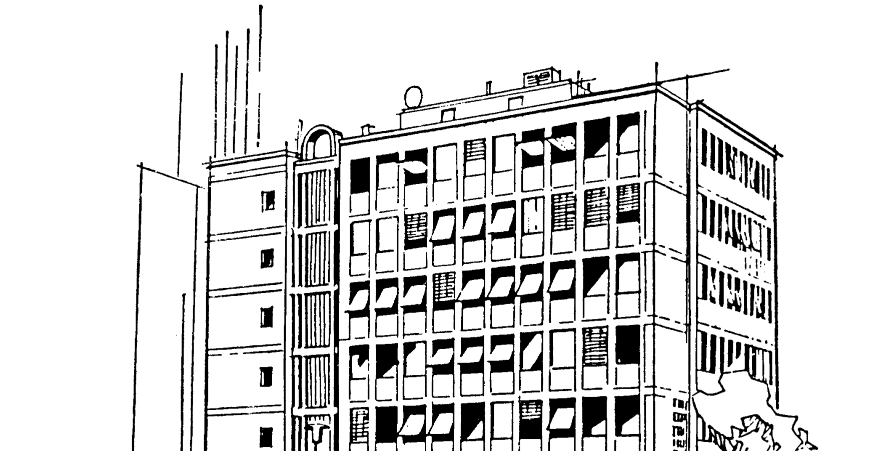
# MASTER'S THESIS

Tasnad Kernetzky

# Evaluation of Power Line Communication Technologies



Technical University of Munich
Inst. f. Communications Engineering
Prof. Dr. sc. techn. Gerhard Kramer

Master's Thesis

# Evaluation of Power Line Communication Technologies

Tasnad Kernetzky

Munich, November 2014

Supervised by
Dr.-Ing. Xi Zhang, Siemens AG
&
Prof. Dr.-Ing. Norbert Hanik, TU Munich

Master's Thesis at the
Department for Wireline Transmission Technology (LÜT),
Institute for Communications Engineering (LNT),
Technical University of Munich (TUM)
Title: Evaluation of Power Line Communication Technologies
Author: Tasnad Kernetzky

Tasnad Kernetzky
Registration number 03607213
Senftlstr. 1a
81541 München
tasnad@mytum.de

Ich versichere hiermit wahrheitsgemäß, die Arbeit bis auf die dem Aufgabensteller bereits bekannte Hilfe selbständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderung entnommen wurde.

I assure the single-handed composition of this Master's thesis, only supported by declared sources.

München, 8.4.2016
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Place, Date (Tasnad Kernetzky)

# Abstract

The idea to transmit data over existing power line grids already arose in the nineteenth century. Power Line Communication systems have been actively developed since the 1920s and are used for transmissions with low data rates over long distances and with high data rates for local networks. Since then, many different specifications were released. Current research topics include gigabit class MIMO concepts on the one hand and low power solutions deployed in Smart Grid applications on the other hand.

This thesis consists of three parts; the first one gives an overview of power line communication technologies, with a strong focus on the HomePlug standard – including a description of its physical and media access layers. The second part summarizes broadband power line communication channel models found in literature and introduces a simulation based on one of them with channel measurements in different setups. Finally, the third part presents network throughput measurements performed under different conditions and with two types of HomePlug modems.

# Zusammenfassung

Die Idee, Daten über vorhandene Stromnetze zu übertragen entstand bereits im neunzehnten Jahrhundert. Stromnetz-Trägerfrequenzanlagen unterschiedlichster Art werden seit den 1920er Jahren aktiv erforscht und für Übertragungen mit niedrigen Datenraten über weite Strecken und hohen Datenraten in lokalen Netzwerken eingesetzt. Seitdem wurden viele Spezifikationen veröffentlicht. Aktuelle Forschungsthemen umfassen einerseits MIMO Konzepte mit Datenraten von bis zu einem Gigabit pro Sekunde und andererseits energiesparende Systeme für den Einsatz innerhalb des Smart Grids.

Diese Arbeit besteht aus drei Teilen, wobei der Erste einen Überblick über Stromnetz-Trägerfrequenzanlagen mit Fokus auf den HomePlug Standard gibt und ebenfalls eine Bescheibung seiner Bitübertragungs- und Medienzugriffssteuerungsschichten umfasst. Der zweite Teil stellt einige in der wissenschaftlichen Literatur veröffentlichten Kanalmodelle für breitbandige Stromnetz-Trägerfrequenzübertragungen kurz vor und umfasst desweiteren sowohl eine Simulation, die auf einem dieser Modelle aufbaut, als auch Methoden zur Vermessung von Kommunikationskanälen. Schließlich präsentiert der dritte Teil Ergebnisse von Netzwerk-Durchsatzmessungen, die unter unterschiedlichen Bedingungen und mit zwei verschiedenen HomePlug Modems erzielt wurden.

# Contents

# 1 Introduction

Power Line Communication (PLC) is a generic term for transmitting information over Alternating Current (AC) and Direct Current (DC) power lines with High Voltage (HV) ($\approx 50kV$ to $1000kV$), Medium Voltage (MV) ($\approx 1kV$ to $50kV$), Low Voltage (LV) ($< 1kV$) or no voltage at all. Using power wires for communication has two main benefits. Firstly, it is a spare transmission channel already installed, mostly unoccupied, ready to use and reaching each non-mobile device. Secondly, it can be less expensive compared to other wireline communication systems, where additional wires have to be installed.

The generic idea of PLC dates back at least to 1838, when performing remote metering of batteries over power lines was proposed [Bro99, Chapter 'Early history' p. 2]. Later, the first commercial telephone system over MV power lines was built in Japan in 1918 [Sch09, p. 1], using a simple method to couple the information signal into power wires.[1] Some years later, HV capacitors became available and were increasingly used for a more efficient coupling method[2] [Sch09, Chapter 'Carrier Wave Telephony over Power Lines Comes of Age' p. 16 f.], which is still in use today and discussed in Chapter 3.1.1.4.

PLC systems can be divided in four big categories:
*Ultra narrowband* PLC long haul networks, which are able to transmit data over long distances of up to some hundred kilometers by using only frequencies below $3kHz$. As communication is very slow over the ultra narrow band, the main purpose of this technology is telemetering and the switching of distant, power demanding loads like street lights and air conditioners [GSW11, Chapter `II A-B` p. 1001 f.].
*Narrowband* PLC networks for building automation purposes. The utilized frequency band makes it possible to create a network with ample performance to control many devices in the building including lighting, heating, washing machines et cetera.

[1] A long wire wound around the power line was used to inductively couple High Frequency signals. While this is an easy to achieve and secure method, its coupling efficiency is bad. Where coupling over wires achieves an efficiency of about 7%, the capacitor method reaches values above 80% [Bel27].

[2] A patent demonstrating coupling carriers into power lines by using capacitors was filed in 1924 [Str25].

*Broadband access* PLC networks [LWR03], which are used for the so-called *last mile*[3] of the internet, as an alternative or addition to other connections, such as Digital Subscriber Line (DSL). Internet over power lines is a niche market, as indicated by the listing of PLC access in all U.S. federal states [And14]. There are only customers in two states, Broadband over Power Lines (BPL) connections in Ohio and Illinois sum up to 1.6 and 0.1 percent of the market share, respectively.

*Broadband local area* PLC networks [GSW11, Chapter `II C` p. 1002 f.], competing with wired and wireless Local Area Networks (LANs) where additional cabling is unfeasible or unwanted and wireless connectivity is bad. The usage of a broad spectrum enables communicating with up to gigabit class data rates, but reduces the transmission range.

Many applications of the four PLC categories mentioned above have been discussed and deployed in the context of *Smart Grid*, a hot topic in todays research and the power infrastructure of the future. Different power distribution segments require distinct PLC technologies:

HV power lines have been used for ultra narrowband PLC links interconnecting distinct segments of the power distribution control network. With a PLC approach, it is also possible to analyze the sanity of a power wire [GSW11, Chapter `V A` p. 1010].

In the MV grid, PLC is mainly used for health reports of aging devices and for islanding control[4] [GSW11, Chapter `V B` p. 1011], simply by adding and checking for a High Frequency (HF) carrier on the power line [BCC03].

Finally, usages of PLC in the LV network include smart metering[5], car-to-grid communication during charging of electrical vehicles, Demand Side Management (DSM)[6] and home energy management systems, which are similar to DSM, but use PLC only for in-home connections and not for the communication with the power supplier [GSW11, Chapter `V C` p. 1011 f.].

[3] The *last mile* is the connection between the endpoint of the optical backbone network and the LAN of the customer.

[4] Islanding is a phenomenon, which occurs when switching off the last access point from the HV to a certain MV network, creating an isolated sub grid with perhaps only one generator. As small islands likely give rise to voltage and frequency fluctuations, they should be avoided and if incidentally created, immediately detected and reconnected to the HV grid.

[5] Smart metering refers to remotely reading power meters of customers, but also to transmitting pricing information and other data in the opposite direction.

[6] DSM is the possibility to activate spread loads (e.g. charging of electrical cars) when much power is available due to fluctuating sources like solar and wind power plants and turning them off, if there is a load peak in the grid or a power shortage.

Besides various applications in the Smart Grid, PLC is becoming more and more popular as an alternative to private networks based on established wired and wireless (typically Ethernet) technologies in the last decade. Compared to the star topology of usual LANs, the undemanding mesh-like interconnection of a PLC system needs no extensive cabling and is therefore a cheap and easy to set up alternative. Although Wireless Local Area Networks (WLANs) have these benefits as well, they have two major disadvantages, too. Firstly, the nature of Radio Frequency (RF) communication implies, that some parts of the intended coverage area can be obscured by obstacles and only reached by additional repeaters. Secondly, the $2.4GHz$ frequency band needed by the widely used IEEE 802.11 compliant wireless devices is very crowded, especially in urban areas[7] [BHC04].

It should be pointed out that PLC networks also suffer from interference, as the transmission medium – the power line grid – is shared between all neighboring transceivers able to hear each other. Although inevitable, this weakness can be overcome by creating distinct networks which can use the full bandwidth and yet cause no mutual interference to each other. Whereas this is nearly impossible for wireless solutions, the power line can be segmented by low pass filters.[8]

Industry automation is another area where local BPL can be used, the fact of not having to introduce new wires is the main reason to prefer it over other technologies. One example is controlling single units of an airfield ground lighting through PLC, a simulation on this topic can be found in [BLH10]. There are many other possible applications of PLC. It can be used for building automation [SK96], i.e. to control domestic appliances, lighting and heating. There is a recent approach to remove large parts of wirings in cars by controlling nodes over their power wires [GKLK14], streaming of audio & video media, distributed sensor & actor networks in factories, et cetera.

As with any other technology, there are also downsides of (especially broadband) PLC. Power lines were not designed to carry high frequencies at all. Properties of the medium which deeply affect communication, are a high attenuation through radiation, impedance mismatches at grid junctions [ZD02, Chapter `II A` p. 1001 f.], loads with partly unpredictable impedances being added to and removed from the grid [CCDE11, Chapter 'Loads Model' p. 167 f.], [CDCE02, Chapter `III B` p. 1003 f.] and periodical, as well as impulsive noise [WBD98, Chapter 3.2 p. 74 f.], [CDCSM10]. Modern PLC systems overcome this

[7] The $5GHz$ band is an alternative, though it is only supported by few devices so far and is likely to be more crowded in the future.

[8] Communication is performed on frequencies much higher than the $50Hz/60Hz$ mains voltage, thus a low pass filter is enough to prevent the signal from propagating to alien networks.

deficiency with frequency selective modulation formats[9], advanced error correction and regular channel estimations. Especially the fact that power lines have to be treated as antennas in the HF range and radiate parts of the signal's power to the environment, gave rise to much criticism of BPL. Amateur radio operators claim that it could cause harmful interference to several of their services in frequency bands between $1MHz$ and $30MHz$, where most BPL systems operate. In 2002, where PLC access networks were discussed intensely, an estimation of radiation has been made [Har02, p. 26 f.]. Considering an exaggerated number of up to one million simultaneous PLC connections, the authors came to the result that interference can be caused even to receivers "outside the communities in which they [the transmitters] are deployed" [Har02, p. 27]. BPL opponents even created a web site [Hen14] in order to present their discontentment regarding PLC radiations.

However, the fact that power wires act as antennas has been considered during the design of BPL systems, leading to notches in the allowed transmission spectrum. This approach mitigates the interference to amateur radio and other services located there. Measurement results can be found in [MRI03], where a network analyzer was used to record the transfer function of a link consisting of a power line and a receiver antenna in the $1MHz$ to $30MHz$ band, comparing the caused radiation to certain limits in international standards. Although the measurement indicates that some of the norms could be violated, using notches seems a satisfying approach to amateur radio operators. As long as the transmitters do not exceed legal radiation limits, no harmful interference in the forbidden bands can be measured [Foc03]. Similar results are reported by an experiment, where Korean radiation limits are fulfilled by using PLC modems of types not further described [RRP08].

The focus of this work lies on the evaluation of broadband power line communications for LANs, with regard to operation performance and channel characteristics. In the next chapter, an overview of current PLC technologies is given, which is then followed by a technical description of the HomePlug specification. In Chapter 4, a channel model and different power line measurements are presented. The last chapter is devoted to performance measurements of PLC links under varied conditions and the description of the used testing environment. Finally, the main results of this thesis are summarized and an outlook of future work is given.

[9] Most BPL modems use Orthogonal Frequency Division Multiplexing (OFDM) to achieve a high spectral efficiency and to be able to cancel transmission in certain frequency ranges.

# 2 Overview of Power Line Communication Technologies

Over the years, many types of PLC systems have been developed and there is more than one way to categorize them. In this chapter PLC systems are grouped according to their used frequency bands: *Ultra narrowband*, *Narrowband* and *Broadband* technologies. Each category has many different members and some of them are not even used any more. Furthermore, one interesting competing technology is Power over Ethernet (PoE) [IEE09], which is an opposite approach – power is distributed over Ethernet wirings. As the technology behind PoE is completely different from PLC, it is not further addressed in this thesis and just mentioned for completeness. A thorough overview of PLC technologies can be found in Figure 2.1 and also in [FLNS11], this chapter only describes the most important ones.

Three terms have to be defined here, namely Physical (PHY) layer, Media Access Control (MAC) layer and Orthogonal Frequency Division Multiplexing (OFDM). PHY refers to the lowest layer of the Open Systems Interconnection model (OSI), providing Forward Error Correction (FEC), scrambling, interleaving, modulation and finally the physical transmission of data. MAC refers to the second OSI layer, providing mainly channel access mechanisms, addressing of destination nodes and data sanity checks (e.g. appending Cyclic Redundancy Check (CRC) sums). OFDM is a modern modulation technique which makes use of the Inverse Discrete Fourier Transform (IDFT) with the Fast Fourier Transform (FFT) algorithm to achieve good spectral efficiencies. For more details, refer to Chapter 3.1.1.2. Furthermore, all discussed data rates in this thesis are theoretical upper limits of the corresponding PHY layer's throughput. To reach these rates, the highest modulation formats[10] have to be used and as few FEC as allowed by the specification. In a real network on a regular power grid, the rates will be much lower, highly depending on the channel's quality and the number of transmitting nodes.

[10] Some specifications have more than one possible mapping of bits to symbols, depending on the measured channel characteristics or operating modes. The term *highest modulation format* refers to the mapping with most bits in one symbol the technology is capable of transcieving.

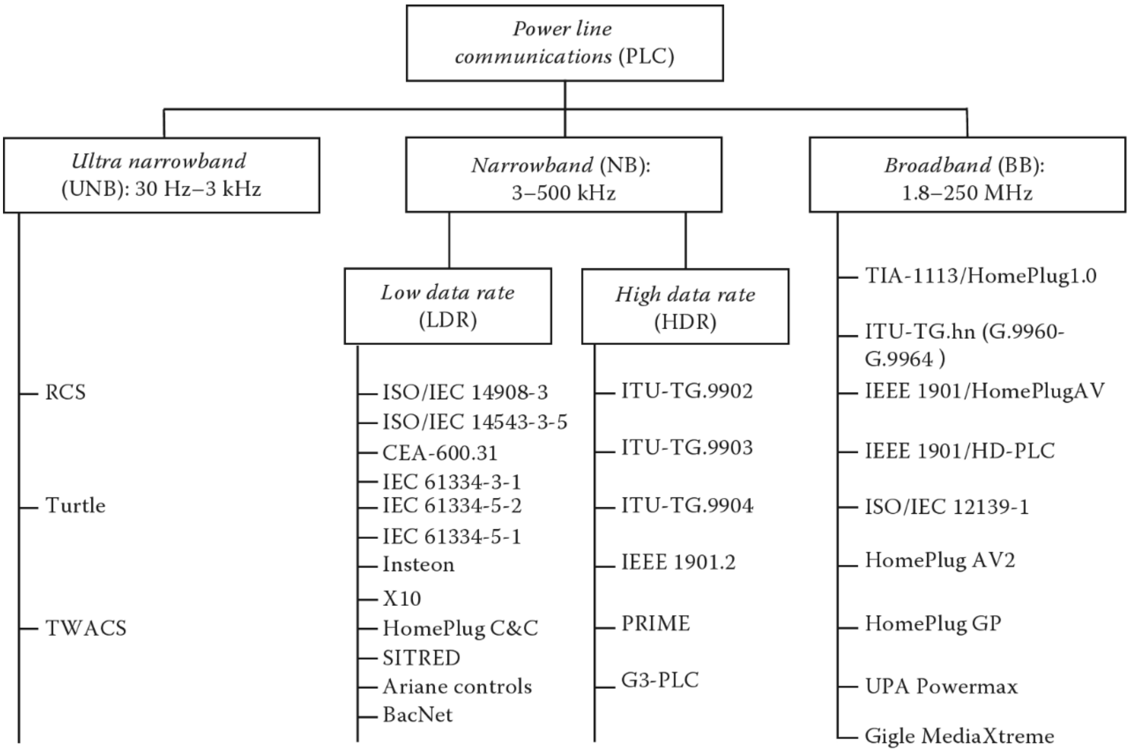


Figure 2.1: Overview of power line technologies, adapted from [BSPS14, Figure 10.1 p. 255].

## 2.1 Ultra Narrowband PLC

Ultra narrowband devices use only the ultra-low frequency band ($300Hz$ to $3kHz$) and the upper part of the super-low frequency band ($30Hz$ to $300Hz$) [BSPS14, p. 253], which is a big advantage for Automated Meter Reading (AMR)[11], Advanced Metering Infrastructure (AMI)[11] and load control purposes. The transmitted signals of these very low frequencies can pass transformers between the LV, MV and even HV grid without the need to install expensive bypass circuits and can reach destinations more than 150km apart [GSW11, I B p. 1000]. A rather old technology (dated back to the 1930s) is Ripple Carrier Signaling (RCS) [Dos97], which is only able to transmit less than a bit per second. More recent systems are Two Way Automatic Communications System (TWACS) [MR82] [MM84] and Turtle [Nor08, IX K p. 10], which both disturb the mains voltage for transmission, but achieve completely different bit rates. Turtle is meant for heavily parallel transmissions, each node sending only 0.001 bit per second, whereas TWACS

[11] The concept of AMR is a one-way communication of water or energy meters to the supplier, AMI extends AMR by a channel back to the devices to be able do deliver pricing information and commands to the customer's devices.

devices can transmit at a data rate up to 120 bits per second [Rie12, Chapter '[0005]' p. 1]. Key attributes of these technologies like frequency range, highest possible modulation format and maximum data rate at the PHY layer are summarized in Table 2.1.

| PLC system | Frequency band $[Hz]$ | Highest modulation format | Maximal PHY data rate $[bit/s]$ |
|---|---|---|---|
| RCS | 125-2000 | ASK | 0.66 |
| Turtle | (-)[12] | Disturbing the mains voltage | 0.001 |
| TWACS | (-)[12] | Disturbing the mains voltage | 120 |

Table 2.1: Key attributes of selected ultra narrowband PLC technologies.

## 2.2 Narrowband PLC

Narrowband communication systems use a subset of the frequency band between $3kHz$ and $500kHz$, depending on the geographical area they operate in. In Europe, radiation limits are regulated by the Comité Européen de Normalisation ÉLECtrotechnique (CENELEC) which defined bands between $3kHz$ and $148.5kHz$. In the U.S. the Federal Communications Commission (FCC) defined the range for PLC communications from $10kHz$ to $490kHz$, the Japanese Association of Radio Industries and Businesses (ARIB) from $10kHz$ to $450kHz$ and the Chinese band goes from $3kHz$ to $500kHz$ [GSW11, p. 1000]. Many authors subdivide narrowband PLC devices in low and high data rate variants. Technologies of the first group operate below $10kbit/s$, some because they are based on outdated technologies and some to achieve a more reliable communication. With modern OFDM based modulations, high data rate narrowband PLC devices operate at up to $800kbit/s$.

The Insteon specification defines a wireless and a PLC PHY layer, the latter able to transmit with ca. $2kbit/s$, using Binary Phase Shift Keying (BPSK) modulation. Regarding the spectral occupation, the Insteon white paper [Ins13] states that a BPSK modulation at $f_0 = 131.65kHz$ with ten zero crossings in one symbol duration ($R = \frac{131.65kHz}{10} = 13.165kHz$) is used. This results in an approximated bandwidth of $B_{\text{M-PSK}} = \frac{2RK}{log_2(M)} \approx 40kHz$ around $f_0$, according to [Coh85, Equation (10) p. 22] if the construction factor

[12] These systems disturb the mains voltage in its zero crossing which makes it impossible to give an exact theoretical bandwidth usage. However, the signaling rate is very slow and the specifications are designed to operate over long distances, thus the occupied frequency range has to be somewhat below $200Hz$.

$K$ is set to its suggested maximum value of $K = 1.5$ and the number of symbols M to $M_{\text{BPSK}} = 2$. A similar home automation technology is KNX (standardized as ISO/IEC 14543-3-5), defining also more than one PHY layer. KNX has two possible slightly different PHY layers which use PLC: *PL-110* and *PL-132*. The former is described in [KNX14, p. 6] and is able to transmit with approximately 1 $kbit/s$. The used modulation format is binary Frequency Shift Keying (FSK) with $f_0 = 105.6kHz$ and $f_1 = 115.2kHz$ to transmit a zero and a one, respectively and a symbol period $T_s = \frac{1}{1200}s$. This results in a center frequency of $f_c = \frac{f_0+f_1}{2} = 110.4kHz$, a frequency deviation of $\Delta f = \frac{f_1-f_0}{2} = 4.8kHz$ and a modulation index $h = 2\Delta f T_s = 8$. The FSK version of Carson's rule $B_{\text{FSK}} \approx \frac{h+1}{T_s}$ [McC10, Equation (5.8) p. 134] yields an approximated bandwidth of $10.8kHz$ around $f_c$. The HomePlug Command & Control specification [Hom08] uses Differential Code Shift Keying (DCSK), which is a spread spectrum modulation format. While data rates are around $7kbit/s$, the spread spectrum nature of DCSK makes communication very reliable [JA09]. The ITU Telecommunication Standardization Sector (ITU-T) made efforts to create the generalized standard G.hnem [ITU12a] [ITU14b] for narrowband PLC systems by defining a highly flexible FFT-OFDM based PHY layer. One configuration is defined in the G.9902 standard, which yields a bit rate of approximately $820kbit/s$ [GMB$^+$14, Table 1 p. 1521]. An overview of G.hnem is found in [OZ11]. The two similar technologies PoweRline Intelligent Metering Evolution (PRIME) [ITU12b] and G3-PLC [ITU14a] are also integrated in G.hnem, realized as configuration parameters of the standard. They are compared in detail in [Hoc11]. While G3-PLC is capable of using the whole FCC band, PRIME is restricted to those defined by CENELEC. An overview of G3-PLC bands and data rates can be found in [BSEG13, Table 4 p. 9]. G3-PLC achieves data rates of up to $300kbit/s$, PRIME about $128kbit/s$. The Institute of Electrical and Electronics Engineers (IEEE) has released its 1901.2 standard, which also aims at unification or at least interoperability of future and present narrowband PLC technologies. The approach is again OFDM based and supports data rates of up to $500kbit/s$, using the FCC band [IEE13]. There are efforts to harmonize IEEE 1901.2 and G.hnem as they are already quite similar [OZ11, p. 37]. Key attributes of all discussed narrowband technologies are summarized in Table 2.2. The list is not complete, several other technologies which are not included are X10, CE-Bus and the Universal Powerline Bus. However, they are somewhat outdated and inferior to the systems described in this chapter.

| PLC system | Frequency band $[kHz]$ | Highest modulation format | Maximal PHY data rate $[kbit/s]$ |
|---|---|---|---|
| Low data rate | | | |
| HomePlug C&C | 100-400 | 6-DCSK | 7.5 |
| Insteon | 112-151 | BPSK | 2.437 |
| KNX (PL110) | 105-116 | BFSK | 1.2 |
| High data rate | | | |
| G.9902 | 34-478 | 256-FFT-OFDM, 16-QAM | 821.1 |
| G3-PLC (FCC) | 10-487.5 | 256-FFT-OFDM, DQPSK | 298 |
| G3-PLC (CENELEC) | 35-91 | 256-FFT-OFDM, DQPSK | 33.4 |
| IEEE 1901.2 | 10-490 | 256-FFT-OFDM, 16-QAM | 500 |
| PRIME | 42-89 | 512-FFT-OFDM, D8-PSK | 128.6 |

Table 2.2: Key attributes of selected narrowband PLC technologies.

## 2.3 Broadband PLC

Broadband PLC systems occupy the frequency range between $2MHz$ and $100MHz$, in rare cases even up to $300MHz$. As these high frequencies do not propagate over long distances in power lines, BPL is restricted to local area networks. However, their broadband nature enables communication with high bit rates, able to compete with Ethernet and IEEE 802.11 wireless networks. The High Definition Power Line Communication (HD-PLC) specification is mainly developed by Panasonic and uses a wavelet OFDM based PHY layer for data rates of up to $240Mbit/s$. An overview of HD-PLC can be found in the white paper [HD-12] and some more details and a comparison with the FFT-OFDM based PHY layer in [GL08, Table 1 p. 70]. The specifications released by the HomePlug Powerline Alliance are described in the Chapter 2.4, including the versions *1.0*, *AV*, *Green PHY* and *AV2*. The International Telecommunication Union (ITU) G.hn and IEEE 1901 standards try to unify the existing BPL technologies. G.hn achieves this through the definition of the new PHY layer G.9960 [ITU11b] with region specific spectral parameters in [ITU11a]. It is able to coexist and share the medium with alien systems like HomePlug and HD-PLC. Occupying the bandwidth of $2MHz$ to $100MHz$, G.9960 is capable of gigabit class data rates. An overview over G.hn can be found in [OG09]. The IEEE 1901 standard [IEE10] defines two PHY layers, an FFT-OFDM based and a wavelet-OFDM based one, derived from HomePlug and HD-PLC, respectively.

The *Inter System Protocol* is also part of the standard, providing coexistence of devices by means of fair medium sharing. Key attributes of broadband PLC technologies are summarized in Table 2.3. Some less common and / or abandoned alternatives such as HomePlug Access BPL, DS2/UPA and Gigle MediaXtream are not included in the list.

| PLC system | Frequency band $[MHz]$ | Highest modulation format | Maximal PHY data rate $[Mbit/s]$ |
|---|---|---|---|
| G.9960 | 2-100 | 4096-FFT-OFDM, 4096-QAM | 1000 |
| HD-PLC | 2-28 | 512-Wavelet-OFDM, 32-PAM | 240 |
| HomePlug 1.0 | 2-28 | 256-FFT-OFDM, DQPSK | 13 |
| HomePlug AV | 2-28 | 3072-FFT-OFDM, 1024-QAM | 197 |
| HomePlug AV2 | 2-86 | 8192-FFT-OFDM, 4096-QAM | 1256 |
| HomePlug Green PHY | 2-28 | 3072-FFT-OFDM, QPSK | 10 |

Table 2.3: Key attributes of selected broadband PLC technologies.

## 2.4 The HomePlug Specification Family

The HomePlug Powerline Alliance was founded in 2000, with the goal to broaden the PLC market and to create a certificate for licensed devices, in order to ensure their interoperability. Today, 60 companies are participating in it, thereunder semiconductor manufacturers, telecommunication companies and others. According to the HomePlug Powerline Alliance in [Hom12a], members of their specification family are utilized by prevalent BPL devices, making up 80% of the world's market share. The rest of this thesis only covers LAN BPL technologies; HomePlug C&C and HomePlug Access BPL are not further described.

The first release was HomePlug 1.0, which is capable of communicating with $13Mbit/s$ and uses the frequency band from $2MHz$ up to $28MHz$. In 2005, the AV specification was released [Hom05] and the data rate increased to $200Mbit/s$, mainly by denser carrier spacing and higher modulation formats. The occupied frequency band remained the same. Later in 2011, the AV2 specification [Hom13] followed and raised the data rate to $2024Mbit/s$[13] [YAA$^+$13, Table 3 p. 19] by extending the frequency range up to $86MHz$, using even higher modulation formats of up to 4096-QAM and a Multiple Input Multiple Output (MIMO) approach by transmitting over the earth wire in addition to the phase and neutral leads. The Green PHY specification [Hom12b] is a variation of HomePlug AV with a reduced data rate of $10Mbit/s$ and increased reliability. It is intended for Smart Grid applications, where high data rates are unnecessary and reliability, low device costs and low power usage are more important.

[13] As with all other systems, the peak data rate of HomePlug AV2 is the theoretical upper limit. To reach it, the transmitter would have to use a 4096-QAM modulation on all carriers, even on those with frequencies up to $86MHz$. Such a frame is very unlikely to be decodable in a realistic power line grid. Field measurements in [Hom13, p. 9] showed a MAC throughput of maximally $500Mbit/s$, though only Single Input Single Output (SISO) capable devices were used.

# 3 Power Line Communication Theory

Although Chapter 2 covered many different PLC technologies, the rest of this thesis only deals with the two related HomePlug specifications AV and Green PHY. Both belong to the category of broadband PLC, operating in the short wave band ($2MHz$ to $30MHz$).[14] This chapter contains figures with recorded waveforms. To acquire them, a probe of an oscilloscope with sampling rate $5GSa/s$ and bandwidth $500MHz$ was connected to the power line network through a capacitor based signal coupling circuit. One plot also contains the AC line cycle, which was recorded with a 10:1 probe connected directly to the power line. The hardware setup is described in more detail in Chapter 5.1.

## 3.1 HomePlug AV

The HomePlug AV specification aims to create an easy to set up BPL LAN, fast enough for High Definition (HD) video and audio streams [Hom05, p. 2]. All STAtions (STAs) in a network are of the same type, have equal rights and there is no need to configure them manually. HomePlug AV is interoperable with HomePlug 1.0, and its coexistence with other BPL systems is ensured by the Inter-System Protocol (ISP) as defined in the IEEE 1901 standard [IEE10, Chapter 16 pp. 1249-1279].

A physical HomePlug AV network is divided into so-called HomePlug AV in-home Logical Networks (AVLNs), which are cryptographically isolated by secret keys. STAs are allowed to participate in more than one AVLN. The basic mandatory architecture of a HomePlug AV certified transceiver microchip is depicted in Figure 3.1. The Higher Layer Entity (HLE) on top can be regarded as an abstract data sink and / or source, either in the same device or in a distinct server connected to the transceiver. Each device consists of a control and data plane. The former is responsible for setting up and managing connections between STAs and also includes the capability to function as a Central Coordinator (CCo). In each AVLN, exactly one device is elected as CCo and manages network memberships and resource allocations. The data plane is responsible for transmitting and receiving the payload data and is structured in three layers: Convergence,

[14] Many current power line systems work in a similar way.

MAC and PHY. Communication between layers and planes is realized by Service Access Points (SAPs) (also called interfaces), which use pre-defined messages comparable to an Application Programming Interface (API) [Hom12b, Chaper 2.1.2 p. 26]. The Convergence Layer's purpose is to translate incoming packets from various protocols to a common interface. According to [Hom12b, Chapter 6.4 p. 322], only Ethernet is supported at the moment. The MAC and PHY layers are described in more detail in the following sections.

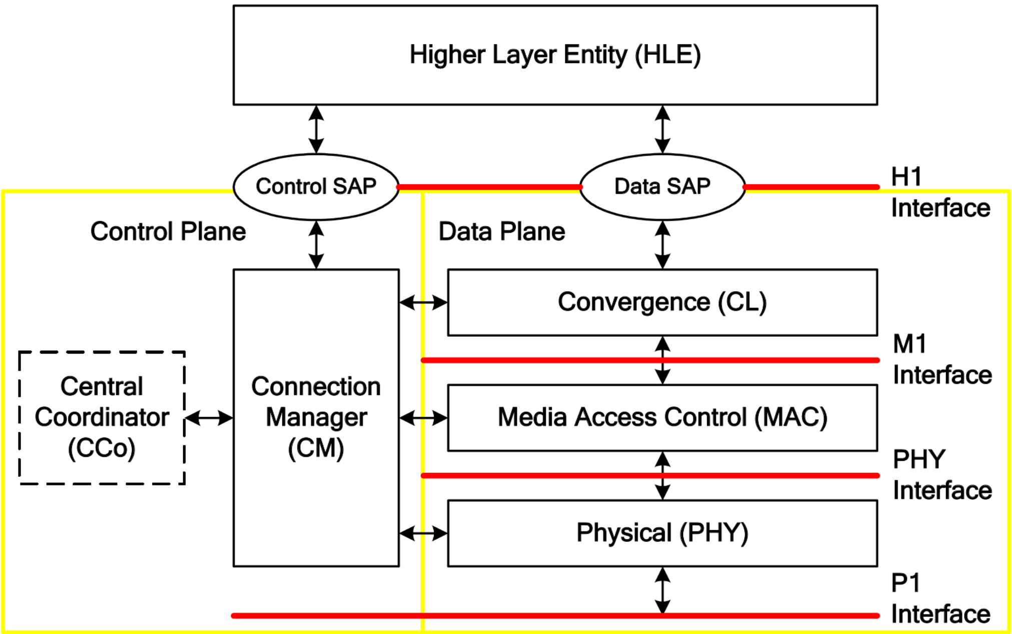


Figure 3.1: The HomePlug AV architecture, taken from [Hom05, Figure 1 p. 3].

### 3.1.1 PHY Layer

The power line channel is a harsh and fast changing environment regarding its noise and transfer function. In order to achieve a reliable communication, the PHY layer of HomePlug specifications is built to be very robust and adaptive. It is the lowest of all layers and performs the physical transmission of data on the power line, including modulation, FEC (also called channel coding), interleaving and scrambling of the data on the transmitter – and the inverse operations on the receiver side. The messages transmitted by the PHY layer are called PHY Protocol Data Units (PPDUs). If HomePlug 1.0 devices are detected in the network, HomePlug AV is also capable of sending so-called *hybrid* PPDUs for the sake of fair medium sharing. They are extended versions of AV-only PPDUs, used to additionally defer HomePlug 1.0 devices from transmitting.

