attenuation (dB)
MU-CU	13 to 14
PAINT	44 to 49
MESH	9 to 11
AL	8 to 11

Table 4.10: Attenuation calculated from only the stable results

4.1.10 Analysis of the shielding efficiency

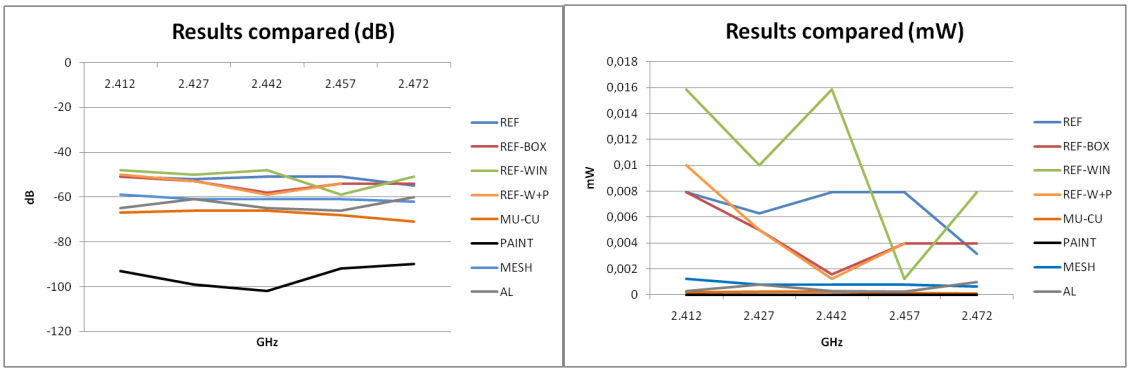
The graphs in figure 4.19 compares the data from both the reference tests and the shielding tests in both dB and mW. These graphs were made to give a clear overview of the measured results and make it easier to compare the measured signal strengths from the different test. The graph in 4.19(b) gives a more clear scope of how weak the measured signal strength in the shielding tests are, compared to the unshielded measurements. Additionally a graph in figure 4.20 shows the amount of attenuation measured from each shielding solution. The numbers in this graph was found by subtracting the shielded results from the results from the corresponding reference test.

Both the results show in table 4.10 and the graphs in figure 4.19(a) and 4.20, clearly appoint the Y-SHIELD paint as the most effective, with an attenuation between 36 to 42, 19 - 36 dB more effective than the next best solution. For the lower signals strengths the results showed an attenuation of the entire transmitted signal. The result from the most stable measurement, found in table 4.10, also shows an attenuation equal or better than the one described in its documentation (40 dB).

The results from the test of the mu-copper foil and the mesh foil (8 to 17 dB and 3 to 9 dB), found in both table and the graphs in figure 4.19(a) and 4.20, was only around a sixth or seventh of the attenuation promised in the documentation of the products (110 and 66 dB). This strongly indicates of signals leaking through the test box when these products were tested. The result of the attenuation for the MESH test at 2.472 GHz is excluded, because of the unnatural weak signal strength of the reference test, REF-W+P, at that frequency.

The somewhat low attenuation results (6 - 14 dB) found in the test of the aluminum foil is more probable. As the shielding was made from a common household article, it is not expected to be as effective as professionally manufactured products.

The graph showing all the results in mW (figure 4.19(b)), clearly shows how great the difference is between the unobstructed signals found in the reference tests compared to the ones found in the shielding test.



(a) Comparison of the results from the different tests in dB(b) Comparison of the results from the different tests in mW

Figure 4.19: Comparison of the different results

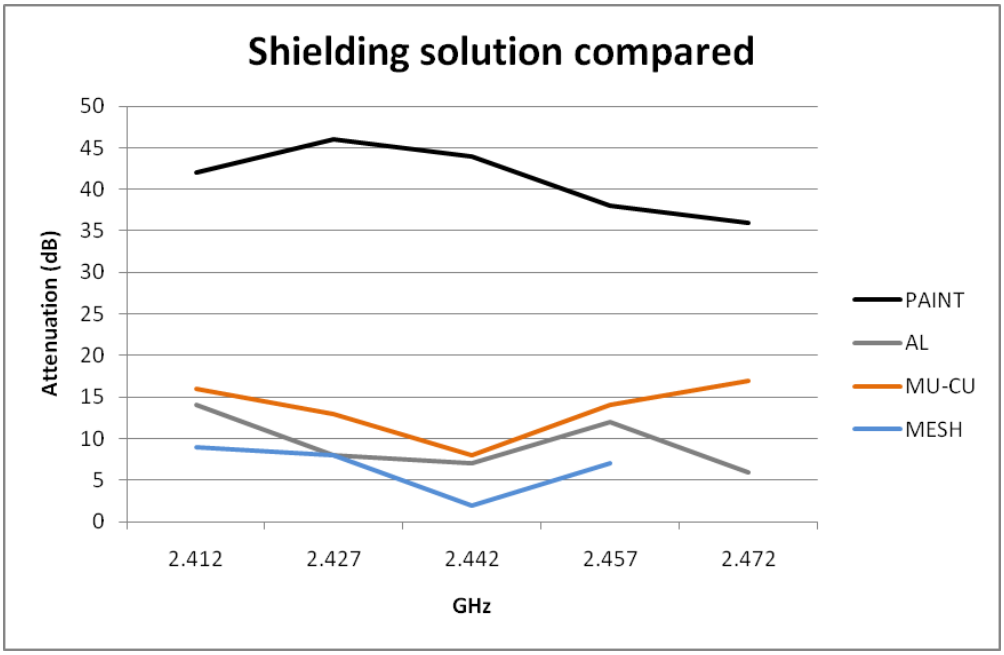


Figure 4.20: The materials compared

4.2 Cost and implementation

The results of the cost of applying the shielding solution, along with freight rates and delivery time, and the time to implement the shielding solution, along with any experiences found during the implementation. The currency conversions were done using a online currency converter widged at XE [57].

