TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MIKKO PIHLANEN

DESIGNING WIRELESS MISSION DATA TRANSFER SYSTEM FOR AIRCRAFT ENVIRONMENT

Master of Science thesis

Examiner: Professor Mikko Valkama

The examiner and topic of the thesis were approved on 8 August 2018

ABSTRACT

MIKKO PIHLANEN: Designing Wireless Mission Data Transfer System for Aircraft Environment
Tampere University of Technology
Master of Science Thesis, 57 pages
November 2018
Master's Degree Programme in Electrical Engineering
Major: Wireless Communications
Examiner: Professor Mikko Valkama

Keywords: Mission data system, Wi-Fi, WLAN, 802.11ac, 802.11ax, 802.11i, 802.1x, WPA2, WPA3, OpenSSH, OpenVPN

This thesis is about designing wireless mission data transfer system for the Finnish Air Force's Grob 115E elementary training aircraft. This thesis explains the use case of the mission data system, and how the wireless implementation for the mission data transfer would change the operation. The target was to design a system that is capable of transferring data wirelessly between the ground station and the Grob aircraft.

The biggest challenge for the implementation was the vast amount of data that was needed to be transferred from the aircraft to the ground station after the flight. Also, the time window during which the transfer had to be completed was very limited. Two WLAN standards, IEEE's 802.11ac and 802.11ax were considered as potential techniques to implement the wireless connectivity. In this thesis the WLAN security was also examined, and two additional methods outside of WLAN standards were suggested for gaining better security for the data transmission.

Wireless system utilizing the 802.11ac standard was tested and OpenSSH and OpenVPN were examined as potential techniques to strengthen the communication security. The results showed that the 802.11ac standard performs well with the communication distances of the wireless mission data transfer system. 802.11ac however has one drawback that highly diminishes its potential as the communication standard for the wireless mission data transfer system. 802.11ac doesn't perform well enough, if there are multiple clients simultaneously transferring data. The newest 802.11ax standard is not yet fully released, but its potential can be recognized, and it will fix the drawbacks of 802.11ac. On the whole, WLAN standards are suitable for implementing the wireless mission data system, if the level of security is identified as sufficient.

TIIVISTELMÄ

MIKKO PIHLANEN: Langattoman tehtävädatansiirtojärjestelmän suunnittelu lentokoneympäristöön
Tampereen teknillinen yliopisto
Diplomityö, 57 sivua
Marraskuu 2018
Sähkötekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Wireless Communications
Tarkastaja: professori Mikko Valkama

Avainsanat: Tehtävädatajärjestelmä, Wi-Fi, WLAN, 802.11ac, 802.11ax, 802.11i, 802.1x, WPA2, WPA3, OpenSSH, OpenVPN

Tämä diplomityö käsittelee langattoman tehtävädatansiirtojärjestelmän suunnittelua Suomen Ilmavoimien Grob 115E-alkeiskoulutuskoneeseen. Työssä käydään läpi tehtäväjärjestelmän käyttötarkoitus ja kuinka tehtävädatansiirtojärjestelmän langaton toteutus tulisi muuttamaan tehtäväjärjestelmän käyttöä. Tavoitteena oli suunnitella järjestelmä, joka mahdollistaa langattoman datansiirron maajärjestelmän ja Grob-lentokoneen välillä.

Suurimpana haasteena toteutukselle oli datan suuri määrä, mikä tulisi siirtää langattomasti lennon jälkeen. Aikaikkuna, jonka sisällä tiedonsiirron tulisi tapahtua on myös hyvin rajallinen. Kaksi WLAN standardia, IEEE:n 802.11ac ja 802.11ax otettiin tarkempaan tarkasteluun mahdollisina tekniikkoina langattoman tiedonsiirron toteuttamiseksi. Työssä tarkastellaan myös langattoman lähiverkon tietoturvaa ja ehdotetaan kahta menetelmää, joiden avulla tiedonsiirron turvallisuutta voitaisiin parantaa. Työssä testattiin langatonta siirtojärjestelmää joka hyödynsi IEEE:n 802.11ac standardia.

Tulosten perusteella 802.11ac standardi sopii hyvin langattomaan tiedonsiirtoon testatuilla etäisyyksillä. 802.11ac kärsii kuitenkin yhdestä vajaavaisuudesta, joka heikentää sen käytettävyyttä tämän työn tarkoitukseen. 802.11ac:n suorituskyky ei ole riittävä, jos usea verkon jäsen lähettää dataa samanaikaisesti. 802.11ax standardia ei ole vielä täysin julkaistu, mutta sen potentiaali on tunnistettavissa ja se tulee korjaamaan 802.11ac:n heikkoudet tämän työn käyttötarkoituksessa. Yhteenvetona WLAN standardit ovat käyttökelpoisia langattoman tiedonsiirron toteuttamiseen, mikäli tietoturvan tason todetaan olevan riittävä.

PREFACE

First I would like to thank Patria Aviation Oy, and especially my supervisor Tommi Kangastie for providing me the opportunity to write this thesis. I want to thank my common-law wife, family and friends for the never-ending support during my studies and the tough thesis writing process. I also want to thank my thesis instructor, Professor Mikko Valkama for the good tips and guidelines for the thesis.

In Tampere, Finland, on 15 November 2018

Mikko Pihlanen

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

3G-SDI	3rd. Generation Serial Digital Interface
AES	Advanced Encryption Standard
AP	Access Point
AS	Authentication Server
BER	Bit Error Rate
B	Byte
BP	Breakpoint
BSS	Basic Service Set
CA	Certificate Authority
CCK	Complementary Code Keying
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CP	Cyclic Prefix
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
DFT	Discrete Fourier Transform
DL	Downlink
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
DSSS	Direct Sequence Spread Spectrum
DTD	Data Transfer Device
EAPOL	Extensible Authentication Protocol Over Lan
ECDSA	Elliptic Curve Digital Signature Algorithm
EIRP	Effective Isotropic Radiated Power
ER	Extended Range
EdDSA	Edwards-curve Digital Signature Algorithm
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FICORA	Finnish Communications Regulatory Authority
FINAF	Finnish Air Force
FSL	Free Space Loss
GbE	Gigabit Ethernet
GI	Guard Interval
GSM	Global System for Mobile Communications
GTK	Group Temporary Key
HE	High Efficiency
HMAC	Hash-based Message Authentication Code
I/Q	In-Phase / Quadrature
ICI	Inter Carrier Interference
IDFT	Inverse Discrete Fourier Transform
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IR	Infrared
ISM	Industrial Scientific and Medical

ITU-R	The Radio Communication Sector of the United Nations International Telecommunication Union
IoT	Internet of Things
KRC	Key Reply Counter
LAN	Local Area Networks
LBT	Listen-Before-Talk
LLC	Logical Link Control
LOS	Line-of-sight
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
MAC	Medium Access Control
MAN	Metropolitan Area Network
MCM	Multicarrier Modulation
MCS	Modulation Coding Scheme
MFD	Multi-Function Display
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MU	Multi User
MiTM	Man in The Middle
NDP	Null Data Packet
NFC	Near Field Communications
NI	Network Interface
NLOS	Non-Line-Of-Sight
OBSS	Overlapping Basic Service Set
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PAN	Personal Area Networks
PER	Packet Error Rate
PHY	Physical Layer
PMK	Pairwise Master Key
PPDU	Physical Protocol Data Unit
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RSA	Rivest–Shamir–Adleman
RTS	Ready to Send
S2S	Station to Station
SAE	Simultaneous Authentication of Equals
SCTP	Stream Transmit Protocol
SNR	Signal to Noise Ratio
SR	Spatial Reuse
SSH	Secure Shell
SSL	Secure Socket Layer
STA	Station
STC	Space Time Coding
TKIP	Temporary Key Integrity Protocol
TLS	Transport Layer Security
TWT	Target Wake Time
TXBF	Transmit Beamforming

UL	Uplink
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V2V	Vehicle-to-Vehicle
VHT	Very High Throughput
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WLAN	Wireless Local Area Networks
WPA	Wi-Fi Protected Access
WiMax	Worldwide Interoperability for Microwave Access
b	bit
mPCIe	Mini Peripheral Component Interconnect Express
mmWave	millimeter Wave

Δf	Subcarrier Spacing
τ_{max}	Maximum Multipath Delay
B	Bandwidth
C	Channel Capacity
c	Speed of Light in Vacuum
d	Distance
d_{BP}	Breakpoint Distance
f	Frequency
f_c	Carrier Frequency
h_{AP}	AP's Antenna Height
h_{STA}	STA's Antenna Height
Hz	Hertz
T_g	Guard Interval
T_s	Symbol Duration

1. INTRODUCTION

Radio technologies have been widely used in aviation industry for many decades. Radios have been used e.g for communication, navigation and altitude measurement. In addition to these flight critical systems, modern aircraft carriers have even begun to offer wireless Internet connections for the passengers during the flight. All of the previously mentioned applications rely on radio frequencies.

Digitalization, Internet of Things (IoT) and ubiquitous networking are trends that are gaining more and more attention every year. It is inevitable that these kind of trends are gaining footing also in well established industries such as aviation and defence. Usually the adoption of new technologies is much slower in these industries.

Modern wireless communication technologies offer a possibility to connect massive number of users and also to transfer data at high rates. Usually technologies have to compromise between the number of users and the data rates, as the radio frequency resources are limited. As the number of mobile phones and other smart devices has become so large, the wireless connection between the devices and the Internet has become self-evident and often it's not even considered.

In this thesis, a wireless mission data transfer system for the Finnish Air Force's (FINAF) Grob aircraft fleet is proposed. Here the mission data system consists of a data recorder, that is used to record data from the flight. This data recorder in question must not be mixed with a so called "black box", which is a term used for data recorders in civil airliners. Black boxes are designed to survive crashes and the recorded data is used to analyze the causes that might have led to the crash. In the Grob platform, recorded data is used to analyze the training mission after the flight. The data recorder in the Grob platform can also be used to bring data from the pre-flight brief to the aircraft. The data could include e.g waypoints that can be used to make the training mission more effective. The wireless part of the mission data transfer system should include transferring the briefing data to the aircraft before the mission, and also transferring the recorded data from the aircraft after the mission. As the wireless mission data system is designed for a defence organization, the security of the wireless communication is given special attention.

The remaining of this thesis is organized as follows. Chapter 2 provides information about the FINAF's materiel and the Grob platform. It will also further introduce the behaviour of the wireless mission data transfer system. Chapter 3 introduces basic wireless communication technologies and a decision of the technology to implement the wireless mission data transfer system is made. This chapter will also introduce

the theoretical background of modern wireless communication systems. Chapter 4 will go through the various standards which are used to build the security of Wireless Local Area Networks (WLAN). Two additional ways for gaining better security are proposed. Chapter 5 introduces the trial system that is used to test the designed system. Test procedures are introduced and also the results. Finally chapter 6 concludes the thesis.

2. GENERAL DESCRIPTION

Patria is performing a large scale avionics upgrade for the FINAF Grob fleet. Grob aircraft (GO) will supersede the current Valmet L-70 Vinka fleet as the elementary training aircraft. FINAF acquired 28 Grob G 115Es from Babcock Aerospace Limited. Aircraft were previously used as training aircraft for the Royal Air Force in England [1]. Grob 115E can be seen in Figure 2.1.

Figure 2.1. *Grob 115E [1]*

The current Valmet L-70 Vinka fleet has served as the FINAF's elementary training aircraft since 1980. The Valmet L-70 Vinka was designed and built by Valmet Oy in the 1970s. The Vinka has gone through minor structural and avionics modifications during the service years. The operational flight training and aircraft maintenance of Vinkas' and Grobs' have been outsourced by FINAF to Patria. [2]

The aim of this thesis is to design and implement a wireless data transfer system system for mission data of the Grob 115E aircraft. The system will consist of Ground Station (GS) which will be fixed to the location where the aircraft are normally operating and the needed equipment that will be installed to the aircraft for enabling the wireless connectivity. This thesis mainly focuses to the selection of the technology that can be used to implement the wireless communication system, the GS and other related systems will be briefly covered. The designed wireless communication system will not be operable in flight, which means that it can be used only when

the aircraft is stationary on ground. For flight safety and to not cause any harmful interference to flight critical systems, it must be ensured that the designed wireless communication system is not functional in flight. This can be done physically or with software. Figure 2.2 represents the environment where the designed wireless mission data transfer system will operate.

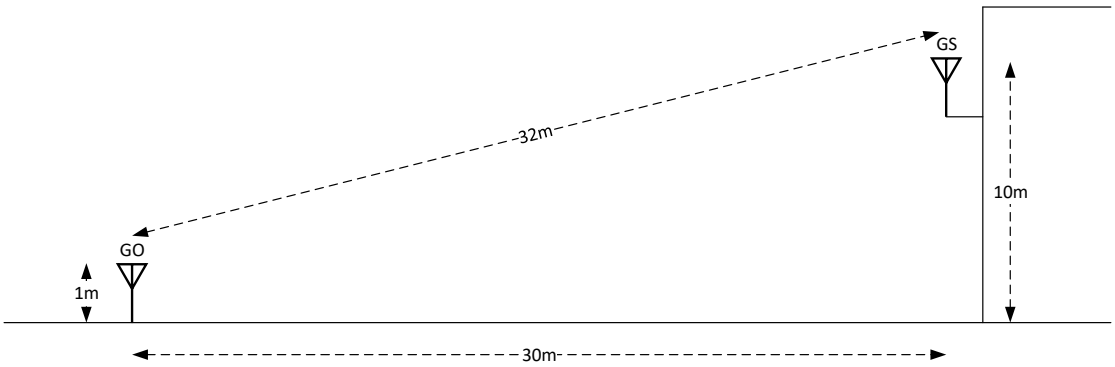

***Figure 2.2**. The communication ranges of the wireless mission data transfer system*

As seen from the Figure 2.2, the communication range is roughly 30 meters. The range will highly limit the possible technical solutions for the wireless communication. The antenna heights of GS and GO are not precise, but the values shown in the Figure 2.2 can be assumed to be feasible. In normal operation there are no buildings, vehicles or other equipment between the GS's and the GO's antennas. Due to this, the radio signal propagation can be examined as Line-of-sight (LOS) propagation. Terms LOS and NLOS (Non-line-of-sight) are used frequently when considering wireless communications.

In the first phase of the Grob upgrade program the data exchange between the aircraft and the ground station will be carried out by using physical transfer media, such as Universal Serial Bus (USB) memory stick. This thesis aims to streamline the data exchange process by suggesting a wireless communication system for the task. The mission data system is used to bring data about the upcoming mission from the pre-flight brief to the aircraft. During the flight, the system will record audio, video and certain flight parameters. After the flight the recorded data will be used to analyze the mission. Figure 2.3 shows the data flow between the GS and the GO aircraft.

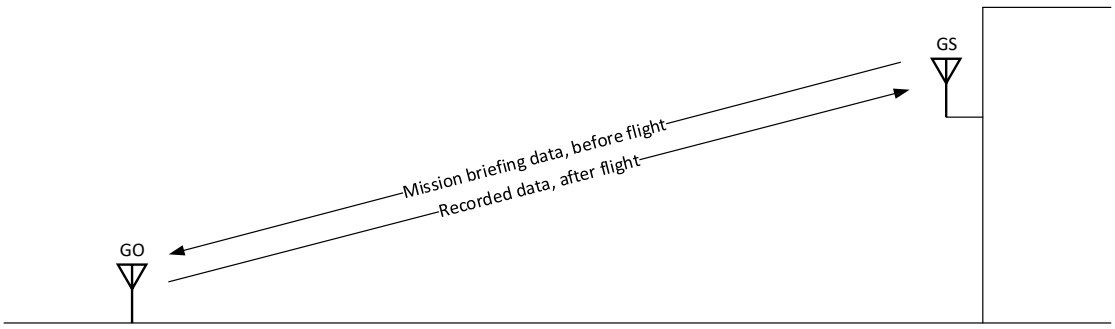

Figure 2.3. *The data flow*

The biggest challenge in the wireless implementation is the massive amount of data. The amount of data that is brought to the aircraft before the flight can be a few kilobytes (kB), but the recorded data including audio, video and flight parameters can be over 4 gigabytes (GB), assuming that the whole flight is recorded and the flight lasts for an hour. Also at this stage, the data recorder is not connected to the aircraft's battery buses, so the data recorder shuts down when the aircraft's power generator is turned off. This fact sets boundaries to the wireless communication system, as it limits the time window during which the data has to be transferred. There are yet no specific requirements for the wireless mission data transfer system, meaning that e.g the time window during which the data has to be transferred is not clearly specified. For being able to choose the wireless communication standard and to be able to reasonably evaluate the results, it is here assumed that the length of the time window is five minutes. Also for calculations, the amount of transferable data is assumed to be 4 GB in total. The wireless mission data transfer system can be simultaneously used by up to 5 Grob aircraft [3].