The structure of a hybrid PPDU can be seen in Figure 3.2 and as a recorded waveform in Figure 3.3. Each PPDU starts with a preamble (either hybrid or not) known by transmitter and receiver, serving for channel estimation and synchronization purposes. Afterwards, a HomePlug 1.0 Frame Control (FC) OFDM symbol (only present in hybrid PPDUs) and a HomePlug AV FC OFDM symbol follow and optionally one or more PayLoad (PL) OFDM symbols (six in the recorded waveform). Under certain conditions it can occur that the FC data does not fit in one OFDM symbol. This happens when insufficient bandwidth is available, which can be due to legal regulations or parallel operation of Frequency Division Multiple Access (FDMA) separated PLC networks. The HomePlug AV specification states that in this case, two symbols should be used for FC. According to [Hom12b, Chapter 3.6.6 p. 83], the power level of the preamble and AV FC symbols are raised by 3dB and that of PL symbols by 2.2dB compared to the 1.0 FC symbol's power level, which is clearly visible in Figure 3.3. The 0.8dB difference between AV FC and PL symbol power is hardly noticeable.

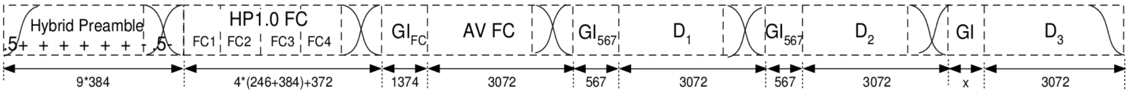


Figure 3.2: The structure of an AV PPDU with one FC symbol, taken from [Hom12b, Figure 3-4 p. 39].

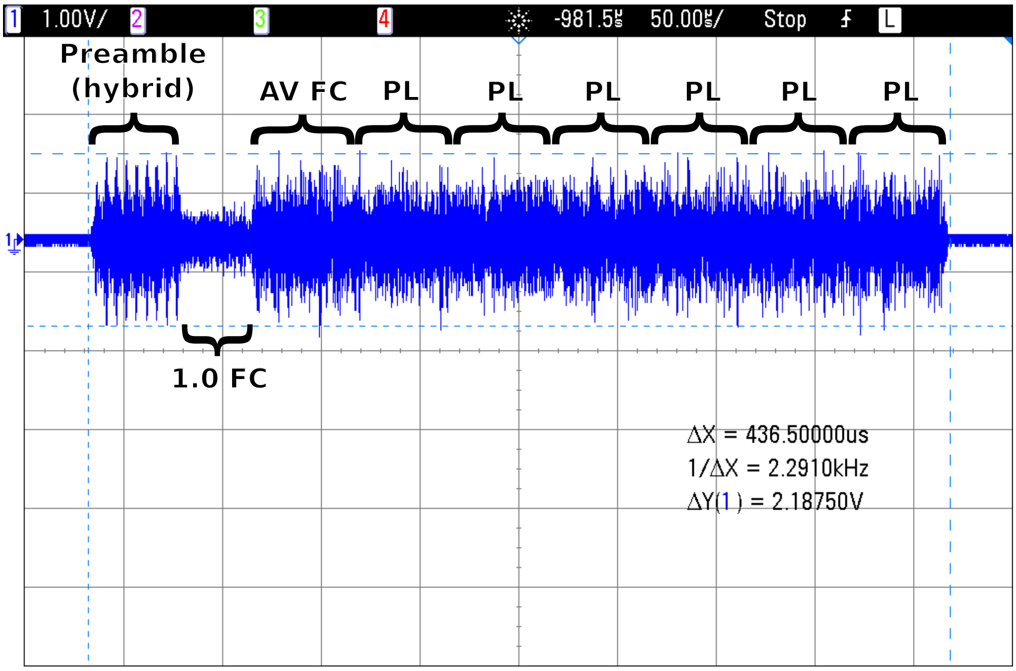


Figure 3.3: A recorded hybrid PPDU waveform.

The structure of the whole PHY layer can be found in Figure 3.4. Interleaving, scrambling and FEC of data is described in Chapter 3.1.1.1, modulation in Chapter 3.1.1.2 and physical coupling in Chapter 3.1.1.4.

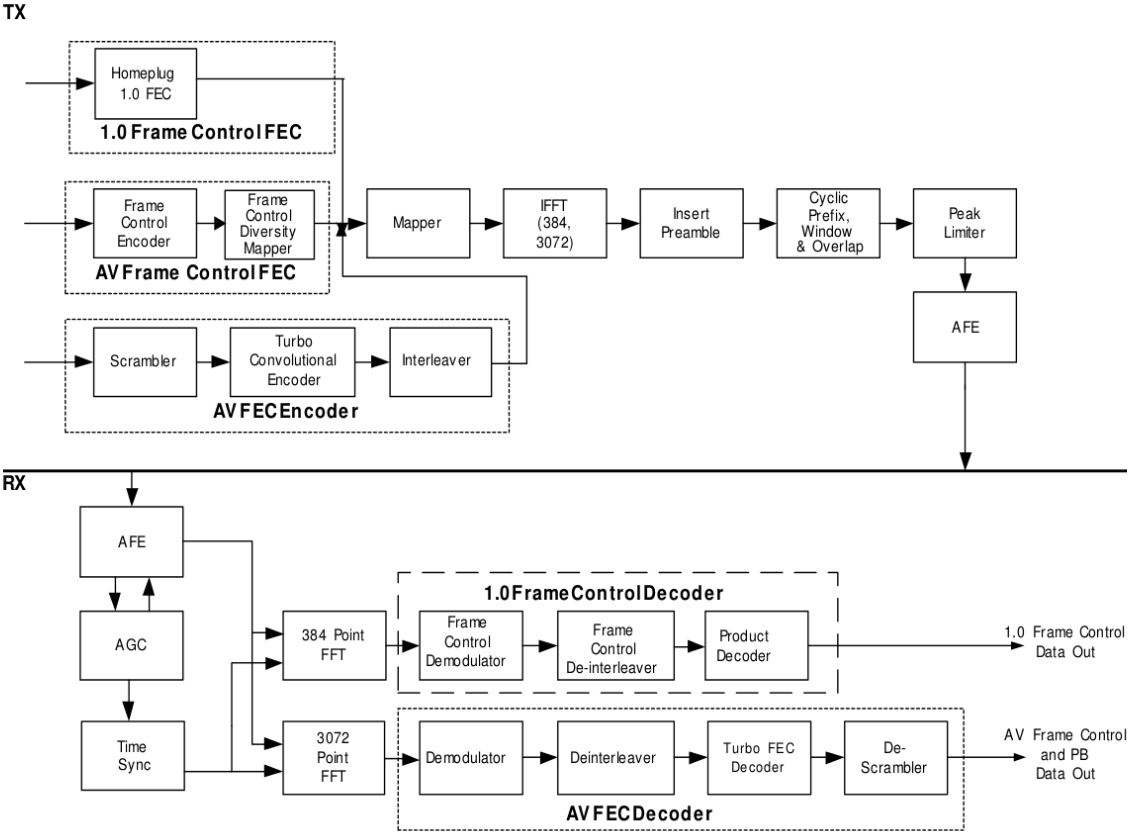


Figure 3.4: Overview of the HomePlug AV PHY layer, taken from [Hom12b, Figure 3-1 p. 36].

#### 3.1.1.1 Channel Coding, Interleaving and Scrambling

On the left in Figure 3.4, a block of data passed by the MAC layer may be one of three types, whose processing slightly differs: HomePlug 1.0 frame control, HomePlug AV frame control or PL data. The first type is only needed for hybrid PPDUs and its encoding is not discussed further in this chapter. The second and third types are contained in each HomePlug AV PPDU and their channel coding, scrambling, interleaving and diversity copying are introduced in the following.

The Turbo convolutional encoder is common for all data blocks (except its block length and whether the output is punctured) and shown in Figure 3.5. Two Recursive Systematic Convolutional (RSC) encoders map the source bits $u_1$ and $u_2$ to $p$ and $q$, respectively. The RSC blocks are identical and depicted in Figure 3.6, except that the second encoder is prepended with a Turbo interleaver with half the length of the processed data block's number of bits. Without puncturing, the input $\begin{bmatrix} u_1 & u_2 \end{bmatrix}$ is mapped onto the output $\begin{bmatrix} u_1 & u_2 & p & q \end{bmatrix}$, which results in a code of rate 1/2. With puncturing of $p$ and $q$,[15] the Turbo encoder has a rate of 16/21.

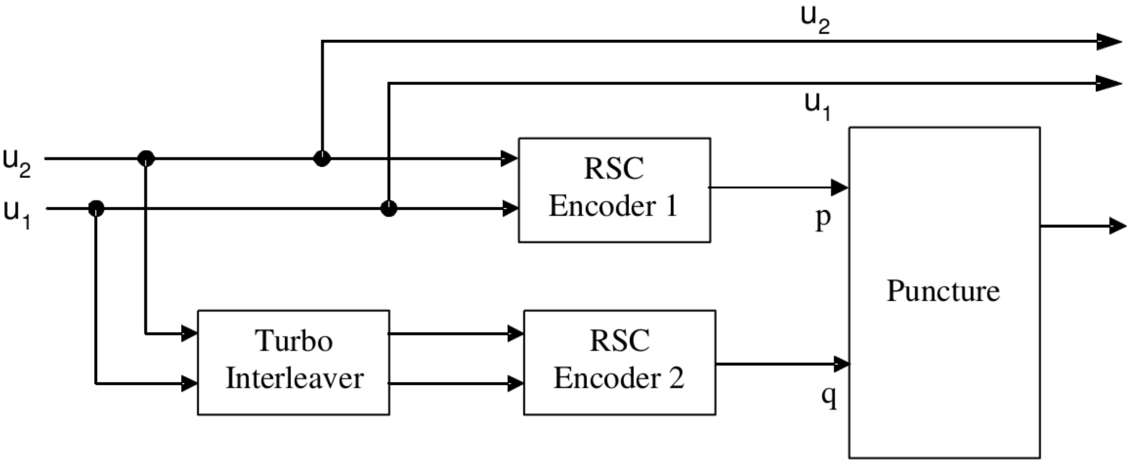


Figure 3.5: Turbo convolutional encoder, taken from [Hom12b, Figure 3.10 p. 44].

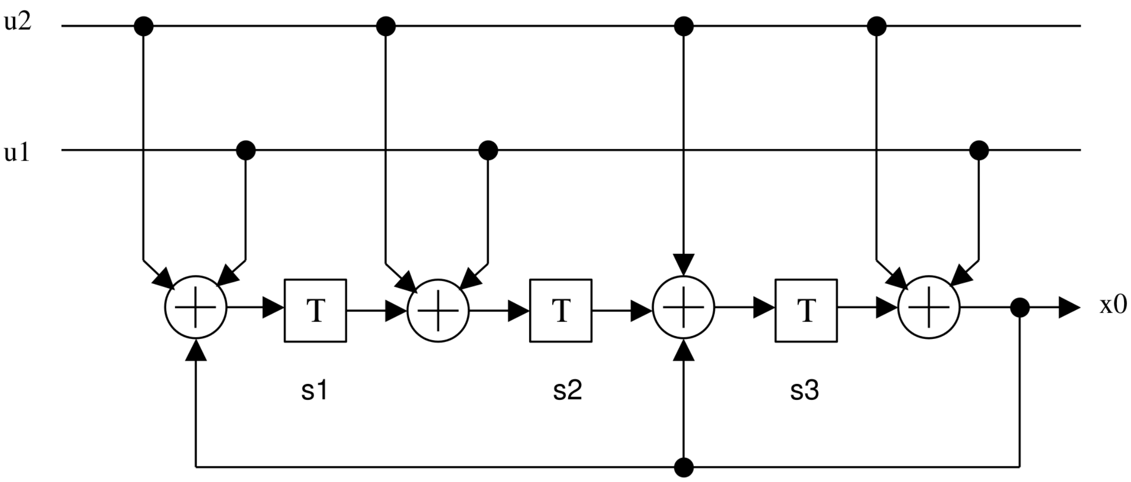


Figure 3.6: 8-state RSC encoder, taken from [Hom12b, Figure 3.12 p. 46].

[15] Puncturing the parity bits $p$ and $q$ is done according to the pattern 1001001001001000 [Hom12b, Table 3.6 p. 47]. Each 0 means, that the parity bit in that position is punctured (not transmitted).

Each FC block contains 16 octets (128 bits) of control data, which have to be transmitted. The first step is the Turbo convolutional encoder without puncturing described above, followed by an interleaver and a diversity copier. The interleaver spreads burstly occurring bit errors across the whole FEC block, which makes its successful decoding more likely [Gol05, p. 270]. The diversity copier replicates each bit across the whole frequency band, until one OFDM symbol is completely filled (or two OFDM symbols, in case the transmitter is configured in two FC symbol mode). HomePlug 1.0 FEC is different and not further discussed here.

Payload data blocks may have a length of 136 or 520 octets (1088 or 4160 bits). The first step is a scrambler, which combines[16] the input data with a pseudo random sequence of bits. This way, even input sequences of very low entropy (few changes between ones and zeros) have a random distribution when transmitted. This is desirable to facilitate synchronization at the receiver and to prevent concentration of the symbol energy in sub bands of the transmission spectrum [Wes09, p. 184]. An interleaver forms the last step of PL data encoding.

#### 3.1.1.2 Modulation

After the input data is scrambled, FEC protected and interleaved, it has to be modulated before its transmission. HomePlug systems use an OFDM scheme to map bits onto transmitted symbols, which is explained in this chapter. “The basic idea of OFDM is to divide the available spectrum into several subchannels (subcarriers)“ [ESB+96, p. 3]. In modern digital transmission systems, the IDFT algorithm is used for that purpose. It transforms a complex-valued vector in frequency domain to a complex-valued vector in time domain. However, it is possible to get a real-valued transmission waveform, if the input to the IDFT algorithm is made conjugate symmetric[17]. It is possible to transform a complex-valued frequency vector of odd length $N$ to a real-valued time vector of even length $2N + 2$, by mirroring each positive frequency to the negative range and conjugating it before passing it to the IDFT. Additionally the DC frequency component and a so-called *Nyquist tone* at the highest possible frequency have to be added. If $\underline{\boldsymbol{X}} = \begin{bmatrix} \underline{X}_1 & \underline{X}_2 & \dots & \underline{X}_N \end{bmatrix}$ contains the complex valued samples in frequency domain and $\underline{\boldsymbol{X}}_{inv}$ denotes $\underline{\boldsymbol{X}}$ with the inverted order of its elements, the time domain waveform $\underline{\hat{\boldsymbol{x}}} = \mathcal{IDFT}(\underline{\hat{\boldsymbol{X}}})$ with $\underline{\hat{\boldsymbol{X}}} = \begin{bmatrix} (\underline{\boldsymbol{X}}_{inv})^* & \underline{X}_0 & \underline{\boldsymbol{X}} & \underline{X}_{Nyquist} \end{bmatrix}$ is real-valued ($\mathcal{Im}\{\underline{\hat{\boldsymbol{x}}}\} = \boldsymbol{0}$).

[16] Each data bit is modulo-2 added to one bit of the pseudo random bit sequence.

[17] A complex function $\underline{f}(x)$ is said to be conjugate symmetric, if $\underline{f}(-x) = \underline{f}^*(x)$. For a function in frequency domain, this means that its values at negative frequencies are complex conjugated and mirrored versions of its values at positive frequencies.

Figure 3.7 shows an example with $N = 9$ and $\underline{\boldsymbol{X}} = \Big[1, \;\; 0, \;\; 0, \;\; -j, \;\; 0, \;\; 0, \;\; 0, \;\; 0, \;\; 0\Big]$. The two non-zero entries in $\underline{\boldsymbol{X}}$ lead to the sum of a slow cosine and a fast sine wave in time domain, both real-valued. The dotted curve (green) shows the superposition of the two sinusoidals with more samples. Although the DC part (the entry $\underline{X_0}$ in $\hat{\underline{\boldsymbol{X}}}$ above) of the signal can also be changed, it is set to zero in many systems. The reason is that transformers in the transmission path block the signal's DC component.

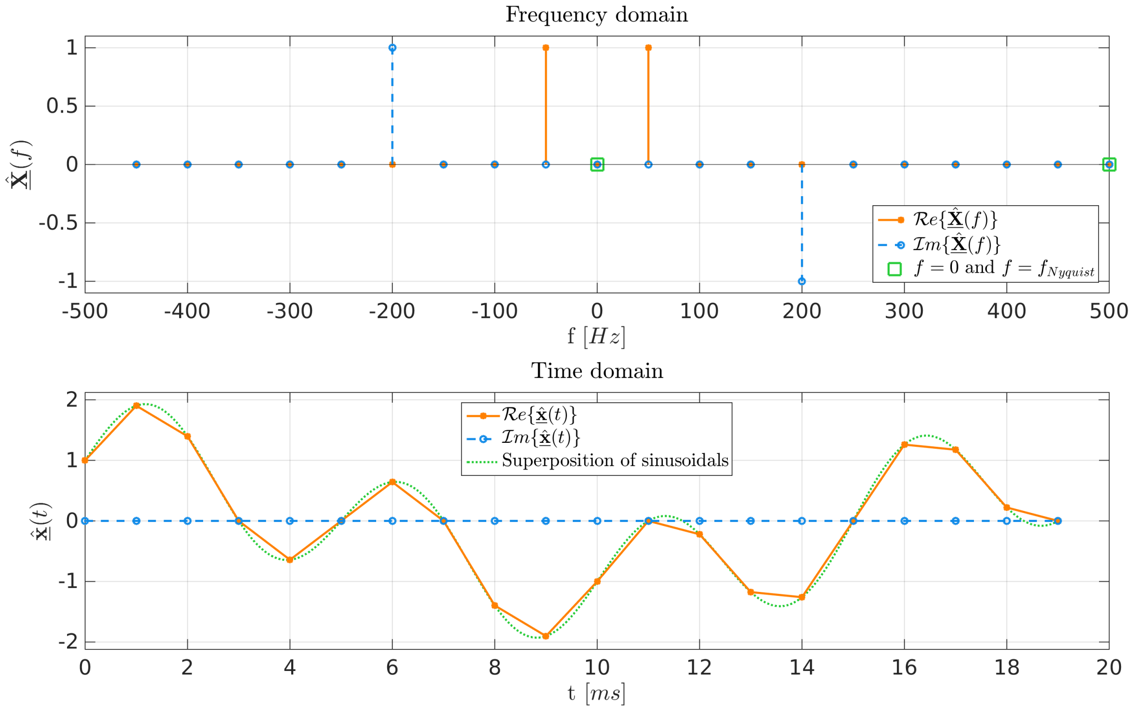


Figure 3.7: Using the IDFT to obtain a real-valued waveform.

In the context of OFDM, each entry in the frequency vector is called *carrier* and can be modulated separately, usually with digital modulation formats. In case of HomePlug, the carriers are modulated with different schemes from BPSK over Quadrature Phase Shift Keying (QPSK) up to 1024-Quadrature Amplitude Modulation (QAM),[18] depending on the channel's quality. As the power line channel can be highly frequency selective (refer to Chapter 4), carriers are affected by different attenuation values. The countermeasure in the HomePlug specification is called *adaptive bit loading*. It describes an algorithm which determines how many bits per carrier are transmitted. If the channel at the frequency of a carrier has low attenuation, higher modulation formats are used and vice versa.

[18] A short introduction into M-QAM modulation schemes and their signal space constellations can be found in [Fre06, Chapter 3.3.2.1 p. 139 ff.].

Additionally, two important OFDM properties have to be fixed in each transmission system: the used bandwidth and carrier spacing. In the adaptive bit loading example in Figure 3.8, the former is fixed to $500Hz$ and the latter to $50Hz$, resulting in nine usable carriers ($N = 9$, $(2N + 2) \cdot 50Hz = 1000Hz$ two-sided bandwidth according to $\underline{\boldsymbol{X}}$ and $\underline{\hat{\boldsymbol{X}}}$ in the previous paragraph). The exemplary channel's transmission properties (attenuation and noise) are assumed to worsen with frequency. According to that, the first carrier is modulated with 16-QAM, carriers two to five with QPSK, six and seven with BPSK and the two highest carriers are switched off. This example also shows one drawback of OFDM: the Peak to Average Power Ratio (PAPR) can be very high and lead to the requirement of Analog Front Ends (AFEs) with a high dynamic range. It is important to take this into account during the design of OFDM transmission systems and take countermeasures like companding the signal [GC02] or minimizing the probability that many carriers are transmitted with the same phase [Hom12b, Chapter 3.5.3 p. 66].

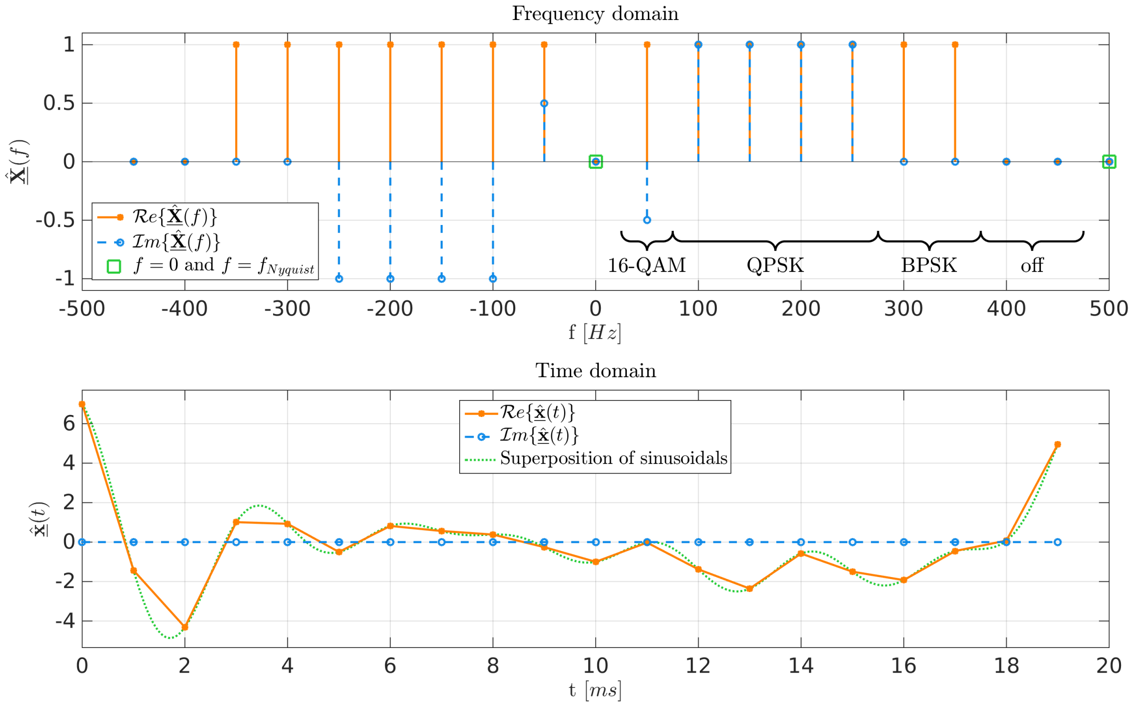


Figure 3.8: Adaptive bit loading example with 16-QAM, QPSK and BPSK.

In case of HomePlug AV, the carrier spacing is fixed to $24.4140625kHz$ and the IDFT size to 3072, which leads to a two-sided bandwidth of $3072 \cdot 24.4140625kHz = 75MHz$. Thus, $N = \frac{3072-2}{2} = 1535$ carriers can be modulated and the occupied positive spectrum range goes from $0Hz$ to $37.5MHz$ with a sampling rate of $75MHz$. To prevent BPL systems from causing interference to amateur and official radio broadcasting services, parts of the spectrum must not be used. A PPDU in frequency domain transmitting on all allowed carriers can be seen in Figure 3.9, which shows a HomePlug AV signal recorded with a spectrum analyzer. Transmissions below $2MHz$ would disturb AM broadcast services, transmissions in the notches and above $28MHz$ amateur radio services. A small part of a PPDU in time domain can be seen in Figure 3.10, its form resembles the superposition of many sinusoidals.

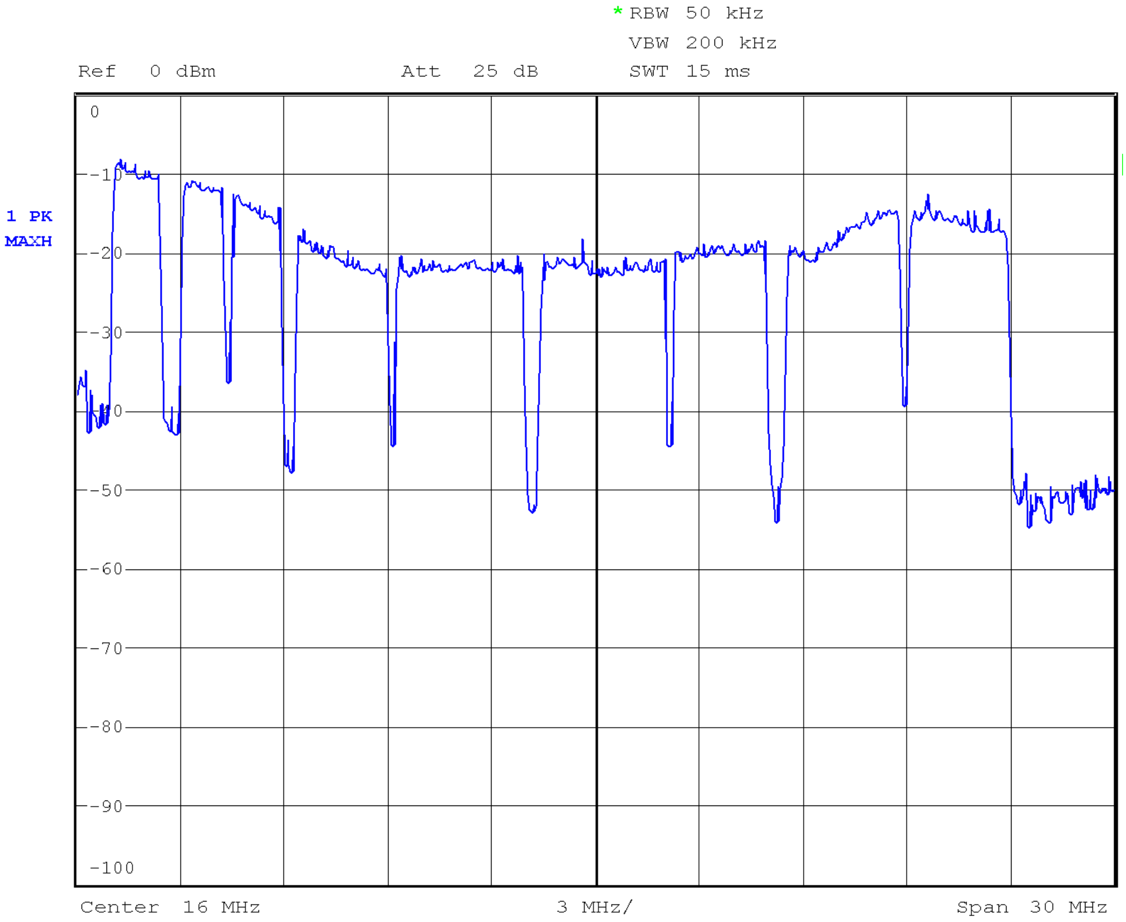


Figure 3.9: Spectrum of a HomePlug AV PPDU.

The last block on the transmitter side in Figure 3.4 prepends each OFDM symbol with a cyclic prefix serving as a guard interval. It protects signals from impairments caused by multi-path propagation in the power line channel, which would otherwise introduce Inter Symbol Interference (ISI). The tone maps can use one of three guard intervals lengths, depending on the longest echo the channel introduces. The choices are 417, 567 and 3534 samples [Hom12b, Table 3-2 p. 40], which translate to $5.56\mu s$, $7.56\mu s$ and $47.12\mu s$, respectively, for a $75MHz$ clock.

On the receiver side in Figure 3.4, all blocks are the inverse functions of their counterpart in the transmitter, except for the Automatic Gain Control (AGC), which estimates the signal's current attenuation and amplifies its power to a fixed level, and the time sync block, which recovers the sampling clock from the received signal.

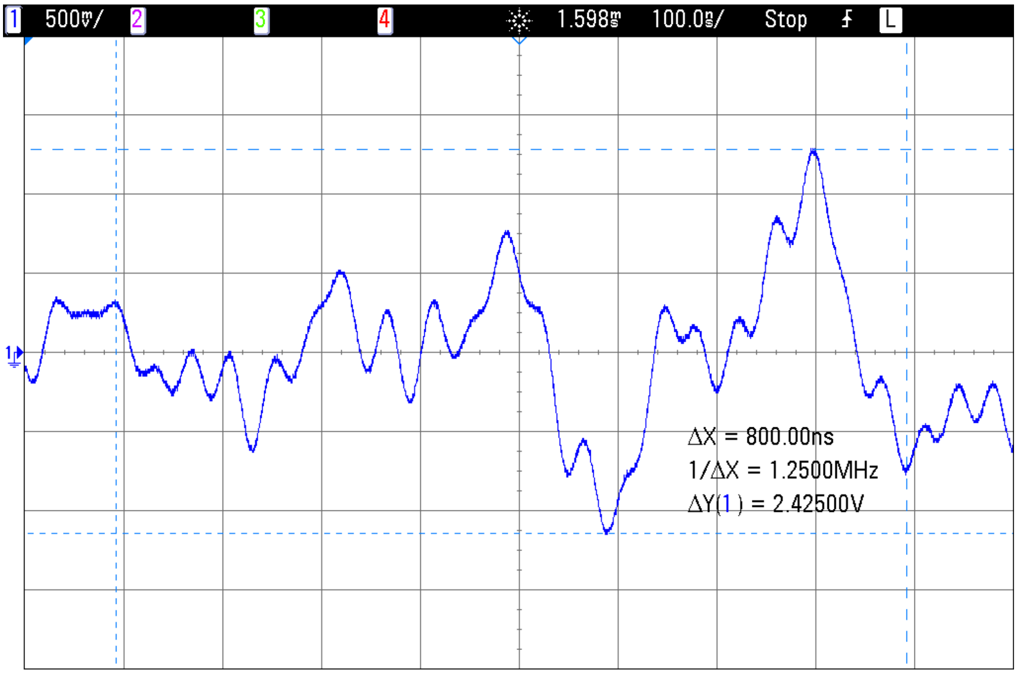


Figure 3.10: Zoom on a part of a HomePlug AV PPDU in time domain.

#### 3.1.1.3 ROBO Modes

HomePlug has four different modulation modes. Normally, payload data is transmitted as described in Chapter 3.1.1.2 with up to 1024-QAM and a channel coding rate of 1/2 or 16/21. Additionally, there are the so-called Robust OFDM (ROBO) modes *MINI ROBO (MINI-ROBO)*, *STanDard ROBO (STD-ROBO)* and *High Speed ROBO (HS-ROBO)*, which are more reliable and used for beacon transmissions, broadcast and management messages, session setups and for initial communication with devices where the channel is not yet estimated [Hom12b, Chapter 3.4.4 p. 52]. To achieve the additional robustness, all ROBO modes use only QPSK modulation and the unpunctured, rate 1/2 Turbo convolutional code. Channel estimation gets unnecessary in all ROBO modes, because they apply the same modulation format to all carriers. This also implies that data is sometimes transmitted on carriers which will definitely not be received correctly. To avoid resulting frame errors, each bit is copied after FEC and interleaving 1, 3 or 4 times[19], depending

[19] Each bit is copied 1, 3 or 4 times means, that it is modulated onto 2, 4 or 5 carriers, respectively.

on the ROBO mode. As the copies are spread across the whole transmission spectrum, it is very unlikely that more than half of them is corrupted [Hom12a, Chapter 'ROBO Modes' p. 13]. ROBO modes also differ in the size of their used PHY Block (PB) lengths. In case of MINI-ROBO, each PB contains 136 octets, all other modes use PBs with 520 octets. Table 3.1 summarizes all ROBO modes. It depends on the level of needed reliability which one is used. Due to the different number of redundant copies, MINI-ROBO is more and HS-ROBO less reliable if compared to STD-ROBO.

| ROBO Mode | Number of Copies | PHY data Rate $[Mbit/s]$ | PHY Block length $[octets]([bits])$ |
|---|---|---|---|
| STD-ROBO | 4 | 4.9226 | 520 (4160) |
| HS-ROBO | 2 | 9.8452 | 520 (4160) |
| MINI-ROBO | 5 | 3.7716 | 136 (1088) |

Table 3.1: ROBO mode parameters, adapted from [Hom12b, Table 3-13 p. 52].

#### 3.1.1.4 Signal Coupling

After FEC, modulation and insertion of the guard interval and the preamble have been carried out, the waveform is passed to the AFE, which basically consists of an amplifier, a coupling transformer (balun) and a capacitor. In Figure 3.11, a coupling scheme with additional protective elements is depicted; in Figure 3.12 the couplers which were used for this thesis are shown.[20]

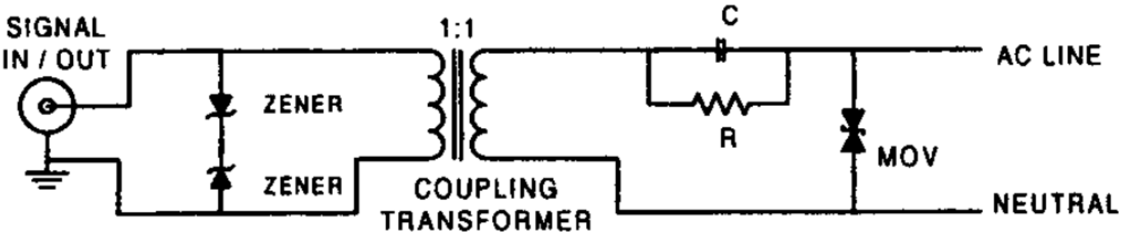


Figure 3.11: Coupling circuit with protection elements, taken from [LSG$^+$00, Figure 5 p. 454].

The capacitor acts as a highpass which blocks the comparatively slow $50Hz$ mains voltage and lets signals with higher frequencies pass through. The balun separates the modem's from the mains voltage's ground – mainly for safety and convenience.

[20] The couplers in Figure 3.12 are mainboards of *devolo dLAN 200 AVpro DIN rail* HomePlug AV modems. They couple signals between the daughter board and up to three phase wires, provide a trigger when the power line cycle has its zero crossing and also deliver power to the daughter board.

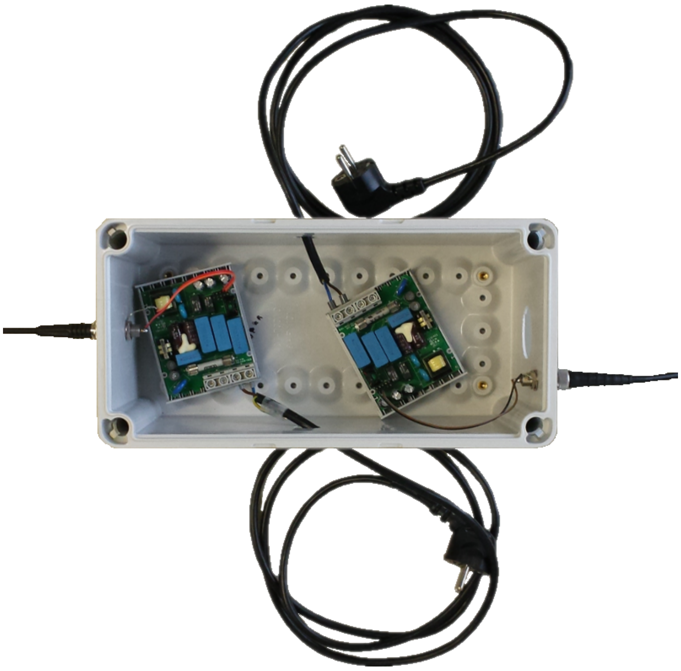


Figure 3.12: The signal couplers used in this thesis.

