ATCZ175 InterOP PROJECT

Working Prinicple of WLAN Systems and Interference Sources

Institute of Electrodynamics, Microwave and Circuit Engineering
Technische Universität Wien

Advisor:
Assoc. Prof. Dipl.-Ing. Dr.techn. Holger Arthaber

by
Proj. Ass. Dipl.-Ing. Christian Spindelberger

October 9, 2019

Contents

Abbreviations

ACK acknowledgment

BLE Bluetooth low energy

BPSK binary phase shift keying

CCA clear channel assessment

CP cyclic prefix

CTS clear to send

DIFS distributed interframe space

DSSS direct spread spectrum sequence

EIRP effective isotropic radiated power

FCS frame check sequence

FEC forward error correction

FFT fast Fourier transform

FH frequency hopping

GFSK Gaussian frequency shift keying

IoT internet of things

IP internet protocol

ISM industrial, scientific, and medical

IFS interframe space

IFFT inverse fast Fourier transform

LAN local area network

LLC logical link control

LTF long training field

MAC medium access control

MTU maximum transmission unit

NAV network allocation vector

OFDM orthogonal frequency division multiplexing

OSI open systems interconnection

PER packet error rate

PHY physical

PLCP physical layer convergence procedure

PMD physical medium dependent

QAM quadratue amplitude modulation

RF radio frequency

RIFS reduced interframe space

RSSI received signal strength indicator

RTS request to send

SIFS short interframe space

SRD short range device

STF short training field

TCP transmission control protocol

UDP user datagram protocol

WLAN wireless local area network

1 Introduction

This document provides a theoretical background of wireless local area network (WLAN) communication systems. The aim is to make the reader familiar with relevant concepts and parameters. It mainly consists of a WLAN related part, discussing important topics such as layer stack up, collision avoidance, and transmission parameters, while common interference sources (Bluetooth low energy (BLE), microwave ovens, SRDs, and radars) affecting WLAN are presented in the second part.

Starting with Section 2, an introduction about the WLAN-related layer stack up and similarities to other transmission standards is given. Proceeding with this topic, the two most important parts concerning this work are discussed. The medium access control (MAC) is described in terms of timing constraints, collision avoidance, and layer interaction. Furthermore, physical (PHY)-layer parameters, such as modulation techniques (OFDM, DSSS) and carrier sensing, are examined. In order to explain these sublayer interactions, practice relevant examples utilizing the user datagram protocol (UDP) and transmission control protocol (TCP) are given. Lastly, basics about potential interference sources will be presented in Section 3. BLE is one of the most serious interferers concerning WLAN. Therefore, details about the PHY layer and channel access schemes are investigated. The final subsections are devoted to further interferers, i.e., microwave ovens, short range devices (SRDs), and radars.

2 IEEE 802.11 Wireless LAN

WLAN is a widely deployed standard for data transmission in the industrial, scientific, and medical (ISM) band. Usually, it is intended to be used as a wireless access point to a network (router). Since the first launch in 1997, the IEEE 802.11 standard has undergone several improvements [1]. Today, different versions are available, such as IEEE 802.11a/b/g/n/ac and many more. In the internet of things (IoT) branch, the state-of-the-art WLAN standard is IEEE 802.11n, implemented with one single antenna. Therefore, the focus will lie on this respective version. The current section about IEEE 802.11 WLAN properties is based on *802.11 Wireless Networks: The Definitive Guide*, written by Matthew Gast [2].

As the layer composition of IEEE 802.11 strongly relates to IEEE 802-based networks, i.e., local area network (LAN), the low level constructs (MAC & PHY) must fit into the required open systems interconnection (OSI) model (Figure 1). The most important parts, considering WLAN, are marked in violet. It is obvious that all IEEE 802 networks have a MAC and a PHY component. The classical data link layer is responsible for an error free

transmission by calculating checksums or making use of channel coding. While the MAC determines specific rules for collision avoidance and how to access the medium, the PHY layer is related to details about data reception and transmission. Thus, WLAN uses the IEEE 802.2 logical link control (LLC) encapsulation, which makes it very powerful because it can utilize higher layer protocols (UDP, TCP). Details about the sublayer realizations will be discussed in the following.

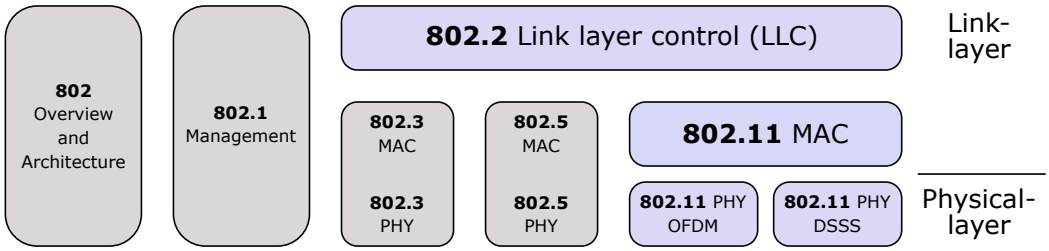

Figure 1: OSI model of IEEE 802.11 embedded in IEEE 802.2 LLC [2]

2.1 Medium Access Control Layer

The access medium of IEEE 802.11 systems is a wireless radio channel and demands specific MAC properties to ensure stable data transmissions. Especially for unlicensed radio channels, e.g., the ISM band, many different interferers such as BLE and microwave ovens occur. Therefore, to check if a transmission was successful, WLAN uses acknowledgment (ACK) frames for confirmation. Figure 2 depicts, how a simple frame transmission between two stations works. Station one (*STA 1*) transmits the desired frame to receiver station two (*STA 2*). If the transmission was successful, *STA 2* replies with an ACK frame. Detecting a damaged packet forces *STA 2* to omit an answer. Depending on the utilized protocol, a retransmission will be sent if the ACK frame was missing.