Because of the bidirectional data traffic between the GO aircraft and the GS, the term data recorder is slightly misleading. For this reason, from now on term Data Transfer Device (DTD) is used from the Grob's data recorder.

The upgraded mission data system will consist of the following components:

- Camera
- Multi-Function display (MFD)
- Data Transfer Device (DTD)
- Memory unit

Camera is used to capture video and audio from the flight. MFD is used to display map and other flight parameters. MFD also processes the needed flight parameters and transfers them to the DTD. DTD records video and audio that is transferred

from camera to DTD via 3rd. Generation Serial Digital Interface (3G-SDI). MFD transfers flight parameters to DTD via RS-422 serial interface. DTD stores the video and flight parameters to the memory unit. The system can be also used to load mission briefing data to the MFD before the flight.

Figure 2.4 presents a high level block diagram of the mission data system. Figure 2.4 also illustrates the wireless part of the mission data system that is to be designed.

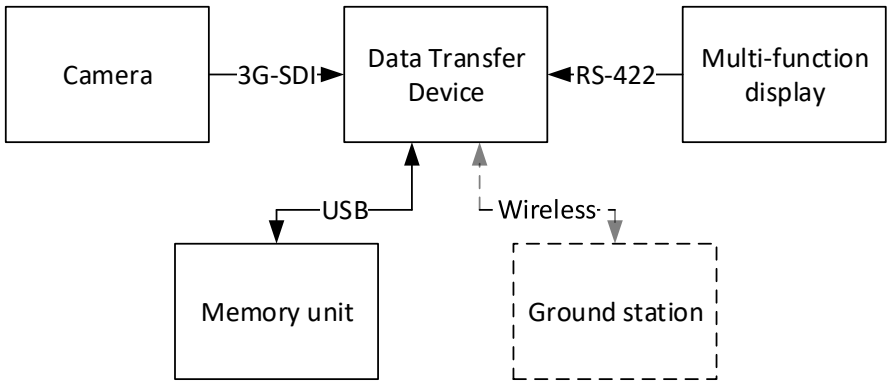

Figure 2.4. *High level block diagram of Grob 115E mission data system*

3. WIRELESS NETWORKS

The evolution of wireless communications started in 1888 when a German physicist, Heinrich Rudolf Hertz discovered radio waves. The unit of frequency, hertz (Hz) has been named after Heinrich Rudolf Hertz. After the discovery of radio waves, wireless communications have been taking giant leaps forward during the years. First packet-based wireless network was developed in 1971 by researchers of the University of Hawaii. This network was called ALOHANET, and it was used to communicate with computers between four islands. [4]

Nowadays there are plenty of wireless technologies available. When designing a system that involves wireless communications, the wireless technology to be used must be chosen wisely. When choosing a wireless communication technology for the task, ground rules are set by required data rate or throughput and communication range.

Wireless communication technologies can be grouped harshly by their range into four categories. Wide Area Network (WAN) includes technologies such as Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE). These three are the most popular mobile cellular network technologies. The upcoming 5G technology belongs partly to WAN, but 5G also introduces e.g millimeter Waves (mmWave) for higher frequencies, which are intended for much shorter ranges [5]. Metropolitan Area Network (MAN) includes technologies like Worldwide Interoperability for Microwave Access (WiMax). WiMax has been used to create city wide wireless networks and to provide Internet access for rural areas. Local Area Networks (LAN) includes one of the most distinguished wireless technology called Wi-Fi. Wi-Fi belongs more precisely to Wireless Local Area Networks (WLAN). In fact, due to its high popularity Wi-Fi has become almost like a synonym for WLAN. Personal Area Networks (PAN) includes many short range technologies, such as Bluetooth and Near Field Communications (NFC).

3.1 Choosing the Wireless Technology

Chapter 2 introduced the existing requirements and the restrictions for the wireless mission data system. The technology for implementing the wireless mission data system is chosen based on these issues. Based on these issues, the throughput is considered as the prime parameter when choosing the communication technology.

The communication range for the mission data system is approximately 30 meters. The range implicates that technologies belonging to PAN would not be sufficient.

Technologies belonging to PAN are often intended for shorter ranges than 30 meters and the throughputs are not adequate. The wireless communication in the 30 m range could be implemented with technologies belonging to LAN, MAN or WAN. Technologies in MAN and WAN are intended for longer ranges than 30 m, but in despite of that they could still be used for the wireless communication in this thesis. As stated before, the biggest requirements for the wireless communication technology are the throughput and also the capacity. In this thesis the throughput from a single GO aircraft to the GS is mainly considered. However in the final implementation, there might be up to five aircraft simultaneously transferring data via the wireless communication system. For this reason, the chosen technology has to support multiple simultaneous users.

Based on previously mentioned aspects, two wireless technologies began to raise interest: Private LTE and Wi-Fi. Private LTE is a cellular technology based on LTE, but it can be deployed and administrated locally by the end user. Wi-Fi is a WLAN technology that is recognized by almost everyone and everywhere. Private LTE solutions are provided for enterprises by for example Nokia. Private LTE could be one possibility for the wireless mission data system, because it can be deployed locally in such way, that the data doesn't have to travel through operators core network. LTE operates in licensed frequencies, but Nokia's Private LTE also has a possibility to be deployed at unlicensed frequencies. This way the deployment would be easier, because frequencies wouldn't have to be split with the local cellular network operators. [6] LTE Advanced (LTE-A) and LTE Advanced Pro (LTE-A Pro) promise data rates up to 3 Gigabits Per Second (Gb/s) in Downlink (DL) and 1.5 Gb/s in Uplink (UL) [7].

Wi-Fi standards are using unlicensed frequencies and the devices that are using these standards are sold by many vendors for both consumers and enterprises. At the time of writing this thesis, the newest fully released Wi-Fi standard capable for the task is 802.11ac. Theoretically the newest revisions of 802.11ac can provide data rates up to 7 Gb/s in both DL and UL directions. [8] 802.11ac has some drawbacks in multiuser (MU) performance in UL communication, but the upcoming 802.11ax that should be released in 2019 brings new features to fix these drawbacks.

In this thesis, Wi-Fi standards were chosen for more precise examination. The main reason for choosing Wi-Fi standards over Private LTE was the ease of deployment. There are numerous of vendors offering devices for Wi-Fi, and because of the high demand the prices are low. However, Private LTE would be a viable solution for the wireless mission data system and it could be further examined in the future.

3.2 Radio Frequencies

Radio spectrum is the part of electromagnetic wave spectrum that is used for radio communications. Radio frequencies are starting from 3 Hz and they go up to 3000

GHz. Radio spectrum is a finite resource and thus it must be used effectively. Radio frequency (RF) planning and regulation are carried out in both international and national levels. The radio communication sector of the United Nations International Telecommunication Union (ITU-R) allocates the global radio spectrum. Finnish Communications Regulatory Authority (FICORA) regulates the frequency usage nationally in Finland. The intention of frequency planning and regulation is to offer interference free radio bands for different telecommunication systems and users. ITU-R has divided the radio spectrum into 9 frequency bands (See Table 3.1).

Table 3.1. *ITU radio frequency bands*

Band	Band name	Abbreviation	Frequency range
4	Very Low Frequency	VLF	3 - 30 kHz
5	Low Frequency	LF	30 - 300 kHz
6	Medium Frequency	MF	300 - 3000 kHz
7	High Frequency	HF	3 - 30 MHz
8	Very High Frequency	VHF	30 - 300 MHz
9	Ultra High Frequency	UHF	300 - 3000 MHz
10	Super High Frequency	SHF	3 - 30 GHz
11	Extremely High Frequency	EHF	30 - 300 GHz
12	Tremendously High Frequency	THF	300 - 3000 GHz

3.2.1 Unlicensed Radio Spectrum

ITU-R has allocated sections of radio spectrum for industrial, scientific and medical (ISM) usage. Originally ISM-bands were especially meant for other use cases than radio communications. These bands were used by e.g microwave ovens, induction heating and other devices or technologies that might cause high interference in the frequency band. Afterwards many low distance radio communication technologies have started to utilize ISM-bands, like WLAN, Radio Frequency Identification (RFID) and Bluetooth. ISM-bands are unlicensed and do not require a permission to be used. The fact that ISM-bands are unlicensed makes them very popular amongst variety of technologies. By using ISM-bands users won't have to pay high fees as in when using the licensed radio spectrum. Due to high popularity, the technologies have to withstand interference from other technologies that are operating at the same frequency band. Although using frequencies from unlicensed radio spectrum will not need any permission to be used, the transmitting powers are always limited. [9] Devices and technologies using unlicensed spectrum will often have to comply with Listen-Before-Talk (LBT) principle, if the transmit power exceeds certain level. The idea of LBT is highly intuitive; the transmitting device listens to the channel before transmitting to avoid interfering other devices. LBT prevents devices from hogging the radio spectrum that is meant to be shared. [10]

The 2.4 GHz ISM-band has been widely used by WLANs. However, many WLAN channels are located higher at frequency. 5.725 - 5.875 GHz ISM-band is also used by

WLANs, but there are more WLAN channels located between these two ISM-bands. FICORA's orders for WLAN networks' frequency usage can be seen from Table 3.2. These frequencies can be used by WLANs in addition to the ISM-bands. Table 3.2 also shows the maximum Effective Isotropic Radiated Power (EIRP) that is allowed in the frequency band.

***Table 3.2**. WLAN frequencies in Finland [11]*

Frequency range	Peak EIRP
863.00 – 868.00 MHz	41 mW
2400.00 – 2483.50 MHz	100 mW
5150.00 – 5250.00 MHz	200 mW
5250.00 – 5350.00 MHz	200 mW
5470.00 – 5725.00 MHz	1 W
57.00 – 66.00 GHz	10 W

3.3 Fundamentals of Wireless Communications

Wireless transmission can be purely analog, or the system can include both analog and digital parts. Even if the data source is digital, the wireless communication system uses electromagnetic waves as the transfer medium, which are analog. In this thesis, the technologies under consideration are utilizing digital transmission, so the analog parts of the typical communication system outside of transmitter and receiver are not discussed. Figure 3.1 represents a block diagram of a transmission system, the channel block contains the used transfer medium, which is radio waves in the case of wireless communications.

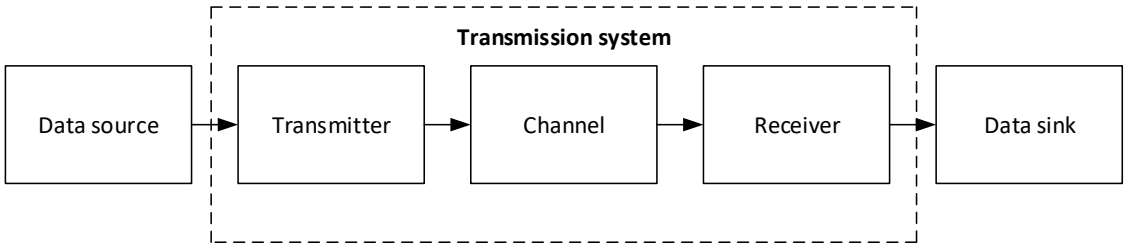

***Figure 3.1**. Simple block diagram of wireless communication system*

The basic parameters that are describing the behaviour and the performance of a digital transmission system are:

- Transfer rate (bits/s)
- Error rate
- Delay

Bit (b) is the basic unit of data that is used in digital communications. Transfer rate of a digital communication system is in many cases represented in bits per

second. It must be noted that the reported transfer rates of a digital communication system often differ from the achieved transfer rate due to overhead caused by different network layers and protocols. Wireless communication systems are prone for interferences which reduces the system performance. Unit Bit Error Rate (BER) is used to describe the error rate of the system. BER represents the percentage of the transferred bits that were erroneous. Delay consists of signal propagation delay and used signal processing methods. The significance of these parameters is heavily dependent on the purpose of the wireless communication system. Some applications, like Vehicle-to-Vehicle (V2V) communication between two automated cars require a small delay. On the other hand, for example IoT applications usually won't have this kind of requirements.

Following sections are covering common techniques that are used in modern wireless communication technologies.

3.3.1 Orthogonal Frequency Division Multiplexing

Orthogonal Frequency Division Multiplexing (OFDM) is a special case of Multicarrier Modulation (MCM). In multicarrier modulation, the transferable bitstream is divided into multiple streams and transferred using multiple subcarriers. Every subcarrier is modulated individually. The idea in MCM is to divide the available channel into smaller subcarriers. The number of subcarriers is chosen in such way that the amplitude response of each channel would be constant. [12]

OFDM is tolerant of time synchronization error, it is bandwidth efficient and thus it has been widely used in wireless communication technologies [4]. The word "orthogonal" in OFDM means that the peak of each subcarrier locates where neighbouring subcarriers' signals crosses the zero. The orthogonality also makes OFDM bandwidth efficient, since the subcarriers can be located near each other in frequency, without causing Inter Carrier Interference (ICI). Orthogonality is achieved by using a subcarrier spacing that is an integer multiple of the inverse of the OFDM symbol duration [12].

Figure 3.2 represents a single OFDM subcarrier, and a OFDM signal consisting of five independent subcarriers.

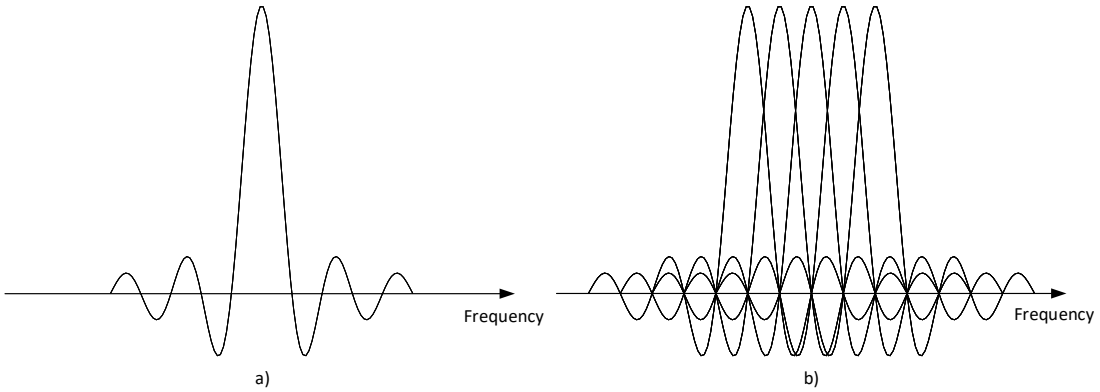

Figure 3.2. *The subfigure a) shows the spectra of a single OFDM subcarrier, subfigure b) shows the spectra of OFDM signal.*

The OFDM symbol of duration T_s is mathematically given by

$$x(t) = \sum_{k=0}^{N-1} X(k) exp[i2\pi f_k t] \tag{3.1}$$

where $X(k)$ is a complex data symbol from the used symbol alphabet. The subcarrier frequencies are defined as

$$f_k = f_0 + k\Delta f \tag{3.2}$$

where f_0 is the frequency of the first subcarrier, k is the subcarrier index and Δf is the subcarrier spacing. The subcarrier spacing, which is the frequency separation of the subcarriers, is given as

$$\Delta f = 1/T_s \tag{3.3}$$

where T_s is the used symbol duration. The smallest usable subcarrier spacing, which also results in the best spectral efficiency is $1/T_s$.

Figure 3.3 represents a simplified block diagram of a OFDM transmission system.