Using a balun, the user can switch the phase and neutral line of the mains voltage without impairing the modem's operation. The depicted circuit is an easy and efficient way of coupling and in the following, a short calculation of signal attenuations at a receiver is performed. In order to be able to get there, the transfer function of the circuit in Figure 3.13 has to be derived.

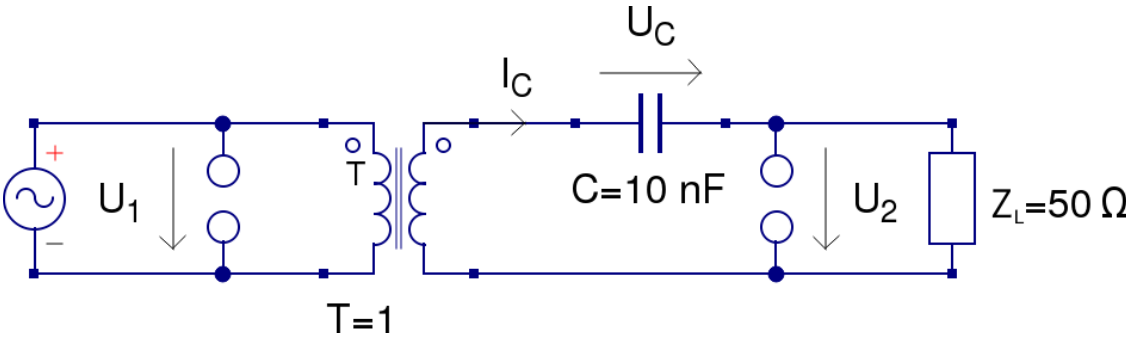


Figure 3.13: Schema of a coupling circuit.

Assuming that the transformer is ideal in the regarded frequency range, it can be omitted in the following calculations.[21] The load impedance $\underline{Z_L} = 50\Omega$ was selected, because it is a

[21] The turns ratio of the balun in the used coupler is $T = 4$. However, for the calculation of the transfer function it is set to 1 here, because it has no effect on the frequency response of the circuit.

very common terminal impedance and the actual value of a receiver is likely to match it. The calculation would also work in the transmitting direction, the only difference would be that $\underline{Z_L}$ reflects the power line network's impedance. However, that value is most often complex, its magnitude can vary between some $\Omega$ and one $k\Omega$ [CDCE02, p. 177] and thus it is not possible to give a predetermined result. Using Kirchhoff's voltage law $\sum_{i \in \text{loop}} \underline{U_i} = 0$, Ohm's law $\underline{U} = \underline{ZI}$ and the impedance of a capacitance $\underline{Z_C} = \frac{1}{j\omega C}$, we get the equations

$$\begin{aligned} \underline{U_2} &= \underline{U_1} - \underline{U_C} \\ \underline{U_2} &= \underline{Z_L I_C} \\ \underline{U_C} &= \frac{1}{j\omega C} \underline{I_C}\,, \end{aligned}$$

with $\omega = 2\pi f$ and $j^2 = -1$. Rearranging leads to the transfer function

$$\underline{H(f)} = \frac{\underline{U_2}}{\underline{U_1}} = \frac{1}{1 + \frac{1}{j\omega \underline{Z_L} C}}\,.$$

By splitting $\underline{H(f)}$ in its real and imaginary parts (assuming that $\underline{Z_L}$ is real)

$$\underline{H(f)} = \mathcal{Re}\{\underline{H(f)}\} + j\mathcal{Im}\{\underline{H(f)}\} = \frac{1}{1 + \frac{1}{(\omega Z_L C)^2}} + j\frac{1}{\omega Z_L C + \frac{1}{\omega Z_L C}}\,,$$

the magnitude transfer function

$$\begin{aligned} \left|\underline{H(f)}\right| &= \sqrt{\mathcal{Re}\{\underline{H(f)}\}^2 + \mathcal{Im}\{\underline{H(f)}\}^2} \\ &= \sqrt{\frac{1}{1 + 2\,(\omega Z_L C)^{-2} + (\omega Z_L C)^{-4}} + \frac{1}{(\omega Z_L C)^2 + 2 + (\omega Z_L C)^{-2}}} \end{aligned}$$

can be calculated. Figure 3.14 shows the power transfer function in Decibels $|\underline{H}|^2_{dB} = 20\log_{10}|\underline{H}(f)|$ for the component values in Figure 3.13 ($T = 1$, $C = 10nF$ and $Z_L = 50\Omega$). The circuit clearly has a high-pass character, it attenuates a $50Hz$ signal's power by $\approx 76dB$ and hardly affects a signal above $1MHz$. This means a mains voltage of $230V$ is attenuated to $\approx 0.04V$ and a $2MHz$ transmission signal's amplitude of $5V$ remains at $4.94V$ after passing the circuit. Thus, the presented method is a simple and effective approach to couple PLC signals between power lines and transceivers.

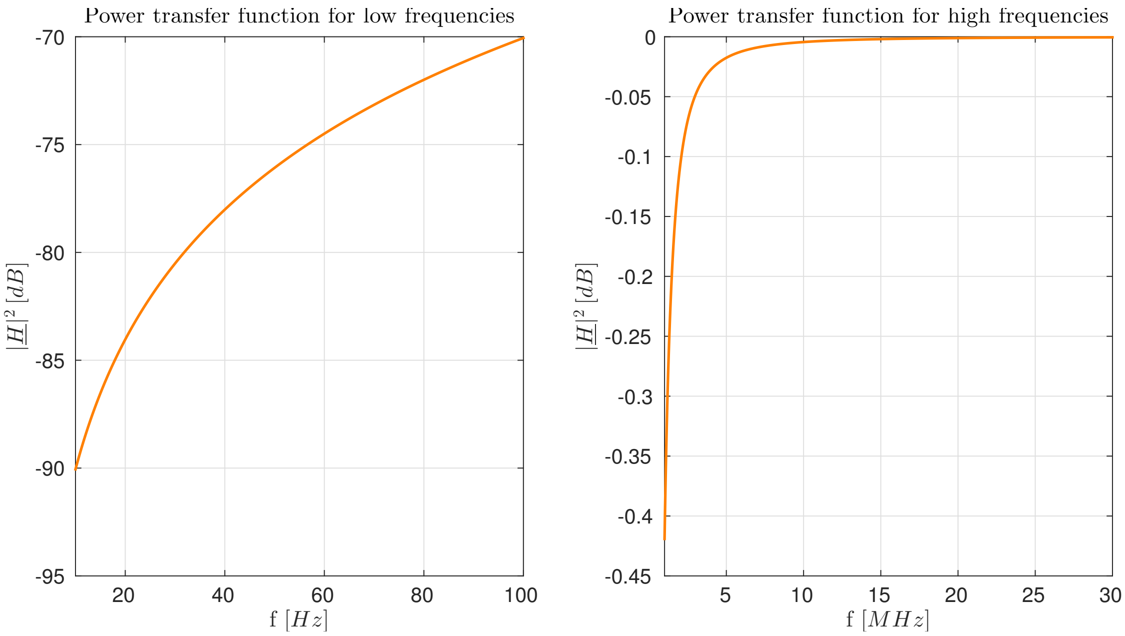


Figure 3.14: Transfer function of the considered coupling circuit.

### 3.1.2 MAC Layer

Analogous to PPDUs, frames of the MAC layer are called MAC Protocol Data Units (MPDUs). There are four different MPDU types: short ones (only FC) and long ones (FC and PL), either with or without an additional 1.0 FC symbol for hybrid operation. One of the tasks of the MAC layer is the generation of FC data for each PB. The FC contains information about the type of the MPDU, to which AVLN it belongs and message type specific information. A complete list of all possible types and fields can be found in [Hom12b, Chapter 4.4.1 pp. 115-154]. The MAC layer also handles the fragmentation of incoming data in PBs of the correct length (136 or 520 octets) [Hom12b, Chapter 5.4.1.3 p. 262 f.], which is depicted in Figure 3.15. The data stream is split in small segments and passed to the PHY layer, together with a header and a check sequence. In case the incoming data length does not fit in an integer number of PBs, a padding is appended.

Although transmission is protected by FEC, the channel still can introduce unrecoverable errors. In that case, the MAC layer has to initiate the retransmission of the corrupted frame, which is called Automatic Repeat reQuest (ARQ). To detect the loss of a frame, the receiver has to respond to each frame with a Selective Acknowledgment (SACK), as described in [Hom12b, Chapter 5.4.8.1 p. 288 f.]. HomePlug also has a burst mode, where up to four MPDUs can be acknowledged with a single SACK [Hom12b, Chapter 5.4.6 p. 281 ff.], which is optional for transmitters and mandatory for receivers.

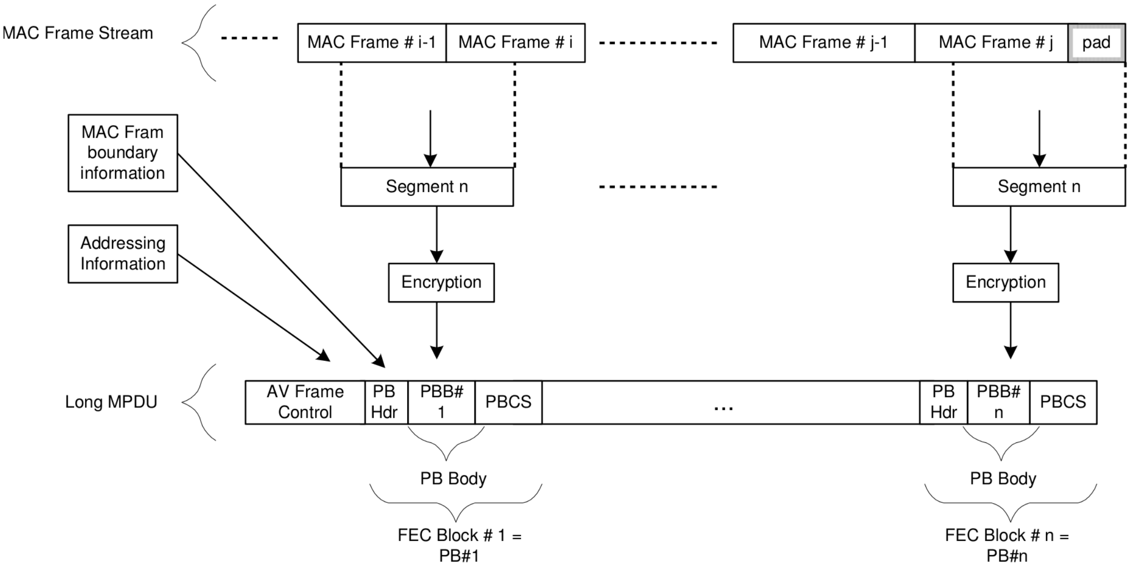


Figure 3.15: Segmentation of the MAC data stream, taken from [Hom12b, Figure 5-17 p. 265].

To be able to use adaptive bit loading, the channel's properties have to be known by both, transmitter and receiver. The MAC layer is responsible to initiate and perform regular channel estimations to update the *tone maps*, which each device keeps for all of its destination STAs. Tone maps are lists which contain the number of bits per carrier and the used OFDM guard interval length. Different tone maps can be associated with different parts of the AC line cycle [Hom12b, Chapter 5.2.6 pp. 238-251].

An example where the transmission of frames and corresponding SACKs can be seen is depicted in Figure 3.16. It shows an Internet Control Message Protocol (ICMP) ping request and the answer to it. The first frame consists of a preamble, followed by a 1.0 FC, an AV FC and one PL symbol. As the ping request has a length of 98 octets, it fits into one PL symbol. The second frame is the SACK from the receiving STA, which is a short MPDU (contains no PL symbols). After a gap of $\approx 2ms$, which results from the processing delays in the modems and HLEs, the ICMP answer is received. As the answer's length is also 98 octets, the PPDU's structure is equal to the request.

The biggest task of the MAC layer is the regulation of channel access. HomePlug can share the power line medium by different mechanisms, which can also be combined. The default is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), where each transmitter has to monitor and contend for the channel and a transmission may only be started if no other STA is occupying the medium.

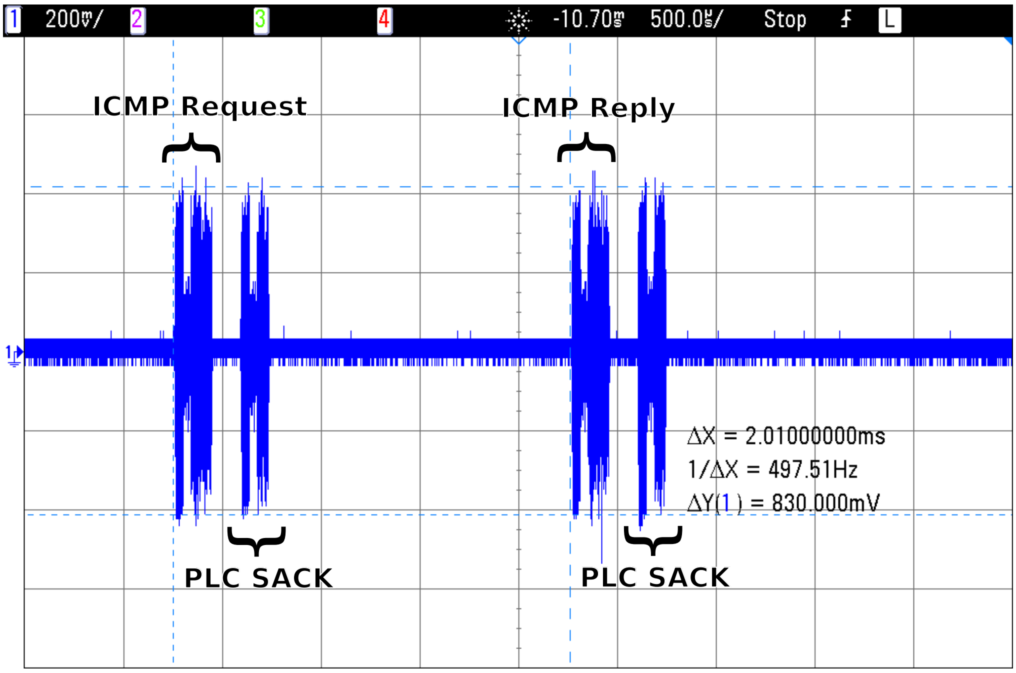


Figure 3.16: Signaling for a ping request and answer.

Additionally, HomePlug FC symbols contain a field which indicates how long the ongoing transmission will take, including the corresponding SACK. STAs willing to send data should try to receive FC symbols from ongoing transmissions and extract this field to know when the next contention phase begins. If the channel is occupied, the transmitter has to back off for a certain amount of time until it starts its next attempt. The waiting time depends on the situation when the collision occurred and is defined in [Hom12b, Table 5-1 p. 212]. The back-off time has to be randomly chosen, so that the two collided transmitters do not try to retransmit again at the same time. Another medium sharing approach is using Time Division Multiple Access (TDMA) slots assigned to links between STAs. The purpose of the connection manager in Figure 3.1 is the management of these TDMA links. To the best of the author's knowledge, TDMA access is not yet implemented in current devices. The FDMA way of channel sharing is assigning disjoint subsets of allowed carriers to STA groups. On one hand, this approach minimizes protocol overhead by allowing transceivers to use the channel without coordination with other groups. On the other hand, communication between STAs in different groups is impossible and the peak data rate is also limited by the reduced set of carriers. Furthermore, there is no specified way to change the set of active carriers during runtime of a device, thus setting up an FDMA group is only possible statically by reconfiguring the devices and is not used in consumer devices.

For Quality of Service (QoS) requirements, the HomePlug specification introduces two ways of prioritizing messages. The first way is the assignment of TDMA slots to links and thus creating contention free periods. This method could guarantee small delays and a certain amount of bandwidth for a connection, if it would be implemented. The second way is to extend the Carrier Sense Multiple Access (CSMA) channel access. At the beginning of each contention phase, two short time slots are designated for priority resolution, in which prioritized devices may transmit Priority Resolution Symbols (PRSs). Transmitters with priority level 3 can transmit a PRS in both slots, devices of priority 2 only in the first slot, devices of priority 1 in the second slot and devices of priority 0 may not transmit PRSs at all. If a transmitter encounters PRSs indicating a higher priority than his, it has to back off from contention. For example, if a device at priority 1 receives a symbol in the first slot, it has to wait for the next contention phase. In Figure 3.17, the first frame is sent with priority 0 and the second with 3. The IEEE 802.1Q standard defines a mechanism to insert a Virtual Local Area Network (VLAN) tag into an Ethernet packet, which inter alia contains a three bit Priority Code Point (PCP) field. It can be used to define the packet's priority of 7 down to 0. If a VLAN tagged Ethernet packet is passed to a HomePlug device from a HLE, the priority should be mapped to the prioritized CSMA power line channel access according to [Hom12b, Table 13-1 p. 692]. Hence, a message with VLAN PCP 7 is transmitted at priority 3, similar to the second frame in Figure 3.17.

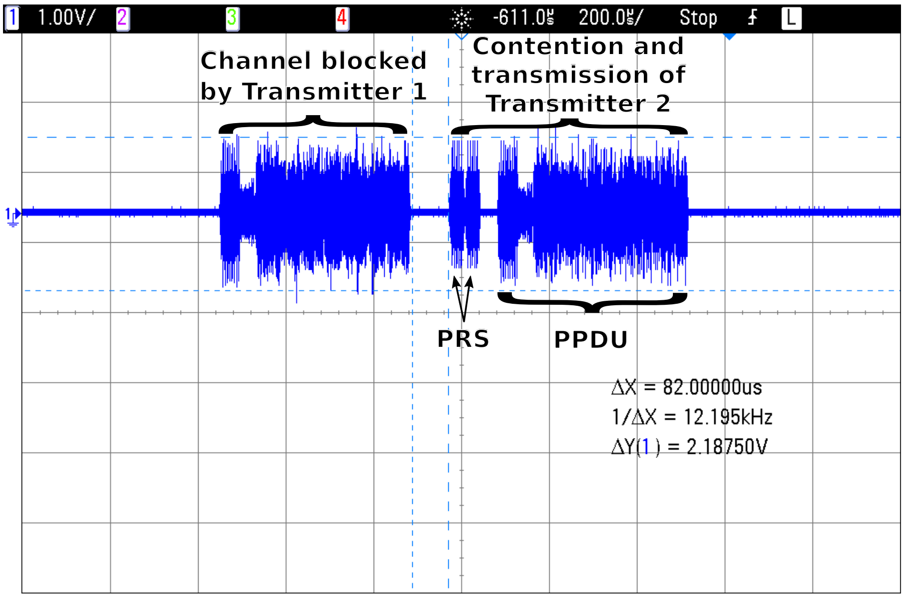


Figure 3.17: CSMA contention for channel access.

As introduced at the beginning of this chapter, each AVLN has one STA selected as CCo. The tasks of a CCo include the management of AVLN memberships, bandwidth control by TDMA slot assignments (not implemented, hence not further discussed) and coordination with other AVLNs and alien networks. To accomplish its tasks, each CCo transmits a *beacon* in regular intervals. It is a long MPDU containing information about the network and transmitted every two AC line cycles with a fixed offset to its zero-crossing. Two beacons and the AC voltage can be seen in Figure 3.18. As the record was made in Germany, the power line frequency is $50Hz$ and beacons are $\frac{2}{50Hz} = 40ms$ apart. The time between two beacons of the same CCo is called *beacon period* and has a specific structure, which is shown in Figure 3.19. STAs can contend for the channel in CSMA regions and are not allowed to transmit in stayout regions, which are set by the CCo and belong to either alien networks or TDMA allocations of other AVLNs. The figure also shows that traffic (a transmitted frame and its SACK in the figure) may continue in the region where the beacon should be transmitted. To maximize the likelihood that they can be sent, beacons are transmitted at priority 3. The two PPDUs in Figure 3.17 are actually the beacons of two AVLNs, the channel was free when the first one was transmitted and the second CCo had to contend for the channel because of the first beacon.

In an environment with high load like in Figure 3.20, failures in channel contention can lead to serious communication errors and degrade throughput. The hardware setup which generated the traffic comprises four STAs, grouped in two pairs spaced approximately $40m$ apart. The probe of the upper (blue) curve is placed near the first STA pair (called transmitters $A$ in the following) and the lower (green) near the other pair (transmitters $B$), yielding an easy distinction of transmitting devices by their amplitude levels. After the first four PPDUs including their SACKs are transmitted correctly, transmitter B introduces an error. A detail plot of the start of the erroneous period is shown in Figure 3.21. Both devices contend for the channel at priority 1 and although transmitter A won the contention by choosing the shorter back off time, transmitter B also begins to send its frame. As information about the channel's state is only gathered when not currently transmitting, the fact that both STAs are active stays undetected by both of them. Since the channel is still reserved for the duration of the SACK in the upper curve, it is transmitted without analyzing the channel. After that, the lower waveform does not contain a valid FC symbol and is taken for noise by the other pair, which starts to send its next frame. After a while ($\approx 2/3$ of Figure 3.20's time span), the devices resemble the situation and transmission continues without errors. The reason for the contention error is a failure in the preamble detection, which could happen because of specific noise or a bug in transmitter B.

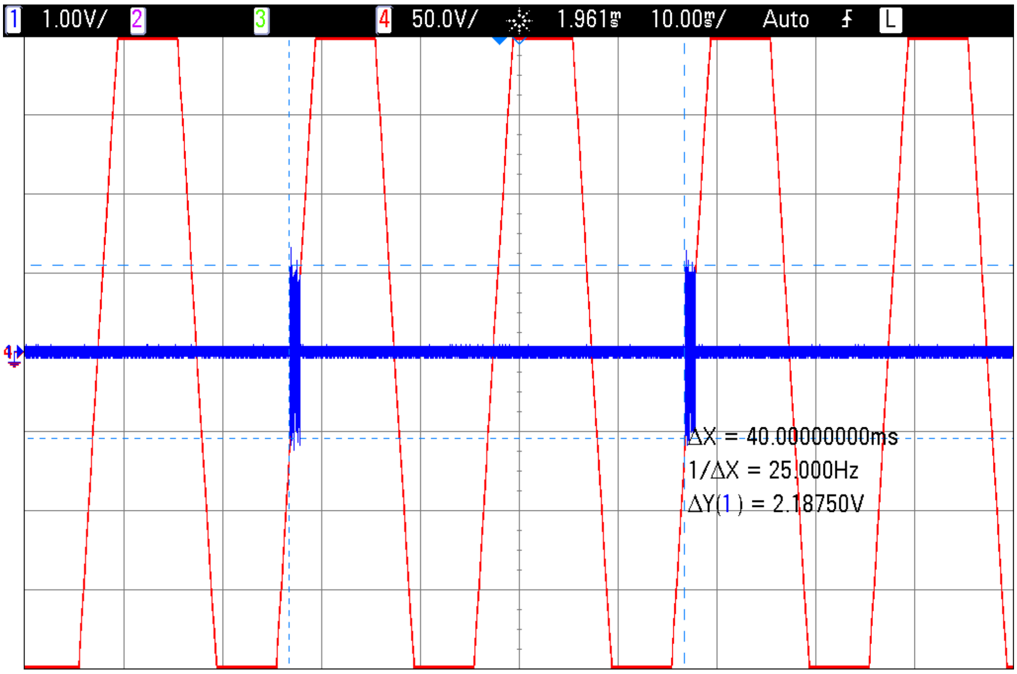


Figure 3.18: Two beacons and the AC line cycle.

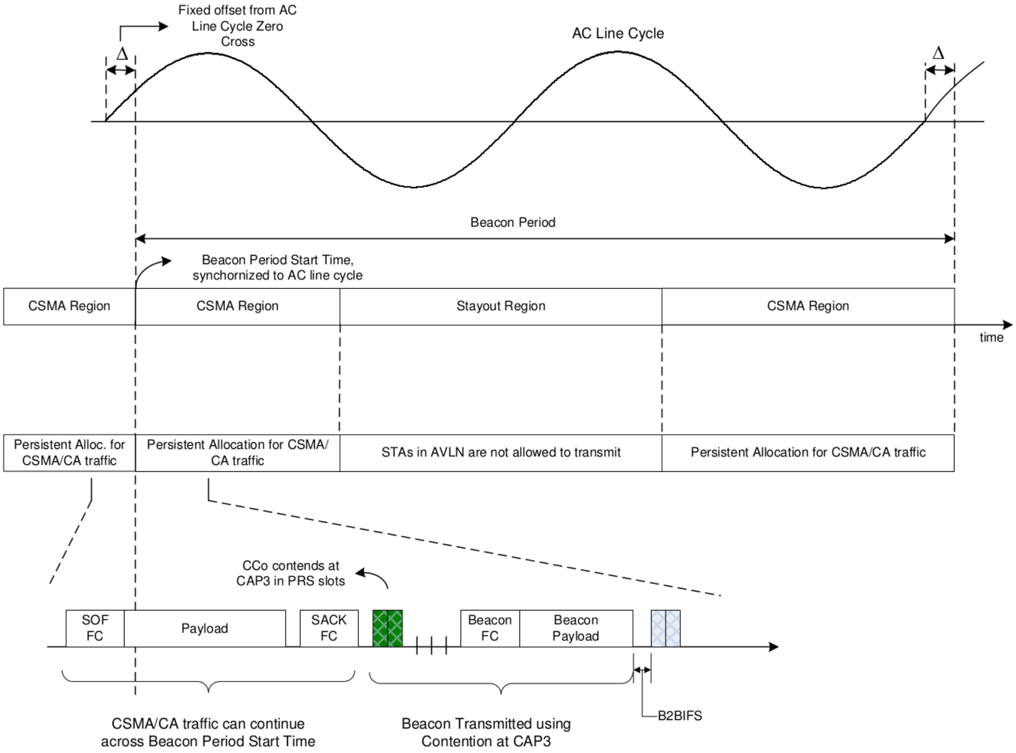

Fixed offset from AC Line Cycle Zero Cross
AC Line Cycle
Δ
Δ
Beacon Period
Beacon Period Start Time, synchronized to AC line cycle
CSMA Region
CSMA Region
Stayout Region
CSMA Region
time
Persistent Alloc. for CSMA/CA traffic
Persistent Allocation for CSMA/CA traffic
STAs in AVLN are not allowed to transmit
Persistent Allocation for CSMA/CA traffic
CCo contends at CAP3 in PRS slots
SOF FC
Payload
SACK FC
Beacon FC
Beacon Payload
B2BIFS
CSMA/CA traffic can continue across Beacon Period Start Time
Beacon Transmitted using Contention at CAP3

Figure 3.19: Beacon period structure in CSMA-only mode, taken from [Hom12b, Figure 5-4 p. 206].

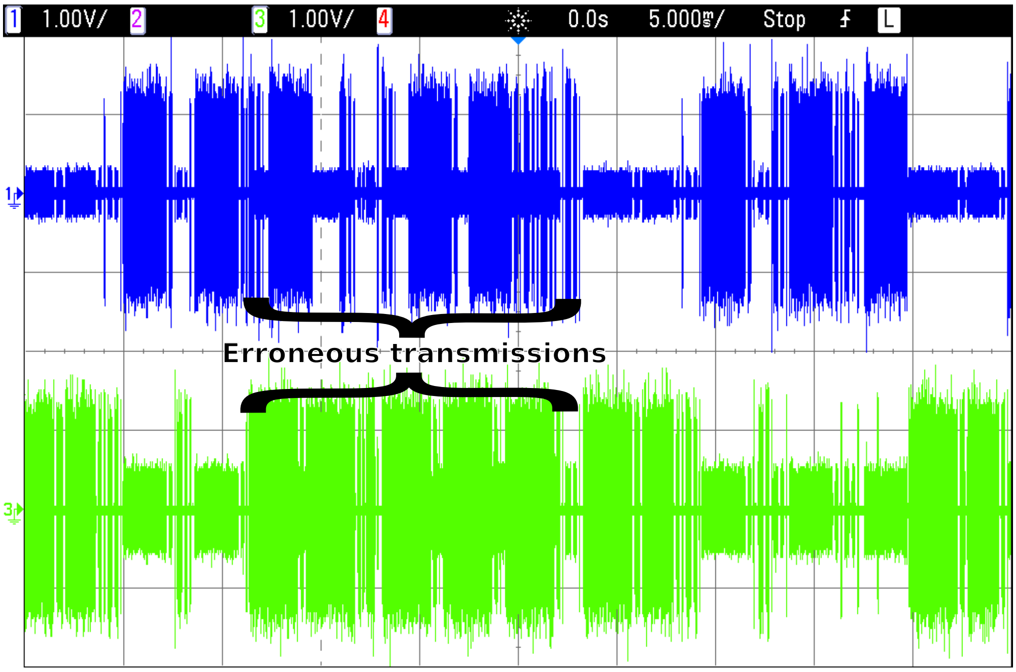


Figure 3.20: Typical high-load traffic between two HomePlug AV device pairs.

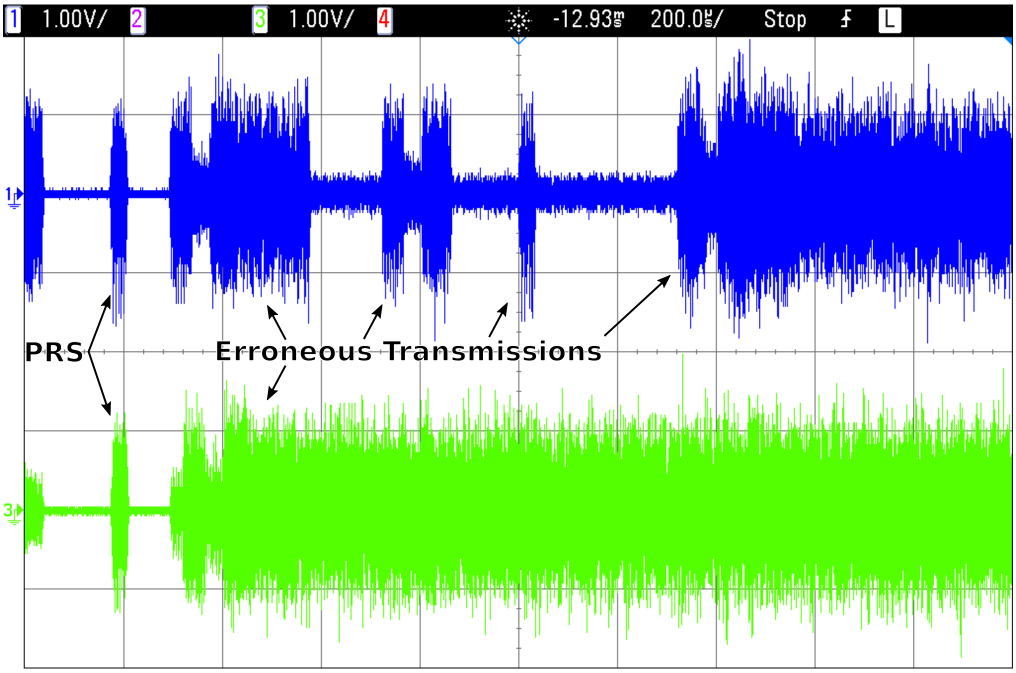


Figure 3.21: Zoom on the beginning of the erroneous traffic in Figure 3.20.

HomePlug AVLNs are cryptographically isolated to prevent eavesdropping on the ongoing communication and to ensure that messages were not manipulated or transmitted by an attacker. Encryptions are performed with the Advanced Encryption Standard (AES)-128 algorithm [Nat01]. Memberships to AVLNs are handled by secret Network Membership Keys (NMKs), which have to be the same for all participating STAs. If a STA wants to join an AVLN, it has to search for its beacon and scan the Network ID (NID) field, which is a hash of the NMK. If it matches its own NID, it can start to join the network by communicating management messages with the CCo. HomePlug AV has two Security Levels (SLs) [Hom12b, Chapter 7.10.3.1 p. 402 ff.] that define which NMK distribution method is allowed. If the *Simple Security Level* is in use, a button on STAs may be pushed to bring them in a setup state, where a random NMK is generated and shared between all STAs. With the *Secure Security Level*, the user has to set the Network Password (NPW) in all STAs manually. The NMK is derived from the NPW and never distributed to other STAs. Figure 3.22 shows the process of generating the NMK and NID: after the user enters the NPW, it is converted to the 128 bit NMK by the Password-Based Key Derivation Function (PBKDF1)[22]. For both security levels, the NMK is run through the PBKDF1 and combined with the SL to obtain the AVLN's NID. Hence, two devices can only join the same AVLN if their NMKs and SLs match. A more detailed overview of the security mechanisms in HomePlug AV is given in [NYGA07]. Once they have joined an AVLN, STAs use another secret key, the Network Encryption Key (NEK), to encrypt the body of transmitted PPDUs (PL data except frame header and footer, refer to Figure 3.15). The NEK is generated once by the CCo and distributed (encrypted with the NMK) to all STAs connected to its AVLN [Hom12b, Chapter 7.10.4 p. 410 f.].

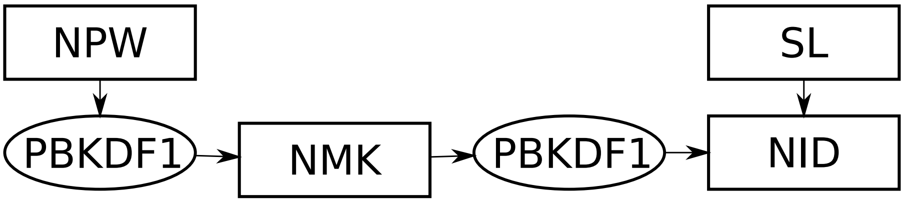


Figure 3.22: Construction of the network id.

[22] The PBKDF1 [RSA99, Chapter 5.1 p. 7 f.] takes a password string of arbitrary length and produces a key of fixed length. It applies a hash function iteratively to the password together with an optional *salt* value. HomePlug AV uses Secure HAsh (SHA)-256, a salt of $0x08856DAF7CF58186$ and 1000 iterations. As the PBKDF1 with SHA-256 produces a 256 bit key, only the leftmost 128 bits are taken as AES key.

## 3.2 HomePlug Green PHY

The HomePlug Green PHY specification is a simplified and fully interoperable version of HomePlug AV, dedicated to Smart Grid scenarios at the consumer's premises. Important design goals were low power usage, interoperability with other HomePlug devices and lower device costs due to less complex hardware: "[...] [T]he HomePlug GP specification was developed specifically to support Smart Grid Applications on the Home Area Network [...] within the customer premises. The HomePlug Alliance had to find a means of reducing cost and power consumption while maintaining HomePlug AV/P1901 interoperability, reliability and coverage.“ [Hom12a, Chapter 'The HomePlug Green PHY Standard' p. 7]. Green PHY is derived from the AV specification by introducing some major simplifications and the new features *power save mode*, *distributed bandwidth control* and *Plug-in Electric Vehicle (PEV) association*.

