FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

Radio Hacking

Eine Einführung in die Funktechnik und Software Defined Radios

Bachelorarbeit 1

Angefertigt an der
Fachhochschule FH Campus Wien
Bachelorstudiengang: Informationstechnologien und Telekommunikation

Vorgelegt von:
Luca Strobl

Personenkennzeichen
1610475032

Vertiefungsrichtung:
IT-Security

Eingereicht am:
17. 01. 2019

Erklärung:

Ich erkläre, dass die vorliegende Bachelorarbeit von mir selbst verfasst wurde und ich keine anderen als die angeführten Behelfe verwendet bzw. mich auch sonst keiner unerlaubter Hilfe bedient habe.

Ich versichere, dass ich diese Bachelorarbeit bisher weder im In- noch im Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Weiters versichere ich, dass die von mir eingereichten Exemplare (ausgedruckt und elektronisch) identisch sind.

Datum: 17.01.2019 Unterschrift:

Kurzfassung

Was haben Garagentore und Autoschlüssel sowie smarte Glühbirnen und Türschlösser gemein?
Sie alle kommunizieren mittels elektromagnetischer Wellen. Da diese Wellen über die Luft übertragen werden, können sie von jeglichen Personen mit geeigneter Hardware und speziellem Wissen mitgeschnitten und analysiert werden. Früher wurde unterschiedliche Hardware für verschiedene Frequenzbereiche benötigt, das einen erheblichen finanziellen Aufwand und sogleich eine Hürde darstellte. Heutzutage kann man jedoch mit einer Investition von lediglich 300 Euro einen Frequenzbereich von 1 MHz bis 6 GHz abdecken. Somit können mit einem einzigen Gerät Signale von Garagentoröffnern, Autoschlüsseln sowie die Kommunikation zwischen Geräten des Internets der Dinge abgefangen und analysiert werden. Dabei spielt die unzulänglich implementierte Sicherheit von den Produkten eine große Rolle. Vollständige Anleitungen im Internet über das Ausnützen von Sicherheitslücken gepaart mit Software Defined Radios öffnen – im wahrsten Sinne des Wortes – Tür und Tor für kriminelle Machenschaften, bestätigt durch zahlreiche Berichte. Zugleich erleichtern Software Defined Radios die Arbeit von Security Researchern, die nun einfacher und schneller Sicherheitslücken aufdecken und melden können – in der Hoffnung, dass diese Lücken noch unbekannt waren und somit gröbere Schäden vermieden werden konnten. Es bleibt jedoch bei einem Wettlauf zwischen den Angreifern und Verteidigern.

Abstract

What do have garage doors, car keys, smart bulbs and smart door locks in common? They all communicate through electromagnetic waves. The fact that these waves are transmitted over the air enables persons with adequate hardware and specific knowledge to sniff and analyze the data. Back in time, different hardware was needed for different frequency ranges. This meant a big investment and thus a hurdle. However, today a frequency range of 1 MHz up to 6 GHz can be analyzed with a single investment of 300 euros. It is therefore possible to sniff signals of garage door openers, car keys and whole communication of the Internet of Things with one single hardware element. Weak security measures play a big role. Entire instructions of how to exploit security flaws paired with Software Defined Radios open the door to criminal activities, confirmed by numerous incidents. At the same time, Software Defined Radios ease the work of security researchers, enabling them to uncover and report security flaws faster – in the hope that these flaws were still unknown and thus preventing bigger damage. However, it remains a race between attackers and defenders.

Abkürzungsverzeichnis

ELVIS	Embedded Lab Vienna for IoT & Security
UHF	Ultra High Frequency
SDR	Software Defined Radio
FPGA	Field Programmable Gate Array
ASIC	Application Specific Integrated Circuit
ASSP	Application Specific Standard Product
SoC	System on a Chip
SNR	Signal to Noise Ratio
IP	Intellectual Property
BER	Bit Error Rate
AM	Amplitudenmodulation
FM	Frequenzmodulation
A/D-Wandler	Analog-/Digitalwandler
D/A-Wandler	Digital-/Analogwandler
PAM	Pulse-Amplitude-Modulation
PCM	Pulse-Code-Modulation
ASK	Amplitude Shift Keying
FSK	Frequency Shift Keying
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
QAM	Quadrature Amplitude Modulation
IoT	Internet of Things

Schlüsselbegriffe

Elektromagnetische Wellen

Software Defined Radio

Field Programmable Gate Array

Dezibel, Filter

Oszillator

Antenne

Amplitudenmodulation

Frequenzmodulation

Digital-/Analogwandler

Analog-/Digitalwandler

Pulse-Amplitude-Modulation

Pulse-Code-Modulation

Amplitude Shift Keying

Frequency Shift Keying

Phase Shift Keying

Quadrature Phase Shift Keying

Quadrature Amplitude Modulation

Pentesting

Internet der Dinge

Keywords

Electromagnetic waves
Software Defined Radio
Field Programmable Gate Array
Decibel
Filter
Oscillator
Antenna
Amplitude modulation
Frequency modulation
Digital to analog converter
Analog to digital converter
Pulse-Amplitude-Modulation
Pulse-Code-Modulation
Amplitude Shift Keying
Frequency Shift Keying
Phase Shift Keying
Quadrature Phase Shift Keying
Quadrature Amplitude Modulation
Penetration testing
Internet of things

Inhaltsverzeichnis

1. EINLEITUNG

1.1 Aufbau

Kapitel 3 liefert einen allgemeinen Überblick über elektromagnetische Wellen und erklärt die Entstehung und die Ausbreitung dieser Wellen.

In Kapitel 4 werden die grundlegenden Komponenten eines Software Defined Radios (SDR) beschrieben. Zuerst wird auf die Hardware-Komponente Field Programmable Gate Array (FPGA) eingegangen. Danach folgt das Dezibel, da es bei der Arbeit mit Signalen häufig vorkommt. Kapitel 4.3 und 4.4 gehen auf elektrische Filter und Oszillatoren ein. Diese werden in Software Defined Radios in Software implementiert, dennoch erfolgt für das bessere Verständnis die Erklärung des Grundprinzips anhand der analogen Komponenten. Darauf folgt eine allgemeine Erklärung von Antennen und von elektronischem Rauschen.

Kapitel 5 behandelt die verschiedenen Signalformen. Die unterschiedlichen Modulationsarten von analogen und digitalen Signalen sowie die Umwandlung von analogen in digitale Signale werden jedoch in der Bachelorarbeit 2 erläutert.

Abschließend erfolgt eine kurze Zusammenfassung dieser Arbeit und eine Vorschau auf die nachfolgende Arbeit und auf die Angriffe, die mit Software Defined Radios möglich sind.

In dieser Arbeit wird als Quelle, falls nicht anders angegeben, das Buch „Handbuch der modernen Funktechnik: Prinzipien, Technik, Systeme und praktische Anwendungen“ von Lobensommer [L95] verwendet.

1.2 Forschungsfrage

Zentrale Fragestellungen dieser Arbeit sind die Angriffspunkte von IoT-Geräten sowie den Attacken zugrunde liegenden Prinzipien und die dafür benötigten Hardwareelemente.

1.3 Ziel

Diese Arbeit hat das Ziel, die Grundlagen der Funktechnik und das Software Defined Radio zu erklären, damit die Angriffe auf IoT-Geräte nachvollzogen und verstanden werden können. Weiters soll mittels der Grundlagen erläutert werden, warum diese Angriffe funktionieren und mit welcher Hardware sie umgesetzt werden können. Zudem wird der Inhalt dieser Arbeit im Wiki des Embedded Lab Vienna for IoT & Security veröffentlicht.

