

ULRR

Effects, classification and mitigation of external interference in IEEE 802.15.4-based wireless sensor networks at 2.4 GHz

Item Type	Thesis
Authors	Zacharias, Sven
Download date	2026-03-07 17:49:28
Item License	https://creativecommons.org/licenses/by-nc-sa/1.0/
Link to Item	https://hdl.handle.net/10344/4029



UNIVERSITY *of* LIMERICK

OLLSCOIL LUIMNIGH

Effects, Classification and Mitigation of External
Interference in IEEE 802.15.4-based Wireless
Sensor Networks at 2.4 GHz

Submitted by Sven Zacharias

For the award of Doctor of Philosophy

Supervised by Dr. Thomas Newe

Department of Electronic and Computer Engineering

University of Limerick, Limerick, Ireland

Co-supervised by Dr. Sinead O’Keeffe & Professor Elfed Lewis

Department of Electronic and Computer Engineering

University of Limerick, Limerick, Ireland

Submitted to the University of Limerick

June 2014

Declaration

This thesis is written to meet the requirements for the degree of Doctorate of Philosophy. It is entirely my own work and has not been submitted to any other university or higher institution. Where the work of other people has been used, it has been fully referenced and acknowledged.

Signed _____

Sven Zacharias

Contents

1	Introduction	1
1.1	Wireless Sensor Networks	2
1.1.1	A Short History of Wireless Sensor Networks	3
1.1.2	Applications	3
1.1.3	Challenges of the Crowded Frequency Spectrum	5
1.1.4	Provisional Solution to the Crowded Frequency Spectrum	5
1.2	Research Objectives	7
1.3	Thesis Structure	7
2	Technical Background	9
2.1	MAC Sublayer	9
2.1.1	Multiple Access Protocols	11
2.1.2	Further MAC Sublayer Tasks	14
2.2	Physical Layer	15
2.3	IEEE 802.15.4	16
2.3.1	Protocol Stacks and Higher Layers	16
2.3.2	MAC Sublayer	20
2.3.3	Physical Layer	25
2.4	IEEE 802.11b, g, n	36
2.4.1	MAC Sublayer	36
2.4.2	Beacon Frames	40
2.4.3	Physical Layer	41
2.5	Bluetooth	43
2.5.1	MAC Sublayer	46
2.5.2	Physical Layer	47
2.6	Microwave ovens	48
2.6.1	Temporal Behavior	49
2.6.2	Spectral Properties	49
2.7	Other Technologies	50
2.8	Summary	51
3	Research Methodology	53
3.1	Hardware used for Experiments	53
3.1.1	IEEE 802.15.4	53
3.1.2	IEEE 802.11, Bluetooth and Microwave Ovens	57
3.2	Software used for Experiments	58
3.3	Summary	59

4	Effects of External Interference	61
4.1	Effects of Interference Reported in Literature	61
4.2	Modeling of Interference	64
4.2.1	Mutual Effects: Open versus Closed Loop	64
4.2.2	Path Fading Model/Path Loss	65
4.2.3	Signal Ratios	72
4.2.4	Frequency Offset Model/Spectrum Factor	74
4.2.5	Interference Channel Model	75
4.2.6	Interference Protocol Model	76
4.2.7	Connectivity Regions	77
4.2.8	Delay Model	80
4.2.9	Example	80
4.3	Effects Related to Technologies	83
4.3.1	IEEE 802.15.4 as Interferer	83
4.3.2	IEEE 802.11 as Interferer	84
4.3.3	Bluetooth as Interferer	86
4.3.4	Microwave Oven as Interferer	87
4.4	Summary	87
5	Classifying Sources of External Interference	89
5.1	Interference Classification Methods Reported in Literature	89
5.2	Significant Features in the Channel Use Pattern	93
5.2.1	IEEE 802.11b, g, n	93
5.2.2	Bluetooth	94
5.2.3	Microwave ovens	94
5.3	Classification Algorithm Details	94
5.3.1	Simple features	95
5.3.2	Transmission start patterns	96
5.3.3	Periodicity	96
5.3.4	Algorithm Timing	97
5.4	Algorithm Testing	98
5.4.1	Controlled Environment	98
5.4.2	Uncontrolled Environment	105
5.5	Summary and Discussion	108
5.5.1	Classification Results	108
5.5.2	Execution Time	109
6	Interference Mitigation	111
6.1	Interference Mitigation Strategies of IEEE 802.15.4	111
6.2	Network Layer	112
6.2.1	Mesh Networking	113
6.3	Data Link Layer	116
6.3.1	Backward Error Correction	116
6.3.2	Packet Fragmentation	117
6.3.3	Clear Channel Assessment and CSMA/CA	121
6.3.4	Packet Scheduling	124
6.4	Physical Layer	125
6.4.1	Forward Error Correction	125
6.4.2	Signal Spreading/Modulation	126

6.4.3	Rate Scaling/Modulation Control	126
6.4.4	Power Control	127
6.4.5	Channel Alignment, Hopping and Agility	127
6.5	Summary	128
7	An Interference-Aware, Self-Adapting MAC Protocol	131
7.1	Related Work Reported in Literature	131
7.2	IASA MAC Details	132
7.3	Trigger	134
7.4	Packets in ContikiOS: Rime Communication Stack and Chameleon Header Transformation Module	135
7.5	WLAN Mitigation	136
7.5.1	Trickle	137
7.5.2	Discussion	139
7.6	BT1 and BT2 Mitigation	139
7.7	MWO Mitigation	140
7.7.1	Testing	141
7.7.2	Discussion	142
7.8	CLEAR, UNKNOWN and INTERNAL Mitigation	142
7.9	Summary and Discussion	143
7.9.1	Hidden Interferer Problem	144
7.9.2	Cooperation Between Different Mitigation Strategies	145
7.9.3	Summary	147
8	Conclusion	149
8.1	Contributions	149
8.2	Future Work	150
A	Decibel	153
B	Packet error model	155
C	Publications	157
C.1	Journals	157
C.2	Book Chapters	157
C.3	Conferences	157
C.4	Seminars	158
C.5	Reviewer for	158

List of Figures

1.1	Basic overview of the building blocks and possible shapes of wireless sensor nodes.	2
1.2	Overview of the 2.4 GHz frequency band as used by different technologies.	6
2.1	Basic tasks and problems of wireless Medium Access Controls (MACs).	10
2.2	Collision risk duration for slotted and unslotted ALOHA/purely random channel access.	11
2.3	Throughput versus traffic for the most common random access protocols.	13
2.4	Different delivery semantics.	15
2.5	Overview of the Radio Frequency (RF) features of wireless transmitters and receivers in the spectrum.	16
2.6	Outline of the ZigBee stack architecture.	17
2.7	ZigBee tree network topology.	18
2.8	Supported MAC modes of IEEE (2003b).	21
2.9	An example of a superframe structure.	21
2.10	Carrier Sense Multiple Access (CSMA)/Collision Avoidance (CA) for unslotted IEEE 802.15.4 network according to (IEEE, 2003b).	22
2.11	Open Systems Interconnection (OSI) Reference Model with IEEE 802.15.4-specified layers relevant for this work and the implementation details in ContikiOS.	23
2.12	Communication flow and basic timing of X-MAC and Low Power Probing (LPP) protocol.	24
2.13	Schematic view of the IEEE Standard 802.15.4 data frame format.	25
2.14	Schematic view of the IEEE Standard 802.15.4 Acknowledgment (ACK) frame format.	26
2.15	The steps of a packet from the handover of the MAC to the transmission of the electromagnetic signal.	28
2.16	Illustration of a harmonic wave and its representation in the complex or I/Q plane.	30
2.17	Principle of the implementation of the I and Q signal channels in a wireless transmitter.	31
2.18	Constellation diagram for Quadrature Phase Shift Keying (QPSK).	32
2.19	I/Q values, signals ($I(t)$, $Q(t)$) and added signal ($s(t)$) over time for QPSK for all four possible combinations of I and Q values.	32
2.20	Transitions between constellation points by I and Q components for QPSK, Offset Quadrature Phase-Shift Keying (O-QPSK) and O-QPSK with a half-sine pulse shaping filter.	33
2.21	The block diagram of a transmitter with half-sine pulse shaped baseband chips as an enhancement to the basic transmitter shown in Figure 2.17a.	33
2.22	Example Power Spectral Density (PSD) of O-QPSK without and with half-sine pulse shaping filtered chip streams.	34
2.23	PSDs of IEEE 802.15.4 measured with Wi-Spy 2.4x and Received Signal Strength Indication (RSSI) values of a Tmote Sky sensor node.	35

2.24	Basic time flow of the Request To Send (RTS)/Clear To Send (CTS)-handshake, the data transfer and the final ACK of IEEE 802.11.	38
2.25	Schematic view of the IEEE Standard 802.11 frame format. The field sizes in bytes are given in parentheses.	39
2.26	Structure of different frames of different versions/configurations of IEEE 802.11. The field sizes in bits are given in parentheses.	39
2.27	Schematic view of different IEEE Standard 802.11 Medium Access Control Protocol Data Unit (MPDU) formats.	40
2.28	Number of frames (packets), transmitted bits and the airtime compared for different data rates of IEEE 802.11b.	42
2.29	PSDs of different IEEE 802.11 modulations measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node.	43
2.30	PSDs of IEEE 802.11n with channel bonding measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node.	44
2.31	Bluetooth network topology.	45
2.32	Comparison of the most important Bluetooth layers to the layers of the OSI Reference Model.	45
2.33	Timing of single- and multi-slot packets.	46
2.34	The Enhanced Data Rate (EDR) packet format.	47
2.35	Bluetooth signals in the spectrum.	48
2.36	Bluetooth spectrum use due to channel hopping.	48
2.37	Typical radiation timing of microwave ovens.	49
2.38	PSDs 2 m away from the front door of a Matsui microwave oven measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node.	50
3.1	Tmote Sky comparison measurements.	55
3.2	Comparison of node RSSI readings to evaluate inter-node variety.	56
3.3	Screenshots of software programs for spectrum analyzing.	59
4.1	Flow of two Open Loop Methods to estimate the effects of external interference.	66
4.2	Path loss (dB) related to distance (m) in the 2.4 GHz band according to the indoor path loss model used in several IEEE 802 documents.	68
4.3	Different paths of signal propagation according to (Farahani, 2008).	69
4.4	Multipath propagation.	70
4.5	Small-scale effects of Rayleigh and Rician fading as simplified illustrative examples.	72
4.6	Overview of popular channel modeling approaches, based on (Mittag, 2012).	73
4.7	Different cases of packet overlap in the time domain that can occur when the victim packet is shorter than the interferer packet and fits in between two interferer packets.	77
4.8	Theoretical and measured relation of Signal to Noise Ratio (SNR) and Packet Reception Rate (PRR).	78
4.9	Overlap of victim and interfering packet.	79
4.10	Comparison of the Bit Error Rate (BER)-based and connectivity region estimation for different IEEE 802.15.4 packet length under IEEE 802.11 interference.	80
4.11	Setup in the RF anechoic chamber for Signal to Interference Ratio (SIR)-Packet Error Rate (PER) experiment.	82
4.12	Calculated relation of SIR to BER and resulting PRR versus measured data points for IEEE 802.15.4.	82
4.13	Ranges of sender- and receiver-side interference for an IEEE 802.15.4 link under IEEE 802.11 interference.	85

4.14	Ranges of sender- and receiver-side interference for an IEEE 802.15.4 link under Bluetooth interference visualized for ranges of the victim nodes in the plane. . . .	86
4.15	Overview of the most important characteristics of different sources of interference.	87
4.16	IEEE 802.11 channel (airtime) utilization over time measured during a conference, plotted with a binning interval of a minute.	88
5.1	Overview of literature structured by classification method.	89
5.2	Distribution of bit errors in IEEE 802.15.4 packets corrupted by IEEE 802.11g. . .	92
5.3	Beacon transmission on a busy network.	94
5.4	Different theoretical ranges of an Access Point (AP) and a laptop client and the resulting zone of only client interference.	94
5.5	Typical RSSI traces of the different sources of interference.	95
5.6	Concept of a simple algorithm to detect periodicity/frequency component p in a discrete, binary signal <i>signal</i> for a given period T given in samples.	97
5.7	Flow and timing of the algorithm.	97
5.8	Algorithm testing for single interfering technologies.	99
5.9	Setup of the experiment “real-world channel utilization”.	102
5.10	Results of a 24-hour long-term evaluation of the classification algorithm in a real-world environment (trace of a single node).	106
6.1	Interference mitigation strategies structured according to the OSI Reference Model Layers, in which they are commonly implemented, and relations between the different strategies.	112
6.2	Overview of the steps and different methods of node localization according to Boukerche et al. (2009b).	115
6.3	Transparent and nontransparent fragmentation.	118
6.4	Probability tree for a maximum of four retransmissions, with a PRR of 75%. . . .	119
6.5	Experiment setup and PRRs of different Clear Channel Assessment (CCA) modes.	122
6.6	Channel access timing and channel use duration comparison of different technologies.	124
6.7	BER calculations for different modes of IEEE 802.11b, IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (Ultra Wide Band (UWB)) and IEEE 802.15.4.	126
7.1	Generalized flow chart of Interference-Aware, Self-Adapting (IASA) MAC.	133
7.2	The communication primitives of the Rime communication stack and their relations.	136
7.3	An example of the architecture of ContikiOS.	137
7.4	Microwave interference corrupting the end of IEEE 802.15.4 packets.	140
7.5	Experiment setup to test the efficiency of packet scheduling under microwave oven interference.	142
7.6	Detailed flow chart of IASA MAC.	144
7.7	Simple example of a detectable and a hidden interferer.	146

List of Tables

2.1	License-free Industrial, Scientific and Medical (ISM) radio bands supported by IEEE 802.15.4 in its different versions.	27
2.2	Symbol-to-chip mapping, values taken from (IEEE, 2003b).	29
2.3	Key features of the different versions of IEEE Standard 802.11 operating in the 2.4 GHz frequency band.	36
2.4	The durations of interframe spacings for different versions of the IEEE 802.11 standard.	38
2.5	Selected airtimes of packets for different IEEE Standard 802.11 versions and settings.	40
2.6	Features of beacon frames from observed APs.	41
2.7	Different modulations supported in the different modulation schemes by IEEE 802.11b and IEEE 802.11g.	41
2.8	Synchronous packet features, based on (Bluetooth SIG, Inc., 2007).	47
2.9	Asynchronous Connection-Less (ACL) packet features, based on (Bluetooth SIG, Inc., 2007).	47
2.10	Bluetooth power classes, based on (Bluetooth SIG, Inc., 2007).	48
2.11	Overview of the technologies operating in the 2.4 GHz frequency band.	51
3.1	Selected parameter specifications for an IEEE 802.15.4-compliant receiver required by (IEEE, 2003b) and the corresponding specifications of a CC2420 radio (Chipcon, 2004).	54
3.2	Equipment used in the course of this work.	58
4.1	Literature on the effect of external interference on IEEE 802.15.4.	62
4.2	Different ranges of interference and their names in literature, when IEEE 802.15.4 and IEEE 802.11 use an Energy Detection (ED)-based CCA mode.	64
4.3	Path loss exponents for different environments.	68
4.4	Different types of small-scale fading (Rappaport, 1996; Mittag, 2012).	71
5.1	Controlled environment IEEE 802.11 experiments for low channel utilization summarized by channels.	101
5.2	Controlled environment IEEE 802.11 experiments for real-world utilization summarized by channels.	102
5.3	Controlled environment Bluetooth experiments summarized by experiments and details of experiment with the worst classification rate.	103
5.4	Controlled environment IEEE 802.11 and Bluetooth experiment summarized by channels.	104
5.5	Controlled environment microwave oven experiment summarized by distance and details of node closest to the oven.	105
5.6	Uncontrolled environment IEEE 802.11 experiments summarized by channels.	106
5.7	Uncontrolled environment microwave oven summarized by channel.	107

6.1 Overview of common interference mitigation strategies. 129

7.1 Comparison of simple moving average and exponential smoothing. 134

7.2 Number of packets at different stages in a simple link communication under
microwave oven interference. 142

7.3 Overview of the interference situation and the efficiency of IASA MAC. 143

A.1 Decibel to linear power ratio conversions and example scale. 153

List of Acronyms

6LoWPAN Internet Protocol version 6 over Low power Wireless Personal Area Networks

8DPSK 8 phase Differential Phase Shift Keying

ACK Acknowledgment

ACL Asynchronous Connection-Less

AFH Adaptive Frequency Hopping

AODV Ad-hoc On-demand Distance Vector

AP Access Point

ARQ Automatic Repeat reQuest

ASB Active Slave Broadcast

ASCII American Standard Code for Information Interchange

ASK Amplitude Shift Keying

ATEX ATmosphères EXplosives

AUX AUXiliary

AWGN Additive White Gaussian Noise

BEC Backward Error Correction

BER Bit Error Rate

BIAS Bluetooth Interference Aware Scheduling

BPSK Binary Phase-Shift Keying

CA Collision Avoidance

CCA Clear Channel Assessment

CCK Complementary Code Keying

CD Collision Detection

CPU Central Processing Unit

CQDDR Channel Quality Driven Data Rate

CRC Cyclic Redundancy Check

CSMA Carrier Sense Multiple Access

CSS Chirp Spread Spectrum

CTP Collection Tree Protocol

CTS Clear To Send

D-ITG Distributed Internet Traffic Generator

DARPA Defense Advanced Research Projects Agency

DBPSK Differential Binary Phase Shift Keying

DCF Distributed Coordination Function

DECT Digital Enhanced Cordless Telecommunications

DH Data High rate

DIFS Distributed (coordination function) InterFrame Space
DM Data Medium rate
DQPSK Differential Quadrature Phase Shift Keying
DSN Distributed Sensor Network
DSSS Direct-Sequence Spread Spectrum
DV Data Voice
EAD Energy-Aware Data-centric Routing
EDR Enhanced Data Rate
ED Energy Detection
eSCO extended Synchronous Connection-Oriented
ETSI European Telecommunications Standards Institute
EV Extended Voice
FCC Federal Communications Commission
FCS Frame Check Sequence
FEC Forward Error Correction
FFD Full Function Device
FHSS Frequency-Hopping Spread Spectrum
FHS Frequency Hop Synchronization
FIM Fingerprint Identification Mechanism
FIR Finite Impulse Response
FTP File Transfer Protocol
GFSK Gaussian Frequency Shift Keying
GNU GNU's not Unix
GPS Global Positioning System
GRAB Gradient Broadcast
GSM Global System for Mobile Communications
HART Highway Addressable Remote Transducer
HCF Hybrid Coordination Function
HT High Throughput
HV High quality Voice
IASA Interference-Aware, Self-Adapting
ID Identification
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IIR Infinite Impulse Response
IP Internet Protocol
ISA International Society of Automation
ISI Inter-Symbol Interference
ISM Industrial, Scientific and Medical
ITA Interference-aware Transmission Adaptation
L2CAP Logical Link Control and Adaptation Protocol
LAN Local Area Network
LEACH Low-Energy Adaptive Clustering Hierarchy

LMP Link Manager Protocol
LPL Low Power Listening
LPP Low Power Probing
LQI Link Quality Indication
LTE Long Term Evolution
M-MPR Meshed Multipath Routing
MAC Medium Access Control
MCFA Minimum Cost Forwarding Algorithm
MCF Mesh Coordination Function
MEMS MicroElectroMechanical Systems
MIMO Multiple Input Multiple Output
MMSPEED Multi-path multi-SPEED protocol
MPDU Medium Access Control Protocol Data Unit
MSDU Medium Access Control Service Data Unit
MTU Maximum Transmission Unit
NAV Network Allocation Vector
NESC Network Embedded Systems C
NTIA National Telecommunications and Information Administration
O-QPSK Offset Quadrature Phase-Shift Keying
OFDM Orthogonal Frequency-Division Multiplexing
OSI Open Systems Interconnection
PAN Personal Area Network
PCF Point Coordination Function
PD-SAP Physical Data-Service Access Point
PEGASIS Power-Efficient Gathering in Sensor Information Systems
PER Packet Error Rate
PG Processing Gain
PHR Physical Header
PHY Physical
 $\pi/4$ DQPSK $\pi/4$ rotated Differential Quaternary Phase Shift Keying
PLCP Physical Layer Convergence Protocol
PLME-SAP Physical Management Entity-Service Access Point
PPDU Physical Protocol Data Unit
PRR Packet Reception Rate
PSB Parked Slave Broadcast
PSD Power Spectral Density
PSSS Parallel Sequence Spread Spectrum
QAM Quadrature Amplitude Modulation
QoS Quality of Service
QPSK Quadrature Phase Shift Keying
RAM Random-Access Memory
RDC Radio Duty Cycling
ReIn-ForM Reliable Information Forwarding using Multiple paths

RFD Reduced Function Device
RF Radio Frequency
RMS Root Mean Square
RSSI Received Signal Strength Indication
RTS Request To Send
RX Receive
SAP Service Access Point
SCO Synchronous Connection-Oriented
SDR Software Defined Radio
SensIT Sensor Information Technology
SHR Synchronization Header
SIFS Short Interframe Space
SIFS Short InterFrame Space
SIG Special Interest Group
SINR Signal to Interference plus Noise Ratio
SIR Signal to Interference Ratio
SNR Signal to Noise Ratio
SoNIC Sensor Network Interference Classification
SPIN Sensor Protocols For Information Via Negotiation
SPI Serial Peripheral Interface
SSID Service Set Identifier
TCP Transmission Control Protocol
TDD Time Division Duplex
TDMA Time Division Multiple Access
TEEN Threshold-sensitive Energy-Efficient sensor Network protocol
TX Transmission
UDP User Datagram Protocol
UMTS Universal Mobile Telecommunications System
USB Universal Serial Bus
UWB Ultra Wide Band
WiMAX Worldwide Interoperability for Microwave Access
WLAN Wireless Local Area Network
WMAN Wireless Metropolitan Area Network
WPAN Wireless Personal Area Network
WPAN Wireless Personal Area Network
WSN Wireless Sensor Network
WS Window Size
WWAN Wireless Wide Area Network

Acknowledgements

I would like to express my gratitude to Dr. Thomas Newe for all the help, patience and advice he has given me in the completion of this thesis. Furthermore, I would like to thank my co-supervisors Professor Elfed Lewis and Dr. Sinead O’Keeffe for their support.

Without the generous scholarship from the Irish Research Council for Science Engineering and Technology (IRCSET) and Intel, this research would not have been possible. Thank you.

Thanks to all in Department of Electronic and Computer Engineerings for their support, especially to all my friends from Lab D2-037 and the Optical Fibre Sensors Research Centre. Victor, although just being a single day older than me, I learnt so much from you.

Also, a big thank you goes to the people of Ireland for the four years of hospitality.

A special thanks to my family for their support and encouragement, without which this would not have been possible. Finally, I would like to thank you, Teresa, for standing by my side, making life more enjoyable and for encouraging me in all stages of this work.

Abstract

The IEEE Standard 802.15.4 defines the low power wireless transmission technology behind Wireless Sensor Networks (WSNs) and ZigBee. Since IEEE 802.15.4 is a low power technology, the mitigation of interference is vital to conserve energy and to extend the lifetime of devices. Most of the IEEE 802.15.4 radios operate in the crowded 2.4 GHz frequency band, which is also used by many other technologies.

A complete study of the common sources of external interference, namely IEEE 802.11-based Wireless Local Area Networks (WLANs), Bluetooth and microwave ovens, is provided. The effects of these coexisting technologies on IEEE 802.15.4 are investigated and the modeling of the interference is discussed.

The possibilities of Energy Detection (ED) (the feature behind Received Signal Strength Indication (RSSI)) and certain Clear Channel Assessments (CCAs) are evaluated. Based on the CCAs, a lightweight interference classification algorithm is presented to classify the common external sources of interference in the 2.4 GHz frequency band without demodulation of the interferers' signals. As the classification algorithm relies on time patterns instead of spectral features, it has no need to change the channel. Thus, it allows the radio both to stay connected to the channel and to receive while the interferer is classified.

Furthermore, interference mitigation strategies are reviewed and evaluated with respect to their effectiveness to overcome the three external sources of interference. By combining the interference classification algorithm and the chosen mitigation strategies, Interference-Aware, Self-Adapting (IASA) Medium Access Control (MAC) is developed. This smart interference-mitigating MAC protocol is implemented in ContikiOS and evaluated.

Chapter 1

Introduction

The development of computer networks started around the 1960s by connecting military systems or mainframes (Leiner et al., 1997). At that time, networks still relied on cables. Although wireless transmissions were known from devices as radio receivers or two-way radios, it needed several technical improvements until computer networks became wireless. Today, the triumph of wireless technologies is manifested in everyday life, ranging from wireless headsets and input devices, mobile phones, wireless Internet on smartphones to wireless routers providing Internet access at home or in the office. These devices provide enormous simplifications for the end users, though different challenges had to be mastered in order to fulfill all technical requirements. As the latter are depending on the spatial scope (or “scale” as referred to by Tanenbaum and Wetherall (2011)), wireless networks are typically classified according to the following:

Wireless Personal Area Networks (WPANs) surround a single person and his/her technical devices and gadgets. This type of network includes Bluetooth headsets and wireless input devices connected to a laptop or a tablet computer.

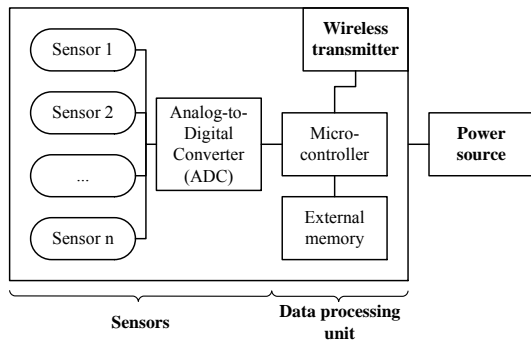
Wireless Local Area Networks (WLANs) have increased considerably in popularity with the success of laptop computers over desktop computers. Today, the word “Wi-Fi”, although originally being an industry consortium, has become a synonym for wireless Internet access.

Wireless Metropolitan Area Networks (WMANs) cover an entire city or urban area. The IEEE 802.16 standard, also known as Worldwide Interoperability for Microwave Access (WiMAX), is a typical WMAN technology and can provide fast Internet in a city. Another WMAN standard is the Long Term Evolution (LTE) technology, known for its fast mobile Internet on smartphones.

Wireless Wide Area Networks (WWANs) have become the focus of scientific interest since the success of smartphones, which reached the mass consumer market around 2007¹. They provide wireless Internet over long distances and thereby offer Internet access in nearly every possible location. Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) are well-known examples of WWANs.

While the preceding network types are mainly downstream data using a star topology, **Wireless Sensor Networks (WSNs)** establish a novel network type, which is based on recent developments in the area of sensory, distributed computing and communication.

¹The first iPhone was released in the year 2007.



(a) Block diagram of a wireless sensor node.



(b) Example pictures of sensor nodes, from left to right: a Tmote Sky (Moteiv Corporation, 2006), a Iris (MEMSIC Inc., 2010a), a MICAz (MEMSIC Inc., 2011), and a MICA2 sensor node in its housing (crossbow technology, inc, 2003).

Figure 1.1: Basic overview of the building blocks and possible shapes of wireless sensor nodes.

1.1 Wireless Sensor Networks

As a contribution to this field of research, this work's scope lies in the improvement of the communication within WSNs by concentrating on external sources of interference and possible strategies for avoiding them. In WSNs, the main direction of data flow is from the client devices, which are also called sensor nodes, to a base station. Due to the inversion of the main communication direction, new challenges arise. In downstream networks, the predominant sender (e.g. a cell tower or a main powered router) can be both strong and power consuming. At the same time, the receivers have limited resources and power. In a WSN, the ratio between sender and receiver is reversed, since the resource-limited nodes send information over multiple hops to their base station. The implications of this inversion are discussed later in this work, e.g. when the author reviews the problem of the sensor nodes being the weakest competitors for the wireless medium. WSNs can achieve data transmission via multi-hopping over the distances of WWANs by means of sensor nodes, which are equally or less powerful than WPAN clients.

A sensor node is generally defined as a cheap and small piece of hardware, which consists of the following four main units: sensors, data processing unit, wireless Radio Frequency (RF) transmitter and an energy source.

- The sensors detect physical phenomena by monitoring scalar values of temperature, pressure, humidity, light intensity, etc. In some cases they even capture multimedia data as sound or video. However, the type of the measured data is not relevant for the scope of this work.
- The sensors are connected to a data processing unit. The latter controls the sensor measurements, the application logic and the radio transmissions. Popular microcontrollers for the processing unit are from the ATmega (Atmel, 2007) or the MSP430 (Texas Instruments, 2010) series. For more demanding tasks, stronger ARM architecture-based microcontrollers have been used (Sun Labs, 2007).
- The wireless transmission of the data is provided by a wireless RF transmitter. In this work, a transmitter compliant to the common IEEE Standard 802.15.4 is used, since this communication standard provides low power consumption and low cost radios.
- As for every operational electronic system, an energy source is needed.

Figure 1.1 provides a general overview of sensor nodes: it summarizes the building blocks of a sensor node in Subfigure 1.1a and shows typical examples of hardware in Subfigure 1.1b.

Sensor nodes are generally designed to be widely spread without pre-configuration. The network between the nodes is built dynamically and it is considered to be self-organizing. With the help of this ad hoc network, the sensor nodes transmit data towards the base station.

1.1.1 A Short History of Wireless Sensor Networks

The current form of WSNs, which have the ability to build an ad hoc network, are a novel technology developed shortly after the year 2000. Their predecessor systems date back to the year 1966.

To the best of the author's knowledge, the first WSN was designed in 1966 and produced in the following year by the United States army in the Vietnam War. The so-called "Igloo White" system consisted of air-dropped sensors to monitor troop movements. Acoustic and seismic data were sent by a radio and received by special aircrafts using analog technology. During the course of this military operation, around 20,000 sensors were deployed along the Ho Chi Minh trail from January 1968 to February 1973 (Correll, 2004).

Military research remained the main sponsor for such systems: for instance the Distributed Sensor Network (DSN) project that connected sensors to the Arpanet (the precursor of the Internet) around 1980, was funded by the Defense Advanced Research Projects Agency (DARPA) (Chong and Kumar, 2003; Carnegie-Mellon University Pittsburgh, 1978). To understand the impact of the DSN project, it has to be mentioned that it was started before the development of personal computers and workstations at a time when Ethernet was just starting to gain popularity. According to Chong and Kumar (2003), the DSN project led to the development of acoustic sensors, high-level communication protocols (e.g. for plotters, graphics and voice) in a resource-sharing network (Sproull and Cohen, 1978), algorithms and distributed software. Even the basics of the Mach operating system (Rashid et al., 1989) were developed in the course of this project. Around the year 2000, the developments in MicroElectroMechanical Systems (MEMS) and other fields of science led to a new DARPA-initiated project called Sensor Information Technology (SensIT) program (Kumar and Shepherd, 2001). Chong and Kumar (2003) regard both the ability to form ad hoc networks in harsh environments, e.g. on the battlefield, and the processing of network information in distributed systems as the two main outcomes of the SensIT research program.

In 1997, again supported by DARPA, the Smart Dust project was announced (Warneke et al., 2001). Based on further miniaturization, sensor nodes as small as a grain of rice (size $< 1 \text{ mm}^3$) or even sand, which are therefore often called "Motes", were planned to be spread in ad hoc fashion without pre-configuration in order to build extremely large WSNs. While the size of a dust particle was not achieved, the project led to affordable commercial-off-the-shelf sensor nodes.

Shortly after, an important WSN deployment was made in 2002, known as the Great Duck Island Deployment (Mainwaring et al., 2002). During a period of nine months, the Leach's Storm Petrel was observed on an island with the help of a WSN consisting of 32 nodes. It became an important project, since it revealed the challenges of the technologies used. However, being over 10 years in the past, the used MICA Hardware Platform is still comparable to the hardware used today and some of these problems are still part of recent research.

Around the same time, WSNs left the research laboratories and became standardized. In 2003, the first IEEE 802.15.4 Standard was released and in 2004, the first version of ZigBee based on this IEEE 802.15.4 Standard was published (IEEE, 2003b; ZigBee Alliance, 2008b). Since 2006, Bluetooth has started the development of a low power standard with features that are comparable to WSNs, though being without multi-hop support (Hunn, 2006).

1.1.2 Applications

The short history of WSNs has already revealed some possible applications of WSNs. However, the possible use of WSNs reaches beyond battlefield surveillance and habitat monitoring. The

following list gives an overview of the wide-ranging applications of WSNs. Since it is not claiming to be complete, see e.g. (Arampatzis et al., 2005; Römer and Mattern, 2004; Zheng and Jamalipour, 2009; Sohraby et al., 2007) for further surveys of applications.

Battlefield surveillance Surveillance systems as the Igloo White system (Correll, 2004) have been the initial starting point for WSNs and are an important application until today. For military scenarios, WSNs reach from surveillance (He et al., 2004) to target classification (Meesookho et al., 2002) and tracking (Li et al., 2002). Furthermore, other battlefield scenarios as sniper detection (Simon et al., 2004) or self-healing mind fields (Merrill et al., 2003) have been reported in literature.

Habitat monitoring and environmental research The requirements of reconnaissance in harsh battlefield environments can be compared to the civil use of WSNs for habitat monitoring and environmental research. As already mentioned, the Great Duck Island deployment by Mainwaring et al. (2002) had an impact on the research community. The observation of zebras (Juang et al., 2002) and the herding of cows (Butler et al., 2004) are further examples of WSNs used to keep track of animals. Furthermore, sensor nodes can be used to identify birds by their calls as shown by (Wang et al., 2003a,b). Not only the fauna, but also the flora has been monitored with the help of WSNs (Biagioni and Bridges, 2002). Beyond the wildlife, the environment can also be monitored, as shown in (Martinez et al., 2004) with the observation of glacier behavior.

Industrial environments With regard to the monitoring of agriculture, Burrell et al. (2004) have researched the use of WSNs in a vineyard. Transportation of food often demands a cool chain management, which also can be enhanced with the help of WSNs (Riem-Vis, 2004). Knot (2004) suggests smart barrels to improve logistics, e.g. these barrels emit a warning signal when dangerous conditions arise.

Health application The advantages of WSNs enable them to operate in harsh environments and therefore, they can be used as a rescue system for buried avalanche victims, as shown in (Michahelles et al., 2003). However, WSNs can also increase emergency and health care in less hostile environments. For instance, elderly, disabled or chronically ill people can be monitored at home, e.g. with the help of smart home offering telemedicine, as presented in (Raad and Yang, 2009). Patient monitoring systems can not only be improved at home, but also in hospitals by using WSNs (Baldus et al., 2004). Further use cases of WSNs are wellness, health and healthcare applications, which have been summarized e.g. by Dishongh and McGrath (2010).

Home automation and Smart Grid WSN-based systems can also improve comfort in everyday life, since smart homes and home automation systems benefit from being wireless and low power. The remote controlling of devices, house hold appliances or lights as well as security and safety applications are evident use cases (Gomez and Paradells, 2010). WSNs can also monitor the energy consumption of individual items and thereby they can help to conserve electrical energy (Kappler and Riegel, 2004). Smart energy and the smart grid are further application areas with large potentials (Gungor et al., 2011).

Education Even the cultural and learning experience benefits from WSNs, as they can enhance the experience in a museum (Rabaey et al., 2000) or even improve the early childhood education in kindergarten with the help of enhanced toys (Srivastava et al., 2001).

1.1.3 Challenges of the Crowded Frequency Spectrum

As the previous historical review of WSNs showed, many initial problems have been sufficiently solved and WSNs currently reach the mass market, resulting in an increasing range of applications. With the increasing utilization of wireless communication, the required frequency channels become a key resource. The problem of integrating WSNs into different environments and its resulting coexistence with other wireless devices is an urgent research challenge. Zhou et al. (2006b) have already predicted both the omnipresence of WSNs and the crowded frequency spectrum in 2006. Due to the spectrum's limitedness, they forecast a "spectrum crisis".

The frequency spectrum is divided into bands: each band is used for different applications and underlies different restrictions by different authorities. However, the 2.4 GHz frequency band ranging from 2.4 to 2.5 GHz, is license-free available worldwide for Industrial, Scientific and Medical (ISM) applications. Therefore, this band is used by many different technologies and among other IEEE 802.15.4-based WSNs, IEEE 802.11-based WLANs and Bluetooth communicate within it. Additionally, further electric appliances as microwave ovens radiate in this frequency band.

In this work, these common sources of RF waves are researched as the main interferers of IEEE Standard 802.15.4, which mostly operates at this frequency. Although these technologies are discussed in detail later, Figure 1.2 gives a first impression of the situation in the 2.4 GHz frequency band. The figure illustrates that WLANs alone allocate a large part of the wireless spectrum. Although there is another frequency band available for some WLAN standards, most WLANs operate at 2.4 GHz. In a recent IEEE presentation, Hart (2013) refers to the 2.4 GHz frequency band as a junk band, since it hosts "[t]oo much [IEEE 802.11] traffic, too many Bluetooth devices/Zigbee devices" and demands a renewal (mainly by changing the IEEE 802.11 Standards). However, the problem of the crowded spectrum is even more dramatic for the low energy IEEE 802.15.4-based devices and waiting for a less interfering version of IEEE 802.11 cannot be regarded as an option. Bluetooth has 79 narrow channels, between which it changes after each packet. Therefore, it is not interfering with a single frequency, but affecting all frequencies. Microwave ovens can be regarded as another source of interference, since they emit waves and thereby interfere with the 2.4 GHz frequency band. Due to their heavy, though steady interference, they are comparable to analog devices as 2.4 GHz radar motion or proximity sensors, microphones or wireless audio/video equipment.

1.1.4 Provisional Solution to the Crowded Frequency Spectrum

The crowded frequency spectrum can be regarded as a major challenge which is an open research question widely discussed in literature.

WLANs are omnipresent and often configured according to a rule of thumb: the WLANs do not interfere with each other when WLAN channels 1, 6 and 11 are used. This rule leaves WSN channels 15, 20, 25 and 26 less or not interfered with by WLAN, since they are within the guard bands of the WLAN channels. Therefore, these WSN channels are the best choices for IEEE 802.15.4. This channel alignment is shown in Figure 1.2 in light gray.

Since WSN channel 26 is as far away as possible from a used WLAN channel, using this channel is the common solution for WSNs. Channel 26 is also pre-set in the two main WSN operating systems (TinyOS and ContikiOS). However, these channel patterns are based on North American frequency band restrictions.

In Europe, the situation is different, since two additional channels (12, 13) are available. In practice, WLAN devices used in Europe frequently use the North American channel alignment due to compatibility reasons, but they are not restricted to it. In Europe, the ideal WLAN channels are 1, 7 and 13 to provide the least inter-WLAN interference. Consequently, WSN channels 15,

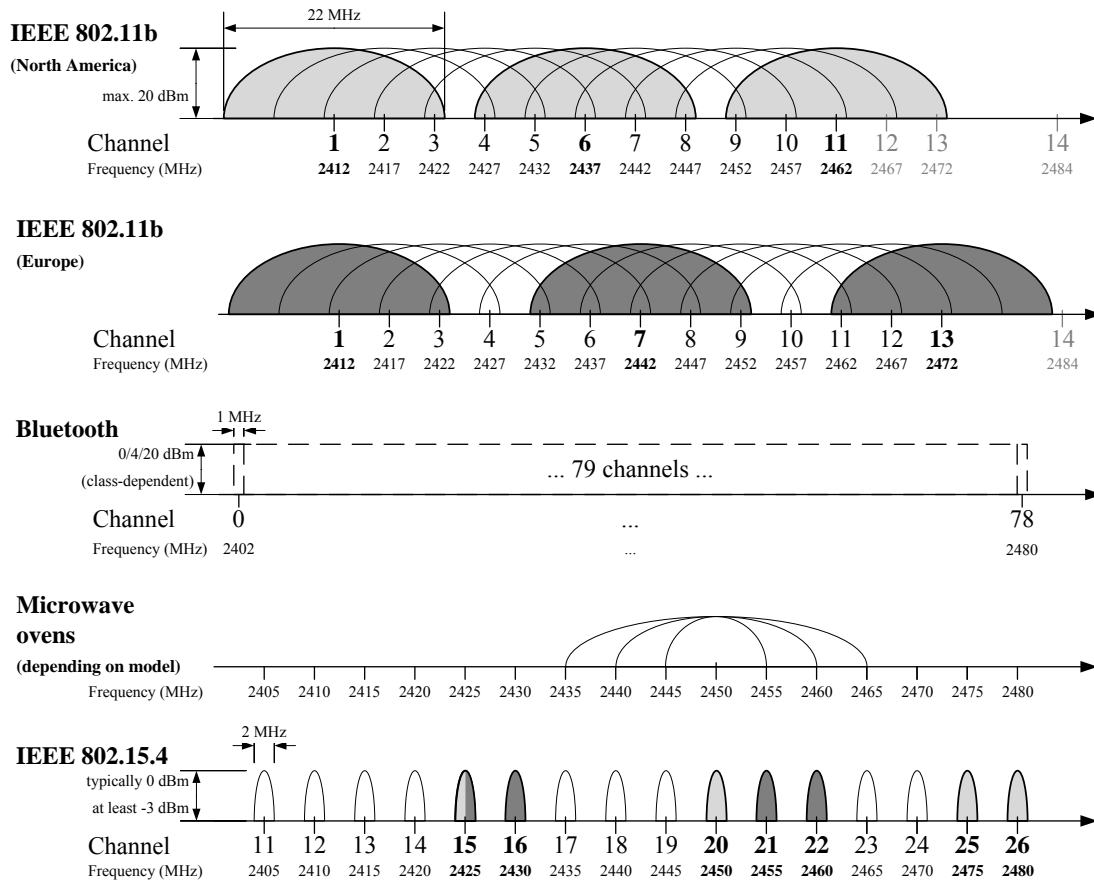


Figure 1.2: Overview of the 2.4 GHz frequency band as used by different technologies. Bold channels are the most frequently used ones: for IEEE 802.11 the non-overlapping (orthogonal) channels are used to achieve maximum WLAN performance without inter-WLAN interference. This leaves some IEEE 802.15.4 channels in the guard bands as less interfered channels and therefore they are the best choice for IEEE 802.15.4 (channel alignment). The channel widths are an approximation of the bandwidth of the signals. The channel powers refer to the full channel. Do not scale spectral mask or output power from this drawing.

16, 21 and 22 are left uninterfered with, as shown in Figure 1.2 in dark gray. Hence, the default WSN channel 26 is interfered with by a WLAN operating on WLAN channel 13.

Furthermore, the channels, which seem to be uninterfered due to the channel alignment of IEEE 802.11, can be interfered with by out-of-band energy. As explained later in this work, the out-of-band energy relates to the distance between interferer and victim device. Therefore, the problem of interference accumulates when IEEE 802.11 and IEEE 802.15.4 operate in close proximity or even inside a single device.

Besides the interference caused by IEEE 802.11-based WLANs, there are further sources of interference that potentially interfere with at other frequencies. Bluetooth and microwave ovens are shown in Figure 1.2, additionally there are proprietary wireless devices that could use ranges of the frequency spectrum. Furthermore, multiple WSNs using channel 26 could result in inter-WSN interference. To date, most WSNs occupy the channel only shortly due to power conserving reasons, but some future applications can result in high channel utilization.

Finally, the interference between different technologies is currently only solved by using IEEE 802.15.4 channel 26, which can be regarded as an unreliable and provisional solution. This state does not only lead to an urgent research problem, but can also be considered as a main motivation of this thesis.

1.2 Research Objectives

This work aims to research external interference affecting IEEE 802.15.4 in the 2.4 GHz frequency band in an urban environment. Therefore, both the technical background of the involved technologies and the understanding of their coexistence are of interest in this thesis. By applying this knowledge, a further objective is accomplished, which is the development of an improved WSN Medium Access Control (MAC) protocol that can be used to mitigate the effects of external interference.

This research project is not only achieved by the extensive theoretical analysis and review of literature, but also with the help of experiments and prototype implementations as proof of concepts. The three main aims of this work are:

1. **to review, research and model the effects of external interference on IEEE 802.15.4**, which includes an investigation of the following aspects:
 - IEEE 802.11-based WLANs, Bluetooth and microwave ovens as sources of interference
 - the two lowest Open Systems Interconnection (OSI) Reference Model Layers (Physical (PHY) Layer and MAC Sublayer)
2. **to enable the detection and further classification of interference with the help of standard-compliant off-the-shelf hardware**, focusing on:
 - the possibilities of IEEE 802.15.4-conform CCA requests for interference detection
 - the classification of external sources of interference with the help of their energy signatures as measured by Clear Channel Assessment (CCA) requests
3. **to overcome the effects of external interference**, with the help of:
 - the application of target-oriented mitigation strategies that are suitable for the individual class of interference

The just mentioned aims are fulfilled by the means of:

1. This thesis provides a comprehensive, detailed study of the **effects of external interference** on IEEE 802.15.4.
2. The **classification of external interference** with the help of the CCA request is developed.
3. Interference **mitigation strategies** are evaluated and included together with the interference classification into Interference-Aware, Self-Adapting (IASA) MAC.

At the end of this thesis, in Section 8.1, the contributions made and thereby the accomplishments of the research objectives are discussed further.

1.3 Thesis Structure

Chapter 2 provides an insight into the technical background of all involved technologies. Since this work focuses on IEEE 802.15.4, it is explained in extended detail, particularly with regard to the two lowest layers of the OSI Reference Model. The analysis of the MAC Sublayer allows estimating the timing and durations of the channel access of IEEE 802.15.4. By referring to the telecommunications engineering background of the PHY Layer, the coexistence in the RF spectrum becomes more transparent. Furthermore, WLANs, Bluetooth and microwave ovens are introduced in this chapter.

Chapter 3 explains the research methodology of this thesis. The hardware and software used for the experimental work are introduced. Since the hardware of the sensor nodes are a key component of the experiments of this thesis, they are extensively evaluated. Concerning its possibilities, different uses are shown beyond the intended communication (i.e. spectrum monitoring and interference emulation) enabled by special software.

After giving the initial background knowledge and clarifying the methodology, the problem of external interference is analyzed in **Chapter 4** with a focus on the interference effects on IEEE 802.15.4. After a review of the literature, the possibilities of modeling the effects of interference are described. A simple yet sufficient modeling approach, which is used throughout this work, is exemplarily explained and evaluated. The different interferer technologies are also analyzed in order to investigate their interference potentials.

In **Chapter 5**, the findings of the previous chapter are used to develop an algorithm to classify the source of external interference. The algorithm uses a CCA request to sample the channel for a second or less without changing it and thereby, the sensor node is not losing connection to its network. This classification algorithm is compared to previously suggested approaches in the literature and finally, it is extensively tested. It enables the sensor nodes to gain insight into their RF environments and thereby to purposefully address certain sources of external interference.

Chapter 6 analyzes the possible interference mitigation strategies and their efficiency against the different sources of external interference. Channel agility is identified to be the most efficient strategy to avoid WLAN interference. Bluetooth interference shows little effects and therefore additional interference mitigation strategies are not justified since they lead to additional overhead. The steady interference pattern of microwave ovens can be overcome with the help of scheduled packets.

In **Chapter 7**, the knowledge about the active interferer gained by the classification algorithm is combined with the most efficient interference mitigation strategy for the particular source of interference. This leads to IASA MAC, whose implementation in ContikiOS is described and discussed. Finally, IASA MAC is presented as a combination of the interference classification algorithm (Chapter 5) and chosen mitigation strategies (Chapter 6) to successfully overcome the effects of external interference (Chapter 4).

In conclusion, **Chapter 8** highlights the contributions made and gives an outlook on possible future work to extend this thesis.

Chapter 2

Technical Background

This chapter looks at the technical fundamentals of the different wave emitting technologies, which are essential for the understanding of the later work.

Firstly, general tasks and concepts of Medium Access Control (MAC) Sublayer and Physical (PHY) Layer are discussed, since the IEEE Standards of the 802 family describe the MAC Sublayer and the PHY Layer in compliance with the Open Systems Interconnection (OSI) Reference Model (Zimmermann, 1980). Secondly, the main technology investigated in this work, IEEE 802.15.4, is reviewed in detail from the higher layers down to the principles of the PHY Layer. For the interfering technologies, namely IEEE 802.11, Bluetooth and microwave ovens, a general overview of their applications is provided. Furthermore, the timing of the channel access and the basic functions of the wave radiation are introduced.

2.1 MAC Sublayer

The MAC Sublayer plays an important role on the timing of the channel access.

The main task of the MAC, as its name suggests, is to control the access to the medium, which is shared among different communication partners. Thereby, collisions are avoided and a fair distribution of the network access is organized. It is often assumed that only communication partners of the same system use a channel, thus external interference is not taken into account. As a simple basic assumption for a single communication device, the channel is busy during the transmission time. During this time span, which is often referred to as the airtime of a packet¹, the actual frequency is physically used. The channel is idle or free between the transmission end time and the start of the next transmission. These basic principles of the channel access are shown in Figure 2.1a. If two wireless devices in range of each other use the same or an overlapping channel at the same time, a collision (or what is commonly known as interference) occurs.

Furthermore, the use of a radio for communication often implies that the sender cannot listen to the channel while sending. This limitation is called half duplex. This means that the sender cannot realize a collision, because it cannot receive its own sent message. To avoid these unseen collisions so-called Collision Avoidance (CA) is applied, which is a Listen Before Talk method. Thus, the medium is checked to be idle before a message is sent. If the node can hear its sent packet to be collision-free, which is the case in wired networks, the radio supports full duplex and there is no need for CA, but Collision Detection (CD) can be used.

Nevertheless, due to the limited range of radio waves, the sender might not be fully aware of the status of the receiver. This can lead to the hidden node problem, which is illustrated in Figure

¹The term packet is used here for the Physical Protocol Data Unit (PPDU) as in IEEE Standards. Therefore, it is not strictly referring to the Network Layer of the OSI Reference Model (Zimmermann, 1980) and can also refer to a MAC frame.

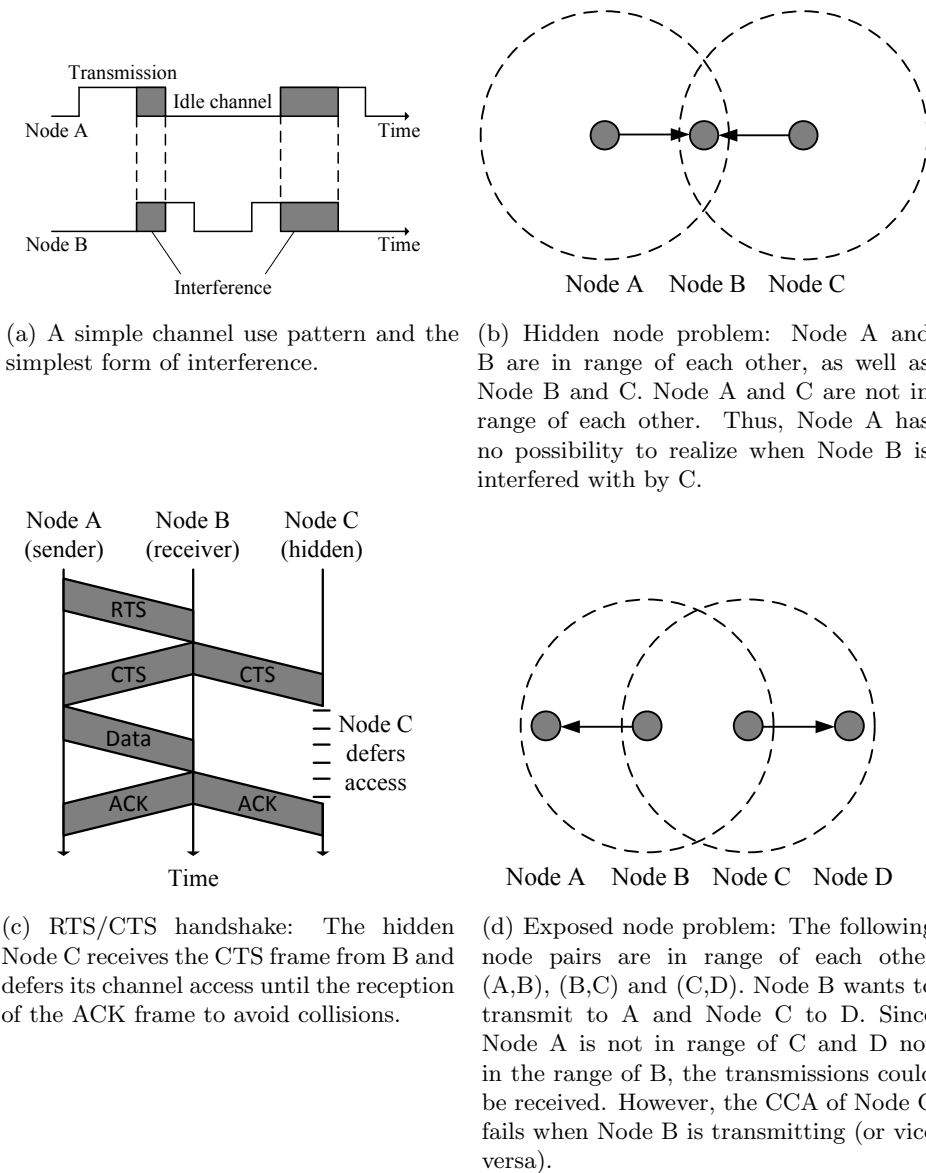


Figure 2.1: Basic tasks and problems of wireless MACs.

2.1b for a simplistic disk model of the communication range and is described in the following. If a sender node A wants to send to a receiver node B within its range, it will check the channel to be free with the help of a Clear Channel Assessment (CCA) before starting the transmission. However, since the receiver might be the target of a transmission of further away node C, the status of the intended receiver B might be hidden to the sender A. An early description of the hidden node problem including a suggested solution with the help of a busy tone sent over an additional (out-off-band) channel can be found in (Tobagi and Kleinrock, 1975).

To overcome this problem Request To Send (RTS) and Clear To Send (CTS) messages can be used to assure that the receiving node is not interfered with by a hidden node (Karn, 1990). The flow and function of the so-called RTS/CTS handshake are shown in Figure 2.1c. In addition to the just mentioned handshakes, short time durations between transmissions remain due to switching and processing times. The RTS/CTS handshake is not only a possible solution to avoid collisions due to the hidden node problem in networks with random medium access, it also addresses the problem of exposed nodes. The exposed node problem is caused by an oversensitive CCA (false positive CCA backoff), as shown in Figure 2.1d (Karn, 1990). Later in this work, this problem is of interest, although not in the classical version of contention, but in the form of sender-side

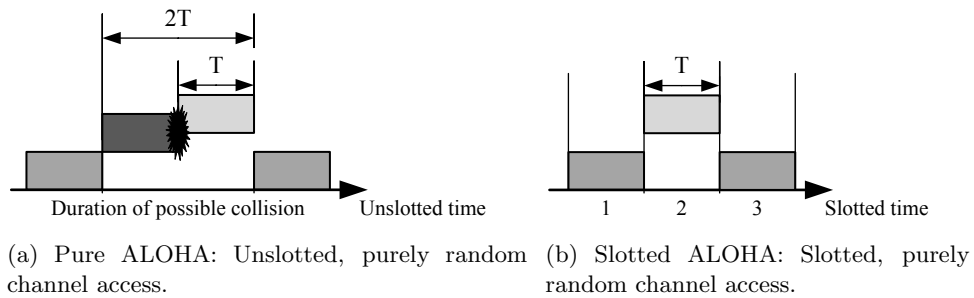


Figure 2.2: Collision risk duration for slotted and unslotted ALOHA/purely random channel access.

interference. There are further strategies to avoid the hidden and exposed node problems. However, even without range problems, collision resolution has to be organized in a network. Some possible fundamental protocols are introduced in the following.

2.1.1 Multiple Access Protocols

According to Tanenbaum and Wetherall (2011), popular multiple access protocols can be roughly classified as follows. The first group of protocols contains fully random access protocols and therefore these protocols are contention-based, i.e. there is competition for the medium. These protocols are normally simple to implement and do not need a hierarchy or central management. The second group includes scheduled or reservation-based protocols. While there is no competition and it is thus possible to predict timing, these protocols are more complex and need coordination and therefore they are harder to scale.

Random Access

For random access protocols two popular representatives, ALOHA and Carrier Sense Multiple Access (CSMA), are introduced. For each of them different versions are given. Furthermore, a general method to compare the throughput is introduced in the following.

ALOHA Aloha is a very basic protocol from the beginning of networking and there are two main versions of it.

Pure ALOHA (Abramson, 1970) is the simpler version of them. A node sends whenever it wants. If a collision occurs, it waits for a random time span before it retries.

Slotted ALOHA (Abramson, 1973) is an improvement of Pure ALOHA with a smaller collision probability. The channel is organized in discrete time slots, which are synchronized for all nodes in the network. A sender is only allowed to transmit at the beginning of such a time slot.

In the following the improved throughput of a slotted medium access is compared to an unslotted medium access and they are mathematically reviewed with the help of a traffic model. This understanding is vital since the concept of slotting can be used by the MACs of IEEE 802.15.4 and 802.11. At the end of the section, a comparison of the throughput of different protocols is given. For the analysis here it is assumed that the airtimes of all packets are equal. Figure 2.2 gives an intuitive illustration of the chances of collisions for the unslotted and slotted case of ALOHA. It can be seen that the probability of a collision halves when the channel is slotted. According to Tanenbaum and Wetherall (2011) and based on the work of Abramson (1970) and Abramson (1973) the probability of a collision can be computed with the help of a traffic model as follows.

A channel access is defined by the frame time T , which is equal for all frames. Furthermore, the generation of frames is assumed to be Poisson distributed with G being the mean number of frames per time unit. A Poisson distribution is a good fit for a network with many nodes, where

each node is independent (the transmissions of the nodes are equal to an infinite series of Bernoulli experiments).

For unslotted ALOHA the risk of a collision persists for two frame durations ($2T$). Since a frame can only be transmitted uninterfered if no other frame (with an airtime of T) is already being transmitted (still using the channel) and no other frame transmission starts within the transmission duration (T). These two cases are shown in Figure 2.2a. The Poisson distributed traffic is described as

$$Pr(k) = \frac{G^k e^{-G}}{k!} \quad (2.1)$$

for the probability Pr that k frames are tried to transmit. The expected mean G is

$$G = g \times w \quad (2.2)$$

where g is the mean rate of events per time unit and w the observed interval in time units to describe the distribution. For unslotted ALOHA the observed interval lasts for $2T$, as this duration is needed as shown in Figure 2.2a. The event rate is 1 and therefore the expected mean G is:

$$G = 1 \times 2G \quad (2.3)$$

Consequently, the probability that no collisions ($k = 0$) occur within a time span of $2T$ is:

$$Pr_{2G}(0) = \frac{(2G)^0 e^{-(2G)}}{0!} = e^{-2G} \quad (2.4)$$

Using the probability of a frame collision, the throughput S can be computed as $S = G \times Pr(0)$, resulting in

$$S = G \times e^{-2G} \quad (2.5)$$

With the help of the first derivation, the maximum of the throughput function $S(G)$ of the unslotted ALOHA protocol can be calculated as:

$$S_{\max}^{\text{unslotted}}(G = \frac{1}{2}) = \frac{1}{2e} \approx 0.184 \quad (2.6)$$

For slotted ALOHA, which has a lower risk due to a potential collision duration of only T , the maximum throughput can be computed the same way resulting in:

$$S_{\max}^{\text{slotted}}(G = 1) = \frac{1}{e} \approx 0.368 \quad (2.7)$$

In general, if the traffic is low (little chance of collision), the throughput is related to the traffic. But when the traffic is high, the throughput is much less than the traffic and converges to zero. Hence, ALOHA does not scale well. The throughput versus the traffic graphs of the two ALOHA versions and other protocols are shown in Figure 2.3. It can be clearly seen that the pure ALOHA curve $S = G \times e^{-2G}$ has its maximum throughput of ≈ 0.184 at $G = \frac{1}{2}$ and that the slotted ALOHA performs better with its maximum being double as high as for pure ALOHA at $G = 1$.

CSMA While ALOHA is only efficient in small networks with light traffic, the CSMA approach scales better than ALOHA and is widely used today. The main improvement is the so-called Listen Before Talk approach. This approach goes back to the aviation radio communication and in the context of packet-based computer networks, it is applied in the form of sensing (listening to) the channel before a transmission (talk) (Kleinrock and Tobagi, 1975).

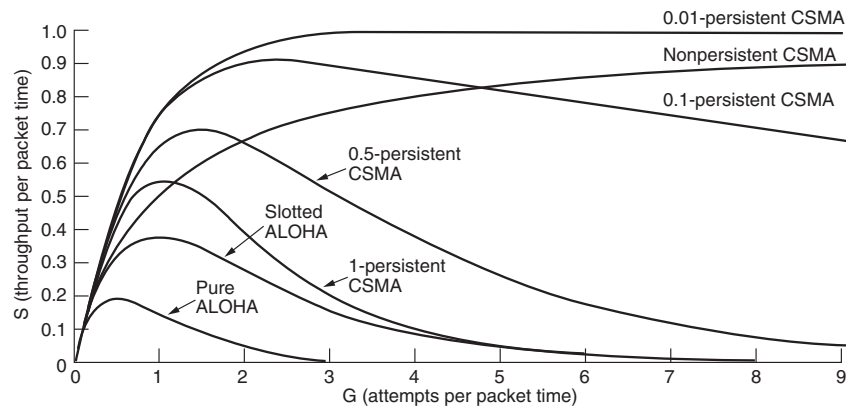


Figure 2.3: Throughput versus traffic for the most common random access protocols. Taken from (Tanenbaum and Wetherall, 2011).

The first variation of CSMA is 1-persistent CSMA. The sender checks the channel until the channel is free and sends immediately. In case of a collision, the procedure is restarted after a random delay.

The improved variation of 1-persistent CSMA is the nonpersistent CSMA. If the sender finds the channel to be free, it sends immediately. If the channel is used, the sender waits for a random period before trying to access it again. Due to this behavior, nonpersistent CSMA is less greedy than 1-persistent CSMA. When packets collide, the sender restarts the sending process after a random delay. Since this approach is less greedy, it results in longer delays, but has a better channel utilization than 1-persistent CSMA.

As for the ALOHA protocol, there is also a slotted version of CSMA. For a slotted channel p -persistent CSMA can be used. If the sender has a free channel, it immediately sends with probability p and with $1 - p$ it defers its transmission until the next slot. If the channel is not free or a collision has taken place, it waits for a random duration and restarts the process. The p -persistent CSMA (Kleinrock and Tobagi, 1975) is the base for the most commonly used MACs of the standards IEEE 802.11 (Distributed Coordination Function (DCF)) and IEEE 802.15.4 (beacon-enabled without guaranteed time slots).

Based on the same throughput computation as explained for ALOHA, a comparison of the throughput of all random access protocols introduced in this section is shown in Figure 2.3. A more detailed discussion of these protocols can be found in (Kleinrock and Tobagi, 1975) or in more recent literature from today's viewpoint, e.g. in (Tanenbaum and Wetherall, 2011).

The just presented CSMA protocol is not used in wireless systems. Due to the half duplex character of wireless communication, collisions are not as easy to be identified as it is assumed for ALOHA and CSMA here. In wireless application the CSMA/CA approach is used, which is a version of p -persistent CSMA. To be formally correct, the condition of a collision cannot be realized directly, but either a sent frame is assumed to be always received or it has to be confirmed with the help of an ACK. For the magnitude of performance as discussed here, these details are not relevant, since other factors (as the same length of all frames) are also simplifications for the modeling.

Reservation-based Access

Besides the random access protocols, there are non-random access protocols: The reservation-based protocols are basically Time Division Multiple Access (TDMA), and they are collision-free protocols.

TDMA gives a time slot to every participant of the network and the node is only allowed to transmit within its slot. This protocol is used by Bluetooth. However, this approach requires synchronization, some central management and it does not scale well, since the delays increase with every new network participant. Another, special version of TDMA is the Bit-Map protocol. The channel is organized in time slots. In an initial reservation window every node can reserve a slot to use it later. This approach is the basic idea behind the guaranteed time slots supported in IEEE 802.15.4.

Throughout this chapter, more approaches are introduced and further specific MAC details are discussed.

2.1.2 Further MAC Sublayer Tasks

Looking at the MAC Sublayer as part of the Data Link Layer, there are tasks that are not the core of the MAC, but still have to be fulfilled with the help of it. In the IEEE standards there are so-called Service Access Points (SAPs) defined and these SAPs explain all the tasks of a layer. Later the SAPs of the discussed layers are reviewed in more detail. Since there is no universal definition of all services, in this general introduction the following list of possible services of the Data Link Layer is based on Kurose and Ross (2001):

Framing: Encapsulating the data (Network Layer datagram) into a frame and decapsulating on the receiver side.

Reliable delivery: Supporting retransmissions, e.g. based on ACKs.

Flow control: Preventing sender and receiver frame buffers from overflowing and dropping frames.

Error detection: Detecting bit errors (normally this function is implemented in hardware).

Error correction: Some detected bit errors can be corrected depending on the error correction code used.

Some of the tasks just mentioned, although situated in the MAC, can be implemented in hardware. A typical example is the automated ACK for IEEE 802.15.4, which is normally implemented in the form of a MAC accelerator.

The term ACK, as used for MAC ACKs introduced in this section, is also used in higher layers, e.g. the Network Layer. However, in the higher layers ACKs are basically unicast packets that are confirmed with the help of MAC ACKs themselves. Unicast packets have a clearly addressed receiver. As illustrated in Figure 2.4, different possibilities of addressing a packet are:

Unicast delivers a message to a single specified node.

Broadcast delivers a message to all nodes in the network/range.

Multicast delivers a message to a group of nodes that have expressed interest in receiving the message.

Anycast delivers a message to any node out of a group of nodes, typically the one nearest to the sending node.

Geocast delivers a message to a group of nodes, typically identified by their geographical location or position in some sort of coordination system. Geocast is a specialized form of multicast.

These addressing schemes are mainly referred to in the context of the Network Layer for routing. Mohapatra et al. (2004) summarize the broadcast, multicast, geocast and anycast properties in

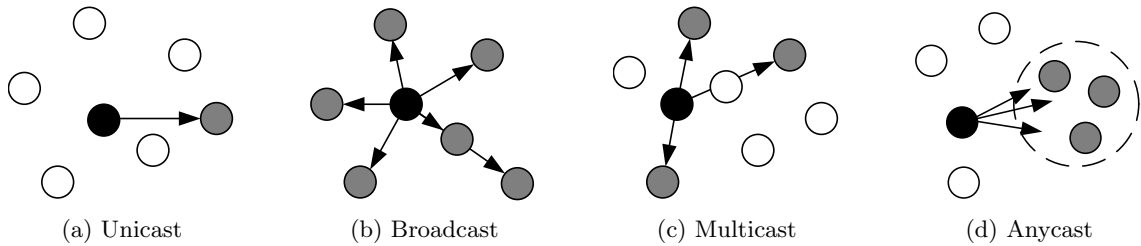


Figure 2.4: Different delivery semantics. The black node is the sender, the gray nodes are intended receivers of a packet and the white nodes are noninvolved.

Wireless Sensor Networks (WSNs) with mobile nodes. They highlight the need to include broadcast and multicast support into the MAC Sublayer.