The most important simplification is the exclusive use of ROBO modes which modulate all carriers with QPSK. Hence, there is no need for channel estimation and administration of tone maps. Furthermore, the PHY layer only uses the Turbo convolutional encoder of rate $\frac{1}{2}$, removing the need for puncturing. The MAC layer is simplified by completely omitting support for TDMA channel allocations.

According to [Hom12a, p. 15], the introduced power save mode [Hom12b, Chapter 5.9 pp. 302-309] can reduce power consumption by up to 95%. Devices can enter one of 11 possible power save schedules by requesting it from the CCo. As depicted in Figure 3.23, each power save period is divided in awake (marked gray in the figure) and sleep phases and lasts $2^n$, $n \in [0, 1, .., 10]$ integer multiples of the beacon period. Hence, it is ensured that all devices' awake phases have regular intersections and all STAs can communicate with each other.

The distributed bandwidth control was introduced to prevent Green PHY devices from disturbing prioritized AV traffic like voice or video transmissions which rely on low jitter values. If a Green PHY device transmitting with non-zero priority detects AV traffic which also does not have zero priority, it reduces its transmissions to maximally 7% of the time on wire. It still may contend at priority 0 to transmit its prioritized and normal messages.

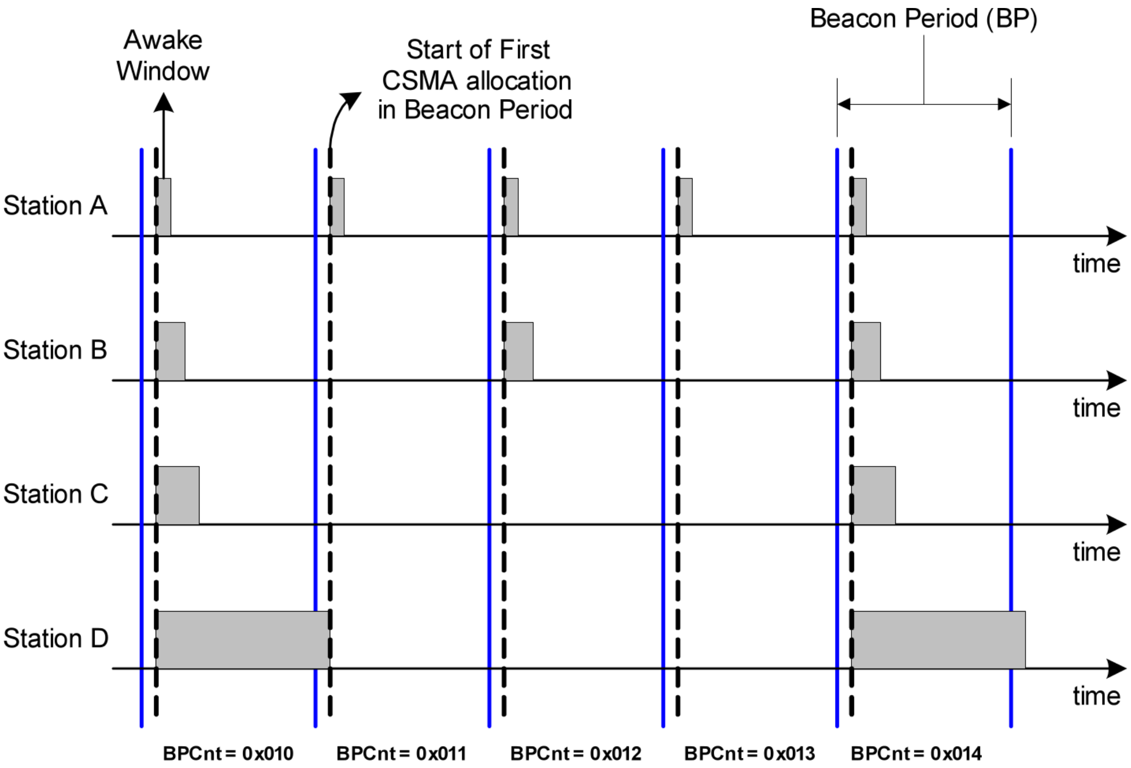


Figure 3.23: HomePlug Green PHY power save schedules, taken from [Hom12b, Figure 5-30 p. 304].

One use-case of HomePlug Green PHY is communication during the charging of electrical cars. The new feature *PEV association* facilitates the distinction between different Electric Vehicle Supply Equipments (EVSEs) (i.e. battery chargers) in the moment a car is connected. There may be several EVSEs in hearing range of the PEV and when plugged in, a private network with the correct charger has to be established. HomePlug Green PHY uses the attenuation of amplitude levels to distinguish different EVSEs, as depicted in Figure 3.24. The first Green PHY STA (the car) has to communicate with EVSE-1, but its signal also reaches EVSE-2 due to RF coupling between neighboring wires. However, due to the additional attenuation caused by the longer propagation path and coupling losses, the signal's level is lower at the second EVSE. PEV association is a simple protocol where the PEV issues a specific broadcast message, all EVSEs receiving it compute the message's amplitude level and report it to the PEV. Upon receiving all answers, the EVSE with the least attenuation is the nearest and chosen as the correct one.

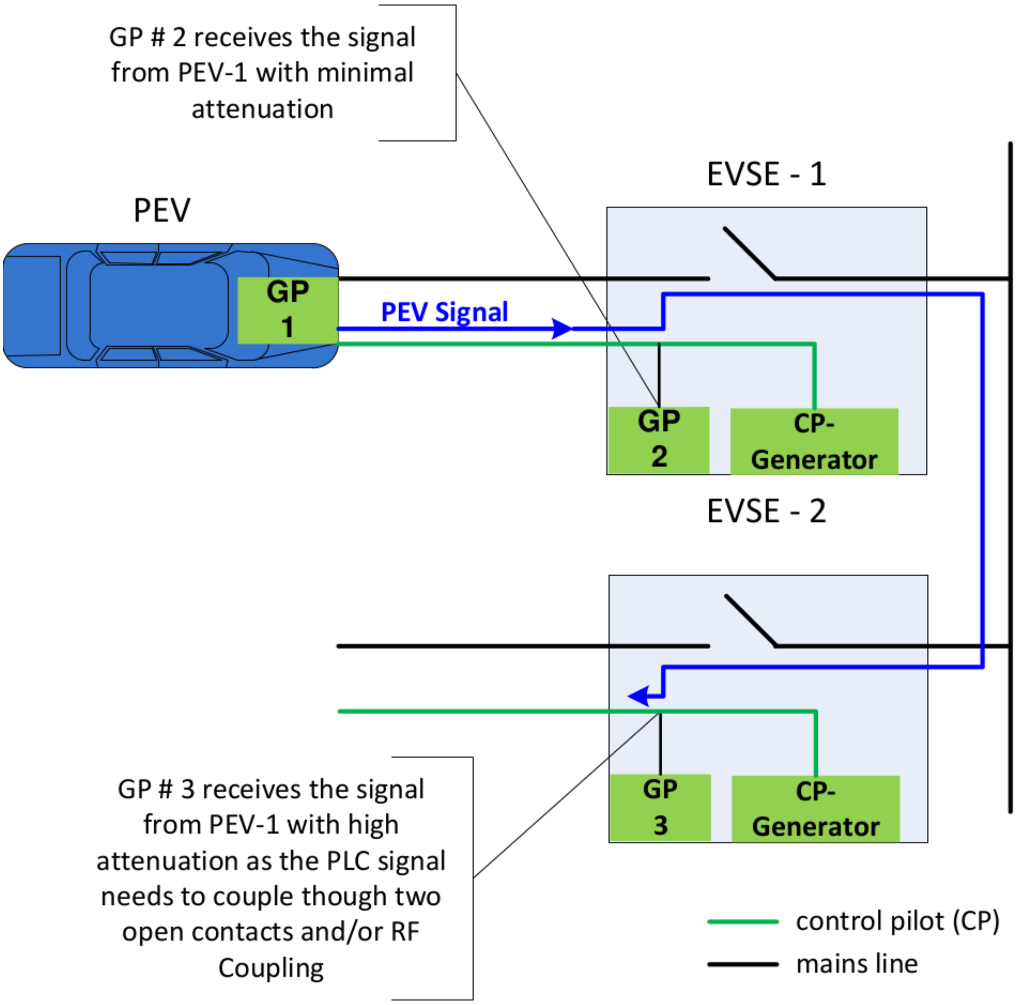

GP # 2 receives the signal from PEV-1 with minimal attenuation
PEV
GP 1
PEV Signal
EVSE - 1
GP 2
CP-Generator
EVSE - 2
GP 3
CP-Generator
GP # 3 receives the signal from PEV-1 with high attenuation as the PLC signal needs to couple though two open contacts and/or RF Coupling
control pilot (CP)
mains line

Figure 3.24: Plug-in vehicle association, taken from [Hom12b, Figure 13-3 p. 719].

# 4 The Power Line Channel

As the power line network in and outside of buildings was built to distribute electrical power and not for communication purposes, it is a very hostile environment for data transmissions. Different effects lead to impairments of transmitted signals which are discussed in the next section. Chapter 4.2 presents two methods for channel measurement with their advantages and drawbacks. In Chapter 4.3.1, a simulation based on the channel model in Chapter 4.1 is introduced and simulation results are compared with their empirically-measured counterparts. Finally, Chapter 4.3.2 presents a simulation of a simple OFDM system transmitting through the measured channels.

## 4.1 Channel Characteristics and Models

The characteristics of power line channels are dominated by three main effects: attenuation, notches (bounded, periodic regions with additional attenuation) and noise, all varying with frequency. The former is mainly caused by the skin-effect and dielectric losses along the signal's propagation path and decreases exponentially with approximately $\sqrt{f}$ [ZD02, Chapter `II.C` p. 2]. As wavelengths of broadband PLC signals are located between $3m$ and $300m$,[23] echoes caused by multipath propagation with path length differences in the range of meters can cause severe notches in the channel's Transfer Function (TF) (more detailed derivation later in this section). In contrast to designated communication networks like coaxial or Ethernet wiring, the power distribution grid was not designed to transmit messages. Power lines are neither shielded, nor twisted and hence subject to more interference from coupled RF signals. Furthermore, household devices can introduce additional noise, as they were designed without stringent radiation constraints. Hence, the noise in PLC networks has three components: conventional thermal Additive White Gaussian Noise (AWGN), narrowband interference from RF transmissions and impulsive noise either following the periodicity of the mains network or appearing in random intervals [Phi99, Chapter 5 p. 19 f.].

[23] The frequency range from $1MHz$ to $100MHz$ commonly used for BPL systems equals a wavelength range from $300m$ down to $3m$.

During the last two decades, several power line channel models for signal attenuation, phase distortion and noise effects have been proposed. In 1998, Waldeck et al. presented a first model for broadband communications with focus on noise, neglecting the characteristic notches present in real power line networks [WBD98, Chapter 3.2 p. 74 f.]. They showed the composition of noise in AWGN, narrowband and impulsive components mentioned above. One year later, a publication with two different approaches to model notches introduced by multipath propagation followed [Phi99] – firstly, in time domain with echoes arriving at the receiver with different delays and attenuation; secondly, in frequency domain by a concatenation of resonant circuits[24], which model distinct loads along the signal's path and introduce notches. Both methods lead to similar results. In 2002, Cañete et al. performed channel measurements after connecting several devices which are likely to be found in a usual home, such as a vacuum cleaner, microwave oven or electric shaver to the power grid [CDCE02]. They measured impedance values and the noise generated by the devices to create a time varying channel model. In 2006, the authors extended their model with periodic noise [CAdRM06] and refined it in 2010 [CDCSM10] by taking into account the difference between the amplitudes of the three noise components. In 2011, they published the complete channel model as a MATLAB simulation [Can11], describing it in more detail in [CCDE11]. In all models mentioned so far, the channel's transmission characteristics are measured and the model parameters fitted to match them, which is called the top-down method. In contrast to that, a bottom-up approach can be found in [MCG$^+$04]. There, a mathematical model is derived from RF theory and its parameters are filled in by measurements of the channel properties such as number of paths, path lengths and cable parameters (geometry, conductivity and permeability). The modeled TF resembles the measured channel. The downside of this approach is the need for cable parameters, which can differ from location to location and cannot be measured easily. Another bottom-up model for an in-car scenario is presented in [LCDD08] and reveals fair results.

A Field-Programmable Gate Array (FPGA) based MIMO channel implementation can be found in [WET14]. It is intended for transmission simulations of modern PLC technologies such as HomePlug AV2 or G.hn, which support MIMO transmissions over the three wires phase, neutral and earth. The channel is implemented using discrete Impulse Responses (IRs) which model echoes and the crossover between MIMO channels.

[24] The authors define a "Series Resonant Circuit" as a serial connection of a resistor, capacitor and inductor with element values adjusted to lead to a resonance frequency at the location of the notch to model.

The model utilized in this thesis comes from the work in [ZD02], which is a top-down approach excluding noise. The ability to also use the model with a slightly modified bottom-up approach was the reason to choose this model over others. Although the results are less accurate in the bottom-up case, it is possible to extrapolate the parameters to other scenarios without having to measure the channel again. Modeling is done in frequency domain and derived from the topology of the mains network, which is segmented into parts which are depicted in Figure 4.1. As the network is built for power distribution, impedance matching is not performed at loads other than PLC modems. The three line segments (1), (2) and (3) in Figure 4.1 have different impedance values $Z_{l1}$, $Z_{l2}$ and $Z_{l3}$ and interconnect two modems located at the points A and C. The modems' impedance is matched to the line segment they are connected to ($Z_{l1}$ for the modem at point A and $Z_{l2}$ for the modem at point C) and the impedance at point D is unequal to $Z_{l3}$. The mismatches at points B and D lead to reflections with coefficients depending on the impedance values

$$r = \frac{Z_2 - Z_1}{Z_1 + Z_2},$$

with the impedance of the section on the path the signal is coming from $Z_1$ and the impedance of the next section $Z_2$. A signal sent by the modem at point A reaches the receiver at point B on an infinite number of different paths: on the direct link $A \to B \to C$, and the longer paths $A \to B \to D \to B \to C$, $A \to B \to D \to B \to D \to B \to C$ and so forth [ZD02, p. 554]. Each path has a different attenuation which is composed of the path loss depending on the length of the link and the magnitude of the product of all reflection coefficients along the path, which are assumed to be real-valued to simplify the model.[25] In a typical power line network, devices with nonlinear loads like signal rectifiers may be present, too. However, the effect is not strong and although this model does not include nonlinear loads, the accuracy of the results is still good.

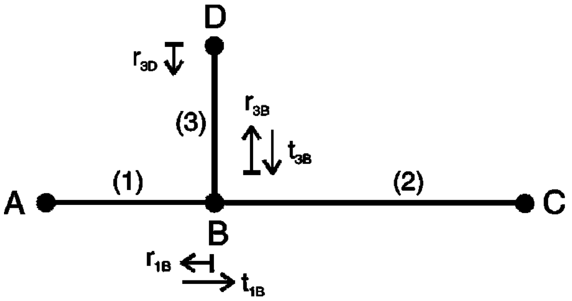


Figure 4.1: A channel with one tap.

[25] According to "Extended measurement campains" the weighting factors of the links can be assumed to be real-valued in "many cases of practical interest" [ZD02, Chapter III B p. 555].

The path loss is caused by a combination of the skin effect, dielectric losses and radiation of the signal power and can be modeled by $e^{-(a_0+a_1 f^k)d}$ with the link's length $d$ and the *attenuation* parameters $a_0$, $a_1$ and $k$. These are fixed for all paths and have to be determined once for each setup by a measurement of the channel. Due to the strong attenuation of longer links, only a reduced number of relevant paths $N$ is considered in practice. According to the Fourier shift theorem

$$\mathscr{F}\left\{x(t-\tau)\right\} = \mathscr{F}\left\{x(t)\right\} * e^{-j2\pi f\tau}\,, \tag{4.1}$$

a signal's propagation time $\tau$ introduces a linear phase component in frequency domain. The fraction of the received and transmitted spectra ($\underline{R}(f)$ and $\underline{S}(f)$, respectively) is modeled by the channel $\underline{H}(f)$, which is a superposition of all N considered propagation paths

$$\frac{\underline{R}(f)}{\underline{S}(f)} = \underline{H}(f) = \sum_{i=1}^{N} \underbrace{g_i}_{\substack{\text{weighting}\\ \text{factor}}} \underbrace{e^{-(a_0+a_1 f^k)d_i}}_{\text{attenuation}} \underbrace{e^{-j2\pi f\tau_i}}_{\text{delay}}\,. \tag{4.2}$$

The link parameters $g_i$, $d_i$ and $\tau_i$ are different for each path $i$. In [ZD02], the authors prefer to substitute the link delay $\tau = \frac{d}{v}$ with the link length and the signal's propagation speed which can be expressed in terms of the speed of light $c_0$. Signals propagate in coaxial cables with $v \approx 0.66 \cdot c_0$ and in power lines with $v \approx 0.5 \cdot c_0$ to $v \approx 0.6 \cdot c_0$. As determining $v$ is an additional and not necessary step, this model is slightly modified to accept link delays and lengths instead of propagation speeds and lengths.

The superposition of all links causes interference at the receiver and hence notches in the TF. To derive notch positions, consider the channel in the form

$$\begin{aligned}
\underline{H}(f) &= \sum_{i=1}^{N} \underbrace{g_i e^{-(a_0+a_1 f^k)d_i}}_{\text{Amplitude}} \underbrace{e^{-j2\pi f\tau_i}}_{\text{Phase}} \\
&= \sum_{i=1}^{N} \underline{H}_i(f) = \sum_{i=1}^{N} A_i e^{-j\varphi_i}\,,
\end{aligned}$$

with the abbreviation functions

$$\begin{aligned}
A_i(f) &= |\underline{H}_i(f)| = g_i e^{-(a_0+a_1 f^k)d_i} \\
\varphi_i(f) &= \angle(\underline{H}_i)(f) = 2\pi f\tau_i\,.
\end{aligned}$$

The channel TF for two paths reads as

$$\underline{H}(f) = A_1 e^{-j\varphi_1} + A_2 e^{-j\varphi_2}$$

and the location of notches can be derived from the magnitude of the TF

$$\begin{aligned}
|\underline{H}|^2 &= \underline{H}(f)\underline{H}(f)^{\,*} \\
&= \left(A_1 e^{-j\varphi_1} + A_2 e^{-j\varphi_2}\right)\left(A_1 e^{j\varphi_1} + A_2 e^{j\varphi_2}\right) \\
&= A_1^2 + A_2^2 + A_1 A_2 \left(e^{j(\varphi_1-\varphi_2)} + e^{-j(\varphi_1-\varphi_2)}\right) \\
&= A_1^2 + A_2^2 + 2A_1A_2\cos(\varphi_1-\varphi_2) \\
&= A_1^2 + A_2^2 + 2A_1A_2\cos(2\pi f(\tau_1-\tau_2))\,.
\end{aligned}$$

The attenuation portions $A_1^2$ and $A_2^2$ are positive and decrease exponentially with $f$, the cosine term causes the notches with periodicity depending on the difference between the path delays $\tau_1$ and $\tau_2$. Since the sign of an exponential function with real argument is positive, the signs of $A_1$ and $A_2$ only depend on those of $g_1$ and $g_2$. If $g_1$ and $g_2$ have the same sign, notches occur when the cosine is minimal

$$\begin{aligned}
\cos(2\pi f_{Notches}(\tau_1-\tau_2)) &\overset{!}{=} -1 \\
\Rightarrow 2\pi f_{Notches}\,|\tau_1-\tau_2| &= \pi + n\cdot 2\pi, \quad n \in \mathbb{N}_0^+ \\
\Rightarrow f_{Notches} &= \frac{n+\frac{1}{2}}{|\tau_1-\tau_2|}\,.
\end{aligned} \tag{4.3}$$

If $g_1$ and $g_2$ have different signs, notches occur when the cosine is maximal

$$\begin{aligned}
\cos(2\pi f_{Notches}(\tau_1-\tau_2)) &\overset{!}{=} +1 \\
\Rightarrow f_{Notches} &= \frac{n}{|\tau_1-\tau_2|}, \quad n \in \mathbb{N}_0^+\,.
\end{aligned} \tag{4.4}$$

The measurement of a channel with two significant paths can be found in the next section.

## 4.2 Channel Measurement

For the estimation of model parameters and comparison of results, the channel's TF has to be measured. For this thesis, an Agilent N8241A ARBitrary waveform generator (ARB) with a symbol rate of $625MHz$ (symbol period of $1.6ns$) was used as transmitter and an Agilent MSO6054A oscilloscope with a bandwidth of $500MHz$ and sampling rate of $5GSa/s$ as receiver. The devices were connected through couplers to a channel consisting of a multi-way connector with an open end like depicted in Figure 4.2. The labels A-D refer to the positions in Figure 4.1 and L is the length of the multi plug itself, measured from the end of its cable to the port furthest from the cable (on the bottom in the figure). As there is nearly no impedance mismatch at point B, this channel has two relevant paths: $A \to B \to C$ and $A \to B \to D \to B \to C$ with a delay difference of $\Delta\tau = \tau_2 - \tau_1 \approx \frac{2L}{v}$ with signal propagation speed $v$ and neglecting that the second path's additional length is slightly shorter than $2L$ (by the distance between input and output ports). The ARB and the oscilloscope are connected with $5m$ coaxial cables to the couplers, which are both connected to the multi plug with $\approx 2m$ power wires, resulting in the shortest link length of $\approx 14m$ from transmitter to receiver. Additionally, the output of the ARB is directly connected to the oscilloscope, in order to be able to record the transmitted waveform, too.

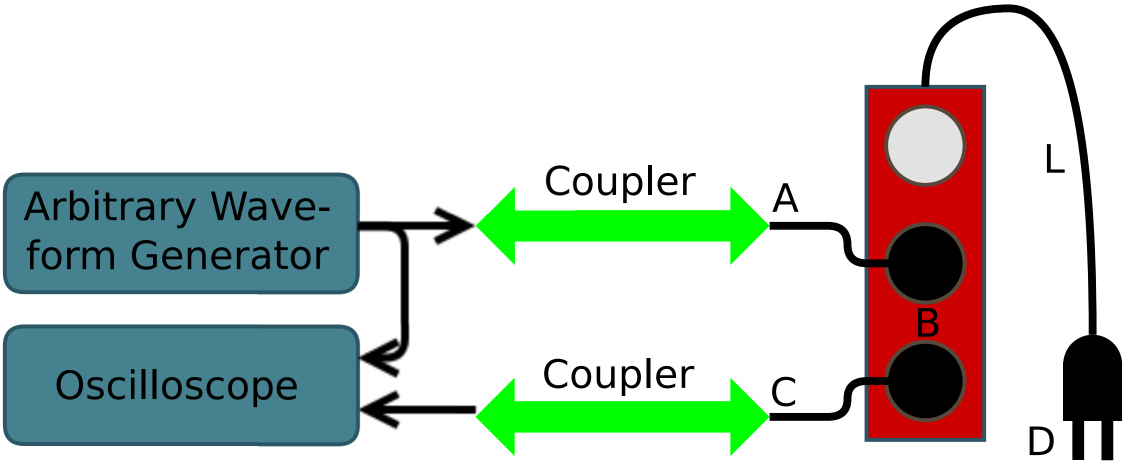


Figure 4.2: Channel measurement setup.

One method to measure the channel is to transmit a sweep signal $s(t)$ in the time interval $[t_0, t_1]$ with linearly increasing frequency in the range $[f_0, f_1]$

$$f(t) = f_0 + \underbrace{\frac{(f_1 - f_0)}{t_1 - t_0}}_{=:k}(t - t_0) = f_0 + k(t - t_0)\,.$$

To get the phase $\phi(t)$ of the transmission signal $s(t) = a\cos(\phi(t))$ with amplitude $a$, the time varying frequency has to be integrated

$$\begin{aligned}\phi(t) &= \phi_0 + 2\pi \int_{t_0}^{t} f(t')dt' \\ (\dots) \\ &= \phi_0 + 2\pi k \left[\frac{1}{2}t^2 + \left(\frac{f_0}{k} - t_0\right) t + \frac{1}{2}t_0^3 - t_0^2 + \frac{f_0}{k}t_0\right] .\end{aligned}$$

A reasonable simplification can be made if $t_0$ and $\varphi_0$ are selected as zero

$$\begin{aligned}\phi(t)\Big|_{\substack{t_0=0\\ \phi_0=0}} &= 2\pi\left(\frac{f_1 - f_0}{2t_1}t^2 + f_0 t\right) \\ \Rightarrow s(t) &= a\cos\left(2\pi\left(\frac{f_1 - f_0}{2t_1}t^2 + f_0 t\right)\right) .\end{aligned}$$

Figure 4.3 shows an example for $a = 0.2V$, $t_1 = 1s$, $f_0 = 1Hz$ and $f_1 = 10Hz$.

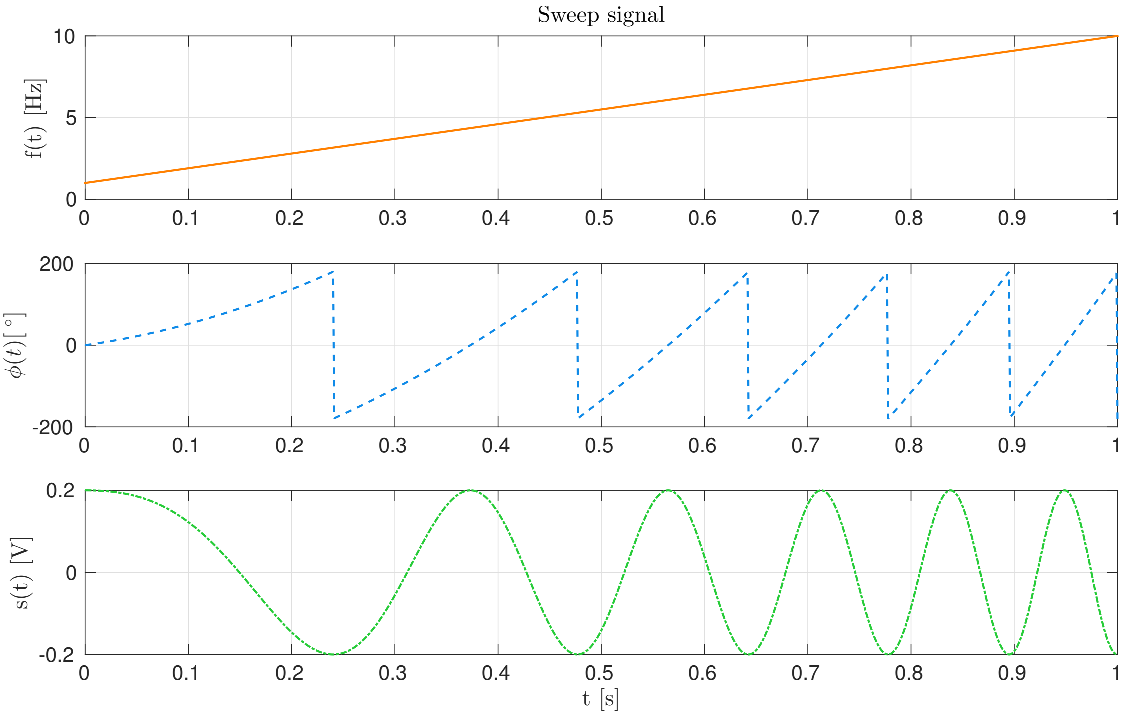


Figure 4.3: Exemplary sweep signal from $1Hz$ to $10Hz$.

If a sweep signal is used for channel estimation, the received waveform divided by $a$ yields the channel TF's magnitude for the frequency range $[f_0, f_1]$. The result for $f_0 = 1MHz$, $f_1 = 30MHz$, $t_1 - t_0 = 1ms$ and a channel as depicted in Figure 4.2 with $L = 3m$ is shown in Figure 4.4. The blue curve in the background is recorded by the probe near the transmitter and the green curve in the foreground by the probe near the receiver. Frequency starts with $1MHz$ at the left ($t = t_0$) and increases to $30MHz$ at the right ($t = t_1 = t_0 + 1ms$). The recorded transmission waveform is not identical to the actually transmitted one, because it also contains interference from reflections. However, the received waveform is exactly what a modem at point C would receive. Although it is easy to deduce the channel's magnitude, deriving the phase from this kind of measurement is difficult.

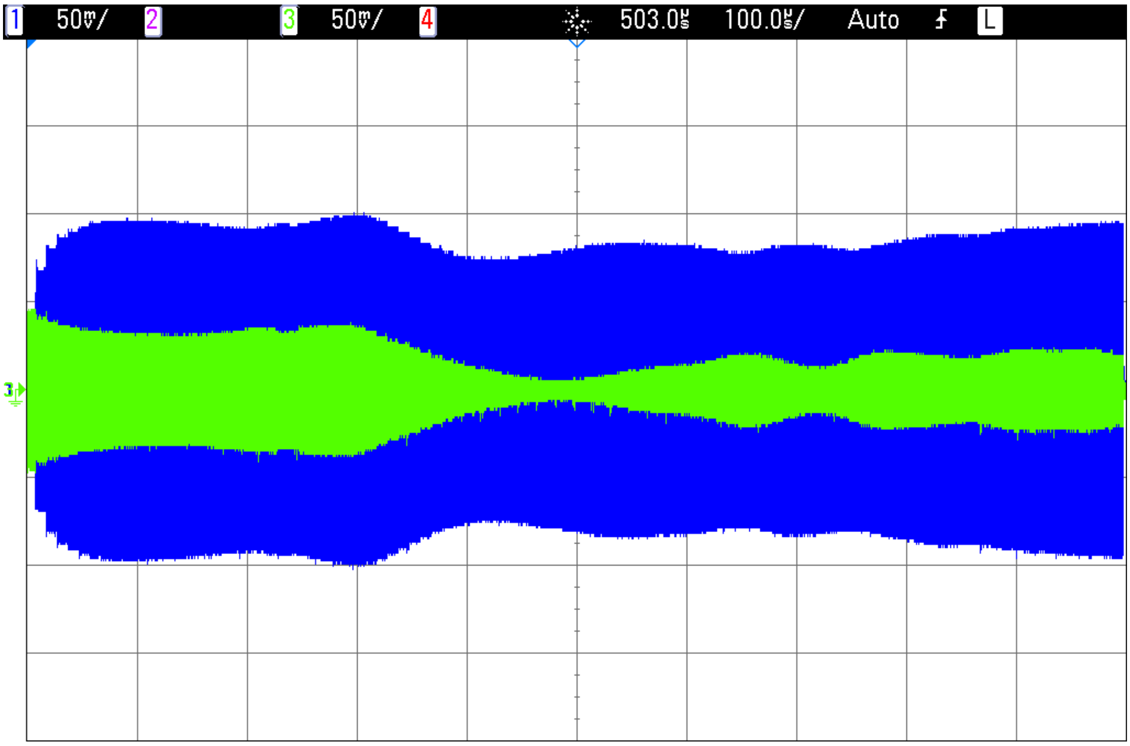


Figure 4.4: Channel measurement with a sweep signal ($1MHz$ to $30MHz$).

A better alternative is to use a short Dirac-like impulse instead of a sweep signal. By transforming transmitted and received signals to frequency domain, the channel can be derived by dividing the spectra

$$\underline{H}(f) = \frac{\underline{R}(f)}{\underline{S}(f)} = \frac{\mathscr{F}\{r(t)\}}{\mathscr{F}\{s(t)\}} .$$

The recorded waveforms of the Dirac approach for the same channel as before are depicted in Figure 4.5. The transmission range is reduced to the marked region between $2ns$ and $40ns$ to measure only the transmitted waveform and exclude the reflections starting at $60ns$. Regarding the transmitted curve (solid orange), it is obvious that the signal is not a true Dirac impulse and its spectrum is shown in Figure 4.6. As the transmission signal $s(t)$ in Figure 4.5 can be decomposed in a convolution of a true Dirac impulse at $14ns$ with a window of the visible shape and $\approx 5ns$ width, the signal's Fourier transform is a multiplication of a constant, a linear phase introduced by the time shift of $14ns$ and the Fourier transform of the window. Since the shape resembles a rectangle, the spectrum is similar to a sinc function[26]. It can be seen, that the spectrum does not differ too much from a constant for frequencies below $100MHz$ which makes the transmitted waveform a fair approximation of a Dirac impulse for the regarded frequencies. The received waveform (dashed blue) clearly shows a direct path starting at $90ns$ and one echo starting at $120ns$.

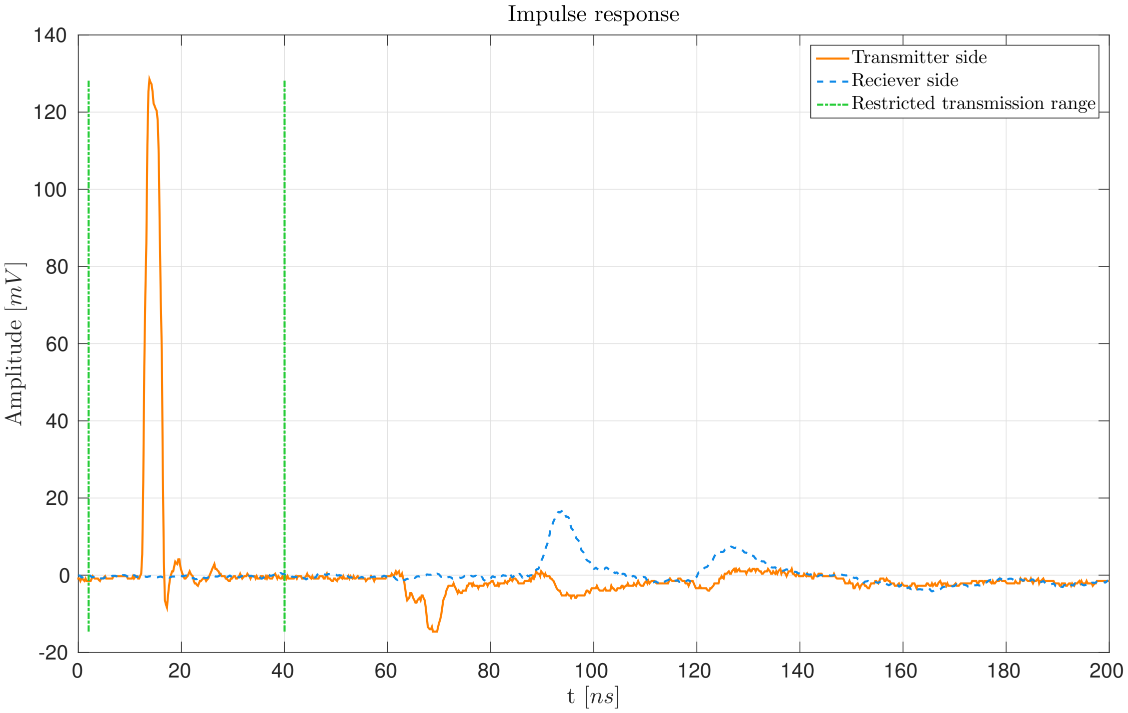


Figure 4.5: Channel measurement with a Dirac impulse.