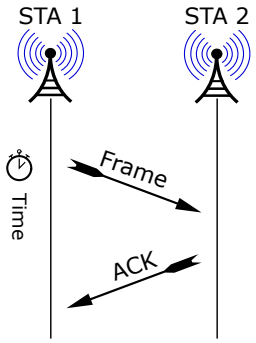

Figure 2: Valid WLAN frame transmission [2]

Hidden Node Problem

A major problem arises concerning multi-user scenarios. Because of limited transmit powers, free space losses, channel variations, and several other effects, the range of a station is limited. This makes it impossible to reach those users that are too far from the station. Assume the following scenario: One access point (server) and two further stations (clients) are present. The first client (*client 1*) wants to start a data exchange with the *server*, but the second client (*client 2*) is too far away to receive any message from *client 1*. What now happens, is that the transmission is corrupted if *client 2* also starts a conversation with the *server* at the same time. This is called the hidden node problem.

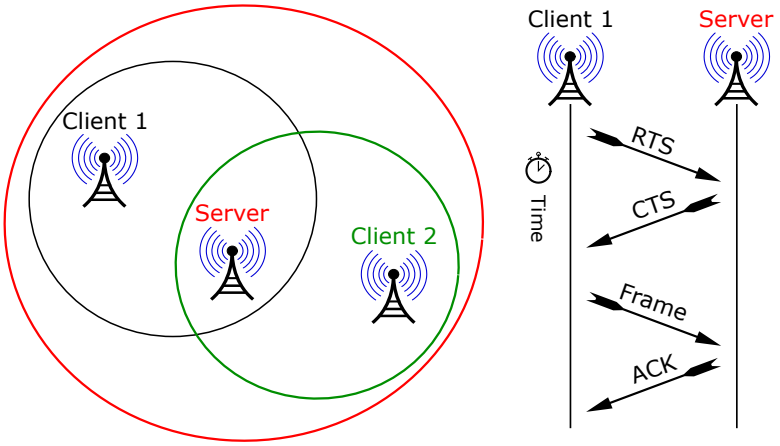

Figure 3: Hidden node problem: distribution of the involved stations and their ranges sketched by colored circles (left), utilization of the RTS-CTS transaction over time (right) [2]

To prevent such errors, the MAC is able to introduce request to send (RTS) and clear to send (CTS) frames. Now, before *client 1* starts a transmission, it first sends an RTS frame and waits for a CTS reply by the *server*. Then, *client 2* also receives this frame and holds the channel free. Figure 3 shows this scenario in detail. On the left side, three WLAN stations are visible. The colored circles mark the respective ranges. Obviously, *client 1* and *2* cannot reach each other. Consequently, the RTS-CTS transaction is performed (right side of Figure 3).

Generally, long data frames tend to be corrupted in a noisy environment. Therefore, WLAN offers two ways to mitigate this problem. The first one is to fragment long sequences into short ones and the second is to implement an RTS-CTS exchange. The indicator for such a transaction is given by the RTS threshold. If the frame length is larger than the defined threshold, an RTS is utilized.

Usually, the fragmentation and RTS threshold are of the same size.

Network Allocation Vector

The MAC header of WLAN frames (Figure 6) introduces the signal duration field, also called network allocation vector (NAV), which can be used to hold the channel free from WLAN interference for a defined time period. This method is called virtual carrier-sensing. Figure 4 depicts a transmission sequence between sender and receiver with an RTS-CTS transaction.

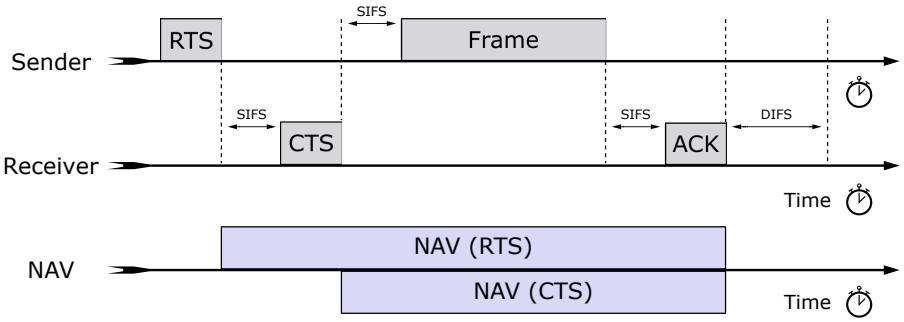

Figure 4: Signal duration indicator [2]

When a frame transmission between two stations starts, the NAV is also received by all other reachable stations and each of them starts a timer. In this time, the channel is held free from WLAN interference until the timer elapses. Furthermore, the NAV can be updated if the frames have been fragmented before. It must be mentioned that the NAV is also sent for transmissions without an RTS and CTS sequence.

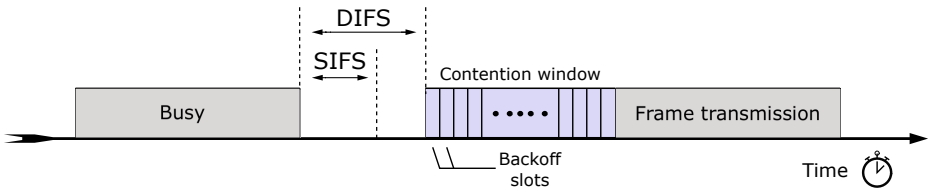

Figure 5: IFS: time constraints which have to elapse before proceeding with a new transmission [2]

Interframe Spacing

One can notice the marked spaces SIFS and DIFS in Figure 4. They are called IFSs. IFSs are utilized to coordinate the channel access among multiple WLAN stations. In IEEE 802.11, several different types are defined depending on the frame type. In the following, the most important ones will be discussed. Figure 5 depicts how they relate to each other.