1.4 Methodik

Dieser Arbeit liegt eine eingehende Literaturrecherche zugrunde.

2. RELATED WORK

Das Buch „Software-Defined Radio for Engineers" von Collins, Getz, Pu und Wyglinski [CGPW18] bietet eine hervorragende Referenz für Software Defined Radios. Es umfasst einen allgemeinen Überblick über die Entstehungsgeschichte von SDRs, Signalverarbeitung, Modulationstechniken von Signalen, Hardwareelemente von SDRs, Anwendung von SDRs sowie weitere tiefergehende Kapitel über Kommunikation, die aber nicht Bestandteil dieser Arbeit sind. Jedoch wird auf die Funktionsweise grundlegender elektronischer Komponenten, wie Schwingkreise, Filter, Oszillatoren, Antennen, DA-Wandler und AD-Wandler, nicht eingegangen. Es werden auch die Ausbreitung elektromagnetischer Wellen und das Dezibel außer Acht gelassen, die aber für das Verständnis von Bedeutung sind. Weiters werden FPGAs nicht näher behandelt.

„Handbuch der modernen Funktechnik: Prinzipien, Technik, Systeme und praktische Anwendungen" von Lobensommer [L95] erklärt hingegen die grundlegenden elektronischen Komponenten, die in „Software Defined Radios for Engineers" [CGPW18] fehlen, berücksichtigt aber keine Software Defined Radios.

Diese Bachelorarbeit soll die wesentlichen Informationen aus den drei Hauptquellen, „Handbuch der modernen Funktechnik: Prinzipien, Technik, Systeme und praktische Anwendungen", „Software-Defined Radio for Engineers" und „FPGAs For Dummies, Altera Special Edition" [M14], herausfiltern und konvergieren, um eine solide Basis für die Bachelorarbeit 2 zu schaffen, in der die Sicherheit von drahtloser Kommunikation mittels SDRs analysiert wird.

3. ELEKTROMAGNETISCHE WELLEN

3.1 Elektrisches Feld

Legt man eine Gleichspannung an einen Kondensator, so entsteht zwischen den Platten ein elektrisches Feld. Dieses Feld setzt sich aus Feldlinien zusammen, die von einer Platte zur anderen reichen, wie in Abbildung 3-1 dargestellt ist. Je größer die angelegte Spannung ist, desto stärker ist das elektrische Feld.

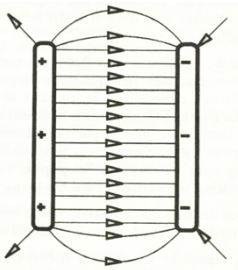

Abbildung 3-1: Elektrisches Feld [L95]

3.2 Magnetisches Feld

Wenn Gleichstrom durch einen Leiter fließt, bildet sich um ihn ein magnetisches Feld aus. Die magnetischen Feldlinien erzeugen konzentrische Kreise um die Längsachse des Leiters. Je größer der Gleichstrom ist, desto stärker ist das Magnetfeld. Abbildung 3-2 zeigt die Ausbildung der konzentrischen Kreise.

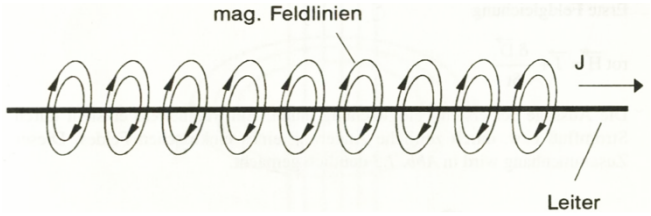

Abbildung 3-2: Magnetisches Feld [L95]

Eine Änderung von Strom oder Spannung bewirkt eine Änderung des magnetischen oder elektrischen Feldes, d.h. die Felder entstehen oder zerfallen. Dabei kann sich die in einem Feld enthaltene Energie nur in die jeweils andere Energieform umwandeln. Somit erzeugt ein zerfallendes elektrisches Feld ein magnetisches Feld und umgekehrt.

3.3 Elektrischer Schwingkreis

3.3.1 Geschlossener Schwingkreis

Die einfachste Form eines Schwingkreises besteht aus der Verbindung von Induktivität und Kapazität. In der Praxis werden dazu eine Spule und ein Kondensator verwendet, die von elektrischem Strom durchflossen werden. Dabei können die Bauteile parallel oder hintereinander geschaltet werden.

Der in Abbildung 3-3 gezeigte Schwingkreis besteht aus einer Stromquelle, einem Kondensator und einer Spule. In der Grundstellung laden sich die Platten des Kondensators auf, dargestellt durch die roten Feldlinien. Dabei wird die obere Platte positiv aufgeladen, die untere negativ. Wird der Schalter umgelegt, so fließt ein Entladestrom, dargestellt über die roten Pfeile, durch die Spule und baut ein Magnetfeld, dargestellt durch die blauen Feldlinien, auf (Abbildung 3-3.b). Während das elektrische Feld im Kondensator zusammenfällt, nimmt der Entladestrom ab. Das Magnetfeld wird maximal (Abbildung 3-3.c). Da kein elektrisches Feld mehr vorhanden ist, gibt es auch keinen Entladestrom mehr und das Magnetfeld bricht zusammen. Dieser Vorgang wiederum erzeugt durch Induktion einen Stromfluss mit entgegengesetzter Richtung, der den Kondensator wieder auflädt (Abbildung 3-3.d). Dadurch baut sich ein elektrisches Feld mit umgekehrter Polarität im Kondensator auf. Wenn dieses Feld maximal ist, gibt es kein magnetisches Feld mehr (Abbildung 3-3.e). Nun entlädt sich der Kondensator erneut und der eben beschriebene Vorgang wiederholt sich.

Aufgrund des Verlustwiderstands wird ein Teil der Energie in Wärme umgewandelt, was eine Dämpfung der Schwingung zur Folge hat. In den Abbildungen ist jedoch eine

ungedämpfte Schwingung zu sehen, d.h. dass die Energieverluste durch ständige Energiezufuhr ausgeglichen werden.

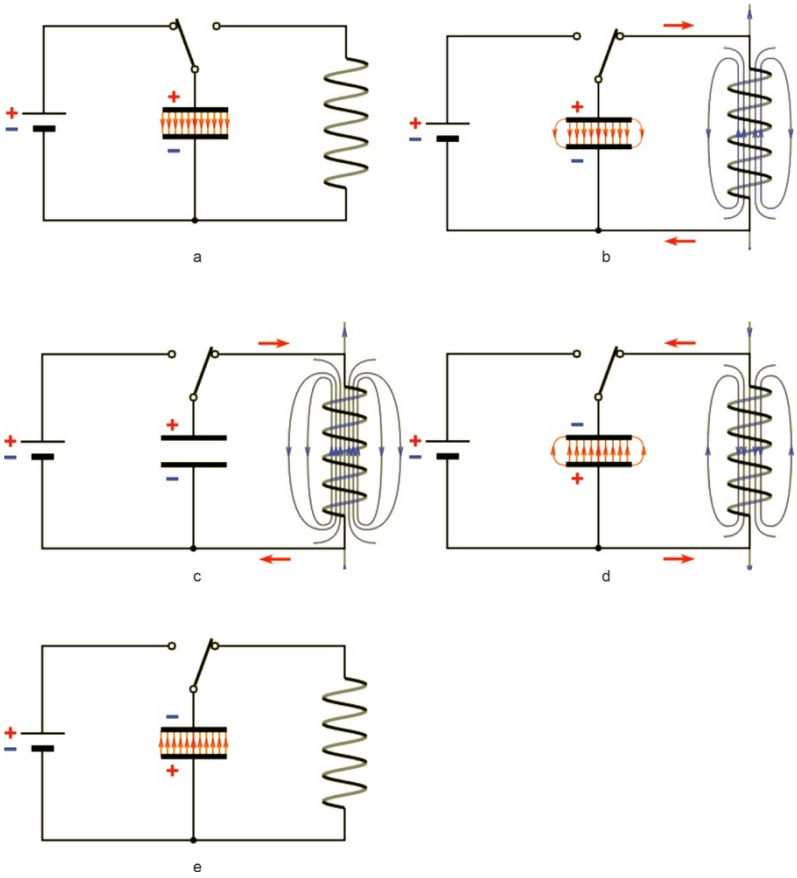

Abbildung 3-3: Schwingkreis [L95]