The derivation of the TF can be seen in Figure 4.7 which is depicting the Fourier transforms of transmitted (solid orange) and received (dashed blue) signals and the resulting TF (dotted green). While all calculations in this thesis are performed in continuous time, the channel measurement and simulation deal with digital data in discrete time. As the

[26] The sinc function is defined as $\text{sinc}(x) = \frac{\sin(x)}{x}\ \forall x \neq 0,\ 1\,\text{for}\,x = 0$.

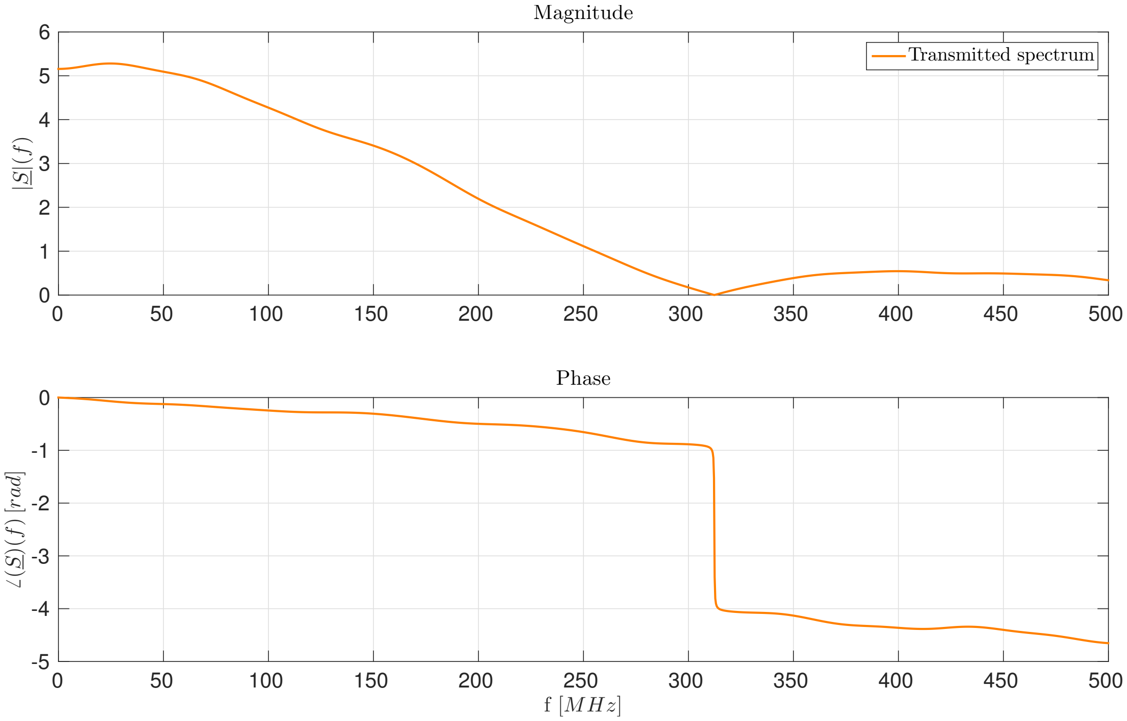


Figure 4.6: The transmission spectrum up to $500MHz$.

continuous Fourier transform is only applicable to signals with infinite time and frequency domain, its discrete counterpart has to be used, which itself implicitly assumes periodic waveforms. If non-periodic data is processed, a windowing function $w(t)$ (or $w(f)$ for the inverse Fourier transform) has to be applied prior to the transform. Without windowing, the spectrum is convolved with a sinc function which introduces unwanted side lobes of peaks. In this thesis, a *Nuttall* window was found to work well, due to its good suppression of side lobes. Since windowing functions highly alter the signal at its beginning and end, the waveforms in Figure 4.5 are shifted before windowing, so that their biggest peaks are in the middle of the window. After the Fourier transform, this shift has to be canceled with the help of the Fourier shift theorem given in Equation (4.1). Moreover, frequencies above $f_{\max}$ are clipped, which is always $100MHz$ in this thesis if not stated otherwise. The complete transform reads as

$$\begin{aligned}\underline{H}(f) &= \frac{\mathscr{F}\left\{r(t-\Delta t_r)\right\}}{\mathscr{F}\left\{s(t-\Delta t_s)\right\}} \cdot e^{+j2\pi f(\Delta t_r - \Delta t_s)} \\ h(t) &= \mathscr{F}^{-1}\left\{\underline{H}(f)|_{f\le f_{\max}} \cdot w(f)\right\}\ , \end{aligned} \tag{4.5}$$

with the time shifts $\Delta t_r$ and $\Delta t_s$ before windowing. The channel's IR $h(t)$ is needed in the next section. A closer look at the phase plot in Figure 4.7 reveals the linear phase at

$f_{\max}$, caused by the signal's propagation time

$$\angle(\underline{H})(f_{\max}) = 2\pi \cdot 100MHz \cdot (92ns - 14ns) \approx 49\,\text{radians}\,,$$

with the delays of the transmitted signal and the first received peak $14ns$ and $92ns$, respectively. According to Equation (4.3), the paths with delay difference $\Delta\tau = \tau_2 - \tau_1 \approx 125ns - 92ns = 33ns$ and the same sign of $g_1$ and $g_2$ lead to notches at

$$f_{Notches} = \frac{n + \frac{1}{2}}{\Delta\tau} \approx (n + \frac{1}{2}) \cdot 30MHz = [15, 45, 75, ...]\,MHz\,,$$

which can be seen in Figure 4.7. The notch for $f = 15MHz$ is also present in the middle of the received sweep signal in Figure 4.4, which ranges from $1MHz$ on the left to $30MHz$ on the right. Note that the shape of the curve is different, because the plot is in linear and not logarithmic domain like in Figure 4.7.

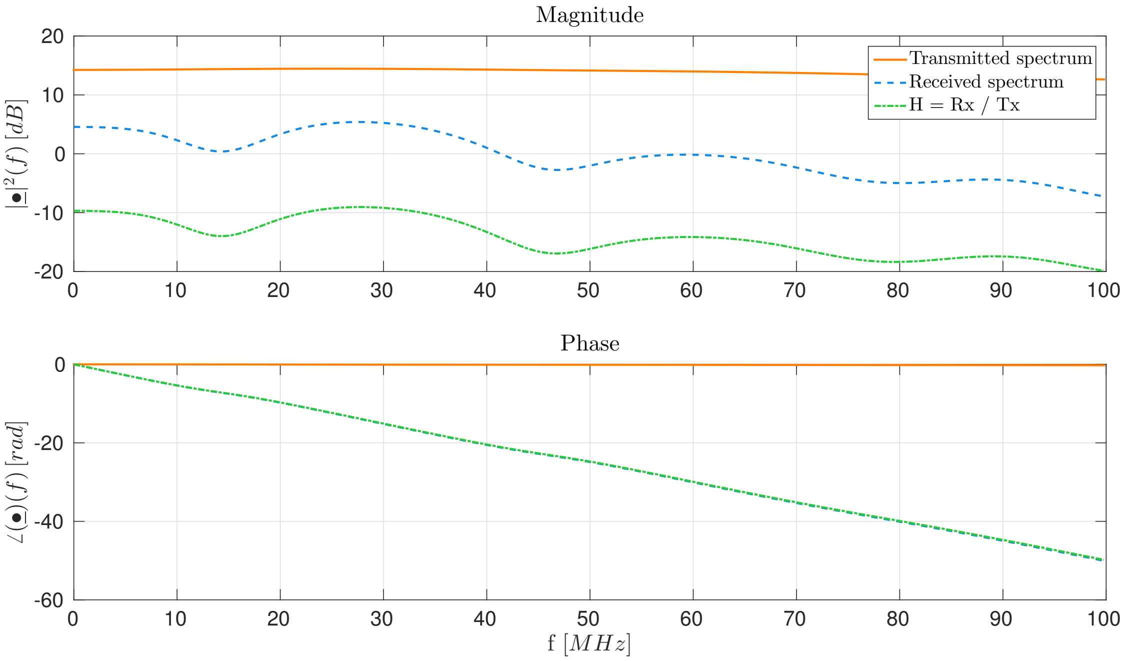


Figure 4.7: Measured channel converted to frequency domain.

## 4.3 Simulation

This section presents a channel model based on the work in [ZD02] and a simple OFDM transmission simulation.

### 4.3.1 Channel Simulation

To represent a measured channel with the model introduced in Equation (4.2), the number of significant paths $N$, the *attenuation parameters* $a_0$, $a_1$, $k$ and *link parameters* $g_i$, $d_i$, $\tau_i$ with $i = [1, 2, \ldots, N]$ have to be derived, for which there are two different methods. The bottom-up approach is to measure the network's topology with link lengths and potential reflections at end points to derive the link parameters. Although a channel measurement still has to be performed to get the attenuation parameters, the model can easily be extrapolated to similar setups by assigning new link parameters. However, while measuring link lengths and delays may be easy, it is nearly impossible to get accurate values for the reflection coefficients. Moreover, as the attenuation parameters model the path loss without reflections, they can only be measured correctly if a reference network without taps is available. The second and top-down parameter estimation method starts with the measured channel and tries to find all parameters by an optimization algorithm without any further knowledge of the underlying network and yields more accurate results. This method is very handy to use, provided that one has access to channel measurement devices like those introduced before. There is no need to manually measure link lengths, delays and reflection coefficients. Despite these benefits, the top-down approach also has its disadvantages. Each channel of interest has to be measured and its parameters optimized, there is no means to extrapolate the model to other setups. Additionally, the resulting link and attenuation parameters only resemble the physical network and do not match it exactly. Both approaches are evaluated in this thesis.

For the optimization of model parameters in the top-down approach, an evolutionary algorithm was used by the authors in [ZD02], as well as in this thesis. Zimmermann and Dostert use a three-step approach, where they derive the attenuation parameters from the measurement by least-squares fitting of a one-link model to the measurement at first. Then they perform a peak detection of the IR to get the number, delay and amplitude of significant paths. In case many echoes exist in the network, they use the evolutionary strategy to further optimize the parameters [ZD02, Chapter *IV B* p. 556]. However, it turned out that for the measurements in this thesis, which are made in smaller networks[27], better results can be achieved with a two-step approach. The first step remains peak detection to get the echo delays (but not amplitudes). If the values of the attenuation parameters are derived by a least-squares approach from the measured channel with taps, they are not accurate due to the deep notches. Even with sophisticated preprocessing, the result is worse than just including the attenuation parameters in the evolution. Thus, the second step is performing the evolutionary algorithm for both attenuation and link parameters. Peak detection is a very difficult process if it is performed on the channel IR derived by the inverse Fourier transform in Equation (4.5). The side lobes introduced by spectral leakage can not be easily distinguished from real channel echoes. Hence, peak detection is performed on the original received waveform.

The general idea behind evolutionary algorithms is to mimic evolution found in nature by implementing *selection*, *reproduction* and *mutation* of *individuals*. Each individual represents one specific set of values for all parameters to optimize, which is randomly generated at the beginning of the algorithm. During selection in each generation, a certain share of the weakest individuals of the population dies and is replaced by children of the fittest individuals. Fitness values are determined for all individuals by the error between the channel model based on their parameter values $\underline{H}_e(f)$ and the measured curve $\underline{H}_m(f)$

$$\begin{aligned}
\varepsilon_{\text{real}} &= \sqrt{\frac{1}{f_{\max}} \int\limits_{0Hz}^{f_{\max}} \mathcal{R}e\{\underline{H}_m(f') - \underline{H}_e(f')\}^2 df'} \\
\varepsilon_{\text{imag}} &= \sqrt{\frac{1}{f_{\max}} \int\limits_{0Hz}^{f_{\max}} \mathcal{I}m\{\underline{H}_m(f') - \underline{H}_e(f')\}^2 df'} \\
\text{Fitness} &= \frac{1}{\varepsilon_{\text{real}}} + \frac{1}{\varepsilon_{\text{imag}}} .
\end{aligned}$$

Although it is possible to do the comparison in time domain, results are better for the method presented above. Spectral leakage introduces a convolution with a sinc function which degrades the IR resulting in slightly inaccurate modeling. Moreover, the Fourier transform unnecessarily consumes additional computational time. During reproduction, the child of two parents gets a randomly selected subset of parameters from one parent and the rest from the other, which mimics the cross-over of chromosome parts in nature. The concept of two chromosomes in biology is not part of the algorithm. Finally, mutation is performed by adding an AWGN to all of a child's parameters. The noise's standard

[27] Zimmermann and Dostert measured power line grids with lengths of $200m$ and longer, whereas the longest link in this thesis is under $50m$.

deviation is adopted to each parameter's value range, which itself is fixed for the whole simulation. Most evolution parameters can be found in Table 4.1. Two methods are used to control the grade of random search vs. evolution: varying population size and mutation rate. If the former is increased, more individuals with a higher spread of parameter values are available for recombination and more children with good parameters can arise – at the expense of more computational power. If the mutation rate is too high, children of fit parents can degrade due to the high noise power affecting their parameters. The values of 400 individuals and 1% of the parameters' range are a compromise which provides a quick increase in fitness per generation and moderate computational power. As indicated by the average and best fitness values per generation in Figure 4.8, saturation of the fitness values occurred after approximately 150 generations. The figure shows the fitness of individuals during evolution for the channel introduced before. To make sure fitness approaches saturation, the number of generations was set to 400. The bounds in Table 4.1 define the allowed values for all parameters. If a child's parameter happens to lie outside the bounds after mutation, it simply gets clipped. The last parameter sets a penalty for children with a link whose propagation speed $v_i = \frac{d_i}{\tau_i}$ is either slower than $0.4 \cdot c_0$ or faster than $0.9 \cdot c_0$ with the speed of light $c_0$. An infinite penalty leads to an instant death of such children, avoiding unphysical results. As the likelihood is very small that all link propagation speeds of all individuals are in the given range after mutation, nearly each generation has some individuals with zero fitness. This is the reason that the curve for worst fitness values in Figure 4.8 is zero for nearly all generations. The distribution of individuals' ages can be seen in Figure 4.9, which does not include newborns. In the example, their share of $\frac{168}{400} = 42\%$ complies to the range fixed in Table 4.1.

| Parameter | Value |
|---|---|
| Number of individuals | 400 |
| Number of generations | 400 |
| Share of population which survives a generation | 50% to 60%, selected randomly in each generation |
| Mutation standard deviation | 1% of each parameter's range |
| Attenuation and link parameter bounds | $a_0 \in [-0.1,\ 0.1] \cdot \frac{1}{m}$<br>$a_1 \in [1.0 \cdot 10^{-11},\ 5.0 \cdot 10^{-7}] \cdot \frac{s}{m}$<br>$k \in [0.5,\ 1]$<br>$g \in [-1,\ 1]$<br>$d \in [5,\ 100] \cdot m$<br>$\tau \in [50,\ 500] \cdot ns$ |
| Penalty for unphysical link speeds | $\infty$ |

Table 4.1: Parameters of the evolutionary algorithm.

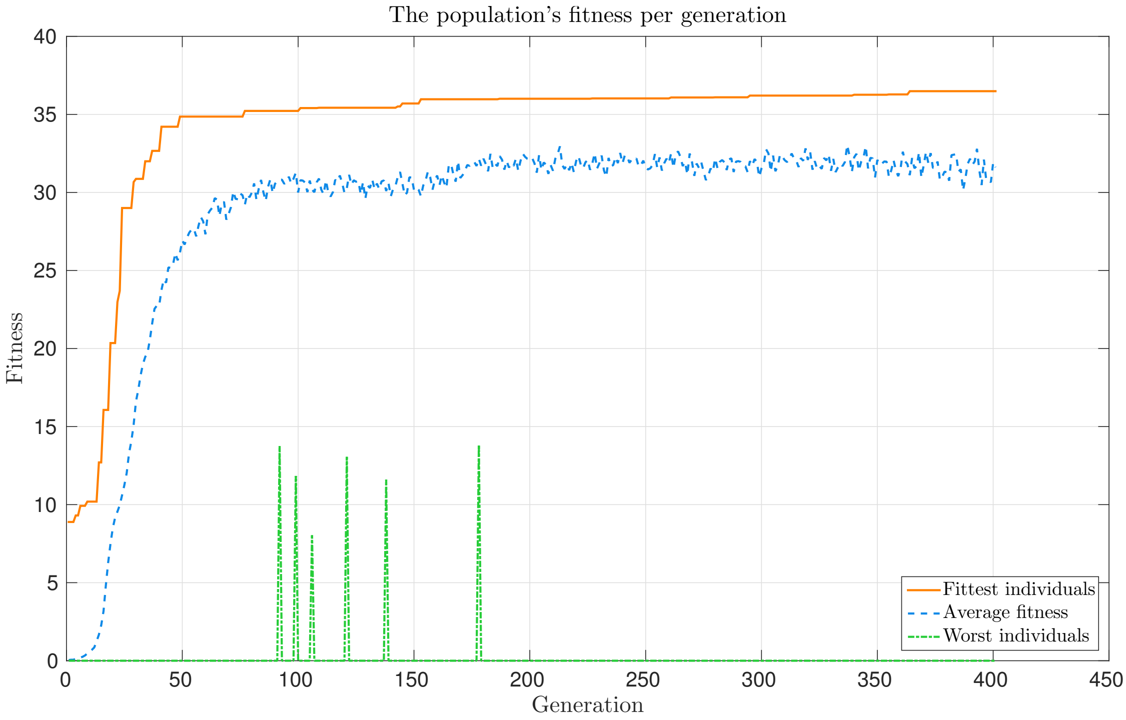


Figure 4.8: The fitness of individuals during evolution.

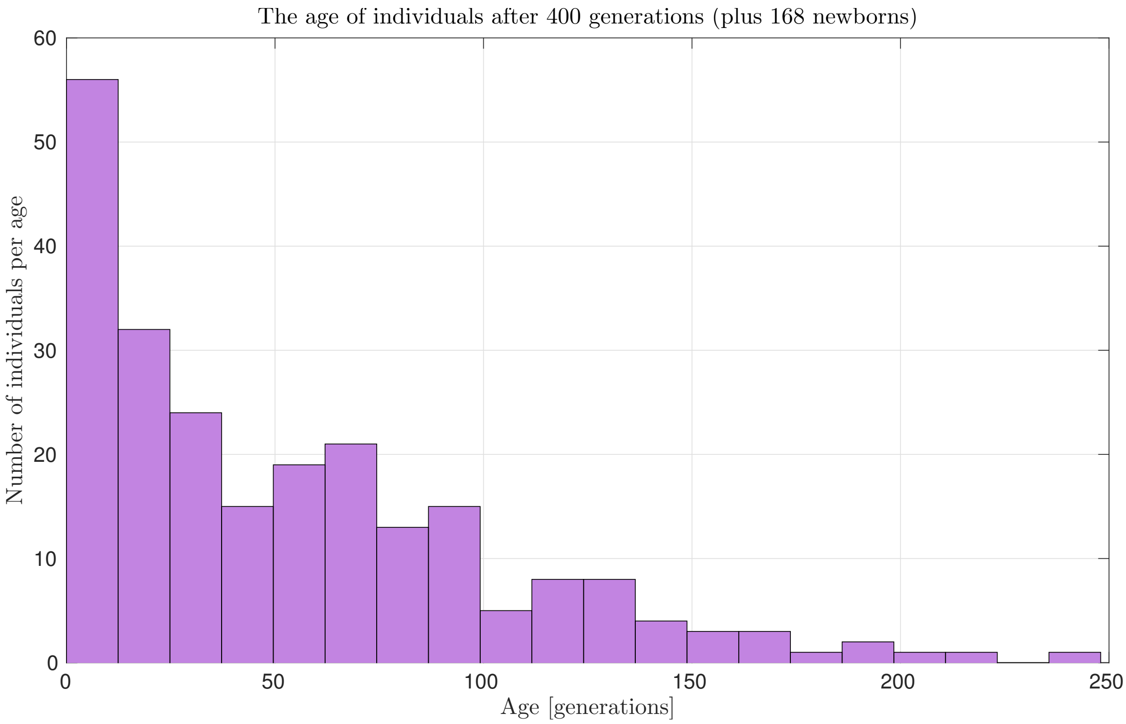


Figure 4.9: Age distribution after 400 generations without newborns.

Turning to the results now, Figure 4.10 depicts the measured channel and two models of it, once with parameters derived by the bottom-up approach (*Composition of link approximations*) and once with parameters derived from the evolutionary algorithm. It is clearly visible, that the latter gives a closer approximation of the channel. However, the former also incorporates the typical characteristics of the channel – the positions of the notches are nearly correct and the angle is also similar to the original. The channel's IR is shown in Figure 4.11. Its shape is different from that in the original measurement presented in Figure 4.5, due to the low pass filtering caused by discarding all frequencies above $f_{\text{max}} = 100MHz$ and convolution with the Nuttall window.

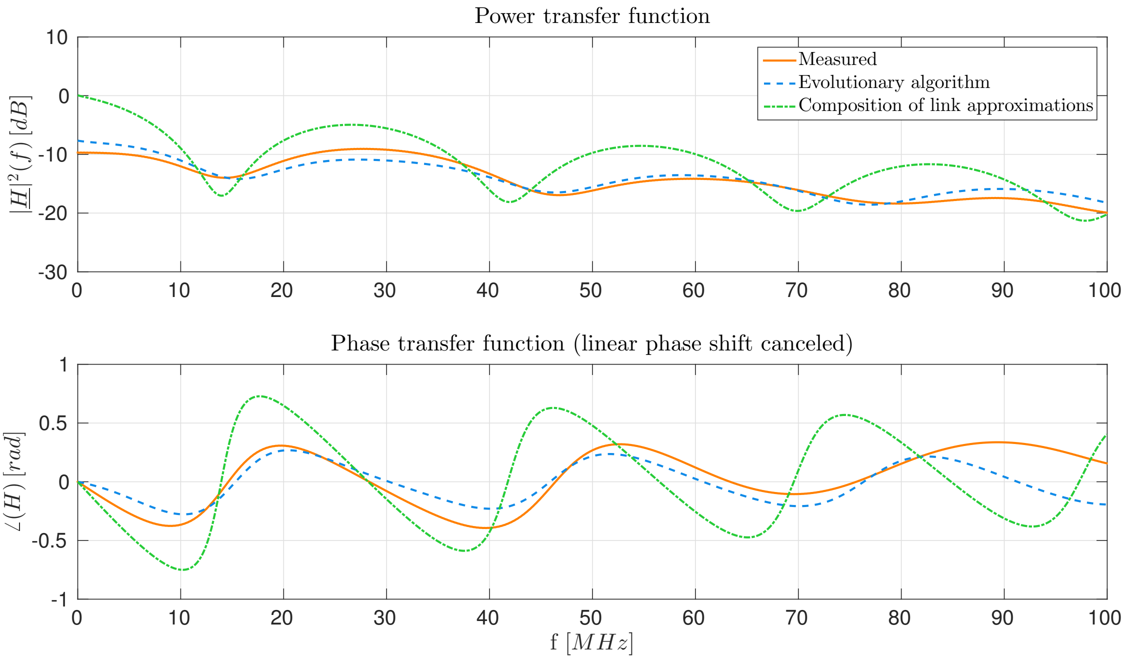


Figure 4.10: The channel of setup 4 in frequency domain.

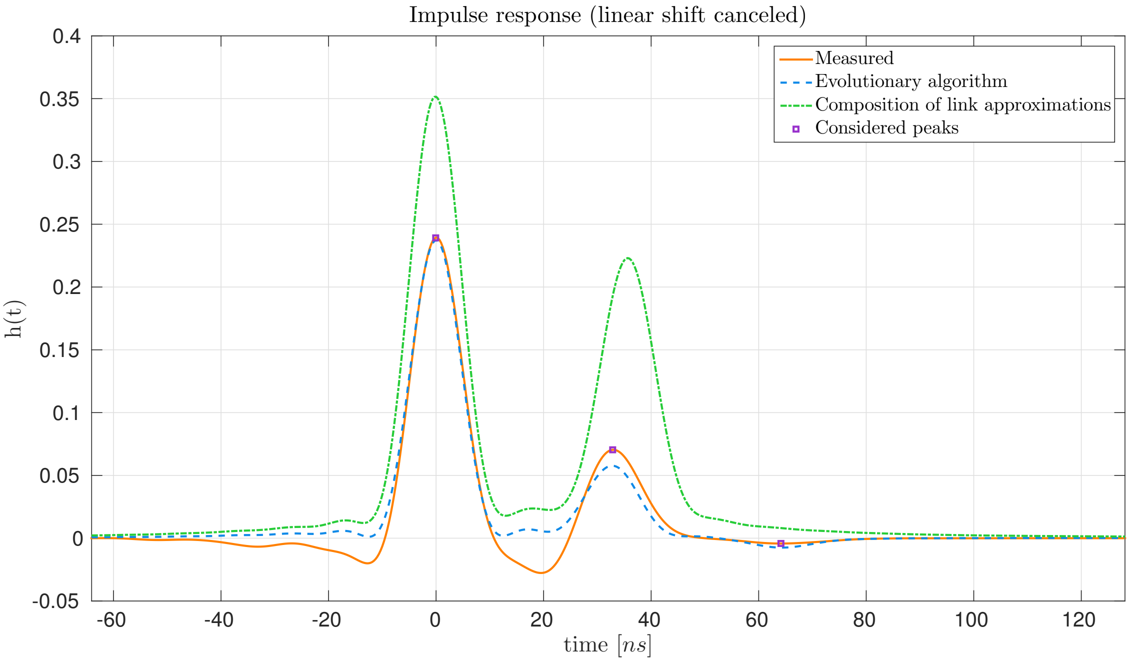


Figure 4.11: The channel of setup 4 in time domain.

The channel plots for setups other than the one discussed so far can be found in the appendix, the attenuation and link parameters derived by evolution are summarized in Table 4.2. A short description of the setups 1 to 6 is given in the following.

- Setup 1.a is a back-to-back experiment, directly connecting the coaxial cables coming from the ARB to the oscilloscope, leaving out the couplers. This setup has only one path of $10m$ length.
- In setup 1.b, the couplers are included and their ends are not plugged into any power line grid, but directly connected. The main path is $14m$ in this setup and the couplers introduce little reflections.
- The setup 2.a is similar to that in Figure 4.2 with Length $L = 1.6m$, except that the end of the multi plug has a matched impedance ($Z_D = 50\,\Omega$). Here, the shortest link is also $14m$ long and as the impedance matching is not perfect, a path with smaller reflection coefficient and a length of $\approx 17m$ is also present.
- 2.b is the same as 2.a with the end left open ($Z_D = \infty\,\Omega$).
- 2.c is the same as 2.a with the end short-circuited ($Z_D = 0\,\Omega$).
- Setups 3, 4 and 5.a are also similar to 2.a, but use other multi plugs with $L = 2.5m$, $L = 3m$ and $L = 3.45m$, respectively.
- In scenario 5.b the multi-way connector with $L = 3.45m$ is connected to the power line grid of an office, resulting in more links, which can not be predicted easily.
- In 5.c the integrated switch on the $L = 3.45m$ multi-way connector is turned off, eliminating the second path.
- Cabling in 6.a is done similarly to 2.a, except that a $10m$ extension cable is inserted between the multi plug and the coupler of the oscilloscope (lengthening the distance between points B and C) to increase attenuation. The path difference is similar, the delay is increased for both pats.
- 6.b is the same as 6.a with a $9.4m$ extension cable.
- 6.c is the combination of 6.a and 6.b with both, the $10m$ and $9.4m$ extension leads concatenated.

| Setup | $a_0$ | $a_1$ | $k$ | Path i | $g_i$ | $d_i$ | $\tau_i$ |
|---|---|---|---|---|---|---|---|
| 1.a | -2.72e-02 | 6.55e-08 | 0.71 | 1 | 0.81 | 7.10 | 5.16e-08 |
| 1.b | 1.38e-02 | 1.26e-07 | 0.76 | 1 | 0.60 | 9.52 | 7.94e-08 |
| | | | | 2 | -0.48 | 26.15 | 9.97e-08 |
| 2.a | 8.49e-02 | 1.43e-07 | 0.72 | 1 | 0.99 | 13.50 | 7.94e-08 |
| | | | | 2 | 0.11 | 14.08 | 1.08e-07 |
| 2.b | 6.30e-02 | 1.67e-07 | 0.73 | 1 | 0.69 | 10.93 | 7.91e-08 |
| | | | | 2 | 0.67 | 20.66 | 1.01e-07 |
| | | | | 3 | -0.88 | 28.58 | 1.22e-07 |
| 2.c | 8.49e-02 | 2.21e-07 | 0.72 | 1 | 0.79 | 9.77 | 7.94e-08 |
| | | | | 2 | -0.91 | 15.87 | 1.00e-07 |
| | | | | 3 | 0.35 | 32.22 | 1.22e-07 |
| 3 | 6.04e-02 | 5.92e-08 | 0.76 | 1 | 0.80 | 13.78 | 7.91e-08 |
| | | | | 2 | 0.43 | 19.64 | 1.09e-07 |
| 4 | 3.88e-02 | 6.62e-08 | 0.77 | 1 | 0.54 | 11.06 | 7.97e-08 |
| | | | | 2 | 0.16 | 14.00 | 1.12e-07 |
| 5.a | 7.83e-02 | 8.48e-09 | 0.86 | 1 | 0.96 | 14.29 | 7.91e-08 |
| 5.b | 6.32e-02 | 3.39e-08 | 0.79 | 1 | 0.54 | 10.06 | 7.94e-08 |
| 5.c | 9.64e-05 | 7.86e-09 | 0.89 | 1 | 0.50 | 13.30 | 8.03e-08 |
| 6.a | 5.05e-02 | 9.99e-08 | 0.76 | 1 | 0.78 | 17.45 | 1.43e-07 |
| | | | | 2 | -0.65 | 45.86 | 1.72e-07 |
| | | | | 3 | -0.91 | 46.70 | 2.08e-07 |
| 6.b | 5.13e-02 | 2.44e-07 | 0.71 | 1 | 0.83 | 17.45 | 1.44e-07 |
| | | | | 2 | -0.38 | 44.32 | 1.72e-07 |
| | | | | 3 | -0.68 | 40.46 | 1.95e-07 |
| | | | | 4 | -0.60 | 47.69 | 2.22e-07 |
| 6.c | 3.41e-02 | 3.42e-07 | 0.68 | 1 | 0.70 | 25.17 | 2.08e-07 |
| | | | | 2 | -0.27 | 62.15 | 2.38e-07 |
| | | | | 3 | -0.97 | 61.75 | 2.71e-07 |
| | | | | 4 | -0.71 | 58.97 | 3.05e-07 |
| | | | | 5 | -0.00 | 60.72 | 3.45e-07 |

Table 4.2: Link and attenuation parameters for all setups.

Regarding setups 6.a to 6.c, it is visible that the recorded waveform is degraded – two effects are involved in changing the signal's shape. The increased curliness comes from the higher impact of noise, due to the lower Signal to Noise Ratio (SNR). The broadening of the impulses is caused by more dispersion due to the higher link length, caused by nonlinear phase components of the TF. Using a higher transmission amplitude could lower the influence of noise, but needs an additional short-wave amplifier, which was not present when the channel measurements were recorded.

In setup 2.c, the path with delay $\Delta\tau = 22.5ns$ and negative reflection coefficient from the short-circuited end of the multi plug introduces notches at the locations

$$f_{Notches} = \frac{n}{22.5ns} \approx n \cdot 44.4MHz \approx [0, 44, 89, ...]\, MHz\,,$$

according to Equation (4.4). It can be seen, that the path with closed end really acts as a short-circuit for low frequencies. The following section presents a small simulation which illustrates the impact of notches and angle distortions on transmissions.

### 4.3.2 Transmission Simulation

A basic OFDM system is used in this transmission simulation to modulate a frame and send it over a measured channel. The transmitter side consists of a data source, an M-QAM mapper and an OFDM modulator, whereas the number of modulation levels $M$ can be freely chosen out of the set $M \in 2^m\, m = [1, 2, \dots]$ and is fixed to $M = 2^4 = 16$ here. The data source can either produce a vector with all zeros, or filled with values randomly chosen out of the set $[0, 1, \dots, M-1]$. The mapper transforms the integer vector coming from the source to a complex representation, using M-QAM, gray-coded assignment of indices and scaling such that the real and imaginary parts of the symbols with maximum power lie on the points $(\pm 1, \pm j)$ (which corresponds to a maximum magnitude of $\sqrt{2}$). The OFDM modulator appends the conjugate-complex negative frequencies equal to the examples in Chapter 3.1.1.2 and adds predefined initial phases to all carriers. During transmission, the OFDM vector is multiplied with the channel's TF, transformed to time domain, perturbed with AWGN and converted back to frequency domain. The receiver firstly scales the frame in such a way that its biggest entry is $\sqrt{2}$ and removes the linear phase introduced by the channel – this step assumes that the receiver has basic knowledge about the channel. Subsequently, the OFDM demodulator removes the initial phases and discards negative frequencies. Finally, the M-QAM demapper reveals the received copy of the source vector.

The transmissions in the rest of this chapter were performed over the channel of setup 4, which is depicted in Figure 4.7. By using the zero-data source and a very high SNR value, the effect of the channel on all carriers can be visualized and is shown in Figure 4.12. The same point in the complex plane (small orange square at $(-1, j)$) is transmitted over all carriers and undergoes different magnitude and phase distortions, depending on the channel at the carrier's frequency. Attenuation of the signal by both path loss and notches affects the symbol's magnitude, phase shifts modify its angle. The linear phase is canceled in the figure, which would otherwise cause a huge frequency dependent clockwise rotation by the angle $2\pi f \Delta\tau$ around the origin $(0, 0j)$.