Short interframe space (SIFS):
Only high-priority events, such as RTS, CTS, and ACK frames are allowed to transmit after one SIFS has elapsed. If such a high-priority transmission has started, the medium becomes busy. Thus, frames transmitted after SIFSs have a higher priority than, for example, frames that are transmitted after DIFS.

Distributed interframe space (DIFS):
Determines the minimum idle time which must elapse before a contention based transmission can be started. One DIFS is followed by a contention window with 31 slots. These slots are chosen randomly by a station and are equally distributed. Now, the station which chooses the first slot, relative to the others, wins and is allowed to transmit a frame afterwards. If two stations choose the same slot and interfere with each other, another greater contention window is utilized.

IFS	2.4 GHz	5 GHz
SIFS	10 µs	16 µs
DIFS	28 µs	34 µs
RIFS	2 µs	2 µs

Table 1: IFS durations for IEEE 802.11n

Table 1 provides information on typical IFS lengths in IEEE 802.11n. In order to decrease latency effects, another type is introduced, called the reduced interframe space (RIFS). It is the shortest space used in IEEE 802.11n. Since newer WLAN revisions launched to the market, RIFSs are often deactivated per default in networks to maintain compatibility.

Frame Format

Corresponding to Figure 1, WLAN utilizes the IEEE 802 LAN topology. Hence, it makes use of the internet protocol (IP) for linking with other stations. In order to address a specific receiver under the mentioned challenges in a wireless data link, the MAC layer generates defined frames. For instance, such sequences let the receivers know if they have to respond or not. Figure 6 depicts a generic MAC frame structure.

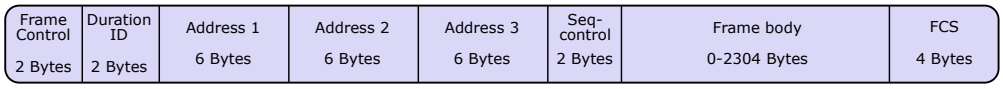

Figure 6: Generic IEEE 802.11 MAC frame [2]

The MAC frame is a very powerful part with plenty configurable properties. Therefore, only the most important ones are presented in the following.

Frame control:
Gives the receiver information about the frame type. In the IEEE 802.11 standard, three different types exist: management, control, and data frames. Management frames are typically broadcasted by access points or association communications. In the section about hidden node problems, RTS and CTS have been introduced, which are control frames. The last type is, due to its name, self explanatory and simply transmits data.

Duration/ID:
The most important use case of the duration field is the virtual carrier-sensing called NAV. With this information each receiver knows for how long the medium will be busy.

Address fields:
The address fields contain the MAC addresses of the receiver and transmitter. The third address is used for filtering the basic service set ID to identify different networks (access points) in the same area.

Frame body:
Moves data between two stations corresponding to higher layer protocols, such as UDP or TCP. The maximum payload in IEEE 802.11 is a data amount of 2,304 Byte. However, in conventional systems, the maximum amount of data is 1,500 Byte. This length is determined by the maximum transmission unit (MTU) size of a system, which will be discussed in Section 2.3.

FCS:
The frame check sequence (FCS) provides the receiver with information whether the received data packet is damaged. The transmitter sends the FCS within the MAC frame and the receiver recalculates the FCS. The transmission is expected to be correct if the two check sums match. Otherwise, the ACK frame is not sent back and a retransmission is forced, depending on the used protocol.

At the end, the total MAC frame is passed to the PHY layer, which applies further operations onto data.

2.2 Physical Layer

The lowest sublevel of the IEEE 802.11 architecture is the PHY layer. In this section, the working principle and further common topics, which appear in the PHY-layer management, will be discussed in detail.

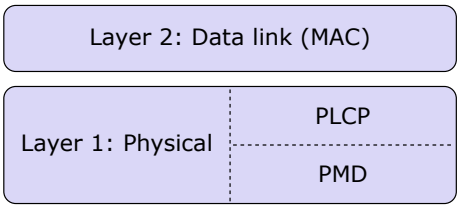

Figure 7: Interaction between MAC and PHY [2]

Figure 7 depicts the PHY-layer structure. It consists of two main parts, the physical layer convergence procedure (PLCP) sublayer and the physical medium dependent (PMD) sublayer. The PLCP sublayer can be interpreted as the interface between MAC and PHY layers. It adds a specific header for frame detection and synchronization to the frame passed by the MAC. Lastly, the PMD sublayer transmits the provided data from the PLCP sublayer by using the radio frequency (RF) front-end. Furthermore, the PHY layer utilizes another important application to mitigate interference perturbations, called clear channel assessment (CCA). The CCA indicates if the medium is idle or busy. This information is directly passed to the MAC for collision avoidance.

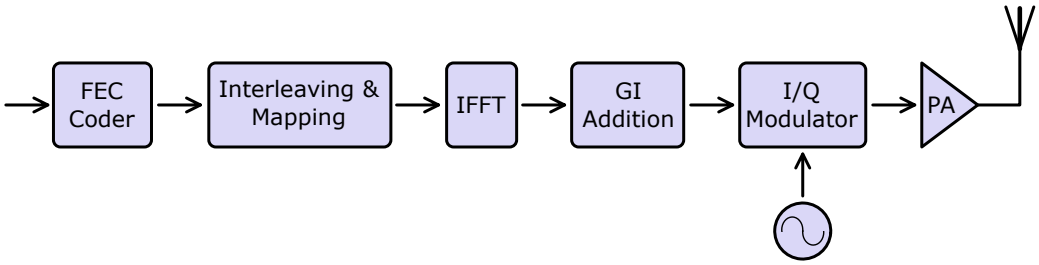

Figure 8: IEEE 802.11 transmission chain [1]

Modulation

The PMD sublayer of current WLAN systems is capable of two different modulation types, called direct spread spectrum sequence (DSSS) and orthogonal frequency division multiplexing (OFDM). DSSS is the older version of the two, but still in use in the IEEE 802.11b standard. With this technique, a bitrate of 11 Mbits/s at 22 MHz bandwidth is achieved.