4.2.1 MU-CU

The Mu-Copper foil, ordered from Holland Shielding Systems, costs 98 EUR per 1 x 2 meter. To cover the inside of the test box, two units of copper foil were required (came in a roll of 1 x 4 meter), however only half of the second unit was used. As the package was quite large the shipping cost was 48 EUR, and as the delivery was stopped by a routine inspection at the custom, the freight time was about 10 days. Deducting the cost of the tools used in the application and for the unused materials, the total cost of purchase for the materials was 195 EUR

Preparing and applying the materials took approximately 3 hours. The sheets was relatively easy to cut, using a Stanley knife. However the chances of obtaining small injuries were quite likely, as the corners and sides of the sheets became quite sharp. Applying the sheets to the test box was quite laborious, as the glue dried quickly and the sheets needed to be places so that the entire inside area was completely covered. However, the sheets proved to be surprisingly bendable. Soldering the ground wire to the material proved to be unproblematic.

4.2.2 PAINT

Ordered from the company EMS for Less, a liter of Y-Shield cost 89.95 USD, and the Y-Shield ground kit cost 59.95 USD. The rate for the freight was quite expensive, 158 USD, but also quite quick, only 2 days from ordering, considering that the company resides in Albany,USA. Deducting the cost of the tool required for applying the paint, the total for the shielding materials was 307.90 USD. However, only about one third of the liter was used in the process of applying the paint to the test box. Considering only the cost of the material that was actually used the total cost was approximately 247.93 USD. Converted to EUR using the exchange rate at 2011-05-21 09:41 UTC (1 USD = 0.706265 EUR, 1 EUR = 1.41590 USD), this comes to 173,18 EUR.

Applying the material to the test box took approximately 30 minutes to apply, but as the paint needed to dry for 24 hours per layer, the total time from starting to apply the paint to the shield was ready for testing took 48 hours and 30 minutes. The paint was fairly easy to apply with a roller (the mandatory application method), and although the entire inside of the test box needed to be thoroughly covered the application was quickly finished. However, the health warnings in the documentation should be taken seriously as the fumes from the paint caused some headaches, nausea and throat irritation.

4.2.3 MESH

The mesh foil is ordered by sending length and width requirements to the manufacturer. There are also a selection of choices of materials, wire thickness, scratch resistance and option for self adhesive. The purchase of a standard 50 x 50 mm sheet with 70 inch wires and self adhesive was 185 EUR (although a sheet of 50 x 100 mm was delivered).

Using a Stanley knife, the foil was easy to cut to the appropriate size, however applying it proved to be more laborious than expected. As the entire window area needed to e completely covered, it took some trial and error to successfully apply the foil. As the result was prone to some air bubbles, this task might better be left for professionals for a esthetically more pleasing result. As the connecting to the rest of the shielding was done by painting, this was done without any difficulty. Cutting the product and applying it to the window took approximately between 30 minutes and an hour.

4.2.4 AL

To apply aluminum foil to the whole test box it took about one and a half roll of aluminum foil with netting pattern (44cm wide, 10 meter long, extra durable) that cost 20.50 NOK per roll. Additionally the Tack-It used for applying the foil to the test box cost 14 NOK per package. As both products was available at the nearest grocery store, neither required any freight rate or delivery time. The total cost for materials was 44.75 NOK, deducting the cost for the tools needed to cut the sheets, etc. Converted into EUR using the exchange rate at 2011-05-21 09:50 UTC (1 NOK = 0.127406 EUR, 1 EUR = 7.84890 NOK), this comes to 5.70 EUR

The task of applying the material to the test box was both quite tedious and careful work, as the foil was fairly fragile. Also two sheets needed to be applied per wall in the test box, as the width of the sheets was 440 mm, 60 mm less than the 500 x 500 mm walls in the test box. Despite these complications the shielding of the test box took about 2 hours and 30 minutes to complete, including adding the grounding.

4.3 Result summary

Considering the results from the efficiency tests, both the Mu-Copper Foil and the Mesh Foil most likely require professionals experienced in applying shielding materials for these solutions to be impervious. This will add to the cost of the already quite high expense of purchasing the materials, and making overall expenses rather costly. The Mu-copper Foil was surprisingly easy to work with, however some skill are required if the sheets are to e soldered together for better performance. The appearance of the material is hardly aesthetically appealing, and although paint or wallpaper may be directly applied to the material, the areas where the sheets meet will, probably, still be visible. Applying the Mesh Foil, making it cover every inch of the window while avoiding air bubbles, proved to be more challenging than initially expected. Disregarding the air bubbles, the visual result gave some loss in transparency, however not

Test name	Product	Efficiency (dB)		Cost (EUR)	Implement Time (hours)	Comments
		Expected	Measured			
MU-CU	Mu-Copper Foil	120	8 - 17	195	~3	Professionals may be needed for a impervious result. Sharp edges
PAINT	Y-SHIELD Paint	40	36 - 42	173,18	~0.5	Similar application as normal paint. Need 24 hour to dry. Health warnings needs to be considered
MESH	Mesh Foil	66	3 - 9	185	~0.5 - 1	Professionals may be needed for a impervious and aesthetically pleasing result
AL	Aluminum foil	-	6 - 14	5.70	~2.5	A bit fragile and flimsy material

Table 4.11: Result overview

more than expected from a pair of sunglasses.