The most commonly used delivery semantics are unicast and broadcast. Although the different implications for the routing are not of interest here, it is obvious that while a unicast message can be easily confirmed by an ACK, this is not always possible for broadcasts. Thus, IEEE 802.15.4 includes an ACK request subfield (IEEE, 2003b) and the Rime stack of ContikiOS also supports it via communication primitives (Dunkels et al., 2007). Furthermore, for cross-layer optimized WSN protocols and for sleeping cycles, the addressing in combination with the confirmation due to ACKs can play an important role. It is vital to conserve energy for WSNs devices and therefore the radio is often duty cycled, i.e. turned off for most of the time. This is normally controlled by the MAC and adds extra complexity. This is often referred to as Low Duty Cycle MAC (e.g. in (Ahmad et al., 2011)) and the resulting implications will be researched later in more detail.

2.2 Physical Layer

The PHY Layer defines the modulation and other factors of the transmission that influence the interference signal strength and the spectral overlap on the interferer side. On the victim side, features of the Radio Frequency (RF) receiver, which are also described in the PHY Layer, are of interest. The PHY Layer is mostly embedded into the hardware and represents the physical communication process.

Although this work does not focus on RF telecommunication engineering, Figure 2.5 gives a short overview of the meaning of the typical radio features. The transmitter properties are more complex than they are presented in the often used simple channel model shown in Figure 1.2, where they are defined by a center frequency in the middle between two limits. Also the center frequency is not always identical to the carrier frequency of the modulation. For instance, Orthogonal Frequency-Division Multiplexing (OFDM) utilizes multiple sub-carriers. Thus, the center frequency f_c is the center of the Power Spectral Density (PSD) of the signal. The PSD is the power in the spectrum related to frequencies. Figure 2.5a illustrates the signal that is emitted by a transmitter. Looking at the spectrum of the signal, the bandwidth of a signal, which is frequently used synonymously to the channel width, can in fact be defined in many ways. Farahani (2008) gives three possible bandwidth definitions: the 3 dB² bandwidth (frequency interval between the 3dB corners), the null-to-null bandwidth (nulls in the PSD as interval limits) and the 99% bandwidth (frequency band containing 99% of the signal power).

Figure 2.5b shows the receiver and how it addresses out-of-band energy with adjacent/alternate channel rejection. Alternatively, the term selectivity can be used synonymously with rejection.

For the sake of completeness, co-channel rejection has to be mentioned as well, since modern, digital modulations can overlap in the spectrum, but do not necessarily add up to a single wrong signal. Thus, two concurrent transmissions in equal range do not lead to a higher Received Signal

²See Appendix A for details about the dB unit.

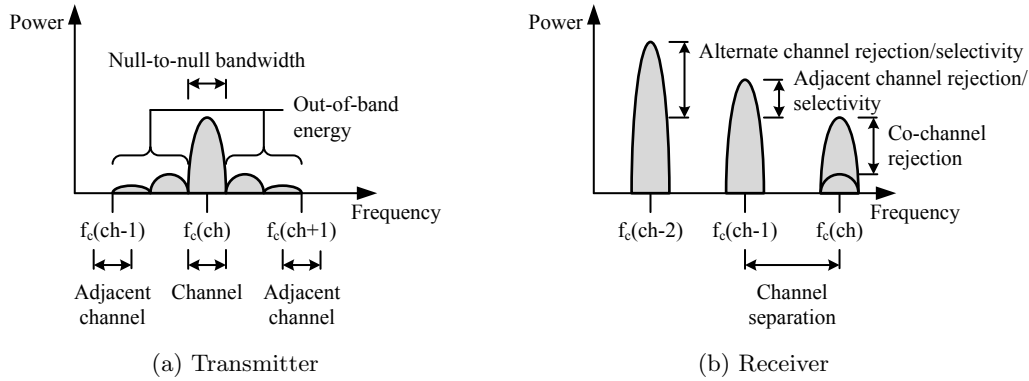


Figure 2.5: Overview of the RF features of wireless transmitters and receivers in the spectrum. The channel ch contains all the frequencies around a center frequency f_c within a certain bandwidth. The out-of-band energy of a transmitter can affect nearby channels and the robustness against this energy is known as alternative/adjacent channel rejection. Figures based on (Grini, 2006).

Strength Indication (RSSI) value. Normally the maximum of both signals will be measured, as mentioned for the Handy Mote in (Boano et al., 2011b).

2.3 IEEE 802.15.4

IEEE Standard 802.15.4-based radio chips are low power communication solutions, which are suitable for Wireless Personal Area Networks (WPANs) and WSNs. However, in contrast to most other wireless communication technologies, the idea behind IEEE 802.15.4 was to deliver an “application enabler” instead of a feature or an application (Gutiérrez et al., 2004). While IEEE 802.11 and Digital Enhanced Cordless Telecommunications (DECT) only enabled already existing technologies as Local Area Networks (LANs) and telephones to be wireless, IEEE 802.15.4 makes novel applications possible that would have been too expensive or too complex when based on wires. Gutiérrez et al. (2004) name, among others, the following two examples as use cases: individually remote controllable light bulbs, which would be too expensive when realized with wires, and a wireless tire pressure measurement system in the automotive sector, where a wired approach would be too complex due to the rotation. Wired sensor networks with a large number of nodes are not feasible, thus IEEE 802.15.4 can also be seen as an enabler for WSNs.

The initial IEEE Standard 802.15.4 (IEEE, 2003b) was published originally in 2003. In 2006 (IEEE, 2006) it was updated and then in 2011 a second update has been released (IEEE, 2011b). The standard defines the MAC Sublayer and the PHY Layer, which are researched in detail in corresponding subsections later.

Radios based on IEEE 802.15.4 are also referred to as ZigBee radios, since ZigBee is based on the IEEE 802.15.4 version of 2003 and as a brand name, ZigBee has a higher publicity and is therefore used to advertise the radios.

Due to its simplicity, the initial 2003 version of the standard is widely used today, while the latest amendments are rarely present in real world deployments. In the following, network stacks that are based on IEEE 802.15.4 are presented.

2.3.1 Protocol Stacks and Higher Layers

IEEE 802.15.4 offers some of the least power-consuming radios and therefore forms the base for many network technologies. These technologies, with some of them being only recently presented, offer different applications ranging from home and end user to industrial scenarios.

using a CSMA-CA mechanism. Its responsibilities may also include transmitting beacon frames, synchronization, and providing a reliable transmission mechanism. A complete description of the IEEE 802.15.4-2003 MAC sublayer can be found in [B1].

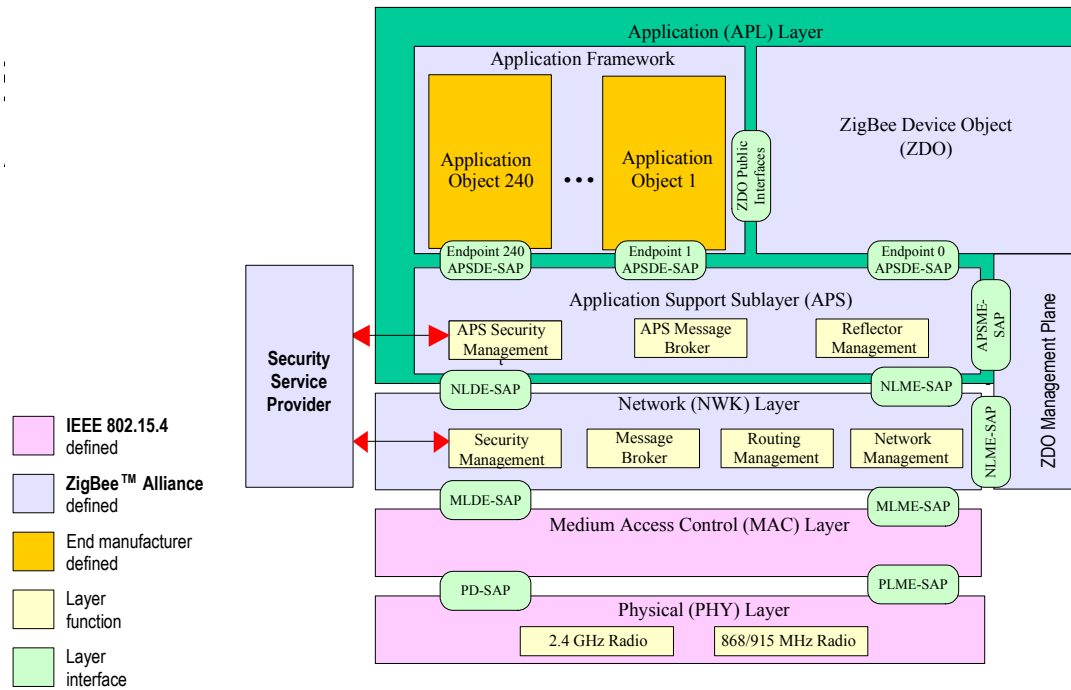


Figure 2.6: **Figure 1.11** the Outline of the ZigBee Stack Architecture. The Application and the Network Layer of ZigBee sit on top of the MAC and PHY Layer of IEEE 802.15.4. The communication between the layers is organized through services, which are defined in the SAPs. Taken from (ZigBee Alliance, 2008b). Copyright © 2007 ZigBee Standards Organization. All rights reserved.

ZigBee

ZigBee is the most prominent protocol stack building on IEEE 802.15.4. This suite of high level communication protocols offers an Application and Network Layer, further it provides security options in the form of a Security Service Provider. Figure 2.6 gives an overview of the architecture of ZigBee and how ZigBee and IEEE 802.15.4 are connected. The connection points, called SAPs as in the IEEE standards, are defined interfaces for each layer offering and accepting different services. Since in this work ZigBee is only covered as a potential application based on IEEE 802.15.4, most of the different services are not discussed further. However, some of the services offered by IEEE 802.15.4, which are used by ZigBee, are discussed later in this section in detail.

ZigBee is maintained by the ZigBee Alliance, which is an industry consortium (ZigBee Alliance, accessed 10 September 2010), and has versions released in 2004, 2006 and 2007. However, all versions are included in the latest standard or as officially called ZigBee specification (ZigBee Alliance, 2008b). The latest version also introduced what is commonly called ZigBee-PRO (ZigBee Alliance, 2008a). ZigBee-PRO offers significantly more features than ordinary ZigBee and makes the standard also more interesting for WSNs.

The MAC of IEEE 802.15.4, which is discussed in Section 2.3.2, offers star and peer-to-peer topologies, with the latter intended as part of a mesh network. These network topologies are built of Full Function Devices (FFDs) and Reduced Function Devices (RFDs). ZigBee goes a step further and provides star, tree and mesh networks built of three different device classes. These three types of devices are:

ZigBee Coordinators are the most powerful devices, which maintain and coordinate the network with overall network knowledge.

ZigBee Routers work as routers in the network by passing on data.

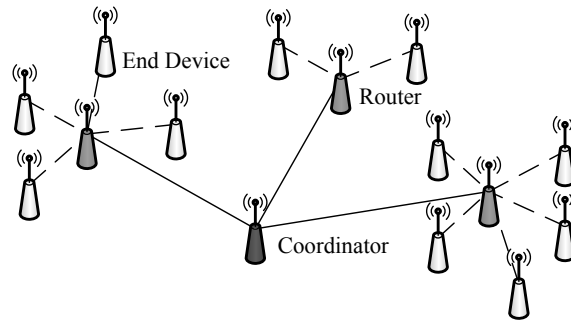


Figure 2.7: ZigBee tree network topology. ZigBee End Devices with limited functionalities send their data to ZigBee Routers, which forward the data to the ZigBee Coordinator, the device that finally maintains the network structure.

ZigBee End Devices have only limited functionalities to save costs and complexity. They just report to their parent nodes.

Figure 2.7 gives an overview of the topology in a ZigBee tree network. Furthermore, a star and mesh network topology is supported by ZigBee. Besides the topology, ZigBee provides two network modes, which are provided by IEEE 802.15.4: a non-beacon CSMA mode and a beacon-enabled mode with guaranteed time slots.

Despite all the features and the big benefit of interoperability, for most WSNs reported in research literature ZigBee is not used, which might be due to the complex specifications, the given profiles and the organization of the ZigBee Alliance.

WirelessHART

A less known stack building on IEEE 802.15.4 is WirelessHighway Addressable Remote Transducer (HART) (HART Communication Foundation, last accessed April 2014). It is the extension of the HART protocol that is used for wired communication in industry.

As it targets control tasks, coexistence is a topic for WirelessHART. Johnston et al. (2010) touch the coexistence issue and give the features to mitigate interference used in WirelessHART or IEEE 802.15.4 as its base:

- mesh networking to support large areas with low transmit power,
- blacklisting and channel assessment,
- channel hopping,
- TDMA,
- power modulation, and
- Direct-Sequence Spread Spectrum (DSSS).

ISA 100 Wireless

International Society of Automation (ISA) 100 Wireless or ISA 100.11a has a similar target scenario compared to WirelessHART, which also targets at industrial automation (ISA 100 Wireless Compliance Institute, last accessed April 2014). On the higher layers, ISA 100 Wireless allows tunneling of different protocols as Fieldbus Foundation, HART, Profibus and others. However, the coexistence strategies are similar to WirelessHART, as expected due to the shared IEEE 802.15.4 foundation. The following strategies are stated in (ISA, 2008):

- adaptive frequency hopping with channel blacklisting,
- short messages,
- listen before talk,
- low duty cycle, and
- low power operation.

Because of the same physical transmission technology, the modulation and DSSS are also implied, although not mentioned in the document.

MiWi

The company Microchip provides the MiWi Wireless Networking Protocol Stack on top of IEEE 802.15.4 (Microchip Inc., last accessed July 2013). It was developed with simpler networks than ZigBee in mind. According to its application node (Flowers and Yang, 2010), it supports up to 1024 nodes with the help of eight coordinators, each able to have 127 children. A packet can be routed over four hops in the network and two hops from the Personal Area Network (PAN) coordinator. With a device hierarchy similar to ZigBee, MiWi supports PAN Coordinator, Coordinator and End Devices.

6LoWPAN

The Internet Protocol version 6 over Low power Wireless Personal Area Networks (6LoWPAN) working group is part of the Internet Engineering Task Force (IETF) and has the aim to extend the Internet Protocol (IP)-based Internet to small, battery powered devices. This idea is commonly known as the Internet of Things. The IP is a very successful protocol with large acceptance and almost unlimited tools and services. The resulting interoperability of 6LoWPAN is a major advantage of it. However, IEEE 802.15.4 capabilities are too limited to support the IP, thus among others the following challenges have to be solved (Montenegro et al., 2007; Hui and Culler, 2008). The IPv6 frame format requires packet sizes larger than what IEEE 802.15.4 can support, thus an adaption layer is introduced. The headers are also compressed to enable IPv6 in WSNs. Furthermore, the duty cycle of the radio and the power consumption have to be solved. Nevertheless, the potential of 6LoWPAN is high and most WSN operating systems offer or support implementations of 6LoWPAN.

Active Messages in TinyOS

TinyOS (Hill et al., 2000) is a popular operating system for WSNs. As one of the first WSN operating systems, it supports more than one network stack, but its default packet format is Active Messages (von Eicken et al., 1992; Levis, 2007). For most messages a TinyOS Frame, also called T-Frame, is used (Hui et al., 2007). It is not fully compatible with the IEEE 802.15.4 MAC format. Nevertheless, TinyOS also supports IEEE 802.15.4 compatible frames and a 6LoWPAN implementation.

A unique feature of TinyOS is that it is based on Network Embedded Systems C (NESC) (Gay et al., 2003). Consequently, all programs implemented in TinyOS have to be written in NESC as well. NESC was designed especially for WSNs and optimized as such for:

- interaction with the environment,
- limited resources.
- reliability, and

- soft real-time requirements³ (Gay et al., 2003).

This led to a component-based architecture based on tasks and events. Long operations are so-called split-phase operations, which call a command and then an event is signaled when the operation is done. Thus, programming in TinyOS is comparable to designing state machines. Besides the advantages of this approach, NESC has drawbacks, including no possibilities to dynamically allocate memory and no support for function pointers. Further drawbacks are, in the opinion of the author, the steep learning curve for a single system and the lack of portability of the source code.

The Rime Communication Stack and the Chameleon Header Transformation Module in ContikiOS

Another operating system for wireless sensor nodes is ContikiOS (Dunkels et al., 2004). ContikiOS is also used for the practical parts of this work. It offers multiple network stacks and MAC Sublayer framers. It supports IPv6, with the help of the 6LoWPAN adaptation layer, and IPv4. Furthermore, there are the Rime communication stack and the Chameleon header transformation module, which support different MAC protocols suitable to save power in WSNs (Dunkels et al., 2007). The Rime stack is a set of communication primitives, including unreliable and reliable unicast and broadcast functions. The Chameleon header transformation module contains among others the header construction. See Section 7.4 for more details about the communication in ContikiOS.

ContikiOS is implemented in the C programming language. While TinyOS due to its NESC base is programmed in a state machine fashion, ContikiOS allows programming in a sequential fashion and supports dynamic memory allocation, function pointers and dynamic linking of binaries. An event-driven programming model is supported due to protothreads in ContikiOS (Dunkels et al., 2006).

Summary

Throughout this section different protocols building on IEEE 802.15.4 have been presented. This indicates the importance of IEEE 802.15.4 as a building block of many systems. Besides these already introduced technologies, there are multiple IEEE task groups that work on standards allowing the use of IEEE 802.15.4 in new scenarios (Heile, last accessed July 2013). Some of these groups develop new PHY Layers. However, other task groups have not yet decided on the PHY Layer: Task Group 4k focuses on Low Energy Critical Infrastructure Monitoring, while Task Group 4p develops a Positive Train Control system to enable communication between trains and network infrastructure for freight, passenger and rail transit (Backof, 2012). The results of the IEEE task group 802.15.4e (IEEE, 2012a), as for instance a new MAC that has improved in meeting industrial requirements, are partly included in the latest release of the IEEE 802.15.4 standard (IEEE, 2011b).

In summary of all results, the term application enabler really matches IEEE 802.15.4. Furthermore, with so many technologies using it, both the robustness of the standard and the ability to coexist are crucial.

2.3.2 MAC Sublayer

The MAC is based below the Network Layer and as its general tasks have been already mentioned in Section 2.1, for IEEE 802.15.4 there are given SAPs. There are two SAPs to the higher Network Layer as shown in Figure 2.6: data service and a management entity service. The data to send is passed with the help of the data service. The interfaces to the PHY Layer are discussed in Section

³Soft real-time systems normally reply to a request within a given time. If the deadline is not met, the system is still functional.

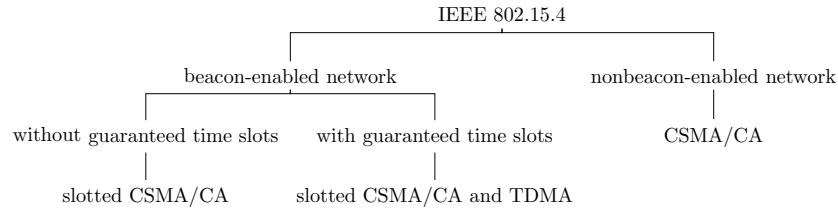


Figure 2.8: Supported MAC modes of IEEE (2003b).

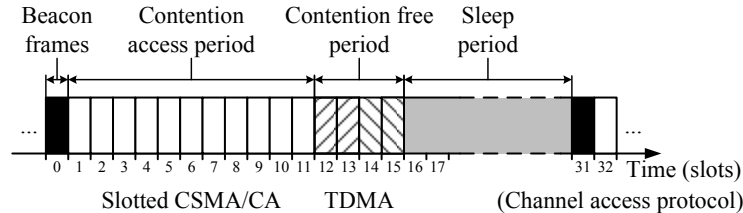


Figure 2.9: An example of a superframe structure. Between two beacon frames there are 16 time slots and an optional sleep period (for this example the beacon interval is 32 time slots, resulting in a 50% duty cycle). The first time slots after the beacon frame are distributed on contention-based access (slotted CSMA/CA). Optionally, the last slots can be accessed contention free by TDMA, after the slots have been reserved in the contention access period (IEEE, 2003b).

2.3.3. Besides the formal definition of the interfaces, the tasks of the MAC are defined as follows (IEEE, 2003b):

- beacon management including beacon transmission by the network coordinator and synchronizing the receiving nodes,
- managing the guaranteed time slots,
- channel access through the CSMA/CA algorithm,
- reliable links between nodes (ACK frames, error detection),
- supporting PAN association and disassociation, and
- supporting device security.

The different supported MAC modes of IEEE 802.15.4 are introduced in the following in order to enhance the understanding of these tasks. The relation between the different modes is shown in Figure 2.8. For a star topology, IEEE 802.15.4 supports a beacon-enabled network mode. Due to the beacons sent by the coordinator, an increased level of coordination in the network is achieved. Furthermore, the chances of packet collisions are reduced by using a slotted CSMA/CA (for an explanation of the increase in performance of slotted over unslotted channels see Section 2.1.1). In a beacon-enabled IEEE 802.15.4 network, the time between two beacons is split into 16 slots. The first slot is used by the beacon frame itself. Besides the slots, there can be a sleep phase after the last slot and before the next beacon frame. Thereby the radios can be duty cycled to save energy, e.g. the time between two beacon frames can be twice as long as the duration of the 16 slots of the contention access period. This flow and the slot structure are also referred to as superframe structure. Additionally to the slotting, guaranteed time slots can be supported. The nodes can reserve one of up to seven guaranteed time slots that follow the time slots of the contention access phase. Hence, after a period of slotted CSMA/CA a TDMA period can follow. The concept is summarized in Figure 2.9.

However, the superframe structure is only supported for star topologies. WSNs normally use multi-hopping and mesh-networking, for which IEEE 802.15.4 offers the peer-to-peer topology.

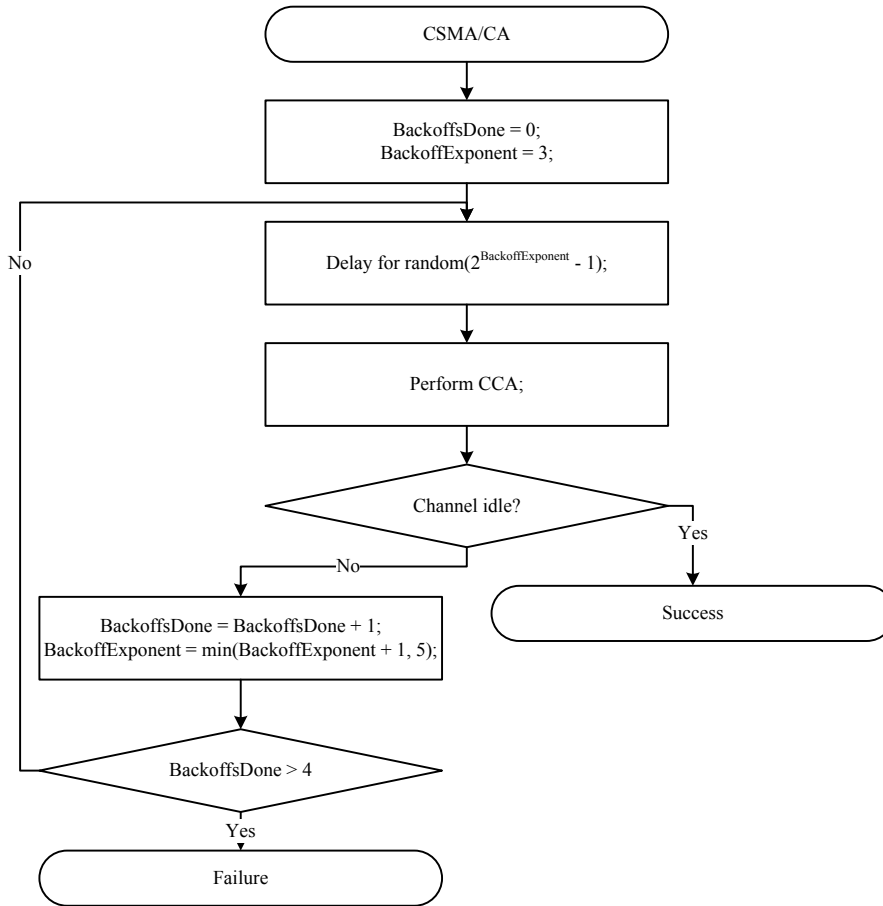


Figure 2.10: CSMA/CA for unslotted IEEE 802.15.4 network according to (IEEE, 2003b). Default values used for variable conditions.

Thus, the advantages of a low collision probability and sleep phases do not apply for WSNs, since IEEE 802.15.4 provides an unslotted CSMA/CA algorithm for nonbeacon-enabled networks.

This simple CSMA/CA algorithm is shown in Figure 2.10. The first network access attempt is delayed for a random period to have a less greedy channel access. After the delay, the channel is checked to be idle. If so, the packet can be sent. If not, the process is repeated with the possibility of a longer delay. When multiple repeats fail, the whole CSMA/CA algorithm fails. The details of the CCA request used to monitor the channel before sending are discussed later in Section 2.3.3. The exact timing is not given here in this overview of the standard, but it will be discussed in detail, when the efficiency of CSMA/CA against interference is researched in Section 6.3.3.

Despite the modes offered by IEEE 802.15.4, there is an enormous number of alternative and not standard-conform MACs for WSNs based on IEEE 802.15.4-compliant radios. In the recent literature, many different WSN MACs have been suggested, discussed and tested, see e.g. (Demirkol et al., 2006; Kredo II and Mohapatra, 2007; Roy and Sarma, 2010; Ahmad et al., 2011) for an overview. As already mentioned in Section 2.3.1, the two most popular operating systems for WSNs in the research domain, TinyOS and ContikiOS, support their own communication stacks including MACs. Since the practical part of this work is implemented in ContikiOS, two approaches implemented in ContikiOS are analyzed exemplarily in the following. While all MACs discussed so far have been designed under the assumption that the radio is turned on all the time (the sleep period in the beacon-enabled network mode of IEEE 802.15.4 is only optional), low power WSN MACs are using duty cycling as a fundamental element. Idle listening is the time period of the radio being on without receiving anything and only waiting for an incoming transmission. It can be assumed for many network setups that the main energy waste is idle listening (Demirkol et al.,

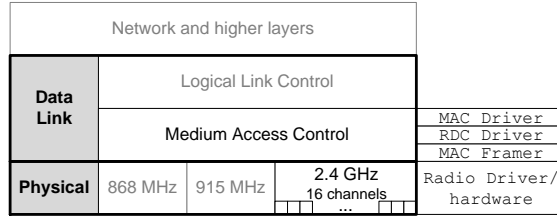


Figure 2.11: OSI Reference Model (left side) with IEEE 802.15.4-specified layers (middle) relevant for this work and the implementation details in ContikiOS (right side). Due to the low duty cycles used to save energy in WSNs, the MAC Sublayer is divided further into an access method (e.g. CSMA/CA) and an RDC part. In the ContikiOS implementation, the MAC parts are a MAC Driver and a RDC Driver, which are shown on the right of the figure.

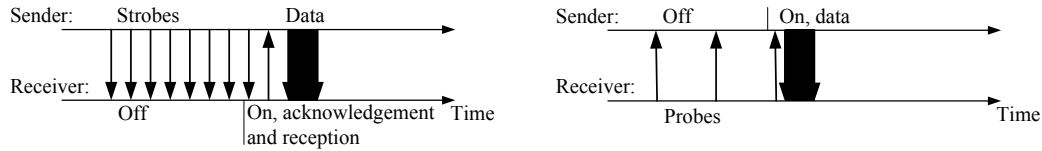
2006). Idle listening is reduced with the help of duty cycling and thereby energy is conserved due to the costs of longer transmission delays. WSN MACs are also referred to by the term Low Duty Cycle MACs (e.g. in (Ahmad et al., 2011)). The duty cycling of the radio to conserve energy is considered to be one of the main challenges. Thereby WSNs are unique compared to classical wireless networks as Wireless Local Area Networks (WLANs) where the focus is put on throughput and other performance metrics.

The implementation of the OSI Reference Model layers in ContikiOS is adapted to the special needs of WSNs and the radio duty cycling resulting in an additional, new layer compared to the OSI Reference Model. Figure 2.11 shows the OSI Reference Model and ContikiOS implementation including the adaptation for WSNs. In ContikiOS, the OSI-defined MAC Sublayer is divided into a Radio Duty Cycling (RDC) Layer and a MAC, which regulates the medium access. As the last step before handing the packet over to the PHY Layer, the MAC Framer, is positioned below the RDC Layer. The RDC Layer, as the lower part of the MAC Sublayer, manages the sleep times of the radio. This looks like an extended CCA to the MAC, since the channel is not only checked to be idle, but the transmission time is also synchronized with the radio sleeping cycle. In ContikiOS, the duty cycle of the radio is often defined by the Channel Check Rate. The MAC Sublayer Driver (e.g. CSMA/CA) on top of the RDC can initialize retransmissions when the RDC Layer indicates a busy channel or a missed ACK.

Radio Duty Cycling

As previously explained, random access protocols are dominantly used in WSNs due to their simple logic, which scales up well. In the following, two unscheduled approaches, namely X-MAC (Buettner et al., 2006) and Low Power Probing (LPP) (Musaloiu-E. et al., 2008), are introduced as examples for specialized WSN MAC protocols. The two approaches put the burden of synchronizing with the sleeping cycle of the receiving node on different partners of the communication: in X-MAC, the sender is announcing/pushing until the receiver is online and in LPP, the receiver is listening/polling for packets.

X-MAC Buettner et al. (2006) present a protocol based on the idea of the Low Power Listening (LPL) approach (Moss et al., last accessed April 2014). The idea behind LPL is that nodes turn off their radio for a time t_{sleep} and after this time elapsed, they turn their radios on, listen to the channel and if there is no announcement of a potential sender, then the nodes go back to sleep for t_{sleep} . If the receiver receives an announcement, it stays awake to receive the packet following the announcement. If a node wants to send, it turns on its radio and sends an announcement, a preamble, for at least the duration of t_{sleep} . Thereby, it is guaranteed that the receiver has realized the senders wish to communicate and after the preamble, the message can be send. This approach clearly minimizes the energy intensive idle listening, Buettner et al. (2006) improve the



(a) In X-MAC the sender tries to establish the communication by sending strobes until the receivers checks the channel after its sleeping period and answers.

(b) In LPP the receiver tries to poll data with the help of probes at the beginning at a certain interval. If a sender wants to send data, it stays awake and waits for the probe of its receiver.

Figure 2.12: Communication flow and basic timing of X-MAC and LPP protocol.

LPL approach in due consideration of some technical details of the radio. Since in the original LPL approach a long preamble for the time t_{sleep} is blocking the channel, energy is wasted with this long transmission and nodes that are not intended to be the receivers also wait for the final packet. Further, a problem of modern radios as the CC2420 (Chipcon, 2004) is the so-called packetizing (the radio includes a controller that returns a full packet at once). Therefore, packetizing radios have problems in generating a long stream of bits as a preamble. However, this can be easily achieved with older streaming radios as the CC1000 (Chipcon, 2002) (these radios allow individual access to the bits by the microcontroller). To overcome these problems, the long preamble is replaced by short announcement packets. These short packets, also referred to as strobes, include the receiver address to just address the intended receiver. By using strobes, Buettner et al. (2006) are also able:

- to make the energy consumption independent of the network density, since only the designated receiver stays awake,
- to allow receivers to send an “early ACK” and thus, to shorten down the preamble time, and
- to discover a collision earlier if two senders intend to reach the same receiver (thus, the later sender can back off immediately and by this further energy is saved).

The detailed flow of X-MAC is illustrated in Figure 2.12a.

The energy efficiency of this approach compared to ZigBee has been investigated and confirmed in (Suarez et al., 2008). Although the ContikiOS implementation of X-MAC is based on (Buettner et al., 2006), it does not support the optimization of the duty cycle parameters as suggested in (Buettner et al., 2006).

Low Power Probing LPP (Musaloiu-E. et al., 2008) can be roughly described as the inverse approach to X-MAC. Instead of the sender initiating the communication, the receiver is announcing its ability to receive messages, basically polling messages. In LPP, all nodes are duty cycled and wake up for just a short time. If a node is awake, it sends a small packet, called probe, to signal that it is awake and then it listens for a short time for replies. A sending node turns its radio on and listens for the probe of the communication partner. Additionally, LPP simplifies routing in networks with a single data sink. The data is polled hop by hop to the base station instead of being pushed to it, for which the sender needs to know an address of a node closer to the base station. Figure 2.12b shows the principle of LPP.

While the macro timing (e.g. the delay after an unsuccessful CCA) might vary between these protocols, the micro timing based on the processes of the PHY Layer (airtime of an packet) are the same throughout all these protocols. For the sake of universal applicability, this work focuses on these micro timings that are consistent throughout the different MACs. Thereby, the results can be transferred to different implementations or can lead to an optimized MAC itself.

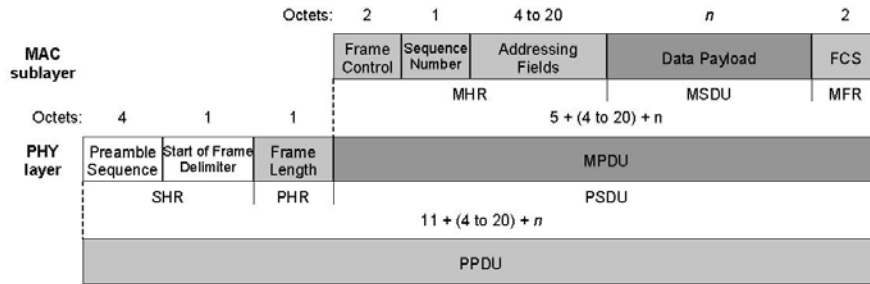


Figure 2.13: Schematic view of the IEEE Standard 802.15.4 data frame format. Taken from (IEEE, 2003b).

Packet Airtimes

In addition to the start time of the channel access, its duration, which is based on the physical data rate, is important for coexistence analysis. Therefore, the maximum and minimum airtimes of a packet on the channel are computed. The maximum MAC payload depends on the frame length, which is limited by the Frame Length field in the Physical Header (PHR). The structure of IEEE 802.15.4 packets is shown in Figure 2.13. Since the Frame Length field includes a reserved bit, it can hold a value equal or less than 127 and thus the Medium Access Control Protocol Data Unit (MPDU) is limited to 127 bytes.

In the recent amendment of the IEEE Standard 802.15.4 (IEEE, 2012a), the MPDU limit is mentioned to be increased to 1,500 bytes, which matches the Maximum Transmission Unit (MTU) of IP networks. The MTU defines the maximum payload size that is transferable within a network without packet fragmentation. The Ethernet standard also defines a MTU of 1,500 bytes (Tanenbaum and Wetherall, 2011; Hornig, 1984). The advantages and disadvantages of packet fragmentation are discussed in detail in Section 6.3.2. However, in this work the older, but practically established limit of 127 bytes is assumed for IEEE 802.15.4.

As shown in Figure 2.13, the PPDU, which is actually transferred over the air, consists of a Synchronization Header (SHR), a PHR and the MPDU. Adding the 6 bytes for the headers increases the maximum PPDU size to 133 bytes. The PPDU is sent with a data rate of 250 kbit/s (in the 2.4 GHz band, compare to Table 2.1), resulting in a maximum channel use of 4,256 μ s (as e.g. stated in (Tytgat et al., 2012; Liang et al., 2010)). The content of a MPDU can differ since not all WSN protocols are based on IEEE 802.15.4-compliant framers at the MAC, especially the Medium Access Control Header (MHR) is subject to variation. This means that the minimum airtime depends on the protocol and the shortest packet cannot be defined uniquely. However, a good reference point for the shortest meaningful packet is the ACK packet, which is defined in the IEEE 802.15.4 standard, and is supported in hardware by some radios (e.g. CC2420). Theoretically, shorter packets than an ACK packet are possible. Such shorter packets are used as strobes in X-MAC to indicate the will to send and as probes in LPP to announce the start of the time window of possible reception. However, these are not defined in IEEE 802.15.4. Figure 2.14 gives the structure of an ACK frame defined in (IEEE, 2003b). The 11 bytes of the PPDU are in the air for 352 μ s. Tytgat et al. (2012) assume a minimum packet airtime of 320 μ s, which equals a byte less.

2.3.3 Physical Layer

After discussing the possibilities of the MAC Sublayer, in the following the basic layer enabling all other higher functions, the PHY Layer, is presented.

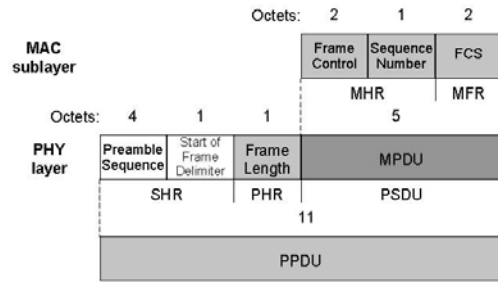


Figure 2.14: Schematic view of the IEEE Standard 802.15.4 ACK frame format. Taken from (IEEE, 2003b).

The functionalities offered by and requested of the PHY Layer are defined by the IEEE in the form of services and interfaces between different layers. These SAPs were already shown in Figure 2.6. The PHY Layer provides all its services through two of these SAPs, the Physical Data-Service Access Point (PD-SAP) and the Physical Management Entity-Service Access Point (PLME-SAP). For a better understanding of the standard, the four types of service primitives have to be mentioned:

- request,
- indication,
- response, and
- confirm.

The PD-SAP passes received messages to the MAC Sublayer (PD-SAP.Indication), accepts messages to be sent (PD-SAP.Request) and confirms the transmission of a message (PD-SAP.Confirm) with the help of these primitives (IEEE, 2003b). The PLME-SAP enables functions that are less obvious:

- enabling and disabling of the transceiver (by turning the radio on and off, energy can be saved),
- CCA (the MAC can request the channel status to manage the channel access),
- Energy Detection (requests the result of an Energy Detection (ED) measurement, also known as a request of an RSSI value), and
- setting and getting communication settings (as the current channel, the transmit power and the CCA mode).

Some of these primitives, as the CCA and the ED are analyzed in depth later in this work due to their importance for the detection of and reaction to interference.

IEEE 802.15.4 in its original release and thereby ZigBee (ZigBee Alliance, 2008b) support three license-free Industrial, Scientific and Medical (ISM) bands: one channel at 868-898.6 MHz in Europe (regulated by the European Telecommunications Standards Institute (ETSI)), ten channels at 902-928 MHz in North America (regulated by the Federal Communications Commission (FCC)) and finally 16 channels in the 2400-2483.5 MHz frequency band for worldwide use, as shown in Table 2.1. The local bands for Europe and North America are also called lower bands and the 2.4 GHz frequency band is called higher band (Gutiérrez et al., 2004). In a more recent version of the standard (IEEE, 2006), the number of channels and features has been increased and finally in the most recent version (IEEE, 2011b), Ultra Wide Band (UWB) technology has been introduced, but

Frequency band & region	IEEE 802.15.4 version		
	2003	2006	2011
868 - 868.6 (Europe)	1 channel for DSSS + BPSK 20 Kbit/s	1 channel for PSSS + ASK 250 Kbit/s 1 channel for DSSS + O-QPSK 100 Kbit/s	
902 - 928 (North America)	10 channels for DSSS + BPSK 40 Kbit/s	10 channels for PSSS + ASK 250 Kbit/s 10 channels for DSSS + O-QPSK 250 Kbit/s	
2,400 - 2,483.5 (worldwide)	16 channels for DSSS + O-QPSK 250 Kbit/s		13 channels for CSS + DQPSK 1,000 Kbit/s

Table 2.1: License-free ISM radio bands supported by IEEE 802.15.4 in its different versions. For each standard the number of provided channels, the spreading, modulation and the achievable data rate are given. The ASK used in the 868/915 MHz band is used for most of the packet, while the SHR is BPSK modulated. The latest standard (IEEE, 2011b) also introduced other frequency bands to be used in Japan and China, and a band for UWB communication, which are beyond the scope of this work.

is not widely available yet. All the different upgrades affecting the three ISM bands can be seen in Table 2.1, however it has to be mentioned that most hardware and most wireless sensor node platforms available today are based on the initial standard version. Additionally, the different data rates of the standard are shown in Table 2.1. The data rates differ with the change of the used modulation in the different frequency bands. For the locally restricted lower bands at 868/915 MHz, a Binary Phase-Shift Keying (BPSK) chip modulation is used. The 2.4 GHz band is supported with an Offset Quadrature Phase-Shift Keying (O-QPSK) modulation. Despite all the recently added options, the 2.4 GHz frequency band is predominantly chosen, which is due to a faster data rate and a worldwide customer audience. Furthermore, it has no additional limitations on its channel use (e.g. the maximum channel utilization is limited to 1% in the 868 MHz band).

Since this work focuses on the 2.4 GHz frequency band and the external sources of interference within this band, the steps from a request called at the PD-SAP down to the electromagnetic waves emitted at the transmitter are exemplarily explained for the O-QPSK modulation in the 2.4 GHz frequency band in the following.

From Packet to Signal

In the following section, the way of a packet through the PHY Layer and its final conversion into electromagnetic signals are discussed. These steps are all defined in (IEEE, 2003b), but not explained and therefore a basic knowledge of telecommunications engineering is required to understand the IEEE standards. These steps happen in the actual hardware of the wireless transmitter and knowledge of them is more of theoretical nature, since the possibilities of influencing the actual modulation are limited in most cases. Recently, cognitive or Software Defined Radios (SDRs)⁴ gained a lot of interest in the research community (Wang and Liu, 2011). Thus, the strict separation between bought, off-the-shelf hardware chips and self-developed software might be dissolved in the near future. Even the fields of telecommunications engineering and computer science would overlap and the knowledge about the PHY Layer processes would become applicable. The following sections aims:

- to give an understandable introduction for computer scientists with little knowledge of the telecommunications domain;

⁴A SDR is the attempt to design a radio where ideally all system components are implemented in software, including nowadays hardware components as mixers, filters and amplifiers (Buracchini, 2000).

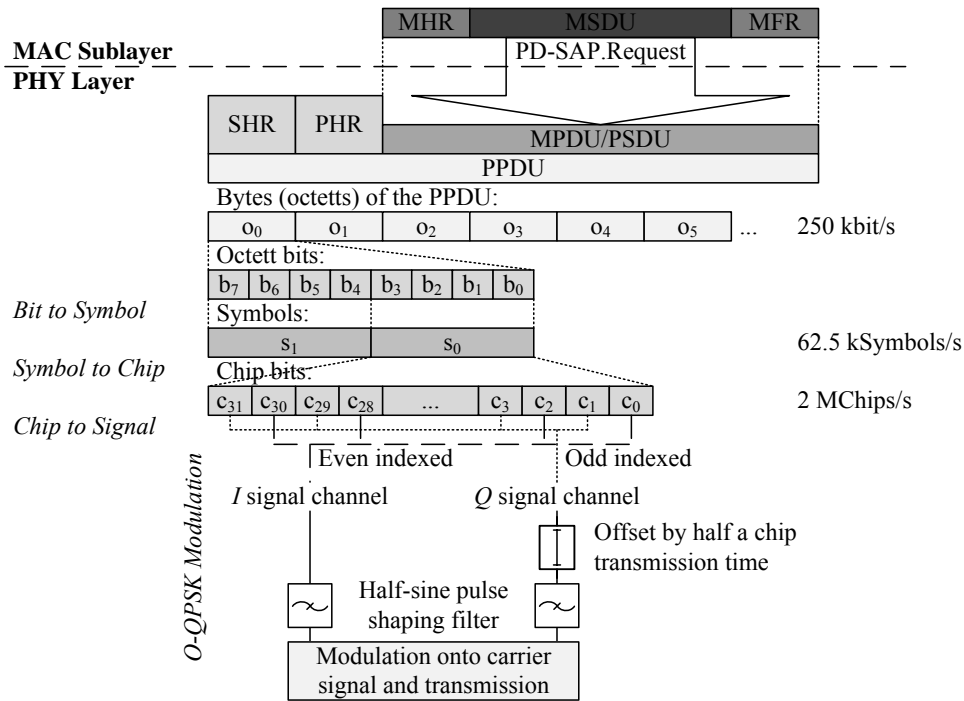


Figure 2.15: The steps of a packet from the handover of the MAC to the transmission of the electromagnetic signal.

- to explain certain commonly used terms of IEEE 802.15.4, e.g. symbols, chips, DSSS and O-QPSK;
- and to give a deeper understanding of the reasons for certain already briefly introduced properties, e.g. the PSD and the difference between data, symbol and chip rates.

The processing in the PHY Layer starts with a packet in the form of a MPDU, passed from the MAC Sublayer through the PD-SAP by a request. The MAC and the framing of the packet on the MAC Sublayer are discussed in Section 2.3.2. This incoming MPDU is extended by a SHR, consisting of a Preamble Sequence and a Start of Frame Delimiter, and by a PHR, including the Frame Length field. Thus the so-called PPDU, the actual binary data of 133 or less bytes, is ready to be processed to the electromagnetic signal that is finally transmitted over the air. Figure 2.15 gives an overview and a thread through the following steps of the packet processing.

Bit to Symbol The data of the PPDU is split into symbols starting at the preamble sequence of the SHR and ending at the end of the packet, which is the Frame Check Sequence (FCS) field of the Medium Access Control Footer (MFR). A data symbol is a nibble (a group of four bits), i.e. every byte (octet) is halved into two symbols beginning with the least significant bit. Thus, a byte of the PPDU consisting of bits $b_0 \dots b_7$ (least to most significant bit), results in data symbols $(b_0, b_1, b_2, b_3) = s_0$ and $(b_4, b_5, b_6, b_7) = s_1$, as shown in Figure 2.15.

Symbol to Chip (Spreading) While the mapping of bits to symbols is a simple grouping, in the next step the symbols are spread to a sequence of chips. There exist 16 different data symbols (4 bits = 16 possibilities) and each of these is mapped to one of 16 nearly orthogonal pseudo-random noise sequences. The principle of spreading a single symbol to a longer chip sequence, which is also known as DSSS, minimizes the required transmission energy. The receiver correlates the incoming sequence with its known chip sequences and thereby retrieves symbols from chip sequences that are almost equal to background noise. A sequence consists of 32 chips, thus the 4 bits of a data symbol are spread by the factor eight, which is also the Processing Gain (PG) of the spreading (\approx

Data symbol (decimal)	Data symbol (binary)				Chip values																																Comment											
	b_3	b_2	b_1	b_0	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}	c_{19}	c_{20}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}	c_{27}	c_{28}	c_{29}	c_{30}	c_{31}												
0	0	0	0	0	1	1	0	1	1	0	0	1	1	1	0	0	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	0	0	1	1	0							
1	1	0	0	0	1	1	1	0	1	1	0	1	1	0	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	1	0	0	1	0	0	1	0	0					
2	0	1	0	0	0	0	1	0	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	1	0	1	0	0	0	1	0	0	1	0				
3	1	1	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	1	1	0	1	1	0	1	1	0	0	0	0	1	1	0	0	1	1	0	1	0	1	0	1	0	1	0				
4	0	0	1	0	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	1	1	1	0	0	0	1	0	0	0	1	1	0	0	1	0			
5	1	0	1	0	0	0	1	1	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	1	0	0	1	0			
6	0	1	1	0	1	1	0	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	1	1	1	0	1	1	0	1	1	0	1	1	0	0	1	1	0	0	1	0			
7	1	1	1	0	1	0	0	1	1	1	0	0	0	1	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	1	0	1			
8	0	0	0	1	1	0	0	0	1	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
9	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
10	0	1	0	1	0	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
11	1	1	0	1	0	1	1	1	0	1	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	1	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	1	0	1	1	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	1	1	1	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	1	1	1	1	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 2.2: Symbol-to-chip mapping, values taken from (IEEE, 2003b).

9 dB, see also Section 4.2.3 for the discussion of the resulting signal ratio improvement). This gain is also known as spreading gain.

The design of the pseudo-random noise chip sequences is shown in Table 2.2 and described in the following. According to Gutiérrez et al. (2004), the chip sequences can be divided into two groups: the sequences for data symbols 0 to 7 (the first group in Table 2.2) and the sequences 8 to 15 (the conjunction of the first group). The groups are identical, but in the second group every odd indexed chip is inverted. Hence, the sequence for data symbol 0 is $c_0, c_1, c_2, c_3, \dots$ and the sequence 8 results from $c_0, \neg c_1, c_2, \neg c_3, \dots$ of sequence 0, which is exemplarily shown in blue for data symbols 0 corresponding to 8 and 1 corresponding to 9.

The sequences within a group are related to each other through circular shifts. Each sequence is generated by four bit rotations in direction of the most significant bit (illustrated for data symbols 14 and 15) (Gutiérrez et al., 2004).

Chip to Signal In the final step, the stream of chips which consists of the concatenated sequences, is converted into electric signals, finally modulated onto a carrier frequency and emitted as electromagnetic wave. A stream of maximally $133 \times 8/4 \times 32 = 8,512$ bit (maximum PPDU of 133 bytes into bits, into symbols, into chips) has to be processed. Before explaining the basics of the Quadrature Phase Shift Keying (QPSK) and giving an outlook on the actual O-QPSK used by IEEE 802.15.4 in the 2.4 GHz frequency band, a brief explanation of digital signal processing in the wireless communication domain is provided for the sake of comprehension.

Digital Signal Processing The complex number or rather the I/Q representation of periodic waves is explained in the following to give an idea of wireless transmitters and the transmission via electromagnetic waves. Then, the basics of phase-based modulations are developed by using the example of QPSK as well as the differences to the pulse shaped O-QPSK are explained, which is used by IEEE 802.15.4 in the 2.4 GHz frequency band.

First, the mathematical description of a periodic sine or cosine⁵ wave as a signal $x(t)$ is:

$$x(t) = A \cos(2\pi ft + \Phi) \quad (2.8)$$

⁵A cosine is a sine that is delayed for $\frac{\pi}{2}$ (orthogonal condition, see Equation 2.11).

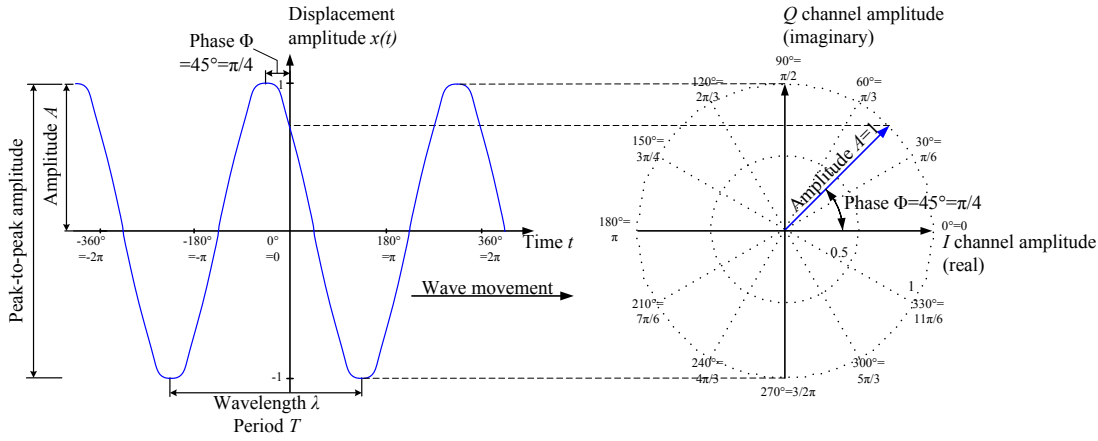


Figure 2.16: Illustration of a harmonic wave and its representation in the complex or I/Q plane. As shown, the key properties of the wave are: The amplitude A is the displacement from the resting position to a peak (crest or trough). In contrast, the peak-to-peak amplitude ranges from crest to trough and is therefore twice the amplitude. The phase Φ is the offset/delay of the wave in relation to a cosine wave. The wavelength λ is the product of the period T and the speed of the wave (for electromagnetic waves the speed equals the speed of light c).

where A is the peak amplitude, f the frequency and Φ the phase of the signal in radian.

If the frequency f is constant, it is referred to as f_0 . The factor 2π and the constant frequency f_0 can also be combined to the constant angular frequency $\omega_0 = 2\pi f_0$. For many trigonometric functions (sine and cosine), the period is 2π . Hence, $\omega = 1$ and as such it can be ignored, which is done in the following.

However, a periodic signal can also be described with the help of complex numbers in the form of complex amplitude \underline{A} :

$$\begin{aligned}\underline{A} &= A e^{j\Phi} \\ &= A(\cos(\Phi) + j\sin(\Phi))\end{aligned}\quad (2.9)$$

The descriptions given in Equation 2.9 are known as Euler or polar form and the trigonometric form, respectively. They describe the signal with the help of a phase vector, also known as phasor, using only \underline{A} and Φ ($\omega = 1$ and is thereby canceled out).

Due to its practical relevance, a form that is often used in telecommunications is the trigonometric notation with I for the real and Q for the imaginary part:

$$\begin{aligned}I &= \Re(z) = \underline{A} \times \cos(\Phi) \\ Q &= \Im(z) = \underline{A} \times \sin(\Phi) \\ \Phi &= \arg(\underline{A}) = \arctan \frac{Q}{I} \\ A &= |\underline{A}| = \sqrt{I^2 + Q^2}\end{aligned}\quad (2.10)$$

where I is the in-phase signal component and Q is the quadrature signal component. A common graphical representation of complex numbers is the complex plane or the unit circle in the complex plane. In the complex plane, a changing phase angle Φ and a complex vector (with the Root Mean Square (RMS) value $A = \sqrt{I^2 + Q^2}$) correspond to a cosine with the amplitude of A offset by Φ , which is illustrated in Figure 2.16. The properties of a wave and its I/Q representation in the complex plane are shown in Figure 2.16 in summary.

The I/Q representation is widely used in telecommunications engineering, because it allows the signal processing in two separate signal channels for I and Q , when the simple orthogonal

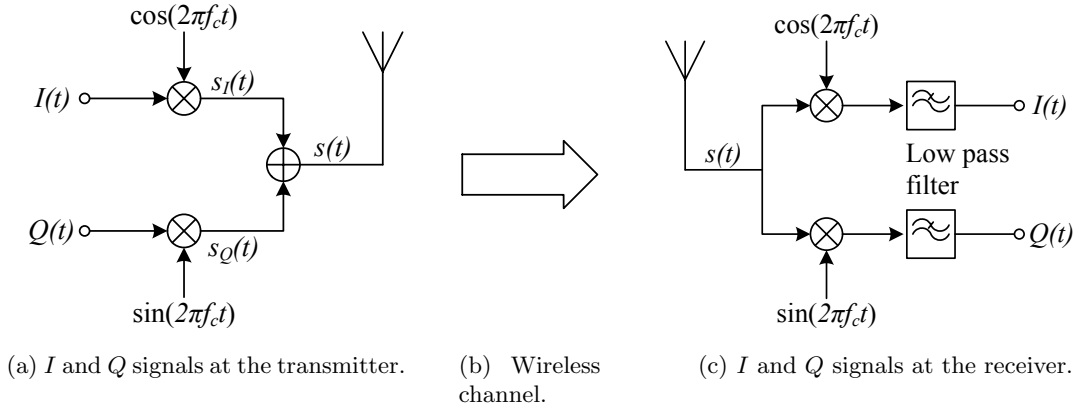


Figure 2.17: Principle of the implementation of the I and Q signal channels in a wireless transmitter. The $I(t)$ and $Q(t)$ signals are generated independently, modulated onto orthogonal carrier signals and added up. Then, the superpositioned signal $s(t)$ is transmitted with the help of an antenna over the wireless channel to the receiver. On the receiver side, the received signal is processed separately for $I(t)$ and $Q(t)$ signals by demodulating the two carriers on two individual paths.

condition, given in Equation 2.11, of a $\frac{\pi}{2}$ phase shift is met for the two carrier signals with a frequency f_c :

$$\sin(2\pi f_c t) = \cos\left(2\pi f_c t - \frac{\pi}{2}\right) \quad (2.11)$$

This allows to use a single carrier signal, which is delayed by $\frac{\pi}{2}$, and therefore a simple implementation can be achieved.

Quadrature Phase Shift Keying For the sake of comprehension, the QPSK is explained in the following as a simpler and therefore easier to understand version of the filtered O-QPSK used in IEEE 802.15.4. The block diagram shown in Figure 2.17 gives an overview of the processing of the I and Q channel. The two individual signal channels, $I(t)$ and $Q(t)$, are the split stream of chip values, where even indexed chips are in the I signal channel and the odd indexed chips are used for the Q signal. Originally, two different pseudo-noise sequences were planned for IEEE 802.15.4: one for the I and one for the Q channel. However, to avoid the complexity of two correlators on the receiver side, a single sequence was chosen (Gutiérrez et al., 2004).

While the original chip bit values of the incoming I/Q signals are either 0 or 1, they are translated according to the constellation diagram, which is shown in Figure 2.18 to -1 and 1 for I and Q , respectively. Since both channels can each code one bit (for the particular case looked at here), resulting in four states, a so-called quadrature modulation is achieved. Each of the signal channels, $I(t)$ and $Q(t)$, is individually modulated onto the carrier signal, thus the new modulated signals are:

$$\begin{aligned} s_I(t) &= I(t) \cos(t) \\ s_Q(t) &= Q(t) \sin(t) \end{aligned} \quad (2.12)$$

Finally, both are added up, resulting in:

$$s(t) = I(t) \cos(t) + Q(t) \sin(t) \quad (2.13)$$

Additionally, the superpositioned signal $s(t)$ is often normalized with the help of factor $\frac{A}{\sqrt{2}}$ to have a signal with a displacement amplitude in the range of -1 and 1 .

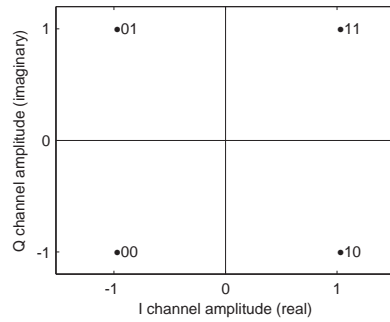


Figure 2.18: Constellation diagram for QPSK. Each of the four points represents two bits: one bit from the I channel and one bit from the Q channel. The wave described by each point is used to transmit these two bits.

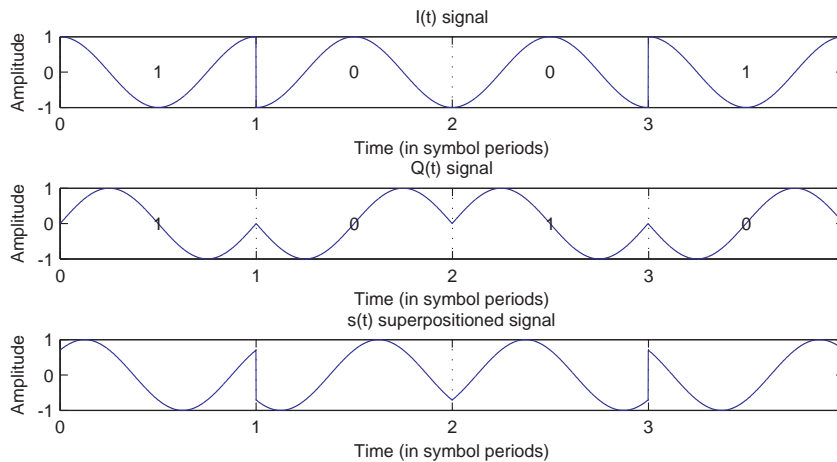


Figure 2.19: I/Q values, signals ($I(t)$, $Q(t)$) and added signal ($s(t)$) over time for QPSK for all four possible combinations of I and Q values. The changes at the bit boundaries are the phase changes that contain the information.

Apparently, the final signal $s(t)$ can have four different shapes, which are shown in Figure 2.19. The amplitude stays the same for all shapes, thus no information is carried by the amplitude and all the information is transported with the help of phase shifts.

Offset Quadrature Phase-Shift Keying used by IEEE 802.15.4 Nevertheless, the just presented QPSK has the problem that for phase shifts of π , the origin of the constellation diagram is crossed ($I = 0$ and $Q = 0$ resulting in no signal). To avoid the resulting cancellation of the signal, the I and Q signals are offset by half a chip transmission duration. This offset between the signal channels improves the QPSK to O-QPSK. The disadvantageous crossing of the origin of the original QPSK and the new transitions between the constellation points are shown in Figure 2.20. The figure shows a vector diagram, which is similar to the constellation diagram, but many I and Q states are plotted, including all the transitions between the four constellation points (Agilent, 2004).

A second disadvantage of the modulation explained so far is the signal bandwidth. The signal bandwidth is the used part of the spectrum and to avoid interference it should be minimized. In order to narrow the shape of the PSD, the streams of chips $I(t)$ and $Q(t)$ are filtered. Instead of streams of binary states -1 and 1 , which are hold for at least a chip duration, the streams are filtered by pulse shaping filters that result in half-sine shaped pulses (Farahani, 2008). The idea

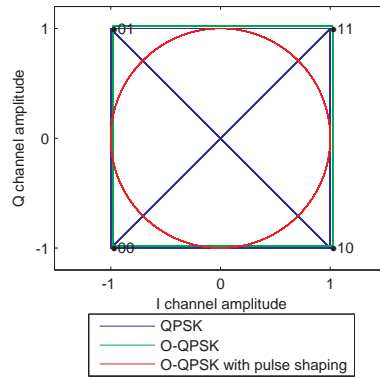


Figure 2.20: Transitions between constellation points by I and Q components for QPSK, O-QPSK and O-QPSK with a half-sine pulse shaping filter (small offset added for O-QPSK for the visibility of overlapping lines).

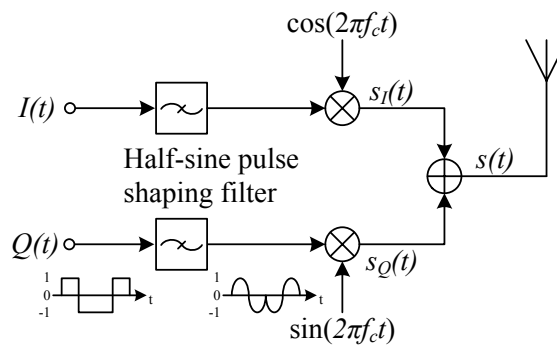


Figure 2.21: The block diagram of a transmitter with half-sine pulse shaped baseband chips as an enhancement to the basic transmitter shown in Figure 2.17a.

behind this enhancement can be explained as follow: while a rectangle impulse results in a sinc^6 function in the spectrum, a sine wave results in a peak at a single frequency (Dirac delta function).

The updated signal flow is illustrated in Figure 2.21 and the resulting effect in the spectrum is illustrated in Figure 2.22. Further, the transition between the constellation points is altered. Now, the transition changes run on a circle as shown in Figure 2.20.

The I/Q signals shown in Figure 2.19, the I/Q vectors in Figure 2.20 and the spectra in Figure 2.22 are simulations for illustrative purposes. For figures of measured signals, the application note for signal generation by Schmitt and Butz (2011) can be consulted. A deeper discussion of the modulation techniques including pulse shaping can be found in (Rappaport, 1996).

Further implementation details, especially internal hardware details of the radio, are specific for certain radio chips and as such beyond the scope of this work. Nevertheless, the CC2420 radio transmitter used for this work is explained in more detail in Section 3.1.1. Moreover, the insight given in this section allows understanding the processes in the PHY Layer and their descriptions given in the IEEE standards. While only the process on the transmitter side is explained in detail, the reception and demodulation of a signal is the inversion of the just presented process. Furthermore, the transmissions and their effects lead to a better understanding of the interfering technologies, since interference only occurs when there is an overlap in the spectrum.

IEEE 802.15.4 in the Spectrum

After discussing the principles of radio waves and the resulting PSD, applied guidelines given in IEEE 802.15.4 are reviewed in the following. As already mentioned in Section 2.2 and shown in

⁶ $\text{sinc}(x) = \frac{\sin(x)}{x}$ or rather $= \frac{\sin(\pi x)}{\pi x}$

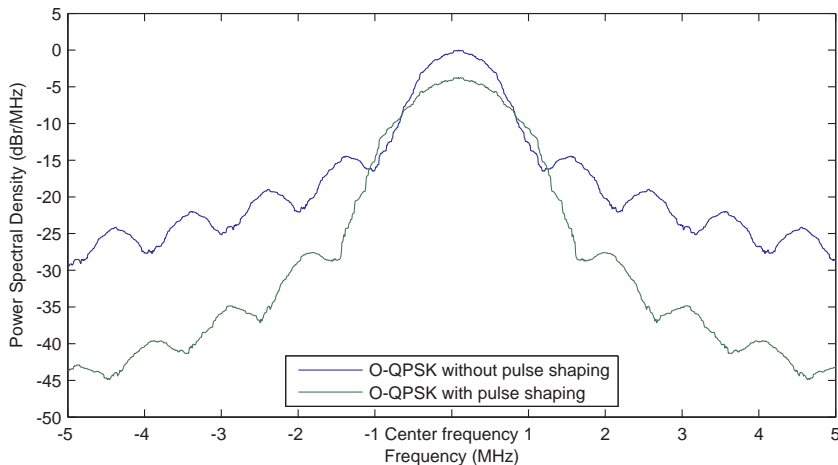


Figure 2.22: Example PSD of O-QPSK without and with half-sine pulse shaping filtered chip streams.

Figure 2.5, a distinction between transmitter and receiver has to be drawn. Since IEEE 802.15.4 is normally the victim of interference, the receiver side gains more interest in the following, but both roles are discussed for the sake of completeness. On the sender side, the transmit PSD mask is restricted at ± 3.5 MHz of the center frequency to -30 dBm as absolute limit or at least to -20 dBm (IEEE, 2003b). The maximum transmit power is not stated in the standard, only a minimum power of -3 dBm has to be supported. The maximum depends on local legal restrictions. Nevertheless, a maximum transmit power of 0 dBm is supported by most sensor nodes. Figure 2.23 illustrates the given transmit PSD mask in red and shows measured PSDs of a Tmote Sky in transmitter test mode collected with the help of Tmote Sky RSSI readings and measurements of a metageek Wi-Spy 2.4x device. More details about the definition of the RSSI values are given in the next section. The characteristics, especially the robustness, of the receivers are also reviewed in Section 4 and Equation 4.12 indicating its resistance to noise.

Clear Channel Assessment

While the just discussed features are depending on the hardware and are used indirectly, the PHY Layer offers the CCA Request. It is the base for the Listen Before Talk MAC strategy (see Section 2.3.2). In the following, the actual process behind the “Listening” to the channel is analyzed. Therefore the CCA Request is normally used in the MAC.

IEEE 802.15.4 uses one of at least three methods to perform a CCA:

CCA Mode 1 Energy above threshold. If the radio detects any energy above a threshold, the medium is considered to be busy.

CCA Mode 2 Carrier sense only. If the radio detects a valid signal (a signal that has been modulated and spread according to the IEEE 802.15.4 standard) the medium is considered busy.

CCA Mode 3 Carrier sense with energy above threshold. If the signal is valid (modulation and spreading) and the received energy is above a threshold, the medium is considered to be busy, as stated in (IEEE, 2003b). In newer versions of the standard (since (IEEE, 2006)), a logical combination (*and* or *or*) of the valid signal and energy level condition can be used for the decision. The here used CC2420 radio, which is introduced in Section 3.1.1, supports an *OR* combination (Chipcon, 2004).