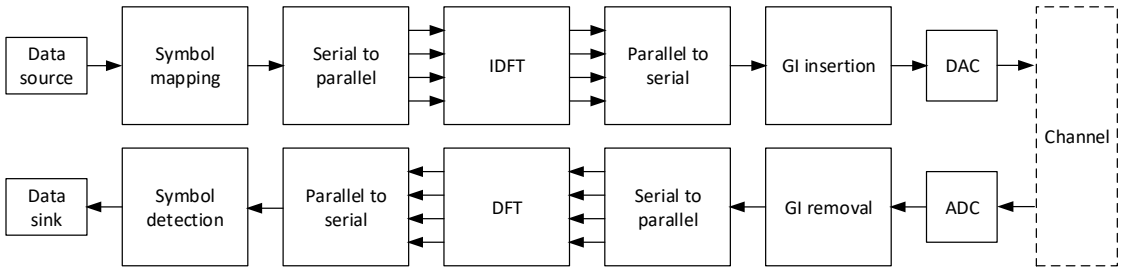

Figure 3.3. *Simplified block diagram of the OFDM transmission system showing the baseband processing parts.*

On the top left corner of the Figure is the input of the transmission system. The data source block consists of digital data that is then mapped into symbols from the chosen alphabet. If the used modulation method is 256 Quadrature Amplitude Modulation (256-QAM), the alphabet consists of 256 different symbols. With 256-QAM, each symbol embodies 8 bits. The next block converts the stream of modulated symbols into multiple parallel streams. The number of parallel streams is the number of used OFDM subcarriers. IDFT block calculates inverse fourier transform (IDFT) for each symbol in each subcarrier. IDFT and Discrete Fourier Transform (DFT) are widely used algorithms in digital signal processing [12]. In OFDM systems, DFT and IDFT are generally implemented with Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT). With FFT and IFFT, the DFT and IDFT operations can be implemented with high efficiency [13]. After IDFT, the parallel streams of subcarriers are serialized and formed into a one OFDM-signal, after which the Guard Interval (GI) is inserted. Guard interval is added to every OFDM symbol to increase its length. In OFDM systems, the GI is often implemented as Cyclic Prefix (CP). With CP, OFDM system is protected against channel delay spread, which is caused by multi-path propagation [14]. Multi-path propagation is a destructive effect, which causes reflected (i.e delayed) signals to be summed to the original signal at the receiver. This unwanted signal summation yields to harmful phenomenon called Inter Symbol Interference (ISI). The length of CP is defined as T_g, and the length of T_g must exceed the length of the maximum multi-path delay τ_{max} of the channel to completely elude ISI. [13]. With the added CP, the length of OFDM-symbol is defined as

$$T = T_s + T_g \tag{3.4}$$

Figure 3.4 represents the time composition of OFDM symbol. Figure 3.4 illustrates how the CP is implemented, CP is the end portion of the symbol that it is used to prefix the symbol itself.

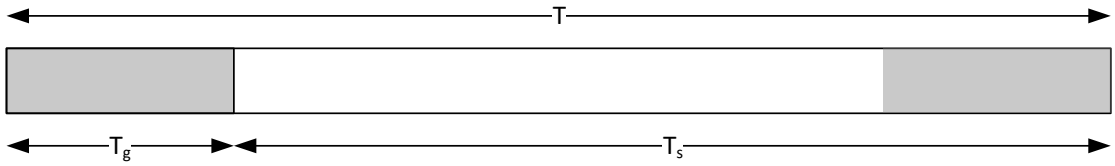

Figure 3.4. *OFDM symbol composition*

The power of OFDM is that the orthogonality of the subcarriers can be preserved despite of multipath propagation with the help of CP. Next the digital OFDM-signal is converted into an analog waveform and transmitted to the wireless channel. The OFDM system in Figure 3.3 in fact produces a complex baseband signal, which has to be modulated with I/Q modulator to generate a passband RF waveform [15]. The receiver functions are more or less the same as in the transmitter, but reversed.

3.3.2 Orthogonal Frequency Division Multiple Access

Orthogonal Frequency Division Multiple Access (OFDMA) is a MU variant of OFDM, and it is well known for its deployment in LTE and WiMax. In OFDMA, channels are consisting of multiple subcarriers, as in OFDM, but the subcarriers are divided into multiple groups instead of just one. These groups are called Resource Units (RU) and they can be shared between multiple users. In OFDM, one user uses all the subcarriers at the same time, so only one user is able to access the channel at a certain time. In OFDMA, RUs are allowing the channel to be occupied by multiple users at a certain time. Figure 3.5 clarifies the basic differences of OFDM and OFDMA, different users have been marked with different colors and unused resources in Figure 3.5 have been marked with grey diagonal pattern.

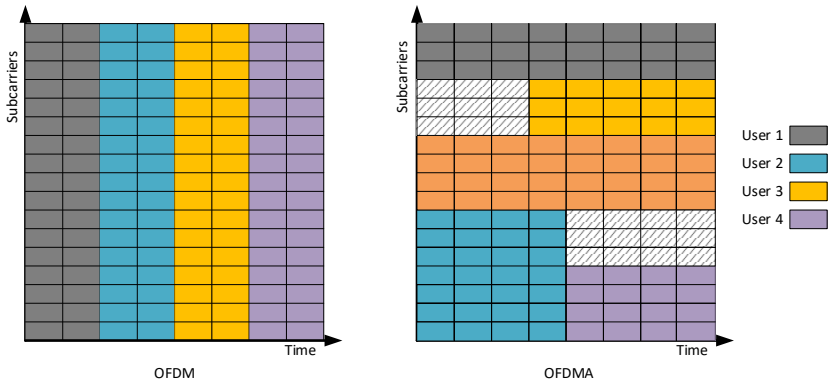

Figure 3.5. *Conceptual illustration that shows differences between OFDM and OFDMA*

OFDMA allows to allocate RUs for users based on the knowledge of the channel frequency response. As the channel frequency response varies especially with mobile users, OFDMA allows to select the most suitable channel (i.e RU) for every user [16]. OFDMA also brings flexibility to the transmission systems, because the transmitter is able to control the gain of each RU separately. Transmitting power of single RU can be increased to better serve users with weaker channel conditions by decreasing the transmitting power for RUs with better channel conditions. The size of the RUs is not fixed, so smaller RUs can be allocated e.g for users that require better Signal to Noise Ratio (SNR).

3.3.3 Multiple-input Multiple-output

Multiple-Input Multiple-Output (MIMO) is a transmission scheme in which the transmitter and the receiver are using multiple antennas to communicate. MIMO can be implemented with Space Time Coding (STC) or with spatial multiplexing. With STC, single data stream is duplicated and transmitted with multiple antennas. Space time codes are used to encode the parallel, redundant streams to make the transmitted signals orthogonal with each other. At the receiver, signals are separated and the original data stream is recovered. [17] With STC, the transmit and receive diversities are used to improve the quality of the transmission.

Other implementation of MIMO is called spatial multiplexing. Spatial multiplexing, which is also referred as true MIMO, is used to boost spectral efficiency. With spatial multiplexing, the transmitter divides the data stream into multiple parallel streams. These streams are transmitted and received with a specified TX/RX antenna pair. Gain in spectral efficiency is achieved by transmitting multiple signals in the same frequency band. Due to multi-path propagation, signals will propagate through the channel by using different routes. This is the basic concept of spatial multiplexing. At the receiver, estimates of the channels are used for correctly detecting separate signals. [18]

The channel capacity C in MIMO system that is utilizing spatial multiplexing can be represented with *Shannon-Hartley Theorem* as:

$$C = M \times B \times log_2(1 + SNR) \tag{3.5}$$

where M is the number or spatial streams, B is the channel bandwidth and SNR is the Signal to Noise Ratio. An example of a MIMO system is presented in Figure 3.6.

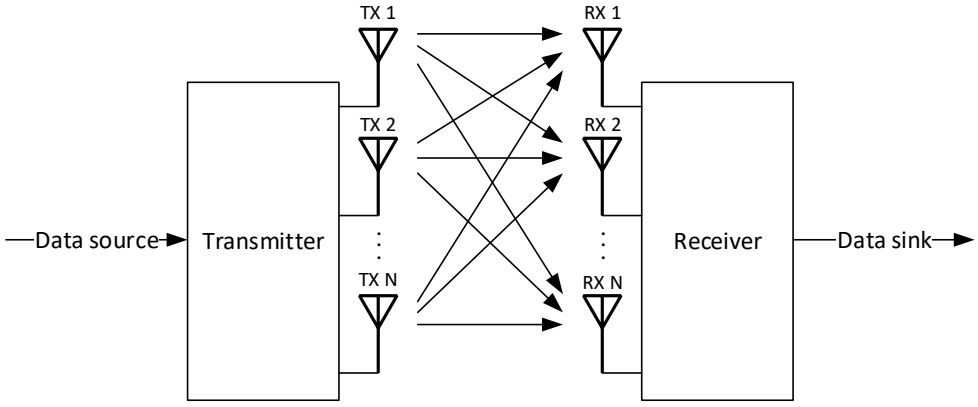

Figure 3.6. *Basic block diagram of a MIMO communication system*

3.3.4 Beamforming

Antenna directivity is a basic concept in RF technology. With directional antennas, the transmission or reception of an antenna can be focused to a specific direction. The value of antenna directivity is known as antenna gain. The higher the antenna gain is, the larger amount of the total power is transmitted or received. Antennas with high gain are often expensive and large in size. Luckily, multiantenna communication systems provide an alternative solution for high gain antennas with beamforming. Beamforming or alternatively beam steering is a concept, in which the transmission or reception of multiple antennas, called an antenna array, can be focused to a certain direction. Beamforming can be used even if the antennas of antenna array are omni-directional, meaning that the antennas radiate in every direction. In beamforming, the phase and amplitude of each antenna's signal are adjusted. This results in a direction-dependent constructive or destructive signal summation. It must be noted that beamforming works most effectively in LOS propagation. Beamforming can be implemented analogically, digitally with the transceiver's Digital Signal Processor (DSP) -algorithms or with the combination of these two. Analog beamformers include multiple phase shifters and one or more signal combiners. [19, 20]

Beamforming can be implemented either implicitly or explicitly. Implicit beamforming means that the beamformer generates the beamforming parameters based on the channel information gathered from the received signal. This means that the beamformee, does not estimate the channel, only the beamformer. On the contrary, in explicit beamforming the beamformee estimates the channel and sends this estimate back to the beamformer. Beamformer will then adjust the beamforming parameters based on the beamformee's channel estimation. Implicit beamforming adds less overhead to the transmission system, but it is less accurate. [21]

3.4 Wi-Fi

Wi-Fi is a trademark of a non-profit association called Wi-Fi Alliance. Wi-Fi alliance is a group of companies that are participating in the development of Institute of Electrical and Electronics Engineers (IEEE) standards. Wi-Fi Alliance was originally founded in 1999. Back then the foundation was called Wireless Ethernet Compatibility Alliance (WECA) and it was renamed to Wi-Fi Alliance in 2003. The need for an association that certifies Wi-Fi products became clear briefly after the first 802.11 standard was published. Many vendors published products that were not fully compatible with the standards. [22] Wi-Fi Alliance's certification ensures that the products meet the standards for interoperability, security and other application specific protocols. Any product that utilizes 802.11 standards and has been certified by the Wi-Fi Alliance will have a Wi-Fi Certified seal of approval.

Against common belief Wi-Fi is not a shortname for Wireless Fidelity. Wireless Fidelity was a slogan that was used by Wi-Fi Alliance in the early days of Wi-Fi. Wi-Fi is simply a trademarked, consumer friendly name for IEEE 802.11 standards. In October 2018, Wi-Fi Alliance announced a new naming policy for the Wi-Fi standards. Wi-Fi Alliance will identify IEEE 802.11n with Wi-Fi 4, 802.11ac with Wi-Fi 5 and the upcoming 802.11ax with Wi-Fi 6. Older IEEE 802.11 standards will not get new names. [23]

Generally when talking about Wi-Fi systems, terms Station (STA) and Access Point (AP) are being used. STA is a single entity, or client that can be connected to the AP or other STAs via the wireless medium. AP includes one STA, and in addition it also provides access to the distribution services via the wireless medium for other connected STAs.

IEEE 802.11 standard is a part of IEEE 802 LAN and MAN networking family and it adopts the 48-bit addressing scheme, which is better known as MAC address scheme. MAC addresses can be used to identify the devices in Ethernet and Wi-Fi networks.

To gain better understanding about the concepts of different network layers, Open Systems Interconnection (OSI) model is often used. OSI model divides the communication systems usually into seven abstraction layers, but there are also variants of the OSI model with different amount of abstraction layers. The IEEE 802.11 standard defines PHY and MAC layers for the Wi-Fi communication. 802.11 PHY layer implements the lowest layer of the OSI model, which is called physical layer. In IEEE 802.11, the second layer consists of MAC layer and Logical Link Control (LLC) layer, these layers together are forming the OSI model's data link layer. The 7-layer OSI-model is presented in Table 3.3

Table 3.3. *OSI model*

OSI model layers	Description	Examples
7. Application	Used by applications that are visible to the user	HTTP, FTP
6. Presentation	This layer's protocols are used for adapting the data for the application layer's applications	TLS, SSL
5. Session	Used to establish communication sessions	NetBIOS
4. Transport	Used to transfer data reliably from end to end, implements flow control, packet segmentation and error control	TCP, UDP
3. Network	Provides methods to transfer variable length data from source to destination	IP, IPsec
2. Data link	Provides the means for transferring data between devices	LLC, MPLS 802.11 MAC
1. Physical	Provides the physical and electrical specifications for the devices	802.11 PHY

3.4.1 IEEE 802.11 Medium Access Control

When the idea of WLAN was elaborated, it was thought as just another Physical Layer (PHY) implementation for the existing IEEE standards. The most dominant standard of IEEE was 802.3, Ethernet. It was quickly realized that the radio medium differs very much from the familiar wire. In wireless environment high attenuation, and the fact that the transmitter can only sense its own signal when transmitting causes collisions to be undetectable. This is the reason why Ethernet's Medium Access Control (MAC), Carrier Sense Multiple Access with Collision Detection (CSMA/CD) could not be applied. It was understood that the wireless medium would need its own MAC, and in 1991 project 802.11 was approved. The MAC for 802.11 is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA follows LBT principle. The transmitting STA listens to the wireless medium before trying to transmit, if there is already an ongoing transmission, the listening STA will wait for a time period defined by binary exponential backoff algorithm. After the waiting period, the STA will retry the transmission. The medium has to be idle before STA begins the transmission. This is the basic principle of the carrier sensing. As collisions can't be detected in wireless environment, the next best thing to do is to try to avoid collisions as well as possible. [24]

Wireless LAN also suffers from another problem that does not occur in wired environment, the hidden node problem. The basic problem is caused by the fact that all STAs in the same WLAN are not able to communicate directly with each other. As said before, the MAC layer of 802.11 already ensures that the STA will only begin transmitting after it has sensed the channel to be idle. Now if the two STAs can't

communicate with each other, they are not able to sense each other's transmissions. An example illustration of the hidden node problem is presented in Figure 3.7.

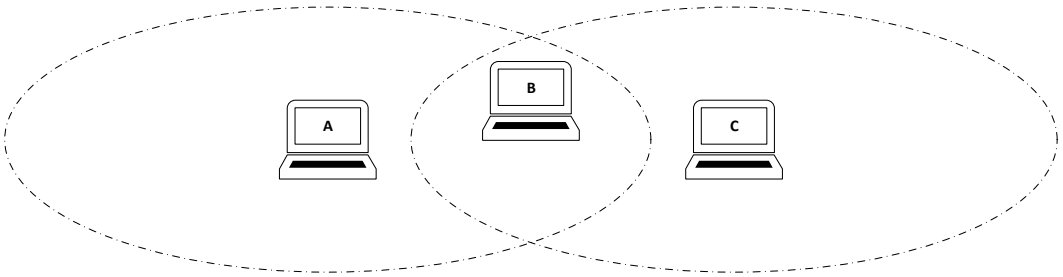

Figure 3.7. *The hidden node problem*

In the example of the Figure 3.7 there are three STAs: A, B and C. The hidden node problem occurs if the STA A has an ongoing transmission to STA B and the STA C would also like to send a frame for STA B. As the STAs A and C are outside of each other's range, STA C can't sense whether the channel is idle or not. Now if the STA C begins the transmission and the channel isn't idle, the ongoing transmission from STA A to STA B would corrupt, as well as the transmission from STA C to STA B.

The hidden node problem is solved by IEEE 802.11 MAC with Request to Send (RTS) and Clear to Send (CTS) protocol. RTS/CTS protocol adds these two additional frames to the MAC layer's frame exchange protocol. The source STA sends a RTS frame to the destination. If the destination senses that the channel is idle, it sends a CTS frame back to the source. This indicates that the channel is really free, and the source can send the actual frame that it wanted to transmit. After the actual frame is received correctly, the destination will send an Acknowledgement (ACK) frame to the source. The CTS frames will be received by every STA that is in the range, and they can delay their own transmissions when the CTS is received. The behavior of the RTS/CTS protocol, and how it solves the hidden node problem, is illustrated in Figure 3.8.