The results in attenuation for the Y-SHIELD paint was almost exactly the same as described in its documentation. The attenuation is also described in the documentation as being per layer, so there is possibility to gain better performance by adding more layers of paint. The cost of the product a lot more affordable than both the MU-copper foil and the Mesh Foil, and one liter would also last for at least thrice the area. It was also later found that the product could be directly ordered from the manufacturer in Germany, and much of the cost of freight would be saved. Applying the paint was not any different than applying normal paint, however application by roller is required. However, the accompanying health warnings should be taken seriously, and the paint should be applied while wearing gloves and a breathing mask, and preferably in a well ventilated area. Finding weak spots may be done visually, and covered by adding an extra layer. The Y-SHIELD Paint has a black color, but can be covered by paint or wallpaper after it has dried.

The attenuation found the result from the test with the aluminum foil was quite low, and there were no indication that this was the result of leaks in the shielding. The material was also a bit to flimsy for the application to be seamlessly. However as the cheapest solution made from a household article, the result was not to bad. Perhaps a thicker, more sturdy version, specially developed for the task might prove to be more effective.

For the process of grounding the shielding, an electrician certificate is recommended for all the products. An overview and summary of the results can be found in table 4.11.

Chapter 5

Discussion and conclusion

This chapter discusses decisions and experiences made concerning the setup and approach of the experiments, the equipment used and the shielding solutions.

5.1 Experimental setup and approach review

Initially the approach was intended to be devised in collaboration with an organization or company, with experience in signal measurements and technical knowledge on the subject. The process of finding a collaborator however, was more difficult than expected. There are few research communities in close proximity to Oslo, and most of those contacted seemed to be too busy to participate in a student project. However Telenor, one of the contacted businesses, responded and agreed on a meeting to discuss the project. Through this meeting, more insight to signal measurements and testing was provided. Moreover the attendees of this meeting seemed to approve on the envisaged approach. The remaining background information and approach decisions were derived from research articles, equipment and product documentation, trial and error. Although much could be learned from doing the actual testing, some background knowledge of how to interpret and predict EMI signal behavior is recommended before starting.

The approaches found in articles and documentation concerning attenuation testing and signal measurement varied in both experimental setup and comprehensiveness. The experimental setup of the related articles either was either shielding an entire room and taking the measurements on the inside, or using directional antennas. No published articles was found using test boxes.

The approach of using test boxes gives the advantage of making the test environment portable and more flexible. Switching between different test scenarios or shielding solutions, just meant removing or switching to the proper test box. Using the test boxes also had the additional benefit of more thoroughly testing the ease of implementation, and the performance of the shielding in corners. Each test box was relatively easy and quick to build, but some experience with handling tools and building materials, ans simple construction is recommended. The material used to construct the test boxes are commonly used to build walls in homes and offices. A disadvantage

with this approach was the opening in the shielding at the floor of the box, making the shield permeable from the underside. A possible measure might be to place a shielded sheet underneath the test box, although care should be taken to connect the shielding in this sheet properly to the shielding rest of the test box. However, based on the result from the test on the Y-SHIELD paint, placing the box on a concrete floor in the lower floor of a building seem to be sufficient.

The testing environment used for testing was not completely free from interference. At the majority of the time however, the noise was so distant and weak that it was hardly registered by the equipment. An exception was the occasional noise from microwave ovens one floor above, and very rarely some noise of unknown origin, both noticeably recognizable on the user interface on the testing equipment. All testing however, ceased when interference from these sources were noticed, thus making sure that the testing result were unaffected. A possible way to avoid some of surrounding noise in the environment, would be to reverse the positions of the transmitter and the receiver, placing the receiver inside the test box. This however, would only have any impact when testing a shielding solutions with good performance. Moreover this way the user interface of the signal monitor would be visually concealed, preventing any feedback from the ongoing test.

The most ideal environment for testing would be inside room with a Faraday cage, preventing any noise from entering the test area. These types rooms are quite rare, and those that exists are usually used to protect vital equipment, and have restricted access. A room containing a Faraday cage, has recently been constructed in the new IFI building. This however, was discovered after half the tests were completed. Moreover this room proved to have some limitation in access as well.

In the related articles, most of the test described included one or perhaps two distances and one or two angles. However, the Stealth Wallpaper testing, described in the Ph.D thesis [52], includes more extensive testing, i.e. four different angles, three different spacing between the wall and the wallpaper and several prototypes of the wallpaper. In the testing done for this report two different distances and angles were first tested to see the impact this had on the measured signal. If any large difference in the measured result based on these test would have been found, more distances or angles would be added in the testing. The results found in the distance tests showed that this type of test was somewhat redundant when comparing shielding solution, although interesting for showing the attenuation of signals due to distance and sometimes useful as a reference. The 2 meter test was therefore skipped in the later tests. Testing with several angles were, although almost identical in most the test, was discovered to be rather useful when reviewing the imperviousness of the shielding implementations.