In newer standard revisions, the OFDM modulation has carried through due to its higher data rates and smaller bandwidth. The main advantages of OFDM are robustness against multipath fading and simplicity of channel estimation. As IEEE 802.11n utilizes the OFDM modulation only, the focus in this section will lie on this technique.

Figure 8 depicts the transmitter chain of the PMD sublayer in IEEE 802.11n (single antenna). At the beginning, a given bitstream is encoded by a forward error correction (FEC) coder. Afterwards the data is interleaved, together with the encoding, ensuring a better performance due to added redundancy and data reordering. The following path can be viewed as an OFDM modulator (Figure 9), which consists mainly of two parts, the OFDM modulation and the cyclic prefix (CP) extension.

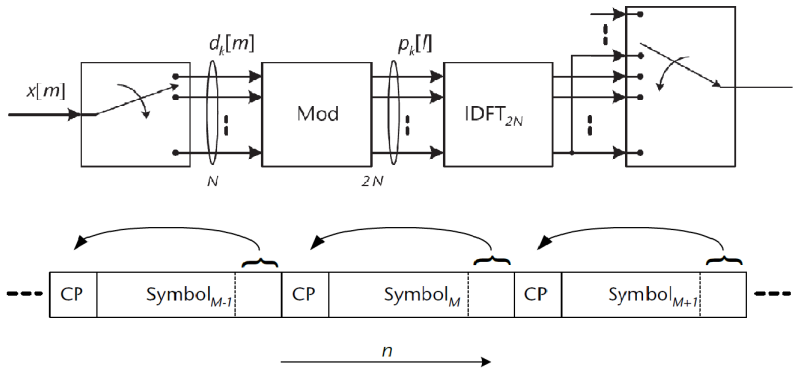

Figure 9: OFDM modulation (top) and applying the cyclic prefix extension (bottom) [3]

The encoded bitstream is mapped onto a desired scheme, for instance, quadratue amplitude modulation (QAM) or binary phase shift keying (BPSK). Afterwards, the serial symbol sequence is transposed into a column vector. Now, the next step is to apply an inverse fast Fourier transform (IFFT). At last, the CP is added to the OFDM symbol. The CP is a fractional part of the created OFDM symbol after applying the IFFT. It is appended to the beginning of the respective symbol, yielding several advantages discussed in the following. After another transpose to a row vector, the baseband signal is mixed up to the desired frequency and passed through the channel.

The cyclic prefix, together with the fast Fourier transform (FFT), offers a major advantage. The receiver stage detects a WLAN frame, strips off the CP and demodulates the signal accordingly with the FFT. Thus, the detected signal is in the frequency domain and the channel estimation results in a simple mathematical division. Nonetheless, the FFT ensures orthogonality only if the signal is periodic, which is established with the CP. Through the periodicity introduced by the CP, the convolution with the channel is circular. Therefore,

with its use, it is possible to absorb all multipath components up to a delay which is not longer than the CP itself. This technique makes OFDM robust against multipath fading.

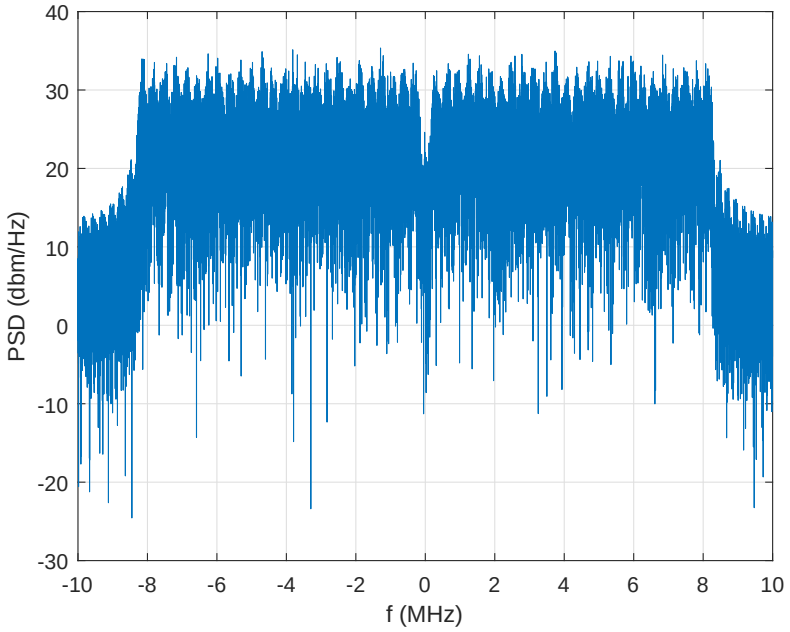

Figure 10: Spectrum of an IEEE 802.11a WLAN frame with BPSK mapping

WLAN shares the ISM band with lots of different standards, such as BLE, Sigfox, HiperLAN, and many more. Due to splitting the data into K parallel streams, according to the FFT size, the spectrum of OFDM is broadband ($\geq$ 20 MHz). Figure 10 depicts the spectrum of a WLAN frame according to the IEEE 802.11a standard. This broadband characteristic makes WLAN susceptible for interference perturbations. Therefore, it will be examined how different interference sources affect the overall performance of communication systems based on WLAN.

Preamble

As already discussed in the previous section, the PLCP sublayer introduces a preamble for frame synchronization and initial channel estimation. In Figure 11, one can see the legacy preamble of an IEEE 802.11a WLAN frame. This sequence consists of a short training field (STF) and a long training field (LTF). The STF is used for coarse signal detection, diversity selection, etc., while the LTF is utilized for fine timing-, frequency-offset synchronization, and channel estimation.