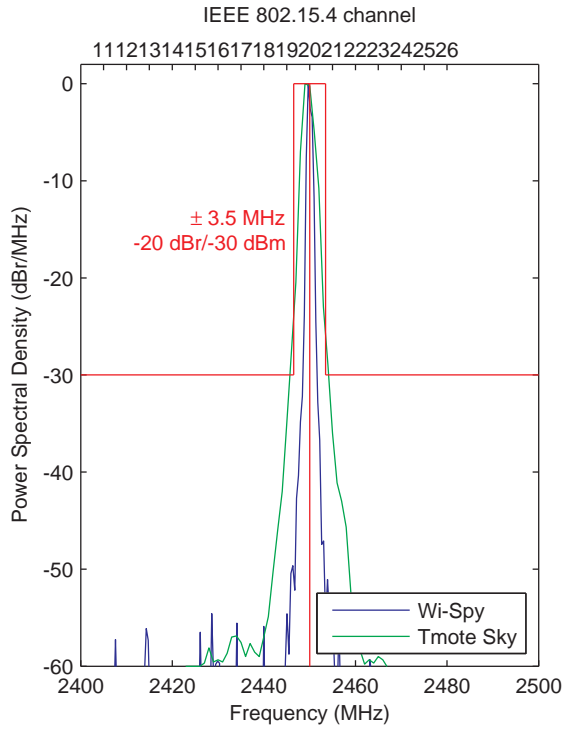


Figure 2.23: PSDs of IEEE 802.15.4 measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node. The sending node generated a modulated spectrum in the transmitter test mode. The transmit PSD mask is plotted in red. The offsets of the curves have been aligned for better demonstration.

With the latest version of the standard (IEEE, 2011b), new CCA modes have been introduced (mainly for UWB communication), but they are not of further interest here. For more details on CCA modes, Ramachandran and Roy (2007) give a detailed review of CCA modes of wideband transmitters. In the following, the technique behind CCA Mode 1, the method of choice to avoid external interference, is reviewed.

The energy that is measured in CCA Mode 1, also referred to as the ED value or better known as RSSI value, is roughly the signal power received at the radio. Therefore, it can be treated as power ratio. When this RSSI/ED sensing is used for the CCA, e.g. in CCA Mode 1, it is only compared to a threshold. But through the measured energy level, the RSSI value gives a valuable insight on the channel status beyond a binary busy/idle decision. The standard (IEEE, 2003b) defines the ED value as an estimation of the signal power within the channel at the receiver. In (Ramachandran and Roy, 2007), the CCA ED is defined as the integral of the squared received signal or the envelope over a given time duration, which is the common definition of the energy E_x of a signal and can be transferred to a discrete signal:

$$E_x = \sum_{n=1}^N |x_n|^2 \quad (2.14)$$

with N being the number of samples x . Since the power P_x of a discrete signal is defined as:

$$P_x = \frac{E_x}{N} = \frac{1}{N} \sum_{n=1}^N |x_n|^2 \quad (2.15)$$

and the duration (the number of energy samples N) of the RSSI measurement is a constant time span, the energy is equal to the power.

	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Initial release year	1999	2003	2009
Use in 2013	Expiring	Widely used	Growing use
Maximum theoretical data rate (Mb/s)	11	54	up to 72.2 or 144.4 (channel bonding)
Modulation scheme	DSSS	OFDM	OFDM
Channel width ¹ (MHz)	22	20	20 or 40 (channel bonding)

Table 2.3: Key features of the different versions of IEEE Standard 802.11 operating in the 2.4 GHz frequency band. ¹Simple channel model.

The RSSI values are internally sampled over 8 symbol periods (128 μ s), which roughly correspond to an 8,192 Hz sampling rate (\approx 122 μ s) that is predominantly used in this work. More implementation details are discussed in Section 3.1.1. However, it has to be highlighted that the signal is measured over a roughly 2 MHz wide channel, as defined by IEEE Standard 802.15.4. Hence, if a signal is narrower than 2 MHz (e.g. Bluetooth), the measured value will be smaller than the signal’s peak energy.

2.4 IEEE 802.11b, g, n

After discussing IEEE 802.15.4 in extended detail, in this Section the WLAN-enabling technologies are reviewed. The IEEE 802.11 Standards are a collection of standards describing the two lowest layers of WLANs, which are nowadays omnipresent. Some of the standards are not used anymore (as the outdated original IEEE Standard 802.11, also known as “legacy mode”) and a few do not work in the 2.4 GHz frequency band. Thus, the standards 802.11b, 802.11g (IEEE, 2007) and 802.11n (IEEE, 2009) are of interest in the following. Table 2.3 gives the most important features introduced in these standards. Recently, all standards have been reviewed by the IEEE and combined into (IEEE, 2012b). The commonly used term Wi-Fi stands for an industry consortium and is also a trademark for hardware that is compatible with other Wi-Fi hardware. Besides the just mentioned standards, there are many task groups dealing with possible aspects of the widely used IEEE 802.11 standards (Stephens, last accessed November 2013). However, the classical use cases of IEEE 802.11 for WLANs in the 2.4 GHz frequency band is discussed in the following as the most likely source of interference for WSNs.

The architecture of IEEE 802.11 supports two topologies: ad hoc networks, which allow devices to connect directly, and the commonly used infrastructure networks, which allow clients to connect to an Access Point (AP). The AP is the central instance, which organizes the network, and normally it is also a gateway that connects a WLAN to the Internet. The connection between nodes is maintained with the help of beacon frames, which are sent periodically by the AP in infrastructure mode or by one of the nodes in an ad hoc network. These beacon frames stand out from the rest of the traffic, because they are not only sent periodically, but also with a low data rate for compatibility reasons. The data rates and the modulations are discussed in Section 2.4.3 and the beacon frames are reviewed in more detail in Section 2.4.2. The IEEE Standards 802.11 define one MAC and multiple PHY Layers: first the relevant parts of the MAC are discussed and then the PHY Layers are reviewed.

2.4.1 MAC Sublayer

The MAC of IEEE 802.11 offers up to four channel access methods: the Point Coordination Function (PCF), the Hybrid Coordination Function (HCF), the Mesh Coordination Function (MCF) and, most commonly used, the DCF (IEEE, 2012b). The PCF is based on the AP managing the medium access by polling the data from the clients. The HCF was introduced by IEEE 802.11e (IEEE, 2005a) and is an enhancement to support Quality of Service (QoS) requirements. The

rarely used MCF offers, as the name suggests, a suitable strategy for mesh networks based on IEEE 802.11. The mesh network methods are studied in IEEE 802.11s (IEEE, 2011a). DCF is a mandatory feature and the most often used coordination function. It is basically a CSMA/CA algorithm. Later in this work, the coexistence between IEEE 802.11 and IEEE 802.15.4 is discussed (see Chapter 4) and although both technologies apply a form of CSMA/CA, the channel access systems are not compatible (see Section 6.3.3). Since IEEE 802.11 is mostly the interferer and the MAC defined by the standard is used almost exclusively, the timing of its channel access is of special interest in the following. Due to the different versions of the PHY Layer with their different data rates, the timing of the channel access of IEEE 802.11 may vary. Nevertheless, in the following the basic flow and the magnitudes of time are explained. In contrast to the MAC of IEEE 802.15.4 and most other commonly used WSN MACs, IEEE 802.11 supports an RTS/CTS-handshake (see Figure 2.1c for an illustration of the handshake flow). Hence, the time flow of messages between two communication partners (the data sender and the data receiver) in an IEEE 802.11-based WLAN using the DCF can be described as follows:

1. The data sender waits for one Distributed (coordination function) InterFrame Space (DIFS) period: The packet is ready to be sent by the MAC and the data sender starts listening to the channel for the duration of a DIFS. If the channel is clear for that duration, an RTS is sent in the next step.
2. The data sender sends an RTS: The RTS frame itself consists, as all frames, of a prefixed Physical Layer Convergence Protocol (PLCP) part (preamble and header) and the actual packet (the MPDU). The PLCP preamble and header are transmitted with a lower data rate to make sure that they are understood by all network nodes in range (and not only by the intended receiver). The MPDU is sent with a higher data rate. The exact structure of the packets will be explained later in this section.
3. The data sender waits for one Short InterFrame Space (SIFS) period: The data receiver has to reply within the duration of a SIFS. The SIFS is so long that the message can be processed, the transmitter can change from receive to transmission mode and the reply can be prepared (the actual Receive (RX)-to-Transmission (TX) time is shorter than a SIFS). However, the SIFS is shorter than the DIFS and thereby the channel is busy again before another noninvolved node starts sending.
4. The data receiver sends a CTS: The RTS is answered with a CTS by the data receiver.
5. The data sender waits for one SIFS period: Again, the duration of a SIFS elapses, in which the CTS is received by the original data sender, which sent the RTS, and the final data packet is prepared.
6. The data sender sends the data packet: After the successful handshake, the data sender can send its data packet, which consists of two different modulated parts.
7. The data sender waits for one SIFS period: After the transmission, the sender waits to receive an ACK.
8. The data receiver sends an ACK: The receiver has received the data packet and checked it to be free of erroneous bits with the help of the FCS. To end the process, the data receiver affirms the packet reception by sending an ACK to the data sender.

The complete flow is summarized in Figure 2.24, in which steps 1 to 8 refer to the preceding numbering of the steps. On noninvolved nodes, which receive the RTS or the CTS, the duration of the following channel use is read from the RTS or CTS. This mechanism is also known as virtual

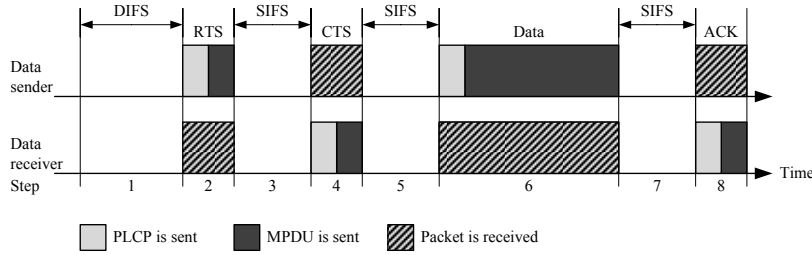


Figure 2.24: Basic time flow of the RTS/CTS-handshake, the data transfer and the final ACK of IEEE 802.11.

	DIFS	SIFS
IEEE 802.11b	50 μ s	10 μ s
IEEE 802.11g	28 μ s	10 μ s

Table 2.4: The durations of interframe spacings for different versions of the IEEE 802.11 standard.

carrier sensing, since a real CCA does not have to be performed as long as the channel use duration is already known. The counter of the reserved channel is also referred to as Network Allocation Vector (NAV). The backoff times are mainly important for the throughput of IEEE 802.11. The DIFS and SIFS timings of the different IEEE 802.11 versions are relevant to see if there is a chance of IEEE 802.15.4 packets to fit in between IEEE 802.11 frames. And as it can be seen in Table 2.4, IEEE 802.15.4 (airtimes given in Section 2.3.2) is too slow to fit in the interframe spaces of IEEE 802.11.

Besides the channel access methods, frame structure and airtimes also differ significantly from IEEE 802.15.4. In Figure 2.25 the structure of IEEE 802.11 frames is shown. Since IEEE 802.11 is designed for IP traffic, the frame sizes are greater and the frame structure is more complex with more reserved fields. Since IEEE 802.11 is not the focus of this work, the description of the different fields is not vital for the understanding of the coexistence and therefore not further explained here. For the coexistence, the airtimes of the packets are more important than the actual content and consequently some representative airtimes are calculated in the following, as it has been done for IEEE 802.15.4 in Section 2.3.2

An IEEE 802.11 MPDU consists of a MAC header, the data and a FCS. The MAC header and the FCS have normally a size of 34 bytes in total for data frames. As shown in Figure 2.25, additional fields can be part of the MAC header, but are not assumed in the following.

In the PHY Layer, the PLCP overhead is added. This overhead depends on the version of the standard and the used version of the PLCP preamble and header. For IEEE 802.11b, there are two different PLCP preamble formats. The long, default format needs 192 μ s to be transmitted and the short header is transmitted in 96 μ s. With IEEE 802.11g the modulations of the PLCP preamble and header changed and therefore for IEEE 802.11g the airtime is 20 μ s (Gast, 2003; Perahia, 2008; IEEE, 2012b) However, in (Duda, 2008) a time of 22.1 μ s is stated, which is irreproducible for the author. The different preamble formats for IEEE 802.11b and g are also illustrated in Figure 2.26.

The preamble airtime for IEEE 802.11n cannot be given universally. Due to three different available modes and different supported modulation and coding schemes, there are multiple possibilities being beyond the scope of this work. The three different preamble modes of IEEE 802.11n are: High Throughput (HT)-mixed (an HT preamble preceded by a non-HT preamble for compatibility reasons), non-HT and HT-greenfield (only a HT preamble). However, the IEEE 802.11n preamble is not necessarily shorter than the one used by IEEE 802.11g, since the Multiple Input Multiple Output (MIMO) training and possible backward compatibility (depending on the mode used) increase the overhead and therefore also increase the airtime of the preamble (Perahia,

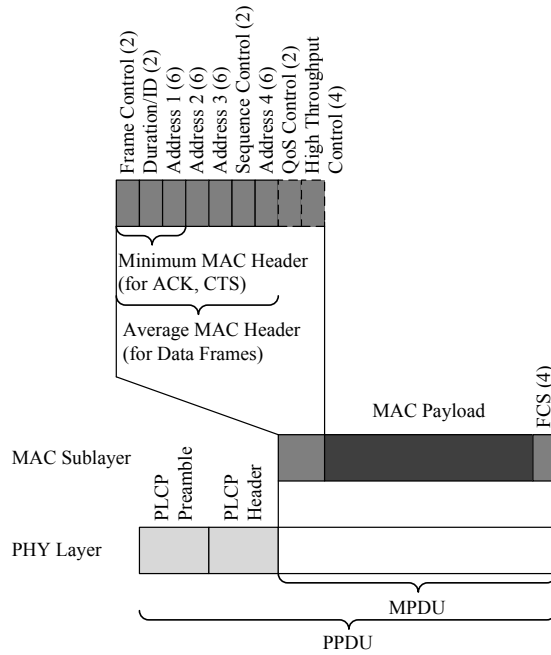


Figure 2.25: Schematic view of the IEEE Standard 802.11 frame format. The field sizes in bytes are given in parentheses.

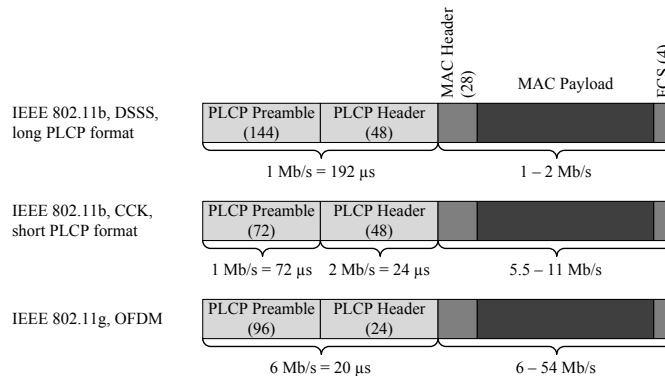


Figure 2.26: Structure of different frames of different versions/configurations of IEEE 802.11. The field sizes in bits are given in parentheses.

2008). Nevertheless, other features of IEEE 802.11n, as the frame aggregation and the increased data rates, can recompense this additional overhead.

Although there are many possible data rates, some key airtimes are computed from exemplary MAC frames at commonly used data rates in the following. The maximum frame body size defined by the maximum Medium Access Control Service Data Unit (MSDU) size is 2304 bytes plus security encapsulation (IEEE, 2007). However, the maximum size of a frame body is finally limited to 2324 bytes by the MAC frame format (IEEE, 2007). With the MSDU being the payload entering the MAC Sublayer, the overhead of the MAC header (30 bytes) and the FCS (4 bytes) is added and thus for the resulting MPDU of 2358 bytes, the maximum airtime can be derived to be 19,056 μ s for IEEE 802.11b at 1 Mb/s with a long preamble. Other configurations lead to different, but shorter durations. More configurations including their calculation method are given in Table 2.5. The computations are based on the *TXTIME* calculation from (IEEE, 2012b).

Hence, IEEE 802.11 often connects to Ethernet networks, which have an MTU of 1,500 bytes, and a realistic maximum packet size is based on this MTU. The 1,500 bytes of payload data have

8.3.1.3 CTS frame format

8.3.1.2 RTS frame format

CHAPTER 2. TECHNICAL BACKGROUND

The frame format for the CTS frame is as defined in Figure 8-14. The frame format for the RTS frame is as defined in Figure 8-13.

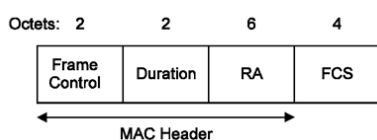


Figure 8-14—CTS frame

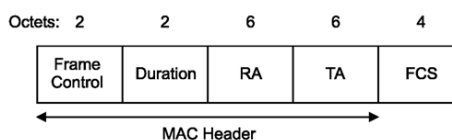


Figure 8-13—RTS frame

When the CTS frame follows an RTS frame, the RA field of the CTS frame is copied from the RA field of the immediately preceding RTS frame. When the CTS is the first frame in a frame exchange, the RA field is set to the MAC address of the transmitter.

Copyright © 2012 IEEE. All rights reserved.

For all CTS frames transmitted by a non-QoS STA in response to RTS frames, the duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval. If the calculated duration includes a fractional microsecond, that value is rounded up to the next higher integer.

Configuration	Maximum airtime for CTS	MTU	RTS airtime for MPDU	ACK/CTS airtime for MPDU	Calculation method (<i>TXTIME</i> from (IEEE, 2012b))
IEEE 802.11b, 1 Mb/s, long PPDUs	19,056 μ s	12,480	352 μ s	304 μ s	$192 \mu\text{s} + \frac{\text{MPDU}_{\text{bytes}} \times 8}{1 \text{ Mb/s}}$
IEEE 802.11b, 11 Mb/s, long PPDUs	1,907 μ s	1,310	207 μ s	203 μ s	$192 \mu\text{s} + \left\lceil \frac{\text{MPDU}_{\text{bytes}} \times 8}{11 \text{ Mb/s}} \right\rceil$
IEEE 802.11b, 11 Mb/s, short PPDUs	1,811 μ s	1,214	111 μ s	107 μ s	$96 \mu\text{s} + \left\lceil \frac{\text{MPDU}_{\text{bytes}} \times 8}{11 \text{ Mb/s}} \right\rceil$
For other CTS transmissions by a QoS STA, the duration value is set as defined in 8.2.5.	372 μ s	248	24 μ s	24 μ s	$20 \mu\text{s} + 4 \mu\text{s} \times \left\lceil \frac{16 \times \text{MPDU}_{\text{bytes}} \times 8 + 6}{216 \text{ bits/symbol}} \right\rceil$

8.3.1.4 ACK frame format

Table 2.5: Selected airtimes of packets for different IEEE Standard 802.11 versions and settings. The frame format for the ACK frame is as defined in Figure 8-15. As reported by Liang et al. (2010); Ansari et al. (2011). ²Liang et al. (2010); Ansari et al. (2011) report 542 μ s/194 μ s, which seems to be due to the unintelligible assumption that the long PPDU format of IEEE 802.11b is used for IEEE 802.11g.

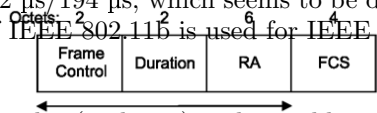


Figure 8-15—ACK frame

a MAC header (28 bytes) and an additional Subnetwork Access Protocol overhead (8 bytes) and thus, according to (IEEE, 2009), the MPDU size is 1,536 bytes.

The ACK frame, which has the same length as a CTS frame, is taken as a reference for the minimum airtime of a packet here. For both frames, the MPDU consists of a Frame Control, Duration and a Receiver Address field and ends with a FCS, as shown in Figure 2.27a. Furthermore, the format of the RTS frame is shown in Figure 2.27b and therefore the time flow of the medium access can now be completely analyzed after being presented at the beginning of this chapter and illustrated in Figure 2.24. In addition to the fields of the ACK/CTS frames, the RTS includes the Transmitter Address to indicate which node wants to send data. The airtimes of the frames are computed as just mentioned for the other airtimes and are also given in Table 2.5.

Depending on the used modulation and coding scheme, IEEE 802.11n times are subject to slight changes, as the frame body limit has been increased to 7,955 bytes. However, at the time of writing, Greenfield setups were only rarely supporting all deployed features and most hardware available was Wi-Fi certified, but only supported some IEEE 802.11n features.

2.4.2 Beacon Frames

As already mentioned, beacon frames sent by the AP are an important identifier throughout all the different IEEE 802.11 versions. The unique characteristics of beacon frames are also highlighted in (Zhou et al., 2010; Ansari et al., 2011; Li et al., 2012) and they are the major identification feature for IEEE 802.11 used later. To provide maximum backward compatibility, the beacon frames are normally sent with the lowest data rate, i.e. 1 or 2 Mb/s.

The following computation of the minimum airtime of beacon frames proves that the sampling rate used by the interference classification algorithm is sufficient to detect beacon frames. The actual minimum airtime of a beacon frame depends, as the previously computed airtimes, mainly on four parts: the PLCP preamble and header, the MAC header, the FCS and the actual MAC payload. Depending on the AP and the network features, the MAC data of a beacon can differ in

Environment	APs/networks	Beacon interval	Frame length	Data rate
Office	24/9	24×100 tu	108...370 bytes	3×1 Mb/s 21×2 Mb/s
Residential	21/21	21×100 tu	97...363 bytes	21×1 Mb/s

Table 2.6: Features of beacon frames from observed APs. More APs than networks (based on SSID) mean that the network was built of multiple APs for better coverage.

Standard	Modulation scheme	Modulation	Data rate (Mb/s)
IEEE 802.11b	DSSS	DBPSK	1
	DSSS	DQPSK	2
	CCK	DQPSK	5.5, 11
IEEE 802.11g	OFDM	BPSK	6, 9
	OFDM	QPSK	12, 18
	OFDM	16-QAM	24, 36
	OFDM	64-QAM	48, 54
IEEE 802.11n	OFDM	1 stream: BPSK, QPSK, 16-QAM, 64-QAM	7.2 - 72.2
	OFDM	2 streams: BPSK, QPSK, 16-QAM, 64-QAM	14.4 - 144.4

Table 2.7: Different modulations supported in the different modulation schemes by IEEE 802.11b and IEEE 802.11g. IEEE 802.11n does not introduce new modulations, but defines 77 modulation and coding Schemes, which include the coding rate, the guard interval and the number of spatial streams.

size. Assuming that a beacon frame has only 50 bytes of payload and is sent with a data rate of 2 Mb/s, an airtime of roughly 200 μ s can be taken as the absolute minimum. Ansari et al. (2011) state a minimum time of 224 μ s, while Zhou et al. (2010) claim the minimum airtime of a beacon frame to be 256 μ s. These are all durations that can be measured with a sample rate of 8,192 Hz, which is used here. See Table 2.6 for an example of typical beacon properties. Although this table is showing a limited data set, it gives a typical example for real world WLAN deployments. Based on experience, the author assumes a beacon interval of 100 tu⁷ for the rest of this work, since this is the default value and the author is not aware of any deployed network using another value for the beacon interval.

The support of a range of beacon intervals increases the computational complexity of the later presented classification and covers only rare, special cases.

2.4.3 Physical Layer

After giving an overview of the options of the MAC, the PHY Layer, which is the layer below the MAC, offers even more modes. As already mentioned, there are multiple PHY Layers described in IEEE 802.11. Table 2.3 shows the different modulation schemes of IEEE 802.11. Note that even within a modulation scheme there are different modulations for different data rates as shown in Table 2.7. Since IEEE 802.11 is not the main focus of this work, these different modulations are not discussed in detail. Nevertheless, when they have an effect on the Packet Reception Rate (PRR) or the classification results, they will be described for the particular case, e.g. see Section 5.4.1.

If the link quality changes between two network participants, the link features for the data traffic, including modulation, can also be altered on the fly. Thus, by using a more reliable modulation, a better link is provided. This adaptation is called automatic data rate scaling (IEEE, 2003a). Rodrig et al. (2005) show this scaling (not only caused by bad links, but also by different abilities of network participants) in IEEE 802.11 traces collected at a conference. Furthermore, their observed ratio of bits sent to channel utilization is interesting. The channel utilization is referred to as airtime usage in their work. In their setup, management frames were only 1.9% (39 of 2040 total MBytes) of the bits transmitted, but in the time domain they were 4% (412 of 9098 s) of the airtime. The author of this work assumes that this imbalance grows even bigger in faster IEEE 802.11 versions as g and n. The measured airtime versus transferred bits of different

⁷A time unit (tu) equals 1.024 ms and is used due to the simple implementation using a base of two.

Figure 5: (a) Retransmission probability as a function of RSSI (upstream traffic only), and (b) number of clients.

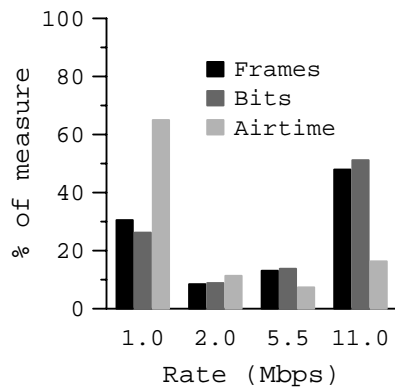


Figure 6: Relative prevalence of transmission rates.

in the *Retry* bit in the 802.11
node retransmits a packet be-
vious transmission was not
e original transmission from
inguish among different re-
ng *retransmission probabil-*
data frames with to the total
re of the quality of the link
ner probability implies that
gements are lost.

on of retransmission proba-
AP) and down-
AP) and down-
its indicate that a trans-
eam than in the upstream di-
nificant variation in retrans-
both directions. Figure 4b
m retransmission probab-
ral trend along downstream
e upstream, there are many
though, downstream proba-
probability varies with sig-
analysis below, we assume
ch other.

more precisely by
we study is the strength of
the floor bounds.
we assume that the relative
asured at a monitor near the
measured with the help of
the relative strengths seen by
of approximately the RSSI
consider downstream traffic
an idea about the real spectral
generated by a Netgear
length has an important fac-
ility, even if it is not an ac-
to check the spectral
tor we study is the effect of
ber of nodes in the network
etermine this measure from
the number of clients active
onsidered active in a given
om it in that interval
e retransmission probability
interval size in this analysis

Number of active clients in the interval compared for different
of IEEE 802.11b. Data measured during a conference. Taken from (Rodrig et al., 2005).
is one minute. The retransmission probability increases with the
number of active clients in the interval. Figure 2.28. Golmie (2006) discusses the
That the retransmissions increase with increased contention has
consequences for rate adaptation. Most adaptation algorithms re-
duce their transmission rate in the face of losses. But if many losses
are caused by contention, rate reduction is unlikely to help. In fact,
rate reduction is exactly the wrong thing to do as it increases con-
tention by occupying the media for a longer time. For this reason,
rate adaptation algorithms should either be driven by throughput [4]
or try to distinguish between the various causes that lead to loss.

6. TRANSMISSION RATE ADAPTATION

The latter were
Little is known about transmission rate adaptation in current hot-
spot environments. In this section we use our trace to investigate
rate adaptation in such settings.

6.1 Summary View

We first investigate the use of different transmission rates in ag-
gregate across all clients. Figure 6 shows the percentage of Frames
and Bits transmitted at each rate, along with the percentage of Air-
time utilized by that rate. The greatest fraction of frames (around
50%) are sent at the highest 802.11b rate of 11 Mbps. This is
because most rate adaptation algorithms have a strong preference
toward this rate. For instance, we see clients that always try to
transmit a new packet at 11 Mbps irrespective of the rate at which
the last transmission succeeded; such clients reduce their rate only
when one of a few consecutive transmissions at 11 Mbps fails. The
figure also shows that Win-Spot uses Frames and Bits, most of the
Airtime is utilized by 1 Mbps data. This is a direct consequence of
1 Mbps frames taking a lot longer than other frames. Hence, while
with the software used here, a dwell time of 122.1 μ s at a frequency and was adjusted in 1 MHz

Additional to the measurements, the spectral masks given in the standards are drawn in red,
to compare between the real characters of the transmitted signal and their limits.

Furthermore, the transmit power is not uniformly distributed in the channel. Soltanian and
Dyck (2001) model the PSD based on a *sinc*² function for the DSSS used by IEEE 802.11b. The
sinc function is the Fourier transformed rectangular function that is squared from the energy to
the power to estimate the density in the spectrum. For OFDM signals, the power spectrum is
more complex to model, but due to the multiple sub-carrier signals the power is distributed more
uniformly and the simplification as a rectangle becomes more suitable (see Liu and Li (2004) for
the derivation of the PSD of an IEEE 802.11a OFDM signal).

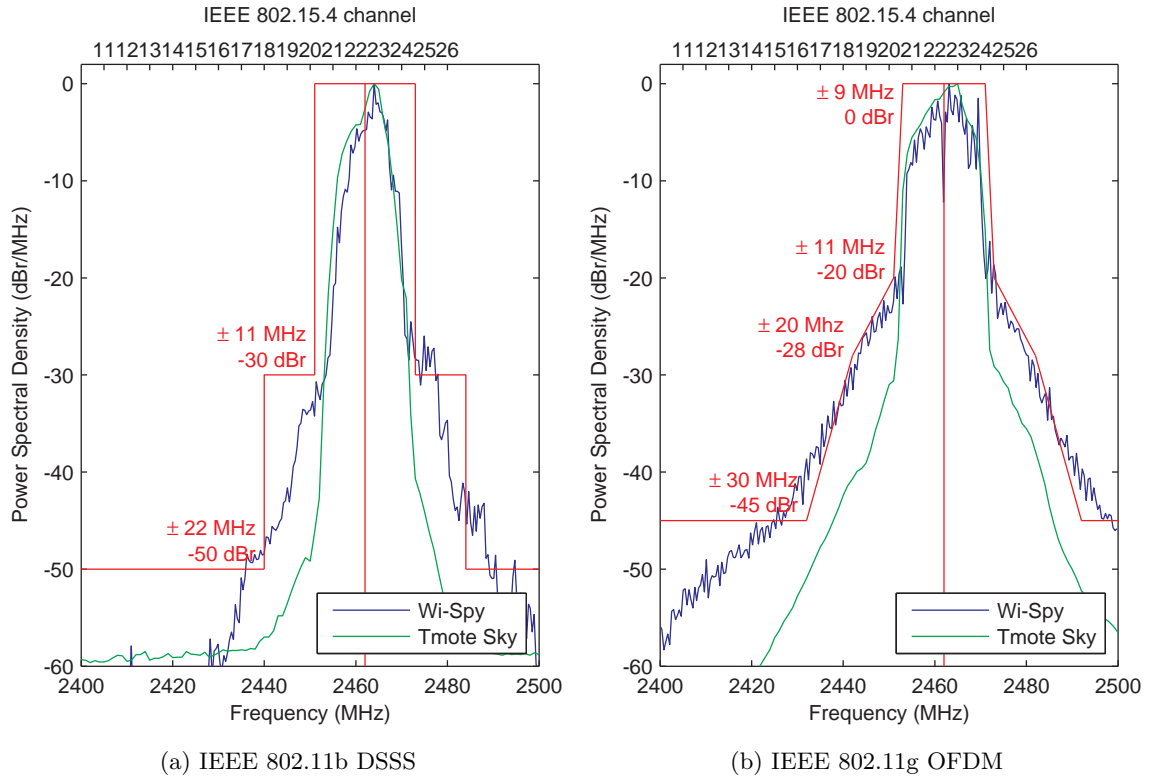


Figure 2.29: PSDs of different IEEE 802.11 modulations measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node. The plotted values are means of 1,800 values measured at 1 s max hold. The transmit PSD mask is plotted in red. The offsets of the curves have been aligned for better demonstration.

Although only a short review of the spectral models is given here, it becomes obvious that the simplified assumption that interference only occurs uniformly in a channel is only an easy model. Petrova et al. (2007) report the observation that interference occurs outside of the IEEE 802.11 channel bandwidth affecting a WSN.

Additional to the commonly used 22 MHz wide channels, IEEE 802.11n also offers 40 MHz wide channels (bonding of two channels), which obviously compounds the problem of interference in the crowded 2.4 GHz frequency band (see Figure 2.30).

The maximum transmit power of IEEE 802.11-compliant devices is subject to local regulations. However, 20 dBm are the common maximum in Europe and many devices send with lower transmit power (especially laptops or other battery-powered mobile devices). Further, they adjust the used transmit power based on the link quality. Typical maximum values would be 17 dBm for an APs and 15 dBm for laptop computers.

2.5 Bluetooth

Bluetooth (Bluetooth SIG, Inc., 2007) is a WPANs solution, which was designed to be a low-cost, medium-power, robust, short-range communication protocol for wireless links to replace cables (as the serial RS-232 interface) for mobile phones and computers. It is managed by the Bluetooth Special Interest Group (SIG). The IEEE approved and standardized older versions of the Bluetooth technology (Version 1.1 and 1.2) in the IEEE Standard 802.15.1 (IEEE, 2005b). Initially, Bluetooth allowed a data rate of 1 Mbit/s and with version 2 the Enhanced Data Rate (EDR) was introduced with new packet types based on different modulations allowing a data rate of 2 and 3 Mbit/s. Bluetooth covers, in comparison to IEEE 802.15.4 and IEEE 802.11, a complete product including

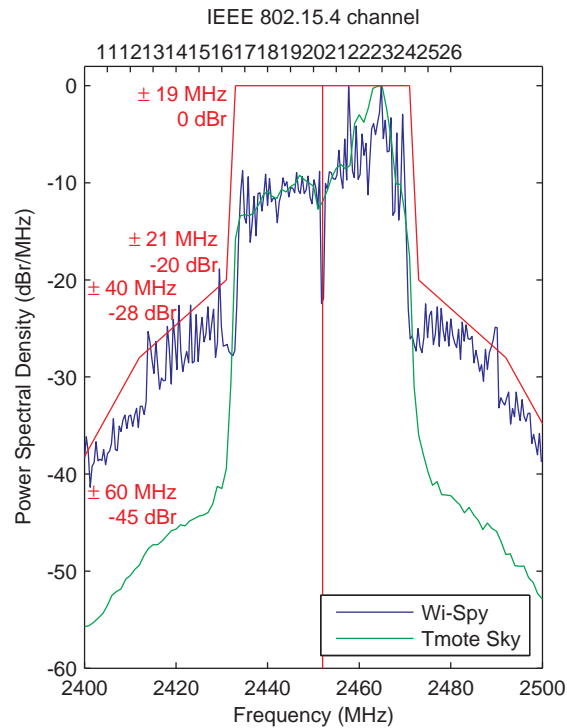


Figure 2.30: PSDs of IEEE 802.11n with channel bonding measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node. The plotted values are means of 1,800 values measured as 1 s max hold. The transmit PSD mask is plotted in red. The offsets of the curves have been aligned for better demonstration.

low level definitions for the radio and a full protocol stack including upper layers. Thus, it is comparable to ZigBee running on top of IEEE 802.15.4.

The network topology of Bluetooth consists of clusters, called Piconets. Up to eight devices form a Piconet. One device of them is the master of a Piconet, the others are slave devices. Piconets can connect to a Scatternet. The seven slaves of a Piconet are in active communication with the master. Up to another 248 ($= 256 - 8$) slaves can be passively attached to the master. They listen for synchronization and are able to become active at any time. This network topology is shown in Figure 2.31. Most Bluetooth devices participate only actively in a Piconet, and Scatternets are used very seldom, because most Bluetooth networks consist only of a few participants.

Bluetooth is still actively developed and Bluetooth Low Energy (Bluetooth SIG, accessed 10 September 2010), formerly known as WiBree (Hunn, 2006), is the latest extension of the standard in version 4. It covers scenarios for end devices with very low capabilities or limited energy resources. In contrast to classic Bluetooth, it has a lower application throughput and is not capable of streaming voice. The data rate is 1 Mb/s and the packet length ranges from 8 to 27 bytes. Instead of the Piconet/Scatternet topology, it uses a one-to-one or star topology. Over 4×10^9 devices can be connected by using a 32 bit address. This creates a partly overlapping use case with ZigBee, but Bluetooth does not support multi-hopping. Recent Bluetooth-supporting devices are named Smart or Smart Ready for the consumer market. Smart devices are Bluetooth Low Energy devices. Smart Ready means that a device, not being a Low Energy device itself, is able to connect to Low Energy devices. For instance, a chest strap of a fitness heart rate monitor using a small coin cell battery is a Bluetooth Low Energy device, advertised as Bluetooth Smart. The smart phone connecting to the chest strap supports the classical Bluetooth stack and the recent Bluetooth Low Energy version and is therefore called Smart Ready. However, Bluetooth Low Energy is not considered in this work, since it was not widely available at the time of writing.

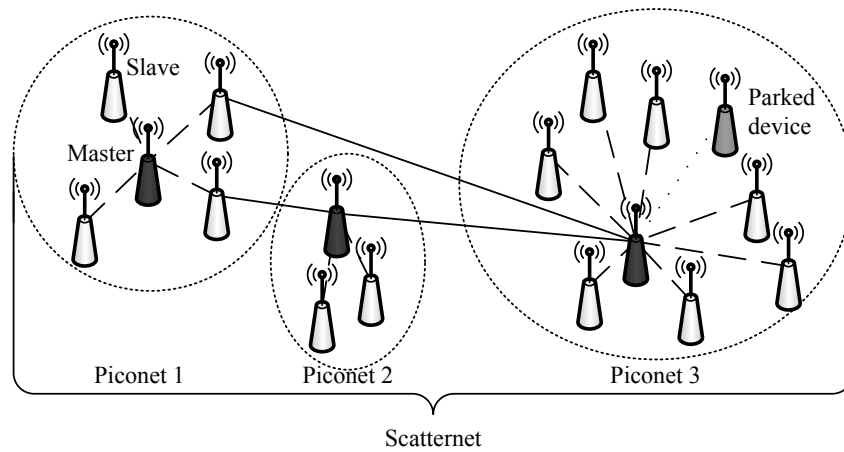


Figure 2.31: Bluetooth network topology. A Piconet consists of one master (dark gray) and up to seven active slaves (white); additionally, up to 248 devices can be passively attached as parked devices (light gray). A Piconet master can be a slave in another Piconet. Multiple Piconets can form a Scatternet.

Application				7 Application (Data)	
				6 Presentation (Data)	
				5 Session (Data)	
RFCOMM	Service Discovery Protocol	TCP/IP	Other	4 Transport (Segments)	
				3 Network (Packets)	
Logical Link Control and Adaption Protocol				2 Data Link (Frames)	Data Link
Link Manager Protocol					Media Access Control
Baseband				1 Physical (Bits)	
Radio Frequency					
Bluetooth				OSI-Model Layers (Data units)	

Figure 2.32: Comparison of the most important Bluetooth layers to the layers of the OSI Reference Model. In the higher layers, RFCOMM emulates serial cable communication and the Service Discovery Protocol identifies services, which are provided by other Bluetooth devices.

Further, note that throughout this work, only the “connection” state of Bluetooth is considered: there are other states, e.g. “inquiry” and “page”, which behave differently in the way that e.g. they have a channel hop rate of 3,200 hops/s. These other states are e.g. used during the connection setup, but not for the exchange of application data.

The layers of Bluetooth do not correspond fully to the OSI Reference Model, but for the sake of a clearly structured section, the differentiation of MAC and PHY Layer is made here: thus, Section 2.5.1 deals with the channel access timing, while Section 2.5.2 discusses the transmission and spectral features.

The Data Link Layer roughly corresponds to Bluetooth’s Link Manager Protocol (LMP) and Logical Link Control and Adaptation Protocol (L2CAP). At the PHY Layer, there are the so-called “Baseband” and “Radio Frequency” in the Bluetooth stack.

Figure 2.32 shows a mapping of the Bluetooth stack to the OSI Reference Model.

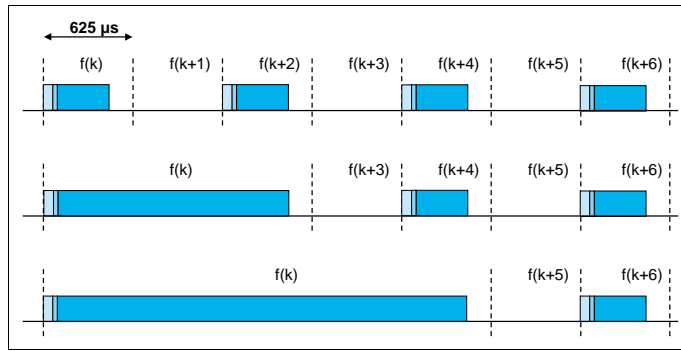


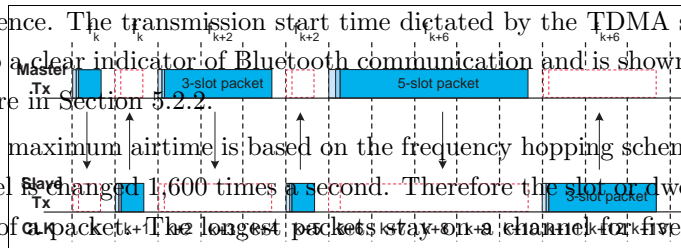
Figure 2.14: Single- and multi-slot packets.

Figure 2.33: Timing of single- and multi-slot packets. Taken from (Bluetooth SIG, Inc., 2007).

When the adapted channel hopping sequence is used, the pseudo-random sequence contains only frequencies that are in the RF channel set defined by the *AFH_channel_map* input. The adapted sequence has similar statistical properties to the non-adapted hop sequence. In addition, the slave responds with its packet on the same RF channel that was used by the master to address that slave (or would have been in the case of a synchronous reserved slot without a validly received master-to-slave transmission). This is called the *same channel mechanism* of AFH. Thus, the RF channel used for the master-to-slave packet is also used for the immediately following slave-to-master packet. An example of the same channel mechanism is illustrated in Figure 2.15 on page 80. The same channel mechanism shall be used whenever the adapted channel hopping sequence is selected.

2.5.1 MAC SUBLAYER

Bluetooth uses TDMA for channel access. Thus, the communication between the master of a Piconet and its slaves uses alternative time slots. The master polls data from the slave and the slave responds in the next time slot. Due to the scheduled access, the channel is not monitored with a CCA, since it is assumed to be at least free of internal interference. The transmission start time dictated by the TDMA scheme (as shown in Figure 2.33) is also a clear indicator of Bluetooth communication and is shown to be an important classification feature in Section 5.2.2.



The theoretical maximum airtime is based on the frequency hopping scheme. According to the scheme, the channel is changed 1,600 times a second. Therefore the slot or dwell time on a channel limits the airtime of a packet. The longest packets stay on a channel for five slot times, thus the maximum airtime of a packet is theoretically limited to 3.125 ms. However, the given time slot is a maximal duration, which should never be used fully due to guard times. As shown in the following, different packet types have different airtimes depending on their structure.

Another feature of Bluetooth's architecture is the support of five different logical links or also called logical transport types. The link types used for data traffic can be roughly divided into synchronous links, including Synchronous Connection-Oriented (SCO) and extended Synchronous Connection-Oriented (eSCO) links, and Asynchronous Connection-Less (ACL) links. The SCO links are normally used for voice transfer and are strictly based on single-slot packets, which are not retransmitted in case of a loss. The newer eSCO links are also used for voice transfer, but they support limited retransmissions and their packet lengths are more variable than the SCO packet lengths. The reliable ACL links are packet-based and can use one, three or five slots. Furthermore, it has to be mentioned that there are two additional link types, the Active Slave Broadcast (ASB) and Parked Slave Broadcast (PSB) links, which are only used for control and network maintenance and are not considered in the following. The link type determines the used packet.

For an overview of packet types and their features, see Tables 2.8 and 2.9. There are also ID, NULL, POLL and Frequency Hop Synchronization (FHS) packets, but they do not transport data and are neglected here.

Most Bluetooth packets are sent with 1 Mb/s and the packets have a simple format: they consist of an Access Code of 72 bit, a Header of 54 bit and the payload that can vary and reach up to 2754 bit. The resulting transmission durations can be computed and are shown in Tables 2.8 and 2.9. The Data Voice (DV) packet is an exception, since it carries voice and data and therefore the payload is split into an 80 bit voice field and a 45-150 bit data field.

If the packet type starts with a number, this number indicates the data rate, and the packet format is different as shown in Figure 2.34. The Access Code and the Header still add up to 162 bit and are transmitted with 1 Mb/s, but then a Guard Time of 5 μs and a Synchronization Sequence

Type	Payload header (bytes)	User payload (bytes)	FEC	CRC (2 bytes)	Maximum used slots	Maximum airtime (μs)
HV1	N/A	10	1/3	No	1	366
HV2	N/A	20	2/3	No	1	366
HV3	N/A	30	No	No	1	366
DV	1 for data part	10+(0-9) for data	2/3 for data	Yes for data	1	356
EV3	N/A	1-30	No	Yes	1	382
EV4	N/A	1-120	2/3	Yes	3	1582
EV5	N/A	1-180	No	Yes	3	1582
2-EV3	N/A	1-60	No	Yes	1	391
2-EV5	N/A	1-360	No	Yes	3	1591
3-EV3	N/A	1-90	No	Yes	1	388
3-EV5	N/A	1-540	No	Yes	3	1588

Table 2.8: Synchronous packet features, based on (Bluetooth SIG, Inc., 2007).

Type	Payload header (bytes)	User payload (bytes)	FEC	CRC (2 bytes)	Maximum used slots	Maximum airtime (μs)
DM1	1	0-17	2/3	Yes	1	358
DH1	1	0-27	No	Yes	1	366
DM3	2	0-121	2/3	Yes	3	1618
DH3	2	0-183	No	Yes	3	1622
DM5	2	0-224	2/3	Yes	5	2854
DH5	2	0-339	No	Yes	5	2870
AUX	1	0-29	No	No	1	366
2-DH1	2	0-54	No	Yes	1	375
2-DH3	2	0-367	No	Yes	3	1627
2-DH5	2	0-679	No	Yes	5	2875
3-DH1	2	0-83	No	Yes	1	375
3-DH3	2	0-552	No	Yes	3	1626
3-DH5	2	0-1021	No	Yes	5	2876

Table 2.9: ACL packet features, based on (Bluetooth SIG, Inc., 2007).

of 11 μs follow. The payload is then extended with a trailer of 2 or 3 bit, according to the data rate.

2.5.2 Physical Layer

Bluetooth’s physical communication is based on a slow frequency hopping scheme, thus the channel is changed after every transmission of a packet. It uses 79 channels, which are each 1 MHz wide and arranged adjacent to each other (see Figure 1.2).

The channel selection of the hopping scheme is based on a pseudo-random sequence and is adapted, when a channel is interfered, which is noticed by missing or corrupted packets. The Adaptive Frequency Hopping (AFH) tries to avoid interfered channels. This principle is illustrated in Figure 2.35a. AFH was introduced in Bluetooth version 1.2, while earlier versions supported only a static frequency and thus depends on the implementation. Nevertheless, it is stated in the standard that at least 20 channels have to be available for hopping (Bluetooth SIG, Inc., 2007).

The general Enhanced Data Rate packet format is shown in Figure 1.3. Each packet consists of 6 entities: the access code, the header, the guard period, the synchronization sequence, the Enhanced Data Rate payload and the trailer. The access code and header use the same modulation scheme as for Basic Rate packets while the synchronization sequence, the Enhanced Data Rate payload and the trailer use the Enhanced Data Rate modulation scheme. The guard time allows for the transition between the modulation schemes.

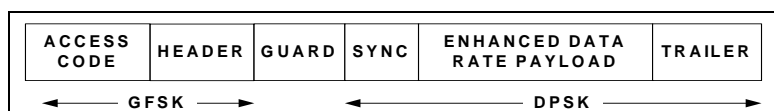


Figure 1.3: Standard Enhanced Data Rate packet format

Figure 2.34: The EDR packet format. Taken from (Bluetooth SIG, Inc., 2007).

1.1 BLUETOOTH CLOCK

Every Bluetooth device shall have a native clock that shall be derived from a free running system clock. For synchronization with other devices, offsets are used that, when added to the native clock, provide temporary Bluetooth clocks that are mutually synchronized. It should be noted that the Bluetooth clock has

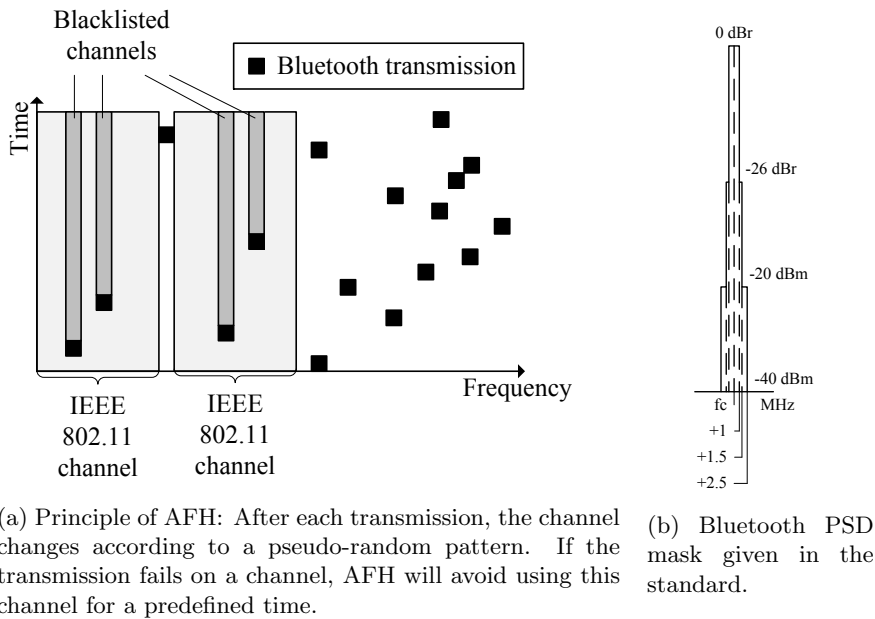


Figure 2.35: Bluetooth signals in the spectrum.

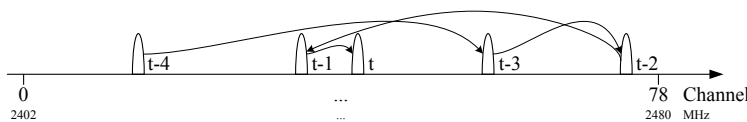


Figure 2.36: Bluetooth spectrum use due to channel hopping.

Bluetooth supports three different data rates based on three different modulations. The basic rate of 1 Mb/s is achieved with Gaussian Frequency Shift Keying (GFSK). When using EDR, the modulation is either changed within the packet to $\pi/4$ rotated Differential Quaternary Phase Shift Keying ($\pi/4$ DQPSK) enabling 2 Mb/s or to 8 phase Differential Phase Shift Keying (8DPSK) enabling 3 Mb/s for the rest of the packet. The details of the different data rates used within a packet, including the resulting airtimes, have been discussed in Section 2.5.1.

Bluetooth supports different transfer ranges/power classes. Table 2.10 shows the details for the different Bluetooth classes. Further, Bluetooth supports an adaptive power control and Channel Quality Driven Data Rate (CQDDR), thus Bluetooth adapts itself to the RF environment.

2.6 Microwave ovens

Microwave ovens are common kitchen appliances, found in many homes and offices, without any attention to emit waves outside the shielded cooking chamber. The food inside the oven is heated by dielectric heating that uses microwaves radiated by a magnetron. However, due to imperfect shielding some radiation escapes from the oven and thereby microwave ovens become unintentional radiators.

Power class	Maximum output power	Nominal output power	Minimum output power	Power control	Free-space range
1	20 dBm	N/A	0 dBm	Mandatory >4 dBm	≈ 100 m
2	4 dBm	0 dBm	-6 dBm	Optional	≈ 10 m
3	0 dBm	N/A	N/A	Optional	≈ 1 m

Table 2.10: Bluetooth power classes, based on (Bluetooth SIG, Inc., 2007).

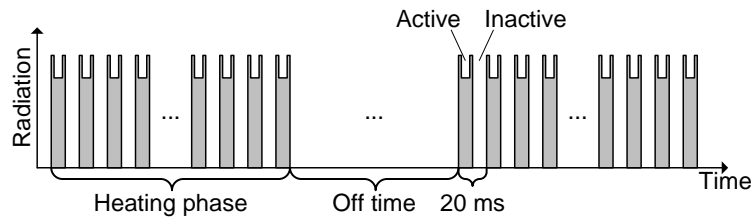


Figure 2.37: Typical radiation timing of microwave ovens. The user-set power level adjusts the length of the off time between heating phases. The active and inactive cycle is based on the 50 Hz frequency of the power supply.

2.6.1 Temporal Behavior

Although the spectral spread and the power of the leaking radiation differs, all three microwave oven models researched by the author show similar patterns: the strongest interference occurs on a channel close to IEEE 802.15.4 channel 20, which is around the stated microwave oven center frequency of 2450 MHz. The signal is periodic with a frequency around 50 Hz, which is the frequency of the power supply (for North America a frequency around 60 Hz can be expected as reported in (Rayanchu et al., 2011)). A period of 20 ms consists of an active phase and an inactive phase, which are roughly of the same length. The active phase has two maxima, one at the beginning and one at the end. In between them is a plateau. The height of this plateau differs depending on the oven model, the time and the channel, but it is generally higher as it is closer to the center frequency.

Furthermore, microwave ovens have different programs or different power levels that can be chosen by the user. However, the actual magnetron that emits the microwave radiation can only work at full power. The user-set power level is achieved by pauses between the heating phases. The active and inactive phases of a 50 Hz period are not altered. After a few seconds of heating, a few idle seconds are given for the heat to spread. This heat spreading times can be easily heard when the microwave oven is not buzzing and when only the ventilation and the turntable operate. These timing patterns are shown in Figure 2.37.

2.6.2 Spectral Properties

While IEEE Standard 802.15.4, 802.11 and Bluetooth are intentional radiators and as such, they apply a form of spectrum spreading to match a channel spectral mask, microwave ovens do not apply spectrum spreading as they are unintentional radiators. Most microwave ovens work around a center frequency of 2.45 GHz. Normally, some details, as the center frequency and power, are stated on a type plate on the back side of the oven. The spectrum spread and the amount of radiation leaking the cooking chamber depends on the actual model. In a National Telecommunications and Information Administration (NTIA) report by Gawthrop et al. (1994), a detailed measurement campaign of 13 microwave ovens is presented. Kamerman and Erkocevic (1997) and Azimi-Sadjadi et al. (2006) argue that the NTIA report draws pessimistic conclusions because of using peak measurements. Additionally to the microwave ovens commonly used in domestic areas, they discuss commercial ovens, which work with two magnetron tubes and generate a different interference pattern. These kinds of ovens, only to be found in gastronomy, are not considered further in this work due to their limited use.

Figure 2.38 shows an example of a measurement of the radiated energy 2 m away from the front of a Matsui microwave oven (the measurement method was equal to the one used for Figures 2.23, 2.29 and 2.30). Although the spectral spread and the power of the leaking radiation differs, all three microwave ovens (models by Matsui, Bush and Quelle) researched by the author show similar patterns: the strongest interference occurs close the stated center frequency of 2450 MHz,

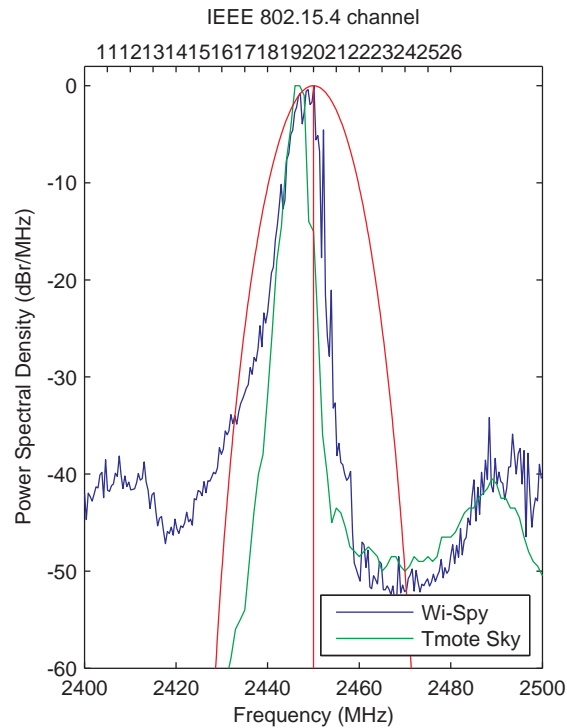


Figure 2.38: PSDs 2 m away from the front door of a Matsui microwave oven measured with Wi-Spy 2.4x and RSSI values of a Tmote Sky sensor node. The plotted values are means of 240 values measured at 1 s max hold. Estimated spectral width is plotted in red. The offsets of the curves have been aligned for better demonstration.

which complies with (Gawthrop et al., 1994; Kamerman and Erkocevic, 1997). In Figure 2.38, the peak is at around 2446 MHz and decreases to both sides. In red, an approximated spectral mask is plotted as it can be expected for most microwave ovens.

2.7 Other Technologies

After discussing the basics of IEEE 802.15.4, IEEE 802.11 and microwave ovens in extended detail, this section deals with other technologies that emit waves in the 2.4 GHz frequency band. These are mainly proprietary technologies as wireless input devices, which are commonly used for personal computers and are not based on Bluetooth. Furthermore, some wireless cameras or DECT phones can interfere in the 2.4 GHz frequency band.

The wireless input devices for personal computers that are not based on Bluetooth could be wireless presenters, keyboards or mice. For example, the company Logitech sells a proprietary wireless technology (Whitepaper, 2009) that has comparable features to Bluetooth-based devices, but uses frequency agility instead of frequency hopping. This means, the channel is only changed when it is interfered. The time series of RSSI readings from such a proprietary wireless device on a single IEEE 802.15.4 channel can be easily misinterpreted as Bluetooth. Both technologies send very short packets and, without additional knowledge of the spectrum, no clear distinction is possible.

Wireless cameras are increasingly based on IEEE 802.11 and thus can be seen as very active IEEE 802.11 clients, although there are some other models sold where no communication standard is given.

Another group of devices is formed by DECT phones, which support different frequency bands. European phones should not operate in the 2.4 GHz frequency band, but at 1.88 to 1.9 GHz (ETSI,

	IEEE 802.15.4	IEEE 802.11b & g	Bluetooth	Microwave oven
MAC Sublayer:				
Access scheme	CSMA/CA	CSMA/CA	TDMA/TDD	N/A
Topology	Star, peer-to-peer	Cell	Star	N/A
Maximum theoretical airtime	4,256 μ s	19,056 ... 371 ² μ s	2,876 ³ μ s	10,000 μ s
Minimum airtime (time of an ACK packet or shortest packet)	352 μ s	304 ... 24 ² μ s	366 ³ μ s	N/A
ED/CCA time	128 μ s	$\leq 15 \mu$ s / $\leq 4 \mu$ s	N/A	N/A
RX-to-TX time	$< 192 \mu$ s	$\leq 5 \mu$ s & $\leq 2 \mu$ s	N/A	N/A
PHY Layer:				
Maximum data rate	250 kb/s	≤ 11 & ≤ 54 Mb/s	1/2/3 Mb/s	N/A
Spreading scheme	DSSS	DSSS & OFDM	FHSS	N/A
Modulation	O-QPSK	DBPSK/DQPSK & BPSK/QPSK/16-QAM/64-QAM	GFSK/ $\pi/4$ DQPSK/8DPSK	N/A
Channels	16	13	79	1
Channel number k to frequency	$f_c = 2405 + 5(k - 11)$ MHz	$f_c = 2412 + 5(k - 1)$ MHz	$f_c = 2402 + k$ MHz	$f_c \approx 2450$ MHz
With k being	11 ... 26	1 ... 13	0 ... 78	N/A
Channel width ¹	2 MHz	22/20 MHz	1 MHz	≈ 30 MHz
Maximum transmit power	Theoretically 20 dBm	20 dBm	0, 4, 20 dBm (class dependent)	N/A

Table 2.11: Overview of the technologies operating in the 2.4 GHz frequency band. ¹Simple channel model. ²See Table 2.5 for details. ³See Tables 2.8 and 2.9 for details.

2005). However, some phones are reported to operate at 2.4 GHz (Rayanchu et al., 2011), but these are only used in North America.

2.8 Summary

This chapter gave an overview of the basics of communication and the principles used in IEEE 802.15.4, IEEE 802.11 and Bluetooth. IEEE 802.15.4 was reviewed in detail, from higher layers down to the PHY Layer, which is used in this work. Further, RSSI/ED and CCA, which are important for the rest of this work, have been discussed. For microwave ovens, the timing of channel occupation and the spectral spread have been researched. Finally, a short outlook on other technologies has been given.

In the next chapter, the hardware used for conducted experiments is introduced. In Chapter 4, the three main sources of external interference will be analyzed for their interference effects, hence the concepts introduced in this chapter are applied and set in relation to each other.

To sum up this chapter, a broad, high-level overview of the four discussed technologies operating in the 2.4 GHz band is given in Table 2.11. Since most of the technologies support different modes, the modes being relevant for this work and explained in this chapter, have been chosen to be presented in the table. For the MAC Sublayer, the timings give a rough impression on the duration of the channel use. In later chapters, the coexistence of the different technologies is researched and thus the numbers given in the table are a good orientation to estimate the probability of interference in the time domain. Also, the reaction timings are given in the form of the times needed for sampling an RSSI value or checking that the energy of the channel is below the CCA threshold. Furthermore, the time needed for the radio to change from the receiving state to the transmitting state (RX-to-TX time) are given. The PHY Layer rows reveal the data rate and modulation details, the spectrum allocation and the transmission energy.

In the literature, there are further comparisons and discussions for special use cases including advantages and disadvantages of all the different wireless technologies. For example, Sidhu et al. (2007) compares IEEE 802.11 with ZigBee, while Baker (2005) draws a comparison between Bluetooth and ZigBee for industrial applications.

Chapter 3

Research Methodology

After introducing all wave emitting technologies in the previous chapter, the following chapter explains the research process and its methods being applied in this work. This thesis is divided into three main parts: the effects, the classification and finally the mitigation of external interference. In all of these parts, a consistent set of hardware was used. Thus, Section 3.1 introduces and evaluates the hardware selection used, while Section 3.2 presents and discusses the software used.

3.1 Hardware used for Experiments

The IEEE Standard 802.15.4 is the main wireless technology researched in this work. For its practical part, the IEEE 802.15.4-compliant Tmote Sky sensor node was used and is discussed in the following. The interfering technologies are reviewed in Section 3.1.2.

3.1.1 IEEE 802.15.4

The Tmote Sky sensor node (Moteiv Corporation, 2006) is a typical sensor node built of commonly used components and can be found in many applications. The node is identical in construction compared to the TelosB sensor node (MEMSIC Inc., 2010b) and is supported by the major sensor node operating systems as TinyOS (Hill et al., 2000) and ContikiOS (Dunkels et al., 2004). The software used in the following is developed in ContikiOS 2.5 and its details are provided in Section 3.2. The radio chip of the Tmote Sky is its most important unit: it is a ChipCon CC2420 2.4 GHz Radio Frequency (RF) transceiver (Chipcon, 2004). In Table 3.1, the features relevant to the receiver and the Energy Detection (ED)/Received Signal Strength Indication (RSSI) of this radio are compared to the requirements of the IEEE Standard 802.15.4. With the help of an offset of approximately -45 dB (Chipcon, 2004), the RSSI value of the CC2420 radio can be roughly mapped to a dBm value indicating the power of the channel. An implementation detail to collect errorless RSSI readings is that the peak detectors in between the amplifier stages are activated (Boano et al., 2011b). Furthermore, Table 3.1 presents the jamming resistance requirements of the IEEE standard on the receiver side and the performance of the CC2420 radio. The channel center frequencies are 5 MHz apart from each other, thus the adjacent channel is 5 MHz and the alternate channel is 10 MHz offset, respectively.

Inter-node Variety

To test the practical work for representativeness and transferability, the Tmote Sky sensor nodes used here have been checked for device-depend varieties of the RSSI readings. The test campaign consists of three experiments, which are also illustrated in Figure 3.1a:

	IEEE 802.15.4 requirement	Typical value of a CC2420 radio	Unit	Comment
Sensitivity	<-85	-94	dBm	
Dynamic range	>40	100	dB	
Accuracy	± 6	± 6	dB	
Linearity		± 3	dB	
Average ED time	128	128	μ s	8 symbol periods
Adjacent channel rejection	0	39	dB	Desired channel ± 1
Alternate channel rejection	30	55	dB	Desired channel ± 2

Table 3.1: Selected parameter specifications for an IEEE 802.15.4-compliant receiver required by (IEEE, 2003b) and the corresponding specifications of a CC2420 radio (Chipcon, 2004).

Experiment 1 The receiving node was placed edge to edge to the fixed sending node in the way that the nodes' short sides, which are situated opposite the Universal Serial Bus (USB) connector, touched each other. It has to be mentioned, that the distances between the antennas were only close to zero, which is due to the size of the sensor node being bigger than its antenna. The sending node was set to transmit a modulated spectrum in the transmitter test mode at full transmit power of 0 dBm.

Experiment 2 The receiving node was placed 2 m away from the sending node. This time the nodes were aligned uniformly with a distance of 2 m between the short sides. The sending node stayed the same node.

Experiment 3 The receiving node had no signal to receive, thus the noise floor was measured without any interferer present in the RF anechoic chamber.

To guarantee repeatability of the results, every experiment was conducted three times in between which the experiment setup was changed. Therefore, eventual inaccuracies in the setup can be excluded (repeat=1,2,3). To minimize the random error, 100 measurements (each one second long) were recorded continuously. Each one-second-long measurement (m) itself consists of 8,192 samples, which were measured in a row and then transmitted to the data collecting laptop and the next measurement started. Thus, the collected data d can be described as $d(\text{node, experiment, repeat}) = \bar{m}_{n=1\dots 100}$. Furthermore, all tests were conducted in an RF anechoic chamber on channel 26, which is often free of any IEEE 802.11 interference, since this channel is out of the North American IEEE 802.11 band, which is also often used in Europe (as already mentioned in Section 1.1.4). All nodes were powered via their USB ports. Figure 3.1b shows a picture of a setup in the RF anechoic chamber.

The results of the measurement campaign are given in Figure 3.2. For each node, each experiment and each repeat a data point with error bars is plotted. The data points are the average of 100 measurements (mean of $(\bar{m}_{n=1\dots 100})$) and the error bars are given for \pm standard deviation. The standard deviation for a single instance of an experiment is so small that it can be neglected, the error bars are therefore sometimes hard to recognize in the plots. The differences between the repeats of an experiment are a bit greater, which could be due to misplacement or the imperfect alignment of the nodes. The maximum range of values for a single node varying between the repeats of the same experiment can be found in Experiment 2, in which the systematic error can also be assumed to be the highest, with a range of ≈ 4.45 dB in the RSSI values of Node 8. Different nodes measured different RSSI values for the same experiment setup. This difference is the crucial quantity of the measurement campaign: the inter-node variety. The highest inter-node variety can also be found in Experiment 2. The difference between the highest and the lowest value measured of any node in Experiment 2 is ≈ 7.38 dB. This includes not only the inter-node variety, but also the systematic error. Although there is a possible influence by these factors, the accuracy is better than the accuracy of ± 6 dB stated in the datasheet. Thus, the RSSI values measured by the Tmote Sky sensor node are a more than suitable metric and can be used not only for interference classification, but also e.g. for localization (Boukerche et al., 2009b).