Because a 2.4 GHz wireless router was selected as the transmitter, the frequencies to test on was restricted to the channels available at the 2.4 GHz. Several of the channels would to used for testing to observe potential differences in attenuation from the different frequencies in the band. As an extra benefit, the measurements from the different channels could be used as reference point when assessing the results. Testing on all thirteen channels was found to be too comprehensive and time consuming,

however only testing on three seemed too restricted. Since each channel had its own 10 MHz spectrum, testing on five channels was found to cover most of the band. The differences between signal strength in regards to frequencies were found to be limited. However, the signal measured had a tendency to be a bit higher than the other frequencies at channel 1 (2.412 GHz), and a bit lower at channel 13 (2.472 GHz). To observe the attenuation and behavior of at different signals strengths, three levels were selected. The difference measured, although found to be rather random for all tests, were useful as reference points when assessing the reliability of the data and to detect when maximum attenuation was reached. The result from the highest transmitted signal was selected, since the objective of the testing ware to find the maximum attenuation of the different shielding solutions.

Initially each test of every frequency all signal strengths, was intended to run for five minutes, collection over 200 lines of data. However, each reference or shielding test then would then last for about 5 hours and, considering that the equipment and testing needed to be supervised the whole testing period, this was found to be too extensive. To slim down the testing time to a more acceptable level, it was reduced to 2 minutes, resulting in approximately 87 lines of data.

To analyze the data, the median of the signal and the 10% and 90% percentiles were selected. The median was chosen as this would represent the middle value of the measured data set, while the two percentiles would show if the median value levitated to the higher values, the lower values or a intermediate. Using avarage and standard deviation were considered, however, no mean was expected as the transmitted signal had a propensity to fluctuate. Additionally as the dB values were of a logarithmic scale, it would be necessary to convert every value to mW, calculate the average, and then convert the values back again to find dB average. As the obtained data consisted of both a vertical set from the 10 MHz spectrum of every channel, and a horizontal set of the per second measurements, the median an percentiles needed to be taken from both.

5.2 Equipment used

Selecting equipment is important for experiments with EMI signals, as this heavily influence the range of frequency and signal strength available for the transmitted and received signal. It also influence the reliability, stability and harmonics of both the transmitted and monitored signal. However, these parameters also heavily influence the cost of the equipment, which along with availability became the foundation for the choice in equipment for this project.

The ideal equipment for sending and receiving/monitoring signals would be a network analyzer, as this enables both sending and receiving with the same device. The right network analyzer would also have a wide range of frequencies and signal strengths available and have the potential for quite accurate measurements (though this varies with the type of network analyzer). With this device there would also be possible to change the antennas for sending/receiving. The major draw-back with a

network analyzer are that they are quite expensive. The price also go up with the frequency and the frequency range (around 23,000 EUR for a Agilent E5071C/260 9kHz to 6.5 GHz network analyzer [58]). This type of equipment would, in other words, be a unrealistic purchase for a one-semester master thesis as it is not available at HiO. An alternative to a network analyzer would be using a signal generator as a transmitter and a spectrum analyzer for receiving/monitoring. The potential for the range of frequencies and signal strength, and accuracy of measurement is about the same as with the network analyzer, though they are less flexible at antenna alterations. The prices are quite a bit lower than the network analyzer, though still quite steep for a one-semester master thesis (around 7,000 EUR for a Anritsu MS2623A 9 kHz to 6.5 GHz spectrum analyzer [59] and 7,000 EUR for a NI PXI-5652 500kHz to 6.6 GHz RF and Microwave signal generator [60]). The third more inexpensive alternative is using a wireless router as a sender and a computer (preferably a laptop) as a sender. This alternative however, limits the choices for frequency range to the 2.4 and 5 GHz WLAN spectrum and signal strengths, and also possess some issues regarding signal stability and harmonics.

In accordance to the initial intension to collaborate with an organization or business, the intent was to borrow the testing equipment available at the hypothetical collaborator. However, it was revealed that the few companies that possessed this type of equipment, only had a small selection which was much in use, and therefore only available for more than perhaps a day. It was therefore decided to use equipment available at HiO, a wireless router for transmitting and a recently purchased, USB-based spectrum analyzer as a receiver.

Initially the intension was to test the shielding solutions from 500 MHz to 6 GHz, to include the mobile phone frequency spectrum and both spectrum used for WLAN. Using a wireless router as a transmitter however limited the frequencies to the WLAN specters and to the frequencies available in the WLAN channels. Furthermore, as the frequency and signal strength configuration had to be done manually and proved to be somewhat time-consuming, it was decided to first test the 2.4 GHz band with type G router and then, potentially, extend the testing to the 5 GHz band. The possibility in signal strength configuration was limited in the default firmware in the wireless router, so new firmware needed to be installed to make options for this available. Installing new firmware on a wireless router however, is careful work as there are a chance of destroying or 'bricking' the router in each step in the process. Therefore consideration and research is recommended regarding the installation procedure and in choosing the firmware version.

Automating the testing process through scripting was considered. No way was found to control the frequency and signal strength configuration through a command line. Little time and effort would nevertheless have been saved through scripting, since the testing and testing equipment needed to be supervised, and the testing setup occasionally needed to be rearranged. The measurement of received signal from the wireless router throughout the testing, showed some fluctuation in the signal transmission. Although affected by fluctuations, it was still possible to interpret the result and compare the shielding solutions.

Before the USB-based spectrum analyzer became available, it was initially intended to use WirelessMon installed on a laptop for signal monitoring. The disadvantage of using WirelessMon as a network card however, is that the wireless network card is used as the receiver. This means that only transmitted signals from wireless routers are registered and only the signals of the connected wireless router is recorded. Additionally the quality of the measurements may vary with the quality of the wireless network card. Wireless

Additionally the interference with probable source is detected and displayed, with options for recording. This equipment was clearly designed for mapping out a wireless network environments over time, and not for intensive attenuation testing. The measurements done by the instrument seemed accurate however, and it was perfectly possible to manage and interpret the recorded data. Although more options for what and how the data was recorded was desired.