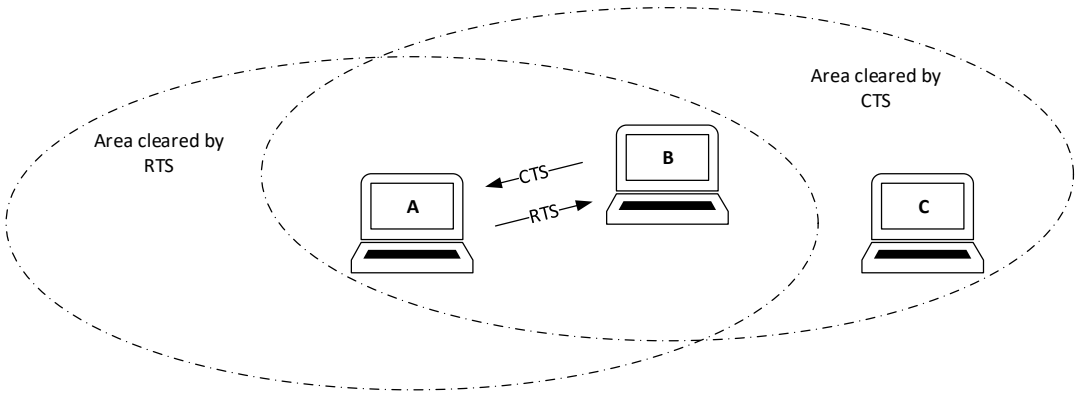

Figure 3.8. *Solving the hidden node problem with RTS/CTS*

In Figure 3.8 there are the same 3 STAs as before, but now the RTS/CTS protocol is in use. The STA in the middle sends a CTS frame to the STA on the left side, after which the STA on the left begins the transmission. The STA on the right side also receives the CTS frame that was sent for the STA on the left and delays it's own transmissions, if there are any.

3.4.2 Evolution of IEEE 802.11 Standards

The first specification for 802.11 was published in 1997 by IEEE's 802.11 working group. This specification only defined 1 Megabits per Second (Mb/s) and 2 Mb/s data rates at 2.4 GHz frequency. At the physical layer it provided three solutions: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR). FHSS and DSSS were operable at 2.4 GHz and IR at 316-353 THz, but commercial IR application was never released. Later 802.11 working group was expanded into two groups, 802.11a and 802.11b. 802.11a worked with 5 GHz and 802.11b with 2.4 GHz. [25]

Both 802.11a and 802.11b were published in 1999. 802.11b introduced Complementary Code Keying (CCK) modulation scheme, which supported up to 11 Mb/s data rates. 802.11a applied OFDM which supported up to 54 Mb/s. Different modulation methods between 802.11a and 802.11b led to interoperability issues with these two standards. 802.11g, which was released in 2003, merged the OFDM modulation from 802.11a to be used in 2.4 GHz.

Table 3.4 shows different 802.11 standards. There can be found many more 802.11 standards and their amendments online, but these are the major standards that have been developed. The maximum data rates shown in this table are maximum data rates per stream. If multiple streams can be used, the data rates will get higher.

Table 3.4. *802.11 standards*

Standard	Frequency	Channel Width	Maximum data rate
Legacy 802.11	2.4 GHz	20 MHz	2 Mbps
802.11b	2.4 GHz	20 MHz	11 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11n	2.4 or 5 GHz	20, 40 MHz	450 Mbps
802.11ac wave1	5 GHz	80 MHz	866.7 Mbps
802.11ac wave2	5 GHz	80, 80+80, 160 MHz	1.73 Gbps

Newer 802.11 standards are using MIMO-OFDM. With MIMO-OFDM the transmitting STA can use more than one spatial streams to gain higher throughput. The first 802.11 standard to support MIMO was 802.11n, that was released in 2009. 802.11n supported a maximum of four spatial streams, which were able to serve a single user.

Transmit Beamforming (TXBF) was introduced by 802.11n in 2009. The TXBF was not a mandatory part of the standard and the decision to implement it was left for the device manufacturers. Many devices are also operating with single antenna, so TBXF can't be used with these devices. Figure 3.9 shows conceptual image of beamforming. The Figure shows two cases, other with no beamforming in use and other with beamforming in use.

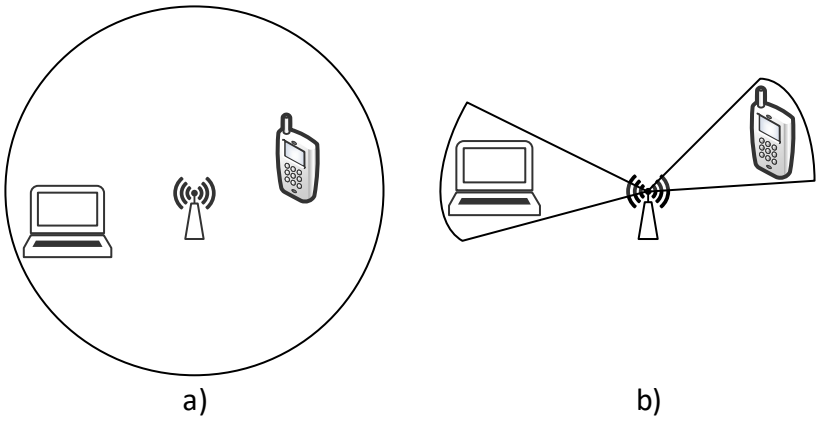

Figure 3.9. *AP and two STAs. Subfigure a) represents an AP without beamforming, b) represents AP that is utilizing beamforming.*

3.4.3 IEEE 802.11ac

IEEE 802.11ac is an amendment to the existing IEEE 802.11 standard and it was published in 2013. 802.11ac was aimed to provide Very High Throughput (VHT) in 5 GHz frequency bands, below 6 GHz. 802.11ac operates only at 5 Ghz frequencies because it uses wider bandwidth than previous 802.11 standards. Frequency bands at 2.4 GHz don't have space for 802.11ac's 80 and 160 MHz channels. There are also many more non-overlapping channels available at 5 Ghz than in 2.4 Ghz [26]. The 802.11ac standard that was published in 2013 is sometimes called 802.11ac Wave 1. IEEE split the development of 802.11ac in two for testing the more advanced features of 802.11ac, the other branch was called 802.11ac Wave 2. The more advanced features of 802.11ac Wave 2 included MU-MIMO, four spatial streams and up to 160 MHz channels with channel bonding. [27]

Compared to previous 802.11n standard, 802.11ac increased the throughput with following mechanisms:

- MU-MIMO
- Larger channel bandwidths of 80 and 160 MHz
- More efficient modulation and coding scheme (MCS) with 256-quadrature amplitude modulation (256-QAM)

MU-MIMO brings the possibility for the AP to transmit different spatial streams for multiple users. This basically means that more than one STA can receive multiple spatial streams simultaneously from the AP. 802.11ac's 256-QAM modulation offers significant boost in the PHY layer throughtput, as one symbol contains 8 bits. 256-QAM can be used with 3/4 and 5/6 coding rates. Coding rate defines the number of redundant bits used in Forward Error Correction (FEC). With coding rate n/m, there are $m - n$ redundant bits per m bits. With 802.11n's highest order modulation, 64-QAM, one symbol contains 6 bits. 802.11n coding rate with 64-QAM is 5/6. While higher modulation methods increase throughput, they will also need better SNR for correct demodulation. Term Modulation and Coding Scheme (MCS) is often used when talking about different coding rates and modulation densities. The used MCS is chosen so that the required transmission reliability and data rate is achieved. 802.11ac's new 256-QAM modulation is used to form two new MCSs, MCS 8 and MCS 9. MCS 8 uses 256-QAM with 3/4 coding rate and MCS 9 uses the same modulation but the coding rate is 5/6. All of the VHT MCSs that are defined in 802.11ac standard, can be seen from Table 3.5.

Table 3.5. *VHT MCSs*

VHT MCS	Modulation	Coding
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

802.11ac was the first 802.11 standard to fully implement TXBF. The TXBF starts with channel sounding. The beamformer sends a Null Data Packet (NDP) for the beamformee, after receiving the NDP, the beamformee analyzes the OFDM training fields associated with each ***TX/RX*** antenna pair. The analyzed results are formed into a feedback matrix, that is based on the amplitude and phase of each signal. After that the beamformee calculates the signal angles and includes them to the feedback matrix. Feedback matrix is then transmitted to the beamformer. The beamformer uses the feedback matrix to create steering matrix, that can be used to create a directional beam from the omnidirectional beam. The channel sounding procedure is presented in Figure 3.10.

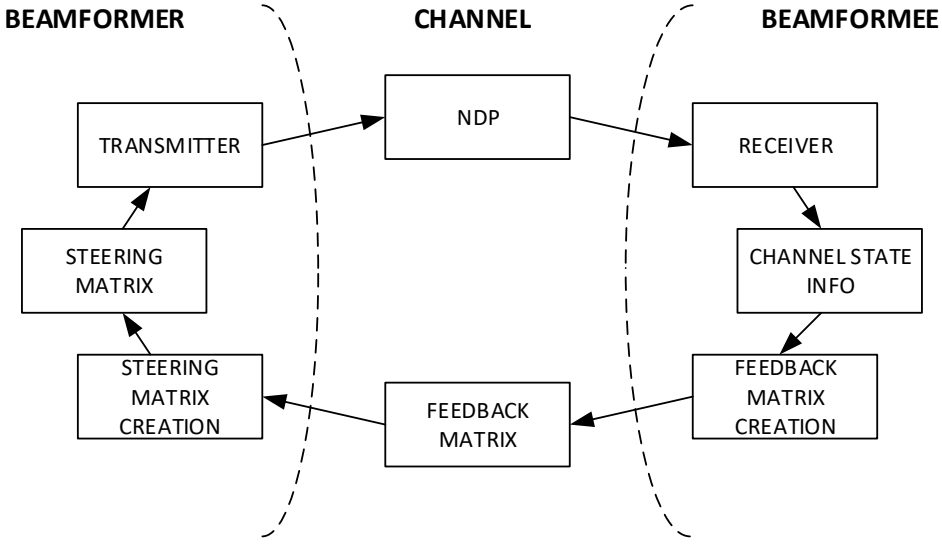

Figure 3.10. *Channel sounding procedure in beamforming*

The 802.11ac standard supports DL MU-MIMO only, because it is assumed that the STAs will consume more data than they produce. Also enabling the MU-MIMO in both UL and DL directions will need much more complex algorithms at the AP and STA.

3.4.4 IEEE 802.11.ax

The next generation WLAN technology is called 802.11ax. IEEE approved 802.11ax in March 2014 and the standard is expected to be complete in 2019. 802.11ax will be a dual-band technology, so it will operate in both 2.4- and 5 GHz frequencies. 802.11ax will bring improvements in per user throughput, operation in user-dense environments and in latencies. The main features of 802.11ax are:

- OFDMA physical layer
- DL- and UL-MU-MIMO
- Trigger frame
- Spatial reuse (SR)
- OFDMA random access
- Target Wake Time (TWT)
- Station-to-Station (S2S) operation

In 802.11ax OFDMA is used in both DL and UL directions.

The subcarrier spacing in 802.1ax has been reduced from previous standards. In 802.11ac, the subcarrier spacing was 312.5 kHz, but in 802.11ax the subcarrier spacing has been reduced to 78.125 kHz. This results in a four times larger amount of subcarriers. [28] Respectively, the OFDMA symbol duration and CP length have been increased by four times. CP is used to eliminate ISI and it can also be used to verify the symbol integrity. With denser subcarriers and longer OFDMA and CP durations, the raw data rate of 802.11ax remains the same as in 802.11ac. However, it increases the data rates by supporting shorter CP lengths in indoor operation, and with 1024-QAM modulation [29].

802.11ax defines four Physical Protocol Data Units (PPDU) to support High Efficiency Single-User (HE SU PPDU), Multi-User (HE MU PPDU), Trigger-Based Multi-User (HE trigger-based PPDU) and Extended Range Transmissions (HE ER SU PPDU). [28] All of these PPDUs are backwards compatible with the previous 802.11 standards.

As discussed in section 3.4.1, devices using legacy 802.11 MAC are only trying to transmit when the channel is sensed to be free. This was the basic princinple of CSMA/CA. In OFDMA multiple users are sharing same frequency band, so 802.11ax

will also need a new MAC layer. With OFDMA, ongoing transmission in the channel does not necessarily obstruct the transmission of other users. The MAC layer of 802.11ax has to be backwards compatible with the legacy 802.11 MAC layer, as backwards compatibility is one of the ground rules of IEEE 802.11 standards.

In 802.11ac, only DL-MU-MIMO was supported, but 802.11ax also implements UL-MU-MIMO. One UL-MU-MIMO RU supports up to eight users and a maximum of four streams per user. 802.11ax introduces new control frame which is called a trigger frame. Trigger frame is used to initiate UL-MU-MIMO transmissions by sending the trigger frame from AP to the STAs. The trigger frame tells each STA information about the UL-MU-MIMO transmission, such as maximum number of spatial streams, RU allocations, allowed transmit power and the exact moment in time when the STAs should start the transmission. All of the STAs that are participating in the UL-MU-MIMO transmission, will transmit their frames at the same time [29]. After the AP has received the frames from the STAs, an ACK frame is sent to all corresponding STAs.

802.11ax introduces Spatial Reuse (SR) operations for achieving better throughput especially in dense environments. Previous 802.11n and 802.11ac standards only allowed transmission when the channel was idle, 802.11ax standard allows transmission on top of ongoing transmission, if one of the SR conditions is met. In 802.11ax STA is able to identify transmissions that are belonging to the same Basic Service Set (BSS). STAs that belong to the same BSS can communicate with each other at PHY-layer. BSS color can be used in early phase to identify whether the transmission belongs to Overlapping Basic Service Set (OBSS). Sensing threshold is used to sense whether the channel is idle or not. With previous 802.11 standards, this sensing threshold was fixed at -82 dBm. In 802.11ax STAs are allowed to use higher sensing threshold for example when ongoing transmission is identified to be from OBSS. Using higher sensing threshold and transmitting on top of OBSS transmissions will improve the performance of the system. [28]

OFDMA random access is a feature that allows AP to assign one or more unallocated RUs for random access. STAs are informed about the random access RUs by AP, and they can use these RUs for UL OFDMA transmissions. OFDMA random access can be useful for STAs that do not require high throughput, or for STAs whose transmissions are infrequent. [28]

802.11ax implements a feature called Target Wake Time (TWT). TWT was already in use in 802.11ah, which was released in 2017. TWT is a Power Saving (PS) feature that allows STAs to sleep between transmissions more frequently. With TWT, STA can request a time to wake up any time in the future from the AP. TWT comes very handy in IoT applications, which will benefit from better power efficiency. In 802.11ax, when STA enters PS mode with TWT procedure, it doesn't have to listen to beacon frames sent by AP. Beacon frame is one of the 802.11 network control

frames that is used to distribute information about the network. TWT can be also used for better UL-OFDMA scheduling, because the AP knows precisely when certain STAs are going to wake up. [30]

Higher order MCSs 10 and 11 are also introduced with 802.11ax. MCS 10 uses 1024-QAM modulation with the coding rate of 3/4. MCS 11 also uses 1024-QAM, but it is paired with 5/6 coding rate. As with 802.11ac, higher order modulation substantially increases theoretical bitrate, but better SNR is required.

4. WI-FI SECURITY ASPECTS

Authentication and confidentiality are the basic measures of wireless security. Authentication means that there needs to be a way to identify that the sender and the receiver are really who they claim to be. Confidentiality stands for securing the transmitted data from eavesdropping. A common attack method that targets network authentication is brute force. In brute force attack, the attacker tries to guess the password or passphrase by simply trying all of the possible combinations. Brute force attack is generally very slow and takes a lot of computing power, but it has and it will stay as a threat with the ever increasing computing power of modern computing systems. Attacks that are targeting confidentiality of the wireless network are trying to decrypt the transmitted data, with or without authentication for the network. The data that the attacker has obtained with eavesdropping must be decrypted in most cases. It is also possible that the attacker wants to decrease the availability of the communication system, which means that the communication system is overloaded with messages or interfered otherwise. This could be done with Wireless Denial of Service (WDoS) attack, jamming or flooding. Popular Wi-Fi attack methods can be seen in Figure 4.1.