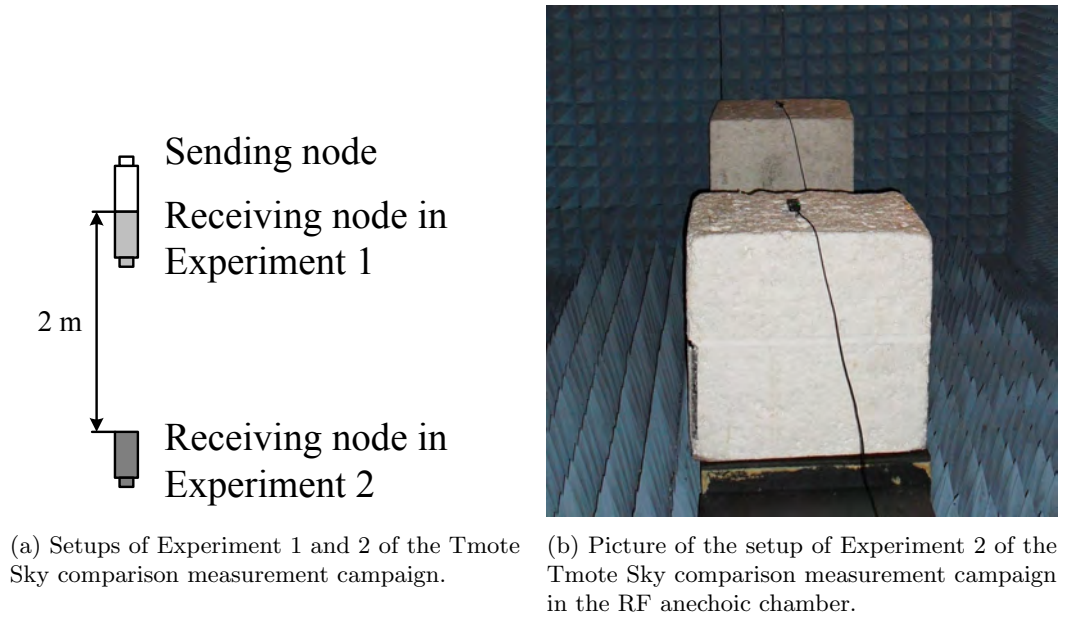


Figure 3.1: Tmote Sky comparison measurements.

While the just presented experiments aimed to evaluate the accuracy among sensor nodes and thereby to consolidate the rest of this work, Chen and Terzis (2010) performed a measurement campaign to show the inaccuracies and non-linearities of RSSI readings. They analyze the offset and linearity among sensor nodes and provide measurements inter alia of Tmote Sky nodes. A drawback of their study is that their experiments were conducted in a quite office space, which is less controlled than the RF anechoic chamber used here and suffers from effects as reflections and multi-path propagation. However, they suggest a calibration mechanism to overcome the non-linearity in the RSSI readings and thereby to improve the accuracy of the measurements. Although non-linearities were not researched here, it can be seen in Figure 3.2 that the differences between two experiments vary for different nodes, which supports the assumption of non-linearity. For example, the difference between Experiment 1 and Experiment 2 differs maximally between Nodes 6 and 7:

$$d(6, 1, \overline{\{1, 2, 3\}}) - d(6, 2, \overline{\{1, 2, 3\}}) \approx 46.14 \text{ dB} \quad (3.1)$$

compared to

$$d(7, 1, \overline{\{1, 2, 3\}}) - d(7, 2, \overline{\{1, 2, 3\}}) \approx 40.53 \text{ dB}. \quad (3.2)$$

The theoretically expected signal drop due to path loss is discussed in Section 4.2.2.

Srinivasan et al. (2008) report varying noise floors between different nodes ranging from -98 dBm to -92 dBm, measured in the TelosB-based Mirage (Chun et al., 2005) testbed. This 6 dBm range corresponds with the range of the results presented here.

Furthermore, Zhou et al. (2006a) present results showing inhomogeneous radio ranges in Wireless Sensor Networks (WSNs) based on experiments conducted with MICA2 (crossbow technology, inc, 2003) and MICAz (MEMSIC Inc., 2011) sensor nodes, with the latter using a Chipcon CC2420 radio. They divide into environment and hardware factors influencing the range, where the hardware factors include differences in output power, noise, and manufacturing differences. In the setup used here, the differences of the output power should have been minimized by powering the nodes via the USB ports and the background noise should have been at a minimum in the RF anechoic chamber. Thus, only manufacturing differences of the hardware should have been observed. Finally, they explain effects on the Medium Access Control (MAC) Layer, e.g.

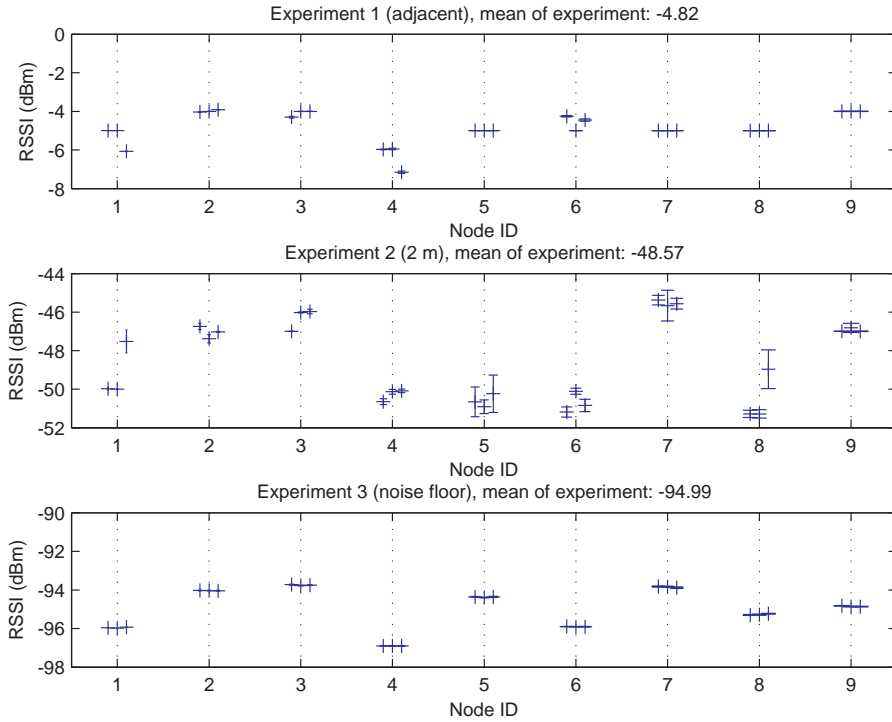


Figure 3.2: Comparison of node RSSI readings to evaluate inter-node variety. Estimated dBm = RSSI value + offset. Data points are average of $\bar{m}_{n=1\dots 100}$, error bars are \pm standard deviation, 3 data points next to each other correspond to 3 repeats of the same experiment on the same node.

failed channel reservations due to failed Request To Send (RTS)/Clear To Send (CTS) handshakes, because they rely on equal transfer ranges.

Nevertheless, for the purpose of this work the achieved accuracy without calibration is sufficient and has been used to monitor the 2.4 GHz frequency band. Besides the RSSI measurements of the Tmote Sky sensor nodes, another device, the Wi-Spy 2.4x, was used in this work (metageek, 2011). It is called a spectrum analyzer for Wi-Fi and is powerful enough for troubleshooting, Wireless Local Area Network (WLAN) deployment planning and RF site surveys, although it is not as powerful as a full professional spectrum analyzer that is used e.g. for radio chip development.

In the following, the possibilities and limits of these two low price solutions are reviewed.

Resolution Bandwidth

The resolution bandwidth is the bandwidth over which the power is measured. For the Tmote Sky, the channel is around 2 MHz wide and can be assumed to be the resolution bandwidth. This also implies that two adjacent Bluetooth signals being closer together than 2 MHz cannot be distinguished and that about three Bluetooth channels are measured at a time. Details about Bluetooth transmission have been introduced in Section 2.5.2.

Wi-Spy 2.4x offers a fine and adjustable bandwidth resolution with a minimum of 54 kHz. However, it suffers from a very long sweep time when used at its finest resolution.

Fully equipped spectrum analyzers also offer an adjustable video bandwidth. The IEEE standards also mention video bandwidths for measurements to check the mask of the Power Spectral Density (PSD). The video bandwidth is a low pass filter in the video circuit. When the video bandwidth is less than the resolution bandwidth, as e.g. required for spectral mask measurements in (IEEE, 2007), the displayed trace is smoothed and certain rapid spikes are not fully shown (Agilent, 2004).

Time Resolution

The time is the second dimension to be considered with regard to spectrum analyzing. The maximum sampling rate of the Tmote Sky for an RSSI reading is defined by the ED over an average of 8 symbol periods, which results in $128 \mu\text{s} \approx 7.8 \text{ kHz}$ (see Table 3.1 for details of the receiver and IEEE 802.15.4 requirements). This moving average of 8 symbol periods results in $128 \mu\text{s} / 8 = 16 \mu\text{s} \approx 62.5 \text{ kHz}$ as the shortest interval of any notable change of an RSSI reading.

This is the theoretical sampling rate of the radio, but for the full system there are further limitations. While the MSP430 microcontroller of the Tmote Sky runs fast enough at 8 MHz, the main limitation is the storage of the measured values, since the Random-Access Memory (RAM) of the used microcontroller has only a size of 10 Kbytes. Due to the operating, system fewer resources are available for the application. Further, the USB port interface allows the transfer of the data to the computer, but has only a limited throughput. A data rate of only $\approx 1 \text{ kHz}$ is achieved in a simple, naive implementation in ContikiOS, when the measured RSSI value is transmitted as an American Standard Code for Information Interchange (ASCII) string with the help of the USB serial port. ContikiOS provides such a simple version of a spectrum analyzer, which sends its measurements to a computer to display them (Eriksson, accessed: July 2013). TinyOS offers the same possibility (Dutra, accessed: July 2013).

Bloessl et al. (2012) present a framework to utilize a TelosB sensor node, which runs ContikiOS for spectrum scanning. Furthermore, they show its feasibility by detecting WLANs.

A highly optimized version of an RSSI scanner software, called Frossi, is presented in (Boano et al., 2011a; Dunkels et al., accessed: February 2012). It uses a boosted Central Processing Unit (CPU) speed, optimized Serial Peripheral Interface (SPI) operations and Run-Length Encoding. A resulting sampling rate of approximately 60.5 kHz for a single channel is claimed when using a buffer or around 11 kHz for streaming over the USB port. However, the sampling rate of Frossi is not always stable and thus not suitable for all applications.

Frossi measures a single channel/frequency (“zero span”), but other tools scan the whole frequency band with the help of sequential measurements at different frequencies. IEEE 802.15.4-compliant radios operating in the 2.4 GHz band have to support a range from 2.405 to 2.48 GHz with a frequency/channel selection adjustable in 5 MHz steps. In (Chipcon, 2004), the RF range is specified from 2.400 GHz to 2.4835 GHz, with a center frequency adjustable in 1 MHz steps. The frequency can be set to be outside the supported band, but this mode of operation is not specified and is thus ignored here. The channel switching time is an essential factor for the sampling speed, since the Phase-Locked Loop of the radio chip has to be re-calibrated. This decreases the sampling rate for a fully optimized version of a full spectrum scan to 3.4 kHz (Boano et al., 2011b).

Wi-Spy 2.4x offers a higher sampling rate of 5 kHz with the lowest dwell time of down to 20 μs at a 23 kHz step sweep. A zero span mode is not supported.

To identify sources of interference with the help of their spectral masks, a peak or quasi-peak mode can be used, thus the sampling can be done in high speed on the node and the output of the data has to be sent only in larger intervals. Thus, short spikes (as Bluetooth or higher data rates of IEEE 802.11) can be detected.

3.1.2 IEEE 802.11, Bluetooth and Microwave Ovens

For the practical interference tests presented later in this work, the following set of hardware was used. The hardware is listed in detail in Table 3.2 and in the following, it is referred to as the device name given in the first column¹.

¹For instance, when the word Laptop is used starting with an upper case letter, it stands for the model Dell Latitude E6400.

Device	Trade name	Specification
Laptop	Dell Latitude E6400	IEEE 802.11n (Intel WiFi Link 5300 AGN) Bluetooth 2.1 EDR (Dell Wireless 370 Bluetooth)
Netbook	Lenovo S9e	IEEE 802.11g (Broadcom adapter) Bluetooth 2.1 EDR (Broadcom 2046 adapter)
Access Point 1	Netgear N150 Wireless Router (WNR1000)	IEEE 802.11n
Access Point 2	AVM FRITZ!Box Fon WLAN7170	IEEE 802.11g
Headset	Samsung WEP-470	Bluetooth 2.1 EDR
Mobile Phone	Motorola Razr v3i	Bluetooth 1.2
Wireless Keyboard	Logitech diNovoMini	Bluetooth 2.0
Microwave Oven 1	Matsui	700 W
Microwave Oven 2	Quelle-Schickedanz AG	800 W

Table 3.2: Equipment used in the course of this work.

3.2 Software used for Experiments

Besides the hardware, different software has been used during the course of this work. In addition to the explicit naming of the software for each experiment, a short list with explanations of the software is provided in the following as an overview. The used software is ordered according to the time of the first use during the practical work and thereby, the following reflects the history of the development of the experiment setups.

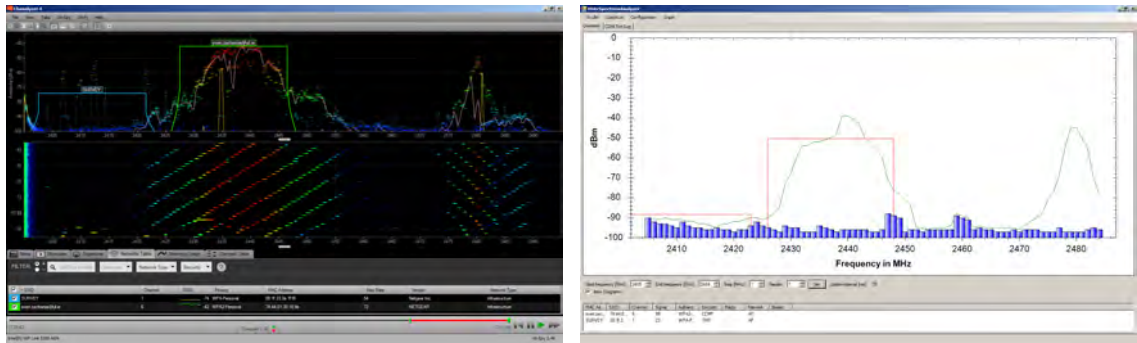
As already mentioned, ContikiOS (Dunkels et al., 2004) is the operating system of choice. In an initial phase of this work, the already introduced protocols X-MAC and Low Power Probing (LPP) (see Section 2.3.2) have been evaluated for their robustness against internal and mutual interference (Zacharias and Newe, 2011a,b; Zacharias et al., 2012b). This evaluation of WSN MAC protocols has revealed some of the basic weaknesses of MACs under interference.

Repeatable channel use patterns have to be generated with the hardware to extend the scope of interference from internal to external interference. Both traffic generators, which generate such repeatable patterns, and traffic monitors, which allow an evaluation of the interference, have been used in this work for in-depth experiments.

WLAN traffic with predefined characteristics has been generated with the help of Distributed Internet Traffic Generator (D-ITG) (Dainotti et al., 2012). The Jperf 2.0.2 software allows testing the maximum throughput of a link and by this, it generates saturated traffic (Richasse, accessed January, 2013). The Wireshark Network Protocol Analyzer (Combs, 2013) and the Microsoft Network Monitor 3.4 (Microsoft, 2010) have been used to monitor and to analyze IEEE 802.11 packets.

Bluetooth is harder to be utilized and monitored due to its full stack architecture, hiding more layers than IEEE 802.11 and IEEE 802.15.4. However, the traffic of the Bluetooth connections can be monitored on the Logical Link Control and Adaptation Protocol (L2CAP) layer with hcidump (Krasnyansky and Holtmann, 2002). This L2CAP layer roughly corresponds to the Data Link Layer of the Open Systems Interconnection (OSI) Reference Model (see Figure 2.32). The Wireshark Network Protocol Analyzer also allows analyzing the logs generated by hcidump.

Traffic and spectrum monitoring are important tools to gain an insight into the coexistence of the different wireless technologies and to understand possible mitigation strategies. Metageek Chanalyzer 4 and Chanalyzer Lab, which are software programs utilizing the Wi-Spy 2.4x hardware (metageek, 2011) have been used for spectrum monitoring. The hardware details of the Wi-Spy 2.4x device have been mentioned in Section 3.1.1. Further, the Frossi (Dunkels et al., accessed: February 2012) software has been used to monitor the spectrum based on RSSI measurements. Since Frossi is running on a Tmote Sky sensor node, the performance of this software solution is based on the used hardware (see Section 3.1.1).



(a) Metageek Wi-Spy 2.4x and Chanalyzer 4.

(b) Self-developed software utilizing Tmote Sky RSSI readings.

Figure 3.3: Screenshots of software programs for spectrum analyzing. A distant WLAN operates at 2,412 MHz, while a closer WLAN operates at 2,437 MHz. A Tmote Sky sends messages at 2,480 MHz. Although the Tmote Sky RSSI readings are less precise than the Wi-Spy 2.4x readings, they give an overview of the wireless environment.

The results of a time series of Frossi have been analyzed for unique patterns with the help of the data mining software WEKA (Hall et al., 2009). The resulting classification criteria have led to a first classification approach (Zacharias et al., 2012c).

The main drawbacks of Frossi, namely the unsteady sampling rate and the high workload, have been overcome with the development of the RSSI-based scanning tools programmed by the author. Thereby, a more reliable and fully embedded live classification algorithm has been enabled (Zacharias et al., 2012a), which has been finally improved to the algorithm presented in Section 5.3. Based on this knowledge of the wireless environment, Interference-Aware, Self-Adapting (IASA) MAC has been designed and its details are presented in Chapter 7. It uses the interference classification algorithm and smartly reacts to the class of interference.

In the course of this work, multiple RSSI collection software programs have been developed and used. The software Chanalyzer 4 shown in Figure 3.3a adds information of WLANs collected with the help of the Wi-Fi network card and thereby completes the Wi-Spy 2.4x measurements. Similar results can be achieved by using the Tmote Sky sensor node instead of the Wi-Spy 2.4x device, as shown in Figure 3.3b presenting a software developed by the author.

The channel can not only be monitored to detect interference, but interference can also be emulated with the help of a CC2420 radio. Boano et al. (2009a) and Boano et al. (2011b) show the use of the CC2420 radio to emulate external interferers. They use the radio chip test modes to create an unmodulated or modulated carrier. For table-top experiments and debugging, these test modes have been used for signal generation during the course of designing the algorithms presented later.

Finally, the software package MATLAB (MATLAB, 2009) has been used for computation, post-processing and visualization.

3.3 Summary

This chapter has introduced the equipment used, the software and the stages of this work. Since this work develops a software solution, the IASA MAC protocol, the author decided to base the development on commonly used inexpensive hardware. The presented tools allow a development process in multiple stages from theoretical analyses to experimental work. The development started at a well-controlled model phase, including the analysis of MAC Sublayers and the effects of external interference to the offline classification of recorded RSSI traces in MATLAB. In the next stage, the target platform, the Tmote Sky sensor node, is used directly for a more advanced version of the

interference classification algorithm. In the final stage, the improved reliable classification results have been used to mitigate the effects of interference by efficient strategies, which have been chosen based on knowledge about the external sources of interference.

In the next chapter, the results and findings of the initial stage, the effects of interference, are presented.

Chapter 4

Effects of External Interference

Interference is a central problem for all forms of wireless networks. In the previous chapter, the fundamentals of different technologies have been introduced and solutions within them, as Carrier Sense Multiple Access (CSMA)/Collision Avoidance (CA) and Time Division Multiple Access (TDMA) have been presented to avoid interference within a homogeneous system. However, the problem of interference is not limited to reactions within a system. It becomes severe when the interference is created by a device outside of the observed system. Thus, interference can be divided into:

Internal interference or competition for the medium is a problem that arises due the fact that multiple nodes of a network use a single, shared medium to communicate. If random access to the medium is used, collisions with other communication partners are likely to occur. The common approaches to overcome this problem and to increase the coordination of communication partners are scheduled access approaches as TDMA or conflict solutions as CSMA.

External interference, this term is also used in (Boano et al., 2011b; Bertocco et al., 2008) or also called cross-technology interference (in (Liang et al., 2010; Rensfelt et al., 2012; Tytgat et al., 2012)) or inter-technology interference (in (Petrova et al., 2006, 2007)). It occurs because a wireless medium (i.e. a specific Radio Frequency (RF)) is not exclusively reserved to a single technology. Thus, some wireless technologies can jam others. This type of interference causes at least one of the technologies to receive corrupted messages. This inferior system is the victim, while the stronger sender is the interferer. It might also be the case that messages of both parties are corrupted.

The latter is harder to manage, since the different network technologies do not coordinate each other and have no knowledge of each other. External interference is also the focus of this work and it is researched in further detail in this chapter.

Furthermore, a distinction can be made between the interference on the sender and the receiver side of the victim network. Mainly the receiver side is of interest, however throughout this chapter, the difference between both is discussed.

To get an overview of the topic, the literature is reviewed in the following, then models to estimate interference are discussed and finally the different scenarios are researched sorted by the different technologies. At the end of this chapter, a summary of the complex topic is provided.

4.1 Effects of Interference Reported in Literature

The ZigBee Alliance claims that ZigBee is robust against even the harshest RF interference. At the Hannover Messe, where multiple different wireless devices were presented and used, including at

Reference	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	Bluetooth	Microwave ovens
IEEE 802.15 Working Group (2010)	A			A	
Jennic (2008)	R	R		R	R
Sikora (2004)	E			E	E
Sikora and Groza (2005)	E			E	E
Boano et al. (2011b)	E			E	E
Azimi-Sadjadi et al. (2006)	A+E			A+E	A+E
Petrova et al. (2006)	A+E		A+E		
Petrova et al. (2007)	E		E		
Yuan (2011)	A+E		A		
Simek et al. (2011)	E				E
Shuaib et al. (2006)	E				
Khaleel et al. (2009)	E				
Penna et al. (2009)	E				
Liang et al. (2010)	E				
Thonet et al. (2008)	E		E	E	E
Chowdhury and Akyildiz (2009)	E				E
Herrera et al. (2008)	E				
Yang et al. (2011)	R	R	R		
Huo et al. (2010)	A+E			A+E	A+E
Howitt and Gutierrez (2003)	A				

Table 4.1: Literature on the effect of external inference on IEEE 802.15.4 (A=analysis, R=review, E=empirical).

least two Wireless Local Area Networks (WLANs), only 555 of 25,676 packets ($\approx 2.2\%$) were lost at the Network Layer (ZigBee Alliance, 2007). ZigBee adds higher layers, which provide e.g. channel management. Therefore, it is not equal to IEEE 802.15.4. Although claimed differently, ZigBee is not immune to interference. The amount of independently published research literature alone indicates the relevance of external interference for IEEE 802.15.4 and thereby for ZigBee. For an overview and to show the severity of interference, literature reporting about external interference is reviewed in the following. Mostly, IEEE 802.15.4-compliant radios are the victims of external interference, thus most literature describes the effects of interference on it. Table 4.1 gives a clear overview of literature dealing with IEEE 802.15.4 as victim. The review table divides the publications into:

- analytical approaches, including simulations and models (marked with “A”);
- reviews and discussions (marked with “R”);
- empirical work, including measurements and experimental work (marked with “E”).

Furthermore, the different sources of interference considered in the publications are exposed.

Since IEEE 802.15.4 and accordingly ZigBee are low power wireless communication standards, interference is one of the main challenges and has been partly considered in the annexes of the standards (IEEE, 2003b; ZigBee Alliance, 2008b). Further, the IEEE working group 802.15 has released a document dealing with the coexistence of Bluetooth and IEEE 802.11b (IEEE, 2003a), and more recently, a report on the coexistence of IEEE 802.15.4 with other IEEE standards (IEEE 802.15 Working Group, 2010). On the website (IEEE 802.19 Wireless Coexistence Working Group, accessed 20th June 2013) of the IEEE 802.19 task group, coexistence assurance documents can be found for all 802 standards.

Jennic (2008) presents an applied introduction for operators of Wireless Sensor Networks (WSNs) to the problem of interference on IEEE 802.15.4.

Deeper insight into the problem can be gained by reviewing the performance studies of IEEE 802.15.4 under interference done by the research community: Sikora (2004) and Sikora and Groza (2005) test IEEE 802.15.4 under the interference of IEEE 802.11b, Bluetooth and microwave ovens. Boano et al. (2011b) also test IEEE 802.15.4 under these interferers, but with a main focus on emulating interference with the help of IEEE 802.15.4-compliant radios. Azimi-Sadjadi et al. (2006) research the effects of IEEE 802.11 using Complementary Code Keying (CCK) modulation,

Bluetooth using Gaussian Frequency Shift Keying (GFSK) modulation, and two microwave ovens. They present simulations and experiments conducted in a testbed. The tests are not over the air experiments, but they use shielded boxes connected by coaxial cables and further equipment to simulate path loss and different sorts of interference. Petrova et al. (2006, 2007) focus on the effects of the coexistence with IEEE 802.11 and its different versions. Yuan (2011) develops a coexistence model of IEEE 802.11 and IEEE 802.15.4. Furthermore, he suggests some mitigation strategies. Simek et al. (2011) provide experiments of IEEE 802.15.4 under interference caused by IEEE 802.11 and a microwave oven. Additional to a laboratory setup, they also test a ZigBee deployment in a flat. More empirical studies can be found in (Shuaib et al., 2006; Khaleel et al., 2009; Penna et al., 2009; Liang et al., 2010; Thonet et al., 2008; Chowdhury and Akyildiz, 2009; Herrera et al., 2008). The reported Packet Error Rates (PERs) vary with the measurement setups, parameters and used devices. Especially for microwave ovens, which have no specifications as communication devices, the reported effects vary widely: From no effects at 1 m (Sikora, 2004; Sikora and Groza, 2005) to a PER of 67% for a 2 m away oven (Simek et al., 2011).

Baccour et al. (2011a) review literature about link quality estimators in WSNs, including interference experiments and mitigation strategies. They conclude some general observations:

- IEEE 802.15.4 is more affected by IEEE 802.11b networks than vice versa, when there is some signal overlap (the signals can spread outside the often assumed channel widths as explained in Chapter 2),
- Bluetooth mostly affects IEEE 802.15.4 and almost not vice versa, and
- microwave ovens can significantly affect IEEE 802.15.4 networks.

Besides empirical studies, many analytical studies have been conducted, delivering more or less complex and precise coexistence models. An extensive overview of all parameters effecting the coexistence of IEEE 802.15.4 and IEEE 802.11 is given in (Yang et al., 2011). Further, they provide an overview of coexistence models and show inherent (permanent) and on-demand solutions. Huo et al. (2010) show the effects of interference devices found in home environments, as IEEE 802.11, Bluetooth, microwave ovens and Digital Enhanced Cordless Telecommunications (DECT) phones, on IEEE 802.15.4. They give a theoretical model to predict the PER and simulations to prove it. Howitt and Gutierrez (2003) present a theoretical model of IEEE 802.15.4 and IEEE 802.11b interference. The interference of IEEE 802.11 on IEEE 802.15.4 is discussed most often in literature due to WLANs being almost omnipresent and due the complexity of IEEE 802.11.

Most of the presented studies concentrate on the effects of external interference on a simple IEEE 802.15.4 link between two nodes at the Medium Access Control (MAC) Sublayer. The most common object of study is interference on the receiver side of the victim network, also called receiver interference in (Tan et al., 2012) or channel collision interference in (Yang et al., 2011). The interference on the sender side of the victim network affects normally Energy Detection (ED)-based Clear Channel Assessments (CCAs) and leads to so-called carrier sensing interference (Tan et al., 2012) or channel occupation (Yang et al., 2011). For short distance links, the difference between sender- and receiver-side interference is small. Later in Sections 4.3.2 and 4.3.3, the modeling introduced in the following is used to give examples of the different ranges of sender- and receiver-side interference caused by IEEE 802.11 and Bluetooth.

Further factors, including e.g. the number of interferers, sending powers, distances, environments, modulations used by the victim and interferer and channel utilizations play an important role for each specific setup.

Since most WSNs duty cycle their radios to save energy, the problem becomes more challenging for real applications. Furthermore, the effects of interference on higher layers, i.e. for routing, have

Reference	IEEE 802.11 backs off for 802.15.4 IEEE 802.15.4 backs off for 802.11	IEEE 802.11 interferes 802.15.4 IEEE 802.15.4 backs off for 802.11	IEEE 802.11 interferes 802.15.4 IEEE 802.15.4 cannot sense 802.11
Yuan et al. (2007)	Region 1	Region 2	Region 3
Liang et al. (2010)	Symmetric region		
Huang et al. (2010)	Blind terminal	Exposed terminal	Hidden terminal

Table 4.2: Different ranges of interference and their names in literature, when IEEE 802.15.4 and IEEE 802.11 use an ED-based CCA mode.

still to be researched fully. An experimental study of the effects of interference on some common WSN MAC protocols is presented in (Boano et al., 2010).

4.2 Modeling of Interference

Due to the complexity of the interference, different models have been developed to estimate it, since the effects of external interference are an important factor for all wireless systems. In general, all models can be divided into Open Loop and Closed Loop interference modeling approaches, as done by Golmie (2006).

4.2.1 Mutual Effects: Open versus Closed Loop

Open Loop approaches do not take mutual effects between the two systems into consideration. These approaches are easier to compute, while Closed Loop approaches are simulations taking mutual effects of both systems into consideration. In the following, the mutual effects that can occur are reviewed for the common sources of interference.

IEEE 802.11

The mutual interactions of two systems, as IEEE 802.15.4 and IEEE 802.11, depend considerably on their CCA modes. Since IEEE 802.11 and IEEE 802.15.4 use CSMA/CA, eventually with an ED-based CCA mode, there can be mutual detection. Therefore, IEEE 802.11 can detect IEEE 802.15.4 traffic and back off for it (as e.g. stated in (Liang et al., 2010)) under certain circumstances. Depending on the signal strength measurable at the different radios, there are three regions of coexistence, if IEEE 802.11 and IEEE 802.15.4 use an ED-based CCA mode. Since these regions have no established names, Table 4.2 gives the names used in literature. The range of the regions increases from the region with mutual backoffs to the last region, in which only IEEE 802.15.4 is affected. The signal loss that is due to distance is called path loss and is described in further detail in Section 4.2.2. If a purely Carrier Sense-based CCA mode is used, IEEE 802.11 will not back off for IEEE 802.15.4 (as e.g. stated in (Tytgat et al., 2012; Gummadi et al., 2007)). Normally, the effect of IEEE 802.15.4 is insignificantly small and IEEE 802.11 can still corrupt IEEE 802.15.4 traffic, even when detecting it, since the timings of both technologies are too different.

Bluetooth

The situation is different for the coexistence with Bluetooth. Since the channel selection of Adaptive Frequency Hopping (AFH) is left open in the standard, it might mark used IEEE 802.15.4 channels as “bad” and avoid them. However, this case is very unlikely due to the low sending power and low channel utilization of IEEE 802.15.4. Normally, IEEE 802.15.4 is causing only little interference on Bluetooth links and the effect of Bluetooth interfering on IEEE 802.15.4 is worse, but still not critical.

Microwave Ovens

Obviously, microwave ovens do not react to any form of wireless network traffic around them. Therefore, Closed Loop approaches are not applicable for microwave ovens.

Open Loop Approach Structure

If not otherwise stated, all the Open Loop approaches presented in the following do not consider the fact that IEEE 802.15.4 can detect external interference and therefore, only receiver-side interference is considered. However, due to the relatively long time between the CCA and the actual transmission in the CSMA/CA algorithm of IEEE 802.15.4, the channel status might change too quickly. The hardware changing time from receiving to transmit mode (Receive (RX)-to-Transmission (TX) time) of the half duplex IEEE 802.15.4 radio is 12 symbol periods = 192 μ s (IEEE, 2003b). CCA is further reviewed as a possible interference mitigation strategy in Section 6.3.3. The fact, that there is normally little to no effect of IEEE 802.15.4 on other systems due to the already named reasons of low transmit power and low duty cycling (also see Section 4.3.1) supports the choice of simple Open Loop modeling approaches instead of complex Closed Loop simulations. Simple Open Loop modeling approaches are preferred to complex Closed Loop simulations, since there is normally little to no effect of IEEE 802.15.4 on other systems due to the already named reasons of low transmit power and low duty cycling (see Section 4.3.1).

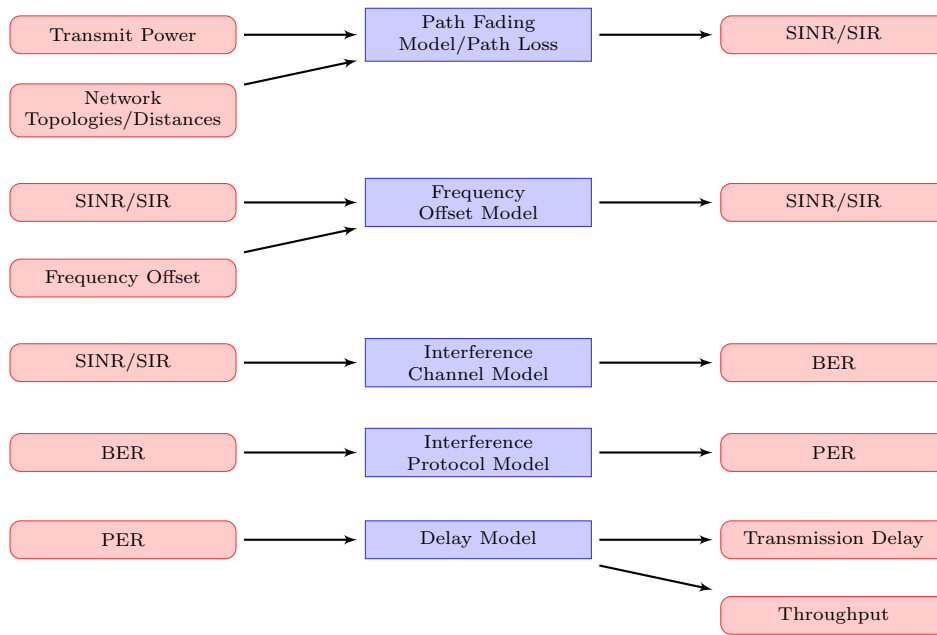
Yang et al. (2011) divide the modeling into multiple steps, at which each step is almost comparable to a module or layer as known in software engineering. Each module has in- and output variables. Further, they review different models for each module. An overview of the system is given in Figure 4.1a. In the following, these model layers are used as an outline. The actual models explained inside each layer might be different, since Yang et al. (2011) have limited their review to IEEE 802.11 and IEEE 802.15.4.

Another coexistence analysis developed by the IEEE based on the Annex E of the IEEE Standard 802.15.4 is presented in (IEEE 802.15 Working Group, 2010) and discussed here. In Figure 4.1b, the computation process of the interference estimation suggested in (IEEE, 2003a) is shown. Firstly, the transmit power of the interferer and the victim sender are reduced by the path loss to estimate the received power at the victim receiver (compare to “Path Fading Model/Path Loss” in Figure 4.1a/Section 4.2.2). Then, the interferer power is adapted by the spectrum factor to represent the actual interference in the IEEE 802.15.4 channel (compare to “Frequency Offset Model” in Figure 4.1a/Section 4.2.4). Based on this power the Signal to Interference Ratio (SIR) is calculated. With the knowledge of the used modulation, this ratio can be converted to the BER (compare to “Interference Channel Model” in Figure 4.1a/Section 4.2.5). The next step is to calculate the PER with the help of the computed BER (compare to “Interference Protocol Model” in Figure 4.1a/Section 4.2.6). In comparison to Yang et al. (2011) the Delay Model is missing, since its outputs do not give new insights into the level of interference and therefore, it is also not considered here.

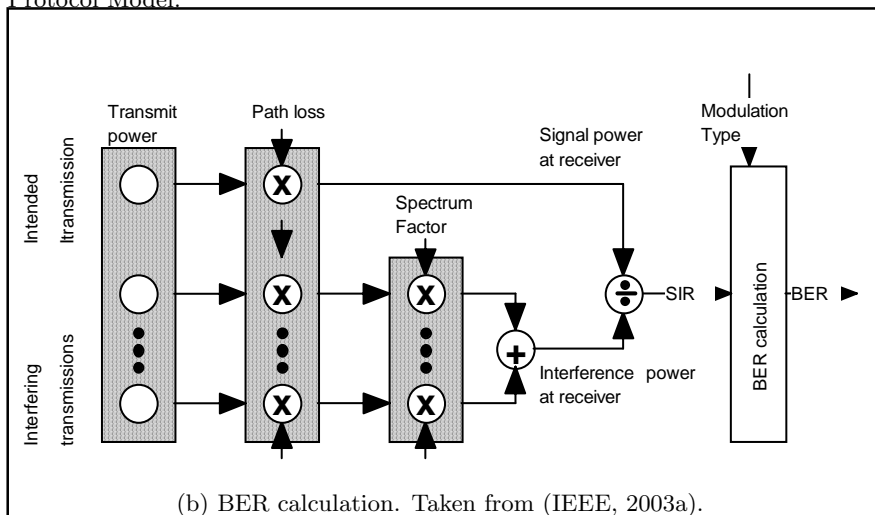
The next sections follow these steps in consecutive order and exemplarily present at least one model for each step, thus allowing to estimate the PER for the coexistence with IEEE 802.11 and Bluetooth at the end of this chapter.

4.2.2 Path Fading Model/Path Loss

The path fading model or path loss is the description of the attenuation of the radio signal transmitted from the transmitter to the receiver. It allows estimating the signal quality (strength) at the receiver. To be precise, the term path loss is a particular path fading model though it is often used for the general concept of path fading models. Therefore in the wider context of modeling



(a) Different modules (“Input/Output systems”) of a coexistence analysis, according to Yang et al. (2011). The variables shown on the right side are the red color variables and the left side are the blue variables. Outputs of one model are used as inputs for the next model. The modules can be combined from top to bottom with the possibility to stop before the bottom, e.g. with the PER returned from the Interference Protocol Model.



(b) BER calculation. Taken from (IEEE, 2003a).

Figure C.3—BER calculation

Figure 4.1: Flow of two Open Loop Methods to estimate the effects of external interference.

C.3.3 Spectrum factor

The spectrum factor represents the combined effects of transmitter and receiver masks as defined in G.3.5 and frequency offset.

In the telecommunications community, the term wireless channel model is also commonly used for fading models in general. Also, the origin of these models, which are closely related to the mechanisms used for wireless signals, the transmission frequency, physical layer, and spectrum factor of the same modulation type for receiver and transmitter with zero frequency offset is taken to be unity.

However, this work gives a short overview based on a computer science point of view, thus it attempts to bridge the gap between these two disciplines.

The SpectrumFactor() procedure defined in Annex D performs this operation for the IEEE 802.15.1 and IEEE 802.11b masks specified in C.3.1.

This section will start with a basic explanation of the path loss due to distance and the computation suggested by the IEEE. Then, the topic is discussed in more detail giving an outlook on the complexity of these estimation models and the physical background of wave propagation.

C.3.4 SIR computation

Path Loss

The SIR is given by the ratio of the received signal power to the total received interference power. The powers are calculated after the spectrum factor has been applied, and so this ratio corresponds to the value after path loss will be explained as a vital computation part for many estimation models in wireless networks. As commonly known, signal strength decreased with distance. This can also be Receiver noise is not considered in this model.

seen in the measurements shown in Figure 3.2. The Received Signal Strength Indication (RSSI) values are dependent on distance, which was changed between the experiments. For instance the drop from the mean of Experiment 1 (nodes adjacent to each other) to the mean of Experiment 2 (nodes 2 m distant) is roughly 43.75 dB. The energy at a receiver can be calculated based on the loss of the power flux density in space. Based on ideal free field circumstances (which are almost achieved in the RF anechoic chamber), it can be assumed that the power spreads as a sphere and the power loss is based on the surface of a sphere ($A_{surface} = 4\pi r^2$). Therefore, the commonly known Friis transmission equation is:

$$\text{Received power} = \text{transmitted power} \times \left(\frac{\text{wavelength}}{4\pi \times \text{distance}} \right)^2 \times \text{gain of transmitter antenna} \times \text{gain of receiver antenna} \quad (4.1)$$

The wavelength is calculated as traveling speed, which is the speed of light c , divided by the frequency f . Since the antennas are assumed to be ideally isotropic, i.e. the electromagnetic wave radiates/is received equally in/from all directions, their gain will be left out and the equation can be shortened to:

$$P_r = P_t \times \left(\frac{\lambda}{4\pi d} \right)^2 \quad (4.2)$$

with P_r being the received power and P_t the transmitted power. When this is put into the equation for signal levels:

$$L_{dB} = 10 \log_{10} \frac{P_1}{P_0} \quad (4.3)$$

where powers $P_1 = P_r$ and $P_0 = P_t$ are related to each other, the path loss PL resolves into:

$$PL_{dB}(d) = 20 \log_{10} \frac{\lambda}{4\pi d} \quad (4.4)$$

This leads to an attenuation of roughly 46.36 dB if a distance of 2 m for Experiment 2, a center frequency of 2480 MHz for channel 26 and the speed of light of 299,710,000 m/s¹ are assumed. The mean measured RSSI level at 2 m away from the permanent sender with 0 dBm was -48.57 dBm, which is 2.21 dB lower than expected. As just shown, this model is valid for short ranges and ideal circumstances.

However, only a direct line of sight with no obstacles is considered so far, but the chance of obstacles blocking the line of sight increases with greater distance.

Therefore, the simple path loss being based on the spherical propagation and described in Equation 4.4 is extended to the so-called log-normal fading:

$$PL_{dB}(d) = 10 \times n \times \log_{10} \left(\frac{d}{d_0} \right) + c + S \quad (4.5)$$

The path loss exponent n describes the attenuation of the signal over distance and $n = 2$ for free space propagation (compare to the combined factor $20 = 2 \times 10$ in Equation 4.4). Path loss exponents for different environments can be found in literature, e.g. in (Rappaport, 1996) as shown in Table 4.3 or a summary of exponents reported in the literature can be found in (Farahani, 2008). The constant c depends on the physical setup. The signal is further attenuated by shadowing, represented by random variable S (Liu et al., 2009). This shadowing variable S is based on a zero-mean Gaussian distributed random variable with a standard deviation σ , which is typically around 8 dB. Assuming the area of high probability under the Gaussian density function of $\pm 2 \times \sigma$, the additional gain/attenuation is with a very high probability (95.4 %) a factor between

¹The speed of light in vacuum is 299,792,458 m/s, but in air the speed is reduced, which has been taken into account here.

Environment	Path Loss Exponent n
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

Table 4.3: Path loss exponents for different environments. Taken from (Rappaport, 1996).

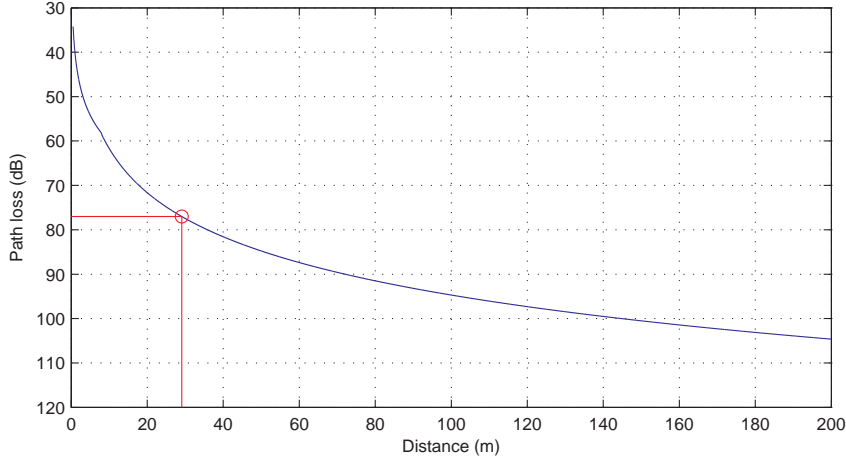


Figure 4.2: Path loss (dB) related to distance (m) in the 2.4 GHz band according to the indoor path loss model used in several IEEE 802 documents. The CCA threshold of -77 dBm (marked in red) is reached at ≈ 29 m when a sender transmits with 0 dBm.

16 dB ($40 = 10^{\frac{2 \times 8}{10}}$) and -16 dB ($0.0025 = 10^{\frac{-2 \times 8}{10}}$ based on $S = 10^{\frac{-\text{Gaussian random variable}}{10}}$) (Kumar et al., 2008).

By combining the last two models (Equations 4.4 and 4.5), the advanced path loss model found in (IEEE, 2003a) can be explained. It has a free-space propagation (Equation 4.4) assumed for line of sight for short distances of less than or equal to 8 m and is extended beyond this with a path loss exponent and a constant:

$$PL_{dB}(d) = \begin{cases} 40.2 + 20 \log_{10}(d) & \text{if } 0.5 \text{ m} \leq d \leq 8 \text{ m} \\ 58.5 + 33 \log_{10}\left(\frac{d}{8}\right) & \text{if } d > 8 \text{ m} \end{cases} \quad (4.6)$$

The wavelength λ is set for 2.45 GHz as the middle of the frequency band (Marquess, 1999). Its range of $\leq \pm 0.05$ GHz does not change the result significantly. Also, the speed of light c in air can differ fractionally. Further, the distance d below 0.5 m is not covered by these equations due to near-field effects.

The resulting relation of path loss to distance is plotted in Figure 4.2. The same equation is e.g. used in (Yuan et al., 2007) and (Yuan et al., 2010b) to calculate the ranges of interference, which have been introduced at the beginning of this section (see Table 4.2). This model is the common approach used in the WSN community, especially by computer scientists.

Experiments in Literature unveiling other factors

Additionally, it has been shown by practical experiments that the orientation of the node and thereby the orientation of its antenna influence the measured RSSI energy values at the receiver (Holland et al., 2006; Lymberopoulos et al., 2006; Polastre et al., 2005). Furthermore, physical parameters as temperature, humidity etc. can influence the radio hardware and the RF wave propagation. However, these factors can be ignored for indoor applications of sensor nodes.

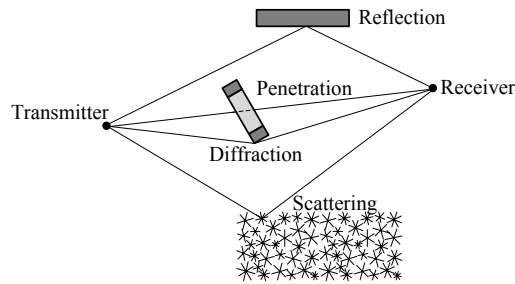


Figure 4.3: Different paths of signal propagation according to (Farahani, 2008).

Boano et al. (2009b) discuss the effects of weather conditions and ATmosphères EXplosives (ATEX) enclosures on the received power of Tmote Sky sensor nodes for outdoor deployments. They conclude that temperature has the highest impact, while rain is less significant and fog is almost negligible. In (Boano et al., 2013), the impact of temperature changes is researched in more detail and a first-order model is suggested to estimate the effect of temperature on the received signal strength. In summary, a 5 dB decrease is reported for the temperature span from 5 to 50°C for the used hardware. With higher temperature, the link quality decreases due to effects on the radio hardware.

Real world radio wave propagation

Furthermore, RF propagation in the real world includes antenna details and the following aspects (Farahani, 2008):

Penetration, which occurs whenever the signal hits an obstacle. The absorption depends on the carrier frequency of the signal, the hit angle, the material of the obstacle and its temperature.

Reflection, which occurs when the signal hits the surface of an obstacle. While a part might penetrate the obstacle, another part is reflected. The amount of the signal reflected depends significantly on the material, e.g. metal is a good reflector.

Diffraction that occurs when the signal path is blocked by a sharp edged obstacle. The signal is bent around the obstacle.

Scattering, which happens if the signal hits an obstacle that has a rough surface. Rough is defined as variations of more than $\frac{\lambda}{8}$, i.e. ≈ 1.5 cm, which is typically the case for trees or bushes.

Figure 4.3 visualizes four possible indirect non-line-of-sight signal paths that have not been considered so far. Bensky (2008) also gives an introduction into the mechanisms of radio wave propagation.

Small-scale fading

For a physically correct description of the wireless communication channel, so-called small-scale fading effects have to be considered. These effects are based on the fact that the transmitted signal is modulated on an electromagnetic wave, which as such has crests and troughs. Due to reflection, scattering and diffraction, multiple copies of the signal arrive through different paths at the receiver. These signals vary in amplitude due to different power losses along the way. Furthermore, the phase of these signals can be different due to the different distances passed. Therefore, the phase might be shifted by half a wavelength resulting in destructive addition or if the phase is aligned in constructive addition. Figure 4.4 shows a simple example, where a signal travels from the transmitter over multiple paths to the receiver. In the shown example, the direct

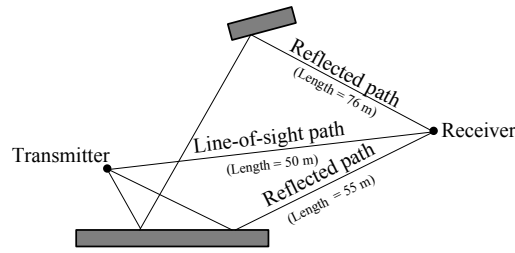


Figure 4.4: Multipath propagation: A simple example of multiple paths that a signal can take from the transmitter to the receiver due to reflections.

line-of-sight path has a length of roughly 50 m, but the indirect reflected paths are roughly 55 and 76 m long. Assuming a wavelength of around 0.1224 m, there is a significant phase shift possible between the different paths and the wave crests and troughs might be offset. Furthermore, different paths require different travel times, which might cause Inter-Symbol Interference (ISI). ISI occurs if the signal of one path is so much delayed that the next symbol already arrived at the receiver due to another more direct path. For this example, the travel times for the different paths at the speed of light are $\approx 1.668 \mu\text{s}$, $\approx 1.835 \mu\text{s}$ and $\approx 2.536 \mu\text{s}$, respectively. Due to the relatively long symbol period of IEEE 802.15.4 (16 μs), the change between symbols is no problem and no ISI occurs.

To take these small-scale propagation effects into account, all possible propagation paths have to be looked at, which makes the fading prediction comparable to a ray tracing technique. Therefore, these approaches are also called multipath channel models. Before giving an overview of the possible channel models, the effects caused by multipath fading are explained and grouped in the following.

First, it has to be distinguished whether the channel changes over time (time variant channel) or is constant (time in-variant channel) (Liu et al., 2009). For the latter, the estimation is simpler, since instead of a random process a random variable is sufficient.

Another differentiation is made between flat fading (narrowband channel) and frequency selective fading (broadband channel). For IEEE 802.15.4, flat fading is the more relevant case, since it uses a relatively narrow channel.

Due to moving the transmitter, receiver, and/or reflecting/scattering obstacles, a Doppler shift can occur, making the whole process of the channel estimation even more complex. The effect caused by the Doppler shift can result in either slow fading or fast fading (Liu et al., 2009; Mittag, 2012). For slow fading, the symbol period (16 μs for IEEE 802.15.4) is shorter than the coherence time. The coherence time indicates how long channel properties are stable. In the slow fading case, the received signal can be considered stable for the time the symbol is transferred. This is the most likely case for IEEE 802.15.4. If the coherence time is smaller than the symbol time, it is referred to as a fast fading channel. Especially, if the delay time spread is too long, ISI occurs, because a previous symbol is delayed so much that it interferes with the next one (Mittag, 2012).

The different effects caused by multipath fading are also summarized in Table 4.4.

Multipath Fading Models

Although a detailed look at the different multipath models is beyond the scope of this work, a rough overview and classification of them is provided in the following. Depending on the fading types, different models are suitable.

Since the ray tracing of every possible path is computationally expensive, stochastic models are frequently used to describe the paths in total instead of ray tracing each individual path. Similar paths can be grouped together and so-called Tapped Delay Line models are used (Mittag, 2012).

Channel properties	
Time-variant	Time in-variant
random process	random variable
Multipath time delay	
Flat/narrowband fading	Frequency selective/broadband fading
signal bandwidth < channel bandwidth	signal bandwidth > channel bandwidth
symbol period > delay spread	symbol period < delay spread
attenuation constant over the full signal	attenuation differs by frequency
Doppler spread	
Slow fading	Fast fading
low Doppler spread	high Doppler spread
symbol period < coherence time	symbol period > coherence time
channel variation slower than baseband signal variation	channel variation faster than baseband signal variation

Table 4.4: Different types of small-scale fading (Rappaport, 1996; Mittag, 2012).

Each signal on each path has individual properties: the attenuation and the phase describe the wave properties of the path. Thus, a complex number is an appropriate description (attenuation := absolute value of complex value, phase := angle of the complex value) of the received signal arriving at the receiver (compare to Section 2.3.3). All paths are combined by superposition and therefore, the signal at the receiver is computed.

Depending on the distribution of the different path properties, the fading is classified into different fading models, e.g. Rayleigh, Rician or Nakagami fading. (Liu et al., 2009).

Rayleigh fading means that no dominant line-of-sight path is present, thus only many indirect paths with roughly the same probabilities arrive. These weak multipath echoes, which are commonly considered to be the worst case, occur e.g. in highly built-up urban areas, forests or tree alleys (Fontán and Espiñeira, 2008). If the random components x and y of a two dimensional vector (or in this case the I and Q components of a complex number) are normally distributed and statistically independent of each other, the absolute value of this vector $\sqrt{x^2 + y^2}$ (or complex number) can be considered to be Rayleigh distributed. This relation results in a Rayleigh distributed amplitude and a uniformly distributed phase (Linnartz, accessed December, 2013). Although a further mathematical discussion is beyond the scope of this work, Figure 4.5 illustrates the effects of multiple incoming Rayleigh- and Rician-distributed paths for an intuitive understanding of the fading. Subfigure 4.5a shows the initially transmitted signal in the time domain and the corresponding constellation diagram of the complex representation of the signal at the sender. Without taking small-scale effects into consideration, the signal would be assumed to arrive at the receiver without any phase change and with an attenuated amplitude resulting in a correct angle. However, it would be represented as a shortened arrow in the constellation diagram. Subfigure 4.5b shows the signal at the receiver after passing through a Rayleigh fading channel. The phases of the different path signals are disordered and the resulting constellation point is incorrect.

The Rician fading model is also sometimes called Rice fading model (e.g. in (Fontán and Espiñeira, 2008)) due to its inventor Stephen Oswald Rice (Rice, 1944, 1945). It is used for a strong line-of-sight path with many indirect side paths. This is the case in e.g. open areas, crossroads or large squares (Fontán and Espiñeira, 2008). The resulting signal varies and its envelope has a Rician distribution. From the mathematical modeling point of view, the Rayleigh distribution is a special case of the Rician distribution. Similarly to the Rayleigh case, Subfigure 4.5c shows the signal at the receiver after passing through a Rician fading channel. Due to a dominant path, the incoming signals are less disordered and the resulting constellation point is correct.

The just mentioned variation in the incoming energy levels has a time frame much shorter than a symbol period, thus it cannot be observed via ED measurements. Nevertheless, a weak and strongly varying signal level can be expected if the signal of a Rayleigh fading channel is measured with a spectrum analyzer or field strength meter with a high enough time resolution. The Rician case would result in a stronger signal that varies less (Fontán and Espiñeira, 2008).

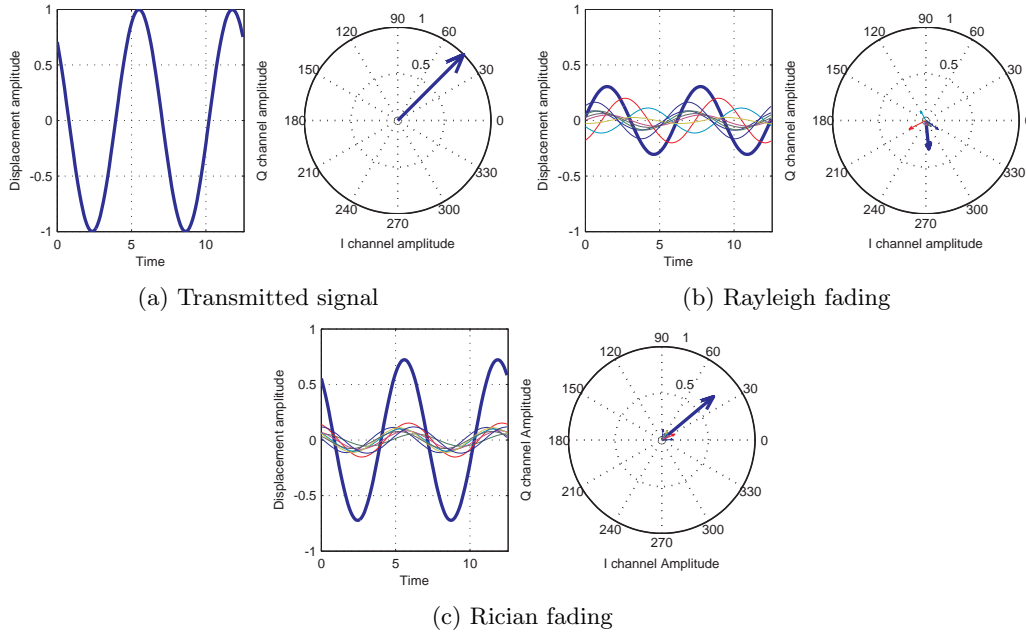


Figure 4.5: Small-scale effects of Rayleigh and Rician fading as simplified illustrative examples (only eight paths, the superposition of the signals is drawn bold).

Although the schematic plots in Subfigures 4.5b and 4.5c are limited to eight paths, the difference in variance can be clearly seen for the two different fading.

The Nakagami fading has to be mentioned for the sake of completeness. It offers a distribution that can be easily calibrated by measurements. Again, if the Nakagami Distribution is parameterized with $m = 1$, it is a Rayleigh distribution (Liu et al., 2009).

Azimi-Sadjadi et al. (2006) provide a short comparison of the channel models for IEEE 802.15.4, including Rayleigh and Rician fading. Matolak and Frolik (2011) claim that Rayleigh and Rician models may not be applicable for static WSNs and that appropriate channel models for WSNs are still an open research question. Additionally, they suggest a Two-Ray Model (Durgin et al., 2002) for static WSNs.

Summary and Outlook

Besides the just introduced models, there are several models/variations describing the channel or, even directly, the BER. The latter are known as binary channel approaches including e.g. the Gilbert-Elliot model. This model abstracts the channel as Markov Chain with a “good” and a “bad” state and thus predicts channel errors that occur in bursts (Gilbert, 1960).

Since the details of these models are beyond the scope of this work, Figure 4.6 gives a short overview and a possible classification of the different approaches. Further details and mathematical background of channel fading models can be found in literature (Rappaport, 1996; Liu et al., 2009; Kumar et al., 2008; Bensky, 2008; Fontán and Espiñeira, 2008).

In addition to the pure radio wave propagation, the tolerance levels of the transmitter hardware have to be taken into consideration (see Section 3.1.1).

4.2.3 Signal Ratios

With the knowledge of the signal attenuation, in the following generalized as path loss, it is possible to calculate the strength of different signals at the receiver. This is an important step to model interference and allows calculating some signal ratios.

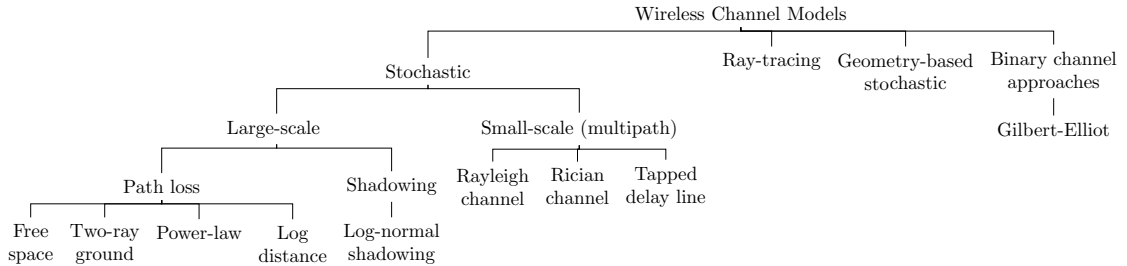


Figure 4.6: Overview of popular channel modeling approaches, based on (Mittag, 2012).

The ratio of signal power to interference power, the SIR, can be simply calculated as:

$$\text{SIR} = \frac{P}{I} \tag{4.7}$$

where P is the signal power at the receiver and I the sum of all interference signals at the receiver. For simple interference setups, the signal power P is the sender power reduced by the path loss and the interference signal I is computed equally for the interferer. However, when no interfering transmitter is present, the background noise is the interference signal limiting the range, thus the calculation of the Signal to Noise Ratio (SNR) is similar, but uses the noise power N instead of the interfering signal power I . Here, interference is assumed to be Additive White Gaussian Noise (AWGN), thus the SNR and the SIR can be used interchangeably. In (Azimi-Sadjadi et al., 2006), a comparison between the interference patterns and AWGN can be found. However, it is also important to note that interferers, based on modulations different to amplitude modulation, are not adding up as AWGN does (Golmie, 2006; Boano et al., 2011b). Thus, I is more likely to be the maximum and not the sum of all sources of interference. Further effects of the simplification are also relevant for the Interference Protocol Model (presented in Section 4.2.5) and are discussed later.

The Signal to Interference plus Noise Ratio (SINR) results when both sources of interference, the external interferer and the noise, are taken into account:

$$\text{SINR} = \frac{P}{(I + N)} \tag{4.8}$$

Normally, the noise is so small that it can be neglected in cases of external interference, since other non-ideal factors (as influences on the path loss or the non-ideal probability distribution of interference) have a greater influence. Further, for measurements (e.g. RSSI) that are done over the air and not with coaxial cables, the measured interference strength also includes the background noise.

Sometimes (e.g. in (Yang et al., 2011; Shin et al., 2007)), the SINR is calculated with an additionally Processing Gain (PG), which enhances the desired signal P :

$$\text{SINR} = \frac{P \times \text{PG}}{(I + N)} \tag{4.9}$$

The PG of Direct-Sequence Spread Spectrum (DSSS) is based on the relation of chip rate to bit rate and for IEEE 802.15.4 in the 2.4 GHz frequency band, it is (Golmie, 2006; Farahani, 2008):

$$\text{PG}_{dB} = 10 \times \log_{10} \left(\frac{2 \text{ Mb/s}}{250 \text{ Kb/s}} \right) \cong 9 \text{ dB} \tag{4.10}$$

If the signal is measured with the help of RSSI, there should be no processing gain added, since the definition of the ED in (IEEE, 2003b) states no attempts to identify or decode the signal.

However, since the PG is a constant summand in the logarithmic scale, it results in an offset of the SIR curve, which is discussed later in this chapter. The offset between computation and measurements is illustrated in Figures 4.8 and 4.12.

Tan et al. (2012) evaluates different interference prediction models including SNR and SINR. Although they are using IEEE 802.11 devices, their work still has relevance to IEEE 802.15.4. They conclude that SINR models show the best precision. However, they are using a testbed where the transmitters are cabled and therefore, they can precisely measure noise N and generated interference I independently of each other.

4.2.4 Frequency Offset Model/Spectrum Factor

The Frequency Offset Model (see Figure 4.1a) or Spectrum Factor (as shown in Figure 4.1b) are intermediate steps that consider the different channel widths, center frequencies and modulations of different standards. However, if the practical scenario allows RSSI measurements, received powers at the radios can be collected. This allows calculations with more precise SIRs and eliminates estimation imprecisions of the path loss and/or the spectrum factor. If no measurements are possible, estimations for the different interfering technologies are given in the following.

IEEE 802.11

IEEE 802.11 has non-hopping channels, which are wider than the channels of IEEE 802.15.4 and therefore, only a portion of the power transmitted by the interferer is allotted to an IEEE 802.15.4 channel. As previously mentioned, the common, simple channel width for IEEE 802.11 is given with 22 MHz. In the simplest model, a fully overlapped IEEE 802.15.4 channel can be assumed to be interfered with by $2 \text{ MHz}/22 \text{ MHz} = 1/11 \approx 9\%$ of the power emitted by IEEE 802.11. Thus, the received energy at the victim receiver is divided by eleven. This assumption is e.g. done in (Yuan, 2011). For channel bonding, resulting in a 40 MHz wide channel, the energy should still be divided by eleven, since two independent channels are bond together and there is no new modulation used.

Strictly speaking, the Power Spectral Densities (PSDs) of the modulations are not rectangular, which has been already pointed out in Section 2.4.3 and can be clearly seen in Figures 2.29 and 2.30. Hence, more detailed approaches can be used. For example, Soltanian and Dyck (2001) suggest modeling the DSSS modulation of IEEE 802.11b as sinc^2 function. This mode of calculation has e.g. been used in (Shin et al., 2007): a power of 17%, instead of the simple $1/11 \approx 9\%$, of the total power is calculated for a setup, in which IEEE 802.15.4 uses a center frequency of 2416 MHz (which is not an official channel) and IEEE 802.11b uses 2418 MHz (not an official channel, compare to Figure 1.2). For more complex modulations, as Orthogonal Frequency-Division Multiplexing (OFDM), this approach becomes more complex. Liu and Li (2004) give a derivation of the PSD for IEEE 802.11a, which uses the same OFDM as IEEE 802.11g, but operates in the 5 GHz frequency band. However, although a precise calculation becomes more complex due to the used sub-carriers, the overall shape is more rectangular for OFDM than for DSSS.

The IEEE document (IEEE 802.15 Working Group, 2010) uses the maximum transmitter spectral mask as the “absolute worst-case scenario”. The spectral masks for IEEE 802.11 are marked in red in Figures 2.29 and 2.30 in Section 2.4.3 of this work.

IEEE (2003b), the document behind the model shown in Figure 4.1b, provides a table with offset-factors for certain frequency offsets of IEEE 802.11b to Bluetooth and vice versa. To calculate these factor with normalized curves, the source code of a function (“SpectrumFactor()”) is given in Annex D of IEEE (2003b).

Bluetooth

Bluetooth differs from IEEE 802.11 in the following two points. Firstly, the channel and thus the center frequency is not fixed. The channel changes between 79 possible channels at a rate of 1600 Hz for single-slot packets.

Secondly, the channels of Bluetooth are 1 MHz wide and therefore narrower than the IEEE 802.15.4 channels with 2 MHz. However, an IEEE 802.15.4 channel covers three Bluetooth channels: two channels half and one channel fully (Gutiérrez et al., 2004). If the Bluetooth radio and the IEEE 802.15.4 radio are extremely close to each other, e.g. built into the same device, a bigger overlap can occur. Azimi-Sadjadi et al. (2006) assume IEEE 802.15.4 channels to be 5 MHz wide (defined by the adjacent channels). Nevertheless, they measure only a PER of 5% caused by a permanent, strong Bluetooth signal interfering their IEEE 802.15.4-based receiver. To be precise, a distinction between a spectrum factor and a channel overlap due to frequency hopping has to be made.

For the spectrum factor, a value of 1 MHz/2 MHz can be assumed. Consequently, Bluetooth is seen as a narrowband interferer by IEEE 802.15.4. This matches the 3 dB decrease given in IEEE (2003b) from a required minimum SIR of 5 dB for noise interference down to 2 dB for Bluetooth interference.