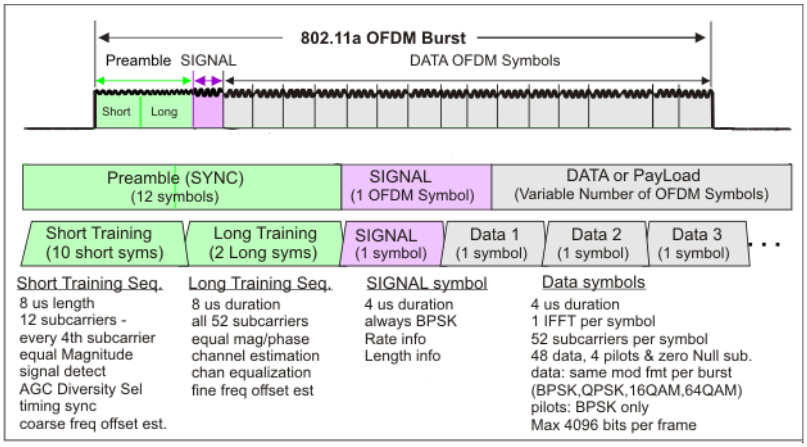

Figure 11: Preamble of an OFDM IEEE 802.11 frame [4]

The STF field consists of a ten times repeated 0.8 µs long training sequence. These fields are generated according to a Barker sequence. This type ensures that the autocorrelation function is minimal at off-peak values. Due to this repeated structure, a certain algorithm, invented by Schmidl and Cox, can be implemented for coarse frame detection [5].

The LTF field is again 8 µs long, but consists of two repeated sections including a long guard interval. This field is used for fine timing- and frequency-offset synchronization by implementing, for instance, a matched filter. More details about detection and synchronization schemes will follow later.

The signal (SIG) field gives the receiver information about the used modulation, coding rate, frame length, and used standard. In order to provide compatibility for all standards, the symbol mapping of the SIG field is always done by utilizing BPSK. Since newer standards, like the IEEE 802.11n, make use of multiple antennas, beamforming, and several diversity techniques, the preamble becomes longer to provide the required information.

Clear Channel Assessment

In the previous section about the MAC layer, the NAV was introduced. This vector is used for virtual carrier sensing, providing a technique for collision avoidance in a multiuser scenario. In order to detect further interfering signals, such as BLE or microwave ovens, the PHY layer adds another method to mitigate interference effects. Before every transmission, the physical layer starts a CCA sequence according to Figure 12. Before a station is allowed to transmit, it listens to the channel, finding out if it is busy or not. The channel sensing consists of two parts. Firstly, a preamble detection with the Schmidl and Cox algorithm is performed. Secondly, an energy detector, which samples data within 4 µs,

is implemented. In the IEEE 802.11a standard, it is specified that the preamble detection must work down to a power level of −82 dBm and the energy detection down to −62 dBm in order to detect every other kind of interference. It must be mentioned here, that state-of-the-art WLAN modules do achieve a much better preamble detection power level of about −92 dBm. If the channel is determined to be free for at least a distributed interframe space (DIFS), a contention window is started. After transmitting the desired frame, the channel is sensed for collision detection again. In the case of detecting interference, violating IFS timing constraints, the backoff strategy is started again. Otherwise, the transmission is completed.

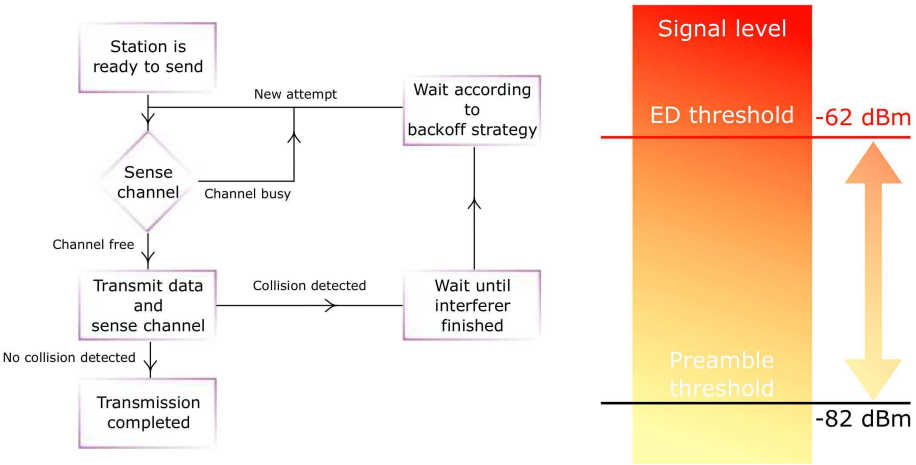

Figure 12: CCA: flow diagram (left), channel sensing thresholds (right) [1]

It must be emphasized that the channel sensing scheme becomes a threshold decision problem and influences the performance of WLAN systems. The throughput between two stations might be reduced significantly if the threshold is set to low values in crowded areas. This problem could be skipped if the threshold is set to the maximum of −82 dBm. Consequently, the received signal power of the two stations must be high enough to neglect the residual interference beyond this power level. One must notice that this solution will only work if the stations are close to each other, since the transmit power in WLAN is limited to about 20 dBm. In addition to this aspect, the decision threshold becomes important for power-critical applications, such as battery-powered devices. Typically, stations adjust their transmit power according to a received signal strength indicator (RSSI) for saving energy. Naturally, this tactic succeeds only if the receiver does not neglect the utilized power level, attenuated by the channel.

2.3 Higher-Layer Protocols

WLAN utilizes the IEEE 802 LLC encapsulation. Therefore, it is able to work with higher OSI layers. In Figure 1, only the first two layers are presented, but the general model consists of seven layers in total. As the goal of this project is to describe interference mechanisms in WLAN systems, it is necessary to characterize them. In order to measure interference effects in real world systems, packet error rates (PERs), throughput, and retransmissions are investigated. Hence, to understand how interference effects on WLAN systems can be characterized, two more layers have to be considered.