3.3.2 Resonanzfrequenz und Resonanzwiderstand

Spule und Kondensator bestimmen die Resonanzfrequenz eines Schwingkreises. Dabei gilt: je kleiner die Kapazität und Induktivität, desto höher die Resonanzfrequenz. In einem Wechselstromkreis ist der Blindwiderstand der Spule X_L und der Blindwiderstand des Kondensators X_C gegengleich frequenzabhängig: bei niedriger Frequenz ist X_C groß und X_L klein. Mit steigender Frequenz nimmt X_C ab und X_L zu. Resonanz tritt ein, wenn beide Blindwiderstände gleich groß sind. Abbildung 3-4 stellt diesen Sachverhalt graphisch dar.

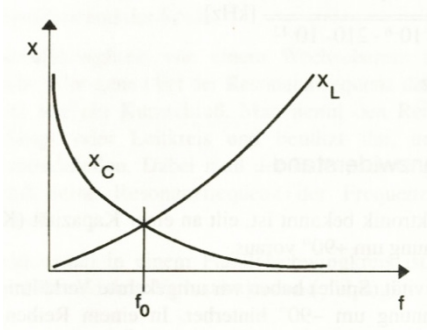

Abbildung 3-4: Frequenzverhalten der Blindwiderstände [L95]

Der Resonanzwiderstand ist ein Scheinwiderstand, der im Resonanzfall auftritt. Im Parallelschwingkreis wird er sehr groß, während er im Reihenschwingkreis gegen null geht. Der Ausgangspunkt für die weiteren Erklärungen ist die folgende Formel:

$$Z_0 = \frac{U_{ges}}{I_{ges}}$$

In einem Parallelschwingkreis kompensieren sich die Ströme durch Spule und Kondensator bei Resonanzfrequenz. Obige Formel zeigt, dass dadurch der Resonanzwiderstand gegen unendlich geht. Dies ist jedoch nur in der Theorie möglich, da reale Bauteile Verlustwiderstände mit sich bringen und den Wert somit beschränken. Das Verhältnis des Stroms im Parallelschwingkreis zum Strom in den Zuleitungen ergibt die Schwingkreisgüte Q. Je höher die Güte, desto stärker die Resonanz, das heißt desto kleiner die Bandbreite eines Schwingkreises.

3.4 Ausbreitung elektromagnetischer Wellen im Raum

Die Ausbreitung elektromagnetischer Wellen im Raum wird von unterschiedlichen Faktoren beeinflusst: die Frequenz und Polarisierung der Wellen, die Art und Höhe der Antennen sowie die Sendeleistung, die Beschaffenheit der Erdoberfläche und die Tageszeit. Allgemein gilt: je höher die Frequenz, desto kürzer die Reichweite. Dabei spielen die Troposphäre und die Ionosphäre eine besondere Rolle. In der Troposphäre können elektromagnetische Wellen gebeugt, gebrochen und reflektiert werden. In diesem Zusammenhang spricht man von der troposphärischen Ausbreitung. Diese Effekte erlauben Funkverbindungen über mehrere hundert Kilometer. Elektromagnetische Wellen in einem Frequenzbereich bis etwa 30 MHz werden von der Ionosphäre vollständig reflektiert. Diese Eigenschaft nutzen manche Telekommunikationssysteme ebenso zur Überbrückung großer Reichweiten. [L95]

Im Folgenden werden elektromagnetische Wellen im Frequenzbereich von etwa 10 kHz bis 30 GHz vorgestellt.

3.4.1 Längstwellen (<30 kHz)

Diese Wellen werden von der Erdoberfläche und der Ionosphäre total reflektiert. Durch starke Sender und große Antennen kann eine Reichweite von mehr 10.000 km erzielt werden. Unterhalb von 10 kHz werden die Wellen von der Erde stark absorbiert. Längstwellen können in Wasser eine Tiefe von bis zu 30 Metern erreichen. Aus diesem Grund werden sie auch für die Kommunikation mit U-Booten verwendet. Aufgrund der stabilen Funkverbindungen mit Längstwellen finden sie auch Einsatz in der Navigation von Schiffen.

3.4.2 Langwellen (30 kHz bis 300 kHz)

Tagsüber breiten sich Langwellen als Bodenwellen aus. Dabei gilt: je höher die Frequenz, desto größer die Absorption durch die Erde. Jener Teil der Langwellen, die in den Raum ausgestrahlt werden, werden von der Ionosphäre absorbiert. Während der Nacht jedoch wird genau dieser Teil von der Ionosphäre reflektiert, was eine Vergrößerung der Reichweite zur Folge hat. Somit muss die Sendeleistung in dieser Zeit um bis zu 50% reduziert werden. Langwellensendestationen bestehen aus Antennenmasten mit 200 Metern Höhe.

3.4.3 Mittelwellen (300 kHz – 3 MHz)

Mittelwellen verhalten sich ähnlich zu den Langwellen. Sie breiten sich als Bodenwellen und Raumwellen aus. Am Tag kommt es wieder zu einer Absorption der Raumwellen durch die Ionosphäre, die in der Nacht durch eine Reflektion ersetzt wird. Wenn diese reflektierten Raumwellen auf die Bodenwellen treffen, können Störungen auftreten, die sich in Lautstärkeänderungen und Verzerrungen äußern.

3.4.4 Kurzwellen (3 MHz – 30 MHz)

Kurzwellen breiten sich hauptsächlich als Raumwellen aus, das heißt, dass die Ionosphäre die Ausbreitung beeinflusst. Dabei werden drei Fälle unterschieden. Entspricht die Frequenz der Kurzwellen der Eigenfrequenz der Ionen, so werden die elektromagnetischen Wellen fast vollständig reflektiert. Ist die Frequenz kleiner, so werden die Kurzwellen stark gedämpft; ist sie größer, so durchstoßen die elektromagnetischen Wellen die Ionosphäre und verbreiten sich im Weltall.

3.4.5 Ultrakurzwellen (30 MHz – 300 MHz)

Für die Ausbreitung von Ultrakurzwellen spielt die Ionosphäre nur mehr eine kleine Rolle. Ab Frequenzen von etwa 140 MHz ist ihr Einfluss überhaupt nicht mehr vorhanden. Ultrakurzwellen breiten sich daher als Bodenwelle aus. Aufgrund der hohen Frequenz ist die Absorption durch die Erde groß, deswegen werden hohe Antennen für die Abstrahlung benötigt. Jedoch muss in diesem Fall auch die Erdkrümmung berücksichtigt werden:

beispielsweise beträgt die Reichweite eines 100 Meter hohen Antennenmastes wegen der Erdkrümmung nur 41 Kilometer.