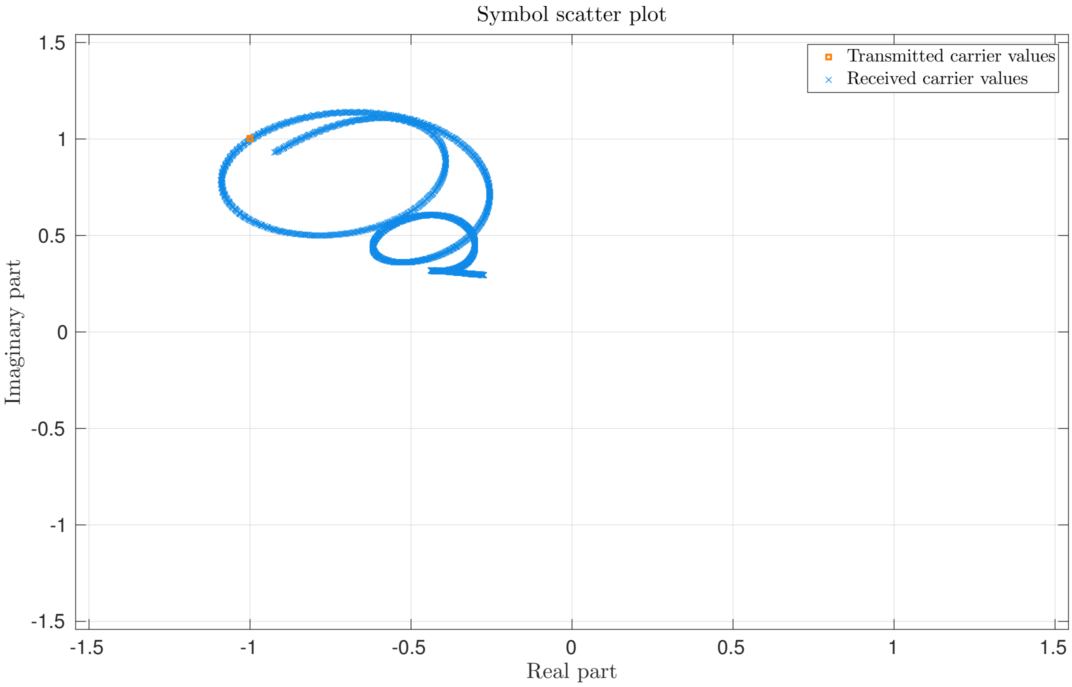


Figure 4.12: Transmitted and received symbol scatter plot for all-zero data.

The symbol space for randomly selected data and SNR $= 15dB$ can be seen in Figure 4.13. The transmitted signal is impaired by

$$\begin{aligned} r(t) &= s(t) + n(t), \quad n(t) \sim \mathcal{N}\left(0,\, \sigma_s \cdot 10^{-\frac{\text{SNR}}{10}}\right) \\ \Rightarrow r(t) &\approx s(t) + n(t) \cdot 32\sigma_s\,, \end{aligned}$$

with white noise $n(t)$ and standard deviation $\sigma_s$ of the signal. Here, all 16-QAM symbols are transmitted and it is obvious that many errors are introduced with this simple equalizer.

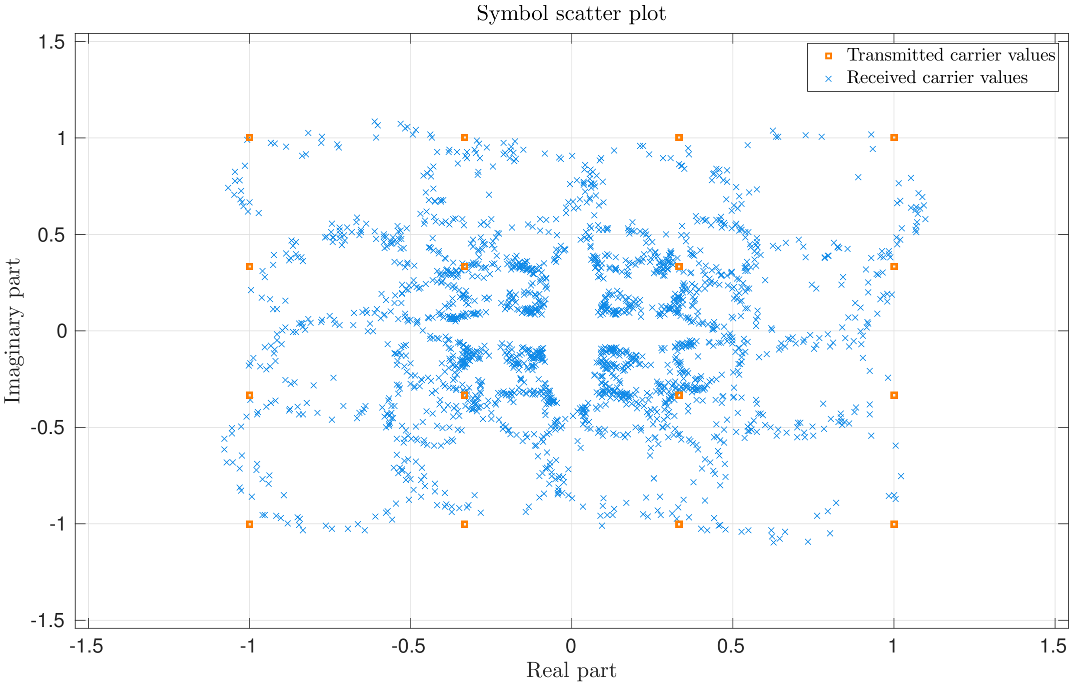


Figure 4.13: Transmitted and received symbol scatter plot for random data.

Figure 4.14 shows source and sink integer vectors prior to and after mapping of the same OFDM frame. The frequency bands with few and no errors ($0MHz$ to $5MHz$ and $20MHz$ to $35MHz$) correspond to TF ranges with no notches and few phase distortions (compare to the channel in Figure 4.7).

As a final remark, PLC channels fairly resemble those in mobile and in-home wireless broadband communications. Multipath propagation and the accompanying notches, interference from other transmissions and the shared medium are common properties. All these similarities lead to the fact that the design of BPL systems like HomePlug is related to those intended for WLAN networks.

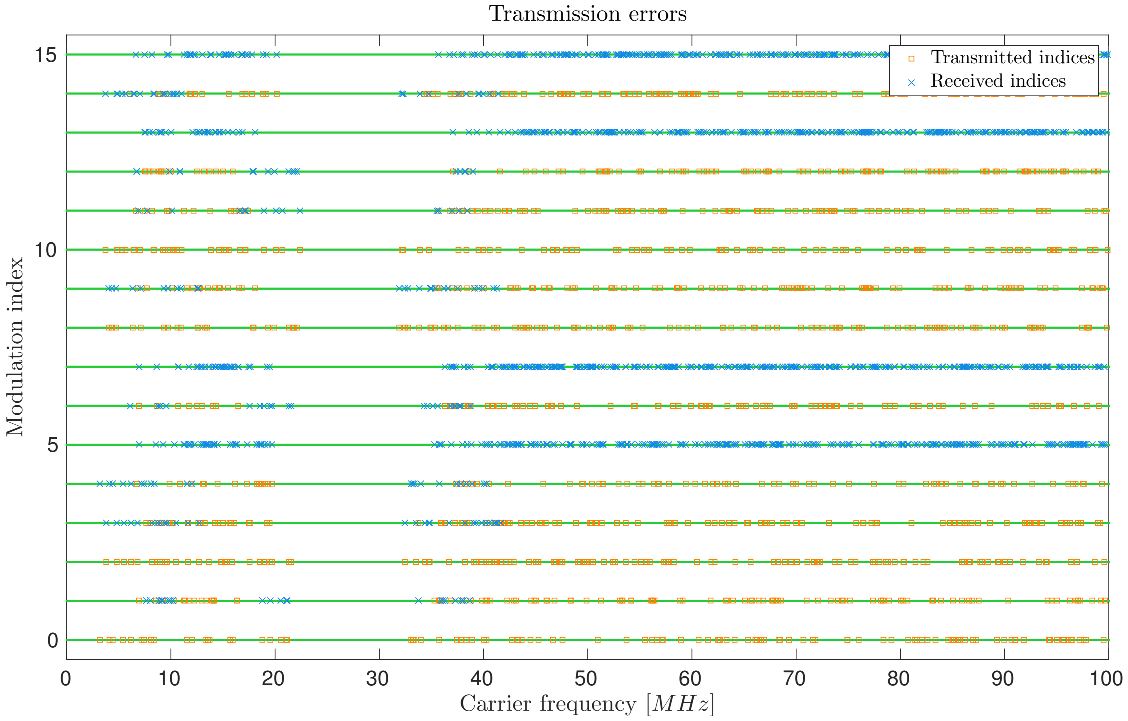


Figure 4.14: Carrier errors upon reception.

# 5 Performance Measurements

Variations of channel properties due to devices connected to and unplugged from the power line grid, fluctuating noise characteristics and the alternating network traffic load in the shared channel medium prohibit a deterministic calculation of network throughput. This chapter provides seven measurements of achieved bandwidth and the latency jitter values between HomePlug AV devices recorded under different circumstances. The test environment and procedure are described first and the results are presented afterwards.

## 5.1 Test Environment

The test setup comprises eight PLC modems, an Agilent N8241A oscilloscope (which was also used for channel measurements in Chapter 4.2) and a Rohde & Schwarz FSQ3 (1155.5001.03) spectrum analyzer which enables the monitoring of ongoing transmissions in frequency domain. Two types of HomePlug AV transceivers were used; six devolo dLAN 200 AVpro DIN rail modems, which are based on the Atheros INT6400 System on Chip (SoC) and two Tatung UDK-21 modems based on the STMicroelectronics STreamPlug 2100 SoC. While the former is an off-the-shelf product, the latter is still in development and provides more flexibility, as its MAC layer is implemented in software running on an ARM processor core. One of the benefits of the STreamPlug device is its ability to use FDMA by applying user defined tone masks to disable carriers. This functionality is used later in this chapter for one of the tests. With the setup depicted in Figure 5.1, up to three parallel and disjunct data streams were transmitted over the PLC network under test. The two instruments can be used to monitor channel contention and frequency usage of running transmissions.

For a complete test environment, network nodes producing and consuming traffic are needed, too. As shown in Figure 5.2, four Linux notebooks were used for this purpose. While three of them (notebooks 2 to 4) were serving as consuming nodes only, the first notebook hosted four Virtual Machines (VMs) with an attached USB to Ethernet adapter for each of them. The VMs 2 to 4 produced network traffic and VM1 was for remotely controlling notebooks 2 to 4 via WLAN and VMs 2 to 4 via the virtual VMware router inside of notebook 1.

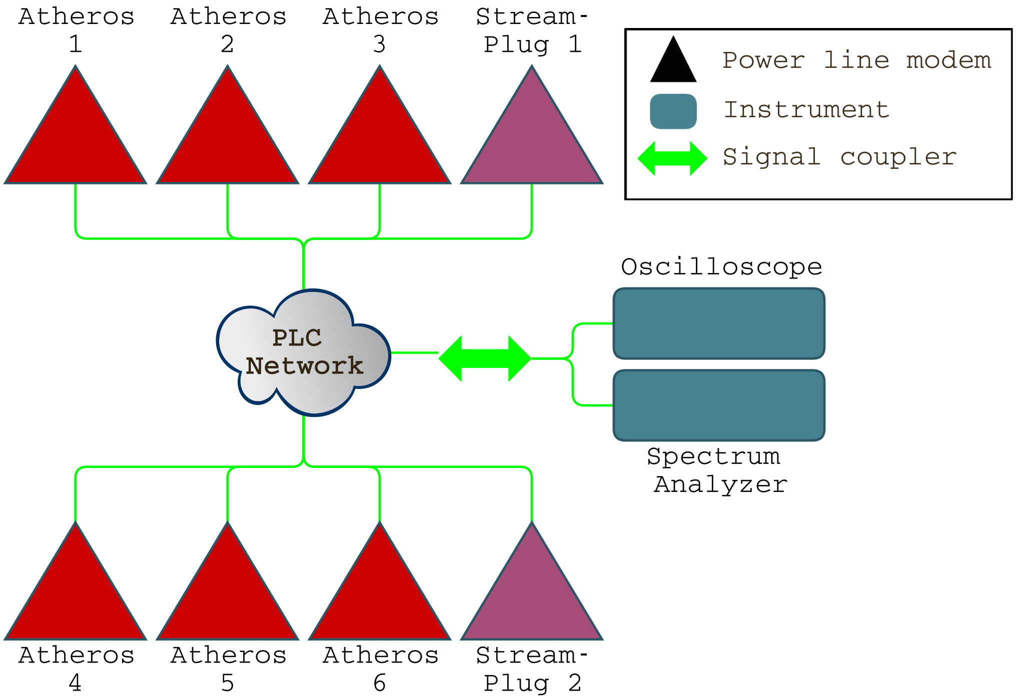


Figure 5.1: The power line part of the test environment.

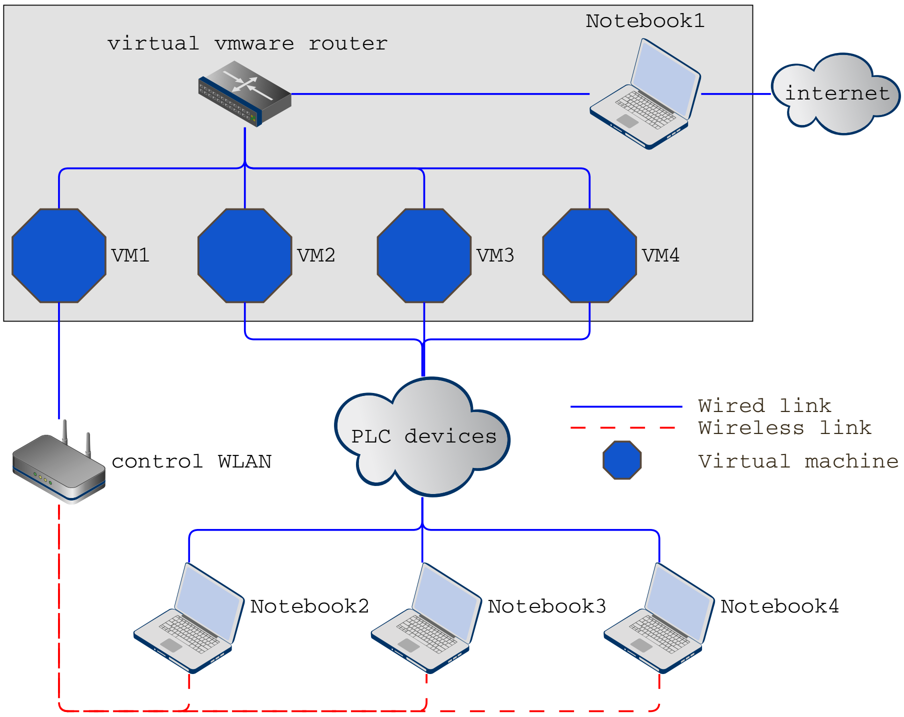


Figure 5.2: The traffic generation part of the test environment.

The bandwidth and delay jitter measurement software *iperf* [GTF+11] was used for all presented results. With this tool, it is possible to perform Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) throughput tests, as well as to determine the delay jitter of the connection between two nodes. Most tests also incorporate prioritized traffic which is transmitted with priority 3 by the powerline modems, like introduced in Chapter 3.1.2. The Linux kernel Internet Protocol (IP) tables on transmitting and receiving nodes were used to append to and process VLAN tags of Ethernet packets, respectively.[28] This way, six different tests were possible: Throughput measurements using the TCP with and without VLAN tags, the same tests using the UDP and finally delay jitter measurements with and without VLAN tags. All results were derived from transmissions with a duration of 20 seconds and at the highest possible data rate.

## 5.2 Measurement Results

The tests presented in this chapter were all performed using the environment in Figure 5.1 and Figure 5.2 with differing settings of the PLC modems, number of used modems and varied powerline networks. All setups have more than one configuration of their parameters, called *variations* from *a* up to *c*. Note that although measurement names here are similar to setup names in Chapter 4.3, they are not related in any way. Furthermore, if not mentioned otherwise, all measurements were obtained with Atheros modems connected to the same multiplug.

### 5.2.1 Measurement series 1

In this setup, the effect of the number of parallel streams was examined. *Variation a* contains one link, *variation b* two links and *variation c* three parallel links. Each column in Table 5.1 shows the results of the different tests (TCP, UDP, Jitter and their prioritized versions). All throughput results reflect a fair share of bandwidth. If more devices are willing to transmit, more time is needed for channel contention which leads to a small loss in total data rates. For example, the total prioritized UDP bandwidth is $86.3 Mbit/s$, $84.9 Mbit/s$ and $78.3 Mbit/s$ for variations a, b and c, respectively; resulting in a loss of $\approx 10\%$ for three parallel data streams compared to only one. If regarding the UDP results without prioritization, the total bandwidth of two links is higher than that of only one. Since the devices were operated in a typical office environment, the noise of the power line channel varied with time, leading to different transmission conditions

[28] At the transmitter, an additional virtual interface was created with the *ip* command which appended a VLAN tag with PCP 7 to all outgoing packets. The virtual interface at the receiver simply discarded the VLAN tag, as it was only used to force PLC modems to transmit packets at PLC priority 3.

and total achievable bandwidths. To obtain more comparable results, longer and multiple measurements recorded at different times of the day could be performed. However, the effects of varying channel properties would not be visible any more and the impact of the examined effects are still visible with theses results.

As all links transmitted at high priority in corresponding measurements, the additional time needed for the PRSs lowered the bandwidth by a small amount and no noteworthy difference between the links' throughputs occurred. Regarding the jitter values, it is evident that they are quite randomly distributed. Failures in channel contention and repeated losses of contentions can lead to higher delays and cause high jitter values.

| | TCP | TCP | UDP | UDP | Jitter | Jitter |
|---|---|---|---|---|---|---|
| | | prioritized | | prioritized | | prioritized |
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 72.1 | 70.2 | 87.6 | 86.3 | 0.114 | 0.156 |
| Measurement variation b | | | | | | |
| Link 1 | 36.0 | 35.7 | 39.5 | 45.4 | 0.561 | 0.152 |
| Link 2 | 32.1 | 31.3 | 49.5 | 39.5 | 0.338 | 1.381 |
| Measurement variation c | | | | | | |
| Link 1 | 21.9 | 21.9 | 26.4 | 26.8 | 0.696 | 0.335 |
| Link 2 | 22.7 | 23.5 | 25.7 | 23.9 | 1.481 | 0.703 |
| Link 3 | 24.6 | 24.4 | 29.3 | 27.6 | 0.488 | 0.441 |

Table 5.1: Throughput results for a different number of parallel steams.

### 5.2.2 Measurement series 2

The second setup measures the impact of prioritization. Variation a in Table 5.2 presents the results for one normal link and a priority link, clearly showing that bandwidth and jitter are far better for the latter. Even if a second normal link is added to the setup (variation b), the single prioritized link uses nearly all of the bandwidth. In variation c, two prioritized links share most of the bandwidth and the single normal link can hardly transmit packets.

| | TCP | TCP prioritized | UDP | UDP prioritized | Jitter | Jitter prioritized |
|---|---|---|---|---|---|---|
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | - | 66.1 | - | 79.5 | - | 0.118 |
| | - | ▭ | - | ▭ | - | ▭ |
| Link 2 | 3.1 | - | 4.9 | - | 2.251 | - |
| | ▭ | - | ▭ | - | ▭ | - |
| Measurement variation b | | | | | | |
| Link 1 | - | 65.8 | - | 82.3 | - | 0.128 |
| | - | ▭ | - | ▭ | - | ▭ |
| Link 2 | 2.6 | - | 1.1 | - | 2.223 | - |
| | ▭ | - | ▭ | - | ▭ | - |
| Link 3 | 1.2 | - | 1.2 | - | 2.109 | - |
| | ▭ | - | ▭ | - | ▭ | - |
| Measurement variation c | | | | | | |
| Link 1 | - | 34.6 | - | 44.4 | - | 0.544 |
| | - | ▭ | - | ▭ | - | ▭ |
| Link 2 | - | 32.6 | - | 39.8 | - | 0.169 |
| | - | ▭ | - | ▭ | - | ▭ |
| Link 3 | 0.1 | - | 0.2 | - | 5.703 | - |
| | ▭ | - | ▭ | - | ▭ | - |

Table 5.2: Throughput results for parallel prioritized and normal traffic.

### 5.2.3 Measurement series 3

Variations a and b in Table 5.3 were recorded with one pair of StreamPlug modems (link 1) and one or two pairs of Atheros modems, respectively. The lower bandwidth share and higher jitter values of StreamPlug modems are probably caused by processing delays in their software based MAC layers. As the modems are still under development, things might change with future firmware releases.

| | TCP | TCP | UDP | UDP | Jitter | Jitter |
|---|---|---|---|---|---|---|
| | | prioritized | | prioritized | | prioritized |
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 5.9 | 3.7 | 11.9 | 6.8 | 13.368 | 14.291 |
| Link 2 | 35.3 | 44.0 | 29.0 | 48.8 | 0.292 | 0.158 |
| Measurement variation b | | | | | | |
| Link 1 | 6.8 | 2.2 | 7.5 | 4.9 | 10.895 | 13.690 |
| Link 2 | 18.2 | 25.8 | 18.9 | 21.7 | 0.283 | 0.412 |
| Link 3 | 18.8 | 27.1 | 21.2 | 22.7 | 1.709 | 0.252 |

Table 5.3: Throughput results comparing StreamPlug and Atheros modems.

### 5.2.4 Measurement series 4

Setups 1 and 4 are identical, except that each link is in a separate AVLN in the latter. As AVLNs do not affect contention, there is no remarkable difference in bandwidths shown in Table 5.1 and Table 5.4. The fact that all results are slightly better in the latter is probably caused by less noise on the power line channel.

| | TCP | TCP<br>prioritized | UDP | UDP<br>prioritized | Jitter | Jitter<br>prioritized |
|---|---|---|---|---|---|---|
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 81.9 | 79.7 | 94.3 | 94.0 | 0.139 | 0.188 |
| Measurement variation b | | | | | | |
| Link 1 | 43.2 | 42.8 | 49.4 | 49.0 | 0.253 | 0.135 |
| Link 2 | 32.5 | 32.7 | 35.9 | 33.3 | 0.144 | 0.127 |
| Measurement variation c | | | | | | |
| Link 1 | 20.9 | 12.4 | 27.0 | 22.1 | 0.261 | 0.369 |
| Link 2 | 20.7 | 23.5 | 27.3 | 21.0 | 3.456 | 0.566 |
| Link 3 | 23.9 | 23.9 | 26.8 | 23.5 | 0.259 | 0.501 |

Table 5.4: Throughput results for a different number of AVLNs.

### 5.2.5 Measurement series 5

To investigate the effect of higher channel attenuation on the throughput, three different channels were used in the fifth setup. While variation a in Table 5.5 is a reference measurement where both modems are in the same multiplug, one modem in variation b is connected through an additional $\approx 50m$ extension lead. In variation c, the two modems are connected to different fuses in the building, which results in further attenuation. The lower the SNR due to higher attenuation, the lower modulation formats can be used, which results in lower throughput values.

| | TCP | TCP | UDP | UDP | Jitter | Jitter |
|---|---|---|---|---|---|---|
| | | prioritized | | prioritized | | prioritized |
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 82.6 | 79.4 | 94.3 | 94.1 | 0.123 | 0.113 |
| Measurement variation b | | | | | | |
| Link 1 | 57.5 | 56.3 | 70.0 | 63.4 | 3.299 | 0.118 |
| Measurement variation c | | | | | | |
| Link 1 | 31.1 | 29.0 | 35.3 | 32.4 | 0.455 | 0.534 |

Table 5.5: Throughput results for different attenuation heights.

### 5.2.6 Measurement series 6

The results in Table 5.6 reflect the impact of notches on transmissions. Variation a is a reference measurement again. For variation b, an additional channel tap was created by plugging an open-ended second multiway connector of length 1.6$m$ into the multiplug the modems are connected to. In variation c, two taps were created with two multiway connectors of lengths 1.6$m$ and 3$m$. As the bandwidths are altered only by ≈ 3% for both taps, the effect is rather negligible.

| | TCP | TCP prioritized | UDP | UDP prioritized | Jitter | Jitter prioritized |
|---|---|---|---|---|---|---|
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 67.3 | 65.6 | 83.8 | 80.7 | 0.158 | 0.104 |
| Measurement variation b | | | | | | |
| Link 1 | 65.1 | 64.5 | 80.7 | 77.9 | 4.949 | 1.026 |
| Measurement variation c | | | | | | |
| Link 1 | 65.0 | 61.6 | 80.5 | 78.4 | 0.149 | 4.573 |

Table 5.6: Throughput results for varied channels.

### 5.2.7 Measurement series 7

In the last measurement series presented in Table 5.7, user defined tone masks were used with the StreamPlug modems to switch off parts of the transmission spectrum. Variation a uses the lower $\frac{2}{3}$ of all available carriers and variation b the upper $\frac{2}{3}$. It can be seen that the higher attenuation in the upper frequency region leads to a small drop in network throughput. The reason for the high jitter value in variation b was probably caused by a bug in the modem's firmware, or burstly appearing noise on the power line. It would be desirable to use half of the spectrum to set up two parallel FDMA separated networks, but the current firmware of the StreamPlug modems was not capable to maintain stable connections with half of the spectrum.

| | TCP | TCP<br>prioritized | UDP | UDP<br>prioritized | Jitter | Jitter<br>prioritized |
|---|---|---|---|---|---|---|
| | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[Mbit/s]$ | $[ms]$ | $[ms]$ |
| Measurement variation a | | | | | | |
| Link 1 | 24.5 | 32.0 | 41.0 | 39.7 | 0.383 | 0.327 |
| Measurement variation b | | | | | | |
| Link 1 | 23.0 | 30.7 | 35.5 | 36.7 | 14.869 | 0.287 |

Table 5.7: Throughput results for reduced transmission spectra.

# 6 Conclusion

Although PLC technologies are widely employed for a long time now, they are still under development. First simple systems were introduced nearly 100 years ago, whereas current PLC research topics include MIMO concepts and transmissions with higher frequency bandwidths to achieve transmission rates of nearly $1Gbit/s$. A multitude of different PLC systems is available and intended for different scenarios like long-distance telemetering, in-home networks, Smart Grid applications et cetera. Each system is optimized to work in its application domain with its own constraints for used frequency ranges, achieved data rates and maximal link lengths. The HomePlug AV standard is the most widespread technology for local high speed PLC networks. It is based on an OFDM PHY layer with adaptive bit loading in the frequency range between $2MHz$ and $28MHz$, as well as Turbo convolutional FEC. The HomePlug AV MAC layer utilizes CSMA for sharing the common power line grid with all active STAs, performs regular channel estimations and manages cryptographically isolated logical networks (AVLNs).

When designing a PLC system, it is important to consider the properties of the power line channel. As its original purpose was to solely distribute electrical energy with low frequencies ($50Hz$ or $60Hz$), the power line grid is an improper communication network. Unshielded wires give rise to interference from alien RF transmissions and radiate the power of transmitted signals partly to the environment, leading to additional attenuation besides the usual path loss due to the skin effect. Reflections at channel taps on the path between transmitter and receiver introduce signal echoes which cause notches in the channel TF's magnitude. Measurements of different channels were presented in Chapter 4, as well as corresponding simulations based on the work of Zimmermann and Dostert in [ZD02] and an evolutionary algorithm.

Finally, PLC performance measurements were presented in Chapter 5, investigating the effects of different changes of the transmission setup on the network throughput and delay jitter. If more than one data stream is transmitted (either in one common or separate AVLNs), the available bandwidth is fairly shared between all transmitters and the channel contention leads to slightly reduced total data rates. If prioritized traffic is present in the network, devices with normal priority are nearly entirely deferred from transmitting. StreamPlug based modems are inferior to Atheros based ones in terms of bandwidth, processing delay and jitter values, but might be improved with future firmware releases, as their MAC layer is built in software. While attenuation due to path loss decreases the throughput with increasing link lengths, additional short channel taps have no significant effect on the transmission. Furthermore, if the transmission spectrum is reduced to $\frac{2}{3}$ of the available bandwidth, utilizing the lower $\frac{2}{3}$ leads to higher data rates than using the upper $\frac{2}{3}$.

Regarding the bad performance measurement results of the StreamPlug based modems, future tests will be needed as soon as an announced next firmware version is released. Moreover, although operating HomePlug AV networks with StreamPlug modems which only use half of the transmission spectrum works sporadically, the current StreamPlug firmware is not capable to maintain reliable connections. Further tests with the new release will have to be carried out to explore the operation of two FDMA separated networks.

As a continuation of the research work on broadband PLC, there are planned activities on the design and implementation of an FPGA based PLC transmission system. The aim is to develop it as configurable as possible in order to fit its primary field of application: enhancing industrial plants by extending them with customizable PLC enabled components.

# Acronyms and Abbreviations

**AC** Alternating Current

**AES** Advanced Encryption Standard

**AFE** Analog Front End

**AGC** Automatic Gain Control

**AMI** Advanced Metering Infrastructure

**AMR** Automated Meter Reading

**API** Application Programming Interface

**ARB** ARBitrary waveform generator

**ARIB** Association of Radio Industries and Businesses

**ARQ** Automatic Repeat reQuest

**AVLN** HomePlug AV in-home Logical Network

**AWGN** Additive White Gaussian Noise

**BPL** Broadband over Power Lines

**BPSK** Binary Phase Shift Keying

**CCo** Central Coordinator

**CENELEC** Comité Européen de Normalisation ÉLECtrotechnique

**CRC** Cyclic Redundancy Check

**CSMA** Carrier Sense Multiple Access

**CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance

**DC** Direct Current

**DCSK** Differential Code Shift Keying

**DSL** Digital Subscriber Line

**DSM** Demand Side Management

**EVSE** Electric Vehicle Supply Equipment

**FC** Frame Control

**FCC** Federal Communications Commission

**FDMA** Frequency Division Multiple Access

**FEC** Forward Error Correction

**FFT** Fast Fourier Transform

**FPGA** Field-Programmable Gate Array

**FSK** Frequency Shift Keying

**HD** High Definition

**HD-PLC** High Definition Power Line Communication

**HF** High Frequency

**HLE** Higher Layer Entity

**HS-ROBO** High Speed ROBO

**HV** High Voltage

**ICMP** Internet Control Message Protocol

**IDFT** Inverse Discrete Fourier Transform

**IEEE** Institute of Electrical and Electronics Engineers

**IP** Internet Protocol

**IR** Impulse Response

**ISI** Inter Symbol Interference

**ISP** Inter-System Protocol

**ITU** International Telecommunication Union

**ITU-T** ITU Telecommunication Standardization Sector

**LAN** Local Area Network

**LV** Low Voltage

**MAC** Media Access Control (OSI layer)

**MIMO** Multiple Input Multiple Output

**MINI-ROBO** MINI ROBO

**MPDU** MAC Protocol Data Unit

**MV** Medium Voltage

**NEK** Network Encryption Key

**NID** Network ID

**NMK** Network Membership Key

**NPW** Network Password

**OFDM** Orthogonal Frequency Division Multiplexing

**OSI** Open Systems Interconnection model

**PAPR** Peak to Average Power Ratio

**PB** PHY Block

**PBKDF1** Password-Based Key Derivation Function (version 1)

**PCP** Priority Code Point

**PEV** Plug-in Electric Vehicle

**PHY** Physical (OSI layer)

**PL** PayLoad

**PLC** Power Line Communication

**PoE** Power over Ethernet

**PPDU** PHY Protocol Data Unit

**PRIME** PoweRline Intelligent Metering Evolution

**PRS** Priority Resolution Symbol

**QAM** Quadrature Amplitude Modulation

**QoS** Quality of Service

**QPSK** Quadrature Phase Shift Keying

**RCS** Ripple Carrier Signaling

**RF** Radio Frequency

**ROBO** Robust OFDM

**RSC** Recursive Systematic Convolutional

**SACK** Selective Acknowledgment

**SAP** Service Access Point

**SHA** Secure HAsh

**SISO** Single Input Single Output

**SL** Security Level

**SNR** Signal to Noise Ratio

**SoC** System on Chip

**STA** STAtion (a HomePlug device)

**STD-ROBO** STanDard ROBO

**TCP** Transmission Control Protocol

**TDMA** Time Division Multiple Access

**TF** Transfer Function

**TWACS** Two Way Automatic Communications System

**UDP** User Datagram Protocol

**VLAN** Virtual Local Area Network

**VM** Virtual Machine

**WLAN** Wireless Local Area Network

# Nomenclature

| Symbol | Meaning |
|---:|---|
| $a$ | Scalar |
| $\boldsymbol{a}$ | Vector |
| $\underline{\bullet}$ | Complex value |
| $\underline{\bullet}^*$ | Complex conjugation |
| $\mathcal{R}e\{\underline{\bullet}\}$ | Real part |
| $\mathcal{I}m\{\underline{\bullet}\}$ | Imaginary part |
| $\lvert\bullet\rvert$ | Absolute value |
| $\lvert\underline{\bullet}\rvert$ | Magnitude |
| $\angle\underline{\bullet}$ | Phase |
| $\log_b(\bullet)$ | Logarithm to the base b |
| $\sqrt{-1} = j$ | Imaginary unit $j$ |
| U | Voltage |
| I | Current |
| C | Capacitance |
| L | Inductance |
| $Z = R + jX$ | Impedance Z, Resistance R and Reactance X |
| $Y = \frac{1}{Z} = G + jB$ | Admittance Y, Conductance G and Susceptance B |

# List of Figures

# List of Tables

# Bibliography

[And14] D. Anderson, “Powerline Broadband Internet In the United States at a Glance,” Feb. 2014. [Online]. Available: http://broadbandnow.com/Powerline [Accessed: 2014-08-31]

[BCC03] R. Benato, R. Caldon, and F. Cesena, “Application of Distribution Line Carrier-based protection to prevent DG islanding: an investigating procedure,” in *Power Tech Conference Proceedings, 2003 IEEE Bologna*, vol. 3. IEEE, 2003, pp. 7–pp.

[Bel27] T. A. E. Belt, “Coupling capacitors for carrier current applications,” *AIEE, Journal of the*, vol. 46, no. 10, pp. 1051–1056, 1927.

[BHC04] M. Biggs, A. Henley, and T. Clarkson, “Occupancy analysis of the 2.4 GHz ISM band,” *IEE Proceedings - Communications*, vol. 151, no. 5, p. 481, 2004.

[BLH10] G. Bumiller, L. Lampe, and H. Hrasnica, “Power line communication networks for large-scale control and automation systems,” *Communications Magazine, IEEE*, vol. 48, no. 4, pp. 106–113, 2010.

[Bro99] P. A. Brown, “Power line communications-past, present, and future,” in *Proceedings of International Symposium on Power-line Communications and its Applications*, 1999, pp. 1–8.

[BSEG13] L. T. Berger, A. Schwager, and J. J. Escudero-Garzás, “Power Line Communications for Smart Grid Applications,” *Journal of Electrical and Computer Engineering*, vol. 2013, pp. 1–16, 2013.

[BSPS14] L. T. Berger, A. Schwager, P. Pagani, and D. Schneider, *MIMO Power Line Communications: Narrow and Broadband Standards, EMC, and Advanced Processing*. CRC Press, Feb. 2014.

[CAdRM06] F. Corripio, J. Arrabal, L. del Rio, and J. Munoz, “Analysis of the cyclic short-term variation of indoor power line channels,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 7, pp. 1327–1338, Jul. 2006.

[Can11] F. J. Canete, “Working group on PLC. Communications Engineering Departament,” 2011. [Online]. Available: http://www.plc.uma.es/channels.htm [Accessed: 2014-07-18]

[CCDE11] F. J. Canete, J. A. Cortés, L. Diez, and J. T. Entrambasaguas, “A channel model proposal for indoor power line communications,” *Communications Magazine, IEEE*, vol. 49, no. 12, pp. 166–174, 2011.

[CDCE02] F. J. Canete, L. Diez, J. A. Cortes, and J. T. Entrambasaguas, “Broadband modelling of indoor power-line channels,” *Consumer Electronics, IEEE Transactions on*, vol. 48, no. 1, pp. 175–183, 2002.