Network Layer

This layer mainly routes the best logical paths between two nodes for an efficient data exchange. Typical hardware devices which relate to the network layer are, for instance, routers, bridges, and switches. In addition to this, it is capable to transmit variable data lengths. If the message is too large for the utilized communication standard, it is fragmented into frames. The maximum data length is defined by the MTU. The MTU size in Ethernet networks is defined to be 1,500 Byte long. Therefore, every payload data that is to be transmitted is fragmented into frames if it exceeds the MTU size. Furthermore, it is able to send these fragments independently and reassemble them again at the receiver side.

Transport Layer

The fourth instance of the OSI model establishes a reliable data link to a desired destination by maintaining quality of service functions, such as flow control, segmentation, and error detection. Depending on the used protocol, the transport layer can enforce retransmissions of packets due to a missing ACK frame. The two most important protocols for this project are the UDP and the TCP.

User datagram protocol (UDP):
UDP is a simple transport layer protocol. Because of the FCS introduced by the MAC frame, UDP is capable to detect errors. However, there is no guarantee that the message has been transmitted successfully. The transmission procedure starts by simply sending the frame. This means that no handshake with the receiver side is necessary. If the transmission was successful, an ACK frame is replied, but if not, the transmitter does not force a retransmission. Hence, UDP always sends packets with maximum data rate and will be used for PER and throughput tests in this work. It must be mentioned that this protocol is not applicable for services which require a high reliability. Therefore, it is often used for applications with an error tolerance, such as video streaming or gaming servers.

Transmission control protocol (TCP):
TCP is a more complex protocol compared to UDP. It implements a linking management, flow control, and error detection. These properties will be explained by a simple data exchange example. First of all, the transmitter establishes a connection with the receiver before a data transfer is started. After each packet, an ACK frame is sent back or not, depending on the error detection. If the ACK frame is missing, a timer is started, after which the damaged packet is retransmitted. During payload data transmission, TCP controls the throughput and adapts it according to occurring retransmissions. At the beginning, it starts with a small window size and increases it continuously until a retransmission is necessary. Thus, it reacts dynamically to interference effects. At the end of a data exchange, the connection is terminated. Consequently, the two involved stations are always in contact with each other to ensure a highly reliable connection. The main applications of TCP are, for example, email exchanges.

3 Interference Sources

Although WLAN is capable of various techniques for interference mitigation, the performance in terms of throughput, PER, and retransmissions is still limited. In the following, common interference effects and the respective sources will be described in detail.

Under ideal conditions, when a given channel is used only by WLAN systems with sufficient transmit power, no interference effects occur because of MAC- and PHY-layer constraints. Unfortunately, in real world scenarios, many distributed access points and their local associated clients share the same channel and the hidden node problem is inevitable. As already explained, this effect is handled by an RTS-CTS transaction. Nevertheless, this problem leads to transmission perturbations for packets that are smaller than the RTS threshold. Furthermore, if a DIFS (Figure 5) has elapsed after a transmission, it is statistically possible that some stations pick the same time slot of the backoff window. This would also lead to interference effects. Since these events do not consider co-existence problems with other standards or microwave ovens, the most important sources are investigated in the following.

3.1 Bluetooth Low Energy

At the beginnings of Bluetooth the main focus was put on connecting cell phones to laptops. Later on, its main application became establishing an audio link between headphones and a smart phone. As these applications required an increased throughput, the data rate of newer Bluetooth-standard revisions was increased from a basic rate of 1 Mbit/s to hundreds of megabits per second. It is clear that an increased throughput causes a reduced battery lifetime.

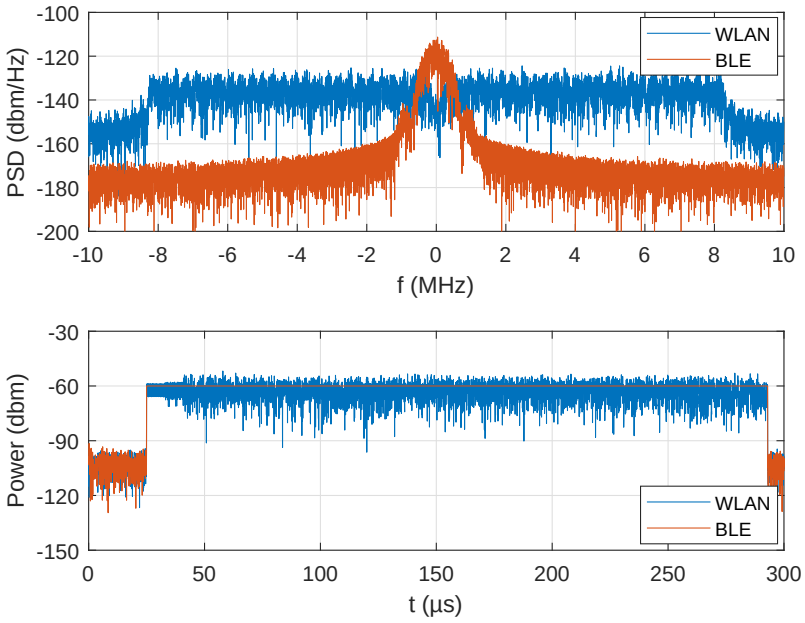

Figure 13: BLE vs. WLAN: spectrum (top) and envelope (bottom)

Therefore, BLE has been launched for low-power applications. It was designed for short lasting communications, for instance, incorporated by wireless sensors. Because of this low-power consumption, it is widely used in the IoT branch besides WLAN. Since BLE does not perform collision avoidance in higher layers (MAC layer), the subject of this section is how the PHY layer of BLE works and which co-existence problems arise [6].

Physical Layer

The PHY layer of BLE utilizes Gaussian frequency shift keying (GFSK) with a bitrate of 1 or 2 Mbits/s and an according bandwidth of 1 or 2 MHz. This modulation keeps the spectral efficiency high by optimizing transitions between symbols. Figure 13 depicts the spectrum and envelope of a BLE- compared to a WLAN packet. Because of the used modulation, the side lobes are decaying fast and ensure low co-channel interference. In comparison with OFDM, the envelope of GFSK signals appears to be almost constant while OFDM shows a noise-like behavior. As a consequence, these two modulation types presumably behave differently as interferers.