The hopping factor is the probability that the channel, to which Bluetooth hops to, overlaps with the IEEE 802.15.4 channel. If this is overlap is the case, the spectrum factor has to be used to calculate the power of the interfering Bluetooth signal received by the IEEE 802.15.4-compliant radio. From the given properties of both technologies, the hopping factor is defined as:

$$\text{Hopping factor} = \text{Channel overlap} \times \frac{1}{\text{Available Bluetooth channels}} = 3 \times \frac{1}{79} \quad (4.11)$$

Microwave Ovens

To the best of the author's knowledge, there are no widely accepted models for microwave ovens published. The author suggests to either measure the radiation for the specific model or to assume the interference spectral density to have its peak at around 2450 MHz, falling below the noticeable threshold at ± 20 MHz.

4.2.5 Interference Channel Model

Based on the SIR, the BER can be calculated. The BER is a link quality indicator, reporting the number of defect bits per time unit.

According to (IEEE 802.15 Working Group, 2010), the BER of IEEE 802.15.4 in the 2.4 GHz frequency band (i.e. using Offset Quadrature Phase-Shift Keying (O-QPSK)) can be calculated as:

$$\text{BER} = \frac{8}{15} \times \frac{1}{16} \times \sum_{k=2}^{16} -1^k \binom{16}{k} e^{(20 \times \text{SIR} \times (\frac{1}{k} - 1))} \quad (4.12)$$

when it is assumed that the interfering signal is similar to AWGN in the same bandwidth.

However, Schmidt et al. (2013) claim that, for packet corruption due to distance, the bit errors are not independently distributed within a packet. The distance results in a weak signal at the receiver and therefore, the SNR (their experiments were conducted in the absence of external interference) is so low that bits are corrupted. These defect bits occur in bursts: some bits are more likely to be corrupted than others (due to the coding) and some packet content is more prone to corruption than the content of other packets.

4.2.6 Interference Protocol Model

While the BER states the probability of a bit being erroneous, the PER is more relevant for networking, since a packet is the smallest resendable unit. Sometimes, the Packet Reception Rate (PRR) is used, which is the complement to the PER, calculated as:

$$\text{PRR} = 1 - \text{PER} \quad (4.13)$$

In general, a packet is assumed to be corrupted as soon as a bit of it is erroneous. If a Forward Error Correction (FEC) mechanism is used, a packet might be recoverable in case of a single bit error, but here these cases are ignored, since FEC is not provided by default in IEEE 802.15.4. Assuming that bit errors are independent events and that the system is under permanent interference, this leads to a simple conversion from BER to PER:

$$\text{PER} = 1 - (1 - \text{BER})^n \quad (4.14)$$

where n is the number of bits in a victim's packet.

It has to be mentioned that the assumption of bit errors being independent events is not true for external interferers, since modulated interference is, strictly speaking, no noise. Section 5.1 reviews approaches that even try to classify the source of interference based on, among others, the position of corrupted bits in a packet. Nevertheless, the calculation model presented here is a useful estimation.

Furthermore, the assumption that the system is under permanent interference is unrealistic, thus the timing of the external interferer has to be taken into consideration. In the following, a concept is presented that is described in (Golmie, 2006) as part of a packet error model. The parts of her concept used here have strong similarities to the “periods of stationarity” in the PHY Layer model presented in (IEEE, 2003a).

Golmie (2006) gives the following equation to compute the probability of a packet error $Pr(PE)$, which is equal to the PER:

$$Pr(PE) = \underbrace{\frac{n}{(C - N_A + 1)}}_{\text{Frequency Offset Model}} \times \underbrace{\frac{1}{T_{BI}}}_{\text{Time step weight}} \times \underbrace{\sum_{k=0}^{T_{BI}} (1 - (1 - \text{BER})^{T_C})}_{\text{Sum of all PERs at time steps k}} \quad (4.15)$$

The Frequency Offset Model can be ignored here, since it has been discussed in more detail in Section 4.2.4. For the sake of completeness, the variables are defined as follows. The value n is the number of frequencies of system A (victim) that are affected by transmissions of B (interferer). C is the number of available spectrum frequencies for A in MHz and N_A is the bandwidth of A . Basically, the spectral overlap with the support of channel hopping is provided. This model has been originally used for a case study of Bluetooth under IEEE 802.11b interference, thus frequency hopping was included.

The remainder of Equation 4.15 is more general and of further interest. While the last part of the equation looks similar to Equation 4.14, it is a time discrete simulation of all possible overlaps that can occur. Especially, the calculation of T_C , the number of interfered bits inserts an additional temporal component. This means that victim A tries to send a packet, which has an airtime T_A (for examples of airtime calculations, see the MAC section for the desired technologies: 2.3.2, 2.4.1, 2.5.1 and 2.6.1). The interferer B sends a packet every T_{BI} time units with an airtime T_B at a set sending interval. The time unit has to be chosen according to the data rate of the victim, thus a time step is equal to the time needed by the victim to transmit a bit.

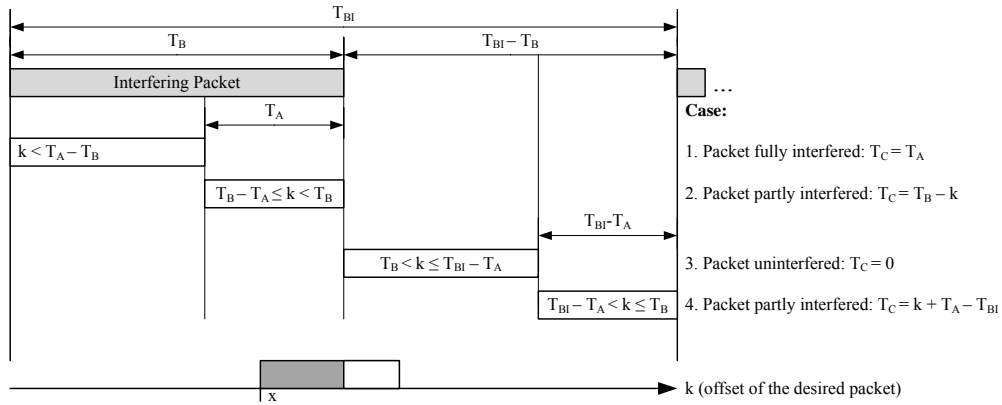


Figure 4.7: Different cases of packet overlap in the time domain that can occur when the victim packet is shorter than the interferer packet and fits in between two interferer packets.

The second factor, the “time step weight”, normalizes the time duration which is observed, with T_{BI} being the interval between two interfering packets as illustrated in Figure 4.7, which is also the run time of the simulation.

The third factor in Equation 4.15 is the sum of all PERs computed on all possible packet overlaps based on the BER. T_C is a number of discrete time steps of interference. It depends on T_A , T_B and k . The variable k is the discrete offset of the packet sent by victim A to the start of the interfering packet (see Figure 4.7). Thus, the value T_C is calculated depending on the setup, where three different setups are divided:

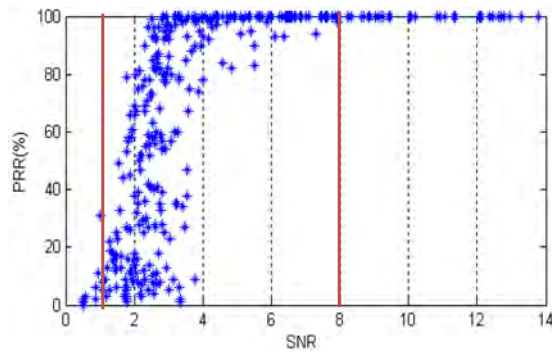
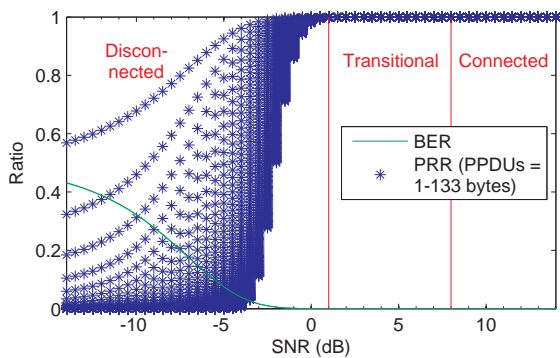
1. $(T_A \leq T_B)$ and $(T_A \leq (T_{BI} - T_B))$, i.e. the victim packet is smaller than the interferer packet and can fit in between two interferer packets
2. $(T_A \leq T_B)$ and $(T_A > (T_{BI} - T_B))$, i.e. the victim packet is smaller than the interferer packet, but does not fit in between two interferer packets
3. $(T_A > T_B)$, i.e. the victim packet is longer than the interferer packet, which is actually quite likely for IEEE 802.15.4 packets, since their data rate is orders slower than the data rate of most interfering systems and therefore, the airtime is relatively long.

T_C is then calculated for each of these setups depending on a specific k with the help of another case structure. For all the detailed cases, see Appendix B or (Golmie, 2006). In Figure 4.7, all T_C decisions for setup 1 are explained and the other cases can be understood similarly. From the figure, it can also be seen that a perfect CCA (with no delays) on the victim side would eliminate the interference of the first case ($k < T_A - T_B$) and the second case ($T_B - T_A \leq k < T_B$).

It has to be noted that the original Equation 4.22 in (Golmie, 2006) skips the case of $T_B = x$ due to a less-than-sign instead of a less-than-or-equal-to-sign. This has been corrected here, the case is resolved then to the logically correct $T_C = 0$ (first uninterfered packet after the interfering packet has been sent).

4.2.7 Connectivity Regions

While most Interference Channel and Interference Protocol Models require a few computation steps, including loops or sums, there is a simplified combination of both models mainly based on measurements: the connectivity regions of a link, or also called reception regions (in (Petrova et al., 2006)). This phenomena has been reported and/or researched extensively for low power wireless links (e.g. (Chen and Terzis, 2010; Boers et al., 2010; Seada et al., 2004; Srinivasan and Levis, 2006;



(a) Calculated relation of SNR to BER and PRR for IEEE 802.15.4. (b) Measured relation of SNR to PRR on TelosB sensor nodes sending with -25 dBm outdoors in the RadialE testbed [Baccour et al. 2011b]. Taken from [Baccour et al., 2011a].

Fig. 6. The PRR/SNR curve. For SNR greater than 8 dBm, the PRR is equal to 100%, and for SNR less than 1 dBm, the PRR is less than 25%. In between, a small variation in the SNR can cause a big difference in the PRR; links are typically in the transitional region. Outdoor environment, using TelosB sensor nodes and -25 dBm as output power (using the RadialE testbed [Baccour et al. 2011]).

Figure 4.8: Theoretical and experimental connectivity regions according to (Baccour et al., 2011a).
 Petrova et al., 2006)). Zunic et al. (2010) examined the distribution of PRRs over all links in the test-bed, for different Inter-Packet-Intervals (IPIs). They found that by increasing the IPI, the number of intermediate links increases as well. This finding was justified by the fact that low IPIs correspond to a short-term assessment of the link. In such short-term assessment, most links experience high temporal correlation in packets reception. That means that over these links, packets are either all received or not. Consequently, the measured PRR over most links is either 100% or 0%. For instance, Srinivasan et al. [2010] found that for a low IPI equal to 10 milliseconds (PRRs are measured every 2 seconds) 95% of links have either perfect quality (100% PRR) or poor quality (0% PRR), i.e., only 5% of links have intermediate quality. High IPIs corresponds to a long-term assessment of the link. The increase of the IPI leads to the decrease in the temporal correlation in packets reception. That means that links may experience bursts (a shift between 0% and 100% PRR) over short periods, and the resulting PRR assessed in long-term period is intermediate. This last observation was also made by Cerpa et al. [2005].
 Recently, several metrics were introduced for the measurement of link burstiness. Munir et al. [2010] define a burst as a period of continuous packet loss. They introduced B_{max} a metric that computes the maximum burst length for a link, i.e., the maximum number of consecutive transmission failures. B_{max} is computed using an algorithm that takes as input (i.) the data trace of packet successes and failures for each link, and (ii.) B_{min} , which is the minimum number of consecutive successful transmissions between two consecutive failure bursts. The authors assume a pre-deployment phase for the determination of B_{max} with respect to each link in the network. However, computed B_{max} values may change during the network operation due to environmental changes. Brown et al. [2011] resolved this problem by introducing BurstProbe, a mechanism for assessing link burliness through the computation of B_{max} and B_{min} during the network operation. The β factor is another metric for assessing link burstiness [Srinivasan et al. 2008]. It is used to identify bursty links with long bursts of successes or failures. The β factor is computed using conditional probability distribution functions (CPDFs), which determine the probability that the next packet will be received after n consecutive successes or failures. It requires a large data trace and thus might be inappropriate for online link burstiness assessment.
 an experiment conducted by the author is presented, which confirms these values.

Figure 4.8: Theoretical and experimental connectivity regions according to (Baccour et al., 2011a).
 Petrova et al., 2006)). Zunic et al. (2010) examined the distribution of PRRs over all links in the test-bed, for different Inter-Packet-Intervals (IPIs). They found that by increasing the IPI, the number of intermediate links increases as well. This finding was justified by the fact that low IPIs correspond to a short-term assessment of the link. In such short-term assessment, most links experience high temporal correlation in packets reception. That means that over these links, packets are either all received or not. Consequently, the measured PRR over most links is either 100% or 0%. For instance, Srinivasan et al. [2010] found that for a low IPI equal to 10 milliseconds (PRRs are measured every 2 seconds) 95% of links have either perfect quality (100% PRR) or poor quality (0% PRR), i.e., only 5% of links have intermediate quality. High IPIs corresponds to a long-term assessment of the link. The increase of the IPI leads to the decrease in the temporal correlation in packets reception. That means that links may experience bursts (a shift between 0% and 100% PRR) over short periods, and the resulting PRR assessed in long-term period is intermediate. This last observation was also made by Cerpa et al. [2005].
 Recently, several metrics were introduced for the measurement of link burstiness. Munir et al. [2010] define a burst as a period of continuous packet loss. They introduced B_{max} a metric that computes the maximum burst length for a link, i.e., the maximum number of consecutive transmission failures. B_{max} is computed using an algorithm that takes as input (i.) the data trace of packet successes and failures for each link, and (ii.) B_{min} , which is the minimum number of consecutive successful transmissions between two consecutive failure bursts. The authors assume a pre-deployment phase for the determination of B_{max} with respect to each link in the network. However, computed B_{max} values may change during the network operation due to environmental changes. Brown et al. [2011] resolved this problem by introducing BurstProbe, a mechanism for assessing link burliness through the computation of B_{max} and B_{min} during the network operation. The β factor is another metric for assessing link burstiness [Srinivasan et al. 2008]. It is used to identify bursty links with long bursts of successes or failures. The β factor is computed using conditional probability distribution functions (CPDFs), which determine the probability that the next packet will be received after n consecutive successes or failures. It requires a large data trace and thus might be inappropriate for online link burstiness assessment.
 an experiment conducted by the author is presented, which confirms these values.

The connectivity region approach does not return a BER, thus to use Equation 4.15 the BER can be assumed to be one and a simplified model can be used to calculate the effects of packet-based interference. Thus, if the SIR is below the SNR threshold of the Connected Region, interference is strong enough to corrupt the packet of the victim and any collision is assumed to result in a packet loss (BER = 1). Therefore, the chance of a packet collision can be simplified to

$$Pr(PE) = \begin{cases} \frac{T_A+T_B}{T_{BI}} & \text{if } \frac{T_A+T_B}{T_{BI}} < 1 \\ 1 & \text{if } \frac{T_A+T_B}{T_{BI}} \geq 1 \end{cases} \quad (4.16)$$

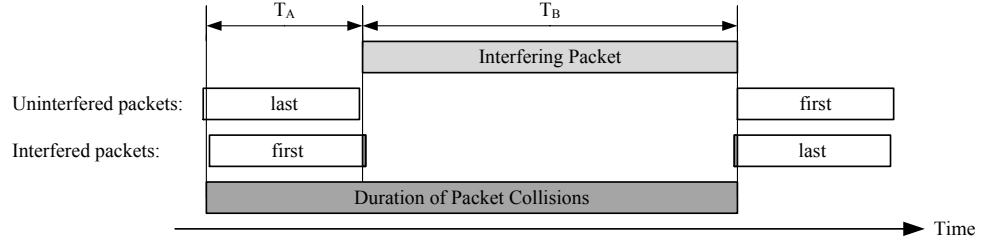


Figure 4.9: Overlap of victim and interfering packet. The victim needs to be uninterfered for its full airtime T_A and is interfered during airtime T_B of the interferer packet, resulting in a time span $T_A + T_B$ where no uninterfered transmission is possible.

if $T_{AI} > T_{BI}$ and no frequency hopping is used. The $T_{AI} > T_{BI}$ condition is likely to be fulfilled, since WSNs have normally longer sending intervals than IEEE 802.11 or Bluetooth. Thus, if the victim wants to send a packet at any random point in time, the channel is busy for a time T_B . Since the packet itself has to be transmitted fully uninterfered for a time T_A before the start of interference, both time durations are added up. This is also illustrated in Figure 4.9 (compare to the free channel duration of $2T$ required for pure ALOHA, illustrated in Figure 2.2a).

In order to predict packet collisions, a slightly different approach can be used for interference caused by a channel hopping technology as Bluetooth with a slot time (corresponding to T_{BI}) that is shorter than T_A . Equation B.4 from setup 3 ($T_A > T_B$) of (Golmie, 2006) can be used and with $N := N(X = 1 \dots T_{BI})$, being the number of potential collisions, it can be resolved to:

$$N = \frac{\overbrace{\left(\left\lceil \frac{T_A}{T_{BI}} \right\rceil\right)}^{\text{Case 1}} \times \overbrace{\left(T_{BI} \left\lceil \frac{T_A}{T_{BI}} \right\rceil - T_A\right)}^{\text{Condition 1}} + \overbrace{\left(\left\lceil \frac{T_A}{T_{BI}} \right\rceil + 1\right)}^{\text{Case 2}} \times \overbrace{\left(T_{BI} - \left(T_{BI} \left\lceil \frac{T_A}{T_{BI}} \right\rceil - T_A\right)\right)}^{\text{Condition 2}}}{\underbrace{T_{BI}}_{T_{BI} \text{ discrete steps for original } X}} \quad (4.17)$$

This can be simplified to:

$$N = \frac{T_A + T_{BI}}{T_{BI}} \quad (4.18)$$

Assuming that any collision leads to a corrupted IEEE 802.15.4 packet, the right (a non-overlapping) channel has to be chosen N times in a row. Thus, the probability of a packet collision and thereby error $Pr(PE)$ is:

$$Pr(PE) = 1 - \left(\frac{\text{Non-overlapping Bluetooth channels}}{\text{Available Bluetooth channels}} \right)^{\frac{T_A + T_{BI}}{T_{BI}}} \quad (4.19)$$

This non-overlapping channel fraction is equal to $(1 - \text{hopping factor})$, as described in Section 4.2.4. The sending interval of the Bluetooth interferer is $T_{BI} = 625 \mu\text{s}$, at least for single-slot packets. The airtime of the victim IEEE 802.15.4 packet can be calculated according to Section 2.3.2.

A comparison of the BER-based approach and connectivity region approach shows that the latter is more realistic, especially when the connectivity regions have been specified in experiments with the specific radio.

Figure 4.8 gives this comparison of the two approaches presented in this section: the BER-based approach and connectivity region approach for permanent interference or noise. In Subfigure 4.8a, a comparison of calculated values to the thresholds is given and in Subfigure 4.8b, the measurements by Baccour et al. (2011a) defining these thresholds are shown.

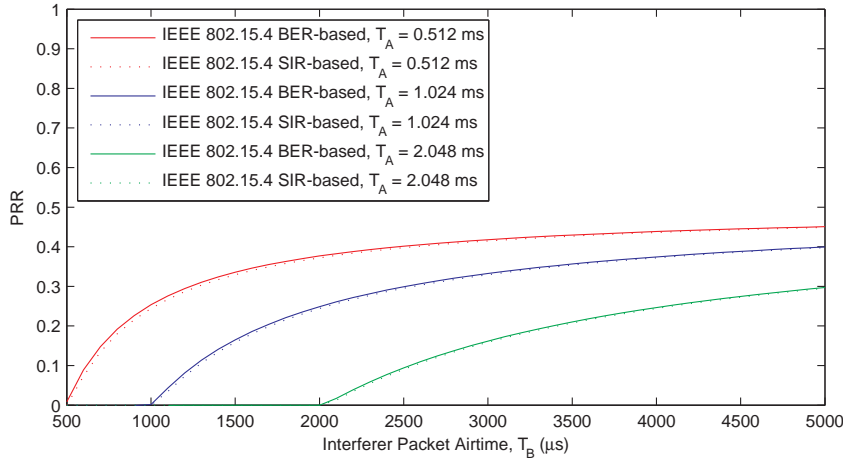


Figure 4.10: Comparison of the BER-based and connectivity region estimation for different IEEE 802.15.4 packet length under IEEE 802.11 interference. The interferer sends with 20 dBm at 20 m distance of the victim receiver, the sending power within the IEEE 802.15.4 channel is assumed to be $2/22$. The victim sender sends with 0 dBm 15 m away from the victim receiver. Thus, a SIR of -5.46 dB can be computed at the victim receiver. This means the SIR is in the Disconnected Region and the resulting BER is 9.585%. The interferer channel utilization is constant at 50% with $T_{BI} = 2 \times T_B$.

The connectivity regions are also easier to calculate than the BER-based approach using Equation 4.12, which is an additional advantage.

4.2.8 Delay Model

Delay Models compute, as the name suggests the delay of a transmission and therefore, a metric of the Data Link Layer.

Shin et al. (2007) define the transmission delay to be the time between the packet being located at the head of the sending queue and the reception of an Acknowledgment (ACK) packet from the receiver. Therefore, this delay includes backoff, CCA, transmission of the packet, waiting for an ACK packet and the reception of the ACK packet. For this, important factors are both the backoff strategy of the CSMA/CA algorithm and the duty cycling of the radio in a low power MAC.

With the help of the delay, the throughput can be calculated. The throughput is the amount of data that can be transferred per time unit. Delay models are beyond the scope of this work and are not reviewed further.

4.2.9 Example

After introducing the different steps needed to estimate the effects of interference, all aspects are summarized and exemplarily explained in this section.

In Figure 4.10, the different models are combined to calculate the PRR of different IEEE 802.15.4 packets under IEEE 802.11 interference. The assumed setup is as follows: The interferer is an IEEE 802.11 device 20 m away from the victim receiver sending with 20 dBm. The power at the receiver can be calculated with the help of the path loss. For the frequency offset, $2/22$ of the interfering power is assumed to be within the IEEE 802.15.4 channel. In the victim network, the sender transmitting at 0 dBm is 15 m away from the receiver. Thus, a SIR of -5.46 dB can be assumed for a try of a reception under interference.

This SIR is clearly in the Disconnected Region. Further, a BER of 9.585% can be computed based on Equation 4.12. This BER shows that a packet collision is very likely to corrupt at least one bit of a packet and thereby the full packet. The airtimes of the IEEE 802.15.4 packets are

0.512, 1.024 and 2.048 ms, which correspond to a Physical Protocol Data Units (PPDUs) with sizes of 16, 32 and 64 bytes, respectively. The packet airtime of the interfering IEEE 802.11 packet varies from 0.5 ms to 5 ms. The sending interval is always $T_{BI} = 2 \times T_B$, resulting in a channel utilization of 50% for all cases. In the figure, it can be seen that both methods show similar results, with the BER-based approach delivering insignificantly more positive estimations. The implications of the different packet lengths are not of interest here, but are discussed in Section 6.3.2. At this stage, it is sufficient to sum up the results shown in Figure 4.10 as the logical conclusion that packets can only be successfully delivered when there is an uninterfered time period longer than the victim packet airtime. Furthermore, the channel utilization of 50% is an ultimate upper limit for the amount of successfully deliverable packets. thus the PRR has to be lower than 50%.

For this setup, the results of the BER-based and the SIR-based approach match well with only insignificant differences. However, from Figure 4.8a it is obvious that there is an offset between both approaches. For example, if the distance of the victim sender to the victim receiver of the previous example is decreased to 10 m, the resulting SIR decreases to 0.35 dBm, which is still in the Disconnected Region, thus the victim still loses its packet as shown in Figure 4.10. However, the resulting BER drops to 0.0072% and therefore, the effect of interference is obsolete, since almost no packet is corrupted. Hence, there are cases where both models deliver different results. These cases are due to the offset that can be seen in Figure 4.8a between the calculated PRRs in blue and the region thresholds marked in red.

This offset was further investigated and experimentally validated by the author. To eliminate the number of unknown variables or unnecessary complexities, the setup included only Tmote Sky sensors nodes, as victims and interferer. The interferer was set into a test mode to generate the permanent interference that is defined as modulated pseudo-random sequence (Chipcon, 2004; Boano et al., 2009a). Therefore, the expected results are similar to a SNR-based approach using long distances to increase the path loss as done by Baccour et al. (2011b) instead of using active interference. The experiments were conducted in an RF anechoic chamber with two sensor nodes as victims and one as interferer. They were all powered via their Universal Serial Bus (USB) ports and operated on channel 20. Thus, there is no frequency offset. The setup is shown in Figure 4.11. The victim nodes were placed on a base line 2.5 m away from the interferer and 0.5 m away from each other on the ground with the battery pack touching the floor. The interferer, Node 6, was also placed on the ground and was permanently sending a modulated test signal. The resulting distance between the interferer and the victims on the circular arc is 2.51 m. The expected path loss for both distances calculated with the help of Equation 4.6 is also shown in Figure 4.11.

A significant difference between computed path loss and real path loss was observed between the two victims because of their short distance: the path loss from Node 2 to 3 was measured to be 29 dBm and the other direction 26 dBm when tested with -10 dBm sending power. The expected path loss was 34.18 dBm for 0.5 m. However, for the short distance of 0.5 m, Equation 4.6 is not fully suitable and it is not recommended to use the equation for closer proximities due to near field effects. Nevertheless, the distances of the setup were limited due to the dimensions of the RF anechoic chamber. The RF anechoic chamber being available to the author is 2.50 m \times 6.50 m, but not fully usable due to the lining with pyramidal radiation-absorbent material. Additional to the imprecisions at close proximities, the orientation of the nodes is an important factor. The antennas are not fully isotropic. The used orientation of the nodes is also shown in Figure 4.11: They have been positioned in such a way that the short sides without the USB connectors of the victim nodes were facing the same short side of the interferer. From the experience of the author, the orientation should not be disregarded for measurements, since the radiation pattern is not perfectly omnidirectional (see (Moteiv Corporation, 2006) for plots of the antenna patterns).

Different combinations of sending powers and interference powers have been used to achieve different SIRs. Then the SIR was measured for each setup individually. For each setup, a number

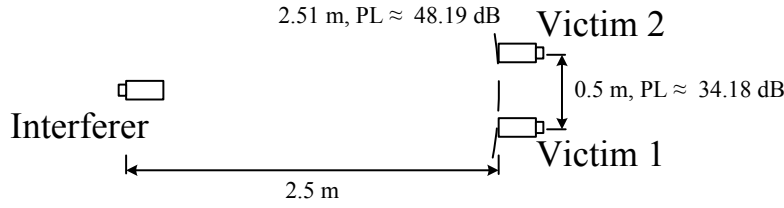


Figure 4.11: Setup in the RF anechoic chamber for SIR-PER experiment (interferer = node 6, victim 1 = node 3, victim 2 = node 2).

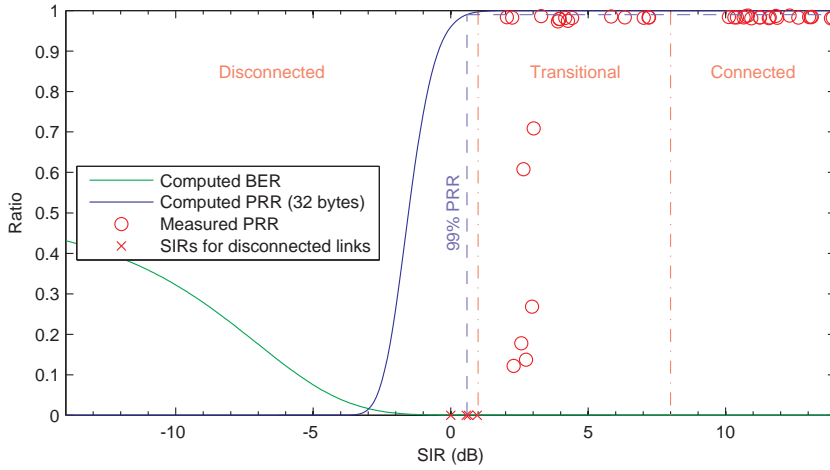


Figure 4.12: Calculated relation of SIR to BER (Equation 4.12) and resulting PRR versus measured data points for IEEE 802.15.4. Additionally, the theoretically computed 99% PRR threshold and the thresholds given in (Baccour et al., 2011a) are shown for the different connectivity regions.

of 10,000 packets, each 32 bytes long, was sent in an interval of 100 ms without any CCA. The whole experiment ran fully automatically overnight. For the most interesting SIR setups, i.e. in the Transitional Region, tests were repeated. Since the SIR was calculated from RSSI measurements, a small variance between repeats of experiments can be seen.

Figure 4.12 shows the measured SIR-PRR values, the calculated BER and PRR curves and the thresholds of the connectivity regions. The results lead to two main conclusions: Firstly, the real PRR in this experiment is worse than the calculated PRR resulting from the BER, which supports the introduced three regions and the thresholds of (Baccour et al., 2011a). Secondly, the Transitional Region, assumed at a SIR between 1 dBm and 8 dBm, is not linear, which supports the definition of the connectivity regions. For example at a SIR of ≈ 2 dB, the lowest SIR of a connection, the PRR was significantly higher than at measurements at higher SIRs. Since the Transitional Region is relatively narrow (7 dBm as measured by (Baccour et al., 2011a), it is problematic to estimate the behavior of a specific node in it. If the actual signal at the receiver can only be estimated, multiple factors will make this estimation imprecise, e.g.:

- The antennas used for sensor nodes are imperfect isotropic antennas.
- The path loss calculation presented here is based on an ideal environment. Real indoor environments can lead to different signal losses.
- The power of the sender might vary due to manufacturing reasons or due to different battery power levels.

Even when the RSSI values measured at the victim are used and the just given sources of error are eliminated, the given accuracy of ± 6 (compare to Table 3.1 and Section 3.1.1) for a Tmote Sky leaves enough space to be either in the Connected or Disconnected Region.

Besides the fact that the here used model was mainly taken from IEEE documents, (IEEE, 2003b) also states that a typical low-cost implementation can be expected to fulfill the 99% PRR at a SNR of 5 to 6 dB. Bertocco et al. (2007) report a similar offset between theoretical and measured PER. They generate interference, thus they relate their PER curves to the SIR. For an interferer power of -25 dBm measured at the Tmote Sky sensor node with the help of RSSI, they observe an offset of 5 dB to the calculations. They explain this offset by channel and system non-idealities or impairments due to channel dispersion, hardware and software errors.

4.3 Effects Related to Technologies

After providing a literature overview and an extensive insight into different modeling approaches, the findings are summed up and categorized for the different interfering technologies. Although research has provided an extensive number of publications and models, the amount of possible combinations and vendor-specific hardware characteristics make the problem of coexistence still an open and active research field.

4.3.1 IEEE 802.15.4 as Interferer

IEEE 802.15.4 is very unlikely to seriously cause packet loss to IEEE 802.11 or Bluetooth. The output power of less or equal to 0 dBm, as supported by most sensor nodes, limits the effects on other technologies. To avoid the effects of IEEE 802.11 on IEEE 802.15.4, which are more intense than the opposite direction, a channel that is not or only little overlapped by IEEE 802.11 will normally be chosen. However, if this is not possible, an IEEE 802.15.4 transmitter appears as a narrowband interferer to IEEE 802.11 and therefore, the processing gain of the spread spectrum used by IEEE 802.11 reduces the impact of IEEE 802.15.4. The coexistence can only become critical if IEEE 802.11 and IEEE 802.15.4 are operating closely together, e.g. they are built into a single device and IEEE 802.15.4 utilizes the channel heavily. With the transmitter test signal, which permanently blocks the channel, the author was able to cause an IEEE 802.11 connection to disconnect and the WLAN was not detected by the Laptop anymore. The WLAN had a center frequency at 2437 MHz and the IEEE 802.15.4 transmitter of the Tmote Sky was sending at 2435 MHz with 0 dBm. The Tmote Sky was plugged into the USB port of the Laptop. A channel utilization of around 50% led to a data rate drop in the WLAN, but still did not force a disconnect, even when the sensor node was as close to the IEEE 802.11 card as possible. A more realistic channel utilization as 1% left the IEEE 802.11 connection without noticeable effects. Yoon et al. (2006) suggest a distance of more than 4 m between both radios to limit the effects of IEEE 802.15.4 on IEEE 802.11 to be negligible. Further analyses can be e.g. found in (Howitt and Gutierrez, 2003) and (Golmie et al., 2005). In (Sikora, 2004), experiments show the SIR drop caused by IEEE 802.15.4.

The effect of IEEE 802.15.4 on Bluetooth is limited, since only three of 79 Bluetooth channels are overlapped and thus no noticeable degradation of the Bluetooth link will take place due to frequency hopping. Even with a permanently blocked channel, the AFH scheme can avoid these channels and therefore minimize the packet loss. Additionally, IEEE 802.15.4 uses roughly twice the bandwidth of Bluetooth and therefore it appears to be a wideband interferer. Hence, only about half of the already low emitted energy of IEEE 802.15.4 is within a Bluetooth channel. The author is not aware of any reported problems of a Bluetooth connection in literature caused by IEEE 802.15.4.

Obviously, on microwave ovens there are no effects of interest.

4.3.2 IEEE 802.11 as Interferer

As seen in the previous chapters, IEEE 802.11 is a very complex standard with multiple modes and varying setups. Additionally, IEEE 802.11-based WLANs are omnipresent nowadays in most environments. A site survey and the attempt to avoid channel overlap between IEEE 802.11 and IEEE 802.15.4 (channel alignment) might not always be possible and/or successful. In TinyOS and ContikiOS, the default channel for WSNs is channel 26, which is outside the band used by most WLAN deployments (see Figure 1.2). Nevertheless, there is out-of-channel interference (see Figures 2.29 and 2.30) or IEEE 802.11 channel 13 can be used in Europe (see Section 1.1.4). In general, IEEE 802.11 interference is seen as the most severe. Also the number of published models and analyses for the coexistence of IEEE 802.11 and IEEE 802.15.4 is large. As it can be seen in Table 4.1, IEEE 802.11 is the most widely researched interferer technology.

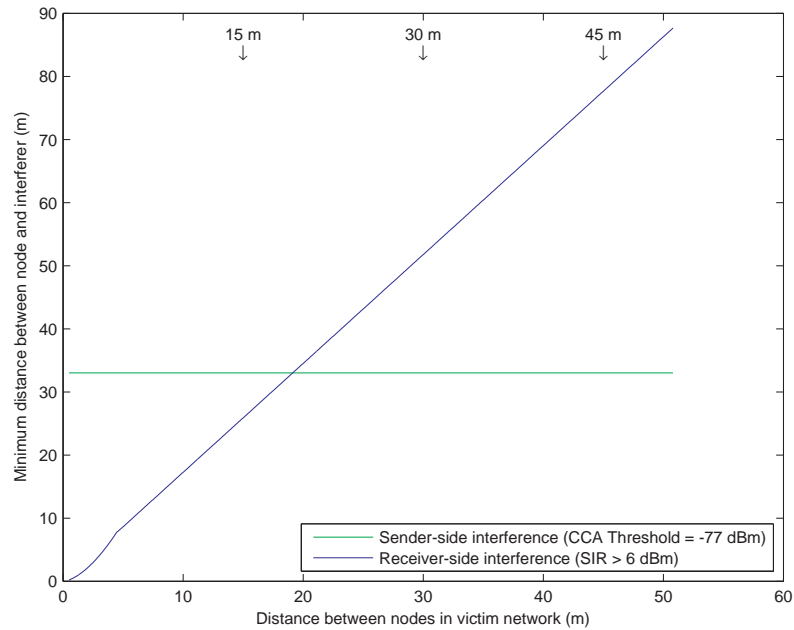
For the physical link quality, it can be assumed that IEEE 802.11 is seen as a wideband interferer and therefore as noise to IEEE 802.15.4. Since the output power of IEEE 802.11 is also spread throughout its 22 MHz wide channel, 9 dB to 10 dB can be subtracted according to (IEEE, 2003b) because of the spectral spread. These -10 dB (= 10%) equal roughly $2/22 \text{ MHz} = 9.09\%$. Due to the noise-like wideband character of IEEE 802.11 interference, the connectivity regions as shown in Subfigures 4.8a and 4.8b can be assumed or the SNR of 5 to 6 dB for a PER of 1% (IEEE, 2003b) can be used as a point of reference.

Alternatively, the interference region concept (see Table 4.2) gives another indication of the expected range of interference.

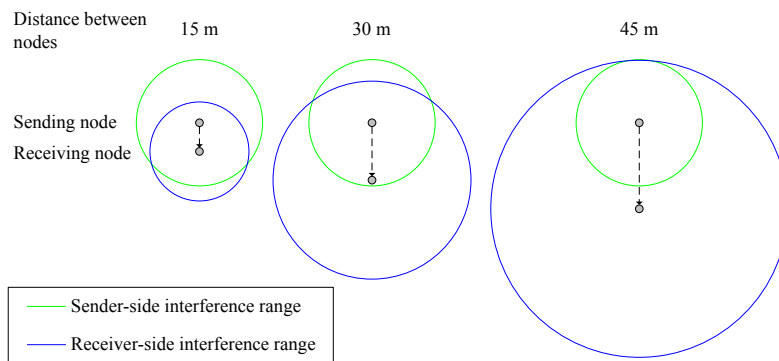
These estimations are all applicable for receiver-side interference. When the default, ED-based CCA mode with a threshold of -77 dBm is used, transmissions on the sender side, which can be received by the receiver, can be suppressed independently of the discussed SIR needed for a reception on the receiver side. Such situations are more likely to occur with larger distances between the sender and the receiver in the victim network. WLANs based on IEEE 802.11 having the largest interference range of all researched technologies are a good example to show the different ranges of sender- and receiver-side interference.

In Figure 4.13, the problems of sender- and receiver-side interference are illustrated. The following assumptions were made for computation: IEEE 802.15.4 victim can successfully receive signals P down to -85 dBm (receiver sensitivity according to (IEEE, 2003b)), which results in a range of approximately 51 m for a 0 dBm transmission according to Equation 4.6 in an indoor environment. The simplified, homogeneous PSD of the IEEE 802.11 interferer sending with 20 dBm results in a power of $2/22 \text{ MHz} \times 20 \text{ dBm}$ in the victim channel. For the sender-side interference the CCA threshold is -77 dBm . To receive the packet successfully, the SIR at the receiver has to be at least 6 dBm.

In Subfigure 4.13a, it can be seen that the CCA threshold stays constant and blocks or delays transmission if the IEEE 802.11 interferer is closer than 33 m. The SIR on the receiver side is not only dependent on the distance of the source of interference (related to I), but also on the distance of the sender, since the received signal P depends on the distance of the transmission. Thus, with a higher distance between the nodes, the received desired signal becomes weaker. For an errorless transmission, the required distance to the source of interference increases up to 86.27 m for 50 m between the victim nodes (compare to the interference range of IEEE 802.11 computed in Section 4.4). In Subfigure 4.13b, these ranges are illustrated for three examples (15, 30 and 45 m between the IEEE 802.15.4 nodes in the victim network). If the interferer is placed in the overlap of the two ranges, the CCA threshold will only prevent transmissions that will fail to be received. For 15 m between the nodes, the CCA threshold can be oversensitive, because it can prevent transmissions that would be successful. However, for the other two distances, the region of receiver-side interference increases. In the 45 m distance scenario, the number of false positive



(a) The ranges between victim and interferer in which receiver- and sender-side interference occurs related to the distance between the nodes in the victim network.



(b) Visualization of the different ranges in the plane. In the overlap of both range circles, the CCA can detect interference energy that would interfere with and jam the transmission.

Figure 4.13: Ranges of sender- and receiver-side interference for an IEEE 802.15.4 link under IEEE 802.11 interference.

backoffs (channel is clear, but CCA reports busy and the transmission is delayed) tends to be towards zero, since the sender-side interference range is inside the receiver-side interference range. This shows that it is hard to find an optimal CCA threshold. Furthermore, the finding of an ideal threshold is more complex than it might seem from this example, which is based on computations, since the ranges will differ in real deployments. A possible approach to adapt the CCA threshold for IEEE 802.15.4 radios under IEEE 802.11 interference is suggested by Yuan et al. (2010a) and Yuan (2011). Nevertheless, a not ideally tuned CCA value is not devastating, since real sources of interference are not sending permanently. If the CCA threshold is oversensitive, MACs using CSMA are only delay transmissions as a result of erroneous CCAs. An insensitive CCA threshold is comparable to the hidden node problem (see Section 2) and ACKs can help to recognize and to overcome the resulting packet loss. In addition, if CCA Mode 2 is used, external interference does not lead to any sender interference. The effectiveness of CCA as part of CSMA to mitigate external interference is further researched in Section 6.3.3.

Besides the interference range, the channel utilization of IEEE 802.11 is also an important factor for the strength of interference. Estimations can be made for given packets, as e.g. shown

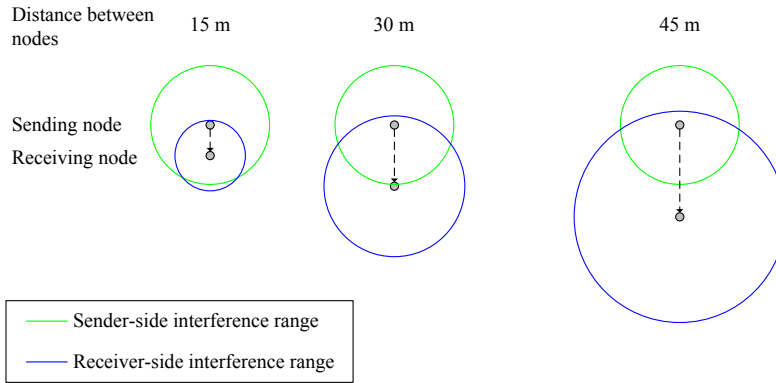


Figure 4.14: Ranges of sender- and receiver-side interference for an IEEE 802.15.4 link under Bluetooth interference visualized for ranges of the victim nodes in the plane.

in Section 4.2.6 and visualized in Figure 4.10. However, for most real WLANs, traffic is too diverse to limit it to predefined packet types. Joseph et al. (2013) measure the channel utilization of WLANs in 179 locations, including different environments and activities. They give the 95th percentile of 10.4% channel utilization for all measurements. Furthermore, they give theoretical, calculated maximal channel utilizations for different data rates. Thus for rough estimations made with little knowledge about the traffic, they give numbers for orientation. For estimating the traffic of multiple clients, they also suggest that the utilization can be multiplied by the number of clients until the theoretical maximum is reached. For a more detailed analysis, e.g. a closed loop approach for IEEE 802.11b/g is presented in the doctoral thesis of Yuan (2011). However, a full review of all the possible cases is beyond the scope of this work.

4.3.3 Bluetooth as Interferer

The interference caused by Bluetooth is limited by two factors.

Firstly, the channel hopping used by Bluetooth limits the interference down to $3/79$ of its initial occurrence and therefore, even a permanent channel use will result in less than 4% occupation of an IEEE 802.15.4 channel. If the Bluetooth Wireless Personal Area Network (WPAN) itself is under further interference by other sources of interference, the AFH algorithm might blacklist channels, but has to leave 20 channels available for hopping. Even in the unlikely case that this happens and the IEEE 802.15.4 is not blacklisted, this would result in a maximum utilization of 15% on the IEEE 802.15.4 channel.

Secondly, the effect of the narrower Bluetooth signal is mitigated due to the spreading used by IEEE 802.15.4. Therefore, according to (IEEE, 2003b), a PER of 1% can be achieved with a SIR of 2 dB under the interference of a Bluetooth signal centered in the desired IEEE 802.15.4 channel. The reported effects found in literature are also only moderate. The worst effects known to the author are reported in (Sikora, 2004) with a PER of 9.9% and in (Huo et al., 2010) with a PER of 10%.

Since the power and thereby the range of Bluetooth interference are less than for IEEE 802.11 interference, the receiver-side interference range increases slower than for IEEE 802.11 (see Figure 4.14). This makes false positive backoffs more likely. However, the calculated ranges are theoretical for Bluetooth, because it is normally used in WPANs and therefore it is used in ranges below ten meters. Bluetooth automatically adapts its transmit power and hence the interference ranges are further limited. Due to frequency hopping, the sender is only shortly interfered and the delay due to false positive backoffs can be neglected, since the second CCA timed by the CSMA algorithm is very likely to be successful. The effectiveness of CCA and its different modes are further discussed as an interference mitigation strategy in Section 6.3.3.

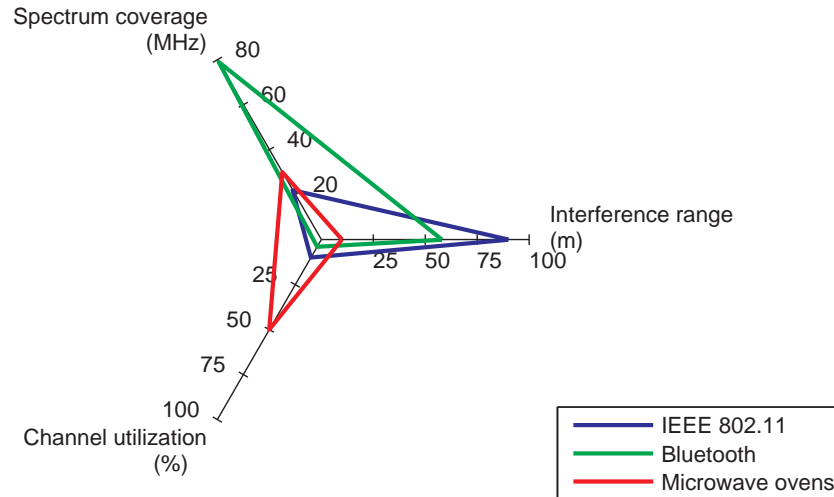


Figure 4.15: Overview of the most important characteristics of different sources of interference.

4.3.4 Microwave Oven as Interferer

The interference of microwave ovens highly depend on the actual model. Normally the range of interference is limited to a single room. For microwave ovens used in residential settings, the channel utilization should not exceed 50% and normally the oven will be only used for durations under an hour. In literature, the reported PERs vary widely:

- from ignorable (oven at a distance of roughly 1 m has no influence on the IEEE 802.15.4 performance (Sikora, 2004; Sikora and Groza, 2005))
- over medium (12% PER for 802.15.4 traffic (Chowdhury and Akyildiz, 2009))
- to heavy (a PER of 25% (Boano et al., 2011b) or a PER of 67% for a 2 m away oven in (Simek et al., 2011)).

From the experience of the author, varying data can be easily explained due to different microwave oven models and heterogeneous measurement setups used.

4.4 Summary

Figure 4.15 illustrates the most important interference factors for the three discussed technologies. The spectrum coverage can be roughly estimated based on the spectral width of the channels given in the corresponding standards. For microwave ovens, experience and measurements found in literature provide a first orientation. Figure 1.2 also shows the situation in the 2.4 GHz frequency band.

The interference range can be calculated with knowledge of the output power of the interferer and the path loss (details in Section 4.2.2). For IEEE 802.15.4, a sensitivity of at least -85 dBm is required and thus a signal with just the same value of power might be received. Furthermore as already mentioned in Section 4.3.2, a SNR of 5 to 6 dB is required according to (IEEE, 2003b) for reception, which can be equally seen as a point of reference for the SIR under wideband IEEE 802.11 interference. Thus, the minimum interference signal still causing interference can be computed as $SIR = 6 \text{ dB} = \frac{-85 \text{ dBm}}{I}$ and therefore $I = -91 \text{ dBm}$. An IEEE 802.11 transmitter sending at 20 dBm emits only $\approx 11\%$ in an IEEE 802.15.4 channel. These 2.2 dBm in the channel decrease to -91 dBm after a distance of roughly 90 m (according to Equation 4.6). With regard to Bluetooth,

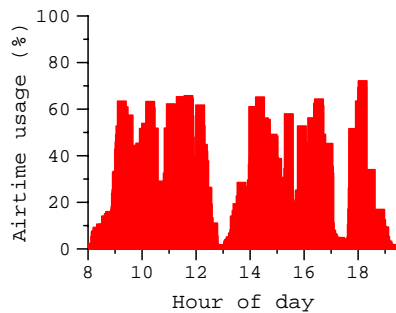


Figure 4.16: IEEE 802.11 channel (airtime) utilization over time measured during a conference, plotted with a binning interval of a minute. Taken from (Rodrig et al., 2005).

the required SIR is 2 dB and the output power can be assumed to be 0 dBm (Bluetooth power class 2 compare Table 2.10), which leads to a range of roughly 58 m. The range for microwave ovens is an estimation based on the experiments done in (Bluetech Power class 2 compare Table 2.10), which leads to a range of roughly 58 m. The channel utilization states the time that the channel is actually in use. For IEEE 802.11, the channel utilization can vary from under 1% for only beacon frames to up to a theoretical value of 97.16% for the lowest data rate (1 Mbit/s) (Joseph et al., 2013). Rodrig et al. (2005) measured the wireless traffic during a conference in 2004 and in Figure 4.16, it is shown how channel utilization varied in their measurements. The utilization of roughly 10% used, in Figure 4.15 based on the results presented in (Joseph et al., 2013). Bluetooth channel utilization is assumed to be 4% when all time slots are used, as explained in Section 4.3.3. For microwave ovens, the channel utilization is typically around 50%, as is illustrated in Figure 2.37 or measured in Figure 5.5d.

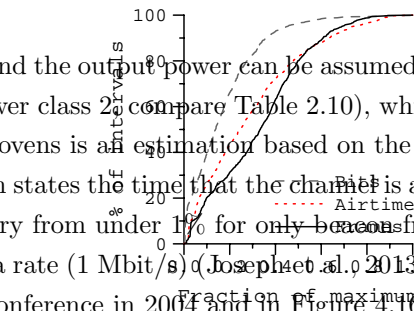


Figure 3: Cumulative distribution of activity per minute.

However, for the channel utilization, it is assumed that the system is on and therefore, the channel utilization is only relevant in time intervals used significantly. Although throughout the day, this is consistent with the results of Yeo et al. [11], which show high variability in activity in an academic department's wireless network. The patterns evident in usage tend to correspond to events in the conference program. For example, there is a noticeable drop over lunch, though activity remained high during the lead-up and talk departure. Back of AP in the ballroom where the talks were given. We also observed high night-time activity (until around 1 am) on some nights. Thus, the usage duration is estimated to be less than eight hours a day, which might be the time a user makes use of the computer's Bluetooth mouse or keyboard. For microwave ovens, the usage time is estimated to be less than eight hours a day, which might be the time a user makes use of the computer's Bluetooth mouse or keyboard. For microwave ovens, the usage time is estimated to be less than eight hours a day, which might be the time a user makes use of the computer's Bluetooth mouse or keyboard.

To see the differences between Frames, Bits and Airtime as measures of utilization, we plotted their cumulative distributions. This is shown in Figure 3. To fit all three measures on one scale, the x -axis values have been normalized to the fraction of the maximum activity observed in an interval. In all cases a small portion of the trace time contains the top third of the loads. Bits is the most skewed measure, with half of the trace minutes having low loads of around 10% or less of the maximum, and less than 10% of the trace minutes having loads above 40% of the maximum. Frames is a much flatter distribution, with more than 90% of the minutes roughly uniformly spread up to 60% of the maximum load. Airtime falls between the other measures. These results suggest that Frames, Bits and Airtime are not interchangeable measures of load even when averaged over small intervals such as a minute.

Frame type and subtype	Airtime (secs)	Bits (MB)	Frames (1000s)	Avg. R (Mb/s)
<i>Data</i>	6802	1884	5540	6
Originals	3616	1276	3988	7
Retransmits	3185	608	1552	4
<i>Control</i>	1418	74	5442	1
Ack.	1332	69	5135	1
RTS	42	3	142	1
CTS	40	2	155	1
PS poll	2	0	10	1
<i>Management</i>	878	82	1098	1
Assoc. Req.	1	0	2	1
Assoc. Res.	1	0	3	1
Authentication	6	0	13	1
Beacon frame	412	39	428	1
Deauth conference,	0	0	0	1
Dissassoc.	6	0.40	13794	1
Probe Req.	177	16.07	333707	1
Probe Res.	270	25.44	296250	1
Reassoc. Req.	0	0.03	2727	1
Reassoc. Res.	0	0.03	621	1
<i>Totals</i>	9098	2040	12080	3

Table 2: Breakdown by frame type and subtype. (Originals that reduce its effectiveness compared to an ideal transmission are not 802.11 frame subtypes; we list them for ease of exposition.)

4. OVERHEADS

We now consider the various overheads involved in data transmission that reduce its effectiveness compared to an ideal transmission. These include management and control frames, 802.11 retransmissions, and PHY and MAC headers. Table 2 presents a breakdown of transmissions by frame type and subtype. For each, it shows three usage measures and the average transmission rate.

As we see that the vast majority of Bits (92%) are for data frames, we see that management frames (mostly beacons and probe requests) and acknowledgements make up 10% of the frames, and acknowledgements make up half the frames (as they are roughly one-for-one with data frames). Moreover, these frames are transmitted at a lower average rate than data frames. Combined with PHY+PLCP headers, which are ignored in this measure, this means that they occupy more of the medium than suggested by their frame counts – data frames obtain only 28% of the data frame category, it is surprising to find that 28% of them are retransmissions (i.e., data frames with a higher sequence number). The impact of these retransmissions is heightened because they occur at a lower average rate than original frames and, only slightly over half (53%) of the data frame Airtime is consumed by original transmissions. This leads us to investigate retransmissions and rate adaptation in the next sections.

As a final source of overhead, we note that a further 31% of the signal since the Airtime is consumed by 802.11 MAC overheads. The cumulative effect of control and management traffic, retransmissions, and PHY and MAC overhead is that 31% of the Airtime is being used to transfer original data to a higher layer). We were somewhat surprised at this relative overall efficiency as we had expected large data frames to be the overheads of short frames.

5. RETRANSMISSIONS

In this section, we explore the retransmission behavior in our traces. We also investigate whether signal strength variations correlate closely with high retransmission rates. We are investigating other potential causes of retransmissions, such as fading, and quantifying their relative impact for future work.

Chapter 5

Classifying Sources of External Interference

In this section, an approach to detect and classify sources of interference based on Clear Channel Assessment (CCA) requests is developed. Firstly, related work reported in the literature is reviewed. Then the unique temporal features of the channel access of all technologies are discussed. Finally, the algorithm with its decision criteria is developed, extensively tested and discussed.

5.1 Interference Classification Methods Reported in Literature

The topics of detecting and classifying sources of interference have gained more attention in the last few years, which is due to their high importance in real world deployments and the increasing use of the 2.4 GHz frequency band. While interference detection is a term for noticing a source of interference, interference classification refers to a process which includes a distinction between different classes and returns the class of the interferer. The classes are mainly corresponding to transfer technologies, as IEEE 802.11 or Bluetooth.

The following overview of literature is structured according to Figure 5.1, which shows a possible taxonomy based on the method used to classify the source of interference. In the figure the main differentiation is made between an active classification process and a passive process that does not require any sensing additional to the normal communication. The first case includes the majority of approaches, which are then further subdivided. Additional probing packets adding overhead can be used. However, the most common approach is using the ED to monitor either the channel or

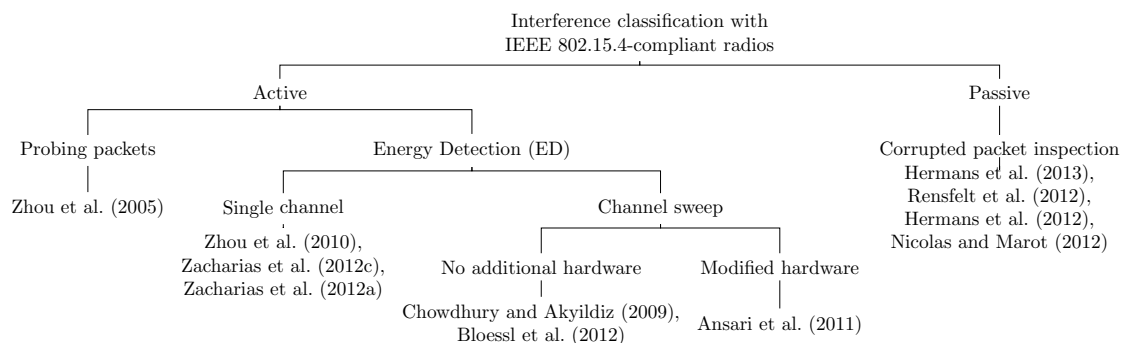


Figure 5.1: Overview of literature structured by classification method.

the full spectrum. The passive classification with the help of corrupted packets has been published only recently and offers a new approach, which is discussed in detail later.

A Radio Interference Detection protocol for Wireless Sensor Networks (WSNs) is presented by Zhou et al. (2005), which is based on sending packets with different power transmissions. They detect only internal interference, but deal with the hidden terminal problem.

An approach to detect IEEE 802.11 is described by Zhou et al. (2010), being based on the same principles as the approach presented here. Their system is called ZiFi and has been implemented e.g. on a TelosB sensor node. The system uses the sensor node for Received Signal Strength Indication (RSSI) sampling and the signal processing is computed on a connected computer. Their algorithm is based on the beacon frames sent by Wireless Local Area Network (WLAN) Access Points (APs) and monitors a single channel. At first, it takes binarized samples from the RSSI register. This stream is then cleaned up by removing parts where the channel is used for a duration that is improper for a WLAN beacon. This signal is then processed by the Common Multiple Folding algorithm, which is also presented in their paper. This algorithm finds the frequency component of the signal for different periods. Unlike the author of this paper, Zhou et al. (2010) consider different beacon intervals than the default 100 tu to be relevant. Robustness of this detection has been tested for different amounts of IEEE 802.11 data traffic and the cross-sensitivity has been validated for ZigBee traffic. While the approach to detect different beacon periods (60...120 tu) can be argued to be an enhancement compared to the algorithm presented here, the author of this work is not able to relate to the decision of Zhou et al. (2010) to use the unusual beacon period of $96 \times 1.024 \text{ ms} = 98.304 \text{ ms}$ throughout all their experiments. The author of this work argues that a beacon interval of 102.4 ms is sufficient and predominantly used (see Section 2.4.2 and Table 2.6). The envisioned applications are also different since Zhou et al. (2010) use their algorithm as a low power pre-switch for IEEE 802.11 network interface cards to conserve energy on laptops or smartphones. The potential of their algorithm for WSNs is not discussed.

The algorithm presented here is based on former work done by the author. In a first approach, a Tmote Sky sensor node is used to collect one second of RSSI readings sampled with the help of the Frossi Software (Dunkels et al., accessed: February 2012). The collected data is classified in Matlab (MATLAB, 2009) on a connected laptop, thus only an offline classification of the source of interference is possible (Zacharias et al., 2012c). However, as already mentioned in Section 3.1.1 the sampling rate of Frossi is not always stable and thus the features used for the classification are different to the features used in this work. Also the offline nature of the work limited the application, but it was a proof of concept.

In (Zacharias et al., 2012a) a live version of the algorithm is shown, which is based on a setup comparable to the work presented here. The sampling of RSSI readings is done for a second with 8,192 Hz and the readings are binarized and stored. After the sampling, timing features of the binarized RSSI trace are extracted and finally a classification decision returns the class of interference.

Nevertheless, the algorithm presented here is an enhancement of the former work: it uses CCA requests instead of RSSI readings. With the help of the faster CCA request, the here presented algorithm supports faster decisions with the possibility of an abort (less execution time means less energy-consuming channel sensing). It also relies on improved criteria enabling better classification results with sound evaluation.

Chowdhury and Akyildiz (2009) present both an approach to classify interference by RSSI noise floor readings of a CC2420 radio and a scheme for channel selection and Medium Access Control (MAC) parameter adjustment. They use a full spectrum scan, which is matched to a pre-measured pattern of an IEEE 802.11b-based WLAN and a microwave oven. The main points of criticism for their paper are the small number of researched devices and that important parameters, as the sampling rate and number of samples, are not given.

Bloessl et al. (2012) present a framework to utilize a TelosB sensor node for spectrum scanning. The spectrum scans can be configured with the help of a job description language. Further, they give an outlook how to detect IEEE 802.11 networks using the framework.

WiSpot by Ansari et al. (2011) is an IEEE 802.11 network detection tool that uses modified hardware based on the TelosB sensor node, by connecting two nodes and thus creating a radio array. With the modified hardware, a full spectrum scan is done and IEEE 802.11 networks are found by their spectral features.

Hermans et al. (2013) and Rensfelt et al. (2012) propose Sensor Network Interference Classification (SoNIC), a system consisting of a classification method and countermeasures to mitigate the effects of interference. The classification method uses individual corrupted IEEE 802.15.4 packets and gathers the data only in periods of normal operation. Hence, the system can be more energy conserving than active sensing. However, as described in (Hermans et al., 2013), packets sent under interference can be either lost (not received) or received. The received packets can be correct (which means that the interference did not affect the link) or corrupted. The corrupted packets can also be partly (leading to less accurate classification) or fully interfered with by the interferer. Hermans et al. (2013) state that the ratio of corrupted packets is 10% to 20% if a link has a Packet Error Rate (PER) above 20%. Further, only packets with a payload greater than or equal to 64 bytes are used for classification. To get all features needed for the classification a successful retransmission has to be achieved so that the position of the corrupted bits in the message can be obtained due to comparison of the corrupted packet and the correct packet of the retransmission. The classification rate based on a single packet seems low compared to the other approaches (almost down to only 60% for microwave ovens and IEEE 802.11). However to avoid misclassifications, multiple classification results are combined. A time span of 30 s or 10 s is monitored until the final decision about the mitigation strategy is made (Hermans et al., 2013). SoNIC collects features based on RSSI, Link Quality Indication (LQI) and corrupted bits from the corrupted packets. These features were then used to build a neural network (feed-forward artificial neural network) (Rensfelt et al., 2012) or a decision tree to classify the data (Rensfelt et al., 2012; Hermans et al., 2013). Rensfelt et al. (2012) report a decision tree consists of 749 nodes using ten features. Hermans et al. (2013) state 731 nodes for the decision tree using six features. The big number of nodes compared to the number of features raises the question that the decision tree might be overfitted. The system is implemented in ContikiOS on a TelosB sensor node. The latest version presented in (Hermans et al., 2013) is extensively tested in a controlled and uncontrolled environment. SoNIC is based on the work of Hermans et al. (2012) in terms of using the dataset collected in a Radio Frequency (RF) anechoic chamber.

Hermans et al. (2012) present an earlier stage classification method that uses the same features collected from corrupted packets, but classifies the data with support vector machines, fixed and floating point neural networks. All SoNIC versions classify the packets into one of the following groups: IEEE 802.11b/g, Bluetooth, microwave oven or insufficient signal strength.

Nicolas and Marot (2012) present an approach called Fingerprint Identification Mechanism (FIM), which identifies the type of interferer. As Rensfelt et al. (2012), they use the bit error pattern of a received, but corrupted packet. Their approach divides into IEEE 802.11b, Bluetooth and weak IEEE 802.15.4 links. Finally, they propose interference mitigation methods and in an initial test, they show the efficiency of their classification and a subsequent link adaptation. Although their approach is promising, they do not present results for newer versions of IEEE 802.11, because they argue that IEEE 802.11g would back off for IEEE 802.15.4 due to its CCA threshold, but this is not always the case as discussed in Section 4.2.1. Furthermore, they do not discuss different IEEE 802.15.4 packet lengths. The positions of erroneous bits within an IEEE 802.15.4 packet interfered with by IEEE 802.11 differ depending on the distance between victim and interferer. Liang et al. (2010) state that in the symmetric region, errors occur primarily at

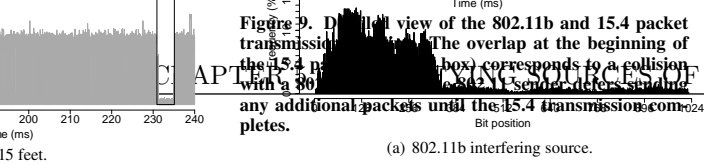


Figure 9. Packet capture analysis showing the overlap of the 802.11b and 15.4 packet transmissions. The overlap at the beginning of the 15.4 packet corresponds to a collision with a 802.11b sender. The receiver does not receive any additional packets until the 15.4 transmission completes.

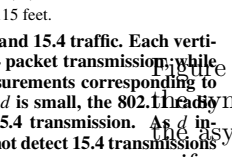


Figure 10. 15.4 packet reception rate as the payload size varies. The PRR drops to zero in the asymmetric region of the 15.4 sender. Since only bits in the front section of the 15.4 packet are corrupted by varying the packet's length does not affect PRR.

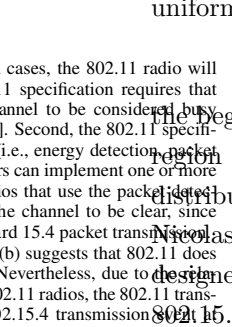


Figure 11. Bit-error distribution for 15.4 packets that failed the CRC check when the interfering 802.11g transmitter is in the asymmetric region. Bit errors are evenly distributed across the whole packet.

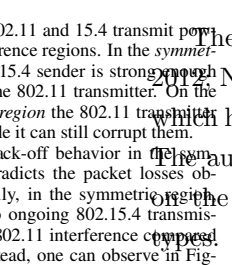


Figure 12. Bit-error distribution for 15.4 packets that failed the CRC check when the interfering 802.11g transmitter is in the symmetric region. Bit errors are skewed towards the beginning of the packet.

4.1. Symmetric Region Techniques

Section 3 shows that in the symmetric region corrupted bits occur at the front of a 15.4 packet. Such corrupted packets work for receiver-side interference,

since there is a CCA-based backoff for microwave packets. In the asymmetric region, corrupted 15.4 packets received in the symmetric region have a wider spread in the number of corrupted bits, and they are also more severely damaged than corrupted packets received in the asymmetric region. While Figure 12 presents the number of corrupted bits, Figure 13 presents the density with which these bits appear over the 15.4 packet. Specifically, it plots the probability mass function (pdf) of the number of corrupted bits in the packet. Small values of n correspond to bursts of corrupted bits, while large values of n correspond to more uniform corruption. The distribution of corrupted bits in IEEE 802.11g is skewed towards the beginning of the packet, which corresponds to, possibly multiple corrupted bits in the symmetric region.

4. Protecting 15.4 packets from WiFi senders

Based on the observations above, we design targeted redundancy mechanisms to compensate WiFi interference on both the zigbee and WiFi links, push back the WiFi transmissions, we investigate techniques for symmetric and asymmetric regions respectively.

4.1. Symmetric Region Techniques

Section 3 shows that in the symmetric region corrupted bits occur at the front of a 15.4 packet. Such corrupted packets work for receiver-side interference, since there is a CCA-based backoff for microwave packets. In the asymmetric region, corrupted 15.4 packets received in the symmetric region have a wider spread in the number of corrupted bits, and they are also more severely damaged than corrupted packets received in the asymmetric region. While Figure 12 presents the number of corrupted bits, Figure 13 presents the density with which these bits appear over the 15.4 packet. Specifically, it plots the probability mass function (pdf) of the number of corrupted bits in the packet. Small values of n correspond to bursts of corrupted bits, while large values of n correspond to more uniform corruption. The distribution of corrupted bits in IEEE 802.11g is skewed towards the beginning of the packet, which corresponds to, possibly multiple corrupted bits in the symmetric region.