[CDCSM10] J. A. Cortes, L. Diez, F. J. Canete, and J. J. Sanchez-Martinez, “Analysis of the Indoor Broadband Power-Line Noise Scenario,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 52, no. 4, pp. 849–858, Nov. 2010.

[Coh85] D. J. Cohen, “Necessary Bandwidth and Spectral Properties of Digital Modulation,” U.S. Department of Commerce, Tech. Rep. 84-168, Feb. 1985.

[Dos97] K. Dostert, “Telecommunications over the Power Distribution Grid–Possibilities and Limitations,” *IIR-Powerline*, vol. 6, p. 9, 1997.

[ESB$^+$96] O. Edfors, M. Sandell, J.-J. v. d. Beek, D. Landström, and F. Sjöberg, “Introduction to Orthogonal Frequency Division Multiplexing,” Sep. 1996.

[FLNS11] H. C. Ferreira, L. Lampe, J. Newbury, and T. G. Swart, “Industrial and International Standards on PLC-Based Networking Technologies,” in *Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines.* John Wiley & Sons, Jul. 2011.

[Foc03] K. Fockens, “HF radio reception compatibility test of an in-house PLC system using two brands of modems,” Oct. 2003.

[Fre06] R. L. Freeman, *Radio System Design for Telecommunication.* John Wiley & Sons, Nov. 2006.

[GC02] Y. Guo and J. R. Cavallaro, “Reducing peak-to-average power ratio in OFDM systems by adaptive dynamic range companding,” in *World Wireless Congress*, 2002.

[GKLK14] T. Gehrsitz, H. Kellermann, H.-T. Lim, and W. Kellerer, “Analysis of Medium Access Protocols for Power Line Communication realizing In-Car Networks,” 2014.

[GL08] S. Galli and O. Logvinov, “Recent developments in the standardization of power line communications within the IEEE,” *Communications Magazine, IEEE*, vol. 46, no. 7, pp. 64–71, 2008.

[GMB+14] A. Gogic, A. Mahmutbegovic, D. Borovina, I. H. Cavdar, and N. Suljanovic, “Simulation of the narrow-band PLC system implementing PRIME standard,” in *Energy Conference (ENERGYCON), 2014 IEEE International*. IEEE, 2014, pp. 1520–1525.

[Gol05] A. Goldsmith, *Wireless Communications*. Cambridge University Press, Aug. 2005.

[GSW11] S. Galli, A. Scaglione, and Z. Wang, “For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid,” *Proceedings of the IEEE*, vol. 99, no. 6, pp. 998–1027, Jun. 2011.

[GTF+11] M. Gates, A. Tirumala, J. Ferguson, J. Dugan, F. Qin, K. Gibbs, and J. Estabrook, “Iperf - The TCP/UDP Bandwidth Measurement Tool,” 2011. [Online]. Available: https://iperf.fr/ [Accessed: 2014-11-05]

[Har02] E. Hare, “Calculated Impact of PLC on Stations Operating in the Amateur Radio Service,” in *C63 Commitee meeting Rockville, MD*, Nov. 2002.

[HD-12] HD-PLC Alliance, “HD-PLC IEEE 1901 technical over view,” 2012.

[Hen14] M. Hengemühle, “Anti Powerline Communication Initiative,” 2014. [Online]. Available: http://www.qsl.net/dl5qe/plc.htm [Accessed: 2014-08-29]

[Hoc11] M. Hoch, “Comparison of PLC G3 and PRIME,” *Institute for Information Transmission, Friedrich-Alexander-University, Erlangen, Germany*, 2011.

[Hom05] HomePlug Powerline Alliance, “HomePlug AV White Paper,” 2005.

[Hom08] ——, *HomePlug Command & Control Overview White Paper*. HomePlug Powerline Alliance, Sep. 2008.

[Hom12a] ——, *HomePlug Green PHY 1.1 The Standard for In-Home Smart Grid Powerline Communications: An application and technology overview*. HomePlug Powerline Alliance, Mar. 2012.

[Hom12b] ——, *HomePlug Green PHY Specification*. HomePlug Powerline Alliance, Apr. 2012.

[Hom13] ——, *HomePlug AV2 Technology.* HomePlug Powerline Alliance, 2013.

[IEE09] IEEE Computer Society, "Amendment 3: Data Terminal Equipment (DTE) power via the Media Dependent Interface (MDI) enhancements (IEEE 802.3at)," in *IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer Specifications.* New York: Institute of Electrical and Electronics Engineers, Oct. 2009.

[IEE10] IEEE Communications Society, *IEEE standard for broadband over power line networks medium access control and physical layer specifications (IEEE 1901-2010).* New York: Institute of Electrical and Electronics Engineers, 2010.

[IEE13] ——, *IEEE standard for low-frequency (less than 500 kHz) narrowband power line communications for smart grid applications.* Institute of Electrical and Electronics Engineers, 2013.

[Ins13] Insteon, "Insteon Whitepaper: The Details," 2013.

[ITU11a] ITU, *Unified high-speed wireline-based home networking transceivers – Power spectral density specification (ITU-T Recommendation G.9964).* International Telecommunications Union, Dec. 2011.

[ITU11b] ——, *Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification (ITU-T Recommendation G.9960).* International Telecommunications Union, Dec. 2011.

[ITU12a] ——, *Narrowband orthogonal frequency division multiplexing power line communication transceivers for ITU-T G.hnem networks (ITU-T Recommendation G.9902).* International Telecommunications Union, Oct. 2012.

[ITU12b] ——, *Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks (ITU-T Recommendation G.9904).* International Telecommunications Union, Oct. 2012.

[ITU14a] ——, *Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks (ITU-T Recommendation G.9903).* International Telecommunications Union, Feb. 2014.

[ITU14b] ——, *Narrowband orthogonal frequency division multiplexing power line communication transceivers – Power spectral density specification (ITU-T Recommendation G.9901).* International Telecommunications Union, Apr. 2014.

[JA09] K. Jones and C. Aslanidis, "DCSK Technology va. OFDM Concepts for PLC Smart Metering," Mar. 2009.

[KNX14] KNX Association, "KNX-Basics," 2014.

[LCDD08] M. Lienard, M. Carrion, V. Degardin, and P. Degauque, "Modeling and Analysis of In-Vehicle Power Line Communication Channels," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 2, pp. 670–679, Mar. 2008.

[LSG$^+$00] C. K. Lim, P. L. So, E. Gunawan, S. Chen, T. T. Lie, and Y. L. Guan, "Development of a test bed for high-speed power line communications," in *Power System Technology, 2000. Proceedings. PowerCon 2000. International Conference on*, vol. 1. IEEE, 2000, pp. 451–456.

[LWR03] W. Liu, H. Widmer, and P. Raffin, "Broadband PLC access systems and field deployment in European power line networks," *Communications Magazine, IEEE*, vol. 41, no. 5, pp. 114–118, 2003.

[McC10] E. McCune, *Practical Digital Wireless Signals.* Cambridge University Press, Feb. 2010.

[MCG$^+$04] H. Meng, S. Chen, Y. L. Guan, C. L. Law, P. L. So, E. Gunawan, and T. T. Lie, "Modeling of transfer characteristics for the broadband power line communication channel," *Power Delivery, IEEE Transactions on*, vol. 19, no. 3, pp. 1057–1064, 2004.

[MM84] S. T. Mak and T. G. Moore, "TWACS, A New Viable Two-Way Automatic Communication System for Distribution Networks. Part II: Inbound Communication," *Power Apparatus and Systems, IEEE Transactions on*, no. 8, pp. 2141–2147, 1984.

[MR82] S. T. Mak and D. L. Reed, "TWACS, a new viable two-way automatic communication system for distribution networks. Part I: Outbound communication," *Power Apparatus and Systems, IEEE Transactions on*, no. 8, pp. 2941–2949, 1982.

[MRI03] E. Marthe, F. Rachidi, and M. Ianoz, "Evaluation of indoor PLC radiation resulting from conducted emission limits," in *Electromagnetic Compatibility, 2003. EMC'03. 2003 IEEE International Symposium on*, vol. 1. IEEE, 2003, pp. 162–165.

[Nat01] National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," *Federal Information Processing Standards Publication*, vol. 197, Nov. 2001.

[Nor08] E. D. Nordell, "Communication Systems for Distribution Automation," *Transmission and Distribution Conference and Exposition, Bogota, Colombia*, 2008.

[NYGA07] R. Newman, L. Yonge, S. Gavette, and R. Anderson, "HomePlug AV security mechanisms," in *Power Line Communications and Its Applications, 2007. ISPLC'07. IEEE International Symposium on.* IEEE, 2007, pp. 366–371.

[OG09] V. Oksman and S. Galli, "G. hn: The new ITU-T home networking standard," *Communications Magazine, IEEE*, vol. 47, no. 10, pp. 138–145, 2009.

[OZ11] V. Oksman and J. Zhang, "G. HNEM: the new ITU-T standard on narrowband PLC technology," *Communications Magazine, IEEE*, vol. 49, no. 12, pp. 36–44, 2011.

[Phi99] H. Philipps, "Modelling of powerline communication channels," in *Proc. 3rd Int'l. Symp. Power-Line Commun. and its Applications*, 1999, pp. 14–21.

[Rie12] D. W. Rieken, "Digital Two Way Automatic Communication System (TWACS) Outbound Receiver and Method," United State of America Patent 0 039 400, Feb., 2012.

[RRP08] J.-G. Rhee, E. Rhee, and T.-S. Park, "Electromagnetic interferences caused by power line communications in the HF bands," in *Power Line Communications and Its Applications, 2008. ISPLC 2008. IEEE International Symposium on.* IEEE, 2008, pp. 249–252.

[RSA99] RSA Laboratories, "PKCS #5 v2.0: Password-Based Cryptography Standard," Mar. 1999.

[Sch09] M. Schwartz, “Carrier-wave telephony over power lines: Early history [history of communications],” *Communications Magazine, IEEE*, vol. 47, no. 1, pp. 14–18, 2009.

[SK96] M. H. Shwehdi and A. Z. Khan, “A power line data communication interface using spread spectrum technology in home automation,” *Power Delivery, IEEE Transactions on*, vol. 11, no. 3, pp. 1232–1237, 1996.

[Str25] M. E. Strieby, “Carrier transmission over power circuits,” United State of America Patent 1,547,242, 1925.

[WBD98] T. Waldeck, M. Busser, and K. Dostert, “Telecommunication applications over the low voltage power distribution grid,” in *Spread Spectrum Techniques and Applications, 1998. Proceedings., 1998 IEEE 5th International Symposium on*, vol. 1. IEEE, 1998, pp. 73–77.

[Wes09] K. Wesolowski, *Introduction to Digital Communication Systems.* John Wiley & Sons, Jul. 2009.

[WET14] N. Weling, A. Engelen, and S. Thiel, “Broadband MIMO powerline channel emulator,” in *Power Line Communications and its Applications (ISPLC), 2014 18th IEEE International Symposium on.* IEEE, 2014, pp. 105–110.

[YAA$^+$13] L. Yonge, J. Abad, K. Afkhamie, L. Guerrieri, S. Katar, H. Lioe, P. Pagani, R. Riva, D. M. Schneider, and A. Schwager, “An Overview of the HomePlug AV2 Technology,” *Journal of Electrical and Computer Engineering*, vol. 2013, pp. 1–20, 2013.

[ZD02] M. Zimmermann and K. Dostert, “A multipath model for the powerline channel,” *Communications, IEEE Transactions on*, vol. 50, no. 4, pp. 553–559, 2002.

# Appendix

The following pages show figures with frequency and time domain representations of measured and modeled channels of all setups which were defined and described in Chapter 4.3.1. For the sake of clarity, the time and frequency domain plots of a setup are presented on one page each. The results for setup 4 can be found in Chapter 4.2.

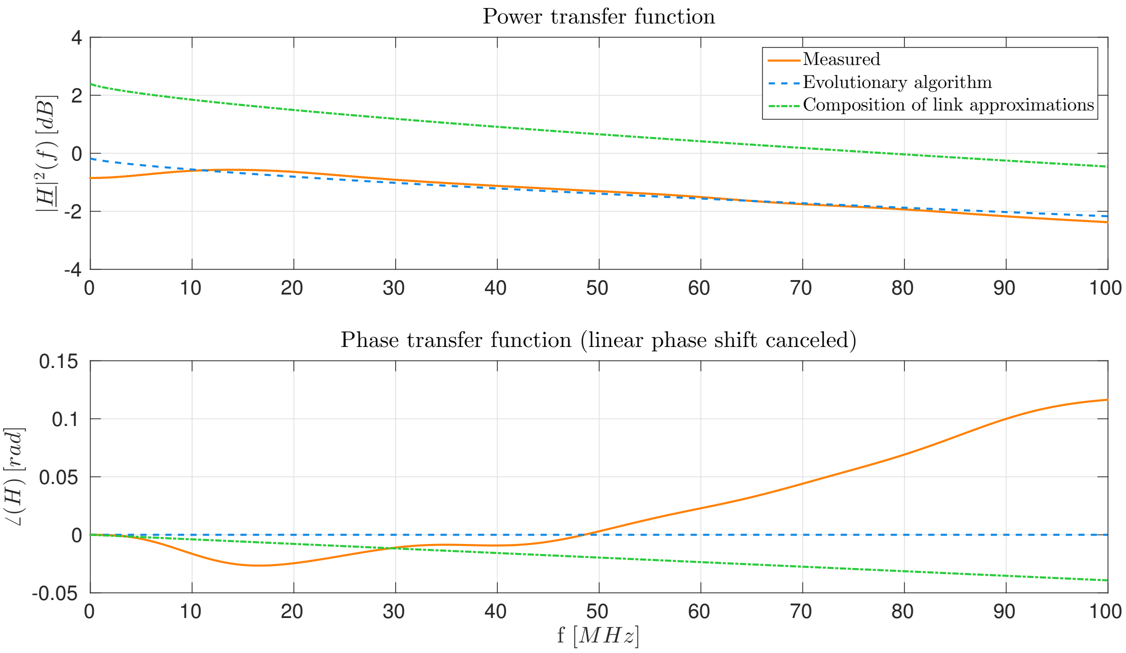


Figure A.1: The channel of setup 1.a in frequency domain.

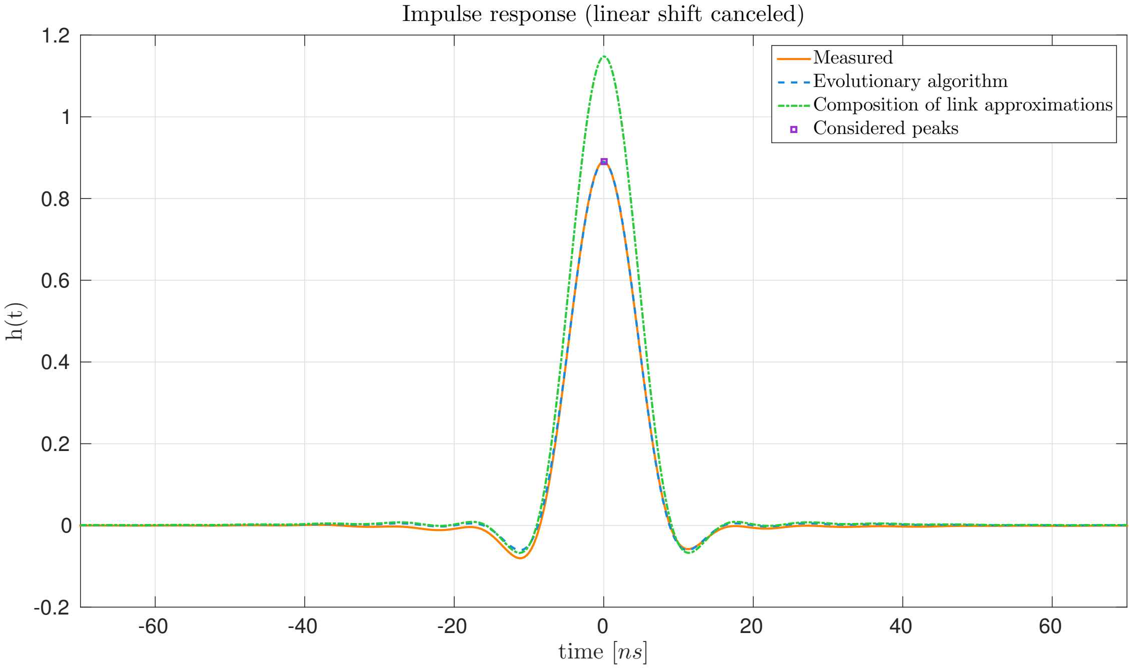


Figure A.2: The channel of setup 1.a in time domain.

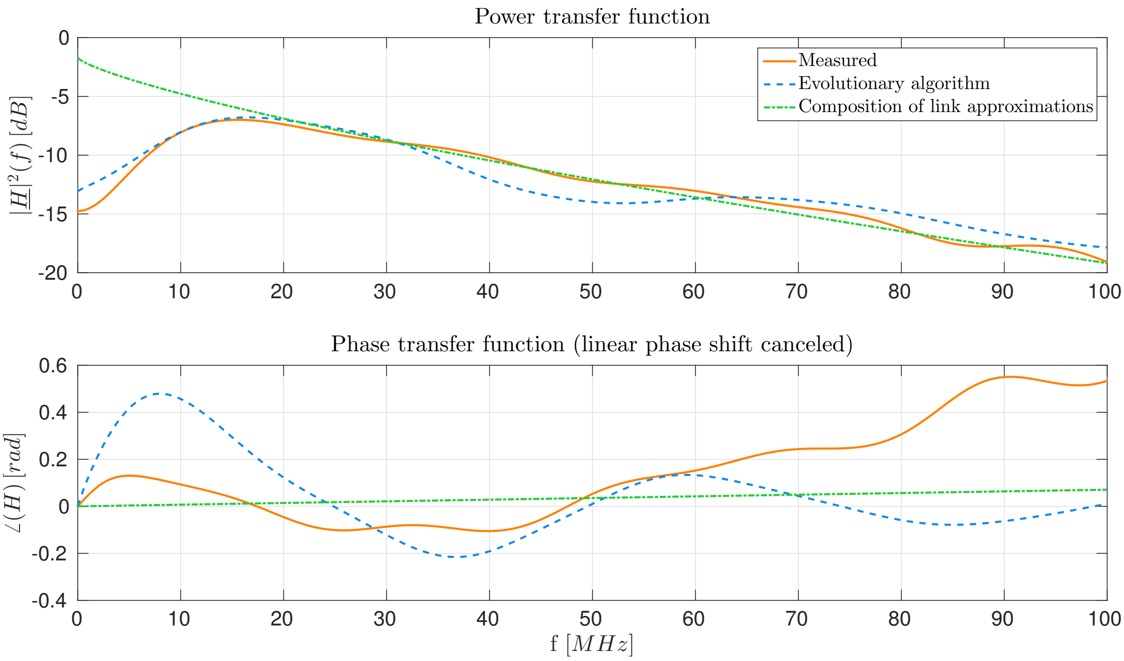


Figure A.3: The channel of setup 1.b in frequency domain.

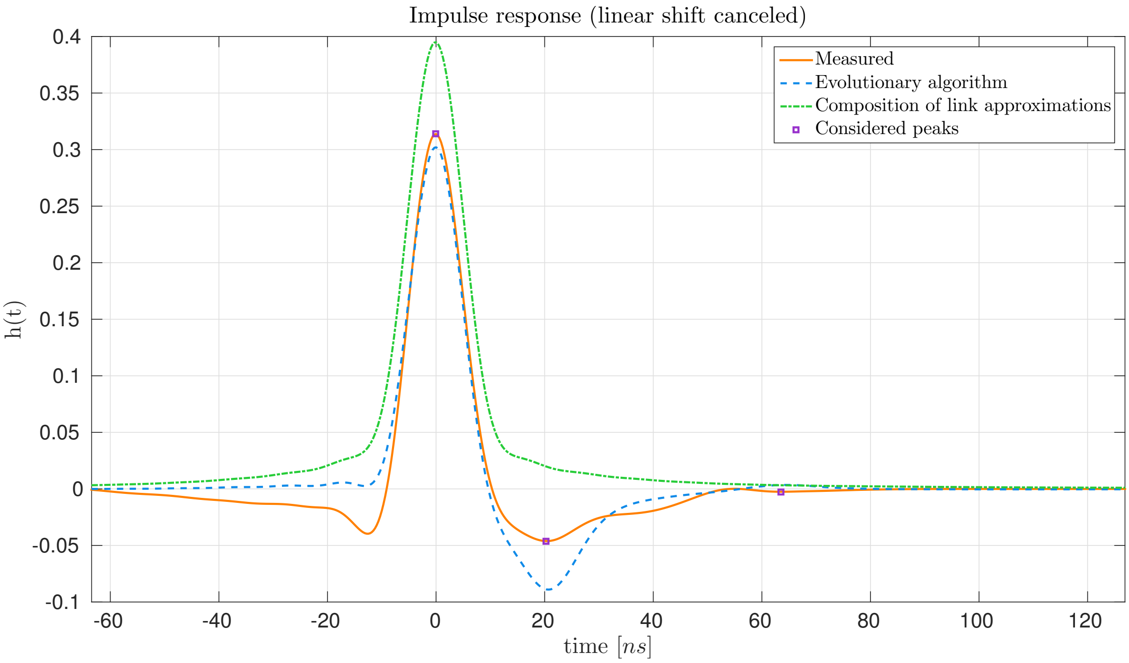


Figure A.4: The channel of setup 1.b in time domain.

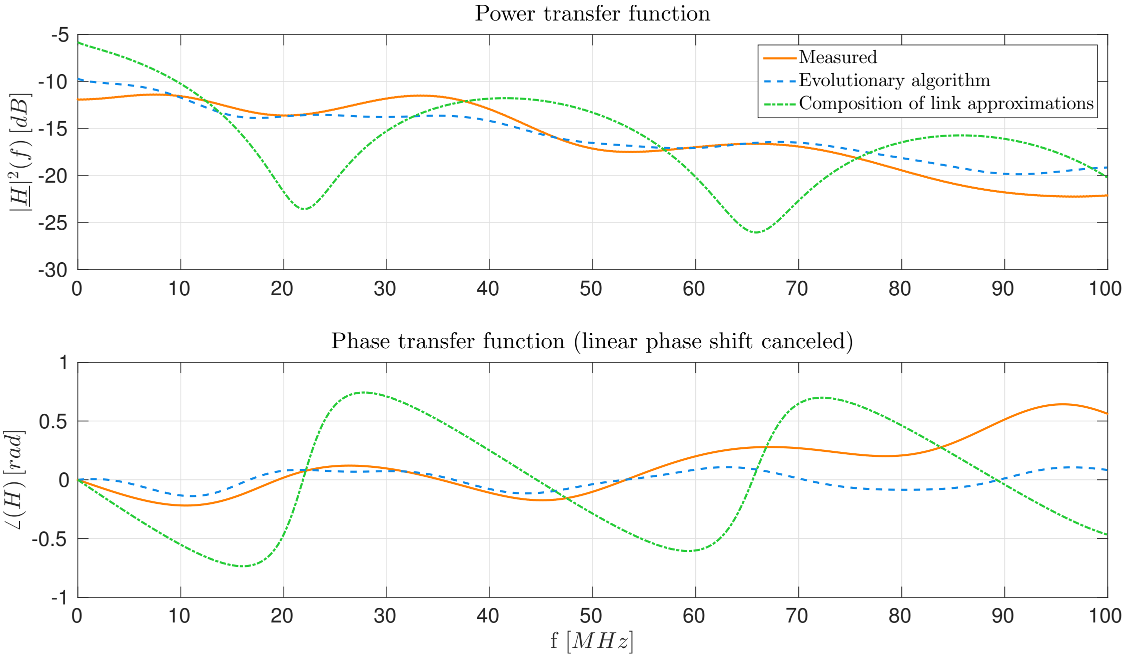


Figure A.5: The channel of setup 2.a in frequency domain.

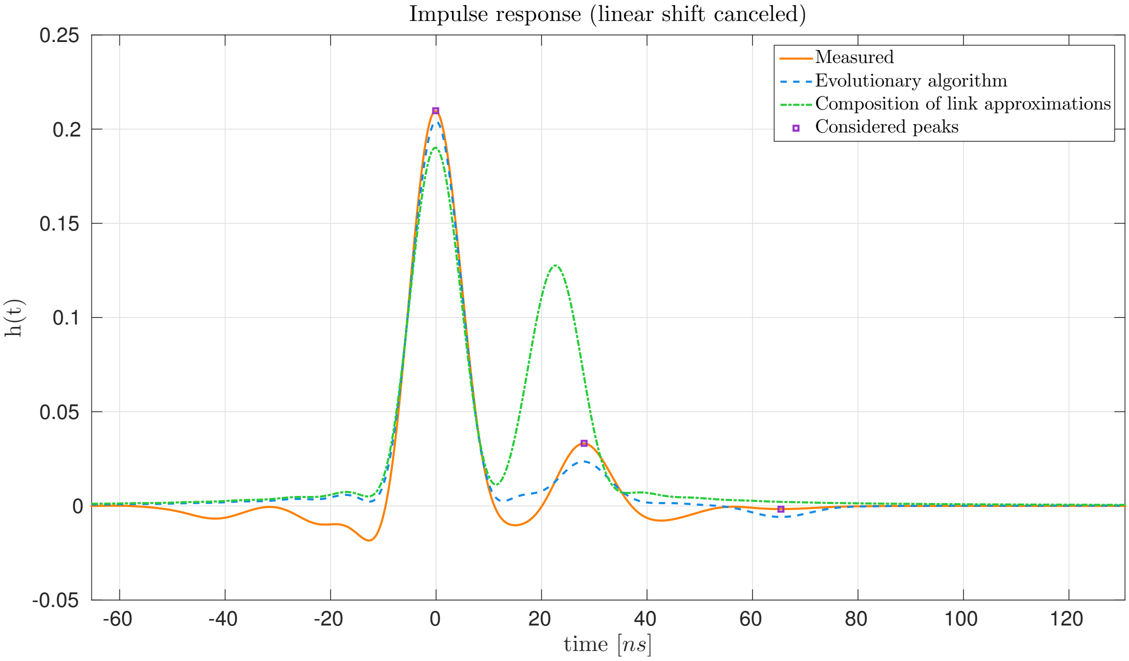


Figure A.6: The channel of setup 2.a in time domain.

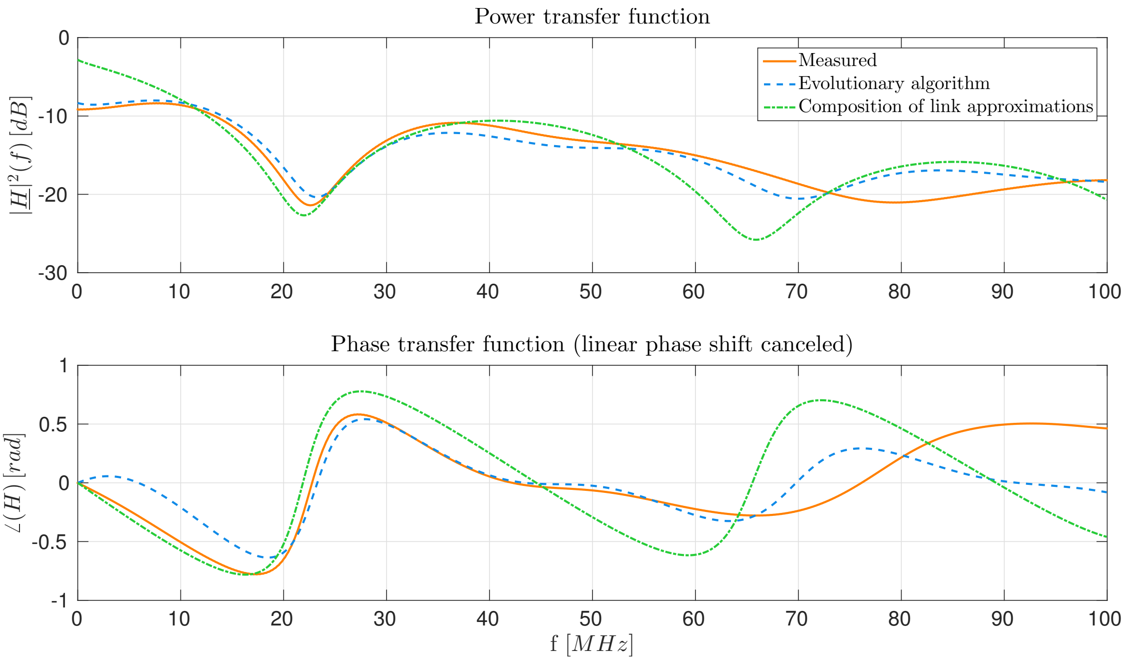


Figure A.7: The channel of setup 2.b in frequency domain.

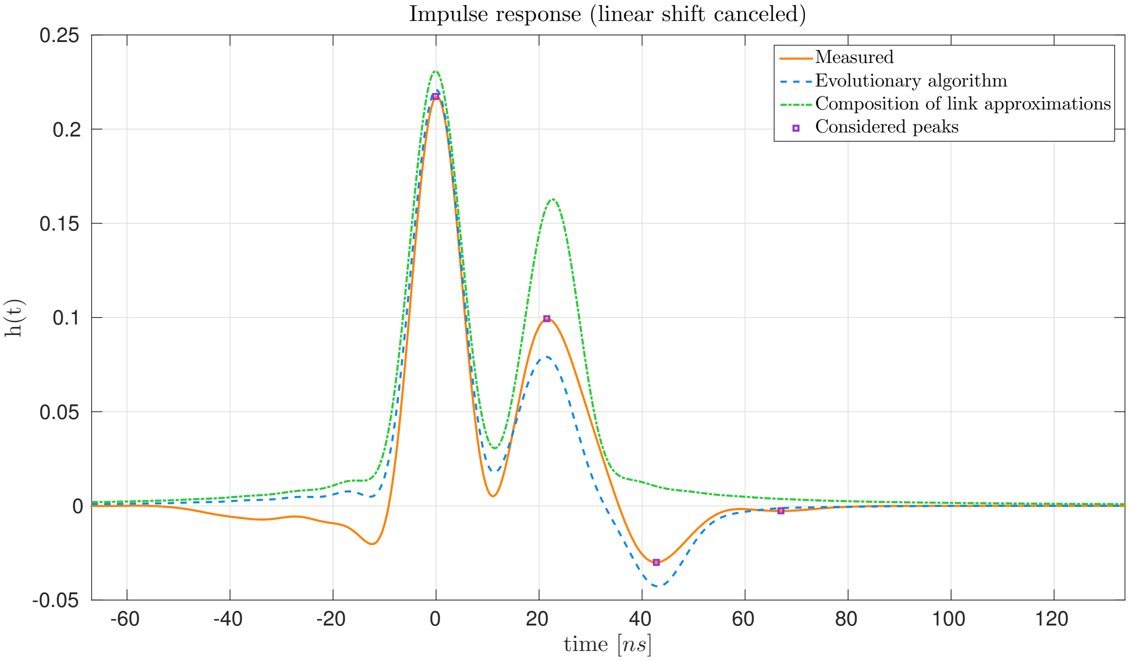


Figure A.8: The channel of setup 2.b in time domain.

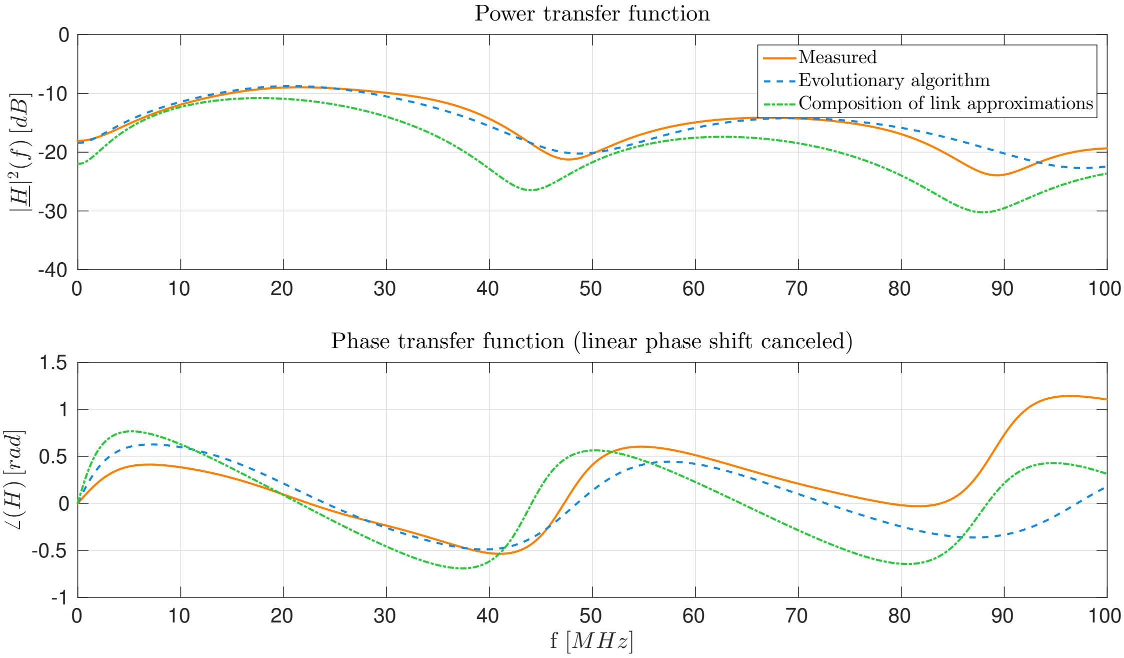


Figure A.9: The channel of setup 2.c in frequency domain.

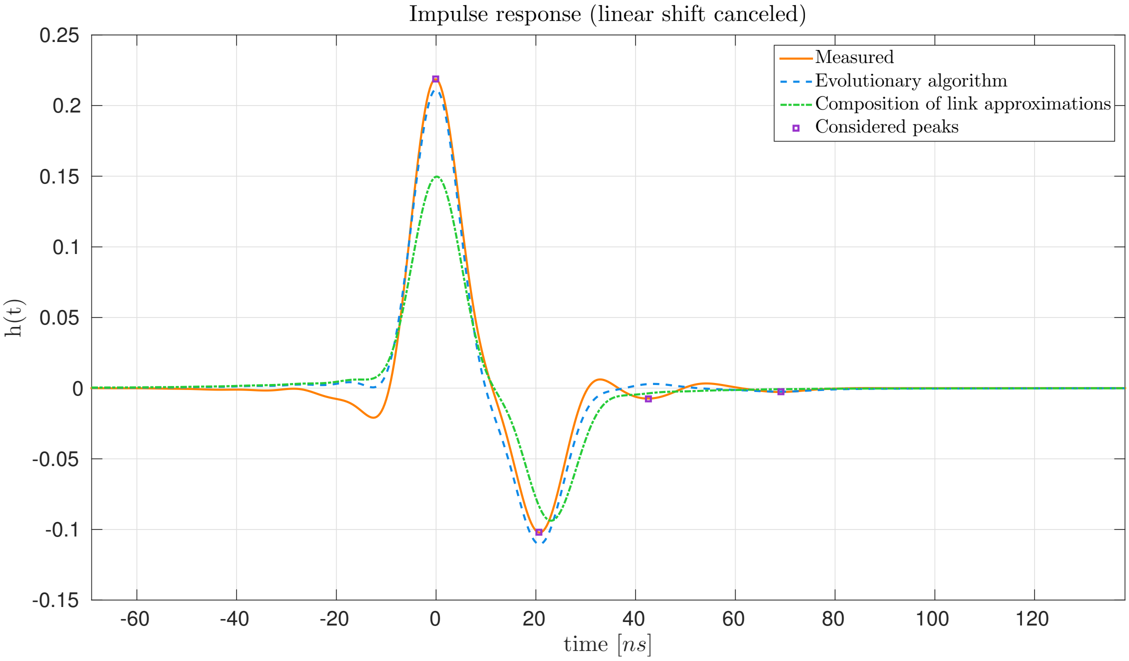


Figure A.10: The channel of setup 2.c in time domain.