BLE uses up to 36 channels in the 2.4 GHz ISM band for data transmission and partly coincides with WLAN bands corresponding to Figure 14. Furthermore, it must be noticed that static advertiser channels are placed for device coupling communications outside of

the main WLAN channels (1,6,11).

In the ISM band, the maximum transmit power is regulated to 10 dBm, which makes it capable of transmitting over long distances. Since modern BLE receivers achieve a receiver sensitivity down to −90 dBm, a minimum SNR of approximately 20 dB, which equals a distance of 250 m, is necessary for correct demodulation [6].

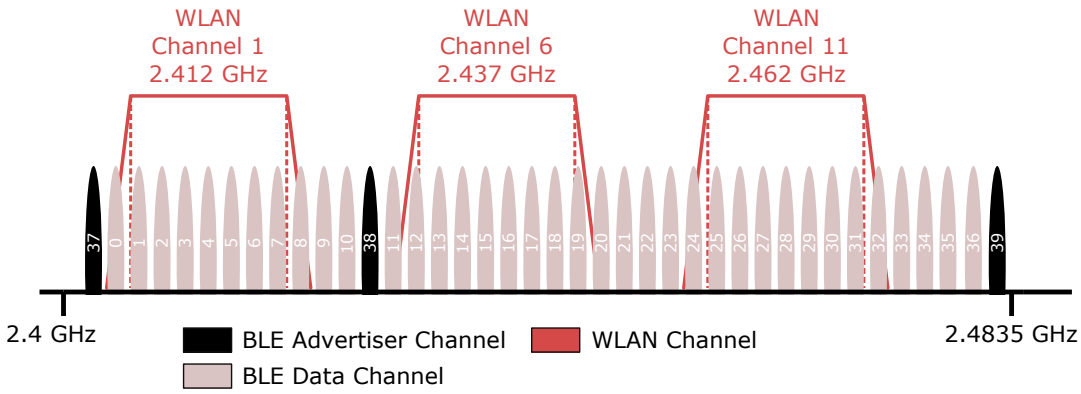

Figure 14: BLE channel separation interfering with main WLAN channels

Since the topic of this project is to investigate interference effects on WLAN communication systems, it is noteworthy that BLE does not perform any CCA before sending data. The reason for that is the implementation of frequency hopping (FH). Corresponding to Figure 14, 36 channels are used in a random fashion during data transmission (hopping). In the ISM band it is allowed to access one single channel for a certain time period. This ensures, that one channel is not blocked over a long time. Because of this frequency hopping technique, a co-existence problem between WLAN and BLE arises. The BLE channels are chosen randomly, but they might interfere with WLAN packets. In order to mitigate transmission perturbations, BLE improved its PHY layer for collision avoidance.

Adaptive Frequency Hopping

The ISM band is used by various different standards. Therefore, a channel sensing scheme is indispensable. Bluetooth utilizes adaptive FH to improve collision avoidance. This simple technique identifies channels which are already in use and remaps them onto channels expected to be free of interference. Figure 15 gives an idea, how this scheme works. Occupied channels are identified in terms of received signal strength indicator (RSSI), SNR, and PER. Nevertheless, it is necessary to maintain a minimum number ($N_{min} = 20$) of remaining channels in an interference scenario. Hence, if less than N_{min} channels are free of perturbations, also occupied ones are considered for transmitting data. Thus, this problem

becomes more important for broadband systems, such as WLAN using modulations with a bandwidth of 40 MHz. Furthermore, because of fading effects, some channels may appear to be free even when they are not.

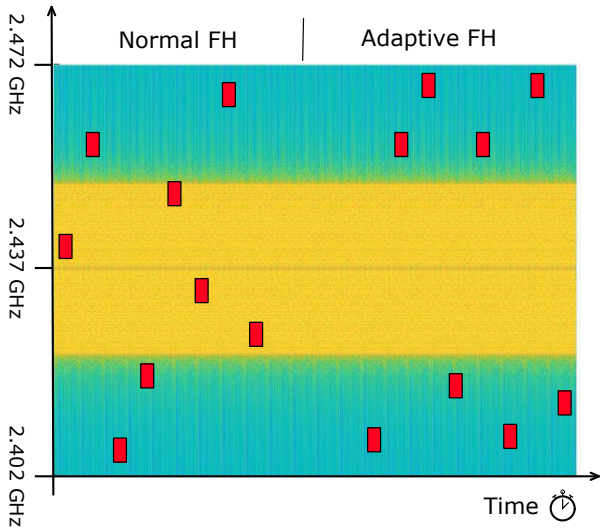

Figure 15: Adaptive frequency hopping: BLE (red), WLAN (yellow)

3.2 Short Range Devices

Besides BLE based communication systems, SRDs are becoming increasingly popular. Typical applications are, for instance, alarm systems, wireless audio, and wireless keyboards. SRDs are using almost all ISM bands. As this document relates to WLAN based systems, the 2.4 GHz band is investigated.

In the previous sections, different collision avoidance- and channel access schemes, such as carrier sensing (CCA utilized in WLAN) and FH (BLE), were discussed. Some SRDs use these techniques as well, but especially the CCA demands a high computational effort. In addition to this, low-power applications, such as wireless keyboards transmit very small packet sizes. Typical keyboards would get along with a 7-bit broad codebook, but through the utilization of additional encryption techniques and protocols the packets are about ~ 100 bit long. Hence, rudimentary channel access schemes, such as the duty-cycle based random access, are utilized. Stations are sending within one time frame T for a maximum time interval $T_s \ll T$. In order to prevent static collisions with other stations, the access of the channel is random. As collisions are likely to happen for high device densities, for instance, the non-slotted ALOHA protocol can be utilized. In order to enhance the reliability of data exchanges, successful transmissions are confirmed by ACK replies. Because of this simple working principle, the duty-cycle based random access scheme suits low data

rate applications, such as wireless keyboards [7].