4.2. Asymmetric Region Techniques

Section 3 shows that in the asymmetric region corrupted bits occur at the front of a 15.4 packet. Such corrupted packets work for receiver-side interference,

since there is a CCA-based backoff for microwave packets. In the asymmetric region, corrupted 15.4 packets received in the symmetric region have a wider spread in the number of corrupted bits, and they are also more severely damaged than corrupted packets received in the asymmetric region. While Figure 12 presents the number of corrupted bits, Figure 13 presents the density with which these bits appear over the 15.4 packet. Specifically, it plots the probability mass function (pdf) of the number of corrupted bits in the packet. Small values of n correspond to bursts of corrupted bits, while large values of n correspond to more uniform corruption. The distribution of corrupted bits in IEEE 802.11g is skewed towards the beginning of the packet, which corresponds to, possibly multiple corrupted bits in the symmetric region.

4.3. Zigbee and WiFi Coexistence

While the approaches reviewed so far concentrate on IEEE 802.11 as sources of interference, Airshark (Rayanchu et al., 2011) detects a full range of wireless devices, and provides the characteristics for these devices, with the help of a Wi-Fi network interface card. An off-the-shelf Wi-Fi network interface card in a laptop is used to sample the noise floor with the help of RSSI readings. But while the IEEE 802.15.4 radios are able to detect the energy of a 2 MHz wide channel, IEEE 802.11 cards are able to detect a single 22 MHz wide channel and provide at best information for a resolution of 0.3125 MHz (Orthogonal Frequency-Division Multiplexing (OFDM) subcarrier spacing). The sampling rate is stated with roughly 2.5 kHz. Thanks to the computing power of a laptop in the following signal processing phase features can be extracted and classified based on a decision tree, allowing simultaneous real-time detection of different classes. Although the results of Airshark are compelling, the hardware used and the full spectrum scan is not comparable to the possibilities of a single sensor node that stays connected to its network.

4.4. Zigbee and WiFi Coexistence

Li et al. (2012) present the main spectral and time features of IEEE 802.11, Bluetooth and ZigBee and how to identify these technologies with a GNU's not Unix (GNU) radio (GNU Radio Members, last accessed August 2013). They also highlight the importance of beacon frames sent by wireless access points and use a Fast Folding Algorithm to detect periodicity for a range of periods. The Fast Folding Algorithm is also the basis for the Common Multiple Folding used in Zhou et al. (2010). Hence the sampling rate of the GNU radio is in the range of millions per second, more time features as Short InterFrame Spaces (SIFSs) can be used for identification than in the RSSI traces of sensor nodes.

5.2 Significant Features in the Channel Use Pattern

As already explained, an IEEE 802.15.4-compliant radio has with the help of the ED the chance to detect the increased power in its channels caused by signals the radio chip does not demodulate. The algorithm presented here collects data with the help of CCA requests, which return binary decisions if the channel is idle or busy, at a sampling rate of 8,192 Hz. A CCA request is performed faster than an RSSI request and therefore leaves more time to process the returned result in between the sampling. Thus, the sample can be analyzed immediately and if a class criterion is fulfilled, the algorithm ends before the maximum runtime of a second and a suitable mitigation strategy can be applied. The class decision criteria are based on the timing pattern of the channel access and occupation duration of the different technologies. The principles of airtime and channel utilization, which have explained in general in Chapter 2, are now reviewed for typical, unique patterns for each technology.

5.2.1 IEEE 802.11b, g, n

The importance of beacon frames due to their unique characteristics has already been emphasized in Section 2.4.2. The rest of the IEEE 802.11 traffic varies too much to be representative or to be used for classification, with many influencing factors as data rate/modulation, numbers of participants and high-level applications. Additionally, the RSSI sampling rate of IEEE 802.15.4-compliant radios are not high enough to detect more sophisticated temporal features of IEEE 802.11 as Interframe Spaces, which would be beneficial for traffic classification.

In Figure 5.5a, a typical example of an RSSI trace of IEEE 802.11 traffic is shown. The beacon frames are easily identifiable. It can also be seen that there is a difference between the energy levels of the beacon frames and the data traffic. In this particular setup, the sensor node collecting the RSSI trace was next to the client laptop, while the AP was a few meters away. Nevertheless by relying on beacon frames only (as most other approaches found in literature (Zhou et al., 2010; Ansari et al., 2011; Li et al., 2012)), there is the risk left of being only under the interference of a client, but being outside the range of the AP as shown in Figure 5.4. However, this case is unlikely, since the AP (mains-operated) normally sends with higher power than the client (often battery-operated). It is not uncommon to have an AP with a transmit power of 17 dBm and a WLAN interface card sending with 15 dBm or less to save power. In theory, four times the power (≈ 6 dB) doubles the range, though this is only the case in an ideal environment. Furthermore, WLANs are also mostly used in buildings where walls have a great impact on the range. In addition, the dominate traffic pattern of WLANs is the downstream from the AP, since most clients request data e.g. from the Internet and the AP delivers it. Thus, the chance of a situation, in which the client is causing serious interference, but the AP cannot be detected by the sensor node anymore is unlikely.

Another case that has to be taken into consideration is that beacon frames have no reserved time slot. However, if the channel is busy due to data traffic (CCA will still report a busy channel) the beacon will be delayed and the next beacon will be transmitted according to the original schedule as shown in Figure 5.3. Since the channel was used at the expected beacon time, although by data traffic instead of the beacon frame, the resulting use pattern is periodic.

However, with relying on the beacon frames an idle WLAN can be detected as potential source of interference and thus the algorithm is especially useful for deployment planning. The use of the algorithm to mitigation the effects of interference caused by a WLAN after the deployment are discussed in Section 7.5.

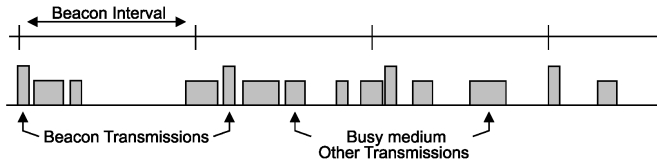


Figure 5.3: Beacon transmission on a busy network. Taken from (IEEE, 2007).

11.1.2.2 Beacon generation in an IBSS

Beacon generation in an IBSS is distributed. The beacon period is included in Beacon and Probe Response frames, and STAs shall adopt that beacon period when joining the IBSS. All members of the IBSS participate in beacon generation. Each STA shall maintain its own TSF timer that is used for dot11BeaconPeriod timing. The beacon interval is established by the STA at which the MLME-START.request is performed to create the IBSS. This defines a series of TBTTs exactly dot11BeaconPeriod TUs apart. Time zero is defined to be a TBTT. At each TBTT the STA shall

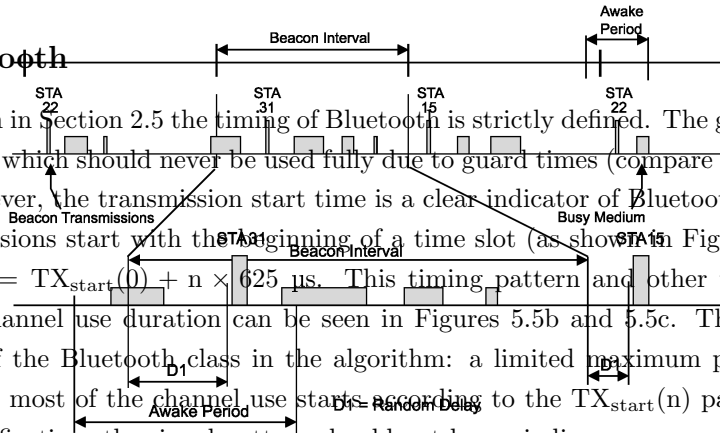
- a) Suspend the decrementing of the backoff timer for any pending nonbeacon or non-ATIM transmission,
- b) Calculate a random delay uniformly distributed in the range between zero and twice aCWmin × aSlotTime,

Figure 5.4: Different theoretical ranges of an AP and a laptop client and the resulting zone of only client interference! Calculation according to (Yuan et al., 2007).

- d) Cancel the remaining random delay and the pending beacon transmission, if a Beacon frame arrives from the IBSS of which the STA is a member before the random delay timer has expired, at which time the ATIM backoff timer shall resume decrementing.

Due to these features IEEE 802.11 is detected if the channel use trace collected with the help of CCA is periodic with a period of 100 tu during its beacon period. The middle period is shorter than 100 tu. The actual measurement and computation of the features is presented in Section 5.3.

5.2.2 Bluetooth



As already shown in Section 2.5 the timing of Bluetooth is strictly defined. The given time slots are maximum times, which should never be used fully due to guard times (compare with Table 2.8 and Table 2.9). However, the transmission start time is a clear indicator of Bluetooth communication, because transmissions start with the beginning of a time slot (as shown in Figure 2.33) and thus time $TX_{start}(n) = TX_{start}(0) + n \times 625 \text{ us}$. This timing pattern and other typical features as the maximum channel use duration can be seen in Figures 5.5b and 5.5c. These already imply the conditions of the Bluetooth class in the algorithm: a limited maximum permanent channel use duration and most of the channel use starts according to the $TX_{start}(n)$ pattern. Further, to prevent misclassifications the signal pattern should not be periodic.

Figure 11-2—Beacon transmission in an IBSS

5.2.3 Microwave ovens

The radiation timing of microwave ovens was explained in Section 2.6.1, here a measured RSSI trace, plotted in Figure 5.5d illustrates the significant periodicity of 50 Hz. Additionally the channel has to be utilized between 30% and 70% of the time.

5.3 Classification Algorithm Details

After explaining and motivating the features used in the classification, in the following the algorithm with its implementation is discussed.

The decision criteria given in the previous section allow a first overview of the classification. These criteria are given formalized in Algorithm 5.1 and rely on different features computed from the CCA requests. In Algorithm 5.1 and in the following, the classes of the algorithm are referred to with short labels: *CLEAR* for no interference, *BT1* for Bluetooth single-slot packets, *BT2* for multi-slot packets, *WLAN* for IEEE 802.11-based WLANs, *MWO* for microwave ovens and *UNKNOWN* for a source of inference that is not known. The algorithm has a further result called

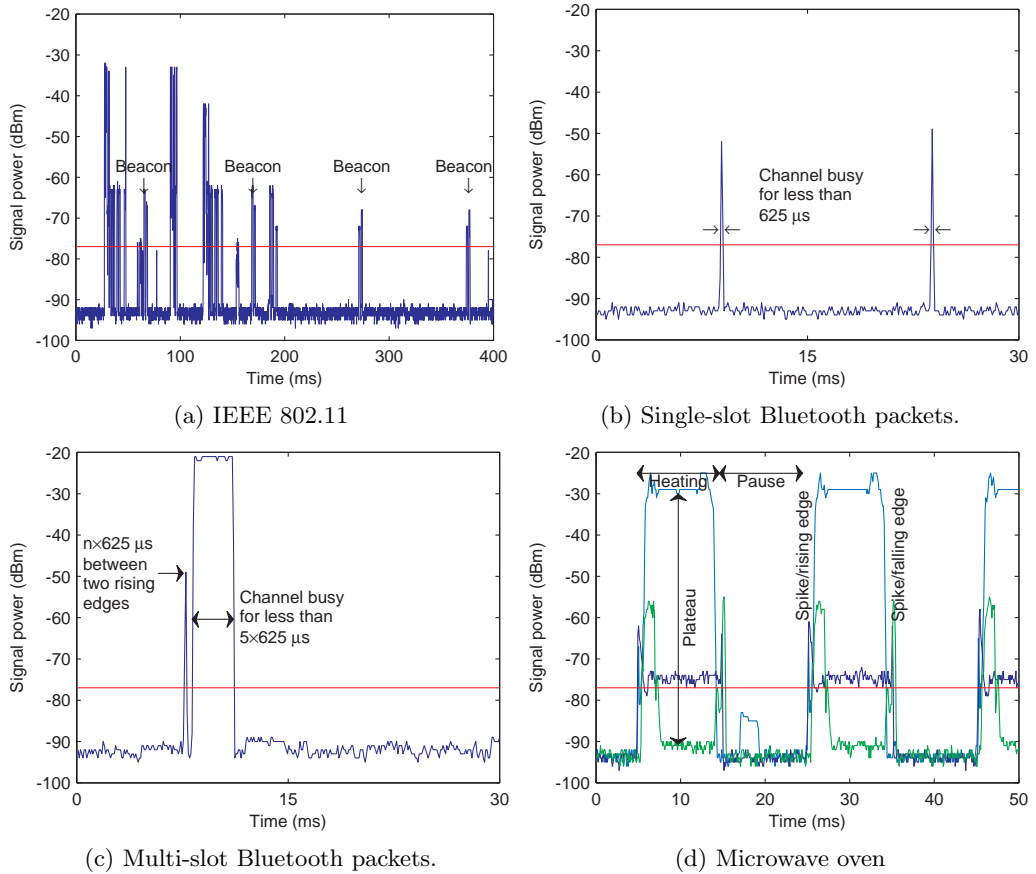


Figure 5.5: Typical RSSI traces of the different sources of interference. CCA threshold of -77 dBm shown in red. Data collected with the help of (Dunkels et al., accessed: February 2012), please note different time scalings of the plots.

INTERNAL, which is returned if the sensor node receives a packet while performing the interference classification algorithm. For the CCA threshold the default value of the CC2420 radio, -77 dBm, was chosen. In previous work (Zacharias et al., 2012c,a), the author used a lower threshold, -85 dBm, which delivers good results for the CC2420 radio, but this value is the minimum sensitivity required by IEEE 802.15.4 (compare to Table 3.1) and therefore only works with radios that exceed the requirements given in the standard. Nevertheless an adaption of the threshold might be useful in certain environments and is discussed in (Bertocco et al., 2007). For the experiments presented in this chapter, CCA Mode 3 was used, since it is based on ED and it is the default mode of the CC2420 radio. However, CCA Mode 1 delivers the same results, since the carrier sense is never triggered. The different CCA modes have been introduced in Section 2.3.3. In Interference-Aware, Self-Adapting (IASA) MAC, the classification algorithm uses CCA Mode 1 to eliminate sender interference. For the pure classification discussed in the following, this can be ignored since it has no effect on the results. The features are calculated while sampling the CCA trace at 8,192 Hz and therefore if a class criterion is fulfilled, the algorithm ends before the maximum runtime of a second and the interference can be mitigated. First, the computation of the features split into three main groups is presented in the following, and then the timing of the decisions is given.

5.3.1 Simple features

Simple features, which are maxima or sums, can be easily computed and are listed in the following:

- the maximum continuous time duration the channel was busy $t_{max\ b}$;
- the maximum continuous time duration the channel was idle $t_{max\ i}$ and

Algorithm 5.1: CLASS CONDITIONS

```

if ( $periodicity(50\ Hz) > 15$ ) and ( $30\% < cu < 70\%$ )
  then return (MWO)
if ( $periodicity^+(0.01\ tu^{-1}) > 5$ ) and ( $t_{max\ i} < 100\ tu$ )
  then return (WLAN)
if ( $t_{max\ b} < 625\ \mu s$ ) and ( $periodicity^+(0.01\ tu^{-1}) \leq 5$ ) and ( $tx_{BT} > tx_{nonBT}$ )
  then return (BT1)
if ( $t_{max\ b} < 3,125\ \mu s$ ) and ( $periodicity^+(0.01\ tu^{-1}) \leq 5$ ) and ( $tx_{BT} > tx_{nonBT}$ )
  then return (BT2)
if ( $cu = 0\%$ )
  then return (CLEAR)
return (UNKNOWN)

```

- the channel utilization cu , which is the number of CCA samples indicating that the channel was busy divided by the number of samples collected.

5.3.2 Transmission start patterns

Transmission start patterns are based on the duration between two rising edges (idle to busy channel transitions). If the time between two successive rising edges is a multiple of the Bluetooth slot time (625 μs), it is assumed to be a Bluetooth pattern. The fits and the misfits are counted as Bluetooth slot patterns tx_{BT} and non-Bluetooth slot patterns tx_{nonBT} , respectively.

Since the sampling time of $\frac{1}{8192}$ s is not an integer multiple of the Bluetooth slot time of 625 μs the duration computation has been implemented in fixed-point arithmetic.

5.3.3 Periodicity

The periodicity (*periodicity*) which is a function returning a metric p here, is computed by a simple algorithm to check if an input signal (*signal*) is periodic. Due to the limited memory and computing power of sensor nodes, a simple approach to find the frequency component for a binary signal has been selected. It is based on correlation and finds a frequency component, since a signal or function is periodic when $f(t) = f(t \pm T)$. The sampled signal is processed and the binary value at a time t is combined with a logical conjunction with the value of the time $t - T$, where T is the desired period. This is done from $t = T$ to $t = N$, where N is the number of samples. The result of each conjunction is added to a temporal array, *buffer*, at position $(t \bmod T)$. The maximum of this temporal array, *buffer*, is the frequency component p . This p can reach a maximum value of $N/T - 1$. The memory needed for *buffer* is little, only T elements have to be held. The principle of the algorithm is also shown in Figure 5.6. This algorithm has a lower complexity than a Fast Fourier transform and does not require floating-point numbers as the Goertzel algorithm. Tests by the author with a fixed-point implementation of the latter have not provided sufficient precision or became too slow on the used hardware. The classification algorithm presented here uses the periodicity for detecting IEEE 802.11 and microwave ovens. Due to the fact that the beacon frames are the periodic element for IEEE 802.11, but in between them the channel utilization can differ extensively, only the busy channel samples have to correlate. Thus the *periodicity* function shown in Figure 5.6 is modified to function $periodicity^+$ by just considering samples of the signal that are *TRUE*. Thereby the idle channel sections of *signal* have not to align periodically. For the microwave oven not only the busy channel durations, but also the idle durations, which are roughly half of a period long, have to align periodically (function: *periodicity*).

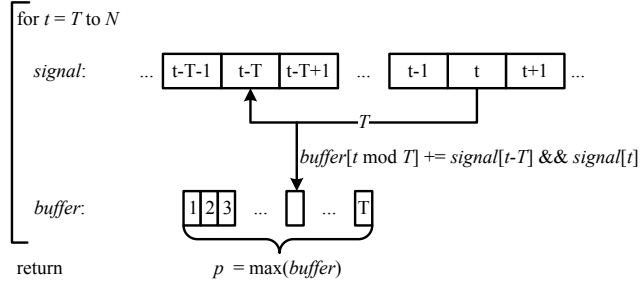


Figure 5.6: Concept of a simple algorithm to detect periodicity/frequency component p in a discrete, binary signal $signal$ for a given period T given in samples. Further, $buffer$ is a temporal array of the length T .

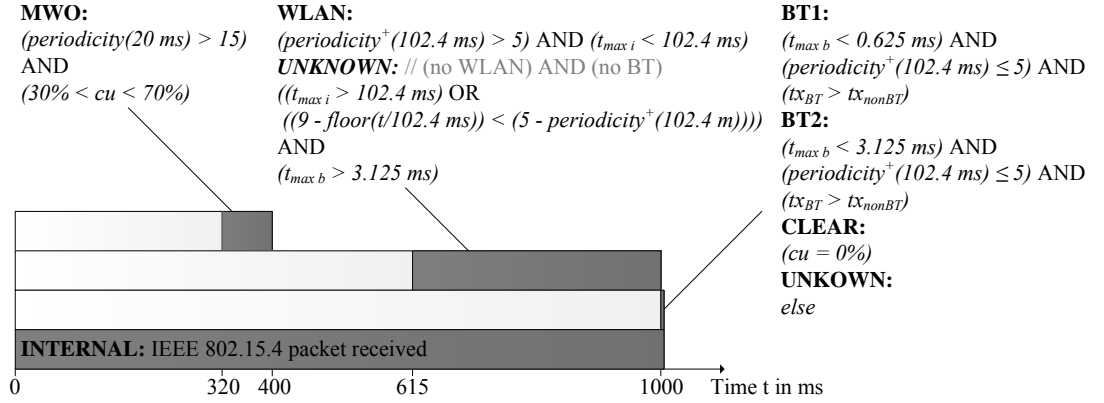


Figure 5.7: Flow and timing of the algorithm: the gray parts show the time windows when different classes can be detected and the algorithm can return before the maximum execution time.

These features are calculated and checked while the sampling of CCA request values is running. The basic conditions for each class are shown in Algorithm 5.1.

5.3.4 Algorithm Timing

An important requirement is to receive an immediate result from the algorithm, since the communication between the nodes of a WSN can be reconfigured faster and energy can be saved. The maximum algorithm execution (radio on) time is one second, which is needed to detect Bluetooth ($BT1$, $BT2$) or a clear channel ($CLEAR$). The channel hopping of Bluetooth leads to little channel use and thus more time is needed to collect enough data for a reliable decision. Other decisions can be made quicker. Especially the microwave oven class (MWO), which is unique in using the channel heavily with a high frequency, can be classified in less time. For a reliable classification, this algorithm relies on a 50 Hz periodicity greater than 15, which means that after 16 completed periods a sample can fulfill the requirements, resulting in a $16 \times 1/50 \text{ s} = 320 \text{ ms}$ minimum execution time of the algorithm. IEEE 802.11 beacon frames ($WLAN$) have a slower frequency of $1000 \text{ ms}/102.4 \text{ ms} \approx 9.77 \text{ Hz}$ or 0.01 tu^{-1} , hence the classification needs more time. To reach a threshold of more than 6 periods, it needs at least $6 \times 102.4 \text{ ms} = 614.4 \text{ ms}$. The full algorithm with its conditions and timings is shown in Figure 5.7.

The algorithm presented here has the advantage that the node is connected to the network all the time and therefore it still can receive messages if the interference is not too heavy. Nevertheless, when a message is received in the sampling process the algorithm is stopped and the *INTERNAL* class is returned, since the received message also affects the CCA sampling. The problem of internal interference can be solved by an explicit sampling phase for the network coordinated by a central manager as it is suggested in (ZigBee Alliance, 2008b) for interference reporting and resolution.

In Chapter 7 the presented algorithm is used within the IASA MAC protocol and thereby shows an application. However, as the literature review revealed (see Section 5.1), there are multiple applications for the interference classification algorithm (e.g. deployment planning (Chowdhury and Akyildiz, 2009)) or for parts of it (e.g. low power WLAN detection (Zhou et al., 2010)).

5.4 Algorithm Testing

An extensive measurement campaign was conducted to test the algorithm: at first, it was tested with selected devices and reproducible data traffic in a controlled environment. Secondly, the algorithm was tested in a real world scenario. The implementation of the algorithm used here classifies a channel three times successively and then changes to the next, higher channel. After channel 26 is classified three times, the classification restarts at channel 11. The *INTERNAL* class was not tested, since it is not a classification result, but more an interruption of the classification process. Therefore, it does not appear in the following results. The hardware used in the following experiments is listed in detail in Table 3.2.

5.4.1 Controlled Environment

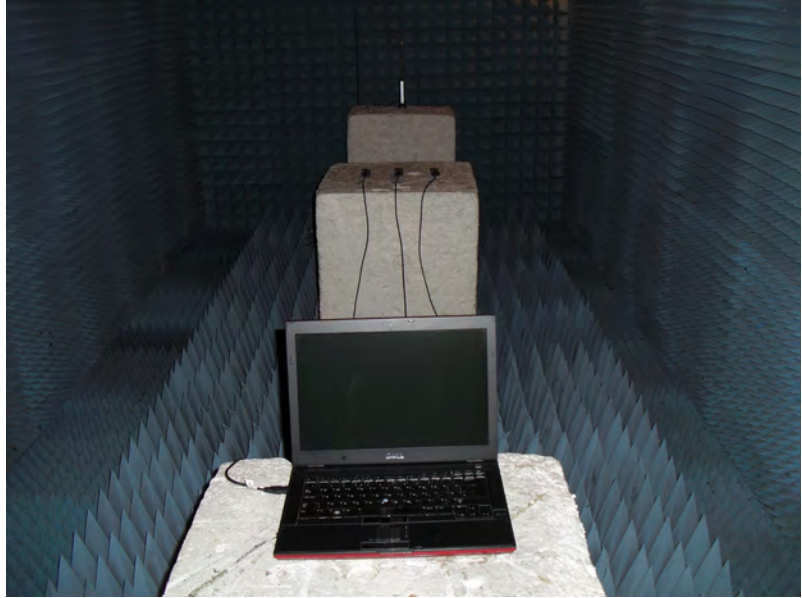
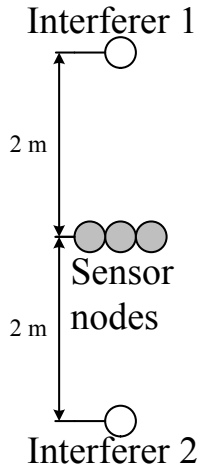
In the controlled environment, an RF anechoic chamber, experiments with reproducible traffic patterns were conducted. One of the experiment setups is shown in Figure 5.8b. First the *WLAN* classification is tested, starting with high channel utilization (i.e. low data rate traffic), which makes the beacon frames sent by the AP harder to distinguish from the rest of the traffic. The medium channel utilization used next, might have similarities to the pattern generated by microwave ovens. Then a less utilized channel is researched (i.e. high data rate traffic), where the beacon frames stand out more, but the modulation schemes change between beacon frames and data traffic. For this the channel utilization might be so low that a misclassification as *BT2* could happen. The next batch of experiments deals with the classification of Bluetooth, where the unexpected, irregular channel selection of the Laptop is uncovered. Additionally, a real WLAN and a mixed environment of IEEE 802.11 and Bluetooth are tested. Finally, the detection of the *MWO* class is evaluated.

IEEE 802.11b, g, n

The IEEE Standard 802.11 affects at least four IEEE 802.15.4 channels (see Figure 1.2). The setup shown in Figure 5.8a was used to test the presented algorithm's ability to classify IEEE 802.11 interference. The interferers, Access Point 1 and the Laptop, were placed 4 m away from each other. Three Tmote Sky sensor nodes running the interference classification algorithm were placed in the middle between Access Point 1 and the Laptop. The Netbook that generated the data was connected to Access Point 1 via Ethernet, which then transmitted the data to the Laptop via IEEE 802.11. The WLAN traffic patterns generated to test the algorithm are described in the following.

High channel utilization To get an idea how the algorithm reacts under heavy channel loads, the tool JPerf 2.0.2 (Richasse, accessed January, 2013) was used. The heaviest congestion on the channel was generated using the slowest data rate, i.e. IEEE 802.11b. Note that, although higher data rates are often supported by today's hardware, the link can fall back to a lower data rate (as used in IEEE 802.11b) in bad RF conditions due to automatic data rate scaling (see Section 2.4.3 and Section 6.4.3). Furthermore, with higher data rates the theoretical, maximum channel utilization decreases (Joseph et al., 2013). With high channel utilization the actual beacon frames sent by the AP are less outstanding from the data traffic.

In the WLAN that was used here, the beacon frames sent by Access Point 1 had a length of 196 bytes at a data rate of 1 Mb/s and were sent at the default, pre-set interval of 102.4 ms. The



(a) Setup of the single technology experiments.

(b) Picture of the RF anechoic chamber setup during an experiment.

Figure 5.8: Algorithm testing for single interfering technologies.

communication between the two IEEE 802.11b communication partners took place on channel 11, which overlaps with the IEEE 802.15.4 channels 21, 22, 23 and 24. The theoretical maximal data rate is 11 Mb/s. In the setup used here, a throughput of up to roughly 5,800 kbit/s was achieved. The test included Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections. The Window Sizes (WSs) for TCP were 56, 1,000 and 2,000 KBytes. The WS has an effect on the number of Acknowledgments (ACKs) and therefore tunes the channel utilization. With fewer ACKs, fewer responses from the network partner have to be transmitted. Additionally, each test was run in a unidirectional, dual (i.e. alternating directions) and trade (i.e. at first in one direction, than in the other) mode. For UDP traffic a 1 MB/s and a 10 MB/s bandwidth link were used, where the second setup saturated the channel. This led to a maximum airtime-based channel utilization of up to 99.44% over one second on IEEE 802.15.4 channel 22 measured by the Tmote Sky sensor node. This measured channel utilization is greater than the given theoretical maximum in (Joseph et al., 2013), but the ED-based measurements of the Tmote Sky are not fast enough to reflect the channel utilization fully correctly.

Eleven different IEEE 802.11b data traffic settings were used in total, which resulted in 300 classifications¹.

The classification of IEEE 802.11 on the four fully overlapping channels achieved very good rates, always greater than 95.33% and had an average of 99.58%.

However, the adjacent channels 20 and 25 suffered from misclassifications and were only classified with 62.00% and 28.67% as *CLEAR*. These two channels were mainly classified as *UNKNOWN*, which can be explained as follows. The data traffic and the beacon frames have different modulation schemes even within the IEEE 802.11b standard. The beacon frames, sent with 1 Mbit/s, use baseband modulation of Differential Binary Phase Shift Keying (DBPSK) and the data traffic, sent with 11 Mbit/s, uses the so-called “higher rate” 8-chip Complementary Code Keying (CCK) modulation scheme (IEEE, 2007). Table 2.7 shows the different modulations of different standard versions. Vanheel et al. (2008) report similar observations, claiming that OFDM

¹Composition: 24 × full spectrum sweep interfered with by TCP WS 56 KBytes, 21 × TCP WS 1000 KBytes, 21 × TCP WS 2000 KBytes, 21 × TCP WS 56 KBytes dual, 21 × TCP WS 1000 KBytes dual, 24 × TCP WS 2000 KBytes dual, 54 × TCP WS 56 KBytes trade, 42 × TCP WS 1000 KBytes trade, 42 × TCP WS 2000 KBytes trade, 21 × UDP Bandwidth 1 MByte, 21 × UDP Bandwidth 10 MBytes

has a wider spectrum than Direct-Sequence Spread Spectrum (DSSS). This effect will become clearer in the following experiments (see Table 5.1). Due to the close proximity owing the limited physical dimensions of the RF anechoic chamber, the effect of the different keyings/modulations observed here is worse than in most real world setups with greater distances between the devices. With greater distance between the IEEE 802.15.4 node and the IEEE 802.11 device, the out-of-band energy of the latter is decreased and thus the problem of misclassification on adjacent channels is minimized. This decrease can be seen in Table 5.6 showing the results of a setup in which Access Point 2 is further away from the node in an uncontrolled environment.

Also the variance between the nodes was very high on the adjacent channels. This is due to the fact, that the nodes were not synchronized. Therefore the nodes might have slightly different sampling windows in time.

The rest of the channels which should not be affected by IEEE 802.11 was classified almost always correctly as *CLEAR*. The few misclassifications, decreasing with more distance of the WLAN center frequency, can only be explained due to out-off-band emissions of the IEEE 802.11 devices or erroneous CCA readings.

Medium channel utilization To evaluate the algorithm for medium channel utilization, different traffic patterns were used as suggested in Penna et al. (2009). The IEEE 802.11b traffic was generated by Distributed Internet Traffic Generator (D-ITG) (Dainotti et al., 2012), while the hardware and spatial setup stayed the same. Rates of 500, 250, 90, 45 and 9 TCP packets per second, each 1500 bytes long were sent, resulting in theoretical data rates of 6000, 3000, 1080, 540 and 108 kbit/s, respectively. Whereas the rate of 6000 kbit/s has not been achieved in our setup, only a rate of 4009 kbit/s could be measured, which is an acceptable performance for an IEEE 802.11b network (taking into consideration that the latter has only a theoretical data rate of 11 Mbit/s). For all three Tmote Sky sensor nodes in all five test cases, the classification of *WLAN* worked flawlessly on channels 21, 22, 23 and 24. Only a single experiment on a single node had a classification rate below 100% being an outlier with 83.33%. This results in 98.89% of correctly classified channels 21, 22, 23 and 24 over all experiments. The adjacent channels, 20 and 25, showed the same problem as described in the previous experiment.

Low channel utilization To investigate low channel utilization ($< 10\%$) further experiments with D-ITG generated traffic were conducted: 10 min of random data traffic have been sent from the Access Point 1 to the Laptop (uniformly distributed packet rate: 1 to 1000 packets per second and uniformly distributed packet size between 1 and 1000 bytes for TCP and UDP).

A summary of the results is shown in Tables 5.1a to 5.1d. The results in the tables are averaged over the three classifying nodes and broken down into channels. The detection results on the four mainly affected channels are very good, only in the IEEE 802.11n experiment (see Table 5.1c), a node (ID = 2) struggled for the TCP experiment on channel 21 for an unknown reason, dragging the average classification rate down and increasing the standard deviation given in parentheses. For 22 MHz wide channels the already discussed phenomena of misclassifications on adjacent channels occurred for all versions of IEEE 802.11. Table 5.1d shows another difficulty regarding IEEE 802.11n using the 40 MHz wide channel bonding. Besides the fact that the 40 MHz wide channel jams almost all the available frequencies, including e.g. the orthogonal IEEE 802.15.4 channel 20 (see Figure 1.2), the second channel cannot be identified by this algorithm. This is due to the fact that the second IEEE 802.11n channel is not used for beacon frames and actually is only connected for the data exchange between communication partners. The issue of the secondary channel of a 40 MHz wide IEEE 802.11n channel bonding is very challenging and to the best of the author's knowledge, it has not found greater recognition in the WSN community yet and remains an open research question.

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Channel	19	94.02 (8.14)	0.85 (1.48)	0.43 (0.74)	0 (0)	0 (0)	4.70 (5.92)
	20	82.05 (21.34)	0.43 (0.74)	0.85 (0.74)	0 (0)	0 (0)	16.67 (21.34)
	21	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	22	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	23	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	24	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	25	61.97 (28.16)	1.28 (2.22)	2.14 (1.96)	8.12 (2.67)	0 (0)	26.50 (25.00)
	26	99.57 (0.74)	0 (0)	0 (0)	0 (0)	0 (0)	0.43 (0.74)

(a) IEEE 802.11b (mainly overlapping channels 21-24 are colored green).

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Channel	19	97.01 (1.48)	0 (0)	1.28 (1.28)	0 (0)	0 (0)	1.71 (1.96)
	20	92.31 (4.62)	0.85 (0.74)	1.28 (1.28)	0 (0)	0 (0)	5.56 (3.70)
	21	0 (0)	0 (0)	0 (0)	99.57 (0.74)	0 (0)	0.43 (0.74)
	22	0 (0)	0 (0)	0 (0)	99.57 (0.74)	0 (0)	0.43 (0.74)
	23	0 (0)	0 (0)	0 (0)	99.57 (0.74)	0 (0)	0.43 (0.74)
	24	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	25	85.90 (2.22)	0 (0)	0.43 (0.74)	5.13 (3.85)	0 (0)	8.55 (2.67)
	26	100(0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

(b) IEEE 802.11g (mainly overlapping channels 21-24 are colored green).

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Channel	19	94.02 (5.92)	0.43 (0.74)	0.43 (0.74)	0 (0)	0 (0)	5.13 (5.59)
	20	85.47 (6.32)	0 (0)	1.28 (2.22)	0 (0)	0 (0)	13.25 (4.12)
	21	0 (0)	1.28 (2.22)	0.43 (0.74)	82.48 (28.16)	0 (0)	15.81 (26.28)
	22	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	23	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
	24	0 (0)	0 (0)	0.43 (0.74)	98.29 (2.96)	0 (0)	1.28 (2.22)
	25	78.21 (5.59)	0 (0)	1.28 (1.28)	8.55 (0.74)	0 (0)	11.97 (4.12)
	26	97.86 (0.74)	0 (0)	0 (0)	0 (0)	0 (0)	2.14 (0.74)

(c) IEEE 802.11n (mainly overlapping channels 21-24 are colored green).

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Channel	15	94.02(3.92)	0(0)	0.43(0.74)	0(0)	0(0)	5.56(4.12)
	16	91.03(3.85)	0.43(0.74)	0(0)	0(0)	0(0)	8.55(3.92)
	17	0(0)	17.09(4.12)	0.43(0.74)	0(0)	0(0)	82.48(3.70)
	18	0(0)	17.95(2.22)	0.85(1.48)	0(0)	0(0)	81.20(1.96)
	19	0.43(0.74)	17.95(1.28)	0.43(0.74)	0(0)	0(0)	81.20(1.96)
	20	0(0)	14.53(4.12)	0(0)	0(0)	0(0)	85.47(4.12)
	21	0(0)	0(0)	0(0)	99.57(0.74)	0(0)	0.43(0.74)
	22	0(0)	0(0)	0(0)	99.15(0.74)	0(0)	0.85(0.74)
	23	0(0)	0(0)	0(0)	99.57(0.74)	0(0)	0.43(0.74)
	24	0(0)	0(0)	0(0)	99.57(0.74)	0(0)	0.43(0.74)
	25	86.32(9.45)	0(0)	0(0)	7.69(5.59)	0(0)	5.98(3.92)
	26	97.44(3.39)	0.43(0.74)	0(0)	0(0)	0(0)	2.14(2.67)

(d) IEEE 802.11n channel bonding (mainly overlapping channels 17-24 are colored green).

Table 5.1: Controlled environment IEEE 802.11 experiments for low channel utilization summarized by channels. Classification results (%) of 78 classifications for each channel for different IEEE 802.11 versions. Low IEEE 802.11 traffic generated by D-ITG. The given result is the mean of three nodes (IDs = 2, 6, 9) and the standard deviation between nodes in parentheses.

Real-world channel utilization Additional to the artificially generated data traffic, the algorithm was tested in a more realistic setup in the RF anechoic chamber. Two clients were connected to the Access Point 1: the Netbook was connected with an IEEE 802.11g (54 Mbit/s) connection and the Laptop with an IEEE 802.11n connection using a single channel (72 Mbit/s). Both clients streamed a video. The spatial setup, which is shown in Figure 5.9, was as follows: the Access Point 1 was placed 1.20 m above the ground, while the Netbook was placed 3 m and the Laptop 5 m in distance to the Access Point 1 on the ground. The sensor nodes were spread between the Netbook and the Laptop. The classification results were again compelling as can be seen in Table 5.2, showing that the data traffic had no influence on the reliability of the AP classification. However, again on channel 21 the results vary most between the nodes. The out-of-band energy leading to misclassifications on adjacent channels increased slightly, since the sensor node were very close to the clients, which also transmit to the AP.

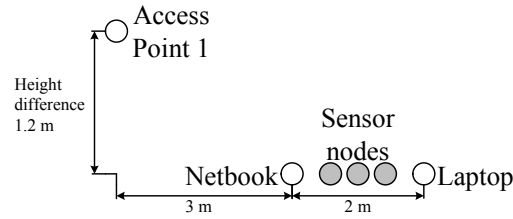


Figure 5.9: Setup of the experiment “real-world channel utilization”.

Channel	Predicted class (%)					
	<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
19	88.30 (13.40)	1.17 (1.01)	0.58 (1.01)	0 (0)	0 (0)	9.94 (11.68)
20	88.89 (7.91)	0 (0)	0.58 (1.01)	0 (0)	0 (0)	10.53 (7.02)
21	8.19 (8.83)	2.34 (2.68)	0.58 (1.01)	75.44 (19.54)	0 (0)	13.45 (9.00)
22	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
23	0 (0)	0 (0)	0 (0)	98.83 (2.03)	0 (0)	1.17 (2.03)
24	0.58 (1.01)	0 (0)	0 (0)	98.25 (3.04)	0 (0)	1.17 (2.03)
25	89.47 (6.33)	1.17 (1.01)	0.58 (1.01)	0 (0)	0 (0)	8.77 (6.33)
26	92.40 (7.09)	0 (0)	0 (0)	0 (0)	0 (0)	7.60 (7.09)

Table 5.2: Controlled environment IEEE 802.11 experiments for real-world utilization summarized by channels. Classification results (%) of 57 classifications for each channel. IEEE 802.11 video streaming with two clients (mainly overlapping channels 21-24 are colored green). The given result is the mean of three nodes (IDs = 2, 6, 9) and the standard deviation between nodes in parentheses.

Bluetooth

The classification quality of Bluetooth was evaluated in multiple experiments. The distance between the two Bluetooth communication partners was 4 m in all experiments described in the following. The sensor nodes were placed in the middle between them, as shown in Figure 5.8a. The traffic of the Bluetooth connection was monitored on the Logical Link Control and Adaptation Protocol (L2CAP) Layer with hcidump (Krasnyansky and Holtmann, 2002) on the Laptop running Linux. The L2CAP Layer roughly corresponds to the Data Link layer of the Open Systems Interconnection (OSI) Reference Model. The Netbook used Windows XP as operating system.

In the first experiment, an audio file was streamed from the Laptop to the Headset. The stream was based on extended Synchronous Connection-Oriented (eSCO) links with 60 information bytes packed into an Extended Voice (EV) packet sent with an Enhanced Data Rate (EDR). The resulting packets stayed in the time limitation under 625 μ s. Hence the according algorithm return is *BT1*, the results are shown in the row “Laptop to Headset (eSCO)” in Table 5.3a. The second experiment “Netbook to Headset (eSCO)” was equal to the previous, but this time the Netbook was used instead of the Laptop.

The third experiment was a data transfer from the Laptop to the Mobile Phone. This experiment was followed by a transfer in the opposite direction. The experiments are shown in the rows “Laptop to Mobile (Asynchronous Connection-Less (ACL))” and “Mobile to Laptop (ACL)”. Again, these two experiments have been repeated with the Netbook instead of the Laptop. Finally, the data was transferred between the Laptop and the Netbook, with the Netbook supporting a newer version of Bluetooth than the Mobile Phone and hence the transfer was different to the one in the previous setup. Again, both directions were tested and are shown in Table 5.3a.

Although Table 5.3a merely shows the example results of a single node for better clarity, the results of other nodes did not vary significantly. Node 2 was used for most of the experiments. The change to Node 9 is due to later conducted experiments after the unequal channel selection of the Laptop was discovered. Since the results are already averaged over 16 channels only a single node and no standard deviation is presented. However, for cases with a high variance between different channels will be discussed in the following.

		Predicted class (%)					<i>UNKNOWN</i>
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	
Experiment	Laptop to Headset (eSCO)[16×39] (Node 2)	0.00	94.71	1.28	0.00	0.00	4.01
	Netbook to Headset (eSCO)[16×69] (Node 9)	0.00	99.37	0.18	0.00	0.00	0.45
	Laptop to Mobile (ACL) [16×57] (Node 2)	11.95	8.99	71.82	0.00	0.00	7.24
	Mobile to Laptop (ACL) [16×45] (Node 2)	0.69	0.00	96.94	0.00	0.00	2.36
	Netbook to Mobile (ACL) [16×66] (Node 9)	0	22.16	76.99	0.00	0.00	0.85
	Mobile to Netbook (ACL) [16×57] (Node 9)	0	0.11	95.72	0.00	0.00	4.17
	Laptop to Netbook (ACL) [16×33] (Node 2)	38.45	0.00	60.42	0.95	0.00	0.19
	Netbook to Laptop (ACL) [16×36] (Node 2)	1.04	0.00	96.53	0.00	0.00	2.43

(a) Bluetooth summarized by experiments. Classification results (%) of different Bluetooth experiments classified by single nodes. The number of classifications is given in brackets. Channel details of the worst results in row “Laptop to Netbook (ACL)” are shown in Table 5.3b.

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Channel	11	0	0	100	0	0	0
	12	0	0	93.94	6.06	0	0
	13	0	0	100	0	0	0
	14	90.91	0	9.09	0	0	0
	15	100	0	0	0	0	0
	16	100	0	0	0	0	0
	17	100	0	0	0	0	0
	18	0	0	100	0	0	0
	19	0	0	100	0	0	0
	20	0	0	93.94	6.06	0	0
	21	96.97	0	0	0	0	3.03
	22	0	0	100	0	0	0
	23	0	0	96.97	3.03	0	0
	24	27.27	0	72.73	0	0	0
	25	100	0	0	0	0	0
	26	0	0	100	0	0	0
	mean	38.45	0	60.42	0.95	0	0.19

(b) Worst Bluetooth results by channels revealing unused frequencies of the Laptop. Detailed classification results (%) of 33 classifications per channel. Bluetooth FTP traffic (ACL packets) from Laptop to Netbook classified by Node 2. This experiment has the worst average classification result of all Bluetooth classifications, since some channels (14, 15, 16, 17, 21 and 25) are clear all the time.

Table 5.3: Controlled environment Bluetooth experiments summarized by experiments and details of experiment with the worst classification rate.

The eSCO packets were classified well in Experiment 1. In Table 5.3a the sum over all channels is shown for the experiment, but a detailed view reveals that most channels had a 100% classification rate, while other channels had a lower rate (down to 69.23%). On these channels the traffic was misclassified as *UNKNOWN*. Experiment 2 reaches a nearly 100% classification rate. The channels in Experiment 2 are more equally used as by the Laptop. The phenomenon of the unequal channels for all connections with the Laptop occurs in all the following experiments.

In the remaining experiments ACL packets were transmitted, using one, three or five time slots and hence making the traffic more difficult to identify. However, as shown in Table 5.3a the classification rates were still satisfactory. Note that almost no misclassifications as *WLAN* and no *MWO* misclassifications were made.

When the Laptop was used as sender, some channels were unused. The worst case, occurring in the experiment “Laptop to Netbook (ACL)”, is shown in more detail in Table 5.3b. Channel 14, 15, 16, 17, 21 and 25 are idle, classified as *CLEAR*, most of the time. Since the author used off-the-shelf hardware and driver software, the reason for this is not fully clear. Although the Wi-Fi card of the Laptop was deactivated during the experiments, a WLAN-Bluetooth coexistence mechanism possibly could have blocked channels. The Netbook-based connections show more uniformly spread results with all channels be equally, correctly classified (with *BT1+BT2* being 99.15% and 95.83% for Experiment “Netbook to Mobile (ACL)” and “Mobile to Netbook (ACL)”).

Channel	Predicted class (%)					
	<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
11	19.84 (20.25)	48.41 (4.96)	22.22 (30.24)	0 (0)	0 (0)	9.52 (14.48)
12	0 (0)	84.13 (17.55)	13.49 (19.25)	0 (0)	0 (0)	2.38 (4.12)
13	0 (0)	59.52 (38.32)	30.95 (45.43)	0 (0)	0 (0)	9.52 (14.48)
14	23.02 (30.15)	60.32 (26.55)	4.76 (4.12)	0 (0)	0 (0)	11.90 (20.62)
15	0 (0)	63.49 (48.81)	36.51 (48.81)	0 (0)	0 (0)	0 (0)
16	0 (0)	71.43 (26.51)	9.52 (12.60)	0 (0)	0 (0)	19.05 (28.97)
17	23.02 (28.41)	48.41 (7.27)	19.05 (26.83)	0 (0)	0 (0)	9.52 (14.48)
18	11.11 (19.25)	57.14 (21.43)	23.02 (35.74)	0 (0)	0 (0)	8.73 (9.62)
19	25.40 (21.99)	54.76 (9.52)	13.49 (17.22)	0 (0)	0 (0)	6.35 (4.96)
20	43.65 (28.41)	30.16 (5.99)	7.14 (10.38)	0 (0)	0 (0)	19.05 (15.61)
21	2.38 (4.12)	0 (0)	0 (0)	94.44 (7.65)	0 (0)	3.17 (3.64)
22	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
23	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
24	0 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)
25	0 (0)	70.63 (24.44)	12.70 (15.85)	0.79 (1.37)	0 (0)	15.87 (25.46)
26	0 (0)	97.62 (2.38)	1.59 (1.37)	0 (0)	0 (0)	0.79 (1.37)

Table 5.4: Controlled environment IEEE 802.11 and Bluetooth experiment summarized by channels. Classification results (%) of 57 classifications for each channel. IEEE 802.11 video streaming with two clients, Bluetooth audio streaming (eSCO) from the Laptop to the Headset (expected classifications are colored green). The given result is the mean of three nodes (IDs = 2, 6, 9) and the standard deviation between nodes in parentheses.

It could be argued that a longer classification time improves the results of the algorithm, but from a theoretical point of view this is unnecessary. A time slot, which is normally the time the frequency is kept, is $1/1600$ s. Since the master has to poll data in a piconet, in the first time slot a packet is requested and then the client keeps the channel for a maximum of five time slots to send the multi-slot ACL packet. This results in two channel changes in six time slots. In theory, this means that at least: $2 \times (1/79) \times (1600/6) \approx 6.75$ times a second the same frequency should be used. Additionally, the IEEE 802.15.4 channel covers three Bluetooth channels and therefore the channel should be used sufficiently to detect Bluetooth. If the channel is utilized less than that (which can be the case for some Bluetooth packet types with negotiable transmit intervals), the sense of interference classification is questionable, since the effect of interference is negligible. In fact, the effect of Bluetooth interference is so weak, that IASA MAC does not react to it, as shown in Section 7.6.

The last IEEE 802.11 experiment, “real-world channel utilization”, was redone with an additional Bluetooth audio link generating eSCO traffic. The video streaming Laptop client used the Bluetooth Headset to listen to the sound. All other setup properties, including the Netbook, stayed the same. The WLAN was already established and used when the Bluetooth connection was established and thus the Adaptive Frequency Hopping (AFH) mechanism or the method used by the Laptop to choose the channel for Bluetooth had enough time to adapt its channel choice before the classification was started. The results are shown in Table 5.4 and attest the expected behavior: Bluetooth is not detected on the channels used by IEEE 802.11 (21, 22, 23 and 24). This behavior is expected since the IEEE 802.11 frequencies are blacklisted by Bluetooth, as shown in Figure 2.35a for an illustration of AFH. If AFH had not been used, the WLAN traffic would dominate on the overlapping channels, which would make the Bluetooth traffic hard to detect.

Microwave Ovens

To test the classification rate of the algorithm for microwave ovens, 500 ml of water in a plastic bowl were placed inside Microwave Oven 1 and heated with full power for 5 minutes. In front of the microwave, nodes were placed 0.5 m, 1.0 m, 1.5 m and 2 m away. The classification results of the most affected channels (18, 19, 20 and 21) are shown in Table 5.5a. These channels around the center frequency of the microwave oven were classified mainly correctly.

As for IEEE 802.11, channels further away of the center frequency of the interferer are much harder to classify since they do not suffer from the typical interference pattern, but from harmonics.

		Predicted class (%)					
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
Distance	0.5 m (Node 4)	0	0	4.17	0	88.89	6.94
	1.0 m (Node 2)	0	0	1.39	0	95.83	2.78
	1.5 m (Node 6)	0	0	1.39	0	86.11	12.5
	2.0 m (Node 9)	0	0	1.39	0	88.98	9.72

(a) Microwave oven summarized by distance. Summed up classification results (%) of IEEE 802.15.4 channels 18, 19, 20, 21. Microwave Oven 1 heating 500 ml water at full power. The number of samples per channel is 18 = average over 72 results shown per setup. Channel details of the nearest node in row “0.5 m (Node 4)” are shown in Table 5.5b.

		Predicted class (%)						<i>cu</i>
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>	
Channel	11	100	0	0	0	0	0	0
	12	100	0	0	0	0	0	0
	13	100	0	0	0	0	0	0
	14	83.33	11.11	0	0	0	5.56	0.01
	15	11.11	77.78	0	0	0	11.11	1.45
	16	5.56	0	16.67	0	38.89	38.89	18.15
	17	0	0	33.33	0	0	66.67	10.24
	18	0	0	5.56	0	72.22	22.22	35.28
	19	0	0	0	0	100	0	44.33
	20	0	0	0	0	100	0	42.43
	21	0	0	11.11	0	83.33	5.56	33.33
	22	5.56	44.44	5.56	0	0	44.44	3.44
	23	72.22	5.56	0	0	0	22.22	0.01
	24	100	0	0	0	0	0	0
	25	100	0	0	0	0	0	0
	26	100	0	0	0	0	0	0

(b) Microwave oven summarized by channels. Detailed classification results (%) of Node 4 being 0.5 m away from Microwave Oven 1. Detailed classification results (%) of 18 classifications per channel. For a better evaluation the measured channel utilization *cu* for the classifications are also given.

Table 5.5: Controlled environment microwave oven experiment summarized by distance and details of node closest to the oven.

Table 5.5b shows the results of 18 full spectrum sweeps for the 0.5 m setup, where the node was closest to the microwave. On channels further away from the center frequency, it might happen that the energy is just around the CCA threshold and only very few CCA requests report a busy channel, which can be mistaken with Bluetooth (*BT2*), since 50 Hz are a divisor of 1600 Hz.

5.4.2 Uncontrolled Environment

In addition to the tests in the RF anechoic chamber, which delivered results from an ideal environment, tests were also conducted in a detached house. This added effects as reflections and multi-path propagation to the setup. Additionally, the devices used in these experiments have not been part of any training set used to develop the algorithm. Therefore, the following tests can be considered to be challenging and far beyond the testing reported for the reviewed algorithms in Section 5.1.

IEEE 802.11g

Access Point 2 was in another room on the second floor, thus the received signal was around -50 dBm at the Laptop next to the sensor nodes on the first floor. The distance between the two devices was around 10 m on the plane and roughly 2.50 m in height with multiple rooms between them. The beacon frames were sent in the default interval of 100 tu at a data rate of 1 Mbit/s and were 189 bytes long. The classification algorithm ran for 10 min, resulting in 51 full channel sweeps. For further details see Table 5.6. Since IEEE 802.11g used channel 1, the IEEE 802.15.4 channels 11, 12, 13 and 14 were supposed to be affected. There was notably less misclassification on adjacent channels, which is due to the fact that the Power Spectral Density (PSD) of the beacon frames sent with a low data rate modulation has a distinct maximum at the center frequency. Furthermore, the distance and therefore the attenuation in this scenario were much higher than in the measurements in the controlled environment (see Section 5.4.1). Even channels 11 and 14,

Channel	Predicted class (%)					
	<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>
11	22.88 (32.89)	0 (0)	0 (0)	57.52 (50.77)	0 (0)	19.61 (18.70)
12	1.31 (2.26)	0 (0)	0 (0)	94.77 (2.26)	0 (0)	3.92 (3.92)
13	1.31 (2.26)	0 (0)	0 (0)	93.46 (1.13)	0 (0)	5.23 (1.13)
14	64.71 (52.87)	0 (0)	0 (0)	31.37 (54.34)	0 (0)	3.92 (5.19)
15	100 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
16	100 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Table 5.6: Uncontrolled environment IEEE 802.11 experiments summarized by channels. Classification results (%) of 51 classifications per channel for low, real-world IEEE 802.11 traffic (mainly overlapping channels 11-14 are colored green). The given result presents the mean of three nodes (IDs = 2, 6, 9) and the standard deviation between nodes in parentheses.

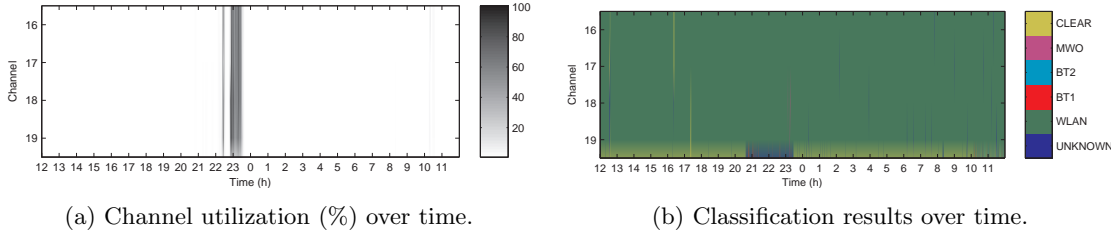


Figure 5.10: Results of a 24-hour long-term evaluation of the classification algorithm in a real-world environment (trace of a single node).

which are fully overlapped by the 22 MHz wide IEEE 802.11 channel were less interfered and thus less often classified as *WLAN*.

Bluetooth

To evaluate the Bluetooth classification rate, again a new untested device was used: the Wireless Keyboard was connected to the Laptop and placed on the same table as the sensor nodes (IDs = 2, 4, 6) and the Laptop. The classification ran for 10 min resulting in 45 full channel sweeps. The test results were acceptable: over all 16 channels, the *BT1+BT2* classification rate showed an average of 73.61%, 75.69% and 60.14% for the three different nodes and almost all of these classifications were the expected *BT1* class. All misclassifications were *CLEAR* or *UNKNOWN* with no particular channel differences. Since there is not much data to transmit for the Wireless Keyboard, it can be assumed that the traffic was very low and therefore hard to detect. However, it is unclear why the channel selection was more homogeneous than in previous tests.

Microwave Ovens

For this experiment, Microwave Oven 2 was used to heat 500 ml of water in a plastic bowl for 5 min and the sensor nodes were placed 0.5 m away from the front side of the oven. As it can be seen in Table 5.7, the classification results were only modest. The best classification rate was achieved on channel 23 (center frequency of 2465 MHz), while channel 20 (2450 MHz) was expected.

However, these results reflect what the channel utilization *cu* shows. The average values were at first increasing from 6.35% for channel 11 to 22.76% for channel 20 and reaching their maxima with 33.14% and 33.89% for channels 22 and 23. Then the value was dropping to 6.92% on channel 26. The fact that microwave ovens are not standardized communication devices is reflected in the values of these measurements.

Long-term IEEE 802.11g

Since all experiments described so far were limited in time duration, a 24-hour long-term experiment was conducted in the same residential environment as all the uncontrolled environment experiments in this section. The channel sweep was timed to start every two minutes and a channel classification

		Predicted class (%)						
		<i>CLEAR</i>	<i>BT1</i>	<i>BT2</i>	<i>WLAN</i>	<i>MWO</i>	<i>UNKNOWN</i>	<i>cu</i>
Channel	11	0 (0)	0 (0)	1.59 (2.75)	0 (0)	0 (0)	98.41 (2.75)	6.35 (0.57)
	12	0 (0)	0 (0)	11.11 (2.75)	0 (0)	0 (0)	88.89 (2.75)	7.57 (0.62)
	13	0 (0)	0 (0)	36.51 (5.50)	0 (0)	0 (0)	63.49 (5.50)	8.66 (0.45)
	14	0 (0)	0 (0)	23.81 (4.76)	0 (0)	4.76 (0)	71.43 (4.76)	10.97 (0.74)
	15	0 (0)	0 (0)	11.11 (2.75)	1.59 (2.75)	7.94 (7.27)	79.37 (9.91)	12.38 (2.68)
	16	1.59 (2.75)	1.59 (2.75)	12.70 (7.27)	1.59 (2.75)	4.76 (4.76)	77.78 (7.27)	10.17 (2.32)
	17	0 (0)	1.59 (2.75)	9.52 (0)	0 (0)	7.94 (9.91)	80.95 (8.25)	11.90 (3.57)
	18	0 (0)	3.17 (2.75)	11.11 (7.27)	0 (0)	14.29 (17.17)	71.43 (12.60)	14.54 (7.30)
	19	1.59 (2.75)	3.17 (5.50)	4.76 (8.25)	0 (0)	15.87 (11.98)	74.60 (5.50)	16.37 (6.90)
	20	0 (0)	0 (0)	4.76 (4.76)	1.59 (2.75)	31.75 (23.97)	61.90 (23.81)	22.76 (7.77)
	21	0 (0)	3.17 (5.50)	3.17 (2.75)	0 (0)	46.03 (7.27)	47.62 (4.76)	26.00 (2.62)
	22	0 (0)	1.59 (2.75)	0 (0)	4.76 (0)	66.67 (8.25)	26.98 (5.50)	33.14 (5.00)
	23	1.59 (2.75)	1.59 (2.75)	3.17 (5.50)	3.17 (2.75)	68.25 (21.47)	22.22 (16.72)	33.89 (6.42)
	24	1.59 (2.75)	0 (0)	1.59 (2.75)	0 (0)	49.21 (21.47)	47.62 (17.17)	24.76 (8.21)
	25	0 (0)	1.59 (2.75)	9.52 (4.76)	3.17 (5.50)	15.87 (9.91)	69.84 (5.50)	15.99 (3.53)
	26	3.17 (5.50)	12.70 (14.55)	12.70 (13.75)	0 (0)	1.59 (2.75)	69.84 (21.99)	6.92 (2.39)

Table 5.7: Uncontrolled environment microwave oven summarized by channel. Classification results (%) of 21 classifications per channel 0.5 m away from Microwave Oven 2 in an uncontrolled residential environment. The given result presents the mean of three nodes (IDs = 2,4,6) and the standard deviation between nodes in parentheses. For a better evaluation the measured channel utilization *cu* for the classifications are also given.

started every two seconds, with three classifications on the same channel before the channel was changed. Thus, the early returns did not affect the timing and 720 full channel sweeps were performed resulting in 2,160 classifications per channel.

Access Point 2 was operating on IEEE 802.11 channel 6, which overlaps with IEEE 802.15.4 channels 16, 17, 18 and 19. During the experiment multiple laptops, a desktop computer and a smartphone have been active as clients. Additionally, Bluetooth traffic was generated by the Wireless Keyboard, which was connected to a generic Bluetooth dongle plugged into the desktop computer.

This experiment generated a trace of the algorithm output over a long time. However, since this experiment was performed in a live environment, there is no ground truth data. Therefore, only the results for the *WLAN* class can be evaluated, since the *WLAN* was, as in common practice, permanently announced. The Wireless Keyboard was just used during a time span in the evening. The *WLAN* classification worked reliably with 99.7222%, 99.5833%, 99.4907% and 99.3056% correct classifications on channel 16 to 19.

In Subfigure 5.10a, the channel utilization is shown, which is commonly used to categorize channels (e.g. (ZigBee Alliance, 2008b)). When Subfigure 5.10a and 5.10b are compared, it can be seen that the presented classification algorithm delivers much more information than the simple channel utilization. Due to the beacon detection, a *WLAN* is detected as a possible source of interference, although it might be idle at the moment and the IEEE 802.11 channel is not used. A simple threshold of the channel utilization cannot detect IEEE 802.11 for most of the time and therefore, channels 16, 17, 18 and 19 would be considered as good choices. In the late evening from 22:30 to 23:30, the channels are under heavy interference, because the *WLAN* was used by multiple clients. In this case, an earlier detection and avoidance of the IEEE 802.11 channels would prevent interference, which would lead to a channel change. Thus, especially the detection of IEEE 802.11 is useful for a long-term channel planning. Since the algorithm also measures the channel utilization internally, the resulting class can be further judged by the actual medium use.

This example shows the potential of the presented algorithm for real world WSN deployments. Furthermore, this algorithm is used for a smart MAC protocol in Chapter 7.

5.5 Summary and Discussion

In this chapter, an algorithm was introduced to classify one second, or in most cases a shorter trace, of CCA samples into one of six classes, namely: idle channel (*CLEAR*), Bluetooth single-slot packets (*BT1*), Bluetooth multi-slot packets (*BT2*), IEEE 802.11-based WLANs (*WLAN*), microwave ovens (*MWO*) or an unknown source of interference (*UNKNOWN*). If the classification is interrupted by receiving an IEEE 802.15.4 packet, the classification of the source of interference is not finalized and the *INTERNAL* class is returned. Related work was reviewed to give an overview of the state-of-the-art. Furthermore, the algorithm classes and the algorithm implementation were described and finally the algorithm was tested in multiple scenarios.

5.5.1 Classification Results

The extensive testing of the algorithm conducted in this chapter allows the following conclusion of the classification performance: The *WLAN* classification worked well for 22 MHz wide channels. The phenomena that adjacent channels were often interfered, but misclassified can, as already mentioned, be explained with the different modulations and the close distance. The PSD of DSSS is slightly rising and falling, almost a bit round (see Figure 2.29a). This implies that channels further away from the IEEE 802.11 center frequency are less affected by the beacon frames and therefore harder to classify. The PSD of OFDM, which is used for the data traffic in the newer versions of the IEEE 802.11 standard, is due to the multiple sub-carriers more rectangular as shown in Figure 2.29b. Therefore the data traffic might still affect an IEEE 802.15.4 channel, on which the beacon frames are received below the CCA limit. Nevertheless, the experiments also showed that the data traffic in the WLAN has little to no effect on the classification rate.

The Bluetooth classification here represented by two classes *BT1* and *BT2*, works satisfactorily. On the used Laptop some channels were avoided, which decreased the overall classification rate. However, if a channel is not used by Bluetooth, it cannot be classified as such, thus the sometimes low classification rate is a pessimistic measure. Also, Bluetooth interferes only very little on a single IEEE 802.15.4 channel and therefore there is little to measure.

The *MWO* class delivered only moderate classification results, especially in the uncontrolled environment. Since microwave ovens have no standards nor specifications for the emission of radiation as communication technologies have, this problem is not fully solvable. Although in countries with a different electrical system providing a different frequency, e.g. North America, the algorithm has to be slightly adapted.

To give an overall classification rate or a comparison to methods suggested in literature is difficult, since multiple factors influence the classification rate, including traffic/modulation of interferer, spectral overlap, distance, and CCA threshold. However, the reported rates and the test setups are shortly reviewed in the following to provide a rough possibility of comparison.

Zhou et al. (2010) evaluate their AP beacon detection with four different APs and traffic generated by D-ITG. Additionally, they check their approach for cross-sensitivity with IEEE 802.15.4 traffic. They report a detection rate of 95%, the frequency offset is not mentioned, but the runtime of the algorithm. If only the two IEEE 802.15.4 channels next to the center frequency of the used IEEE 802.11 AP are used, the algorithm presented here has a higher detection rate in the controlled environment and a comparable rate in the uncontrolled environment.

Chowdhury and Akyildiz (2009) evaluate their approach with simulations and do not state a classification rate for IEEE 802.11 or microwave ovens. Similar no statement is made by Bloessl et al. (2012) and Nicolas and Marot (2012).

Ansari et al. (2011) state a 96% detection rate of IEEE 802.11, but they only detect a single class in a near-ideal environment without any cross-sensitivity or control group.

The publications of Hermans et al. (2012); Rensfelt et al. (2012) and Hermans et al. (2013) developing SoNIC are the most comparable to the algorithm presented here and since the latter publication is the most recent and best evaluated one, the author will refer to it. Hermans et al. (2013) claims to detect the predominant source of interference in an office environment with 87%. However, confusion matrices given in their work show that especially the IEEE 802.11 detection is relative low with 82.0%. Further due to not clear frequency offsets and different devices used, the rates cannot be directly compared to the work presented here. As already mention in Section 5.1 the algorithm presented here is, to the best of the author’s knowledge, the only one distinguishing between single-slot (*BT1*) and multi-slot (*BT2*) Bluetooth packets. The author believes that the Bluetooth packet length has effects in the pattern of the corrupted bits. Further, it is not only the varying airtime of Bluetooth, but also the modulations changes (see Sections 2.5.2 and 2.5.1 for details).

Additionally, the detection of bonded channels used by IEEE 802.11n has not been discussed in literature, yet.

A common limit is that only a single, at least per channel, source of interference can be detected. Airshark (Rayanchu et al., 2011) can detect multiple interferers at once. However, due to the used IEEE 802.11-based hardware and a computer for their computations, they have more possibilities than approaches based on IEEE 802.15.4-compliant radios and microcontrollers have. Due to the inability of IEEE 802.15.4 radios to demodulate signals and the blurry ED, this limit is very challenging to overcome. Nevertheless, in the unlikely case of different interferers overlapping in frequency, the approach presented here only detects the source with the highest channel utilization. This is also equal to the timing of decisions (see Figure 5.7): Microwave ovens (which do not back off for other participants), IEEE 802.11 and then Bluetooth (being the weakest technology with inbuilt external interference avoidance with the help of AFH).