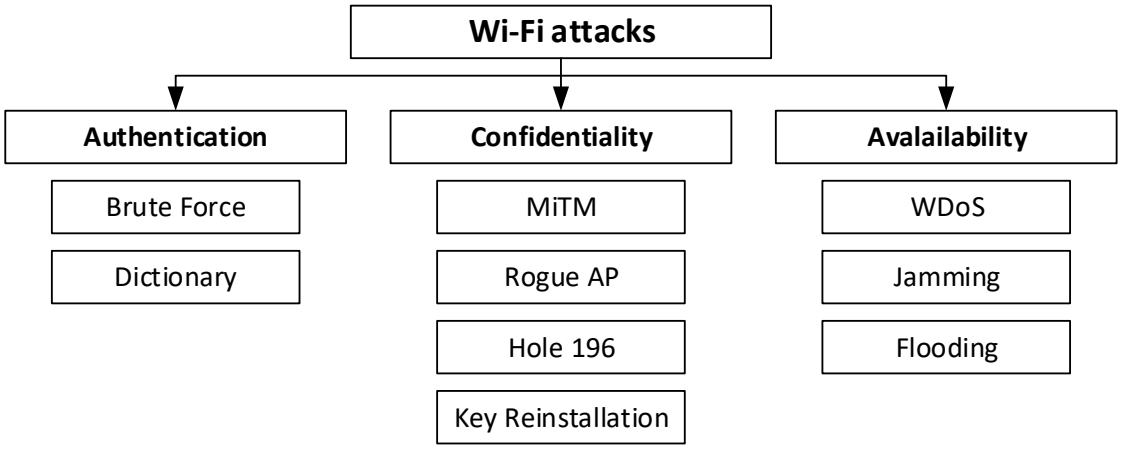

Figure 4.1. *Wi-Fi attack methods, alleviated from [31]*

The wireless security protocols used with 802.11 are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2 which is a successor of WPA. WEP was brought to Wi-Fi as a security measure already in 1999 with 802.11b. Nowadays WEP has been widely replaced with newer security protocols, so this thesis doesn't cover WEP any further.

In this thesis' use scenario, the wireless communication system is located at restricted

area. So it is quite unlikely that an attacker would gain immediate access to the hardware of the communication system. This makes at least one attack method that targets confidentiality, rogue AP, harder to execute. Rogue AP attack method means that someone installs a new AP to the network and does not configure the wireless security correctly. Rogue AP attacks can be executed accidentally by an employee, or by a hacker. Also the effective range of the designed communication system is small, so eavesdropping or other kind of attacks can't be easily executed. In Man in The Middle (MiTM) attack, attacker places a device in the middle of two trusted devices that are communicating with each other. Attacker then seeks to intercept messages or insert malicious packets for the devices. Hole 196 attack targets Wi-Fi's WPA2 security, and it can be used to inject malicious multicast and broadcast packets into the network. Hole 196 attacks requires successful authentication. [32] Key reinstallation attack will be introduced in subsection 4.2.1.

In the following sections protocols that are affecting Wi-Fi security are introduced.

4.1 IEEE 802.1x

IEEE 802.1x specifies means for network administrators to restrict the connection of non-authenticated devices to the IEEE 802 LAN network. The standard applies for both wired and wireless communications, using for example 802.3 (Ethernet) or 802.11 (WLAN) standards. The 802.1x ensures secure connection between two network ports, ports being physical network ports with Ethernet, or logical ports with WLAN devices. The stations that are connected to the 802 LAN network are transmitting and receiving data frames according to 802 LAN MAC. [33] 802.1x operates at layer 2 of the OSI-model. OSI-model can be seen from Table 3.3 in section 3.4.

The 802.1x defines three members of the network authentication process, Authentication Server (AS), authenticator and supplicant. Devices that need to authenticate themselves for connecting to the network, are called supplicants. The supplicant is directly connected to the authenticator, but never to the authentication server [34]. The authenticator relays messages between the supplicant and the authentication server, or any other device after having authenticated successfully. 802.1x defines logical ports named uncontrolled and controlled port [35]. Before the supplicant has been successfully authenticated, all traffic is passed via uncontrolled port. Correspondingly, after successful authentication traffic is passed through controlled port. The authentication server is sometimes called RADIUS-server (Remote Authentication Dial In User Service). The name RADIUS server comes from the protocol that is used in the communication between the authenticator and the authentication server. The protocol used between the authenticator and the supplicant is called EAPOL (Extensible Authentication Protocol Over Lan). Figure 4.2 shows the basic network members and protocols defined in 802.1x.

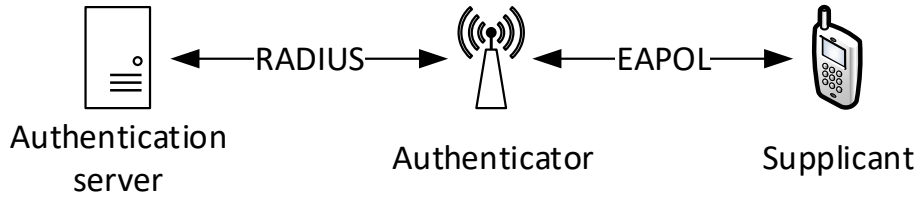

Figure 4.2. *802.1x network members and authentication protocols*

The authentication server holds the information about each supplicant that can be authenticated. Because every supplicant has personal user credentials, network administrator is able to deny access for single supplicant and other credentials are still in use. 802.1x however increases complexity for setting up the network, because every supplicant has to be correctly configured. Incorrectly configured devices are causing security issues, especially in wireless networks utilizing 802.1x [36].

4.2 IEEE 802.11i

In 2004 the IEEE released a standard named 802.11i, which was developed to enhance the security weaknesses of WEP and WPA. WPA was previously released in 2002 and it was based on a draft 3 version of 802.11i standard. WPA was released as a intermediate solution for the security flaws in WEP. After 802.11i was fully released, Wi-Fi Alliance released WPA2, that is based on and fully interoperable with 802.11i. [37] Wi-Fi certified devices have implemented Wi-Fi Protected Access II (WPA2) technique since 2006. 802.11i introduced a new protocol called four-way handshake that is used in changing cryptographic keys between the network members. The four-way handshake protocol is designed so that the keys are never disclosed. This means that the actual passphrase, or Pairwise Master Key (PMK) in this context, is never transferred during the authorization process. Figure 4.3 presents the four-way handshake protocol.

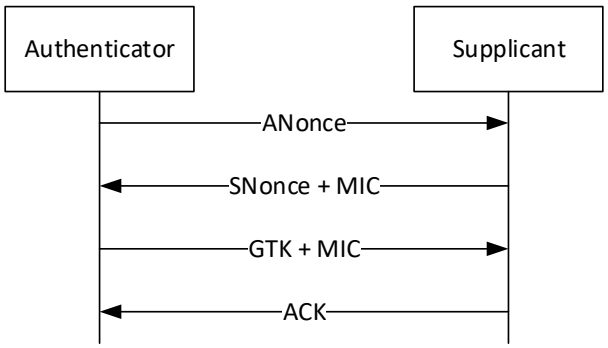

Figure 4.3. *The four-way handshake protocol of 802.11i*

When the four-way handshake begins, the authenticator sends Authenticator Nonce (ANonce) message for the supplicant. ANonce is a pseudorandom sequence generated

by the authenticator, this message also includes a Key Reply Counter (KRC) field. The supplicant then generates the Pairwise Transient Key (PTK) from ANonce, Supplicant Nonce (SNonce) and the Pairwise Master Key (PMK) that is known by both authenticator and supplicant. After the PTK has been generated, supplicant sends SNonce, Message Integrity Check (MIC) and KRC with the same value as in the first handshake message to the authenticator. Next the authenticator also generates the PTK with the ANonce, PMK and the received SNonce. Authenticator then generates Group Temporary Key (GTK). After supplicant has received the GTK and validated the message, it will send an acknowledgement (ACK) message for the authenticator. After the authenticator has received the ACK message, the authentication procedure is complete. [35]

After successful authentication, PTK is used for encrypting and decrypting messages between the supplicant and authenticator. The supplicant uses GTK for decoding broadcast messages, which are meant for every authenticated supplicant. Every message in the four-way handshake is transmitted using the EAPOL protocol defined in IEEE 802.1x [38]. After the authentication, the authenticator opens IEEE 802.1x controlled port for the supplicant.

4.2.1 WPA2

WPA2 enhances its successor WPA by introducing Advanced Encryption Standard (AES) based encryption algorithm CCMP. CCMP comes from CMC-MAC Protocol, which is an abbreviation for Counter Mode Cipher Block Chaining Message Authentication Code Protocol. CCMP provides better security than previously used Temporary Key Integrity Protocol (TKIP). WPA2 contains two operation modes: WPA2-Personal and WPA2-Enterprise. WPA2-Personal uses Pre Shared Key (PSK) for authentication. The authentication process is executed using the four-way handshake introduced in IEEE 802.11i. By using WPA-2 Personal the network does not need the authentication server, as every user uses the same PSK for authentication. WPA2-Personal is generally suitable for home use, or for small offices. The drawback of WPA2-Personal is that if the PSK is compromised and it must be changed, the new PSK has to be manually reconfigured for every user. WPA2-Enterprise uses per user credentials and the authentication server defined in 802.1x.

For many years WPA2 was thought and also proved as secure, when configured properly [39]. However, in 2016 two researchers from the University of Leuven discovered weaknesses in the four-way handshake protocol of 802.11i. They found out that the four-way handshake could be cracked with a special Key Reinstallation Attack, which the authors have named as KRACK. In KRACK attack, the authenticator is cloned and the fake authenticator cloned by the attacker is set to intercept messages between the authenticator and the supplicant. Basically the fake authenticator works just as in MiTM attacks. KRACK targets to intercept the 4th. message from getting

to the authenticator. When the authenticator does not receive the 4th. message, that is the ACK message, it retransmits the 3rd. message. As per the 802.11i standard, the supplicant installs the PTK after receiving the 3rd. message. Now if the authenticator retransmits the 3rd. message, it causes the supplicant to reinstall the PTK, which resets the nonce used in encoding the data. In short, this allows the attacker to replay, decrypt and/or forge messages. [38, 40]

Quickly after the KRACK attack was brought into general knowledge, the device vendors began to provide security updates to repair the four-way-handshake protocol. Nowadays the network can be protected from the KRACK attack, if it is made sure that the devices' softwares are up-to-date and the vendor has fixed the issue.

4.3 WPA3

The Wi-Fi Alliance announced the arrival of Wi-Fi Protected Access 3 (WPA3) in the beginning of 2018. The upcoming devices that are based on IEEE 802.11ax, will support WPA3 [41]. WPA3 brings a new PSK authentication and key generation procedure that is based on Simultaneous Authentication of Equals (SAE). SAE provides a secure generation of cryptographically strong encryption keys. [42] At the time of writing this thesis, the available documentation about WPA3 is very limited and therefore the topic can't be processed thoroughly.

4.4 Additional Security Measures

Previously mentioned security protocols are used to authenticate users to the network and secure the transmitted data between two users. In addition to these protocols, the data transmission can be further enhanced with a number of ways. In the following subsections, implementations of Virtual Private Network (VPN) and Secure Shell (SSH) are considered as possible ways to further enhance the security. VPN can be used to create secure, encrypted end-to-end tunnels between two network locations. VPN is often used by companies to provide access for the employees, or various stakeholders to access companies' network resources. VPN offers security and cost savings, because more secure networks can be implemented with using the existing Internet infrastructure. SSH can also be used to create encrypted, secure tunnels between two network locations. With VPN generally all network traffic is sent through the VPN tunnel. With SSH, every application has to be specifically configured for using the SSH tunnel.

For the implementation of VPN, there are plenty of options. VPN has increased its popularity and the number of commercial VPN services for both businesses and private personnel is increasing rapidly. OpenVPN was chosen for implementing VPN in this thesis because of its high level of documentation and the fact that its open-source and free to use. For the SSH tunnel OpenSSH is used, primarily for the same reasons as OpenVPN.

It must be noted that every additional security layer adds complexity, which increases the deployment time as well as restricts the throughput of data.

4.4.1 OpenVPN

OpenVPN is an open-source application originally written by James Yonan. The initial release of OpenVPN occurred in 2001. OpenVPN communicates through TCP/IP stack and TUN/TAP interfaces. The TUN and TAP interfaces are software interfaces (i.e not physical interfaces), and they are referring to network tunnel and network tap. TUN operates at layer 3 (network layer) with IP packets and thus it is capable for creating end-to-end tunnels between two OpenVPN processes. TAP can be used to monitor Ethernet frames at layer 2 (data link layer), TAP mode is also called bridging mode. [43] The OSI model and the different network layers were introduced in Table 3.3 at chapter 3.4. Figure 4.4 represents a conceptual image of the message flow when using OpenVPN. Abbreviation NI is used from the physical Network Interface. Figure shows how the TUN interface is used to monitor messages from an user application. TUN interface routes the message to OpenVPN process, which encrypts and repackages the message. Next the message is sent to the recipient via Internet. The recipient processes the message in reversed order. [43]

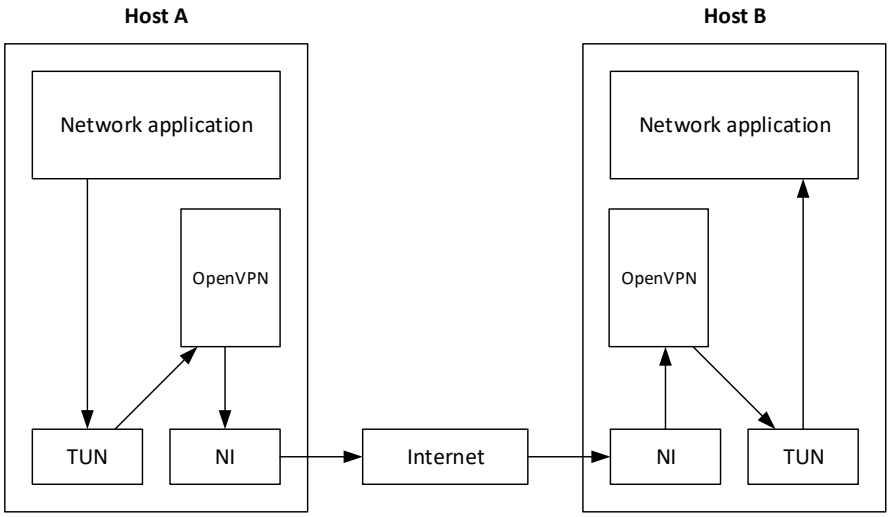

Figure 4.4. *OpenVPN*

OpenVPN provides two security models: static key and Transport Layer Security (TLS). With static key model, two peers are using pre-shared keys for authentication and encryption. By default, there are two separate keys for both sides, other for authentication and another for encrypting and decrypting messages. The authentication keys are called HMACs (Hash-based Message Authentication Code). The pre-shared keys are identical for both sides. It is also possible and more secure to generate four keys for both sides. With four keys, there are keys for sending HMAC, receiving HMAC, encrypting a message and decrypting a message. Regardless of

the number of the used keys, when using static keys, the keys have to be securely distributed for the both sides. Using pre-shared keys is generally thought as not secure. However, the security of pre-shared keys can be increased by keeping the lifetime of the keys short and generating new keys often. [44] Authentication and encryption with static keys, identical keys on both sides can also be called symmetric encryption.

The second security model is TLS. TLS is Secure Socket Layer's (SSL) successor and it has become a de facto standard for authentication and encryption in Internet. [43, 45] TLS is used by almost everyone and everyday in modern web browsing. During authentication with TLS, both sides are exchanging certificates with each other. Certificates have to be signed by mutually trusted Certificate Authority (CA). TLS is using asymmetric encryption, which in this case means, that both sides have two encryption keys: public and private. The public key is shared with the other side, and the messages are encrypted using the recipient's public key. The keys are generated in a way that only the private key of the recipient is able to decrypt the message. [43, 44]

4.4.2 OpenSSH

SSH is a protocol originally developed by Tatu Ylönen in 1995. SSH provides means for securely logging into remote computer over the network. SSH initiates a remote terminal shell, that can be used for example to run commands on the remote computer. OpenSSH is a software implementation of SSH, and it was initially released in 1999 [46]. SSH is using client-server architecture. For creating the SSH tunnel and logging in to the remote computer, the remote computer has to have a SSH server running. [47] Figure 4.5 presents the message flow between the OpenSSH client and server. The message encryption is done by OpenSSH, and it is completely transparent for the user.