3.4.6 UHF-Bereich und Mikrowellen (300 MHz – 30 GHz)

Ab 300 MHz werden elektromagnetische Wellen von Gebäuden und Hügeln reflektiert. Dadurch treffen bei einem Empfänger mehrere Wellen aus verschiedenen Richtungen ein, wodurch sich die Laufzeiten und Phasenlage der einzelnen Wellen unterscheiden. Diese Art von Empfang wird Mehrwegeempfang genannt. Die Folge davon sind Dämpfungen und Verzerrungen. Aus diesem Grund sind bei Mobilfunkempfängern Entzerrer notwendig.

4. SOFTWARE DEFINED RADIO

Der Begriff des „Software Radio“ geht zurück bis ins Jahr 1984. 1993 sprach Joseph Mitola erstmals von einem „Software Defined Radio“ (SDR). Der technische Fortschritt ist maßgeblich an der steigenden Popularität von Software Defined Radios beteiligt, denn er senkte die finanzielle Hürde auf wenige hundert Euros. [CGPW18]

„Software Defined“ meint dabei die Signalverarbeitung bis zu einem gewissen Maß in Software durch Signalprozessoren oder FPGAs. Zentrale Parameter der Funkübertragung, wie die Modulation und Kanalcodierung, können über die Software eingestellt werden. Die Folge davon ist eine immense Flexibilität, da nun nicht mehr verschiedene Geräte für unterschiedliche Frequenzen verwendet werden müssen. Zusätzlich ermöglichen Open Source Programme wie GNU Radio[1] mittels einer GUI eine einfache Programmierung von SDRs.

Software Defined Radios finden Anwendung im Bereich des Amateurfunks, beim Militär und in der zivilen Welt. Bekannte Produkte sind zum Beispiel Michael Ossmanns HackRF One[2], Nuands bladeRF[3] und die USRP-Modelle von Ettus[4]. Dabei erstreckt sich der Preis von etwa 300 Euro[5] (HackRF One) bis über 5000 Euro[6] (Ettus USRP X310). Die Unterschiede liegen im unterstützten Frequenzspektrum, in der Bandbreite und im verbauten FPGA. Tabelle 1 liefert einen Überblick über die populärsten Modelle.

Modell	Transceiver[7]	USB	Frequenzspektrum	Bandbreite	Sampling Rate	Preis
HackRF One[2]	half duplex	2.0	1 MHz – 6 GHz	20 MHz[8]	20 MHz	363 €[5]
Nuand bladeRF 2.0 micro xA4[3]	full duplex	3.0	47 MHz – 6 GHz	56 MHz	61,44 MHz	580 €[9]
Ettus USRP B210[10]	full duplex	3.0	70 MHz – 6 GHz	56 MHz	61,44 MHz	1210 €

Tabelle 1: Spezifikationen von drei SDRs

[1] https://www.gnuradio.org/, aufgerufen am 10.12.2018

[2] https://greatscottgadgets.com/hackrf/, aufgerufen am 10.12.2018

[3] https://www.nuand.com/product/bladerf-xa4/, aufgerufen am 10.12.2018

[4] https://www.ettus.com/, aufgerufen am 10.12.2018

[5] https://www.antratek.de/hackrf-one-sdr-software-defined-radio?gclid=EAIaIQobChMIvs3kjrPq3gIVE5SyCh0bjQBuEAQYBCABEgKTCfD_BwE, aufgerufen am 10.12.2018

[6] https://www.ettus.com/product/details/X310-KIT, aufgerufen am 10.12.2018

[7] Ein Transceiver ist ein elektronisches Bauteil, das aus einem Transmitter und einem Receiver besteht.

[8] https://www.rtl-sdr.com/hackrf-initial-review/, aufgerufen am 10.12.2018

[9] https://www.antratek.de/nuand-bladerf-2-0-micro-xa4-sdr/, aufgerufen am 10.12.2018

4.1 Field Programmable Gate Array (FPGA)

Field Programmable Gate Arrays erschienen erstmals Mitte der 1980er Jahre. Ein FPGA ist ein integrierter Schaltkreis, auf den eine logische Schaltung geladen werden kann. Die Stärke von FPGAs gegenüber ASICs[10] und ASSPs[11] liegt in der Programmierung: die Funktion kann nach der Produktion definiert werden. Dies ermöglicht eine große Flexibilität, denn somit kann die Adaption an neue Standards oder Neukonfigurationen durchgeführt werden, nachdem der Chip im Feld installiert worden ist, daher auch der Term „field programmable“. ASSPs und ASICs hingegen sind für eine bestimmte Aufgabe entwickelt, die vor der Produktion festgelegt wurde. Dadurch sind ihre Schaltkreise fest verdrahtet und ihre Funktionalität kann somit nachträglich nicht geändert werden. [M14]

Der Unterschied zwischen FPGAs und ASICs und ASSPs kann mit den folgenden zwei Metaphern veranschaulicht werden.

Die erste Metapher verwendet eine Schnur und verschiedenfarbige Perlen. Die Perlen werden auf die Schnur aufgefädelt und komplexe Muster können nach Bedarf erzeugt werden. Dabei beschreiben die verschiedenen Farben die unterschiedlichen logischen Operationen. Die Gesamtheit der aufeinanderfolgenden Perlen bestimmt die Funktion. Muss jedoch die Farbe mancher Perlen beispielsweise in der Mitte der Schnur geändert werden, so müssen alle nachfolgenden Perlen von der Schnur genommen werden. Dieses Design ist unflexibel und repräsentiert ASICs und ASSPs. [M14]

In der zweiten Metapher werden LEGO-Bausteine verwendet. Dabei stehen die einzelnen Farben wieder für gewisse logische Operationen. Aus den LEGO-Bausteinen wird nun ein Tisch mit vier Beinen gebaut. Wenn zum Beispiel das hintere linke Tischbein in Form und Farbe geändert werden muss, so kann der Umbau unabhängig vom restlichen Tisch erfolgen. Kleine Anpassungen können erfolgen, ohne das komplette Design verändern zu müssen. Diese Metapher beschreibt FPGAs. [M14]

„Gate Arrays“ beschreiben zweidimensionale Arrays von Logikgattern. Ein Logikgatter führt einfache logische Operationen wie AND, OR und NOT durch. Wird eine große Anzahl dieser Logikgatter miteinander verbunden, so können damit komplexe Funktionen erstellt werden. [M14]

FPGAs bestehen jedoch nicht mehr nur aus Logikgattern, sondern beinhalten auch die sogenannte Hard IP. IP steht für Intellectual Property und bezeichnet vordefinierte Hardware-Blöcke, die häufig gebrauchte Funktionen implementieren. Das heißt, dass moderne FPGAs nach der Produktion bereits über DRAM-Kontroller, PCIe-Kontroller, Taktgeneratoren und Speicherblöcke verfügen. Somit kann ein FPGA auch als system on a Chip (SoC) bezeichnet werden. Systemarchitekten suchen sich einen FPGA mit der

---

[10] Ein Application-Specific Integrated Circuit (ASIC) ist ein integrierter Schaltkreis, der für eine bestimmte Aufgabe zugeschnitten ist, wie zum Beispiel ein Bitcoin-Miner.