5.3 Review shielding solutions

For shielding products there was limitations in both the assortment of type and shape of the shielding, and in manufacturer and vendors. However, with consideration to time and expenses testing all the available products would be unrealistic, so a selection was chosen to represent the range of shielding products and material available. When selecting products to test it seemed important to study both the more classic and well known solution to compare with the more recent discoveries in the field. Other considerations were taken into account were how easy and time consuming the materials would be to apply, how probable it would be to implement onto an existing office area, and cost, all with regards to both likely requirements from a company and the to the restriction in time and budget for this project. Another product likely to be important to test, was shielding solutions for windows, as this would be a highly probable problem area when shielding an entire building or office. Additionally it seemed interesting to investigate how inexpensive a functioning EMI shield could be made. Aluminum foil was the most obvious option of material, as this is both cheap and commonly available.

When first searching for distributors of shielding solutions, only three suitable were found, BAE systems, Holland Shielding System and EMF for less. BAE Systems was found through a Ph.d. research project regarding testing of the frequency selective surface (FFS) called stealthy wallpaper. This type of product would have been interesting to test, as its frequency filtering qualities gives the possibilities to filter certain frequencies while letting others through, solving the issues of blocking mobile frequencies. They however, did not reply to any inquiries, and thus was excluded from the project.

Holland Shielding Systems is a company residing in the Netherlands, that specialize in electromagnetic shielding. The company has several solutions to shielding, from electronics to entire chambers including walls, windows, doors and ventilation shafts. Their solutions for shielding chambers, a MU-copper wallpaper and windows, a wired

laminated mesh was chosen to be tested as the representatives for classical and window shielding. The product prices were not published on neither the web site nor in the product catalog, so inquiries were made to the company regarding this through e-mail. In addition little information was given about installation procedure regarding application method and other products that were needed for installation, neither from the documentation on the web page nor during the e-mail correspondence when ordering. It was therefore assumed that application and grounding instructions, and any products required for installation would be included in the order. This assumption proved to be incorrect, as only the product materials were included in the received package, without any instructions. New inquiries were made to the company through e-mail and, the contact person still seemed a bit reluctant with his instructions, a make-shift solution was devised and conducted for both the Mu-copper foil and the mesh foil. It was discovered however, that there was high probability that both products were incorrectly applied, as both was measured to perform poorly. Several small measures were tried find the cause and improve it. However, none of these measures were sufficient to improve the results, and as the resources of time and options were exhausted, no real solution to stop the shielding from leaking. A more detailed explanation of the purpose of the purchase and more inquiries about application, a more impervious application might have been the result. A language barrier however is suspected as a reason for this incident, as both the purpose was it mentioned in the first correspondence and details for installations were later requested.

The Y-SHIELD paint was ordered from EMI for less which have a large assortment of EMF products, from meters and detectors, shielding devices to books and videos on the topic. The budget and available time for the project only gave an opportunity to test the Y-SHIELD paint, however, several other products distributed by this company, like shielding film, fabrics and curtains, would been interesting to study. At the first glance, due to the basic appearance of their web site and some of the odd assortment of products, like EMI shielding underware and ghost hunting kits, EMI for less could is easy to dismissed as unprofessional. The dealings with the company however, have quite to contrary been the opposite. The statistics and instructions of the products are all easily visible and available, the results from the products have been according the enclosed documentation and the response from inquiries has been quick and informative. The accuracy of the result of the implementation compared to the result described in the documentation, reveals the importance of a uncomplicated implementation with good instructions. The fare rate of the delivery, although really quickly delivered, were quite expensive, as the business, resides in Albany USA. A way discovered to avoid some of this expenses, were to order the products directly from the manufacturer, YSHIELD EMR-Protection. This company also delivers shielding window films, and other shielding solutions for walls, ceilings and floors. More of the products manufactured from this company would have been tested, since they both seems to be both better documented regarding application and less expensive than the many of the alternatives.

5.4 Future research

Through the course of this project, during background research or during the testing, ideas for other projects surfaced. Most of the ideas imagined were based on solving the question of how to maintain the signal from desired frequencies, while shielding the undesired signals.

One approach to solving this question, was discovered when testing the shielding solutions without connecting the ground wire. The difference in result concerning attenuation between a grounded and ungrounded Y-SHIELD paint, was observed to be approximately 20 dB. Although this difference also should be tested for the frequencies of desired signals, it would be possible to turn much of the attenuation on and off by installing a switch onto the ground wire. Furthermore, this switch could be replaced by a relay, controlled by a Wireless Intrusion Detection System (WIDS) programmed to audit the wireless network. In theory this setup would create a Wireless Intrusion Prevention System (WIPS), that could turn on a EM shield if any threats is detected. More research however, is required investigate the throughput of ungrounded EM shields, the options for external relay control for existing WIDS and/or the possibilities for creating an add-on if this is option is missing.

Another possible approach of filtering frequencies is using a repeater. The hypothetical procedure of incorporating a repeater is placing a directional antenna at the exterior of the shielded area, sampling any signals on desired frequencies, and one antenna at the interior of the shield, distributing or repeating the sampled signals. This approach was initially intended to be tested in this thesis, but was later excluded due to limitations in time and equipment.