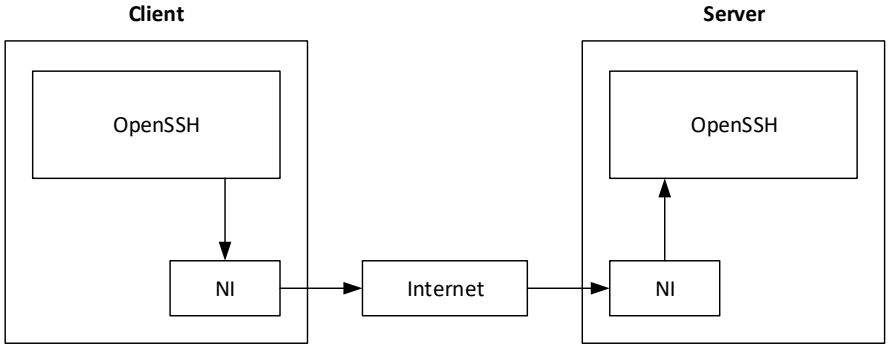

Figure 4.5. *OpenSSH*

When connecting with SSH, the server and client need to have their cryptographic keys generated. SSH uses asymmetric encryption, so both client and server will

have two keys, private and public. By default, OpenSSH (version 7.8) generates the cryptographic keys by using Rivest–Shamir–Adleman (RSA) cryptosystem. Other options are: Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA) and Edwards-curve Digital Signature Algorithm (EdDSA). The security of different key generation algorithms is not evaluated in this thesis. [48, 47]

5. TRIAL SYSTEM AND MEASUREMENTS

Chosen technologies for the wireless mission data transfer system will be examined by estimating the received signal strength and measuring the data throughput of the system. As stated in chapter 2, the final system will be deployed in a location where the communication range of the system is roughly 30 meters. The attenuation of the wireless signal will finally affect the data throughput of the wireless system. For estimating the data throughput before the actual measurements in this thesis, the signal attenuation is evaluated. For evaluating the signal attenuation, different channel models are introduced.

5.1 Channel Models and Link Budget Analysis

The equipment used in testing the wireless mission data system, are supporting maximum bandwidth of 80 MHz. 802.11ac also operates only at 5-6 GHz frequencies. Due to these facts, only WLAN channels located at 5-6 GHz and with 80 MHz channel width for gaining maximum throughput are used.

The IEEE TGax task group has defined channel models based on ITU-R channel models [49]. In this thesis, channel model for outdoor with LOS propagation is considered as the closest channel model for the final deployment environment. The designed wireless system will only be operable when both the AP and STA are stationary. This means that the effects caused by relative movement between the AP and STA, like Doppler spread can be ignored [50]. The channel models defined IEEE TGax are created for 802.11ax, but they should be also applicable for 802.11ac. The same channel model can also be found from reference [51], and it is named as LOS Urban Micro (UMi) channel model. The TGax and 3rd. Generation Partnership Project (3GPP) have defined an outdoor Path Loss (PL) model for a LOS link as:

$$PL_{LOS}(d) = 22.0\log_{10}(d) + 28 + 20\log_{10}(f_c), \quad if\, 10m \leqslant d < d_{BP} \tag{5.1}$$

$$PL_{LOS}(d) = 40\log_{10}(d) + 7.8 - 18\log_{10}(h_{AP} - 1.0) - 18\log_{10}(h_{STA} - 1.0) + 20\log_{10}(f_c), \quad if\, d_{BP} \leqslant d < 5000m \tag{5.2}$$

where d is the distance between AP and STA, h_{AP} and h_{STA} are the antenna heights of AP and STA, f_c is the center carrier frequency in gigahertz (GHz) and d_{BP} is

the Breakpoint (BP) distance. BP is a term used for the distance after which the propagated signal starts to attenuate drastically. BP distance is affected by frequency, antenna heights and objects that are in close proximity of the LOS signal path [52].

The BP distance can be calculated as:

$$d_{BP} = \frac{4(h_{AP} - 1.0)(h_{STA} - 1.0)f_c \times 10^9}{c} \tag{5.3}$$

where $c = 3 \times 10^8$ (m/s), which denotes the speed of light.

It can be noticed that by substituting values h_{AP} and h_{STA} from Figure 2.2 to the equation 5.3, the breakpoint distance becomes zero. Breakpoint distance becomes zero, because the effective antenna heights are calculated from the actual antenna heights. For this channel model, the effective environment height of 1 m is substracted from the actual antenna height and this results in zero value, if either the h_{STA} or h_{AP} is 1 m. Giving that at the moment, the h_{STA} antenna height of 1 m was just a fair assumption, it might be beneficial to find out the BP distance and the PL with this channel model using suitable antenna heights. Let's assume that the used antenna heights are 10 m for the h_{AP} and 2 m for the h_{STA}. Substituting these values and a f_c of 5.5 GHz in to the equation 5.3, the d_{BP} becomes 660 m. This BP distance implicates that within the ranges of the communication system in this thesis, the BP distance is not exceeded under any circumstances. Because of this, the PL can be calculated with equation 5.1. The resulted PL values are shown in Table 5.1. The PL model was defined for distances between 10 m and the BP, so distances under 10 m are not shown.

Table 5.1. *Path loss at different distances and frequencies using TGax's outdoor LOS channel model*

PL (dB)	10m	15m	20m	25m	30m
5.530 Ghz	64.9	68.7	71.5	73.6	75.4
5.610 Ghz	65.0	68.9	71.6	73.7	75.5

The simplest channel path loss model is the Free Space Loss (FSL). FSL defines the signal loss in decibels at the given distance when there are no obstacles. The FSL is often used as a basic reference for the path loss. In [53] the FSL is given as:

$$FSL = 20\log_{10}(d) + 20\log_{10}(f_c) + 32.4 \tag{5.4}$$

where d is the distance between AP and STA in kilometers (km) and f_c is the center carrier frequency in megahertz (MHz). It can be seen that the antenna heights will not affect the FSL.

Table 5.2 shows FSL for every continuous WLAN channel that is allowed for outdoor use in Finland and located at 5-6 GHz for distances between 1m and 30m [11]. Even that the differences in the FSL between these frequencies are not significant, it can be seen that the FSL gets higher as the frequency gets higher.

***Table 5.2**. Free space loss at different distances and frequencies using FSL channel model*

FSL (dB)	1m	5m	10m	15m	20m	25m	30m
5.530 Ghz	47.3	61.3	67.3	70.1	73.3	75.3	76.8
5.610 Ghz	47.4	61.4	67.4	70.1	73.4	75.4	77.0

By comparing values in Tables 5.1 and 5.2, it can be seen that the PL values with FSL are higher than the ones with TGax's channel model. Because the TGax's channel model is much more specific and it is created almost explicitly for the given situation, PL values calculated with TGax's channel model are used.

Based on PL that was calculated with different channel models, link budget of the Wi-Fi communication link can be calculated. Link budget calculations are basic calculations used in estimating the range and the quality of wireless communications and it involves summing all the gains and losses between the transmitter and the receiver. Usually link budget calculations are used to find out the received signal strength. With knowledge of the receiver's sensitivity, the transmitting power can be adjusted to achieve suitable signal strength at the receiver. In this thesis, appropriate formula for logarithmic link budget calculations could be:

$$P_{RX} = P_{TX} - L_{TX} + G_{TX} - L_{PL} + G_{RX} - L_{RX} \tag{5.5}$$

where P_{RX} is the signal strength at receiver, P_{TX} is the TX power, L_{TX} is a loss that constitutes of cable and connector losses at the transmitter, G_{TX} is the antenna gain at transmitter, L_{PL} is the PL for the wireless channel, G_{RX} is the receiver's antenna gain and L_{RX} are the cable and connector losses at the receiver.

The transmitting power of the used Wi-Fi transceiver is 15 dBm, when 80 MHz channel and 3 spatial streams are used [54]. The antennas that are in use at the transmitter offer 7 dBi antenna gain [55]. At the receiver, the antenna gains are not known but a 5 dBi gain would be a fair assumption. The cable and connector losses could not be measured for this thesis, but the length of the cables on both transmitter and receiver is less than 30cm. For the cable and connector losses, an assumption of 3dB loss is made for both transmitter and receiver. With these values and a PL calculated with TGax's channel model and, the received signal strength with 5.530 GHz center frequency at 30 m distance becomes -54.4 dBm.

It would be useful to compare the calculated received signal strength to the receiver sensitivity reported by device manufacturer. However, the manufacturers of the used

devices are not informing these values. For this reason the received signal strength is compared to the sensitivity values that are specified at IEEE 802.11ac standard. The 802.11ac standard specifies minimum receiver sensitivities for different MCS rates. The values are telling the minimum level for the receiver's input signal that has to be demodulated with a maximum of 10% Packet Error Rate (PER). Table 5.3 shows the minimum 802.11ac receiver sensitivities that have been specified in the IEEE 802.11ac standard. [8]

***Table 5.3**. IEEE 802.11ac minimum receiver sensitivities for 80 MHz channel*

MCS	Minimum Sensitivity (dBm)
0	-76
1	–73
2	–71
3	–68
4	–64
5	–60
6	–59
7	–58
8	–53
9	–51

From Table 5.3 can be seen that with received signal level of -54.4 dBm that was calculated earlier, the standard specifies that the maximum achievable MCS would be MCS 7. It must be noted that the standard really specifies the minimum values, and the devices' sensitivities can be better (i.e lower) than the values in Table 5.3. Declarations for MCS rates in 802.11ac can be seen from Table 3.5. 80 MHz channel bandwidth, short GI length, three spatial streams and MCS 7 would result in 975.0 Mb/s PHY throughput. The data rate at PHY layer often differs much from the actual achieved throughput. This partly results from the MAC layer's efficiency, which is usually not higher than 70 %. With 975.0 Mb/s PHY data rate, the achieved throughput could be up to 682.5 Mb/s. [27]

5.2 Test Equipment

The test equipment consist of two PCs and a wireless AP. The first PC is just an ordinary laptop and it is connected to the AP via Ethernet. From now on, this laptop is just referred as PC. The second PC is the DTD, which is used for data recording in the Grob aircraft, this PC is from now on referred as DTD. The wireless connectivity for the DTD is achieved with a wireless network adapter. The wireless network adapter chosen for the task is SparkLAN WPEQ-353ACNI. The wireless adapter is connected to the DTD with Mini Peripheral Component Interconnect Express (mPCIe). The SparkLAN WPEQ-353ACNI was chosen for its support for IEEE 802.11ac with the maximum of three spatial streams. The maximum achievable throughput for this wireless adapter is (in theory) 1.3 Gb/s at PHY layer. The

Sparklan WPEQ-353ACNI is configured as a STA, so the DTD works as a STA during the tests. The SparkLAN WPEQ-353ACNI is based on Qualcomm Atheros QCA9890-BR4B chipset [54]. The hardware specifications of PC and DTD are shown in Table 5.4.

Table 5.4. *Specifications of DTD and PC*

	DTD	**PC**
CPU	Intel Celeron J1900	Intel Xeon E3-150M v5
RAM	2 GB	32 GB
OS	Ubuntu 18.04 LTS	Ubuntu 18.04 LTS

The wireless AP chosen for the tests is ASUS RT-AC68U, which also supports IEEE 802.11ac and a maximum of three spatial streams. The Asus RT-AC68U uses Broadcom's BCM4360 Wi-Fi transceiver. The ASUS RT-AC68U is configured to wireless AP mode, so it also provides the IP routing services for the clients. The PC and DTD are configured to the same subnet. The wireless access point is set to use only 802.11ac standard, and the 2.4 GHz radio is turned off. The wireless security is configured to use WPA2-PSK (WPA2-Personal) that uses CCMP encryption. WPA2-Personal is used instead of WPA2-Enterprise for easier setup. The encryption algorithms used by WPA2-Personal and WPA2-Enterprise are the same, the only difference is the used authentication method. From now on, WPA2-Personal with CCMP encryption is referred as WPA2. Conceptual image of the test system is shown in Figure 5.1

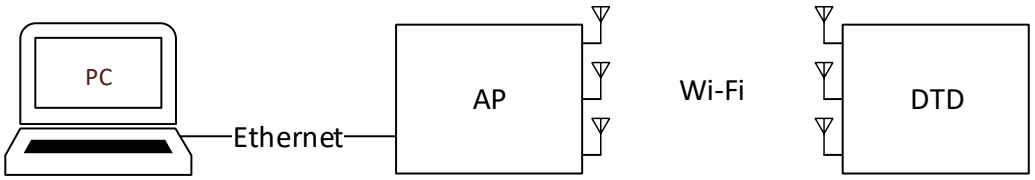

Figure 5.1. *The test system*

5.2.1 Configuration of OpenSSH and OpenVPN

Following paragraphs will introduce the used configurations for the OpenSSH and OpenVPN servers and clients. These configurations were used in the tests. It is also introduced how the encryption keys are distributed from the server to the client.

OpenSSH server is running on the PC, and the DTD is configured as a OpenSSH client. Server and client are configured to use public key authentication. The key-pair was created on the OpenSSH server using command *ssh-keygen*. This command is used to create the key-pair that includes the private and public key. By default the used OpenSSH version (OpenSSH 7.6) generates a 2048-bit RSA keys, which are used in tests. The public key is appended to a file called *authorized_keys* with the following command

```
$ cat id_rsa.pub >> ~/.ssh/authorized_keys
```

The *authorized_keys* file is used to store public keys for every client that is allowed to initiate SSH connection. The private key is then transferred to the DTD with USB memory stick. Usually with SSH the key exchange is executed another way around. Meaning that the client generates the key pair, and the public key is then transferred to the server, usually with SSH. In this scenario, the USB memory stick can be thought as a secure transfer media and it can be used to transfer the private key for the client. The location and the name of the private key file on the client can be configured case-by-case. After the public key has been added to the server, and the corresponding private key has been transferred to the server, client is able to connect to the server with SSH without password authentication. The used OpenSSH server configuration is:

```
PubKeyAuthentication yes
PasswordAuthentication no
AuthorizedKeysFile .ssh/authorized_keys
```

Server configuration tells OpenSSH server to enable public key authentication, disable password authentication and tells the location of the file that has the authorized hosts' public keys. Used configuration for the OpenSSH client is:

```
Host *
PubkeyAuthentication yes
PasswordAuthentication no
IdentityFile ~/.ssh/id_rsa
```

Client configuration tells OpenSSH client to apply the configurations for every host, enable public key authentication, disable password authentication and specifies the location of the client's private key.

With OpenVPN, the server is again running on the PC, and the DTD is configured as a OpenVPN client. In these measurements, the OpenVPN server is configured simply to create point-to-point tunnel between the server and client and server. Virtual TUN interfaces are used for creating the tunnel. For authentication, static keys are used. This means that one key is generated in the server and then transferred to the DTD same way as with SSH. The same static key is used for encrypting and decrypting messages in both ends. The static key is generated with command

```
$ openvpn --genkey --secret static.key
```

Here the *static.key* is the name of the generated key. The used configuration for the OpenVPN server is:

```
dev tun
ifconfig 10.8.0.5 10.8.0.6
secret static.key
```

The server configuration tells OpenVPN to create a TUN interface and assign the IP addresses for the server and the client. Secret static.key tells the name and the location of the encryption key. The used configuration for OpenVPN client is:

```
remote 192.168.1.5
dev tun
ifconfig 10.8.0.6 10.8.0.5
secret.static key
```

Client configuration specifies the IP address of the OpenVPN server, creates the TUN interface, assigns the IP addresses and tells the name and the location of the encryption key.

5.3 Test Environment

Throughput tests will be executed outside and in open space. Different communication distances will be tested by altering the distance between the AP and the DTD. The communication distances to test between the AP and DTD were chosen as 1 m, 15 m and 30 m. The 1 m distance was chosen to find out the maximum achievable throughput of the system. The 30 m distance is very close to the range of the wireless mission data transfer system when it is finally implemented, so this distance is the most interesting one. 15 m distance was chosen from between of these distances. The biggest interest in this thesis is the uplink performance of the wireless system. So the throughput from the DTD to the PC is the most intriguing part and thus mainly tested.

The antenna heights in tests differ from the antenna heights that were presented in Figure 2.2. To make measurements easier to conduct, the AP and DTD are placed on a level surface and the antenna heights for both are 1 m. Conceptual image of the test environment is shown in Figure 5.2.