[11] Ein Application-Specific Standard Product (ASSP) ist ein integrierter Schaltkreis, der ebenso eine spezifische Funktion erfüllt, aber im Gegensatz zu ASICs an mehrere Kunden verkauft wird. Ein Beispiel dafür sind Mikrocontroller.

integrierten IP, die sie benötigen und passen den gesamten Chip über die Logikelemente an ihre spezielle Anwendung an. [M14]

FPGAs unterscheiden sich von Mikroprozessoren auch durch ihre Performance. Während letztere bei einer Multiplikation die Instruktion aus dem Speicher laden, sie decodieren, die Zahlen laden und multiplizieren und zuletzt das Ergebnis speichern müssen, können FPGAs mehrere Operationen gleichzeitig durchführen. Diese Operationen können sich sogar unterscheiden. Beispielsweise erzeugt eine 128-Element Matrix 128 arithmetische Pipelines, von denen jede gleichzeitig Berechnungen durchführt. Dies steigert sowohl die Performanz als auch die Energieverbrauch. [M14]

4.2 Dezibel

Das Bel (B) ist ein logarithmisches Leistungsverhältnis. Im Gegensatz zu anderen physikalischen Größen wie Volt oder Ampère stellt es eine Hilfsmaßeinheit dar. Das heißt, dass die jeweilige Größe auch durch eine einfache Zahl beschrieben werden kann. Der Verstärkungsfaktor v beschreibt das Verhältnis der Ausgangsleistung PA zur Eingangsleistung PE:

$$v = \frac{P_A}{P_E}$$

Wenn v > 1, dann spricht man von Verstärkung, wenn v < 1 spricht man von Dämpfung. Es liegt weder Verstärkung noch Dämpfung vor, wenn v = 1.

Bei Logarithmierung des Verhältnisses ergibt sich die Einheit Bel:

$$v = lg\frac{P_A}{P_E}\ B$$

Das Dezibel ergibt sich bei der Multiplikation des Logarithmus mit dem Faktor 10:

$$v = 10 * lg\frac{P_A}{P_E}\ dB$$

Betrachtet man die Situation, in der weder Verstärkung noch Dämpfung vorliegen, hat der Verstärkungsfaktor v den Wert 1. Da der Logarithmus von 1 gleich 0 ist, ergibt sich ein Wert von 0 dB.

Warum wird auf die komplizierte Pseudoeinheit Dezibel zurückgegriffen, die ein Zehntel des Logarithmus vom Verhältnis zweier Leistungen beschreibt?
Für ein System, in dem zahlreiche Verstärkungen und Dämpfungen vorkommen, müssen die Einzelergebnisse nur addiert bzw subtrahiert werden, um ein Ergebnis zu erhalten. Komplexere Multiplikationen und Divisionen, die Rundungsfehler mit sich bringen, können dadurch vermieden werden.

Für das Rechnen mit dem Dezibel gibt es die folgende Vereinfachung: alle drei Dezibel verdoppelt sich die Verstärkung bzw halbiert sich die Dämpfung.

4.2.1 Absoluter Pegel

In obiger Erklärung wurde der relative Pegel verwendet, das heißt, dass der Leistungspegel einen beliebigen Wert annehmen kann. Der absolute Pegel hingegen bezieht sich auf ein

festgelegtes System aus Widerstand, Spannung und Leistung. Die Hochfrequenzübertragungstechnik verwendet als Leistungsbezug 1 mW an 75 Ω. Die Bezugsspannung beträgt 274 mV. Der Verstärkungs- oder Dämpfungsfaktor wird in dBm angegeben.

4.3 Elektrische Filter

Ein elektrisches Filter ist eine Schaltung, die bestimmte Frequenzen abschwächt. Passive Filter benötigen keine externe Stromversorgung und können aus einer Kombination von Spulen und Kondensatoren (LC-Filter) oder aus einer Kombination von Widerständen und Kondensatoren (RC-Filter) aufgebaut werden. Sie können nur zur Frequenzselektion verwendet werden, das heißt nur für das Filtern eines Signals. Der Einsatzbereich passiver Filter erstreckt sich über den gesamten, technisch nutzbaren Frequenzbereich. Aus diesem Grund sind sie für die Hochfrequenztechnik von großer Bedeutung.

Aktive Filter hingegen benötigen eine externe Stromversorgung. Sie bestehen aus einer Kombination von Operationsverstärkern, Widerständen und Kondensatoren und ermöglichen sowohl Frequenzselektion als auch Signalverstärkung. Die verwendeten Operationsverstärker legen die obere Grenzfrequenz fest, die zwischen 100 kHz und 1 MHz liegen kann. Dabei ist zu beachten, dass die Kosten mit der Höhe des Frequenzbereichs steigen. Aus diesem Grund können aktive Filter nur bis zu einem bestimmten Frequenzbereich wirtschaftlich hergestellt werden. Ein weiterer Nachteil gegenüber passiven Filtern ist die Empfindlichkeit von Operationsverstärkern gegenüber Temperaturveränderungen.

Im Folgenden werden Tiefpass-, Hochpass- und Bandpass-Filter nur kurz vorgestellt, da diese Arbeit ein grundlegendes Verständnis voraussetzt.

Tiefpass-Filter dämpfen Frequenzen oberhalb der Grenzfrequenz f_g während sie niedrigere Frequenzen kaum oder überhaupt nicht dämpfen. Die Güte eines Tiefpass-Filters wird durch die Steilheit der abfallenden Flanke der Filterkurve bestimmt. Dabei gilt: Je steiler die Flanke, desto höher die Güte. In der Funktechnik werden Tiefpass-Filter vorwiegend zur Dämpfung von Oberwellen[12] eingesetzt.

Das Hochpass-Filter ist das Gegenstück zum Tiefpass-Filter. Es dämpft Frequenzen unterhalb der Grenzfrequenz f_g.

Bandpass-Filter werden verwendet, um ein bestimmtes Frequenzband durchzulassen. Der grundlegende Aufbau besteht aus zwei Parallelschwingkreisen und einem Reihenschwingkreis. Die Güte der einzelnen Schwingkreise bestimmt die Frequenzselektivität. Bandpass-Filter finden in Sendern und Empfängern Anwendung.

[12] Oberwellen sind Vielfache der Trägerfrequenz und würden ohne Dämpfung zusammen mit dem Signal gesendet werden, was eine Störung anderer Funkfrequenzen zur Folge haben kann.

4.4 Oszillatoren und Signalgeneratoren

Oszillatoren stellen das zentrale Element in Sendern und Empfängern dar. Sie werden zur Erzeugung der Trägerfrequenzen sowie für die Modulation und Demodulation verwendet. Für die kommenden Erläuterungen werden die folgenden zwei Eigenschaften definiert:

Oszillatoren erzeugen ein sinusförmiges Ausgangssignal und Signalgeneratoren erzeugen Ausgangssignale, die sich deutlich von sinusförmigen Signalen unterscheiden.

Oszillationen sind sich wiederholende zeitliche Veränderungen. Man unterscheidet dabei zwischen mechanischen Oszillatoren, wie dem Faden- oder Federpendel, und elektronischen Oszillatoren, wie Resonanzkreise aus LC-Gliedern oder Quarzoszillatoren. Erstere führen Pendelbewegungen durch während letztere ein periodisches elektromagnetisches Wechselfeld erzeugen.

4.4.1 Grundschaltungen von Oszillatoren

Oszillatoren bestehen im Allgemeinen aus einem Verstärker und einem frequenzbestimmenden Bauteil, wie LC-Glieder oder Quarze.