In SoNIC (Hermans et al., 2013; Rensfelt et al., 2012) a weak IEEE 802.15.4 link is an additional class, but the approach presented here using ED instead of corrupted bits, makes the distinction easy, since for weak links there is no high background noise level generated by external interferers. This thesis focuses on external interference in the 2.4 GHz frequency band and therefore weak signals due to long distances between the nodes are not considered further.

Another influencing factor is internal interference. Since the algorithm presented here can still receive packets, it can react to traffic within its WSN. However the CCA trace is influenced due to the IEEE 802.15.4 traffic and the algorithm represents the packet reception with the help of the *INTERNAL* pseudo-class. Depending on the use of the classification the *INTERNAL* result might lead to a restart of the algorithm.

5.5.2 Execution Time

Besides the classification rate, which should be as high as possible to prevent the decision for an unsuitable mitigation strategy, the execution time is a vital feature of interference classification. The execution time, i.e. the time after which enough samples have been collected to end the algorithm and return a result, is important to adapt the communication as fast as possible. For most experiments conducted, it has been close to the theoretical minimum. In theory, at least 5040 samples (≈ 615 ms, as shown in Figure 5.7) are needed to classify IEEE 802.11. In the experiments for high, medium and low channel utilization, the data sets were classified quickly with an average of 5187.95 samples (≈ 633 ms) calculated of all datasets that have been classified as *WLAN* of all nodes. This fast response was expected in such an ideal environment, but also in the real world tests described in Section 5.4.2 the response was only slightly slower with an average return time of 5650.41 samples (≈ 690 ms). The algorithm thereby outperforms Zifi (Zhou et al., 2010) stating a detection time of 786.4 ms (for a beacon interval of 96 tu instead of the default 100 tu) per channel.

WiSpot (Ansari et al., 2011) equipped with additional hardware is faster for a single channel with 500 ms (RSSI mode) or 266 ms (RSSI+CCA mode), but is designed as a full spectrum scanner resulting in a whole spectrum scanning duration of 3.75 s (RSSI mode) or 2.33 s (RSSI+CCA mode). However, the interference classification algorithm presented here has no need to change the channel and thus the sensor node can permanently stay connected to the network. For the other classes no reference timings could be found. Only SoNIC offers a comparable range of classes. The interference classification in SoNIC is based on corrupted packets and therefore depends on how many packets are sent in the WSN and on the resulting number of received corrupted packets. For an analysis the packet must also be received uncorrupted from a retransmission. However, in (Hermans et al., 2013) the final decision for the resulting mitigation strategy is made after a voting phase 30 s or 10 s.

Chapter 6

Interference Mitigation

After discussing the effects and classification of external interference, this chapter presents solutions to the problem of interference. Since interference, either due to background noise, internal, or external sources of interference, is a common problem in wireless communication, different approaches to mitigate the effects of interference have been developed over time. In the following, the most important and suitable ones for IEEE 802.15.4 are discussed.

6.1 Interference Mitigation Strategies of IEEE 802.15.4

To overcome the problem of internal and external interference, different approaches have been developed and presented in literature. These approaches are commonly known as interference mitigation strategies, but they can also be referred to as coexistence mechanisms (e.g. by Farahani (2008)), transmission adaptation (e.g. by Chowdhury and Akyildiz (2009)) or countermeasures (e.g. by Nicolas and Marot (2012)). In the following, the term interference mitigation will be used. As an introduction to this topic, the state-of-the-art is reviewed.

IEEE (2003b) mentions the following mechanisms of IEEE 802.15.4 to improve the coexistence with other wireless devices:

- The *neighbor piconet capability* is stated to be out of scope in (IEEE, 2003b) and is therefore left in a vague and open description. In this work, routing in the Network Layer for mesh networks is discussed in general, since piconets are just applicable in Hierarchical Routing topologies (also being introduced in Section 6.2.1).
- A *low duty cycle* refers to the transmission of a few, short packets that lead to a low channel utilization. The attempt of splitting data into short packets (packet fragmentation) is analyzed in Section 6.3.2.
- The *Clear Channel Assessment (CCA)* has been already reviewed with regard to different aspects, but in the following it is reviewed as part of the Carrier Sense Multiple Access (CSMA)/Collision Avoidance (CA) approach in Section 6.3.3.
- The *Energy Detection (ED)* and the *Link Quality Indication (LQI)* are also mentioned in (IEEE, 2003b). The ED has been extensively examined throughout this work and is an important building block for other mitigation strategies and as such, it is reviewed within these strategies. The LQI is not fully specified in (IEEE, 2003b), but it should use the ED as part of it to indicate the quality/strength of a received packet (e.g. by a Signal to Noise Ratio (SNR) estimation).
- The *Modulation* has been explained in Section 2.3.3 and is reviewed concerning the benefits of interference mitigation in Section 6.4.2.

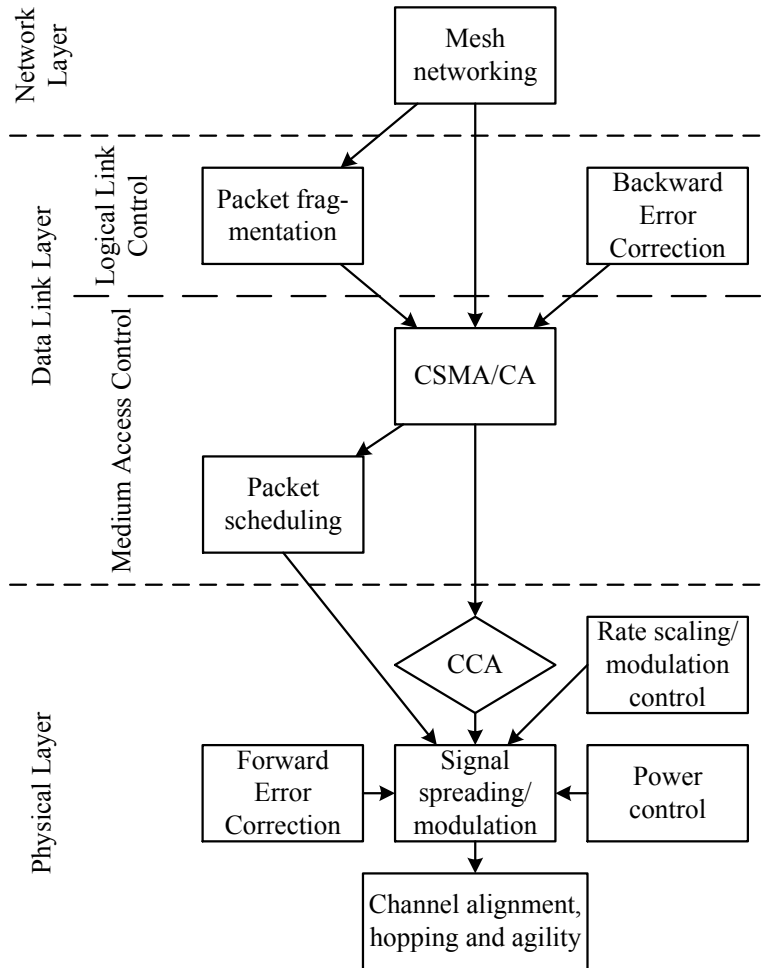


Figure 6.1: Interference mitigation strategies structured according to the OSI Reference Model Layers, in which they are commonly implemented, and relations between the different strategies.

- *Low transmit power* is an obvious property of a low power technology such as IEEE 802.15.4. However, the idea of using as little power as required in the form of power control is researched in Section 6.4.4.
- *Channel alignment* and *dynamic channel selection* are discussed in Section 6.4.5.

Some approaches from this basic list are related to others and some provide interference mitigation more as a side effect than as a main intention. In the following, these approaches and further strategies are discussed. Figure 6.1 gives a rough classification according to the Open Systems Interconnection (OSI) Reference Model Layers and shows the common interconnections between the different approaches. These approaches will be discussed in order, from the higher layers down to the Physical (PHY) Layer.

6.2 Network Layer

The Network Layer is only implied, but not specified in IEEE 802.15.4 and therefore it is beyond the main focus of this thesis. However, it cannot be fully ignored, since it has the potential to avoid interference. The main task of the Network Layer is the routing of packets from an initial sender to the final receiver. In Wireless Sensor Networks (WSNs), multi-hop communication in a mesh network topology is one of the most emphasized and promising features (IEEE, 2003b; ZigBee

Alliance, 2008b; HART Communication Foundation, last accessed April 2014) and therefore its implication to overcome interference are discussed in the following.

6.2.1 Mesh Networking

As mentioned in Section 2.3.3, only a limited transmit power and thereby limited communication range is supported by IEEE 802.15.4. Furthermore, in Section 6.4.4 the advantages and disadvantages of variable transmit powers are discussed. Hence, WSNs can be organized as mesh networks in the Network Layer in order to overcome long distances. Nodes that are locally interfered (e.g. the nodes in the kitchen next to an operating microwave oven) can be avoided by rerouting the traffic around them if the network is large and dense. Up to now, there is no dominant routing protocol suitable for all WSNs, although Internet Protocol version 6 over Low power Wireless Personal Area Networks (6LoWPAN)-based solutions gain popularity (as mention in Section 2.3.1).

6LoWPAN and ZigBee rely on the principle of Ad-hoc On-demand Distance Vector (AODV) routing (Perkins and Royer, 1999; C. Perkins, 2003). AODV is a flat routing protocol and this group of protocols is introduced in the following.

While an extensive review of all the available routing protocols is beyond the scope of this work, a short overview of the main research directions is given in the following. More extensive overviews are given in (Boukerche et al., 2009a; Akkaya and Younis, 2005). The introduced protocols are grouped by the common name for the approach found in literature.

Flat Routing Protocols

Flat routing protocols are used in homogeneous WSN topologies. The latter are accepted as a suitable topology for large, random deployments, e.g. when an enormous number of identical sensor nodes is spread from an airplane over an area of interest. These sensor nodes have no Identification (ID) or special functionality and do not need to know about their exact positions.

Flat routing protocols are e.g. Gradient Broadcast (GRAB) (Ye et al., 2005), the Minimum Cost Forwarding Algorithm (MCFA) (Ye et al., 2001) and the already mentioned AODV (Perkins and Royer, 1999; C. Perkins, 2003).

Hierarchical Routing Protocols

In hierarchical routing protocols, the nodes are grouped into different levels of a hierarchy. These levels may fulfill different functionalities or may be clusters, which represent local areas in the network.

Examples for hierarchical routing protocols are Low-Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman et al., 2000), Power-Efficient Gathering in Sensor Information Systems (PEGASIS) (Lindsey and Raghavendra, 2002), Threshold-sensitive Energy-Efficient sensor Network protocol (TEEN) (Manjeshwar and Agrawal, 2001) and the Data Aggregation-Exact and Approximate Algorithms (Al-Karaki et al., 2004). The ZigBee device classes (Coordinator, Router and End Device) organized in a tree topology can also be classified as a hierarchical routing approach (see Section 2.3.1 for details).

Multi-path Routing Protocols

Multi-path routing protocols utilize multiple paths from a source to the destination to effectively route around failed nodes or invalid links. Thus, dropped out nodes or heavily interfered links do not require retransmissions. This kind of routing provides the most robust solutions to overcome external interference of all presented routing approaches. Most other routing strategies need to send broadcast messages to find an alternative route. This produces additional traffic and the

original message is delayed. On the other hand, multi-path routing wastes power due to the redundant transmissions. Routing protocols working with multiple paths are e.g. Meshed Multipath Routing (M-MPR) (De et al., 2003), Highly Resilient, Energy-Efficient Multipath Routing in WSNs (Ganesan et al., 2001) and Reliable Information Forwarding using Multiple paths (ReIn-ForM) (Deb et al., 2003).

Data-centric Routing Protocols

Data-centric routing is also known as attribute-based routing (e.g. by Kumar et al. (2008)). The sender is not identified, since its identity is not relevant for routing decisions. The content of the message determines the route and often these protocols work with so-called “Agents”, “Queries” or “Interests” to subscribe to certain events and thereby to route them. The event type can e.g. be represented by a message type field in the header.

Data-centric routing has been used e.g. in the form of: Directed Diffusion (Intanagonwiwat et al., 2000), Sensor Protocols For Information Via Negotiation (SPIN) (Heinzelman et al., 1999), Energy-Aware Data-centric Routing (EAD) (Boukerche et al., 2003), Constrained Shortest-Path Energy-Aware Routing (Youssef et al., 2002) and Rumor (Braginsky and Estrin, 2002).

Geographic Routing Protocols

Geographic routing protocols are also called location-based routing (e.g. in the overview given by Akkaya and Younis (2005)). The sensor nodes know about their positions, which is not only important for the use of the sensed data, but can also improve routing decisions. In order to gain knowledge of their positions, nodes can be preconfigured, they can have Global Positioning System (GPS) units, they can learn their positions with the help of a localization algorithm or they know about their positions from another source of information. There are multiple approaches to localize nodes, all of which generally use three steps. Figure 6.2 gives a short overview of the three steps: the distance estimation, the position computation and the final localization algorithm. Some typical localization algorithms are discussed below.

In the Ad Hoc Positioning System (Niculescu and Nath, 2001), some landmark nodes know their positions and hence they compute the average hop distance. Then trilateration¹ is used to get the position of non-landmark nodes, which are a single hop away. These neighbor nodes become landmark nodes themselves after knowing their positions. This algorithm is repeated until all nodes know their positions.

Recursive Position Estimation (Albowicz et al., 2001) is based on the same idea as the Ad Hoc Position System, but the nodes need only two landmark nodes as references, since the direction of spreading eliminates one of the two possible intersections of range circles of the reference nodes.

Another approach is to use mobile beacon nodes that know their current positions, e.g. they are equipped with a GPS module (Sichitiu and Ramadurai, 2004). Hardware extensions and the possibility to send and receive ultrasonic signals as in the Cricket Location Support System (Priyantha et al., 2000) allow precise distance estimations based on the arrival time difference of an ultrasound and a radio signal.

Regardless of the way of determining the positions, it is assumed that nodes know their precise positions for geographic routing. However, the type of position information can also vary between physical (absolute positions) and virtual coordinates (distances or hops).

Typical examples of geographic routing protocols are Geographic Routing with No Location Information (Rao et al., 2003), Energy-Efficient Forwarding Strategies for Geographic Routing in

¹Trilateration is the process of determining the location of a point with the help of distances. In contrast to trilateration, triangulation is based on angles.

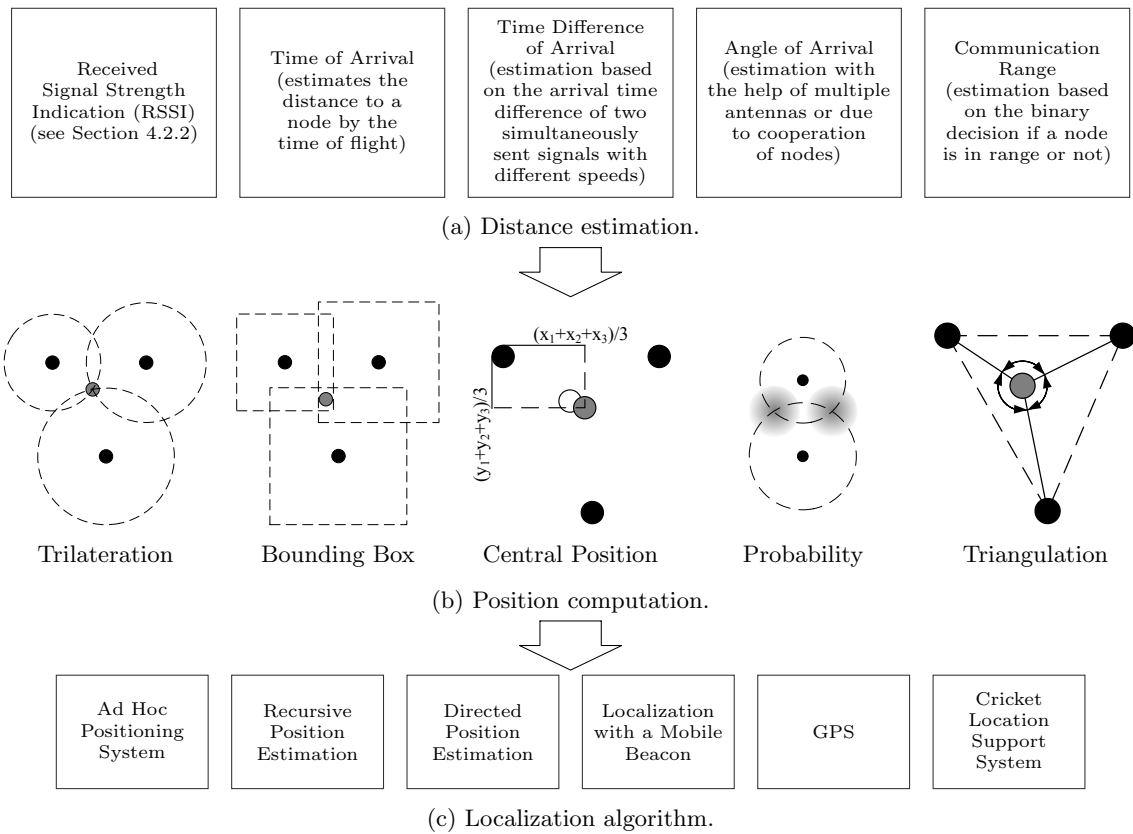


Figure 6.2: Overview of the steps and different methods of node localization according to Boukerche et al. (2009b). In the first step 6.2a, the distance or angles between two nodes are estimated. Then in step 6.2b, the position of the nodes is computed based on the estimated distances/angles. Finally in the main step 6.2c, the gained information is used to map all nodes of the WSN. The steps may differ depending on the network and the types of sensor nodes.

Lossy WSNs (Seada et al., 2004) and Geographic Routing with Limited Information in Sensor Networks (Subramanian and Shakkottai, 2005).

Quality of Service-based Routing Protocols

Quality of Service (QoS) describes the quality of communication from the perspective of the user, i.e. to which degree the user's needs are satisfied by the connection. For instance in end user applications, the QoS indicates if speech quality and delay is suitable for telephony or if a video is streamed without jitter. Thus, QoS is not a single feature of a network connection, but a combination of properties (including delay, jitter and throughput). For WSNs the required service quality can be a maximum delay time and minimum throughput to guarantee a certain degree of real-time behavior. To achieve QoS, different OSI Layers have to work together. However, especially the Medium Access Control (MAC) Layer plays an important role, since the MAC organizes the timing of the channel access.

Typical approaches for QoS-based routing protocols are SPEED (He et al., 2003), which supports soft real-time requirements, and its enhanced version Multi-path multi-SPEED protocol (MMSPEED) (Felemban et al., 2006).

Summary

After this short overview of routing approaches, it is obvious that routing itself is a challenging task, especially in WSNs where nodes tend to be unreliable and have to reserve energy. Thus,

achieving the maximum capacity of a single link should be preferred to passing the problem of unreliable links up to the Network Layer.

6.3 Data Link Layer

According to the OSI Reference Model, the Data Link Layer guarantees a reliable and correct transmission between nodes. As shown in Figure 6.1, the Data Link Layer can be divided into two sublayers. The Logical Link Control Sublayer provides error-free packet transmissions (by checking incoming packets (see Section 6.3.1) and preparing outgoing packets (see Section 6.3.2)), while the MAC Sublayer manages the channel access.

6.3.1 Backward Error Correction

Backward Error Correction (BEC) methods resend erroneous packets. These methods are also known as Automatic Repeat reQuest (ARQ) (Tanenbaum and Wetherall, 2011). The main challenge for and difference between BEC mechanisms is how to check which packet successfully reached the receiver. For instance in the Request To Send (RTS)/Clear To Send (CTS)-Handshake (illustrated in Figure 2.1c), the receiver uses an Acknowledgment (ACK) packet to confirm the reception of the packet. Although the handshake was presented as a possible solution to overcome the hidden node problem in Figure 2.1c, it additionally provides the information needed for BEC. To judge if the data arrived correctly at the receiver, the Frame Check Sequence (FCS) is used to quickly make a decision. If the FCS is valid, an ACK packet is sent back to the initial sender. This use of ACK is also provided in (IEEE, 2003b), and is commonly known as positive ACK, since it signals that the packet has been received.

In contrast, a receiver can explicitly request a packet that was missed. In this version, the detection of a missing packet can be realized with the help of a counter in a subsequent packet or by identifying a corruption with the help of the FCS. This approach is also referred to as negative ACK, since for each corrupted/missing packet a resend request is transmitted. Positive ACKs increase the overhead, since for each packet an additional ACK packet has to be sent. On the other hand, negative ACKs require additional buffers to store already sent packets. If the original packet was lost, the request for a retransmission can also fail to be received.

Although BEC is required for reliable data transmission, the author argues that the avoidance of losing packets in the first place is more efficient, especially to mitigate high Packet Error Rates (PERs). It is more suitable to use BEC on top of other interference mitigation strategies, but on its own it cannot be used to overcome heavy interference. If only a small amount of packets is randomly interfered and thereby lost (e.g. due to Bluetooth interference), BEC with its retransmissions can be sufficient. External interference frequently occurs in bursts, which is another challenge for retransmissions. While interference is based on a random distribution of noise in most models, this classical assumption is not suitable with regard to retransmissions. The irregular interference can still be present when the MAC retransmit. This timing problem is further discussed in Section 6.3.3.

Another drawback of retransmissions is the increased channel utilization due to the additional packets. Depending on the Radio Duty Cycling (RDC), the energy consumption can be higher, since the radio has to stay online for an additional time duration. Detailed timings of the RDCs of WSN MACs are beyond the scope of this work, though a short introduction was given in Section 2.3.2.

6.3.2 Packet Fragmentation

An often mentioned feature of IEEE 802.15.4 is the low duty cycle of the communication (IEEE, 2003b; ISA 100 Wireless Compliance Institute, last accessed April 2014). In this context, the duty cycle does not refer to the radio duty cycle (i.e. the on- and off-times of the radio), but to the channel utilization. Most of the initial use cases that were thought of during the design of the original IEEE 802.15.4 Standard (IEEE, 2003b) require only a small amount of data to be transferred. Therefore, the packet length was strictly limited. This small amount means only a few short packets are transferred and this results in low channel utilization and hence a small chance of collisions.

However, if more data has to be transmitted, either required by the application or due to scaling of a multi-hop network, it is a commonly suggested solution to increase the Packet Reception Rate (PRR) by using short packets. As the amount of data to be transmitted stays the same, multiple short packets have to be sent. This method is also referred to as adaptive packet length (Farahani, 2008). In their standard work for computer networks, Tanenbaum and Wetherall (2011) mention short packets or frame segments, called fragments, as supported by IEEE 802.11. Split packets are referred to as fragments in the following.

The basic idea behind packet fragmentation can be shown with the help of the relation of PRR and Bit Error Rate (BER). Equation 4.14 indicates that the probability of a successful reception of a packet, the PRR, increases with shorter packets (smaller number of bits n). However, in order to receive the same amount of data, more packets p have to be transmitted and the probability that multiple packets are successfully received is:

$$\text{PRR}_{\text{Fragment 1}} \times \text{PRR}_{\text{Fragment 2}} \times \dots \times \text{PRR}_{\text{Fragment } p} = \text{PRR}^p = (1 - \text{BER})^{n \times p} \quad (6.1)$$

where all packets have the same size and therefore the same number n of bits to transmit. Since the total amount of data ($n \times p$) stays constant, there is neither a theoretical gain nor loss in the PRR of the whole process.

However, this is just a mathematical relationship assuming that there is no packet overhead, no implementation overhead, no retransmissions and ideal random noise interference. In the following, the advantages and disadvantages of packet fragmentation are discussed in the context of real WSNs under external interference.

Packet Overhead

Firstly, packets in real systems have overhead and for an IEEE 802.15.4-conform packet, at least 15 bytes of overhead (compare to Figure 2.13) are added per packet for different fields:

- 4 bytes Preamble Sequence + 1 byte Start of Frame Delimiter + 1 byte Frame Length = 6 bytes in the PHY Layer;
- 2 bytes Frame Control + 1 byte Sequence Number + at least 4 bytes Addressing + 2 bytes FCS = 9 bytes by the Framer in the MAC Sublayer.

Taking this into account, the relation given in Equation 6.1 based on Equation 4.14 is not valid anymore and p has to be replaced. The data payload, the maximum size of a Medium Access Control Service Data Unit (MSDU) is limited to 118 bytes. Thus, the number of required packets to transmit d bytes of data payload is:

$$p = \left\lceil \frac{d}{118} \right\rceil \quad (6.2)$$

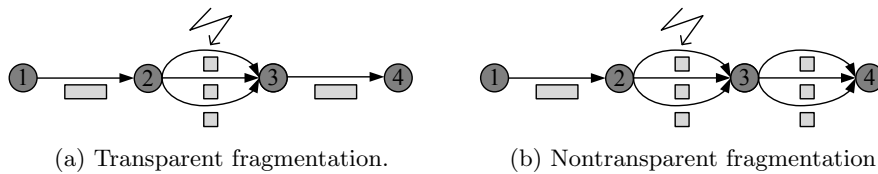


Figure 6.3: Transparent and nontransparent fragmentation. In this example, only the link between Node 2 and 3 is interfered.

If d is a multiple of 118 bytes, the splitting into packets works out even. Then the PRR of the packets that were successfully sent at the first attempt is:

$$\text{PRR} = (1 - \text{BER})^{((118+15) \times 8 \times p)} \quad (6.3)$$

For shorter segments, the MSDU size has to be decreased from 118 bytes and more packets including more overhead have to be sent, which consequently results in a lower probability of successfully receiving all packets at the first attempt.

Fragmentation Implementation

Another factor is the implementation of the fragmentation in the communication stack, although this can be considered as part of the packet overhead. In (Tanenbaum and Wetherall, 2011), different reasons for packet fragmentation are mentioned from an Internet perspective at the Network Layer, including:

1. Hardware,
2. Operating system,
3. Protocols,
4. Compliance with several international and national standards,
5. Desire to reduce error-induced retransmissions to a certain level, and
6. Desire to prevent one packet from occupying the channel too long.

In combination, these reasons limit the Maximum Transmission Unit (MTU) of a network path. Although the factors are simple in WSNs due to the assumption of a homogenous environment, the implications for the implementation are transferable. According to Tanenbaum and Wetherall (2011), fragmentation can be either implemented transparently or nontransparently. Both possibilities to implement packet fragmentation are summarized in Figure 6.3.

Transparent fragmentation (Figure 6.3a) breaks a packet into fragments at the sender and reassembles them at the next receiver of a multi-hop path. Thus, the fragmentation and reassembling takes place at each node if required for the following link. For a large WSN, this means that the packet could be reassembled multiple times in a communication path from a sender to a final receiver over multiple hops. As shown exemplarily in Figure 6.3a, the first link is uninterfered and therefore a long packet is transmitted from the first sender to hop 1. The link between hop 1 and hop 2 is interfered and to improve the chances of a successful transmission, the packet is fragmented and sent piecewise to hop 3, where the packet is reassembled from the fragments. The full packet is then forwarded in one piece from hop 3 to the final receiver over an uninterfered link.

In the nontransparent approach (Figure 6.3b), the fragments are not reassembled until the final receiver is reached at the end of a multi-hop route. Thus after the first fragmentation, the fragments are forwarded independently of each other.

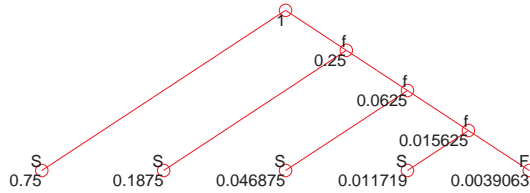


Figure 6.4: Probability tree for a maximum of four retransmissions, with a PRR of 75%. The nodes are labeled with f for failure or with s for success, where capital letters indicate an end state. The probability of no successful delivery at all is $P(PE) \approx 0.391\% = \text{PER}^{\text{retransmissions}}$. Therefore, the total probability of receiving the packet is $P(PR) \approx 99.609\% = 1 - P(PE)$.

To reassemble the fragments, additional information has to be placed inside the header. This can be done in the form of a fragment number for sorting the incoming fragments or in the form of an absolute offset of the data and a flag if the fragment is the last fragment of a packet as done in the Internet Protocol (IP) (Information Sciences Institute, 1981). Additionally, the reassembling of packets adds additional workload, which is especially the case for the nontransparent fragmentation buffers which are needed to reorder out of sync fragments.

Packet Retransmission

The third factor connected with fragmentation is packet retransmission. If a packet is received erroneously, e.g. when the FCS reveals corrupted bits or the packet is not received at all, it has to be resent. BEC methods to detect and to retransmit lost packets were described in Section 6.3.1. By taking retransmissions into consideration, the estimation equation of a successful packet delivery becomes more complex, since for each retransmission a probability tree similar to the one shown in Figure 6.4 has to be built for each retransmission.

However, these probability trees assume a steady PRR and thus they are not realistic for external interference as argued in the next section.

Interference beyond Random Noise

As already discussed in Section 4.2.3, external interference is commonly modeled as random noise. Schmidt et al. (2013) show that even background noise (a low SNR) has some error patterns and that erroneous bits are not independently distributed. Even more, random noise does not fully reflect the real characteristics of external interference and thus the mathematical equations in the previous two sections are only partly representing real world interference scenarios. Azimi-Sadjadi et al. (2006) show the impact of external interferers on the channel. The exact differences depend on the source of interference. Nevertheless, a common approach is to consider external interference as noise that is turned on and off. Therefore, the time overlap between interference period/interfering packet and the desired victim packet plays an important role. Using the symbols and interrelationships introduced in Section 4.2.6, the implications of a more realistic modeling of the interference source are discussed.

If the interferer is strong enough to cause interference (see Signal to Interference Ratio (SIR) in Section 4.2.3 and the explanation of the connectivity regions in Section 4.2.7), the packet can be assumed to be corrupted as soon as the interferer is active.

Therefore, the packet has to fit in the idle period of the interferer for an error-free packet transmission, i.e. the packet airtime has to be shorter than the interference-free gap between the end of the interference and its next start. This can be expressed with the notation used in this work as $T_A < T_{BI} - T_B$, where T_A is the airtime of the victim packet and T_B , T_{BI} are the airtime and the sending interval of the interferer, respectively (compare to Figure 4.7). Thus, in some scenarios larger packets might always fail and only smaller packets can be used. As the packet

lengths and channel access times are summarized in Section 6.3.3, it will become obvious that the variance of the airtime enabled by packet fragmentation is not significantly changing the ratio of the airtimes of the different technologies.

However, if the more realistic non-permanent interference is assumed, the probability of a successful retransmission changes depending on the backoff duration, which is used in the CSMA/CA algorithm (see Section 6.3.3 for discussion). Therefore, the simple probability tree presented in the previous section is not a reliable model.

Efficiency Related to Technologies

As stated in the previous section, external interference is more complex than random noise and therefore, the efficiency of fragmentation against different sources of interference is reviewed in the following.

There is not enough time in between two IEEE 802.11 packets (interframe spacings of 10 to 50 μs as given in Table 2.25) to send an IEEE 802.15.4 packet (at least 352 μs is required as explained in Section 2.3.2). Furthermore, it will be shown in Section 6.3.3 that IEEE 802.11-based Wireless Local Area Networks (WLANs) are too fast for IEEE 802.15.4 to react and thereby, a targeted use of interframe spacings is not possible. However, Huang et al. (2010) use so-called WiFi White Spaces, i.e. the time when there is no traffic on the channel, to submit IEEE 802.15.4 packets. Since these idle periods can still be shorter than the airtime of a long IEEE 802.15.4 packet, Huang et al. (2010) use packet fragmentation. Their fragment lengths are based on packet traffic patterns, but not on the timing of packets defined by the basic standards.

On the packet level, packet segmentation provides only limited benefit for the coexistence performance in terms of decreasing the collision probability. Depending on the scenario, different positions of the corrupted bits within an IEEE 802.15.4 packet are reported in literature due to the interference by IEEE 802.11. In the symmetric region (see Section 4.1 for details about the symmetric region), most bits corrupted by IEEE 802.11 are at the beginning of a packet (Liang et al., 2010). Hence, a shorter packet would not significantly increase the PRR. In the asymmetric region, the spreading of the corrupted bits is more equal through the victim packet with multiple bursts, as also reported by Hermans et al. (2012); Nicolas and Marot (2012); Liang et al. (2010). Therefore, shorter packets could only increase the PRR of a single packet in the asymmetric region. However, the previously mentioned disadvantages remain for transmitting multiple fragments. Additionally, the effect of interference decreases with the interfering IEEE 802.11 device being further away (in the asymmetric region). The packet lengths and/or the IEEE 802.11 modulations as well as the CCA modes might have differed between the experiments reported in literature (Liang et al., 2010; Hermans et al., 2012; Nicolas and Marot, 2012) and thereby varying results are reported.

Bluetooth is a relatively weak and channel hopping interferer. However, the collision probability increases with each channel change, since there is a growth of the probability of hopping to a frequency that overlaps with the used IEEE 802.15.4 channel. Although shorter victim packets decrease the collision probability slightly, the effect of interference by Bluetooth is limited. Since the size of IEEE 802.15.4 packets is already short, the advantage of even smaller fragments does not pay off due to the overhead. Even with a not IEEE 802.15.4-compliant MAC header, the overhead of 5 bytes on the PHY Layer has to be added. A more realistic overhead (including the receiver address, information about the fragment etc.) can be assumed to be 15 to 18 bytes, e.g. when implemented in ContikiOS. Since the average probability of a collision with Bluetooth is quite small, it is assumed that approximately three quarters of the packets are uninterfered (see Equation 4.19). Furthermore, PRRs under interference of $\geq 90\%$ are reported in literature (see Section 4.3.3) and therefore, an occasional retransmission of a full sized packet is sufficient.

Nevertheless, Nicolas and Marot (2012) suggest shorter packets to mitigate Bluetooth interference, but results showing an improvement are not provided.

Microwave ovens with their well-defined cycle times and the relatively long and stable idle periods of roughly 10 ms leave enough time for the longest possible IEEE 802.15.4 packet transmission (4,256 μ s), including ACK and collision avoidance, as shown in Section 6.3.3.

Summary

In summary, the common assumption that packet fragmentation mitigates the effects of external interference has to be negated. In general, it is not beneficial for the already small IEEE 802.15.4 packets with only a Medium Access Control Protocol Data Unit (MPDU) payload of up to 127 bytes, since the additional overhead exceeds the benefit of shorter packets.

Golmie (2006) reviews packet fragmentation to improve Bluetooth resistance against IEEE 802.11 under the headline “Myths and common pitfalls” and concludes that fragmentation leads to more collisions. Although Bluetooth accesses random channels, her results support the just presented analysis.

6.3.3 Clear Channel Assessment and CSMA/CA

Many MACs are based on the CSMA/CA algorithm, whose basics have been introduced in Section 2.1.1. Initially, CSMA/CA was developed to solve the problem of internal interference and to provide a fair coordination in the network. In the following, the appropriateness of CSMA/CA to mitigate external interference is discussed.

The CCA request is a main part of the CSMA/CA algorithm and thus the CCA is recapped to evaluate the effectiveness of the CSMA/CA approach used by IEEE 802.15.4 to mitigate external interference. The CCA modes were already introduced in Section 2.3.3 and especially the ED-based CCA mode has found wide use in this work. The possibility of an ED-based CCA to detect external interference was reviewed by giving the airtimes of different technologies (see Chapter 2). These airtimes were compared to the sampling rates. Furthermore, RSSI measurements were used to monitor the spectrum (see Section 3.1.1).

It was proven that CCA using an ED-based mode is able to detect the traffic of external sources of interference, although some short packets are too fast to be reliably recognized. Furthermore, the ED-based CCA has been practically used in the interference classification algorithm (see Chapter 5).

Clear Channel Assessment

It has been shown that CCA using mode 1 and 3 detect external interference and therefore IEEE 802.15.4 backs off, while mode 2 does not trigger a backoff and the channel is accessed without checking for external interference.

The author conducted an experiment comparing different CCA modes to confirm the effect of sender-side interference. The definition of sender-side interference has been given in Section 4.1. The setup consisted of two nodes having a distance of 1 m between them and being 2.5 m away from the interfering network. Each experiment was based on 10,000 packets, which have been sent from Node 1 to Node 2 with an interval of 100 ms in-between. The MPDU of the IEEE 802.15.4 packets had a size of 32 bytes. To clearly see the effect of the CCA mode, the channel was checked with the help of a CCA request before sending (ED threshold was set to the default -77 dBm). The following interference scenarios were used. For IEEE 802.11, the Access Point 1 sent to the Laptop using IEEE 802.11b and g. For both versions, Distributed Internet Traffic Generator (D-ITG) transferred 250 Transmission Control Protocol (TCP) packets per second,

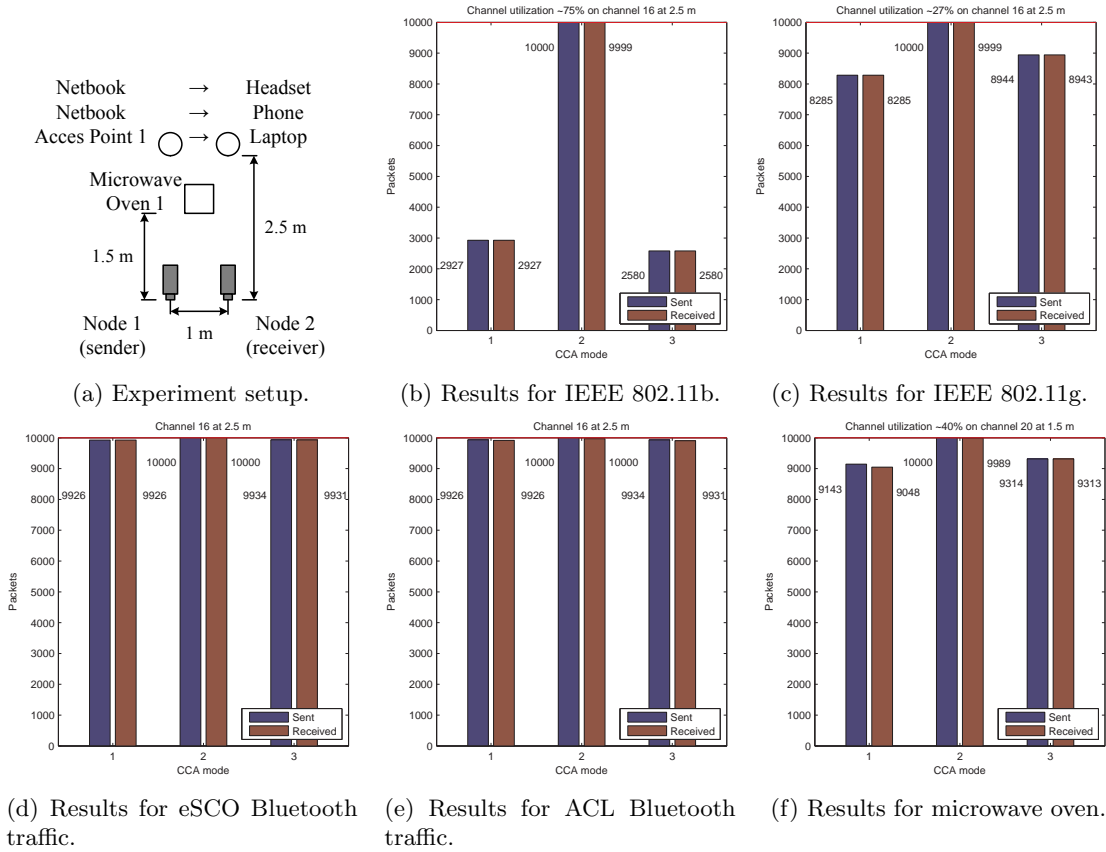


Figure 6.5: Experiment setup and PRRs of different CCA modes.

each 1,500 bytes in size. Additionally, the Access Point (AP) announced its network with 201 bytes long beacon frames at a data rate of 1 Mb/s at the standard 100 tu beacon interval. The resulting channel utilization on IEEE 802.15.4 channel 16, fully overlapped by the used IEEE 802.11 channel 5, was around 75% for IEEE 802.11b and roughly 27% for IEEE 802.11g measured with the help of the Wi-Spy 2.4x device. The Bluetooth tests were the Netbook sending to the Headset (extended Synchronous Connection-Oriented (eSCO)) or to the Phone (Asynchronous Connection-Less (ACL)). For Microwave Oven 1, a shorter distance of 1.5 m between the victim network and the interfering oven was chosen due to weaker interference strength. The results for the microwave oven were gathered on channel 20. Further, each experiment was split into four runs of 2,500 packets, since the heated 500 ml water had to be replaced with fresh lukewarm water. The setups are illustrated in Figure 6.5a and the results of the different CCA modes are shown in Figures 6.5b to 6.5f.

The analysis of the experiments shows the expected results: due to the full sending power of 0 dBm as well as the close distance between victim sender and interferer, communication is possible even under the influence of interference. Therefore only sender-side interference in the form of false positive CCA backoffs is observed. CCA Mode 2 does always send (since it only backs off for IEEE 802.15.4-conform modulated signals). Almost all packets are received due to the good SIR, which lies in the connected region (see Section 4.2.7). As expected, the number of backoffs in CCA Mode 1 and 3 are roughly identical. The number of sent packets is also almost identical to the number of received packets and thus proves that pure sender-side interference occurred due to the not ideally set CCA ED threshold.

Bertocco et al. (2008) report similar results. They measured the PER of Tmote Sky sensor nodes using different CCA modes under different sources of interference. They argue that the amount of false positive backoffs for IEEE 802.11 disturbs the communication significantly greater

than the actual collisions. In their experiments, the PER affected by a 1 m away WLAN decreased from 75% down to 0.5% by changing the CCA mode from 1 to 2. For Bluetooth there were only small differences, but even for internal interference caused by another sensor node, a turned off CCA delivered the best PRR. Their victim network nodes were only 1 m away from each other and thus, they do not represent a typical scenario, since the interference is not strong enough to jam the desired signal, as it was the case in the previous experiment. Bertocco et al. (2008) report an IEEE 802.11 interfering signal of around -50 dBm at the victim receiver. Therefore, a SIR in the connected region can be assumed.

Many experiments are conducted in the connected region due to the lack of physical space in fully controlled environments. Although weaker sending powers in the victim nodes can simulate distance, it is hard to only interfere with the receiver, since the sending power of interfering devices can normally not be adjusted precise enough.

Bertocco et al. (2008) do not mention all details about the experiment (e.g. neither packet lengths on the victim network nor the exact Bluetooth traffic), did not perform their experiments in a Radio Frequency (RF) anechoic chamber, had no microwave oven included, and used a polling protocol on the victim side. Therefore, their results differ slightly from the results of the presented experiments, but they show the same trend. These experiments give the impression that ED-based CCA modes only generate false positive backoffs. However, if the distance between the nodes in the victim network increases, a simple change of the CCA mode does not solve the problem of interference anymore. This is the case because the SIR at the receiver drops. Furthermore, the interferer can be next to the receiver and is thus too far from the victim sender to be realized. Yuan et al. (2010a) suggest an adaptive CCA mechanism for IEEE 802.15.4 as a trade-off between internal interference and false positive backoffs caused by external interference. Therefore, the previous section highlighted the importance of the CCA mode and the CCA threshold.

CSMA/CA

As the previous experiment of sender-side interference indicates, CCA is not always an appropriate tool since it can be over- or insensitive. Furthermore, the reaction and backoff timing of the CSMA/CA algorithm has to be compared to the timings of the interfering technologies to reach a conclusion. Therefore, the following discusses the CSMA/CA algorithm of IEEE 802.15.4 to avoid external interference if the interference is correctly realized by the CCA and the victim packets are so weak at the receiver that they are corrupted by external interference. The algorithm for unslotted CSMA/CA has previously been introduced in Section 2.3.2 as a medium access algorithm for uninterfered environments.

In Figure 6.6, the timings of the different discussed technologies are illustrated using the same scale for comparison. The figure makes it obvious that the CSMA/CA fails to avoid external interference. It illustrates the fastest data rate possible in IEEE 802.11b with long preambles. However, the Distributed (coordination function) InterFrame Space (DIFS) before the RTS and the Short InterFrame Spaces (SIFs) between the packets are so short that they are hard to notice. If IEEE 802.11g is used, these spacings are decreased to 10 μ s. Therefore, higher data rates of IEEE 802.11 are too fast to be reliably noticed and addressed by IEEE 802.15.4 with a Receive (RX)-to-Transmission (TX) time of 192 μ s, since the channel status observed by the CCA can change too fast. However, even if the interference is noticed and no backoff is used, the TX-to-RX time is too long to react appropriately.

Bluetooth packets sent on different frequencies due to Adaptive Frequency Hopping (AFH) cannot be foreseen by CCA and thus, there is no effective protection possible against Bluetooth hopping to a frequency used by IEEE 802.15.4.

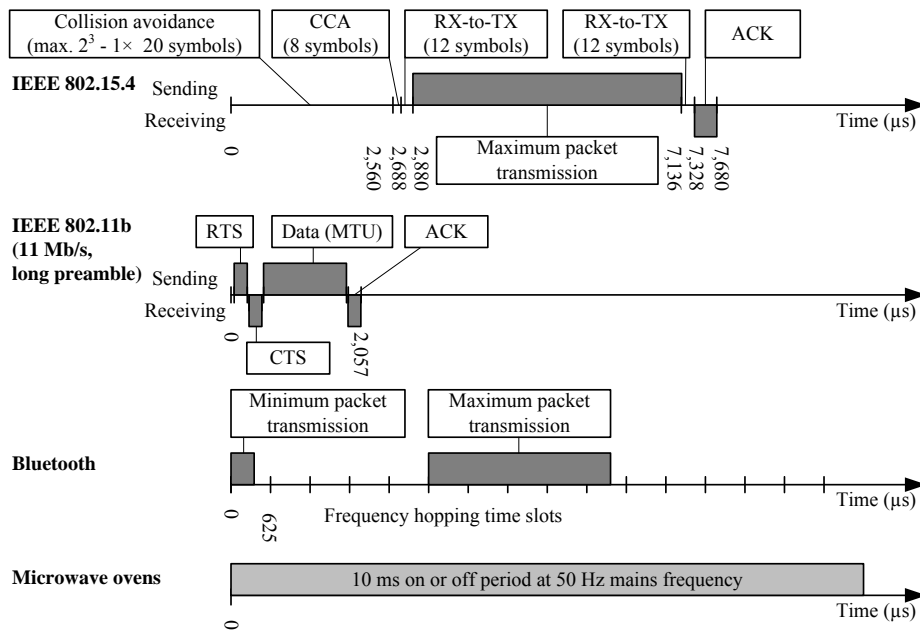


Figure 6.6: Channel access timing and channel use duration comparison of different technologies. IEEE 802.15.4 has the lowest data rate and therefore the slowest access. For IEEE 802.11 a slow, dated configuration is shown and even there the DIFS and SIFSs are hard to see because of their short duration. For Bluetooth the shortest and longest data transmissions are shown. For more background details of the different technologies see Chapter 2.

Microwave ovens (with their steady on and off durations of 10 ms each) can be reliably detected and IEEE 802.15.4 reacts fast enough to use the free periods. However, the backoff interval and the CA at the beginning of each attempt of transmission are inefficient for the coexistence with microwave ovens. In Section 7.7, it will be shown that a packet scheduling approach independent of the CCA mode can be used to mitigate the effects of microwave oven interference.

Summary

In summary, it can be assumed that CSMA/CA, as suggested in (IEEE, 2003a), is not particularly useful to prevent external interference. The long time duration between the CCA request and the transmission start makes even a correct CCA useless against most external interferers since they operate with considerably faster speeds than IEEE 802.15.4. Therefore, more adequate methods should be used to mitigate external interference, while the CCA mode can usually be changed to mode 2 to efficiently prevent internal interference.

Besides the timing of the CCA operation in IEEE 802.15.4, the CSMA backoff timing also plays an important role for the chance of a successful retry. Srinivasan et al. (2008) suggest the β -factor to describe the “burstiness” of a channel. To overcome this latter, they suggest to send packets as quick as possible until a transmission fails. After a fail, the transmission backs off for a long time (e.g. half a second) and then it retries. By this, the retransmission gets a reception probability independent of the first collision. Depending on the duty cycle, a WSN might not use the CSMA/CA times stated in (IEEE, 2003b), but a timing synchronized with the RDC. In the following section, the specific timing of the transmission is discussed as a mitigation strategy.

6.3.4 Packet Scheduling

A mitigation strategy that can overlap with the energy conserving RDC is the scheduling of packets, since they are sent at specific times or in specific intervals. If packet scheduling is used

to avoid interference, the transmission of the packet is delayed until the channel is free or at least assumed to be free of interference. The increased delay between the initial request to send and the actual transmission is normally in the range of milliseconds and therefore, it is acceptable for most applications of WSNs, especially because it can be assumed that the channel would be blocked by the interferer anyway. Thus, this method rarely introduces additional delay, but avoids unsuccessful transmission attempts. Depending on the RDC, the duty cycle of the radio can be adapted and thereby no energy is wasted. The resulting delay is a necessary drawback of low power duty cycle MACs for WSNs.

Packet scheduling can also be seen as a modified CSMA/CA algorithm. An example of packet scheduling is the Network Allocation Vector (NAV) used by IEEE 802.11 for the virtual carrier sensing (see Section 2.4.1).

Chowdhury and Akyildiz (2009) use a combination of packet scheduling and a maximum power impulse at the beginning of a packet to suppress IEEE 802.11b before sending an IEEE 802.15.4 packet. Their approach is based on the assumption that the IEEE 802.11 network uses an ED-based CCA mode and is able to detect IEEE 802.15.4 (see Table 4.2 for the different cases of mutual awareness). Huang et al. (2010) present an approach that uses the traffic distribution on a macro level. They identify whitespaces between packet clusters and predict the next whitespace to transmit data within it. As already mentioned in Section 6.3.2, they also adjust the packet length to fit in the idle spaces.

Interference caused by Bluetooth cannot be addressed by packet scheduling due to Bluetooth's random, not predictable frequency hopping. Additionally, the slot durations are short (625 μ s) and therefore hard to synchronize with the help of typical sensor node hardware.

By contrast, microwave ovens have a simple, slow and steady channel use pattern that is well utilizable by packet scheduling, as shown in (Rensfelt et al., 2012; Chowdhury and Akyildiz, 2009). In this work, packet scheduling is also used to overcome interference caused by microwave ovens (see Section 7.7 for further details). It is further evaluated in Section 7.7.1 as a mitigation strategy in the Interference-Aware, Self-Adapting (IASA) MAC.

6.4 Physical Layer

The PHY Layer is crucial for the packet transmission, since it defines the form of the packet's electromagnetic wave and the power used to transmit it. The more reliable the actual transmission is, the less the problem of interference occurs. However, the PHY Layer offers only limited methods to optimize the transmission, which is due to its hardware base.

6.4.1 Forward Error Correction

Instead of resending missed packets as done by BEC approaches, Forward Error Correction (FEC) approaches add redundancy to the packets to make them more robust against corruption. Liang et al. (2010) argue that IEEE 802.15.4 packets are corrupted within the first few bits by interfering IEEE 802.11 packets in the symmetric region (see Section 4.1 for the latter). They implemented multiple headers, which can be seen as a primitive form of FEC, to overcome the problem of corrupted bits at the beginning of a packet. The Synchronization Header (SHR), Physical Header (PHR) and Medium Access Control Header (MHR) are sent twice, resulting in a redundancy of 16 bytes. In the asymmetric region, the errors are more uniformly spread and therefore, they apply more complex error correction schemes: Hamming Code and Reed-Solomon Code.

Besides the improved PRR, the durations for performing the encoding and decoding are only acceptable in particular applications. The Reed-Solomon Code on the used TelosB sensor needs 36 ms for the encoding and over 104 ms to check a received packet to be error-free. The computation

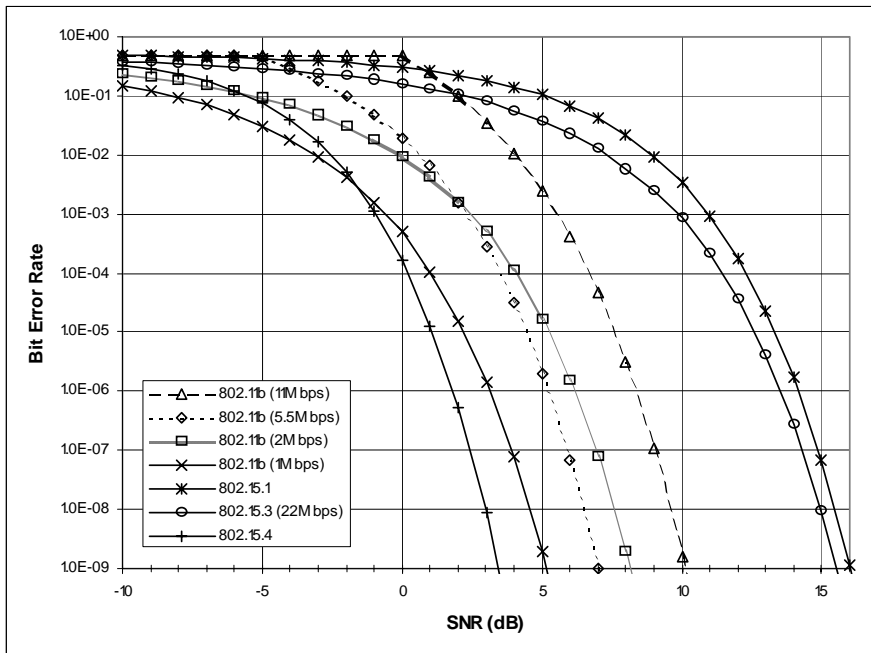


Figure 6.7. BER results for IEEE Std 802.11b, IEEE Std 802.15.1, IEEE Std 802.15.2, IEEE Std 802.15.3, and IEEE Std 802.15.4. It can be seen that IEEE 802.15.4 has a lower BER than other communication technologies in a low SNR. Taken from (IEEE 802.15 Working Group, 2010).

The simulation output, illustrated in Figure 6, Figure 7, Figure 8, Figure 9, Figure 10 and Figure 11, shows time increase in the packet size. Here, the Link Layer Allocation of devices with such a long delay. Renfell et al. (2012), tried to include FEC into their Sensor Network Interference Classification (SNIC) protocol as a mitigation strategy. Therefore, to performable issues, they use channel occupancy and perform dynamic channel selection is an important mechanism, for 802.15.4-based WSNs, the sense of FEC is questionable, since the overhead and complexity do not pay off. A second observation is that transmit power level is the dominant factor in co-channel interference situations. When a low-power IEEE 802.15.4 device is moved toward an IEEE 802.11b or IEEE 802.15.3 device, the IEEE 802.15.4 device is the first to degrade. IEEE Std 802.15.1-2005 and this standard have similar power levels and their interference effects on each other are similar.

6.4.2 Signal Spreading/Modulation

As already discussed in Chapter 4, the Offset Quadrature Phase Shift Keying (O-QPSK) used by IEEE 802.15.4 in the 2.4 GHz frequency band (see Section 2.3.3 for details) offers a basic level of robustness against interference due to its Processing Gain (PG). Since the modulation and demodulation are built into hardware, there are no parameters to optimize. The O-QPSK used by IEEE 802.15.4 is a robust modulation, as the required SIRs discussed in Section 4.4 prove. The comparison with modulations of other wireless IEEE standards, shown in Figure 6.7, also supports the statement that the IEEE standard 802.15.4 was designed with robust communication having priority over data rate.

6.4.3 Rate Scaling/Modulation Control

If the modulation can be changed as in IEEE 802.11-compliant devices, this is also known as rate scaling (which has been discussed in Section 2.4.3 for IEEE 802.11) or modulation control (Golmie, 2006). Besides the lack of support in the IEEE 802.15.4 standard, a modulation change to a more robust modulation normally reduces the throughput and thereby increases the channel utilization. Golmie (2006) argues that the channel utilization increases for IEEE 802.11 at a downscaled rate and that an increased cycle channel utilization results in a higher probability of collisions with the external source of interference in the time domain. Therefore, a modulation change is more suitable for packet loss, which results from a weak signal caused by a long distance between sender and receiver.

6.4.4 Power Control

Power control is the increase or decrease of the transmit power of the transmitter and thereby it changes the transmission range or rather the link quality (which is indicated by the SNR or SIR). Power control (Golmie, 2006) is also referred to as Dynamic RF Output Power Selection (Farahani, 2008), and the basic idea is already introduced in IEEE (2003b) with the low transmit power itself and the possibility of different transmit power levels. Strictly speaking, power control does not mitigate the effect of external interference on the victim side, but it can overpower it. An increased transmit power boosts the received signal at the victim receiver and therefore improves the SIR. However, since IEEE 802.15.4 is a low power solution and power is a key resource in most WSNs, it is often not an option to increase the transmit power. Furthermore, most hardware used for wireless sensor nodes today does only allow transmitting with up to 0 dBm. On the interferer side, power control, i.e. decreasing the transmit power, limits the interference range to an unavoidable minimum.

6.4.5 Channel Alignment, Hopping and Agility

Based on the modulation, a channel width can be defined for wireless transmissions and the available spectrum is divided into channels. Farahani (2008) considers the adjacent channel performance as another mechanism for coexistence. Here, the adjacent channel rejection is not being reviewed as an independent factor, since it is a feature of the radio chip. Nevertheless, the performance of the adjacent channel rejection in combination with other properties of the radio transmitter influences the possibilities of the channel selection and advanced channel changing strategies (see Section 2.2 for details). It is obvious that the choice of the channel is vital and therefore multiple approaches exist. In general, there are three main approaches how to choose and when to change the channel. They are introduced in the following three sections.

Channel Alignment

Channel alignment (also referred to as Static Channel Assignment by Baccour et al. (2013)) is the decision for an uninterfered channel before the deployment or at a setup phase directly after the deployment. This fixed channel plan might work for small, spatially limited WSNs, e.g. by avoiding all IEEE 802.11-based WLANs (see Figure 1.2). For many WSNs, the deployment planning and channel alignment is limited to choosing channel 26. This naive strategy has already been discussed in Section 1.1.4. However, for WSNs operating over long time or large areas, a more dynamic spectrum allocation strategy has to be used.

Channel Hopping

Bluetooth uses AFH to avoid interference in its single-hop links. The details of the frequency hopping scheme and the channel selection are described in Section 2.5.2. However, frequency hopping systems are hard to implement for multi-hop WSNs, since all nodes have to be synchronized to be tuned in at the same time on the same channel. Baccour et al. (2013) refer to this frequency hopping as continuous hopping.

Channel Agility

Channel agility (also called Reactive Hopping by Baccour et al. (2013)) is widely used (Hermans et al., 2013; Nicolas and Marot, 2012; ZigBee Alliance, 2008b) in order to still benefit from the chance of avoiding interference in the spectrum. This agile channel access only changes the channel, when interference occurs, which can be noticed by multiple indicators. However, the channel change

still has to be communicated through the network, which causes overhead. If the degradation of the channel is anticipated, Baccour et al. (2013) refer to it as Predictive Hopping.

Channel alignment and agility is especially useful to avoid interference caused by IEEE 802.11 with its relatively permanent channels, as e.g. shown by Nicolas and Marot (2012). Channel agility is also the mitigation strategy chosen in this work to overcome IEEE 802.11 and is therefore further discussed in Section 7.5 with its practical challenges as the channel announcement. Since Bluetooth hops through the full 2.4 GHz spectrum, a channel change makes no sense to avoid Bluetooth interference. Furthermore, Bluetooth itself tries to avoid interference due to AFH. For microwave ovens, a channel change can be useful, since the interference decreases further away from the center frequency of the microwave oven (as shown in Figure 2.38). However, packet scheduling efficiently mitigates the effects of interference due to the dedicated timing pattern of microwave ovens.

6.5 Summary

The previous discussion of mitigation strategies shows that many different approaches exist and that they are often related and dependent on each other. In literature, further reviews and discussions of mitigation strategies can be found.

Baccour et al. (2013) review mitigation strategies to avoid external interference in IEEE 802.15.4-based WSNs and divide them into different dimensions: frequency diversity, space diversity, hardware diversity, time diversity and redundancy. Hardware solutions have not been considered in this work, since the underlying RF transceivers and thereby the hardware properties for commonly available sensor nodes are given. Changing the hardware can be considered to be both costly and complex and hence these solutions are beyond the scope of this work.

Farahani (2008) divides mitigation strategies into non-collaborative and collaborative mitigation strategies. Non-collaborative methods have no active knowledge of their wireless neighbors, are common and already used by default in IEEE 802.15.4. For collaborative methods, the interfering and victim network are, at least partly, managed by a central controller.

Due to the structure of this chapter and the overview given in Figure 6.1, a placement of the mitigation strategies in the OSI Reference Model Layers has already been provided. The technical background is also structured based on the OSI Layers in Chapter 2 and therefore, this grouping allows a comparison of the mitigation strategy and the relevant methods and properties of the communication stack. In Table 6.1, the presented strategies of this chapter are summarized. The table presents their classifications into OSI Layers, the diversity dimension (Baccour et al., 2013), the communication partner taking the burden of the strategy, the effectiveness and the drawbacks of each strategy.

In the next chapter, the knowledge of the different interference mitigation strategies is combined with the ability to classify a source of interference, which has been demonstrated in Chapter 5. This results in the following design of the IASA MAC protocol.

Mitigation strategy	OSI Layer	Dimension (Baccour et al., 2013)	Sender or receiver burden	Efficiency	Drawbacks
Mesh networking	Network Layer	Space	Sender	Against locally restricted interference	Large, dense WSN required
BEC	Logical Link Control	Time	Sender	Against any kind of interference	Overhead of dumb retransmissions
Packet fragmentation	Logical Link Control	Time	Both	Against random noise interference	Packet and implementation overhead, higher channel utilization
CCA and CSMA/CA	MAC	Time	Sender	Against internal interference	Oversensitive CCA causing false positive backoffs, delayed transmissions
Packet scheduling	MAC	Time	Sender	Against periodic interference patterns, e.g. microwave ovens	Not effective against random interference
FEC	PHY Layer	Redundancy	Receiver	Against random noise, very short bursts of interference	Computation overhead, longer packets
Signal spreading/modulation	PHY Layer	Frequency	Both	Against random noise and narrowband interferers	Implementation in hardware, trade-off between data rate and robustness
Rate scaling/modulation control	PHY Layer	Frequency	Sender	Against random noise and narrowband interferers	Implementation in hardware, trade-off between data rate and robustness, higher channel utilization
Power control	PHY Layer	Space	Sender	Against any kind of interference	Power requirements and restrictions
Channel alignment, hopping and agility	PHY Layer	Frequency	Both	Against interference at a certain frequency	Channel synchronization between network participants

Table 6.1: Overview of common interference mitigation strategies.

Chapter 7

An Interference-Aware, Self-Adapting MAC Protocol

After reviewing and discussing the possible methods to mitigate the effects of interference, an Interference-Aware, Self-Adapting (IASA) Medium Access Control (MAC) protocol is presented in the following. It includes the interference classification algorithm developed and evaluated in Chapter 5. For the classified sources of interference (possible classes are: *CLEAR*, *BT1*, *BT2*, *WLAN*, *MWO*, *UNKNOWN* and *INTERNAL*), suitable mitigation strategies are implemented.

7.1 Related Work Reported in Literature

Recently, the idea of a communication protocol that adapts to the link quality or to the type of external interference has been suggested in literature, although a consistent system has not been established yet. IASA MAC is comparable to all protocols that react individually to different kinds of interference, i.e. the mitigation strategy is dynamically matched to the kind of interference. Therefore, the following mitigation strategies are not considered in this work: rate scaling/modulation control (see Section 6.4.3), Adaptive Frequency Hopping (AFH) (see Section 2.5.2) or further approaches (e.g. the Bluetooth Interference Aware Scheduling (BIAS) suggested by Golmie et al. (2003) or the improvements by Boano et al. (2010)) that just use a single mitigation strategy.

Nevertheless, protocols that react individually to different types of interference have been suggested in literature. Since interference classification is part of these approaches, they have already been reviewed from the perspective of interference classification in Section 5.1.

The approach of Chowdhury and Akyildiz (2009) identifies the source of interference, tries to find the best channel in a setup phase and smartly adapts the transmission to avoid later occurring interference. In the initial setup phase an idle channel is chosen. If no idle channel is available, a channel interfered with by a microwave oven is chosen and as the last option, it is fallen back to a channel overlapped by a Wireless Local Area Network (WLAN) interferer. After this setup, the so-called Interference-aware Transmission Adaptation (ITA) reacts to interference. ITA tries to force coexisting WLANs to back off by sending a full power preamble of the IEEE 802.15.4 node. This requires an Energy Detection (ED)-based Clear Channel Assessment (CCA) mode used by the WLAN as well as short distances between the devices (see Section 4.2.1 for a discussion of the interference regions between IEEE 802.11 and IEEE 802.15.4). To avoid microwave oven interference, packet scheduling being synchronized to the interference pattern of the oven is chosen. Unfortunately, the ITA was only evaluated by simulations.

Another combination of interference classification and mitigation is the Sensor Network Interference Classification (SoNIC) approach described by Rensfelt et al. (2012) and Hermans et al. (2013). Rensfelt et al. (2012) suggest that a drop in the Packet Reception Rate (PRR) is the trigger for the interference classification and the following mitigation. They describe three mitigation strategies: both channel change and Forward Error Correction (FEC) (as suggested by Liang et al. (2010)) are suggested to overcome WLAN interference, while packet scheduling counters microwave oven interference. However, only the packet scheduling was implemented and tested. The FEC approach was rejected after initial trials due to the high computational overhead (as already discussed in Section 6.4.1). Hermans et al. (2013) support two mitigation strategies, which the author of this work also implemented parallel to their contribution: channel change against IEEE 802.11 and packet scheduling against microwave ovens. The details of the channel change and the packet scheduling used by IASA MAC are discussed in Section 7.5 and 7.7, respectively.

Nicolas and Marot (2012) present the already discussed Fingerprint Identification Mechanism (FIM) and extend it with a prototypical link adaptation to mitigate IEEE 802.11 interference by changing the channel to a non-interfered channel.

7.2 IASA MAC Details

After the demarcation between IASA MAC and other approaches as well as a short review of comparable approaches reported in literature, this chapter provides the flow of IASA MAC and a detailed description of the implementation.

The IASA MAC protocol has two different main states. The normal state is the communication state, in which the network operates uninterfered without any restrictions. If no interference occurs, this state is kept and IASA MAC does not differ from an ordinary MAC protocol. However, as assumed and consistently motivated throughout this work, the Wireless Sensor Network (WSN) will be affected by interference at some point in time. When this happens, the interference has to be detected in the communication state before an efficient, interferer-specific mitigation strategy can be applied. If the Packet Error Rate (PER), computed with the help of missing Acknowledgments (ACKs), increases over the default threshold of 25% at a node, external interference is suspected to be the reason. Since it can be assumed that IASA MAC is used in WSNs, where a reliable delivery of packets is required, the use of ACKs is common. This Backward Error Correction (BEC) also provides a basic protection against weak interference (e.g. Bluetooth interference). Internal interference is avoided due the use of Carrier Sense Multiple Access (CSMA)/Collision Avoidance (CA) relying on a CCA Mode 2 request. If the PER increases over 25%, these initial methods are not sufficient anymore and the classification algorithm developed and discussed in Chapter 5 is used to gain more information about the form of interference. As a result of the interference classification, a mitigation strategy is chosen and applied.