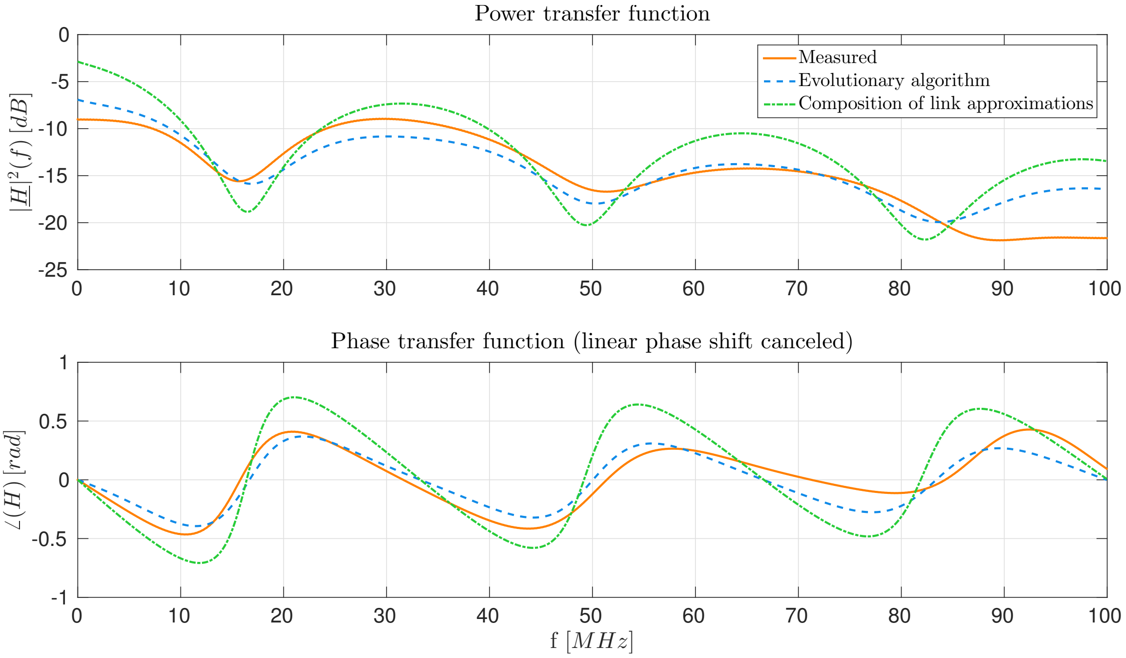


Figure A.11: The channel of setup 3 in frequency domain.

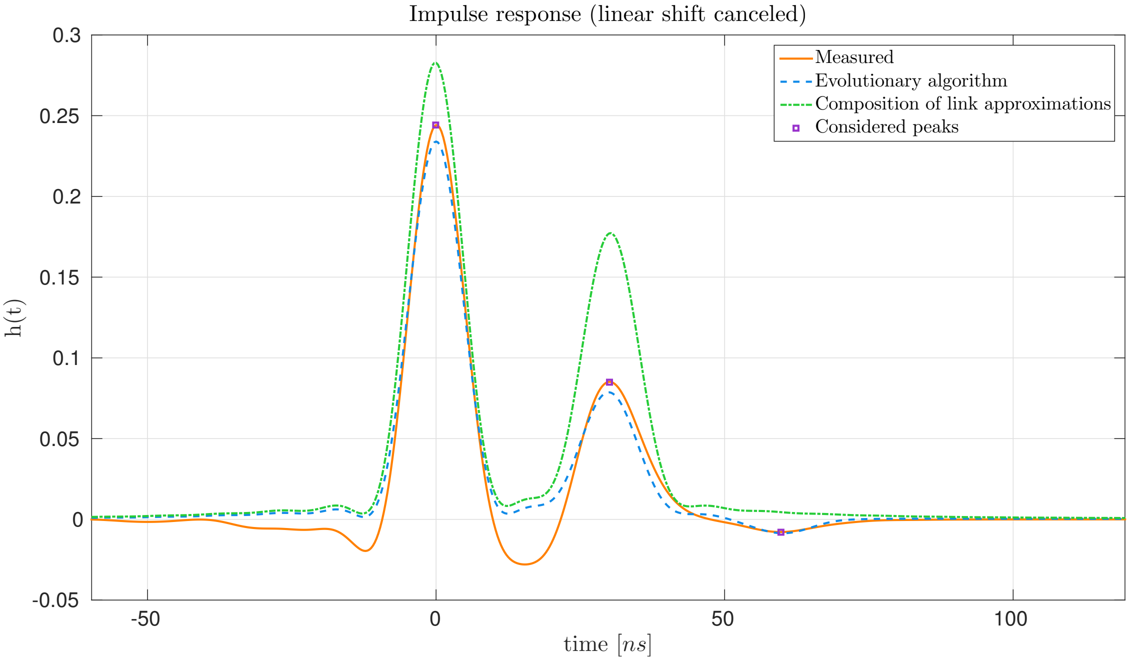


Figure A.12: The channel of setup 3 in time domain.

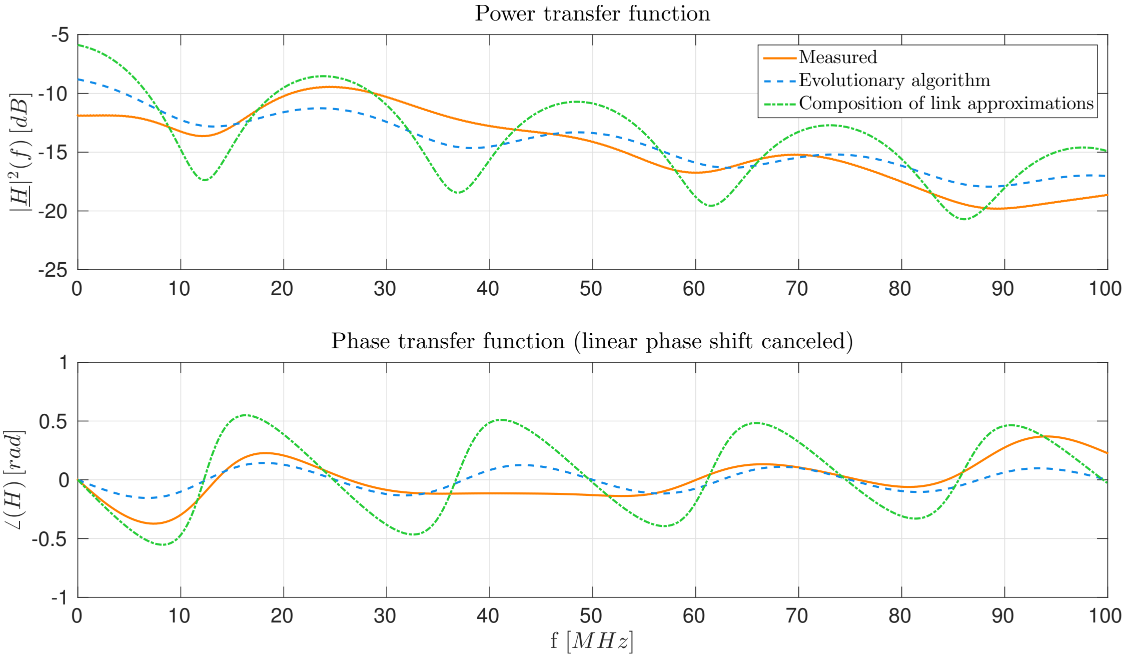


Figure A.13: The channel of setup 5.a in frequency domain.

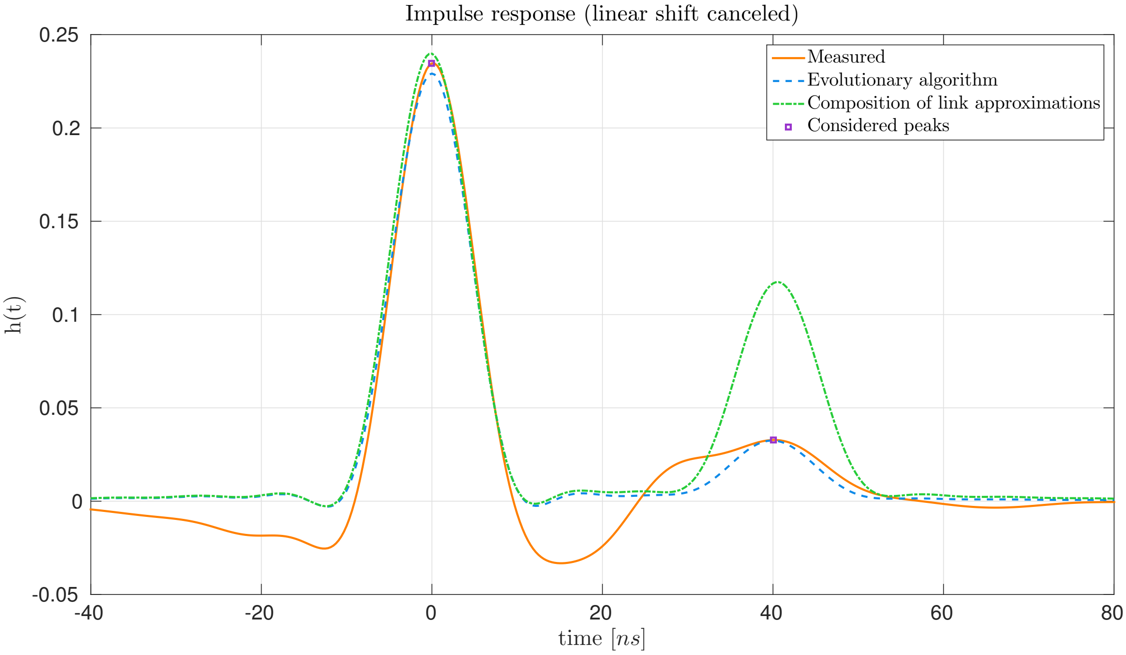


Figure A.14: The channel of setup 5.a in time domain.

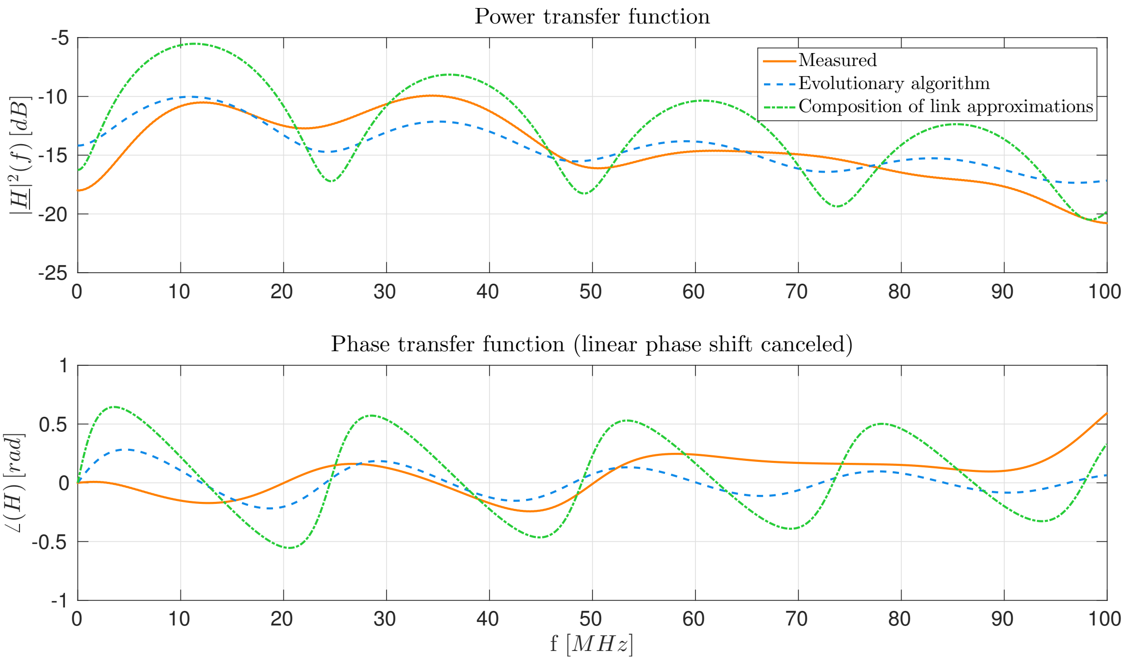


Figure A.15: The channel of setup 5.b in frequency domain.

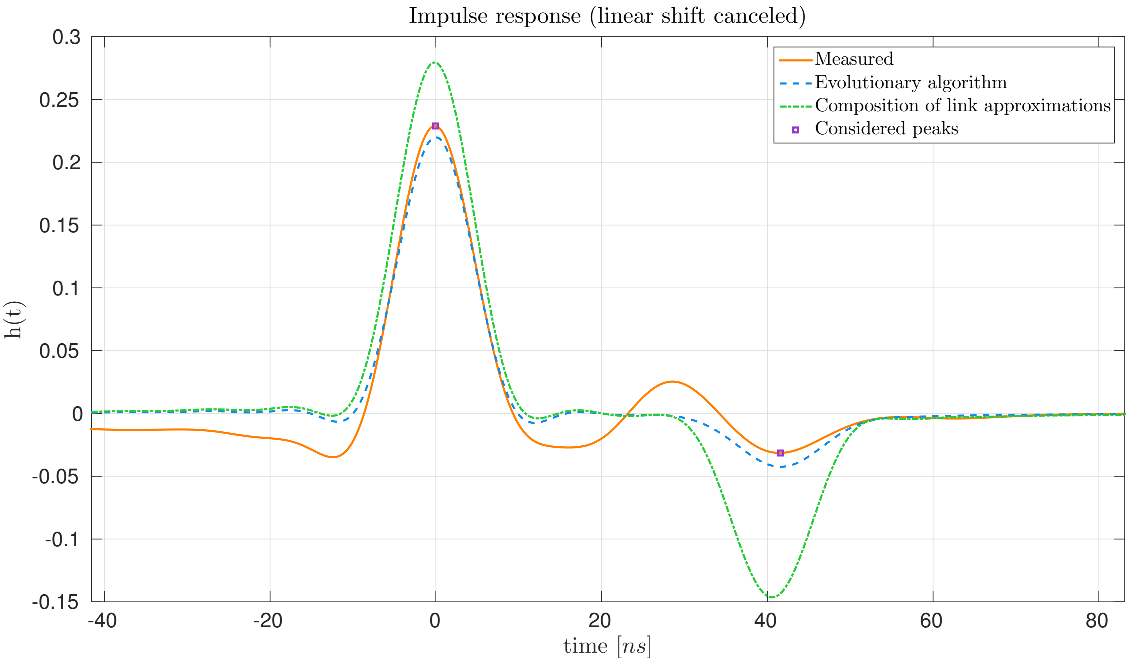


Figure A.16: The channel of setup 5.b in time domain.

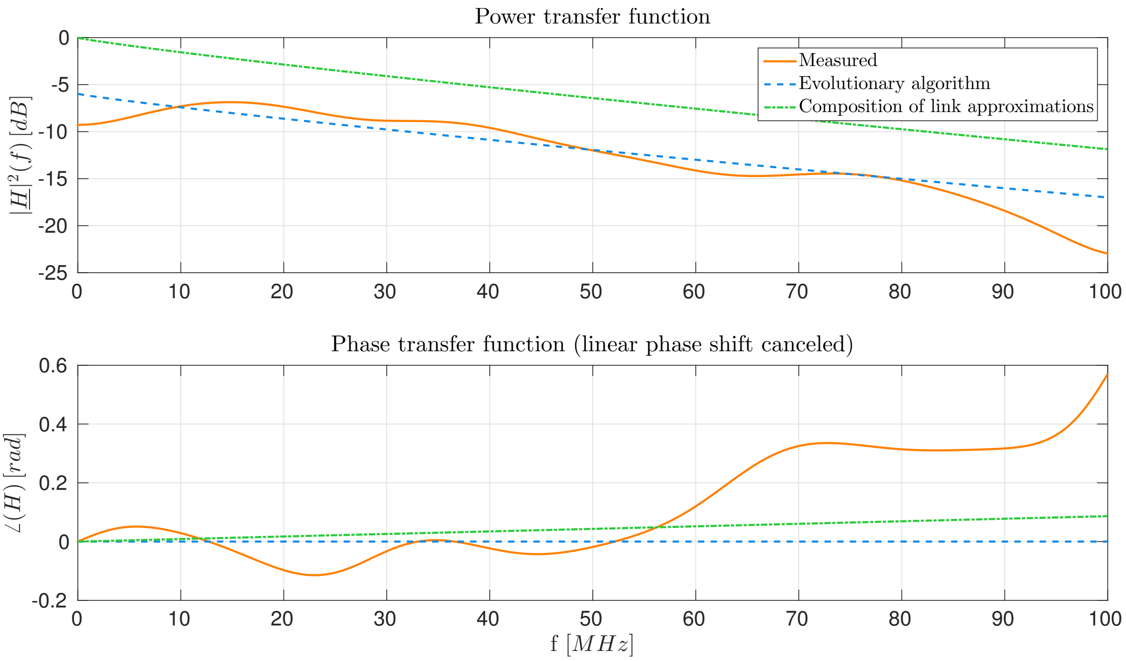


Figure A.17: The channel of setup 5.c in frequency domain.

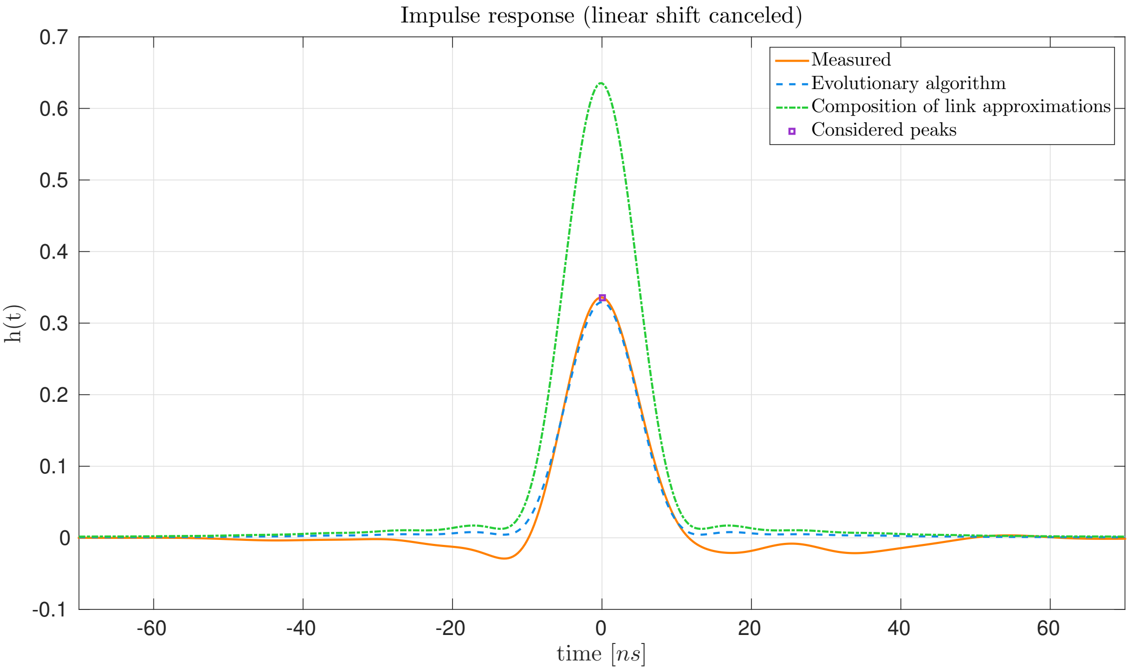


Figure A.18: The channel of setup 5.c in time domain.

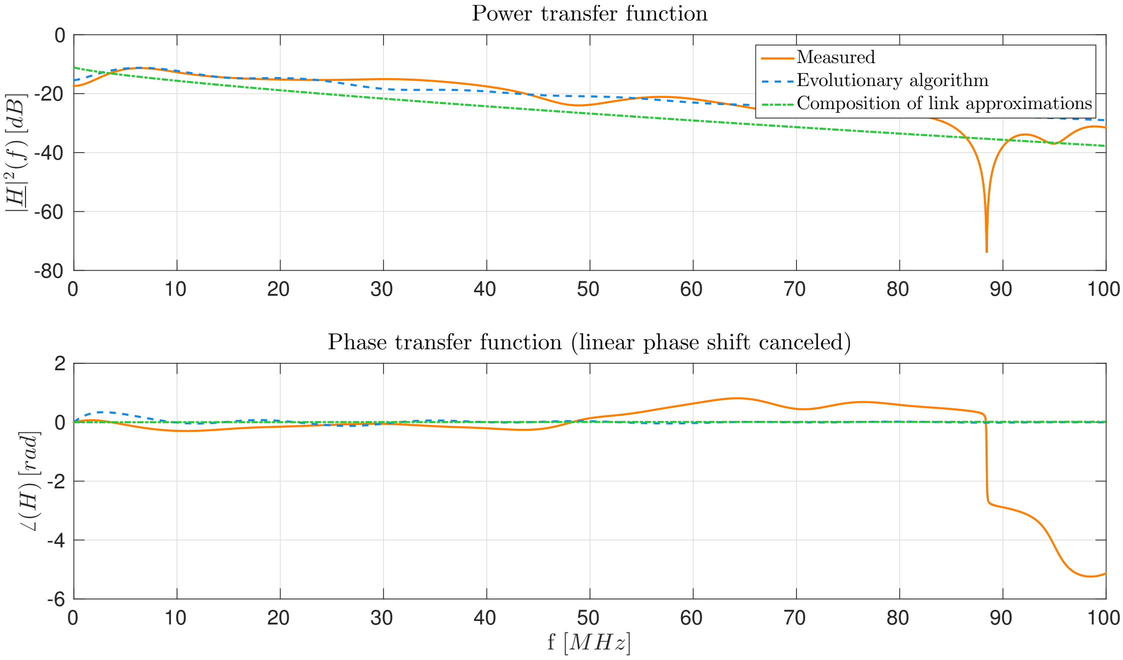


Figure A.19: The channel of setup 6.a in frequency domain.

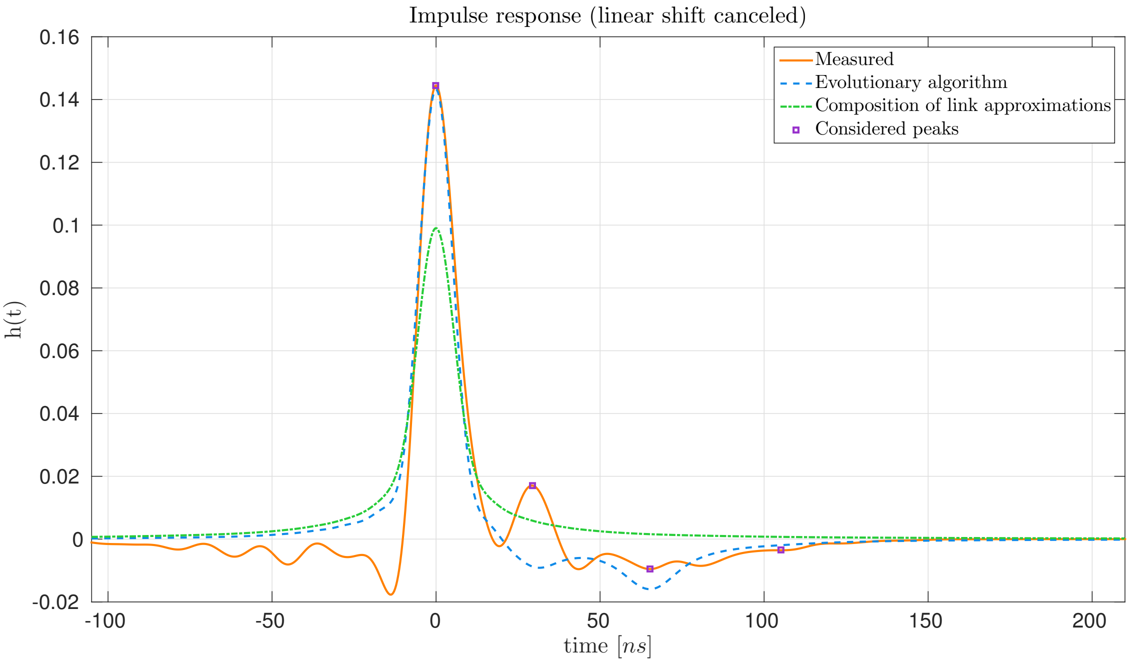


Figure A.20: The channel of setup 6.a in time domain.

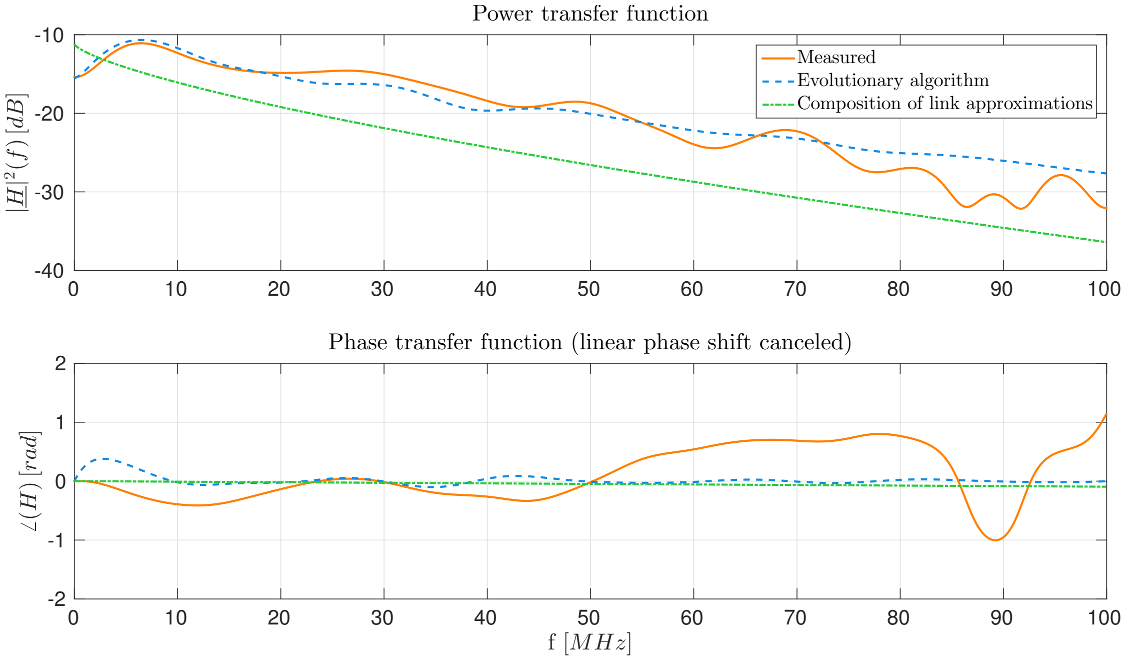


Figure A.21: The channel of setup 6.b in frequency domain.

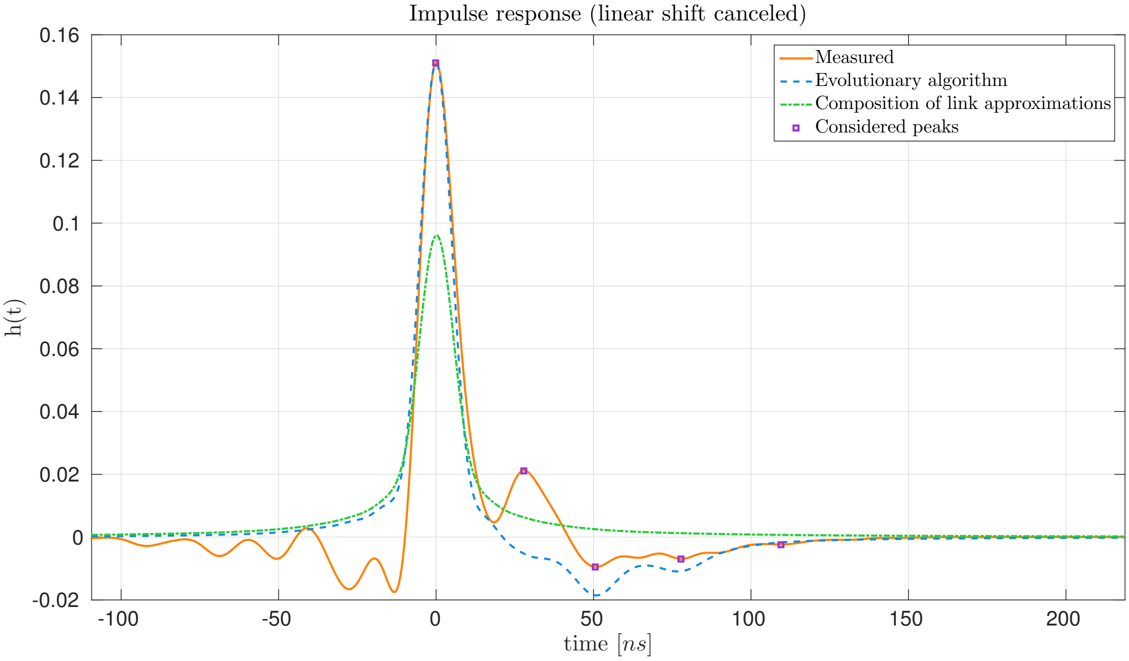


Figure A.22: The channel of setup 6.b in time domain.

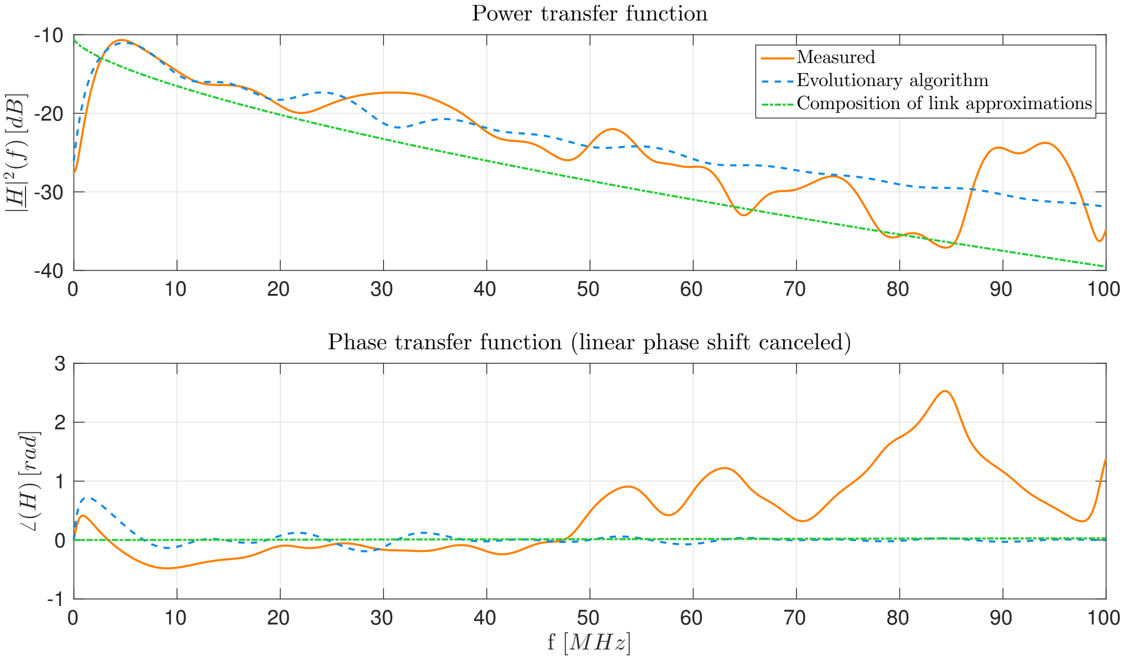


Figure A.23: The channel of setup 6.c in frequency domain.

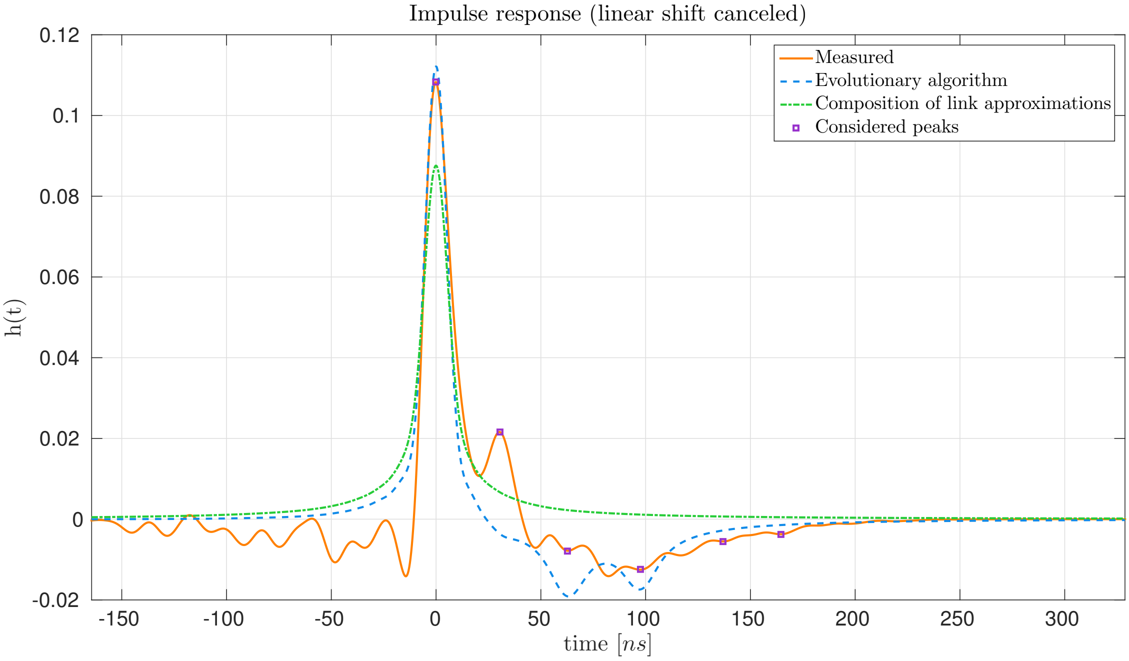


Figure A.24: The channel of setup 6.c in time domain.