In einem Oszillator wird ein Teil des Ausgangssignals auf den Verstärkereingang zurückgeführt. Dieses Prinzip wird Rückkopplung genannt. Dabei wird zwischen der Gegenkopplung und der Mitkopplung unterschieden. Bei ersterem hat das Rückkopplungssignal eine entgegengesetzte Phasenverschiebung zum Eingangssignal, wodurch eine Dämpfung stattfindet. Bei der Mitkopplung hingegen ist das Rückkopplungssignal in Phase mit dem Eingangssignal. Der Oszillator beginnt selbstständig zu schwingen, wenn die Mitkopplungsspannung gleich der Eingangsspannung ist.

Dieser Sachverhalt soll mit einem kleinen Beispiel illustriert werden. Der Verstärker weist einen Verstärkungsfaktor V von 50 auf. Die Ausgangsspannung beträgt 100 mV und der Kopplungsfaktor K beträgt 2%. Dadurch werden 2 mV auf den Eingang des Verstärkers zurückgekoppelt, genauer gesagt mitgekoppelt. Aufgrund der Verstärkung liegen am Ausgang wieder 100 mV.

Es lässt sich folgende Bedingung für die Erzeugung von Schwingungen festlegen:

$$V * K = 1$$

Oszillatoren können auch ohne ein Eingangssignal zu schwingen beginnen. Dazu muss am Verstärker eine Spannung angelegt sein, die durch das Eigenrauschen des Verstärkers am Ausgang eine sogenannte Rauschspannung bewirkt. Über die Mitkopplung und die Verstärkung wird die Ausgangsspannung so lange erhöht, bis der Verstärker begrenzt. Die Schaltung beginnt dann zu schwingen, wenn der Kehrwert des Rückkopplungsfaktors kleiner ist als der Verstärkungsfaktor:

$$V * K > 1$$

Die Art der erzeugten Signale wird durch die frequenzbestimmenden Komponenten von Oszillatoren bestimmt. LC-Oszillatoren und Quarzoszillatoren erzeugen Sinus-Schwingungen, RC-Oszillatoren erzeugen symmetrische und asymmetrische Rechteck- und Dreiecksignale.

4.5 Antennen und Antennengewinn

Werden die Kondensatorplatten eines geschlossenen Schwingkreises voneinander entfernt, so bildet sich ein offener Schwingkreis. Dadurch vergrößert sich die räumliche Ausdehnung des elektrischen Feldes; sie ist maximal, wenn die Kondensatorplatten voneinander wegweisen, wie in Abbildung 4-1 zu sehen ist.

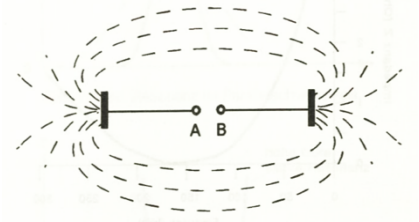

Abbildung 4-1: Offener Schwingkreis [L95]

Abbildung 4-1 zeigt die einfachste Form eines offenen Schwingkreises, den Dipol. Entfernt man davon zusätzlich die Kondensatorplatten, so ergibt sich die Grundform der Antenne (Abbildung 4-2). Dabei bestimmen die Länge und der Durchmesser des Dipols die Induktivität, Kapazität und den ohmschen Widerstand. Zusätzlich definiert die Länge des Dipols dessen Resonanzfrequenz.

Wird der Dipol von einem hochfrequenten Wechselstrom durchflossen, bauen sich abwechselnd magnetische und elektrische Felder auf, lösen sich vom Dipol als elektromagnetische Wellen ab und breiten sich im Raum aus.

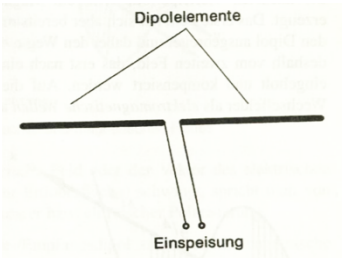

Abbildung 4-2: Grundform der Antenne [L95]

Theoretisch strahlt eine Antenne elektromagnetische Wellen gleichmäßig in alle Richtungen ab. Das räumliche Strahlungsbild (Strahlungsdiagramm) einer solchen Antenne würde eine perfekte Kugel zeigen. Antennen mit dieser Eigenschaft werden isotrop genannt, sind aber in der Praxis nicht realisierbar, weil jede Antenne in einer bestimmten Richtung mehr Strahlungsleistung abgibt. Diese Richtung wird Hauptstrahlrichtung genannt.

Der Antennengewinn beschreibt das Verhältnis der Strahlungsleistung einer bestimmten Antenne zur Strahlungsleistung einer Bezugsantenne in Dezibel. Ist die Bezugsantenne die isotrope Antenne, so wird der Gewinn in dBi angegeben.

Es ist wichtig zu erkennen, dass der Antennengewinn allein auf der Fokussierung der zugeführten Hochfrequenzenergie in eine bestimmte Richtung beruht und nicht auf einer

Verstärkung der elektromagnetischen Energie. Diesen Sachverhalt soll das folgende Beispiel illustrieren.

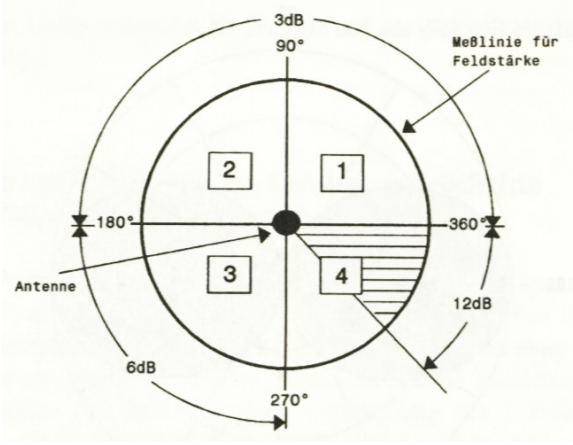

Abbildung 4-3: Antennengewinn [L95]

Abbildung 4-3 zeigt den horizontalen Schnitt einer Antenne, deren Abstrahlung in vier Sektoren unterteilt wurde. Der Kreis beschreibt den Ort der Messung. Ein isotroper Strahler würde in allen vier Sektoren die gleiche Leistung aussenden. Strahlt jedoch eine Antenne diese Leistung nur in den Sektoren 1 und 2 ab, so wird ein Gewinn von 3 dB erzielt. Wird die Leistung weiter auf den Sektor 3 reduziert, so steigt der Gewinn auf 6 dB. Wird das Abstrahlen auf einen Bereich fokussiert, der der Hälfte des vierten Sektors entspricht, wird ein Gewinn von 12 dB erreicht.

Die wirksame Strahlungsleistung (Equivalent Radiated Power) einer Antenne setzt sich aus dem Produkt der Leistung und dem Gewinn einer Antenne zusammen. Strahlt eine Antenne mit einem Gewinn von 10 dBi eine Leistung von 15 W ab, ist die wirksame Strahlungsleistung 150 W. Aufgrund der Reziprokität gilt der Gewinn einer Sendeantenne auch für die Empfangsantenne.