When researching related work an article by Kalle-Antti Suominen and group, concerning optical shielding for cold collisions [61] was discovered. While perhaps irrelevant with regards to the project in this thesis, it gave inspiration to a solution for shielding with options for deactivation. The article describes a method to repel colliding atoms using an optical laser, which raised the question if the same method could be done using a laser to repel electromagnetic signals entering or leaving a specified area. Another imagined approach on the same topic, would be to use the noise canceling method, called active noise control (ANC) [62], sometimes used in headphones for the same purpose. To utilize this method a pair of antennas, one wide and the other one adjustable direction, might be used as another way to cancel unwanted signals. The wide antenna used for scanning the area for signals and record undesired signals, and the directional antenna used to cancel the undesired signals based on the recordings of the other antenna.

This thesis is covering shielding performance at the Wi-Fi 2.4 GHz spectrum, however shielding performance at other frequency spectrum could be useful to investigate. In addition to testing 5 GHz to cover the rest of the Wi-Fi spectrum and 500 MHz to 2.2 GHz to cover the mobile phone frequencies, more in-depth test could be done with devices using the Bluetooth (2402 to 2483.5 GHz) and Zigbee frequencies (frequency specification seems to be under development). Additionally, since MIMO (Multiple In

Multiple Out) is a technology that recently have become rather popular in the wireless communication community, studies regarding MIMO and shielding could be interesting. Since the MIMO technology uses multiple antennas to utilize of the multipath phenomenon for an improved communication performance, studies of the performance with both absorbing and reflective shielding materials could useful. The hypothesis is that an electromagnetic shield with signal absorbing abilities might therefore hurt the performance of networks using this technology, while an electromagnetic shield with signal reflecting abilities might, on the other hand, improve the performance.

5.5 Summary and conclusions

Wireless communication and WLAN has the recent years become the most common way of communicating. This is due to easy configuration, acessability and lower prices. The popularity and widespread use however, has also has created additional security problems. Different WLAN can interfere or be mistaken for each other. The more serious security issues includes eavesdropping, DoS attacks and introduction of rogue access points. Several measures to counter these issues exists, like control of transmission power, signal hiding techniques and encryption. The wireless security technique covered in this thesis, concerns site shielding using signal canceling or signal reducing materials.

Using shielding as a security method is considered as an expensive security method, comprehensive to implement. These assessments were found in articles considering wireless security, although no references was found regarding the cost and implementation of shielding solutions. As a response to these assessments the research in this thesis is revolves around comparing different shielding solutions in regards to efficiency, cost and implementation.

The shielding solution chosen for testing includes Mu-copper foil, Y-SHIELD paint, EMI/RFI transparent shielding foil (Mesh foil) and common aluminum foil. These shielding solution are chosen as representatives for the classic Faraday cage, the modern shielding design, shielding for windows and the cheap homemade alternative.

The experimental setup utilized in this theses, includes using a test box constructed of steel profiles and plaster boards, with the shielding solutions applied to the interior. These materials are commonly used as building materials in homes and offices, and are light and easy to handle. The properties of the material, combined with the shape of test boxes, create a testing environment which is both mobile and exchangeable. The covering and shielding of the floor however, is a challenge in this approach.

The frequency band covered by this thesis is the 2.4GHz band, which is the band most commonly used today. In order to do performance testing of the applied solutions, a transmitter was placed on the inside of the test box, while a monitoring receiver was placed on the outside. The receiver was placed at a 1 and 2 meter distance and at 0° and 45° angle in relation to the transmitter to test for potential signal leakage caused

by distance or angle. Both the total cost, and time and effort used for implementation were considered for the installation of each of the shielding solutions.

The attenuation of both the Mu-copper foil and was measured to be between 8 to 17 dB and 3 to 9 dB, respectively. This is considerably lower than the attenuation described in the documentation of the products. It is therefore strongly suspected these results are caused by flaws in the implementation. It can therefore be assumed that these materials needs to be installed by experienced professionals in order to reach their true potential regarding attenuation. Hiring experts for the installation would however add to the expense of the already quite costly materials. The Y-SHIELD paint on the other hand, was found possess to a 40 dB attenuation, the exact attenuation according to the documentation. The implementation of the product proved to be uncomplicated when following the enclosed instructions, and the cost was, if perhaps not inexpensive, affordable. The paint incidentally, releases slightly toxic fumes when applied, so the health warnings needs to be carefully considered. The measured attenuation of the aluminum foil was between 6 - 14 dB, which could be considered to be rather low, and nothing in the results indicated that this could be caused by flaws in the installation. The process of applying the material was relatively straight forward, although some consideration was needed regarding the flimsiness of the material. The cost of the material was the cheapest in the test, although this was one of the requirements for the inclusion.

The results of the comparison of the shielding solutions, shows that with the Y-SHIELD paint it is possible to deploy an affordable shielding with decent attenuation and non comprehensive implementation. For a completely impermeable shielding solution, a more extensive and costly installation is required, probably done by professionals. The shielding solution for windows covered in this thesis, was found to be expensive and difficult to properly implement. Other less expensive alternatives exist, although remaining untested by this thesis. The results found using aluminum foil, reveal that although inexpensive, the tested format of material attenuates to low to be considered in most cases.

Considering the issue in shielding regarding canceling desired signals, several types of frequency selective surface (FSS) materials have been developed. However, because none of them were commercially available, no FFS shielding were tested in this thesis. The low attenuation results from testing the shielding materials without grounding suggest another possible solution. This solution includes installing a switch connected to the ground wire to enable and disenable the attenuation performance in the shielding material. Furthermore, this opens for shield control by a wireless IDS, creating a Wireless IPS. The introduction of a repeater is also a possible solution to frequencies filtering.