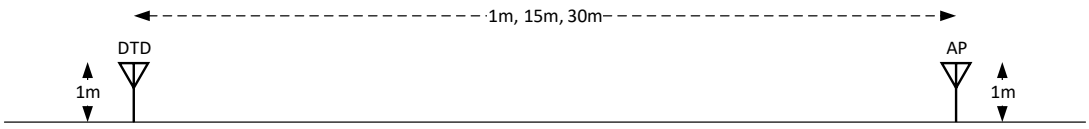

Figure 5.2. *Conceptual image of the test environment*

5.4 Test Procedures

Throughput will be measured with iPerf3. IPerf3 is an open source command line tool that can be used to test network throughput using UPD, TCP or Stream Transmit Protocol (SCTP). IPerf3 is used to log the achieved throughput once per second. Every measurement lasts for 60 seconds. In this thesis, TCP is mainly used for the throughput tests. UDP tests are performed only with WPA2, without OpenSSH and OpenVPN. The basic difference between TCP and UDP is that TCP is connection based protocol and UDP is connectionless. TCP provides packet error detection, and errors can be corrected with retransmissions. UDP does not quarantee that the recipient receives packets in right order and without errors. For this reason UDP would not be a probable protocol choice in the final system.

The throughput of the test system will be measured with WPA2, WPA2 with OpenSSH tunnel and WPA2 with OpenVPN tunnel. Measurements will be executed for the three communication distances. The quality of the wireless link can be monitored with a linux command line tool called Wavemon. Wavemon gives information about the received signal strength and the RX rate at DTD, which is constituted of the used MCS, bandwidth, GI length and the number of spatial streams. Unfortunately the used device driver for the DTD's wireless adapter, Ath10k, does not share information about the used TX rate. The used Ath10k driver version is 10.2.4-1.000037. The transmitter and receiver are not *necessarily* using same RX and TX rates. Even that they are not, it is interesting to monitor the RX rate of the DTD if it would give some clue about the used TX rate. TX and RX rates can't be set manually, the rates are modified automatically by DTD and AP based on the channel conditions. Also the AP does not share information about the received signal strength, so it is only possible to monitor the received signal strength at the DTD.

Prior to official tests, it was found out that the TCP congestion control is causing troubles for the throughput tests. TCP congestion control is trying to maximize the throughput of the network by reducing the TCP packet size if there are errors or the network is congested. Correspondingly the TCP packet size should grow if there are no errors. [56]. The problems were related to too small TCP congestion window, which caused low throughput between the DTD and PC. The TCP congestion window is adjusted by the sender, and the problems occurred when sending packets from DTD to PC. Several congestion control algorithms were tested, and the best results were obtained with a congestion control algorithm called Reno. For this reason, Reno algorithm is used for TCP congestion control in DTD.

With iPerf3, by default the data flows from client to the server and the main interest is in the uplink throughput from DTD to PC. For this reason the iPerf3 server process is always started on the PC and the client on the DTD. The iPerf3 server is started with command:

```
$ iperf3 -s
```

5.4.1 WPA2

With WPA2 only, best results were obtained by starting the iPerf3 client with command:

```
$ iperf3 -c 192.168.1.5 -P 128 -w 200k -t 30
```

Here the *-c* stands for client operation mode, after which the server's IP address is given. *-P 128* means that 128 TCP connections is created in parallel and option *-w 200k* tries to set the transmit and receive buffer sizes. *-t 30* tells that the test lasts for 30 seconds.

With WPA2 only it is also possible to measure UDP throughput with iPerf3. For UDP measurements, the iPerf3 client was started with command:

```
$ iperf3 -c 192.168.1.5 -P 5 -w 200k -u -b 1300M -t 30
```

Here the parameter *-u* tells iPerf3 to used UDP protocol and *-b 1300M* sets the target throughput to 1300 Mb/s, which is the maximum achievable throughput of the system.

5.4.2 WPA2 and OpenSSH

To test iPerf3 with WPA and OpenSSH, an OpenSSH tunnel has to be created for the task. OpenSSH allows to forward local port to remote host's port with command:

```
$ ssh -L 5201:192.168.1.5:5201 mikko@192.168.1.5
```

This command uses OpenSSH to connect local port number 5201 to remote host's port number 5201. The port 5201 was chosen because it is the default port for iPerf3 server. For authentication and encryption OpenSSH uses the previously generated and distributed keys. After creating the OpenSSH tunnel, the iPerf3 server has to be started on the PC with the same command as before. The command for starting the iPerf3 client and using the OpenSSH tunnel is:

```
$ iperf3 -c localhost
```

IPerf3 now uses localhost's port 5201, that is forwarded to PC's port 5201 via OpenSSH. Other command line parameters of iPerf3 didn't affect the throughput positively. UDP traffic doesn't work via OpenSSH tunnel with this configuration, so it is not tested.

5.4.3 WPA2 and OpenVPN

For WPA2 with OpenVPN tunnel tests, the OpenVPN server and client has to be set up. This can be done by command:

```
$ openvpn <configuration file>
```

The configuration file for OpenVPN is given here, and the same command works for both server and client. After starting the OpenVPN server and client, the iPerf3 server can be started on the PC. The iPerf3 client on the DTD is started with command:

```
$ iperf3 -c 10.8.0.5
```

Now the iPerf3 client is connected to the server on 10.8.0.5:5201. Using UDP instead of TCP, parallel connections or altering the buffer sizes did not affect the throughput with WPA2 and OpenVPN.

5.5 Results

Results are presented in subsections, every tested communication distance has its own subsection. Tests that were introduced in the previous section are performed for every communication distance.

5.5.1 1 Meter Distance

Figure 5.3 presents the achieved throughput with 1m distance between the AP and DTD. In these tests, the DTD reported that RX rate of 866.7 Mb/s was used. This RX rate comprises of MCS 9, 80 MHz bandwidth, short GI and two spatial streams.

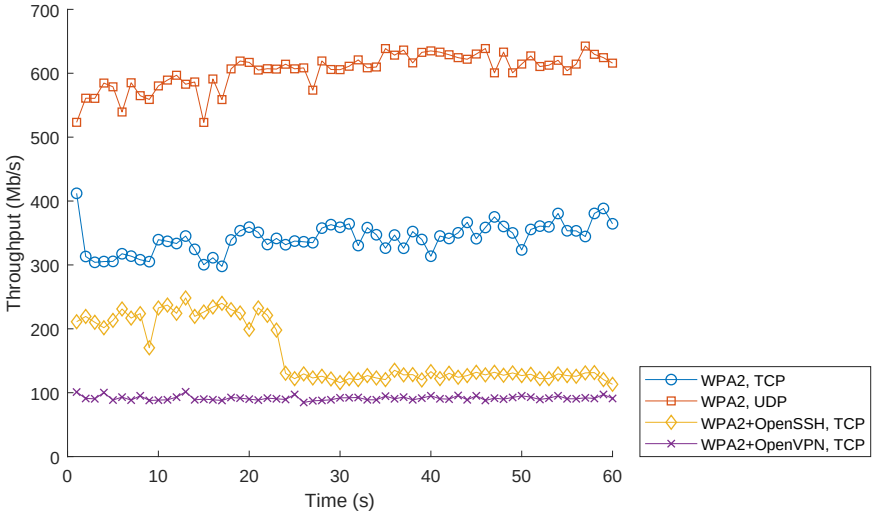

Figure 5.3. *Throughput at 1 m distance*

The results are quite consistent, but there can be seen a drop in the throughput with WPA2 + OpenSSH. TCP traffic with WPA2 + OpenVPN tunnel resulted in steady 100 Mb/s throughput.

5.5.2 15 Meter Distance

Figure 5.4 presents the achieved throughput with 15 m distance between the AP and DTD. In these tests, the DTD reported RX rate of 585.0 Mb/s, which consists of MCS 4, 80 MHz bandwidth, short GI and three spatial streams.

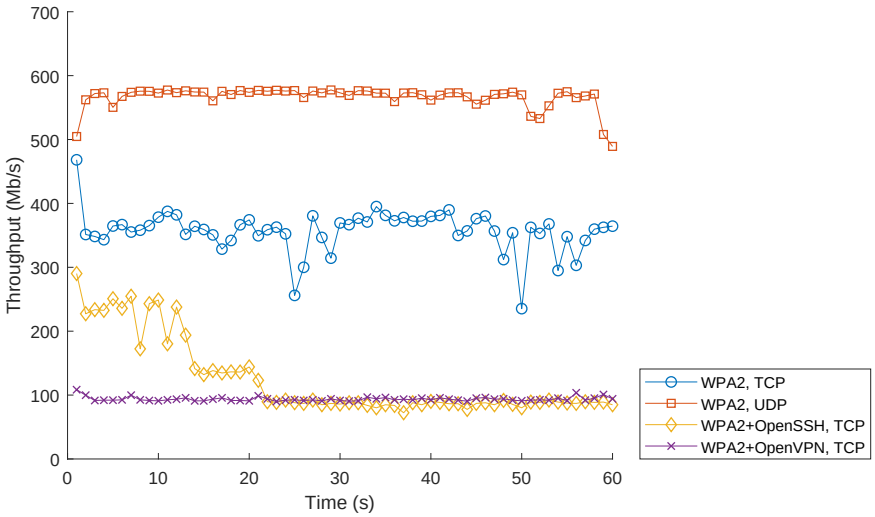

Figure 5.4. *Throughput at 15 m distance*

Results from 15 m distance are not greatly different than the results from 1 m

distance. TCP throughput with WPA2 was actually higher than at 1 m distance, but there are bigger falls and the throughput isn't as steady as at 1 m. The WPA2 + OpenSSH throughput started to drop sooner than in 1 m distance and it actually dropped below the WPA2 + OpenVPN throughput.

5.5.3 30 Meter Distance

Figure 5.5 presents the achieved throughput with 30 m distance between the AP and DTD. In these tests, the DTD reported that RX rate of 585.0 Mb/s was used. This RX rate is the same as in tests at 15 m distance.

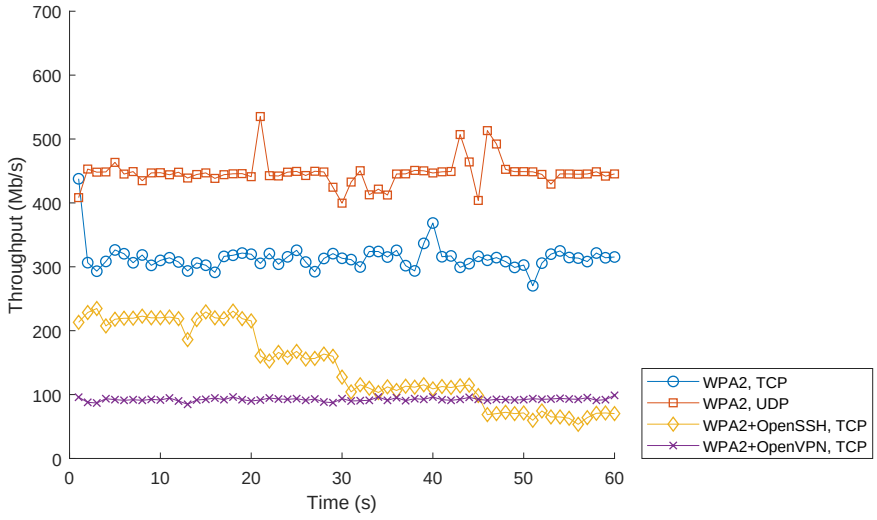

Figure 5.5. *Throughput at 30 m distance*

The results in Figure 5.5 show that the throughput dropped for every test as the distance went from 15 m to 30 m, except for WPA2 + OpenVPN with TCP traffic.

5.6 Result Analysis

Results show that the throughput of WPA2 + OpenSSH with TCP traffic drops drastically even though the channel conditions remain the same. This phenomenon results most likely from the used protocols. As the OpenSSH (and SSH altogether) is using TCP, and in these tests the test traffic was created with iPerf3 using TCP, this result could be anticipated. In general, using TCP over TCP is bad practice, especially in lossy networks. The drop in TCP throughput is called TCP meltdown [57]. The achieved throughput before it drops (i.e the first 10 seconds of each test) can be thought as the real performance of WPA2 + OpenSSH tunnel, because the drop in the throughput doesn't result from OpenSSH itself. OpenSSH adds overhead and as a result the throughput reduces by approximately 100 Mb/s.

From results in Figure 5.4 can be seen that the RX rate that DTD reported can't correlate with the used TX rate. The achieved throughput with UDP is 566.0 Mb/s in average, so the used TX rate has to be higher than the reported RX rate, which was 585.0 Mb/s. The reported RX rate is the maximum throughput at the PHY layer, and the achieved average throughput at transport layer (UDP) is only about 20 Mb/s lower. As stated in subsection 5.1, the efficiency of the MAC layer is roughly 70 %. Contradictions between the reported RX rate and the possible TX rate lead to a conclusion that the RX and TX rates are not comparable, and it is not reasonable to further compare these rates.

At every tested distance the throughput of WPA2 + OpenVPN remained more or less the same, and the achieved throughput was about 100 Mb/s. When looking into the cause of this, it was found out that the OpenVPN tunneling causes high load for Central Processing Unit (CPU) on both server and client. During the tests, OpenVPN server process consumed 25% of the PC's CPU, and the OpenVPN client process consumed 99% of the DTD's CPU. For this reason, it can be said that the DTD's CPU performance is most likely restricting the WPA2 + OpenVPN throughput. After finding out how CPU intensive the OpenVPN was, brief tests were performed to find out how much OpenSSH stresses the CPU's of the DTD and PC. The result was that OpenSSH stresses the DTD's CPU 25% during the throughput test with iPerf3. At PC the CPU usage was far less, only 10%.

At 30 m distance, the average throughput with UDP was 447.0 Mb/s. If the 70 % MAC layer efficiency is taken into account, the resulted data rate at PHY layer is 639.0 Mb/s. Based on the link budget calculations presented in subsection 5.1, the maximum achievable PHY layer data rate at 30 m distance is 975.0 Mb/s. From these results, it can be seen that the link budget calculations were not quite accurate. Basically this means that the used MCS could have been MCS 5 instead of the MCS 7, that was the maximum achievable MCS rate based on the link budget calculations.

When comparing the results from 30 m distance to the set requirements for the wireless mission data system, it can be found out, if the performance of the designed system is sufficient or not. Table 5.5 shows the transfer times for 4 GB of data with the tested protocols. UDP is not listed because UDP can't be used as is to reliably transfer data. UDP tests were executed to find out the maximum achievable throughput of the system, and to be able to assess the overheads caused by TCP, OpenSSH and OpenVPN. The throughput values that were used in the calculations were 300 Mb/s for WPA2, 200 Mb/s for WPA2 + OpenSSH and 100 Mb/s for WPA2 + OpenVPN.

Table 5.5. *Results vs. requirements*

Used protocols	Time to transfer 4 GB of data
WPA2	1 min 49 s
WPA2 + OpenSSH	2 min 43 s
WPA2 + OpenVPN	5 min 27 s

From Table 5.5 can be seen that the throughputs with WPA2 only and WPA2 + OpenSSH would fulfill the requirements. The requirement was that the system has to transfer 4 GB of data in 5 minutes. The WPA2 + OpenVPN also comes pretty close to fulfill the requirements.

6. CONCLUSIONS

The target of this thesis was to design a wireless mission data transfer system for use with FINAF's Grob aircraft. Thesis concentrated on the selection of the wireless communication technology and the security of the wireless communication. After brief evaluation Wi-Fi standards were recognized as promising technologies for implementing the wireless mission data transfer system, based on their high data rates and the low prices of the equipment.

The Wi-Fi standard used in this thesis for the trial system and measurements, IEEE 802.11ac could provide sufficient throughput for transferring the mission data, but the results achieved in this thesis will only apply for a single STA. In the final implementation, there might be up to 5 Grob aircraft simultaneously using the wireless mission data system.

The upcoming IEEE 802.11ax standard will bring new features, like for example the UL MU-MIMO, which would be almost essential feature for the wireless mission data transfer system. At the time of writing this thesis, first consumer grade devices based on draft 3.0 version of IEEE 802.11ax standard are starting to roll out. The draft 3.0 version of IEEE 802.11ax was released in June 2018. The first devices that are starting to roll out are wireless routers, but there are yet no wireless network adapters that could have been used in this thesis instead of the Sparklan adapter. At the moment 802.11ax seems like a very good option for the technology choice to implement the wireless mission data transfer system.