4.6 Elektronisches Rauschen

Rauschen ist ein Signal, das durch Störspannungen erzeugt wird und das Informationssignal überlagert. Bei Antennen tritt unter anderem das elektromagnetische Rauschen auf. Dieses wird bedingt durch Einflüsse von außen, wie kosmischer Hintergrundstrahlung, Solar Flares, Blitzentladungen bei Gewittern sowie elektrischen Geräten. Es werden verschiedene Arten von Rauschen unterschieden, diese sind aber nicht Bestandteil dieser Arbeit.

Elektromagnetisches Rauschen bestimmt in Bezug auf Funkübertragungen die Qualität des übertragenen Signals. Damit ein Empfänger ein Nutzsignal korrekt auswerten kann, muss der Pegel über jenem des Störsignals liegen. Das Verhältnis von Nutzsignalleistung zu Störsignalleistung ist der Störabstand S, auch genannt signal to noise ratio (SNR). Der Wert wird in Dezibel angegeben.

5. SIGNALE

5.1 Signalformen

In Kapitel 3.3 wurde der Schwingkreis erklärt, der aufgrund der Verluste in der Spule und im Kondensator eine gedämpfte Sinus-Schwingung erzeugt. Diese gedämpfte Sinus-Schwingung ist in Abbildung 5-1 dargestellt. Dieser Dämpfung kann durch andauernder Energiezufuhr entgegengewirkt werden. Dadurch wird eine kontinuierliche Sinus-Schwingung erzeugt, wie in Abbildung 5-2 zu sehen ist.

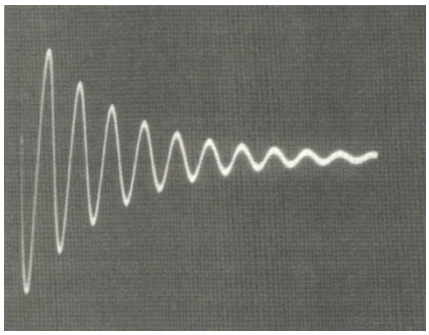

Abbildung 5-1: Gedämpfte Schwingung [L95]

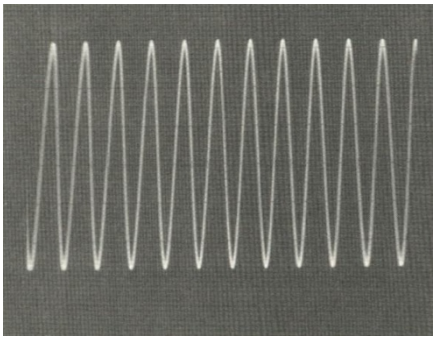

Abbildung 5-2: Kontinuierliche Schwingung [L95]

Die Sinus-Schwingung stellt die am häufigsten vorkommende Signalform dar. Sie wird neben anderen wichtigen Signalformen in Abbildung 5-3 gezeigt.

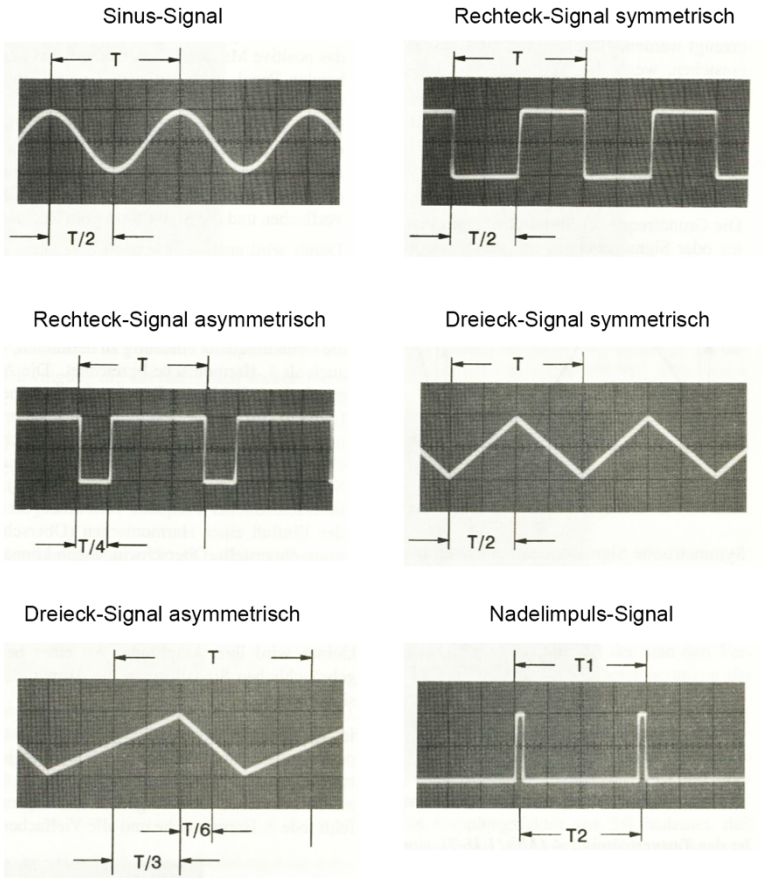

Abbildung 5-3: Signalformen [L95]

Ohne Dämpfung durch Tiefpassfilter würden die sogenannten Oberschwingungen gemeinsam mit der Trägerfrequenz übertragen werden, was zu einer Störung des Funkverkehrs führen kann. Werden Signale erzeugt, die keine reine Sinus-Schwingungen sind, entstehen Oberschwingungen. Diese werden auch als Harmonische der Grundfrequenz bezeichnet und sind Frequenzen, die ein Vielfaches der Grundfrequenz betragen. Die Grundfrequenz, auch als 1. Harmonische bezeichnet, eines Oszillators weist die maximale Amplitude auf. Harmonische einer Grundfrequenz sind durch kleinere Amplituden charakterisiert. Dabei gilt: Je höher die Zahl der Harmonischen, desto geringer die Amplitude. Zusammen mit der Grundfrequenz prägen sie das Aussehen der Signalform. Die Signalform wiederum definiert die Harmonischen, deren Amplitude sowie deren Phasenbeziehung. Abbildung 5-4 zeigt die Veränderung einer Grundschwingung durch eine Oberschwingung.

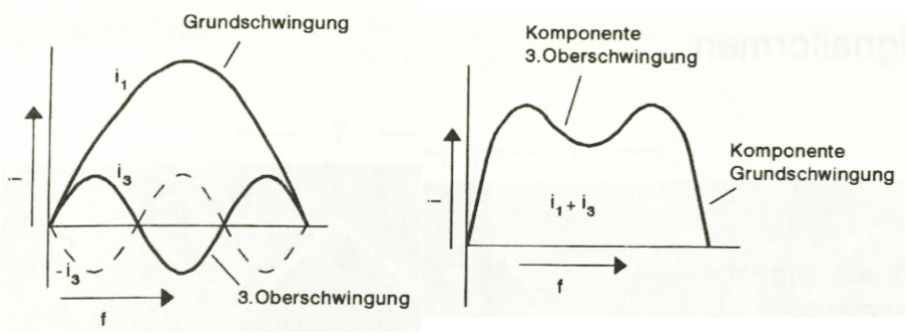

Abbildung 5-4: Veränderung der Grundschwingung durch eine Oberschwingung [L95]

5.2 Modulation und Demodulation analoger Signale

Modulation ist die Veränderung eines Trägersignals durch die zu übertragenden Informationen. Demodulation ist die Extraktion der ursprünglichen Informationen aus dem übertragenen Signal. Diese Technik ist notwendig, um gegenseitigen Beeinflussungen mehrerer Sender entgegenzuwirken.

Die Amplituden- und Frequenzmodulation werden in der Bachelorarbeit 2 vorgestellt.