Bibliography

[1] Jack W. Plunkett. *Plunkett's Wireless, Wi-fi, RFID & Cellular Industry Almanac 2008*. Plunkett Research ltd., 2008.

[2] I. Cuiñas, P. Gómez, M.G. Sánchez, and A.V. Alejos. Using Vegetation Barriers to Improving Wireless Network Isolation and Security. *e-Business and Telecommunications*, pages 428–438.

[3] Douglas E. Comer. *Computer Networks and Internets*. Pearson Education Ltd, 2009.

[4] William Stalling. *Data and Computer Communication*. Pearson Education Ltd, 2011.

[5] Richard W. Kroon. *A/V A to Z : An Encyclopedic Dictionary of Media, Entertainment and Other Audiovisual Terms*. Jefferson, NC, USA, 2010.

[6] Nathan J. Muller. *Wireless A to Z.* McGraw-Hill Professional Publishing, 2002.

[7] Heikki Niilo Koivo and Mohammed Elmusrati. *Systems Engineering in Wireless Communications*. Wiley, 2009.

[8] Harvey Lehpamer. *Transmission Systems Design Handbook for Wireless Networks*. Artech House, 2002.

[9] Alan J. Fenn. *Adaptive Antennas and Phased Arrays for Radar and Communications*. Artech House, 2007.

[10] John Minkoff. *Signal Processing Fundamentals and Applications for Communications and Sensing Systems*. Artech House, 2002.

[11] William H. Tranter. *Wireless Personal Communications : Emerging Technologies for Enhanced Communications*. Kluwer Academic Publishers, 1998.

[12] Barry Lewis and Peter Davis. *Wireless Networks for Dummies*. Wiley, 2004.

[13] Paul Bedell. *Wireless Crash Course (2nd Edition)*. McGraw-Hill Professional Publishing, 2005.

[14] Joseph Bocuzzi. *Signal Processing for Wireless Communications*. McGraw-Hill Professional Publishing, 2007.

[15] Tom Carpenter and Planet3 Wireless Staff. *Wireless# Certification Official Study Guide (Exam PW0-050)*. McGraw-Hill Professional Publishing, 2006.

[16] K. Pahlavan, T.H. Probert, and M.E. Chase. Trends in local wireless networks. *Communications Magazine, IEEE*, 33(3):88 –95, March 1995.

[17] IEEE Standard 802.11. Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE Standard, 2007.

[18] Michael A. Gallo and William M. Hancock. *Computer Communication and Network Technologies*. Thomson Learning Inc, 2002.

[19] M. Choi, R.J. Robles, C. Hong, and T. Kim. Wireless Network Security: Vulnerabilities, Threats and Countermeasures.

[20] J. Hindström. Hotbilder inom statiska WLAN nätverk.

[21] L.J. Lee, J.C. Kan, J.C. Lee, and M.K. Leung. Implementation of Low Cost Security for WLAN Router Networks (November 2004).

[22] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing*. Pearson Education Inc., 2007.

[23] A. Kessel, S. Goodwin, and D. Boger. Wireless Local Area Network (WLAN) Vulnerability Assessment and Security, 2005.

[24] K. Hiltunen. WLAN attacks and risks. *White Paper, Ericson*, 2008.

[25] H. ABDULLAH. A RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WIRELESS LOCAL AREA NETWORKS (WLANs) INTRUSION SECURITY RISKS. 2006.

[26] N.A. Sunday. Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures. 2008.

[27] D. Johansson and A.S. Krantz. Practical WLAN Security. *TDDC03 Projects, Spring*, 2007.

[28] H.I. Bulbul, I. Batmaz, and M. Ozel. Wireless network security: Comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols. In *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, pages 1–6. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[29] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, and S.V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, pages 321–332. ACM, 2009.

[30] Ernie Jackson. Antenna measurements with the network analyzer. Power point lecture from Antennas and Propagation (AP) Society of the IEEE Long Island Section, December 10 2008. http://www.ieee.li/pdf/viewgraphs/antenna_measurements_network_analyzer.pdf.

[31] DD-WRT. About dd-wrt. Producers website, 2011. http://www.dd-wrt.com/site/content/about.

[32] DD-WRT community. What is dd-wrt? Distributed on the DD-WRT wiki, 2011. http://www.dd-wrt.com/wiki/index.php/Main_Page.

[33] Wikibooks. Tomato firmware. Distributed on Wikibooks, January 5 2011. http://en.wikibooks.org/w/index.php?title=Tomato_Firmware&stable=1/.

[34] polarcloud.com. Tomato firmware. Producers website, December 8 2006. http://www.polarcloud.com/tomato.

[35] Radio-Electronics.com. Understanding rf signal generator specifications. Website for electronics engineers, April 25 2011. http://www.radio-electronics.com/info/t_and_m/generators/rf-signal-generator-specs-specifications.php.

[36] Radio-Electronics.com. How to use a spectrum analyzer. Website for electronics engineers, April 25 2011. http://www.radio-electronics.com/info/t_and_m/spectrum_analyser/spectrum_analyzer.php.

[37] TutorialsWeb. An introduction to spectrum analyzers. Tutorial at TutorialsWeb, April 25 2011. http://www.tutorialsweb.com/rf-measurements/spectrum-analyzer.htm.

[38] Tequipment. Fluke networks airmagnet spectrum xt, May 23 2011. http://www.tequipment.net/FlukeNetworks-AirMagnetSpectrum.html.