Link budget calculations couldn't be exploited properly for the tested system. The used equipment did not have enough options for monitoring the used TX powers nor the received signal strengths. If the system will be further tested, at least the AP has to be chosen differently. The Asus RT-AC68U that was used during measurements in this thesis did not allow choosing the WLAN channels freely. Because of this, the WLAN frequencies that are intended for outdoor use, and thus allow using higher TX powers could not be used. The WLAN frequencies for outside use in Finland allow a maximum TX power of 30 dBm (1 W) EIRP, which means that the radiated power including antenna gain can't exceed 30 dBm. The wireless network adapter used in this thesis had the maximum TX power of 15 dBm when using 80 MHz channel and three spatial streams. With antenna gain the EIRP was increased to 22 dBm. It can be said that with devices that would support higher TX powers and allowing to freely choose the used channels, the throughput of the system could be potentially increased.

There were also problems with the TCP congestion control, and the results even at 1 m distance didn't come close to the theoretical maximum throughput of the used devices (1.3 Gb/s). There is no doubt that after further research and configuration the throughtput results could be better. It also must be noted that the Ethernet connection between the AP and the PC was a Gigabit Ethernet (GbE) connection. The GbE connection didn't restrict the throughput in the measurements in this thesis, but in the final implementation the wired connection between the AP and the GS server has to be taken into account.

If the wireless communication is secured with either of the proposed methods, OpenSSH or OpenVPN, the USB memory stick can be used to safely distribute the encryption keys as described in section 5.2. The keys would be generated with a server computer that is a part of GS. Even if the system would use static or symmetric encryption keys, the system could be thought secure if the lifetime of the keys is kept short. Encryption keys can be generated so that every client (Grob aircraft in this case) would have a unique encryption key, and the key would be valid only for one mission.

In addition to the wireless communication technology and the additional security measures like OpenSSH or OpenVPN, the wireless mission data transfer system needs software implementation to actually transfer the files from the aircraft to the GS or the other way. With OpenSSH, for example scp or rsync could be used to transfer files. Scp is a file copy program implemented by OpenSSH [48] and rsync is a program that can be used to synchronize or transfer files between two computers e.g through SSH tunnel. With WPA2 only and with OpenVPN, some kind of file server system could be used. For the file transfer there are multiple options.

Even though that it was mentioned in chapter 5.6, that UDP can't be used as is to reliably transfer data, it would be be interesting to find out the performance of UDP transmission, if the error detection and correction would be implemented by hand. If the wireless mission data transfer system is further examined in the future, this could be a part of the study.

When the wireless mission data transfer system is finally implemented, it has to made sure that the system does not cause RF emissions during the flight. If the final system is using Linux as operating system, one possibility is to use a Linux kernel feature called rfkill. Rfkill can be used to turn off radio devices with software. Some radio devices actually have a hardware switch that can be toggled with rfkill. Even if the rfkill would be available to use, its behaviour would have to be verified with additional tests and measurements. [58]

Other options for the wireless mission data transfer system should also be considered, if the time window that was specified to be 5 min proves to be too long, and the data should be transferred faster. One possibility is to use the existing physical transfer

media, which is the USB memory stick in this case, to transfer the large video files. Wireless part of the mission data transfer system could still be used for transferring the mission briefing data to the aircraft, and for transferring the flight parameters to the ground station after the flight. Wireless mission data transfer system could also be used for fleet management purposes, that could include for example uploading new software versions for the MFD. The use case of the wireless mission data transfer system is heavily dependent on the length of the time window that can be used to transfer data. Because the requirements for the wireless mission data transfer system were not explicitly specified, it can't be unambiguously stated whether the designed system is usable or not.

In this thesis, the wireless mission data transfer system was designed around the data recorder of Grob aircraft, which was referred as DTD. However, anything that is presented in thesis isn't necessarily bound to the DTD. This means that the techniques presented in this thesis could be easily used with another platform and/or other devices. Despite the used platform and devices, based on the results it can be said that in the final system has to balance between the level of security, and the time that is used for data transfer.

BIBLIOGRAPHY

[1] Ilmavoimat. *Grob G 115E*. 2018. URL: https://ilmavoimat.fi/documents/1951206/2016308/Ilmavoimat+-konetyyppitietoja+Grob+G115E+%287_18%29.pdf/515dd33e-5e34-4865-887b-67c238c39ba4/Ilmavoimat+-konetyyppitietoja+Grob+G115E+%287_18%29.pdf.pdf.

[2] Ilmavoimat. *Valmet L-70 Vinka*. 2018. URL: https://ilmavoimat.fi/documents/1951206/2016308/Ilmavoimat+-+konetyyppitietoja+Valmet+L-70+Vinka+%281_18%29.pdf/26daacdc-796b-4671-8478-67e86e713147/Ilmavoimat+-+konetyyppitietoja+Valmet+L-70+Vinka+%281_18%29.pdf.pdf.

[3] J. Virtanen and J.M Taskinen. Patria Aviation Oy, Tikkakoski. Interview on 15.2.2018. 2018.

[4] Eldad Perahia and Robert Stacey. "Next Generation Wireless LANs - 802.11n and 802.11ac, second edition". In: Wiley-IEEE Standards Association, 2013. ISBN: 978-1-107-01676-7.

[5] *5G new radio network*. Nokia. 2018. URL: https://onestore.nokia.com/asset/205407 (visited on 10/18/2018).

[6] Nokia. *Private LTE*. 2018. URL: https://networks.nokia.com/solutions/private-lte (visited on 10/25/2018).

[7] 3GPP Jeanette Wannstrom. *LTE Advanced*. 2013. URL: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced (visited on 10/25/2018).

[8] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*. Tech. rep. New York, USA: IEEE Standards Association, 2013.

[9] Abhaykumar Kumbhar. "Overview of ISM Bands and Software-Defined Radio Experimentation". In: *Wireless Personal Communications* 97.3 (Dec. 2017), pp. 3743–3756. ISSN: 1572-834X. DOI: 10.1007/s11277-017-4696-z. URL: https://doi.org/10.1007/s11277-017-4696-z.

[10] Ho Quang-Dung, Daniel Tweed, and Le-Ngoc Tho. "Requirements and Regulations in the 5 GHz Unlicensed Spectrum". In: *Long Term Evolution in Unlicensed Bands*. Cham: Springer International Publishing, 2017, pp. 11–20.

ISBN: 978-3-319-47346-8. DOI: 10.1007/978-3-319-47346-8_2. URL: https://doi.org/10.1007/978-3-319-47346-8_2.

[11] Viestintävirasto. *Taajuusjakotaulukko*. Finnish. 2018. URL: https://www.viestintavirasto.fi/attachments/maaraykset/Taajuusjakotaulukko_suomi_3.1.2018.pdf.

[12] John Terry and Juha Heiskala. "OFDM Wireless LANS: A Theoretical and Practical Guide". In: 2001. ISBN: 978-0-672-32157-3.

[13] Hermann Rohling. "OFDM Concepts for Future Communication Systems". In: 2011. ISBN: 978-3-642-17495-7.

[14] Hermann Rohling. "Multi-Carrier Techniques for Broadband Wireless Communications". In: 2007. URL: https://ebookcentral.proquest.com/lib/tut/detail.action?docID=1085263.

[15] Li Ye. "Basic Concepts". In: *Orthogonal Frequency Division Multiplexing for Wireless Communications*. Ed. by Li Ye and Stuber Gordon. Boston, MA: Springer US, 2006, pp. 19–46. ISBN: 978-0-387-30235-5. DOI: 10.1007/0-387-30235-2_2. URL: https://doi.org/10.1007/0-387-30235-2_2.

[16] H. Yin and S. Alamouti. "OFDMA: A Broadband Wireless Access Technology". In: *2006 IEEE Sarnoff Symposium*. Mar. 2006, pp. 1–4. DOI: 10.1109/SARNOF.2006.4534773.

[17] Hermann Lipfert. "MIMO OFDM Space Time Coding – Spatial Multiplexing Increasing Performance and Spectral Efficiency in Wireless Systems". In: 2007.

[18] Ahmed Bannour and Matin Abdul Mohammad. "Coding for MIMO-OFDM in Future Wireless Systems". In: 2015. ISBN: 978-3-319-19152-2. DOI: https://doi-org.libproxy.tut.fi/10.1007/978-3-319-19153-9. URL: https://ebookcentral.proquest.com/lib/tut/detail.action?docID=1085263.

[19] Aki Hakkarainen. *I/Q Imbalance in Multiantenna Systems: Modeling, Analysis and RF-Aware Digital Beamforming*. Tampere University of Technology. Publication. Tampere University of Technology, Jan. 2017. ISBN: 978-952-15-3871-1.

[20] A. Hakkarainen et al. "Widely-linear beamforming and RF impairment suppression in massive antenna arrays". In: *Journal of Communications and Networks* 15.4 (Aug. 2013), pp. 383–397. ISSN: 1229-2370. DOI: 10.1109/JCN.2013.000069.

[21] H. Lou et al. "A comparison of implicit and explicit channel feedback methods for MU-MIMO WLAN systems". In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. Sept. 2013, pp. 419–424. DOI: 10.1109/PIMRC.2013.6666172.

[22] G. R. Hiertz et al. "The IEEE 802.11 universe". In: *IEEE Communications Magazine* 48.1 (Jan. 2010), pp. 62–70. ISSN: 0163-6804. DOI: 10.1109/MCOM.2010.5394032.

[23] *Wi-Fi Alliance introduces Wi-Fi 6*. Wi-Fi, Newsroom. 2018. URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6 (visited on 10/06/2018).

[24] Bob O'Hara and Al Petrick. "Medium access control (MAC)". In: *IEEE 802.11 Handbook:A Designer 39s Companion*. Wiley-IEEE Standards Association, 2005. ISBN: 9781118098851. DOI: 10.1109/9781118098851.ch3. URL: https://ieeexplore-ieee-org.libproxy.tut.fi/xpl/articleDetails.jsp?arnumber=5769880.

[25] Kevin J. Negus and Al Petrick. "History of wireless local area networks (WLANs) in the unlicensed bands". In: *Info : the Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media* 11.5 (2009), pp. 36–56. ISSN: 1463-6697. URL: https://search-proquest-com.libproxy.tut.fi/docview/275033398?accountid=27303.

[26] L. Verma, M. Fakharzadeh, and S. Choi. "Wifi on steroids: 802.11ac and 802.11ad". In: *IEEE Wireless Communications* 20.6 (Dec. 2013), pp. 30–35. ISSN: 1536-1284. DOI: 10.1109/MWC.2013.6704471.

[27] Cisco. "802.11ac: The Fifth Generation of Wi-Fi". In: (2018), pp. 1–15. URL: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf.

[28] D. J. Deng et al. "IEEE 802.11ax: Highly Efficient WLANs for Intelligent Information Infrastructure". In: *IEEE Communications Magazine* 55.12 (Dec. 2017), pp. 52–59. ISSN: 0163-6804. DOI: 10.1109/MCOM.2017.1700285.

[29] National Instruments. "Introduction to 802.11ax High-Efficiency Wireless". In: (2018), pp. 1–10. URL: ttp://www.ni.com/white-paper/53150/en/.

[30] Cisco. "IEEE 802.11ax: The Sixth Generation of Wi-Fi". In: (2018), pp. 1–20. URL: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/white-paper-c11-740788.pdf.

[31] M. A. Abo-Soliman and M. A. Azer. "A study in WPA2 enterprise recent attacks". In: *2017 13th International Computer Engineering Conference (ICENCO)*. Dec. 2017, pp. 323–330. DOI: 10.1109/ICENCO.2017.8289808.

[32] M. Agarwal, S. Biswas, and S. Nandi. "Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks". In: *IEEE Communications Letters* 19.4 (Apr. 2015), pp. 581–584. ISSN: 1089-7798. DOI: 10.1109/LCOMM.2015.2400443.

[33] "IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control". In: *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)* (Feb. 2010), pp. 1–205. DOI: 10.1109/IEEESTD.2010.5409813.

[34] Edwin Lyle Brown. "Coding for MIMO-OFDM in Future Wireless Systems". In: 2006. ISBN: 9781420044652.

[35] "Amendment 6: Medium Access Control (MAC) Security Enhancements". In: *IEEE Std 802.11i-2004* (2004), pp. 1–205. DOI: 10.1109/IEEESTD.2010.5409813.

[36] Alberto Bartoli et al. "Secure Configuration Practices of WPA2 Enterprise Supplicants". In: (2018).

[37] Jie Wang and Zachary A. Kissel. "Introduction to Network Security : Theory and Practice." In: 2015.

[38] Mathy Vanhoef and Frank Piessens. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". In: *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2017.

[39] Changhua He et al. "A Modular Correctness Proof of IEEE 802.11I and TLS". In: *Proceedings of the 12th ACM Conference on Computer and Communications Security*. CCS '05. Alexandria, VA, USA: ACM, 2005, pp. 2–15. ISBN: 1-59593-226-7. DOI: 10.1145/1102120.1102124. URL: http://doi.acm.org/10.1145/1102120.1102124.

[40] Jyh-Cheng Chen, Ming-Chia Jiang, and Yi-wen Liu. "Wireless LAN security and IEEE 802.11i". In: *IEEE Wireless Communications* 12.1 (Feb. 2005), pp. 27–36. ISSN: 1536-1284. DOI: 10.1109/MWC.2005.1404570.

[41] Wi-Fi Alliance. *Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security*. 2018. URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security.

[42] D. Harkins. "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks". In: *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*. Aug. 2008, pp. 839–844. DOI: 10.1109/SENSORCOMM.2008.131.

[43] Markus Feilner. "Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using this Powerful Open Source Application". In: 2006.

[44] Jon C. Snader. "VPNs illustrated: Tunnels, VPNn, and IPsec". In: 2005. ISBN: 0-321-24544-X.

[45] S. Turner. "Transport Layer Security". In: *IEEE Internet Computing* 18.6 (Nov. 2014), pp. 60–63. ISSN: 1089-7801. DOI: 10.1109/MIC.2014.126.

[46] OpenSSH. "OpenSSH Project History". In: 18.6 (2018). URL: https://www.openssh.com/history.html.

[47] Richard E. Silverman Daniel J. Barrett. "SSH, the Secure Shell: The definitive guide". In: 2001. ISBN: 0-596-00011-1.

[48] Michael Stahnke. "Pro OpenSSH". In: 2006. ISBN: 1-59059-476-2.

[49] IEEE. *IEEE 802.11ax Channel Model Document*. 2014. URL: http://www.ieee802.org/11/Reports/tgax_update.htm (visited on 10/30/2018).

[50] L. Krasny et al. "Doppler spread estimation in mobile radio systems". In: *IEEE Communications Letters* 5.5 (May 2001), pp. 197–199. ISSN: 1089-7798. DOI: 10.1109/4234.922758.

[51] 3GPP. *3GPP TR 36.814*. 2017. URL: http://www.3gpp.org/ftp/Specs/archive/36_series/36.814/ (visited on 10/30/2018).

[52] Saleh Faruque. "Radio Frequency Propagation Made Easy". In: 2015. ISBN: 978-3-319-11394-4. DOI: 10.1007/978-3-319-11394-4.

[53] Simon R. Saunders. "Antennas adn Propagation for Wireless Communication System". In: 2007. ISBN: 978-0-470-84879-1.

[54] *WPEQ-353ACNI*. Sparklan, WPEQ-353ACNI product datasheet. 2018. URL: http://www.sparklan.com/p3-filedown.php?PKey=0f67jlIx4YYfwB9gV5s606k%5C2%CC%891sUoMLFgttsc2r_rNA (visited on 10/05/2018).

[55] *Delock WLAN 802.11 ac/a/h/b/g/n Antenna RP-SMA plug 5 - 7 dBi omni-directional with tilt joint black*. Delock, datasheet. 2018. URL: https://www.delock.com/produkt/88899/pdf.html?sprache=en (visited on 10/31/2018).

[56] Eman Abdelfattah. "Performance Evaluation of TCP Congestion Control Mechanisms". In: *Novel Algorithms and Techniques in Telecommunications and Networking*. Ed. by Tarek Sobh, Khaled Elleithy, and Ausif Mahmood. Dordrecht: Springer Netherlands, 2010, pp. 251–256. ISBN: 978-90-481-3662-9.

[57] Olaf Titz. *Why TCP Over TCP Is A Bad Idea*. 2001. URL: http://sites.inka.de/bigred/devel/tcp-tcp.html (visited on 10/22/2018).

[58] About rfkill. *About rfkill*. 2015. URL: https://wireless.wiki.kernel.org/en/users/documentation/rfkill (visited on 10/26/2018).