5.3 Digitalisierung analoger Signale

Aufgrund der eingeschränkten Möglichkeiten der Analogtechnik, ein bestimmtes Maß an Qualität wirtschaftlich zur Verfügung zu stellen, hat sich die Digitaltechnik durchgesetzt. Beispielsweise können in der Analogtechnik Störungen nur auf Kosten der Frequenzbandbreite beseitigt werden. Digitale Modulationsverfahren hingegen zeichnen sich durch eine wesentlich bessere Ausnutzung des Frequenzspektrums aus. Zudem können die Sendeleistungen aufgrund der Verbesserung des SNR verringert sowie neue Möglichkeiten zur Fehlererkennung und Fehlerkorrektur genutzt werden. [L95]

Aus diesen Gründen werden digitale Signale für Funkübertragungen gewählt. Diese werden aus analogen Signalen erzeugt. Damit der Mensch die Information interpretieren kann, muss nach der Übertragung das digitale Signal wieder in ein analoges umgewandelt werden. Für die Umwandlungen werden Analog-/Digitalwandler (A/D-Wandler) und Digital-/Analogwandler (D/A-Wandler) verwendet. [L95]

A/D-Wandler & D/A-Wandler sowie die Modulation analoger und digitaler Signale werden in der Bachelorarbeit 2 behandelt.

6. KONKLUSION

Diese Bachelorarbeit lieferte einen grundlegenden Überblick über elektromagnetische Wellen, elektronische Komponenten zur Signalerzeugung, Signalverarbeitung sowie Signalübertragung, Software Defined Radios, Signale und deren Modulationstechniken.

Im ersten Kapitel wurden die elektromagnetischen Wellen behandelt. Es ging um elektrische und magnetische Felder sowie um die Erzeugung dieser Wellen durch Schwingkreise. Abschließend wurde die Ausbreitung der Wellen erklärt, die sich je nach Frequenz unterschiedlich verhält.

Im nächsten Kapitel folgte das Software Defined Radio. Dabei wurden grundlegende Hardwarekomponenten wie FPGAs, elektrische Filter, Oszillatoren und Antennen erläutert. Da im Gebiet der Kommunikation das Dezibel die zur Messung der Signalstärke verwendete Einheit ist, wurde es in diesem Kapitel ebenso behandelt.

Zentrales Thema des letzten Kapitels „Signale“ waren die Modulationsarten von analogen und digitalen Signalen.

Der Inhalt dieser Bachelorarbeit wird im Wiki des Embedded Lab Vienna for IoT & Security (ELVIS) veröffentlicht.

7. VORSCHAU

Software Defined Radios ermöglichen eine neue Art des Pentestings. Während man vor einiger Zeit noch spezielle Hardware benötigte, die auf ein enges Frequenzspektrum limitiert war, so sind mit SDRs der Kreativität keine Grenzen mehr gesetzt. Für nur wenige hundert Euros bekommt man ein Gerät, das im Frequenzbereich aller gängigen Kommunikationsprotokolle operiert. Egal ob es sich dabei um das Funkgerät zum Öffnen des Garagentors, um Türschlösser oder um Autos handelt, denn eines haben sie alle gemein: sie kommunizieren drahtlos.

Durch den Vormarsch der IoT-Geräte und den – nachgewiesenen – kritischen Sicherheitslücken ebendieser sind mit Software Defined Radios krimineller Energie – im wahrsten Sinne des Wortes – Tür und Tor geöffnet. Und das mit einer einmaligen Investition! Denn den Kern der SDRs stellen sogenannte FPGAs dar. Diese logischen Bausteine lassen sich je nach Bedarf programmieren, sei es, dass man im Frequenzbereich von 300 MHz, in dem Garagentoröffner arbeiten, mitschneiden will, oder sei es, dass man im Bereich von 2,4 GHz operiert, um das „smarte“ Türschloss zu öffnen. Mit einem einfachen Klick lädt man die entsprechende Software auf das SDR und kann sich auf das Ziel fokussieren.

Zahlreiche Berichte belegen, dass oben genanntes keine Phantastereien sind: Tobias Zillner hat bereits 2015 demonstriert, wie sich ein smartes Türschloss, das mit ZigBee kommuniziert, illegal öffnen lässt[13]. Samy Kamkar erklärte in einer Präsentation auf der DEF CON, wie man das Signal eines Garagentoröffners mitschneidet und erneut sendet und sich so illegal Zugang verschaffen kann[14]. Zudem zeigte er eine Methode, um Autos mit einem SDR aufzusperren. Dabei umgeht er die präventative Maßnahme des Rolling Codes der Autohersteller[15].

Die Gefahr liegt im Konkurrenzdruck des freien Marktes. Die Hersteller von IoT-Geräten versuchen sich in diesem Segment zu etablieren und streben die Marktherrschaft an. Durch diesen Druck liegt der primäre Fokus allerdings nicht auf der Implementierung von

[13] https://www.youtube.com/watch?v=F1bq4oj5quw, abgerufen am 10.12.2018

[14] https://www.youtube.com/watch?v=UNgvShN4USU, abgerufen am 10.12.2018

Sicherheitsmaßnahmen. Außerdem wird die Interoperabilität und Einfachheit vor die Sicherheit gestellt. Dies sind Gründe für die drastischen Sicherheitslücken, die die meisten der IoT-Geräte aufweisen. Nun liegt es an den Penetration-Tester und Sicherheitsexperten, diese Geräte zu testen und die Lücken den Herstellern zu melden, bevor sie von Kriminellen genutzt werden kann. Das ist jedoch nicht immer so einfach, wie von Samy Kamkar in seiner Präsentation beschrieben. Er hat eine Sicherheitslücke in der Smartphone App RemoteLink von OnStar entdeckt, mit der sich ein Chrysler unerlaubterweise entsperren ließ. Er kontaktierte sodann GM, wurde aber vom technischen Support zurückgewiesen, bis er endlich einen Sicherheitsexperten der Firma erreichte. Dieser kümmerte sich um das Problem und die Lücke wurde so bald wie möglich geschlossen[15].

Penetration Tests mit SDRs sind ein spannendes Thema, noch dazu hat man als Tester eine beinahe unbegrenzte Auswahl an zu untersuchenden Geräten. Man könnte sogar von einer Spielwiese sprechen.

Aus diesem Grund wird in der Bachelorarbeit 2 auf die praktische Anwendung von Software Defined Radios eingegangen. Anhand des bladeRF von Nuand werden die Installation in einer Linux-Umgebung sowie erste Schritte der Frequenzanalyse erklärt. Das Ziel der Arbeit ist das Abfangen des Signals eines Garagentoröffners und das erneute Abspielen, um die Garage zu öffnen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bücher

[L95] Lobensommer, H.: Handbuch der modernen Funktechnik: Prinzipien, Technik, Systeme und praktische Anwendungen. Franzis-Verlag GmbH, Poing, 1995.

[CGPW18] Collins, T., Getz, R., Pu, D., Wyglinski, A.: Software-Defined Radio for Engineers. Artech House, 2018.

[M14] Moore, A.: FPGAs For Dummies, Altera Special Edition. John Wiley & Sons, Inc., Hoboken, 2014.

[B06] Beuth, K.: Digitaltechnik: Elektronik 4. Vogel Industrie Medien GmbH & Co KG, Würzburg, 2006.

[P07] Prösch, R.: Technical Handbook For Radio Monitoring I. Books on Demand GmbH, Norderstedt, 2007