[39] PassMark Software. Wirelessmon, monitor wireless 802.11 wifi. Producers website, February 14 2011. http://www.passmark.com/products/wirelessmonitor.htm.

[40] Aaron Weiss. Introduction to netstumbler. Tutorial on Wi-Fi planet, 3 2006. http://www.wi-fiplanet.com/tutorials/article.php/3589131/Introduction-to-NetStumbler.htm.

[41] Vegar Jansen. Netstumbler; dette lille programmet hjelper deg å kartlegge dine trådløse omgivelser. Article on DinSide, February 27 2008. http://www.dinside.no/512161/netstumbler.

[42] Danny Briere, Pat Hurley, and Edward Ferris. *Wireless Home Networking For Dummies*. Wiley, 2008.

[43] D. D. L. Chung. Electromagnetic interference shielding effectiveness of carbon materials. *Carbon*, 39(2):279 – 285, 2001.

[44] J.S. Im, J.G. Kim, and Y.S. Lee. Fluorination effects of carbon black additives for electrical properties and EMI shielding efficiency by improved dispersion and adhesion. *Carbon*, 47(11):2640–2647, 2009.

[45] Holland Shielding System BV. Faraday cages - mu copper cage. Product information from producers webpage, April 26 2011. http://www.faradaycages.com/index2.php?p=Content id=130 nav=Faraday 20cages&nav_grp=Mu 20copper 20faraday 20cage.

[46] MR Meshram, N.K. Agrawal, B. Sinha, and PS Misra. Empirical relationship between δ and ferromagnetic resonance frequency in hexagonal ferrite-based microwave absorbing paint. *Microwave and Optical Technology Letters*, 36(5):352–355, 2003.

[47] M. R. Meshram, Nawal K. Agrawal, Bharoti Sinha, and P. S. Misra. Characterization of m-type barium hexagonal ferrite-based wide band microwave absorber. *Journal of Magnetism and Magnetic Materials*, 271(2-3):207 – 214, 2004.

[48] YSHIELD EMR-protection. Yshield shielding paints. Product information pdf from producers webpage, April 26 2011. http://www.yshield.eu/pdf/YSHIELD-EN-ShieldingPaints.pdf?x31faa=cj0r1m7l96a1t14pqe3og6e2b4.

[49] Less EMF Inc. Emf shielding & conductive paint. Product information on distributors webpage, April 26 2011. http://www.lessemf.com/paint.html.

[50] Junichi Hirai and I. Yokota. Electromagnetic shielding glass of frequency selective surfaces. In *Electromagnetic Compatibility, 1999 International Symposium on*, pages 314 –316, 1999.

[51] Holland Shielding System BV. Faraday cages - emi/rfi shielding windows. Product information from producers webpage, April 26 2011. http://www.faradaycages.com/index2.php?p=Content&id=148&nav=Faraday 20cages&nav_grp=EMI/RFI 20shielding 20windows.

[52] H.H. Sung. Frequency selective wallpaper for mitigating indoor wireless interference. *PhD Thesis-University of Auckland*, 2006.

[53] G.H.H. Sung, K.W. Sowerby, and A.G. Williamson. Modeling a low-cost frequency selective wall for wireless-friendly indoor environments. *Antennas and Wireless Propagation Letters, IEEE*, 5(1):311 –314, dec. 2006.

[54] Akihiko Ito, Hidetoshi Ebara, Hidemi Nakajima, Kouji Wada, and Osamu Hashimoto. An experimental study of a ?/4 wave absorber using a frequency-selective surface. *Microwave and Optical Technology Letters*, 28(5):321–323, 2001.

[55] Holland Shielding System. Holland Shielding System, May 18 2011. http://www.faradaycages.com/index2.php.

[56] Ali Rahimi, Ben Recht, Jason Taylor, and Noah Vawter. On the effectiveness of aluminium foil helmets: An empirical study. 2005. http://berkeley.intel-research.net/arahimi/helmet/.

[57] XE. Currency converter widget. Currecny exhange website, May 21 2011. http://www.xe.com/ucc/.

[58] Alltest Instruments inc. Anritsu ms2623a. Webpage of distributer of electronic test equipment, May 21 2011. http://www.alltest.net/.

[59] TestEQUITY. Agilent e5071c (ena) rf network analyzers. Webpage of distributer of electronic test equipment, May 21 2011. http://www.testequity.com/.

[60] National Instruments. Ni pxi-5652 rf and microwave signal generator with modulation capability. Webpage of distributer of electronic test equipment, May 21 2011. http://www.ni.com/.

[61] Kalle-Antti Suominen, Murray J. Holland, Keith Burnett, and Paul Julienne. Optical shielding of cold collisions. *Phys. Rev. A*, 51(2):1446–1457, Feb 1995.

[62] S.J. Elliott and P.A. Nelson. Active noise control. *Signal Processing Magazine, IEEE*, 10(4):12 –35, oct 1993.

Appendix A

Firmware installation

1. Reset the router
   (a) Hard reset 30/30/30
2. Download DD-WRT Micro or Mini 12548 or 12874
3. Check MD5 hash
4. Prepare the computer
   (a) Turn of firewall
   (b) Turn of antivirus
5. Log on to web GUI (192.168.1.1)
   (a) Java enable, security disabled
   (b) Write the IP
   (c) Write username and password
6. Upload firmware
   (a) Do not close browser
   (b) Do not interrupt any of the processes
   (c) Be extremely patient
7. Wait for 3+ minutes
8. Relog into the web GUI
9. Decide on a version, but not the Mega
10. Do a power cycle
11. Do a hard reset