State-of-the-art SRD transceiver chips, such as the *CC2500* from *Texas Instruments*, are capable of all common modulation types (GFSK, QAM) and channel access schemes (FH, CCA). Depending on the application, an occupied bandwidth (99 %) between 91 kHz and 489 kHz at a maximum transmit power of 1 dBm is achieved. Furthermore, RSSI measurement functions are implemented. As these kind of integrated chips are highly flexible, SRDs are a serious interference source for WLAN communication systems. Especially low-power applications, using rudimentary channel access schemes, neglecting carrier sensing, presumably affect data exchanges extensively. In addition to this, the transmit power is high enough to perturb WLAN receivers close to SRDs.

3.3 Microwave Ovens

The widespread use of microwave ovens, for instance, in hospital environments affects WLAN systems operating in the 2.4 GHz ISM band. As microwave ovens usually have a high power level, compared to other communication standards, they can be detected easily. The spectrum of microwave ovens spreads over a wide frequency range for long time intervals. It is possible to describe the emission characteristics by a narrowband signal with a bandwidth smaller than 1 MHz and a center frequency of 2.45 GHz. The broadband spectrum is modeled by significant variations of the center frequency. The radiation pattern can be approximated isotropic with a maximum effective isotropic radiated power (EIRP) level up to 33 dBm, while the mean EIRP is about 5 dBm. Furthermore, the periodically emitted RF power depends on several individual device characteristics, such as type, load, and make of the oven.[8].

Type	**Emission pattern**
Transformer type	emits once per AC power cycle, every 20 ms
Switching type	emits twice per AC power cycle, every 10 ms
Inverter type 1	emits once per inverter switching-cycle typically, every 35 µs
Inverter type 2	emits twice per inverter switching-cycle typically, every 17.5 µs

Table 2: Switching characteristics of microwave ovens depending on power supply realization [8]

As the emission pattern strongly depends on the type of the implemented power supply, Table 2 indicates some examples describing the time periodic behavior for different realizations. Obviously, the radiation pattern for the first two types extends over long time intervals and for the inverter types over short times, but the off-time is also much shorter. Hence, if the collision avoidance of a WLAN system would detect a microwave oven burst and no PER occurs, still the throughput would be decreased. As a consequence of these properties, it is clear that the throughput as well as the PER of WLAN systems may suffer significantly from this type of interference.

3.4 Radar Systems

Until now, interference sources of the 2.4 GHz ISM band have been discussed. But the 5 GHz band also suffers from perturbations caused, for instance, by weather radar systems. Radar signals are typically very short duration pulses. As no specific timing constraints, such as IFSs, have to be fulfilled it is a challenging task to identify such signals.

Refering to *ETSI EN 301 893 V2.1.1 (Annex D)*, radar signals can be described by different patterns [9]. The short pulses are sent periodically within one burst (L), demonstrated in Figure 16. Typical pulse width parameters are between 0.5 µs and 30 µs.

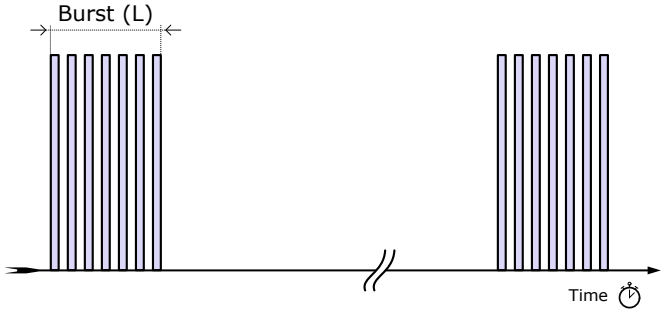

Figure 16: Example of a radar pattern

In order to mitigate such interferers, the dynamic frequency selection scheme has been implemented for WLAN systems working in the 5 GHz band. This technique forces an access point to change the transmit channel randomly if a radar signal is detected by the CCA. Consequently, the data transfer between two stations is interrupted during this change. Especially wrongly detected events identified as radar signals cause a downgrade of the throughput. Furthermore, not all channels utilize the dynamic frequency selection scheme, i.e., channel 36. Therefore, radar signals can influence WLAN communication systems considerably.

References

[1] IEEE Standards Association, IEEE Std 802.11, 2016. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 1, 7, 11

[2] Matthew Gast. *802.11 Wireless Networks: The Definitive Guide*. O'Reilly, Sebastopol, Canada, 2002. 1, 2, 3, 4, 6, 7

[3] Travis F. Collins, Robin Getz, Di Pu, Alexander M. Wyglinski. *Software-Defined Radio for Engineers*. Artech House, 2018. 8

[4] Keysight Technologies `http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/Content/ofdm_80211-overview.htm` 10

[5] Timothy M. Schmidl, Donald C. Cox. *Robust Frequency and Timing Synchronization for OFDM*. IEEE Trans. Commun., Vol 45, No. 12, December 1997. 10

[6] Robin Heydon. *Bluetooth Low Energy: The Developers Handbook*. Prentice Hall, 2013. 14, 15

[7] IMST GmbH, 2012. *Channel Access Rules for SRDs*. `https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Koexistenzstudie_EN.pdf?__blob=publicationFile&v=2` 17

[8] Youping Zhao, Brian G. Agee, Jeffrey H. Reed. *Simulation and Measurement of Microwave Oven Leakage for 802.11 WLAN Interference Management*. IEEE Int. Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications Proceedings, 2005. 17

[9] Harmonised European Standard. *ETSI EN 301 893 V2.1.1, 5 GHz RLAN; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU*, 2017. 18