Based on the discussion of possible mitigation strategies in Chapter 6, the following mitigation strategies have been chosen for the different sources of interference. If the interference is caused by IEEE 802.11, a channel change is organized in the network. Bluetooth interference is ignored, since any countermeasure leads to more overhead than benefit. In normal cases, the PER caused by Bluetooth stays considerably under 25%, regardless of the use of single- or multi-slot packets (see Section 4.3.3). Microwave oven interference is mitigated with the help of packet scheduling. Finally, IASA MAC returns to the communication state. If the interferer has been classified to be a microwave oven, the packet sending is scheduled in the following. If it has been identified as *WLAN*, the channel has been changed or will be changed shortly. An overview of this generalized flow is given in Figure 7.1.

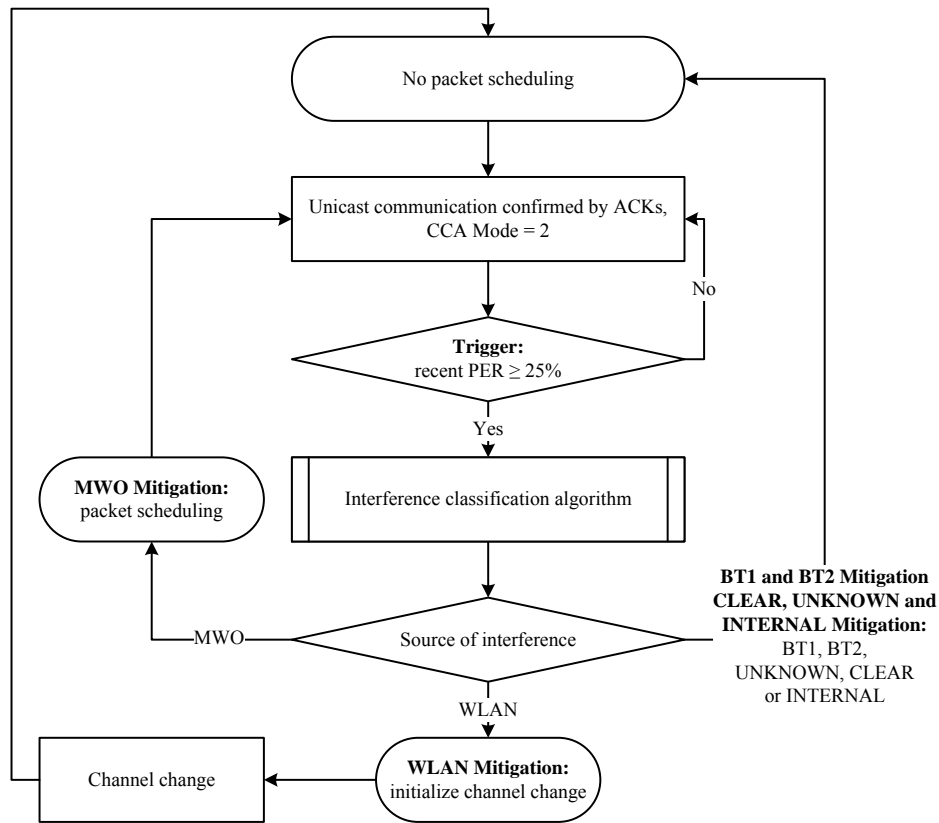


Figure 7.1: Generalized flow chart of IASA MAC. The bold titles correspond to the following sections.

The generalized flow chart of IASA MAC can also be compared to the approach of avoiding interference by channel estimation before a channel selection, as mentioned by Golmie (2006). She divides the process (in her work for Bluetooth) into two stages: an estimation phase and an online phase. The estimation phase is the time period, in which the channel quality is measured, or in the context of IASA MAC, it is the runtime of the classification algorithm (see Section 5.3.4 for the timing details). The online phase is the time of normal communication, which is also the main part of the IASA MAC protocol. The whole process of channel estimation is repeated after an estimation interval. Here, a more dynamic approach was chosen and a trigger was used instead of a time interval. Between these two phases, an exchange of the channel classification information happens (feedback), thus both communication partners have the same information and a mitigation strategy can be applied.

In IASA MAC, only channel change information is exchanged. The reduced exchange of information is an advantage in multi-hop WSNs, since an update that is disseminated to every node involves significant communication overhead. The lack of consistency between nodes caused by the minimized feedback is discussed in Sections 7.9.1 and 7.9.2.

The ratio of estimation phase and online phase is also an indicator of the efficiency of the classifier. To use the terms of Golmie (2006), the algorithm presented here allows an implicit estimation, since communication is still possible while the classification takes place. A full spectrum scan can be considered to be explicit, because the classification process does not allow further communication. Nevertheless, for an efficient WSN the estimation phase, i.e. the time used for classifying, has to be minimized to conserve as much energy as possible (for IASA MAC the maximum is 1 s, see Section 5.3.4 for the exact timings of the different classifications). By preferring a dynamically triggered estimation phase to a fixed estimation interval, the overhead is further

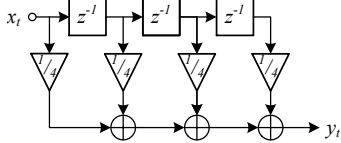
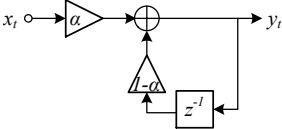
	Simple moving average	Exponential smoothing
Explicit computation	$y_t = \frac{1}{n} \sum_{k=0}^{n-1} x_{t-k}$	$y_t = \sum_{k=0}^{t-1} (1-\alpha)^k \alpha x_{t-k} + (1-\alpha)^t x_0$
Implicit computation	$y_t = y_{t-1} - \frac{x_{t-n}}{n} + \frac{x_t}{n}$ starting after y_n , which is calculated explicitly	$y_t = \alpha x_t + (1-\alpha)y_{t-1}$ with $y_0 = x_0$
Parameters	n is the length of the time window.	$\alpha \in (0, 1)$, where greater α gives more importance to more recent values.
Reaction to new values	The last n values are equally important (until weighted average is used), older values are not considered, group delay of $\frac{n-1}{2}$.	The most recent value is the most important, all values are considered, with older values being less important than more recent ones.
Implementation properties	n values have to be stored, addition and multiplication ¹ , decimal numbers required	x_t and n_{t-1} have to be stored, addition and multiplication ¹ , decimal numbers required
Filter design	for $n = 4$: 	

Table 7.1: Comparison of simple moving average and exponential smoothing. ¹If multiples of two are used, the multiplication operations can be implemented with the help of bit shifts in fixed-point arithmetic.

reduced. In the context of cognitive radio MAC protocols, Cormio and Chowdhury (2009) refer to the two time durations as “sensing and transmission time” instead of estimation and online phase.

The details of the different states of IASA MAC are described in the following sections.

7.3 Trigger

As just mentioned, IASA MAC sends packets in its normal communication state, which are confirmed with the help of ACKs by the receiver. Based on the number of received ACKs, the PER can be calculated. In contrast to all the PERs given in this work so far, the PER for IASA MAC is not computed at the end of an experiment, but live while transmitting packets. Thus, not all packet transmissions are of interest for the PER, only the most recent ones are of importance. In consideration of the latter, a filter that indicates a recent trend in the data can be used. In the case of IASA MAC, the data are a stream of binary values indicating whether the ACK was received or not.

A typical example of such a trend-highlighting filter is the arithmetic mean over a time window, known as moving average filter, which can be understood as a simple Finite Impulse Response (FIR) filter with low pass characteristics. Another approach is exponential smoothing, which is used in IASA MAC for the following reasons: it is easier to compute, it gives more importance to the latest values and it thereby allows a quick reaction. For performance reasons, it has been implemented in fixed-point arithmetic. Exponential smoothing is an Infinite Impulse Response (IIR) filter, which is shown in the comparison of both filters in Table 7.1 (Barkat, 2005).

Additional to the drop of the exponentially smoothed PRR to 75% or below, further auxiliary conditions have to be fulfilled before IASA MAC starts an interference classification that results in a mitigation strategy. IASA MAC uses a short waiting period after applying a strategy in order to avoid an oscillation as well as to give the mitigation strategy a sufficient amount of time to show an effect. At least 2 min have to expire between a *WLAN* or *MWO* classification including its resulting mitigation strategy and the next restart of a new interference classification on the same node. Especially for the channel change resulting from detected *WLAN* interference, a faster restart is not useful, since the other nodes have to be informed about the channel change. The details of the *WLAN* mitigation are given in Section 7.5. The waiting period is 30 s for all other classification results (*BT1*, *BT2*, *CLEAR*, *UNKNOWN*, *INTERNAL*), which lead to no explicit mitigation strategy.

Sending intervals vary from less than a second to over an hour between different WSNs or even within a single WSN. Therefore as an additional condition, more than 50 transmission attempts have to be made since the last mitigation started.

However, the just given conditions are default values, which have proven to be reasonable in test setups and experiments done by the author. They might not be ideal for certain WSNs and therefore, they might have to be optimized for special cases.

Furthermore, it has to be mentioned that the PER cannot be computed for all types of packets. The addressing of a packet has to be clear to confirm its reception. Only a unicast packet has a single, clear receiver and can therefore be confirmed by an ACK (see Section 2.1.2 for an introduction to the different delivery semantics). Therefore, all the previously mentioned packets are assumed to be unicast packets. Unicast and broadcast are, among others, implemented in the Rime communication stack as communication primitives. The latter are functions in ContikiOS that can be called (Dunkels et al., 2007). For a more detailed understanding of the implementation of the unicast-based trigger conditions and the mitigation strategies, the two main components of the ContikiOS network architecture are explained in the following: the Rime communication stack and the Chameleon header transformation module (Dunkels et al., 2007).

7.4 Packets in ContikiOS: Rime Communication Stack and Chameleon Header Transformation Module

The network architecture in ContikiOS is built of two main components, the Rime communication stack and the Chameleon header transformation module. On the Data Link Layer, the Rime communication stack offers different communication primitives, which are often related to each other (Dunkels et al., 2007). The unicast implementation (*uc*¹), which is used by IASA MAC, offers a best-effort single-hop unicast. This means that the packet is transmitted once and the receiving nodes in a one-hop range check whether their address matches the receiver address of the packet. If this is the case, the receiving node starts processing the packet.

This *uc* unicast is based on an identified best-effort single-hop broadcast (*ibc*), which is a packet without a receiver address, but with a sender address. This *ibc*, in turn, is derived from the anonymous best-effort single-hop broadcast (*abc*). The basic *abc* broadcast carries no sender information, thus it contains the data payload with a minimum of overhead. The idea of varying overhead for different packet types is explained later for the Chameleon header transformation module, which allows the dynamic construction of packet headers.

The Rime communication stack offers more communication primitives, as the reliable single-hop unicast (*ruc*) that is based on the stubborn single-hop unicast (*stuc*) being derived from the *uc* used here. The *stuc* unicast periodically transmits a packet until it is stopped. This is for instance done by the derived *ruc* when the reception was confirmed by an ACK.

All communication primitives supported by the Rime communication stack, which is comparable to a kit of building blocks, are shown in Figure 7.2.

While further architecture details of the Rime communication stack are beyond the scope of this work, all communication primitives can be broken down to a so-called logical channel and to additional packet attributes. The packet attributes play an important role for the Chameleon header transformation module. Chameleon is implemented below the logical channel. Note that this logical channel is not identical to the physical frequency channel. It is an abstract concept comparable to a port known from Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Each channel has a set of protocols and packet attributes. An overview of

¹Function or module names in italics are used by Dunkels et al. (2007), while the names of the implementation in ContikiOS vary slightly.

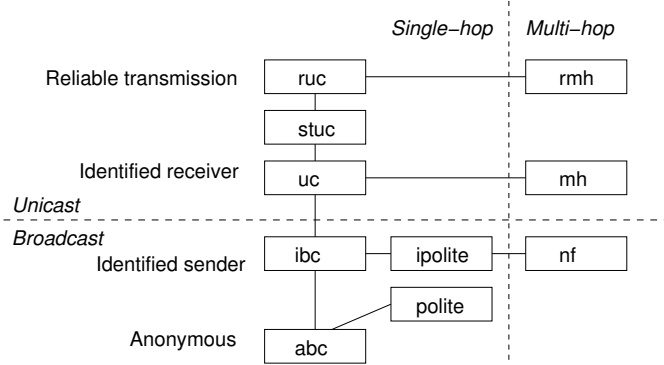


Figure 6. The communication primitives in the Rime

stack and how they are layered. The Rime communication stack and their relations. The communication primitives are the implementation names of the primitives (from top to bottom): *ruc* stubborn single-hop unicast, *rmh* hop-by-hop reliable multi-hop unicast, *stuc* stubborn single-hop reliable multi-hop unicast, *uc* stubborn single-hop unicast, *mh* hop-by-hop reliable multi-hop unicast, *ibc* identified best-effort unicast, *ipolite* identified best-effort unicast, *nf* network flooding, *polite* network flooding, *polite* network flooding. When an event occurs that needs to be forwarded to the application, Chameleon associates the event with the channel on which the event occurred. The next time the channel is active and a packet is sent towards the local application, Chameleon sets the appropriate packet attribute for the packet that is sent up through Rime. The feedback information may also be piggybacked on acknowledgement packets that Chameleon produces for the benefit of the application.

4 The Rime Protocol Stack

The Rime protocol stack provides a set of communication primitives ranging from best-effort local neighborhood broadcast and reliable local neighbor unicast, to best-effort network flooding and hop-by-hop reliable multi-hop unicast. Applications or protocols running on top of the Rime stack may use one or more of the communication primitives provided by the Rime stack.

4.1 Rime Communication Primitives

The protocols in the Rime stack are arranged in a layered fashion, where the more complex protocols are implemented using the less complex protocols. The communication primitives in the Rime stack and how they are arranged is shown in Figure 6.

4.1.1 Anonymous Best-effort Single-hop Broadcast

The anonymous best-effort single-hop broadcast primitive (*abc*) is the most basic communication primitive in Rime. It provides a way to send a data packet to all local neighbors that listen to the channel after the initial deployment phase. Since the IEEE 802.11 standards are so complex and the sending power overpowers IEEE 802.15.4 transmissions, there is no commonly successful mitigation strategy other than avoiding the used IEEE 802.11 channels in the spectrum. However, to avoid false positive CSMA/CA backoffs causing sender-side interference, CCA Mode 2 is used

ng
ound a lightweight layering
primitives are designed in a
mplex communication prim-
is is inspired by work in the
g [20], where many simple
mplex mechanisms such as
with many simple layers al-
f composition of layers; we
ate if provable properties are

ghtweight layering principle
ne communication primitives
plement and Figure 2 will
plementations of the primi-
ns are the implementation names of the primitives (from top to bottom): *ruc*
ant for memory constraints
ions may attach to any layer-
express precisely how much
s that they need. In more
uch as the TCP/IP protocol
e to express such fine-grained
ble, a TCP/IP application that
ot guaranteed delivery cannot
protocol architecture.

7.3. Furthermore, a logical channel is the interface between the Rime communication stack and the used channels

ations
the Chameleon header trans-
modules in Chameleon pro-
ributes supplied by the Rime
in the packet attributes into a
By transforming the packet
t format, the Chameleon ar-
ible with another node that
ever, header transformations
another communication pro-

7.5 WLAN Mitigation

personated contains protocol
ime protocol, the Chameleon
he missing parts of the im-
mpersonates. For example, a
module must implement the
ver Ethernet, and a header
slates a reliable bulk transfer
m must implement the SYN
mission can start.

7.5.1 WLAN Mitigation

channel alignment should be
WLAN interference. This
advantages and disadvantages
ack up to the application run-
of this includes both the
of the radio link quality

7.5.1.1 Anonymous Best-effort Single-hop Broadcast

WLAN interference. This
advantages and disadvantages
ack up to the application run-
of this includes both the
of the radio link quality

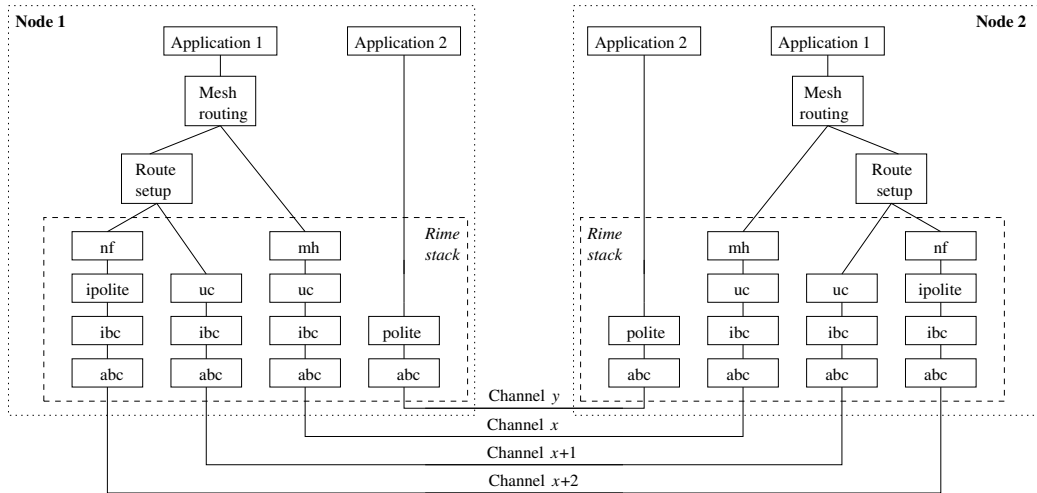


Figure 5. Two applications communicating using Rime. One uses a mesh routing protocol running on top of the Rime stack and one uses the Rime stack directly. Each communication path uses its own logical channel. See Section 4.1 for explanations of the names in the protocol stack.

Also, the underlying individual logical channels of each primitive can be seen. See Figure 7.2 for details about sender-side interference strategy that is executed when the interference has recently been used to reduce the size of IPv6 headers as part of the 6lowpan standardization effort [27].

Traditional header compression requires the header compression module to both parse the original header format and to bit-pack the optimized header format. With packet attributes, header compression is naturally included in the architecture. Header parsing is performed on incoming packets, and the production of bit-packed headers is as discussed above, already a part of the architecture.

3.2 Logical Channels

Communication in the Chameleon architecture uses different logical channels. Each channel has its own set of protocols and packet attributes. The communicating parties must agree beforehand on the particular set of protocols to be used for a particular channel.

Figure 5 illustrates the concept of logical channels in the Chameleon architecture (see Section 4.1 for explanations of the names in the protocol stack). Two applications, Application 1 and Application 2, on two different nodes and communicate with each other using four logical channels, y , x , $x + 1$, and $x + 2$.

Application 1 uses a mesh routing protocol, which in turn uses a route discovery protocol, and the best-effort multi-hop unicast Rime primitive, mh. Both nodes know that the mh primitive uses logical channels that

the route discovery protocol uses channels $x + 1$ and $x + 2$, and that channel y is used by Application 2. Both nodes have agreed on this channel configuration before the communication is set up. The situation is similar to how all Internet hosts agree on that TCP port 80 is used for HTTP communication and that TCP port 25 is used for SMTP.

The logical channels are opened at run-time. When an application opens a logical channel for a stack of Rime primitives, the primitives register the packet attributes they use with Chameleon. Chameleon uses this information both when constructing outgoing headers and when parsing incoming headers.

The process of constructing and parsing headers is deterministic and reversible. When a packet is sent on a channel, I_{min}

$$I_{max} = \log_2 \left(\frac{t_{max}}{I_{min}} \right) \tag{7.1}$$

Algorithm 7.1: TRICKLE ALGORITHM, ACCORDING TO (LEVIS ET AL., 2011).

```

/* Parameters: */
Imin; // minimum interval size
Imax; // maximum interval size
k; // redundancy constant
/* Internal variables: */
I; // current interval size
t; // a time within the current interval
c; // counter
/* 1. initialization: */
I := value in range of [Imin, Imax];
/* 2. interval begins: */
c := 0;
t := random[I/2, I];
/* 3. incoming consistent transmission: */
c ++;
/* 4. time t reached: */
if (c < k){transmit;}
/* 5. interval I expires */
I := 2 * I;
if (I > Imax){I = Imax;}
/* 6. incoming inconsistent transmission: */
if (I > Imin){
  I = Imin;
  go to step2;} //new interval begins

```

The parameter t_{max} is given in time units and is mainly important for nodes joining the network after the initial flooding. The pseudo-code of Trickle is shown in Algorithm 7.1. The basic idea of Trickle is that a node sends its version (e.g. the timestamp of its information) after a random time (step 4 in Algorithm 7.1). However, if many consistent transmissions have been received, i.e. other nodes announce having the same version, there is less need of broadcasting its own, well-established version, since all other nodes seem to be up-to-date (step 3 and the condition in step 4). The opposite applies if the node receives inconsistent transmissions, i.e. announcements of newer or older versions: then the node tries to transmit sooner (step 6). Both a flooding and the resulting congestion of the network by a packet storm can be avoided by transmitting only sooner and not immediately after detecting the inconsistency. It can happen that multiple nodes are interfered with by IEEE 802.11 and therefore the channel agility is triggered on all of them. If two or more nodes start to disseminate an update through the network, Trickle still works well, since this is the same situation that occurs after a few broadcasts in Trickle.

A big advantage of Trickle is that the channel utilization is equal for dense networks and sparse networks, although the latter require logically more transmissions per node to propagate a message.

With the help of Trickle, a new channel can be announced throughout the network by IASA MAC. After a waiting period, in which it can be assumed that all nodes are informed about the upcoming channel change, the actual channel is changed. The new channel can be chosen:

- randomly (preferably, it should be at least four channels away from the current channel due to the typical spectral width of IEEE 802.11),
- after an energy scan on potential new channels (which increases the time period of being disconnected from the rest of the network) as suggested e.g. in (ZigBee Alliance, 2008b), or
- based on a preference vector.

The latter has been implemented here, since preferred channels as 15, 20, 25 and 26 can be determined before deploying the network. IASA MAC uses the implementation of Trickle in ContikiOS to spread the new channel.

This Trickle implementation is preconfigured with $I_{min} = 1$, $I_{max} = 4$ and the redundancy constant $k = 1$ (k is named *DUPLICATE_TRESHOLD* in the source code). The given interval times correspond to multiples of the *INTERVAL* parameter, which is set to 1 s for IASA MAC. Therefore the maximum interval (t_{max}) reaches 16 s after four (I_{max}) rounds. Thus, finally the network is roughly updated once every 16 s in an endless loop. However, since a channel change is performed, the propagation of the new channel becomes obsolete after the channel change. After the node changed to the new channel, the propagation of the new channel is not required anymore, since all possible receivers are already communicating on the new channel. To guarantee a reliable propagation of the channel change, the channel is changed 1 min after a new channel propagation message has been received. This waiting period of 1 min, which allows at least six rounds of the Trickle algorithm to be executed, is used to spread the new channel announcement before leaving the actual channel and not participating in the propagation anymore. In the IASA MAC implementation, the Trickle announcements are explicitly canceled when changing the channel. The times used here have proven to be suitable for the WSNs used in the course of this work, however for other requirements (e.g. extremely large WSNs), the timing intervals might have to be adjusted. With the help of the detailed explanations given in this section, the matching of parameters to a specific requirement of a WSN is assumed to be possible.

7.5.2 Discussion

The efficiency of the channel agility mitigation strategy to avoid IEEE 802.11 interference is hard to evaluate, since the wireless environments differ significantly. Thus, a single channel change can solve the problem of interference or in worst case scenarios, multiple channel changes are required. Nevertheless, the timing of the channel agility can be definitely stated. The classification timing is given in Section 5.3.4 (between 615 and 1,000 ms) and after the classification at least 1 min expires. In this waiting period of 1 min, packets can be received over the still interfered channel. If the new channel is also significantly interfered with (e.g. by another IEEE 802.11-based WLAN), the next interference mitigation can be triggered after a time of 2 min after the classification, i.e. 1 min after the actual channel change (as explained in Section 7.3).

7.6 BT1 and BT2 Mitigation

The interference caused by Bluetooth, either based on single- or multi-slot packets (class *BT1* and *BT2*, respectively), is the weakest of all forms of interference researched in this work. Additionally, it occurs randomly due to frequency hopping. As already mentioned in Section 6.3.2, a suggested solution to mitigate the effects of Bluetooth interference is to fragment the already short IEEE 802.15.4 packets (Nicolas and Marot, 2012), but this approach is not feasible due to the overhead and the limited size of IEEE 802.15.4 packets.

Since Bluetooth is a weak and random interferer, an appropriate solution to mitigate its interference is the use of ACKs and retransmissions. The possibilities of BEC to overcome weak interference have been discussed in Section 6.3.1. Furthermore, CCA Mode 2 is chosen. Although a CCA detection of Bluetooth is possible with the help of an ED-based CCA, the reaction of IEEE 802.15.4 is too slow, as already discussed in Section 6.3.3. Therefore, CCA Mode 1 and 3 with their ED-based CCA requests are not beneficial. Both ACKs and CCA Mode 2 are used in IASA MAC.

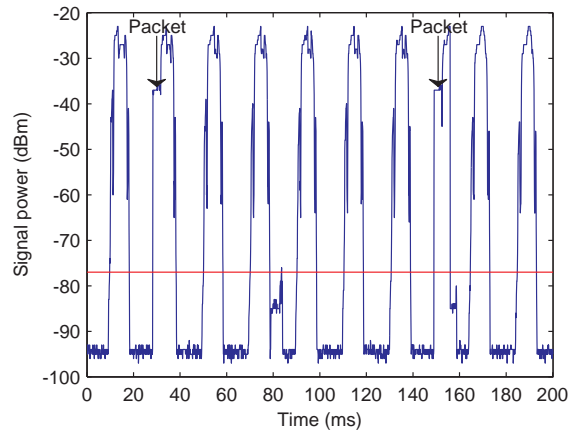


Figure 7.4: Microwave interference corrupting the end of IEEE 802.15.4 packets. The packets are sent after successful CCA requests, but the end of the packets are corrupted by the interference of the microwave oven.

7.7 MWO Mitigation

As already mentioned in Section 6.3.4, the stable timing pattern of microwave oven interference, although utilizing the channel heavily, allows avoiding the periods of interference. By using packet scheduling, the author has chosen the same approach as Rensfelt et al. (2012), since it is the obvious consequence of the temporal interference pattern. Packets on the sending node are timed to be sent 20 ms or any multiple of 20 ms after the last successful transmission start time. For the actual timing, a Radio Duty Cycling (RDC) Layer (see Section 2.3.2) that is already part of many WSN MACs has been used here. In ContikiOS, an RDC driver, IASA RDC, has been developed to provide the required packet scheduling to overcome the microwave oven interference. Since most WSNs send packets in intervals longer than 20 ms, no additional buffers are needed. Levis et al. (2004) claim that the TinyOS networking stack running on the MICA2 sensor node (crossbow technology, inc, 2003) can handle around 40 packets per second, i.e. a packet can be sent every 25 ms. However, if special requirements desire higher data rates, the packet scheduling can be extended with a buffer at the sender side. In contrast to WLAN and Bluetooth interference, an ED-based CCA mode (1 or 3) allows prompt reactions to mitigate the effect of the microwave ovens. However, in IASA MAC, CCA Mode 2 has been chosen to provide the best results (see Section 6.3.3) and to prevent internal interference in the WSN. Although ED-based CCA can detect the microwave oven interference and the reaction speed is not an issue, CCA is in some cases limited to sender-side interference and cannot guarantee that the packet is delivered. After a CCA request correctly indicates a clear channel, the end of the packet can be corrupted, as shown in Figure 7.4 and therefore the ACKs are used to guarantee a successful reception.

The length of the packet has only a minor influence on the PRR when using IASA MAC with its improved RDC. The packet length plays a role for finding the right initial cycle start, after which it becomes less important. The uninterfered time of approximately 10 ms within the 20 ms period of the microwave oven signal is long enough so that the longest possible IEEE 802.15.4 packet including an ACK can be transmitted without being interfered (compare to Figure 6.6).

As already mentioned in Section 2.6.1, a different mains frequency (60 Hz instead of 50 Hz) is used in North America. This results in a $16.\bar{6}$ ms period instead of 20 ms and therefore, at least 8 ms can be assumed to be uninterfered. This time period is also long enough to send the longest possible IEEE 802.15.4 packet including an ACK.

In most cases, the duration of microwave oven interference is limited to a time under an hour. The first IASA unicast packet, which is sent 30 minutes after the start of the packet scheduling,

restarts the interference classification algorithm, since it is likely that the interference is over. See Section 7.3 for the explanation of triggering the interference classification and details about IASA unicast packets.

7.7.1 Testing

To show the effectiveness of the mitigation approach, an experiment in the Radio Frequency (RF) anechoic chamber has been conducted. Since only the packet scheduling is researched in this experiment, the interference detection and classification phase have not been tested. The classification and its success rate have been discussed in detail in Chapter 5.

Microwave Oven 1 was placed 1.5 m away from the sensor nodes, which had a distance of 0.5 m between them, as shown in Figure 7.5. A sensor node (Identification (ID)=1) was sending 10,000 packets with a Medium Access Control Protocol Data Unit (MPDU) of 33 bytes to the other sensor node (ID=2). Each packet was confirmed with the help of an ACK having a MPDU of 5 bytes. The sending interval was chosen randomly between 90 and 110 ms, which can be assumed to be faster than in many uses cases. However, a better evaluation of the approach was possible through the high packet rate. Due to the randomly chosen interval, synchronization effects were avoided and random channel access, as performed by CSMA/CA, was simulated. However, the CSMA/CA Driver of ContikiOS was deactivated, since it includes retransmissions. Furthermore, the sender transmitted with a power of only -25 dBm and channel 20 was used. Due to this reduced sending power, a longer distance between the two nodes is simulated. In the evaluation of this mitigation strategy by Rensfelt et al. (2012), packet loss is caused primarily by CCA failures and therefore, only sender-side interference is tested.

The experiment presented here simulated either a network (sender and receiver) under interference or receiver-side interference, depending on the used CCA mode. The case of pure sender-side interference has already been discussed with the help of an experiment in Section 6.3.3. As in the just mentioned experiment in Section 6.3.3, 2,500 packets have also been transmitted at once for this experiment and then the water in the microwave was replaced by fresh lukewarm water.

The numbers of received packets indicating the efficiency of the packet scheduling are given in Table 7.2. Furthermore, the influence of the CCA mode is shown by comparing CCA Mode 2 and CCA Mode 3, which is the default ED-based mode of the CC2420 radio (Chipcon, 2004). In addition to the given PRR at the Application Layer of the receiving node, the packet loss is broken down further in Table 7.2.

While the total number of 10,000 packets was the initial value for each setup, some packets were not sent due to contention drops when the channel was reported busy by the CCA. Contention drops occurred for CCA Mode 3 (CCA Mode 1 can be assumed to be similar to CCA Mode 3, see Figure 6.5). The column “Packets received” of Table 7.2 shows the number of correctly received packets on the receiver side (in the Application Layer), which suffered from a high packet loss if no packet scheduling was used.

The packet loss between the “Packets sent” and the “Packets received” is due to the low Signal to Interference Ratio (SIR), which was in the disconnected region when the microwave oven was radiating (see Section 4.2.7 for the concept of connectivity regions). The experiment comparing the effects of the CCA modes in Section 6.3.3 showed almost no packet loss on the receiver side. The higher transmit power of the nodes led to a higher SIR and thereby only sender-side interference was researched.

The second last column in Table 7.2 shows how many packets have been successfully acknowledged. ACKs are also lost due to a low SIR, but they are sent in the opposite

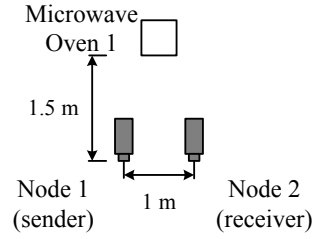


Figure 7.5: Experiment setup to test the efficiency of packet scheduling under microwave oven interference. Channel 20 was used.

Packet scheduling	CCA mode	Packets intended to send	Packets sent	Packets received	Packets acknowledged	Interference type
No	2	10,000	10,000	6,474	6,260	Receiver side
No	3	10,000	9,529	6,436	6,213	Sender & receiver side
Yes	2	10,000	10,000	9,855	9,850	Receiver side
Yes	3	10,000	9,875	9,790	9,782	Sender & receiver side

Table 7.2: Number of packets at different stages in a simple link communication under microwave oven interference. The causes of loss were determined with the help of the statistics of the Rime communication stack.

communication direction. The reason of the packet loss of both data packets and ACK packets is the spatially limited setup size in the RF anechoic chamber.

The experiment by Rensfelt et al. (2012) show similar results, although their packet loss was lower, which could be caused by the closer distance of only 0.5 m instead 1.0 m between the sensor nodes, by differences between the microwave ovens or by a different packet sending interval. Rensfelt et al. (2012) report a PER decrease from 12.71% to 2.54% as well as an almost equal decrease of failed CCAs from 12.46% to 2.45% due to packet scheduling. The results suggest that only sender-side interference was addressed in their setup. In contrast, the experiment of this work investigates both sender- and receiver-side interference by using CCA Mode 3 and 2, respectively. The CCA mode can be neglected, since the difference between CCA Mode 2 and 3 was only 68 packets in the experiment, which is less than one percent of the original 10,000 packets. Nevertheless, CCA Mode 2 is used in IASA MAC for a maximum PRR and to avoid sender-side interference.

7.7.2 Discussion

Although packet scheduling delivers a considerable improvement of the PRR, it has to be mentioned that channel agility, i.e. a channel change, represents another strategy to overcome interference caused by microwave ovens. However, the PRRs achieved with the help of packet scheduling make the overhead of a channel change unnecessary, including its propagation and the uncertainty of the quality of the new channel. These properties have been discussed for the WLAN mitigating channel agility in Section 7.5.

7.8 CLEAR, UNKNOWN and INTERNAL Mitigation

If the channel is classified as *CLEAR*, there is obviously no need to mitigate any interference, since the interference is over and no mitigation strategy has to be applied.

For unknown sources of interference (class *UNKNOWN*), no appropriate mitigation strategy can be chosen, thus the default settings of IASA MAC are used. Certainly, the interference classification algorithm and the mitigation strategies can be extended to suit different use cases and RF environments.

	IEEE 802.11	Bluetooth	Microwave ovens
Expected worst PER	75%	10%	60%
Classification time	615 ... 1,000 ms	Not triggered due to low PER $\leq 10\%$	320 ... 400 ms
Correct classification rate	> 90%	N/A	> 80%
Mitigation strategy	Channel agility: triggered channel change	N/A	Packet scheduling
Overhead, delay and disconnection due to mitigation strategy	> 60,000 ms delay before channel change, in which interfered communication is possible; short, partly disconnected due to channel change (exact timing depends on success of Trickle); additional packets of Trickle	N/A	Short delay (≤ 20 ms) for every transmission
Expected PER after mitigation	Depending on new channel	N/A	< 5%

Table 7.3: Overview of the interference situation and the efficiency of IASA MAC.

The internal interference class (*INTERNAL*) is returned by the classification algorithm when an IEEE 802.15.4 packet has been received during the sampling and thereby the sampling process is falsified by the energy of the IEEE 802.15.4 packet. For normal use cases of WSNs, it is unlikely to have a PER of above 25% because of internal interference, since there are less packets sent in a WSN and the MAC organizes a fair use of the medium. Hence, it is more likely that the interference is caused by another source, but the IEEE 802.15.4 packet has been received despite the external interference. In very dense networks with short sending intervals, the problem of interrupting the sampling phase of the classification algorithm can occur due to internal traffic. However, if such a high internal packet rate is able to be received, the severity of external interference is limited. If the PER stays over 25%, the classification is repeated after the waiting period of 30 s.

7.9 Summary and Discussion

After discussing all elements of IASA MAC in detail, the generalized flow chart of IASA MAC given in Figure 7.1 can be extended to the detailed flow chart shown in Figure 7.6. This figure presents the full conditions, which trigger an interference classification. Furthermore, it shows the timing of the channel change announcement running concurrently to the normal mode of communication on the sensor node. The channel change is announced to overcome the *WLAN* interference class. It can also be seen that the complexity of IASA MAC is moderate and therefore the IASA MAC implementation is compact, with a single additional communication primitive (IASA unicast) in the Rime communication stack and a simple RDC Driver (IASA RDC). Since the PER is only gathered by normal packets (IASA unicasts), there is no transmission overhead when no interference occurs.

The PER is not only the trigger for the interference mitigation in IASA MAC, it is also a main performance indicator of the wireless links. The expected PER before and after the mitigation is within the ranges shown in the overview of IASA MAC in Table 7.3. Furthermore, an insight into the effects of mitigation is given with the help of the PER ranges. The initial unmitigated PERs have already been motivated in Section 4.4. The table also states the timing of the classification algorithm, as discussed in Section 5.3.4, and the expected classification rates based on the evaluation of the classification algorithm in Section 5.4.

A comprehensive experimental evaluation of IASA MAC is not feasible due to the unlimited possible setups. Nevertheless, the performance of the single mitigation strategies has been shown in isolated setups throughout this chapter. In the following, the overhead and the efficiency are discussed in two scenarios that are beyond the RF anechoic chamber experiments. Both scenarios are based on asymmetric interference ranges. Asymmetric interference can be caused in larger WSNs if they are only partly interfered with by a single source of interference or if different parts of the WSNs are interfered with by different sources of interference.

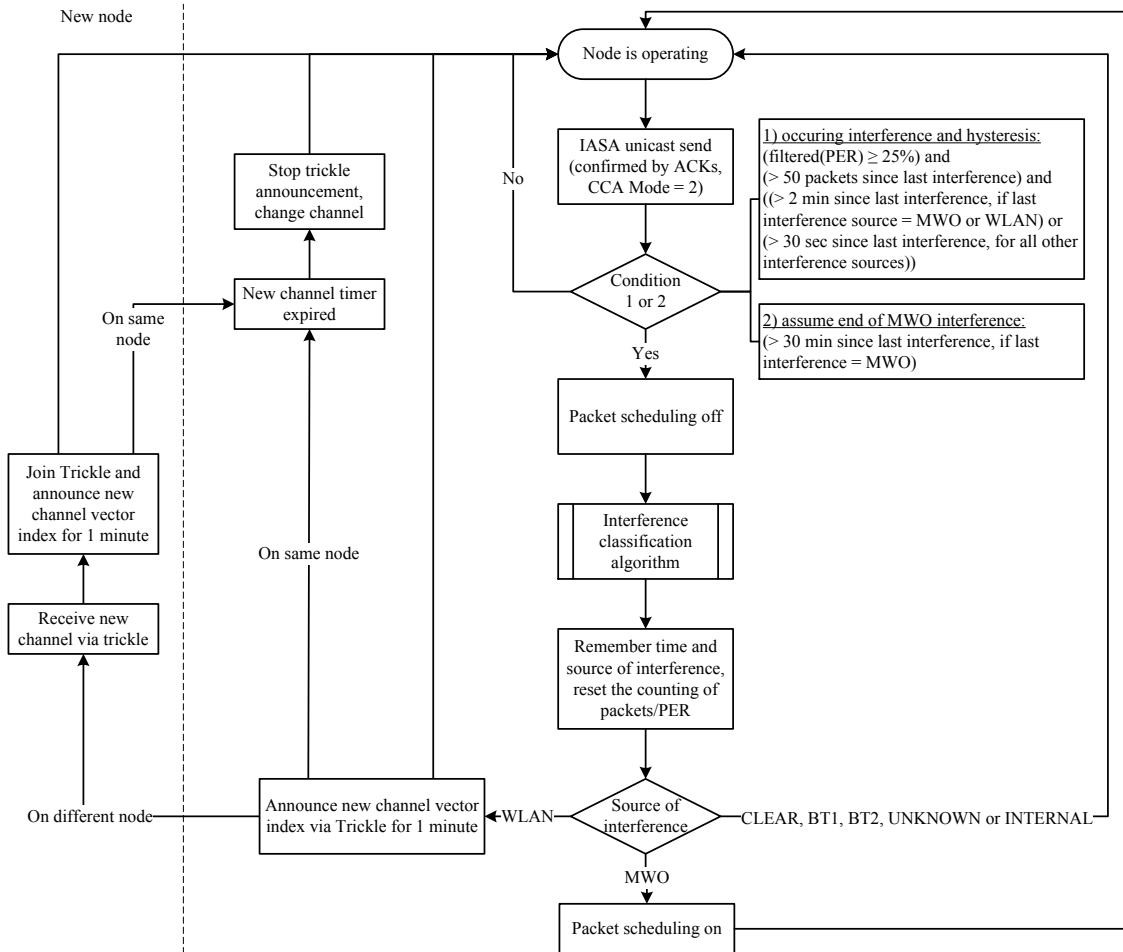


Figure 7.6: Detailed flow chart of IASA MAC. Extends the chart shown in Figure 7.1 by the full conditions that trigger IASA MAC interference mitigation strategies (underlined conditions 1 and 2 have been drawn in extra boxes for the sake of readability) and the concurrently running Trickle operations.

7.9.1 Hidden Interferer Problem

WSNs can cover large areas due to their multi-hop capabilities and therefore it is plausible that interference is limited to some nodes of the network. Especially the relatively short interference ranges of microwave ovens make such a scenario plausible, even for smaller deployments. For instance, a WSN used for home automation or monitoring covers a single house or flat. Even within this dwelling, parts of the WSN can be interfered with by a microwave oven, while others are uninterfered. Hence, sensor nodes in a kitchen are assumed to be interfered, and the nodes in another room, e.g. the living room, are not. The links from nodes in the kitchen to nodes outside the kitchen are all interfered on the sender side. The wireless links from the uninterfered sensor nodes in the living room to the interfered nodes in the kitchen can be assumed to be interfered on the receiver side.

The sender-side interference of the kitchen nodes is eliminated when using CCA Mode 2, as suggested in IASA MAC. The other direction, from the living room to the kitchen, is more challenging. These links suffer from the external interference caused by the microwave oven. However, due to the missing ACKs, the receiver-side interference is also noticed by an uninterfered node in the living room trying to send to the kitchen. Therefore, the interference classification is triggered on living room nodes. It depends on the precise setup when the living room nodes are able to classify the interferer with the help of their CCA requests. The following gives a simple, theoretical mathematical analysis of such a problem.

The default CCA threshold of the here used CC2420 radio (Chipcon, 2004) is -77 dBm in CCA Mode 1 and 3. For most of the RF anechoic chamber experiments, this is over-sensitive leading to false positive CCA backoffs. This is due to a high SIR, which is provided by sensor nodes that are positioned closely together. In the case of spatially small setups, the CCA request allows the classification of distant interferers (affecting nodes in more than one hop distance). If the deployment is spatially larger, there is the risk that the sender might not be able to detect the source of interference that is interfering with the intended receiver. This is a version of the hidden node problem, which has been already introduced shortly in Section 2.1.

The hidden node problem or variances of it were discussed throughout the course of this work. For instance, the relation of the CCA range and the communication range has been explained in Section 4.3.2 (being illustrated in Figure 4.13) and in Section 4.3.3 (Figure 4.14). This comparison of sender- and receiver-side interference ranges is based on the same fundamental limitation as the hidden node problem. Another variation of this range problem was discussed in Section 5.2.1 in the form of an interfering WLAN consisting of an Access Point (AP) and a client node. The interference classification algorithm is only able to detect the WLAN AP and therefore, Section 5.2.1 has analyzed the risk of being only under the interference of the client, while being outside the range in which the AP is detectable. This risk has been shown to be negligible, which is due to different typical transmit powers of APs and WLAN clients.

The hidden interferer problem, which is a version of the hidden node problem, occurs in the example of a WSN being partly interfered with by the microwave oven. In Figure 7.7, this variance of the fundamental problem of limited ranges is illustrated with the help of an example. As shown in the figure, the following conditions define such a problem. Obviously, the communicating nodes (S_1 and S_2) have to be able to communicate without being interfered, i.e. the power $P_{S_1}@S_2$ of the message sent by S_1 has to be high enough to be received at S_2 . For the potential hidden interferer to be relevant, its interference power $P_I@S_2$ has to be high enough at S_2 to generate a $SIR_{(S_1,I)}@S_2$ that is below the decodable minimum of the radio of S_2 . So far, these two conditions describe an interference problem. Finally, it has to be checked whether the interferer is hidden to the sender. The power of the interferer received at the initial sender S_1 has to be below the threshold of the CCA and therefore S_1 cannot notice the interferer.

These conditions and the computation of the examples in Figure 7.7 show that a closed-form decision can be formulated for a single case after the selection of an appropriate path loss model (see Section 4.2.2). For a more precise description of the real world, obstacles as walls and more effects of real world radio wave propagation (see Section 4.2.2) can be included in the model. However, the mathematical solution to the problem is not always a good estimation of the real world and the modeling of the environment can be complex.

As a pragmatic solution for practical deployments, the Signal to Noise Ratio (SNR) margin should be chosen to be higher than required. Thereby, the resulting SIR caused by external interference is also high enough to overcome the problem of the hidden interferer when interference occurs.

7.9.2 Cooperation Between Different Mitigation Strategies

A second potential problem arising with WSN deployments over large areas is the situation that parts of the network can be interfered with by different sources of interference. Section 5.5.1 discusses the results of the interference classification algorithm in a scenario of multiple sources of interference overlapping in the frequency spectrum with roughly the same signal strength. Only the interferer with the highest channel utilization is classified in this case. In the unlikely scenario of multiple interferers, the detection of microwave oven interference is preferred to the detection of the other classes, while WLAN interference is still preferred to Bluetooth interference.

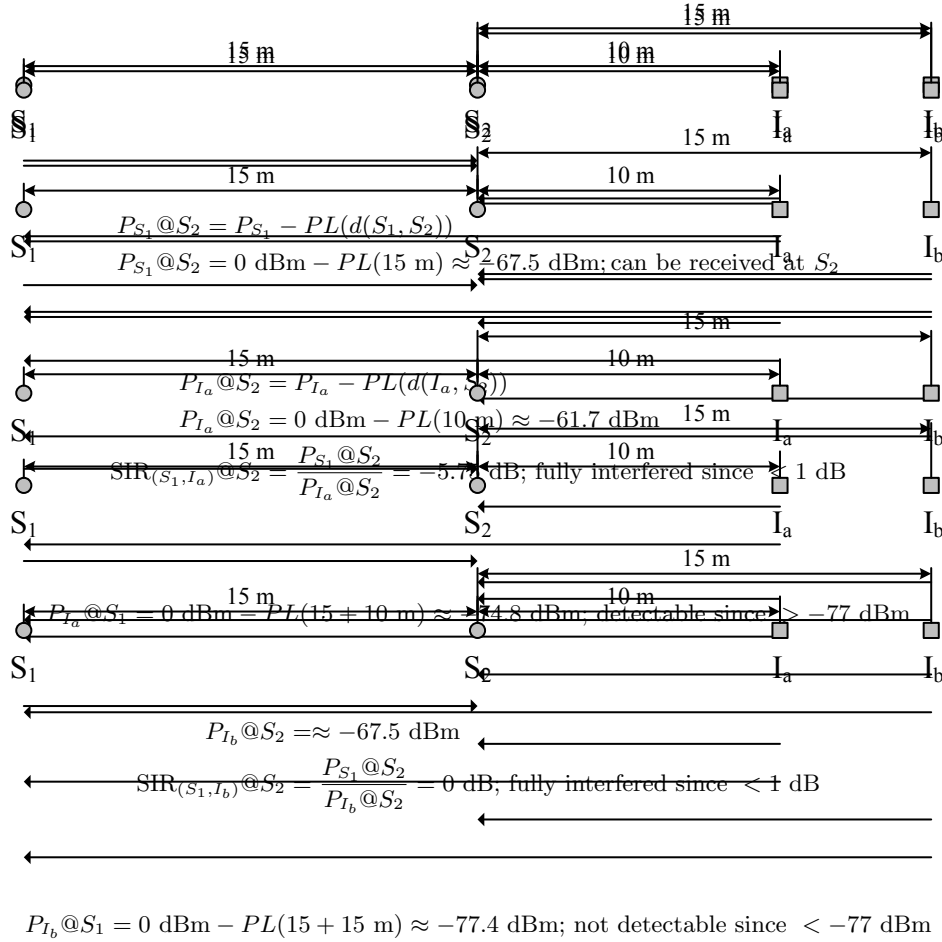


Figure 7.7: Simple example of a detectable and a hidden interferer. The receiving sensor node S_2 is under interference of I_a or I_b . The sensor node S_1 tries to detect interferer I_a or I_b with the help of a CCA request. For the loss of transmit power over distance, the path loss suggested by the IEEE (see Equation 4.6) is assumed. The uninterfered communication of S_1 with S_2 is possible, while in both given cases a and b , the interferer is strong enough to corrupt the communication of S_1 to S_2 . Sensor node S_1 can detect interferer I_a with the help of its CCA, while I_b is hidden to S_1 .

In the following, the case of asymmetric interference is of interest, where nodes apply different mitigation strategies. This is explained with the help of the example given in Figure 7.7. The initial situation is described in the following. Sensor node S_1 tries to reach node S_2 , but due to the interference of interferer I_a , the packets cannot be received by S_2 . Due to the missing ACKs, S_1 is aware of the interference. S_1 starts to classify the interferer I_a , which is within its CCA range. For this example, I_a is assumed to be a microwave oven and therefore, S_1 starts the packet scheduling. In the other direction of the communication link, S_2 is not aware of any external interference, since the energy of the microwave oven is not realized by CCA Mode 2 requests. The interference of I_a does not cause all packets sent by S_2 to S_1 to be corrupted (the resulting $SIR_{S_2, I_a}@S_1 = 7.3 \text{ dB}$ is in the upper range of the transitional region, see Section 4.2.7). Therefore, interference mitigation of S_1 is not triggered. In the resulting asymmetric constellation, a node applying an interference mitigation strategy (S_1 using packet scheduling) and a node not using a mitigation strategy (S_2) communicate.

A sensor node applying the microwave oven mitigation strategy used by IASA MAC, i.e. the packet scheduling of IASA RDC, can still receive not scheduled packets from uninterfered sensor

nodes without any restrictions. It is obvious that not scheduled nodes can receive scheduled packets.

Channel agility, as used to overcome the interference caused by IEEE 802.11-based WLANs, is always changing the channel of the full WSN and thereby affecting all nodes including uninterfered nodes. Therefore, there is no communication barrier between interfered and uninterfered nodes. The case that parts of the WSN are interfered with by different WLANs on different channels can lead to a longer search for a common uninterfered channel. The danger of a disconnection of the network due to different channel change announcements is avoided with the help of the waiting periods described in Section 7.5.1. Only if Trickle failed in reaching nodes within 1 min, the case that some nodes use an older channel would be given. However, if the network is denser, the spread over hops does not only work in one direction, but also backwards. Thus, a left out node is attempted to be reached multiple times: The initial announcing node (hop 0) reaches all nodes within its range (hop 1). These nodes spread the message further and reach nodes from the previous and the next hop distance (hop 0 and 2). The nodes at hop distance 2 also reach nodes further away (hop 3) and previous nodes (hop 1). Therefore, nodes of each hop distance are attempted to be reached two times.

7.9.3 Summary

In this chapter, IASA MAC was presented and discussed. IASA MAC is a prototype for the new emerging research direction of cognitive networks. It achieves a remarkable improvement of the PRR under interference, without requiring Software Defined Radio (SDR) hardware by using available hardware and only algorithms. The feasibility of the mitigation strategies used in IASA MAC has been proven by analysis and practically by giving a possible implementation in ContikiOS, which is a widely used WSN operating system. This implementation has been described in detail.

Channel agility has been chosen to mitigate IEEE 802.11-caused interference. While the channel change has already been suggested in (Nicolas and Marot, 2012; Rensfelt et al., 2012; Hermans et al., 2013), the details of its implementation within an interfered WSN have not been discussed in their work. In (Nicolas and Marot, 2012), a hard-coded channel change in a single setup is used in a prototype. The SoNIC solution by Rensfelt et al. (2012) and Hermans et al. (2013) does not mention details of the channel change and its coordination within the WSN. In IASA MAC, the chosen and evaluated Trickle algorithm provides a practically proven solution to the problem of the channel change announcement.

Finally, IASA MAC is a combination of the interference classification algorithm (Chapter 5) and the chosen mitigation strategies (Chapter 6) to overcome the effects of interference (Chapter 4): as such, it combines the three main objectives of this work.

Chapter 8

Conclusion

In this thesis, the effects, classification and mitigation of possible interference sources in the 2.4 GHz frequency band were reviewed, namely Wireless Local Area Networks (WLANs), Bluetooth and microwave ovens. The major problem motivating this thesis arises out of the congestion of the frequency spectrum, which is due to the currently rising popularity of wireless technologies. The only common solution so far is to use IEEE 802.15.4 channel 26 for Wireless Sensor Networks (WSNs). This has been proven to be unreliable and therefore, a demand arises for a detailed study of the sources of interference and the improvement of coexistence.

The effects of interference were reviewed in Chapter 4. Additionally, the modeling approach used throughout this work was explained and discussed. This approach allows for an estimation of the severity of each class of interference.

In Chapter 5, the different interference classes were described with the help of unique properties, which allow for the classification of external sources of interference. The resulting classification algorithm was implemented and extensively tested.

After detecting and classifying external interferers, countermeasures were investigated in Chapter 6 with regard to their efficiency against the different interference classes.

For each source of interference, the most efficient interference mitigation strategy was selected, which led to the implementation of Interference-Aware, Self-Adapting (IASA) Medium Access Control (MAC) in Chapter 7. IASA MAC enables the recognition and classification of occurring interference at 2.4 GHz, resulting in the application of a suitable and efficient mitigation strategy to the particular source of interference. The following chapter concludes this thesis by highlighting the contributions made. Furthermore, possible aspects are identified to extend this work and to indicate directions for future research.

8.1 Contributions

This thesis has made the following contributions:

1. With regard to its comprehensiveness, this thesis provides the first most complete study of external interference in IEEE 802.15.4-based WSNs in the commonly used 2.4 GHz frequency band.
 - It combines the higher layers programmed in software with the basics of telecommunications engineering used in the Physical (PHY) Layer in hardware. Thereby it bridges the gap of many works of the WSN research community that leave out or strongly simplify the lowest layer. Due to the additional insight into the PHY Layer, interference can be understood on a deeper level than only modeling the binary presence of interference.

- Furthermore, no other work has researched the three parts of effects, classification and mitigation of external interference in combination and such detail by looking at a number of technologies. Comparable works are either based on other technologies or have limited scopes.
2. The experiments and analyses of this thesis are beyond comparable literature of the same coverage. Due to the extensiveness and consistency of the experimental work underlying this thesis, a greater comparability of different interference classification and mitigation approaches is achieved. The soundness of experiments has been achieved through the following:
 - All controlled experiments were conducted in a Radio Frequency (RF) anechoic chamber.
 - The used victim sensor nodes have been evaluated for reasons of comparability.
 - Bluetooth was divided into two classes (single-slot and multi-slot traffic) and thereby examined in more detail than in other works.
 - Different IEEE 802.11 versions have been considered and the effects of resulting data rates and packet formats on IEEE 802.15.4 have been discussed.
 3. The possibilities of Energy Detection (ED)-based Clear Channel Assessments (CCAs) have been evaluated for interference detection and classification, but also for spectrum analyzing. An IEEE 802.15.4-compliant ED-based CCA request is sufficient to detect interference caused by microwave ovens, Bluetooth and low data rates traffic of IEEE 802.11 (as used by beacon frames sent by WLAN Access Points (APs)).
 4. A major contribution of this work lies in the development of the first ED-based interference classification algorithm that only uses a single channel and therefore allows the sensor node to stay connected to the WSN. Additionally, the algorithm offers detailed classes, a short sampling time, a high classification rate and a low complexity.
 5. This thesis evaluates interference mitigation strategies against all three external sources of interference. Channel agility is most suitable to overcome WLAN interference, while packet scheduling can be used to overcome microwave oven interference. Bluetooth only weakly interferes with IEEE 802.15.4 and therefore mitigation strategies additional to Acknowledgment (ACK)-based retransmissions are not required.
 6. IASA MAC, which combines the interference classification algorithm and the mitigation strategies, is developed and implemented in ContikiOS. The challenge of announcing the channel change in a multi-hop WSN under IEEE 802.11 interference is solved by using the established Trickle algorithm. Also the discussion of IASA MAC reaches beyond the common limited evaluation scope of two interfered victim sensor nodes of a direct link.
 7. This work has resulted in multiple publications, which are given in Appendix C in detail.

8.2 Future Work

The three parts of this thesis, interference effects, classification and mitigation, already suggest the scope and complexity of the problem of external interference in WSNs. This topic is wide-ranging, since not only the victim technology has to be analyzed and understood, but also the interfering technologies have to be examined into detail. Furthermore, the different communication standards have several versions, differences in software implementations and hardware component tolerances, which are all affecting the coexistence. The wireless channel can also vary in different ways, which

are depending on a large number of factors. Adding up to the complexity, diverse possible setups of victim and interfering devices can be differentiated: a single source of interference, multiple sources of interference either of the same or different types, varying locations and distances between devices, the use of different CCA modes, etc.

In summary, there are unlimited possibilities and therefore, an optimal solution to every possible setup of external interference cannot be found. Therefore, the topic of external interference in WSNs stays an active and interesting field of research, even after this comprehensive thesis.

The following aspects have to be taken into consideration for future work to extend this thesis. The scope of this work has been limited by the intended use in urban environments and as such, some assumptions about the interferer and the victim sensor nodes have been made. An extension of this work is possible by changing these assumptions.

- This thesis covers the three typical sources of interference in the 2.4 GHz frequency band in an urban environment. Nevertheless, further wave emitting technologies exist:
 - The problem of IEEE 802.11n using channel bonding (see Section 2.4.3) has only been mentioned and has not been further investigated in this work due to its rare appearance. However, it can become more present in the near future and then it has to be addressed.
 - The latest versions of Bluetooth (see Section 2.5), especially Bluetooth Low Energy, have not been considered in this thesis due to their seldom occurrence at the time of writing. Since Bluetooth Low Energy uses lower power than classical Bluetooth, it is assumed that Bluetooth Low Energy has no significant effect on IEEE 802.15.4. Therefore, a deeper analysis of Bluetooth Low Energy remains as an open task for future work.
 - As already mentioned in Section 2.7, the consideration of proprietary technologies could also extend this work.
- The experimental work was conducted with a Tmote Sky sensor node as a victim device. Although this node is equipped with the widely used CC2420 radio transmitter and can be seen as a representative for many sensor nodes, experiments on other sensor nodes or radios could show different results especially in the context of interference and connectivity ranges.
- New problems arise when IEEE 802.15.4 is used at a different, local frequency band.

IASA MAC is a research prototype, which can be further optimized towards the final application.

- The optimization of the thresholds and waiting periods within IASA MAC (explained in Chapter 7) could be fruitful for specific use cases.
- IASA MAC is lacking the features of an energy conserving Radio Duty Cycling (RDC) (compare to Section 2.3.2), which can be added in a future version.
- Cross-layer optimization of IASA MAC is an interesting research challenge. Especially an interference-aware routing protocol based on IASA MAC's technology could provide further interference mitigation. IASA MAC considers all links to be equal, but a more differentiated approach could be beneficial.

Besides the direct extension of this work, the findings and knowledge of this thesis can be used in different contexts.

- The interference classification algorithm can be used for WSN deployment plannings or as a low power WLAN detector, as already mentioned in Section 5.3.4.
- The knowledge of the effects of interference and the typical interference patterns can be used for WSN simulations or interference emulations for WSN development.

Appendix A

Decibel

Logarithmic units are commonly used in science and technology to give the ratio of two values of the same unit. In this work, the ratio of two different powers, P_0 and P_1 , is given in dB (e.g. signal power to noise power (Signal to Interference Ratio (SIR)) or a signal power P_1 is quantified in dBm based on the reference power P_0 of 1 mW. Further, the dB relative unit dBr is used to indicate the relative difference from a level that is apparent from the context.

The following Table A.1 gives the conversion and an example scale.

Decibel power ratio	Linear power ratio	Comment
$L_{dB} = 10 \log_{10} \frac{P_1}{P_0}$ (dB)	$L = 10 \frac{P_1}{P_0}$	
$L_{dB} = 10 \log_{10} L$	$L = 10^{\frac{L_{dB}}{10}}$	
20	100	maximum IEEE 802.11 transmission, Bluetooth class 1
17	50.119	typical IEEE 802.11 AP transmission
15	31.623	typical IEEE 802.11 laptop transmission
10	10	
9	7.943	IEEE 802.15.4 PG
8	6.310	
7	5.012	
6	3.981	$\approx 4\times$
5	3.162	$\approx 3\times$
4	2.512	Bluetooth class 2
3	1.995	$\approx 2\times$
2	1.585	
1	1.259	
0	1	typical IEEE 802.15.4 transmission, Bluetooth class 3
-1	0.794	
-2	0.631	
-3	0.501	required IEEE 802.15.4 transmission, $\approx \frac{1}{2}\times$
-4	0.398	
-5	0.316	$\approx \frac{1}{3}\times$
-6	0.251	$\approx \frac{1}{4}\times$
-7	0.200	
-8	0.158	
-9	0.126	
-10	$0.100 = 10^{-1}$	
-20	$0.010 = 10^{-2}$	
-30	$0.001 = 10^{-3}$	
-40	$0.0001 = 10^{-4}$	
-50	$0.00001 = 10^{-5}$	
-60	$0.000001 = 10^{-6}$	
-70	$0.0000001 = 10^{-7}$	
-77	0.00000019	CC2420 CCA threshold
-80	$0.00000001 = 10^{-8}$	
-85	0.000000003	IEEE 802.15.4 required sensitivity
-90	$0.000000001 = 10^{-9}$	
-94	0.0000000004	CC2420 sensitivity
-100	$0.0000000001 = 10^{-10}$	

Table A.1: Decibel to linear power ratio conversions and example scale.

Appendix B

Packet error model

The packet error model by Golmie (2006) is introduced in Section 4.2.6 on a system level. It assumes that a victim system A transmits packets under interference of a system B , where A might slowly hop channels after each transmission. Thus, it is initially used to predict the interference of IEEE 802.11b on Bluetooth. The following symbols are used:

n is the number of frequencies of A affected by B .

C is the available spectrum range (MHz) for hopping of A .

N_A is the bandwidth (MHz) of A .

T_A is the airtime (in bit durations or a finer time unit) of the transmitted packets of A .

T_B is the airtime (in bit durations or a finer time unit) of the transmitted packets of B .

T_{BI} is the time interval (in bit durations or a finer time unit) between the start of two transmissions of B .

X is the transmission start time (in bit durations or a finer time unit) of A . It is a specific $k = [0, \dots, T_{BI}]$ for the call of the computation of T_C .

T_C is the time span (in bit durations or a finer time unit), in which A and B overlap, i.e. the duration of interference.

The probability of a packet error $Pr(PE)$, which corresponds to the Packet Error Rate (PER), is then calculated based on three factors, with Bit Error Rate (BER) being dependent on the strength of interference (see Section 4.2.5 for details).

$$Pr(PE) = \underbrace{\frac{n}{(C - N_A + 1)}}_{\text{Frequency Offset Model}} \times \underbrace{\frac{1}{T_{BI}}}_{\text{Time step weight}} \times \underbrace{\sum_{k=0}^{T_{BI}} (1 - (1 - \text{BER})^{T_C})}_{\text{Sum of all PERs at time steps k}} \quad (\text{B.1})$$

While the Frequency Offset Model is the overlap in frequency, the last two factors work out the overlap of packets in time. The Time step weight normalizes the result of the Sum of all PERs. This last factor is a sum of all possible cases of time overlap, and within it the exponent T_C is most interesting, because its calculation depends on the different cases of interference. The different cases of interference are:

1. $(T_A \leq T_B)$ and $(T_A \leq (T_{BI} - T_B))$:

$$T_C = \begin{cases} T_A & \text{if } X < T_B - T_A \\ T_B - X & \text{if } T_B \leq X < T_B \\ 0 & \text{if } T_B \leq X \leq T_{BI} - T_A^1 \\ X + T_A - T_{BI} & \text{if } T_{BI} - T_A \leq X \leq T_{BI} \end{cases} \quad (\text{B.2})$$

The times used and cases described in Equation B.2 are illustrated in Figure 4.7.

2. $(T_A \leq T_B)$ and $(T_A > (T_{BI} - T_B))$:

$$T_C = \begin{cases} T_A & \text{if } X < T_B - T_A \\ T_B - X & \text{if } T_B - T_A \leq X < T_{BI} - T_A \\ T_B + T_A - T_{BI} & \text{if } T_{BI} - T_A \leq X < T_B \\ X + T_A - T_{BI} & \text{if } T_B \leq X < T_{BI} \end{cases} \quad (\text{B.3})$$

3. $(T_A > T_B)$:

$N(X)$ is the number of interfering packets that affect a desired packet:

$$N(X) = \begin{cases} \left\lceil \frac{T_A}{T_{BI}} \right\rceil & \text{if } X < T_{BI} \left\lceil \frac{T_A}{T_{BI}} \right\rceil - T_A \\ \left\lceil \frac{T_A}{T_{BI}} \right\rceil + 1 & \text{otherwise} \end{cases} \quad (\text{B.4})$$

For each interfering packet i within the transmission of the victim packet, the time collision T_i is calculated:

$$T_i = \begin{cases} \max(T_B - X, 0) & \text{if } i = 1 \\ T_B & \text{if } i = 2, \dots, N(X) - 1 \\ \min(X + T_A - (N(X) - 1) \times T_{BI}, T_B) & \text{if } i = N(X) \end{cases} \quad (\text{B.5})$$

Finally, T_C is the sum of all errors resulting from $N(X)$ collisions with interfering packets and it can be computed as:

$$T_C = \sum_{i=1}^{N(X)} T_i \quad (\text{B.6})$$

¹Original condition in (Golmie, 2006) is “if $T_B < X \leq T_{BI} - T_A$ ”, but this ignores the case $X = T_B$.

Appendix C

Publications

C.1 Journals

Zacharias, S., Newe, T., 2011. Competition at the wireless sensor network MAC layer: Low power probing interfering with X-MAC. *Journal of Physics: Conference Series* 307 (1), 012038.

Zacharias, S., Newe, T., December 2011. Robustness against interference in wireless sensor networks. *Simulation Notes Europe - Journal on Developments and Trends in Modelling and Simulation* Volume 21 Number 3-4, pp. 171–175.

C.2 Book Chapters

Zacharias, S., Newe, T., December 2010. Technologies and architectures for multimedia-support in wireless sensor networks. In: Chinh, H. D., Tan, Y. K. (Eds.), *Smart Wireless Sensor Networks*. InTech, Ch. 22, pp. 373-394.

C.3 Conferences

Zacharias, S., Newe, T., 12-14 October 2010. Architectures for wireless multimedia sensor networks. In: Intel European Research and Innovation Conference (ERIC Ireland). Intel, Leixlip.

Zacharias, S., Newe, T., May 2011. Robustness against interference in wireless sensor networks. In: ASIM-Workshop. Vol. 5. Wismar.

Zacharias, S., Newe, T., October 2011. Multimedia home monitoring system for use with wireless sensor networks. In: Intel European Research and Innovation Conference (ERIC Ireland). Intel, Leixlip.

Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., February 2012. Coexistence of different wireless sensor networks - MAC protocol interference between X-MAC and low power probing. In: 1st international Conference on Sensor Networks. Rome, Italy.

Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., June 2012. Identifying sources of interference in RSSI traces of a single IEEE 802.15.4 channel. In: The Eighth International Conference on Wireless and Mobile Communications (ICWMC). IARIA, Venice, Italy, pp. 408-414.

Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., October 2012. 2.4 GHz IEEE 802.15.4 channel interference classification algorithm running live on a sensor node. In: IEEE Sensors. IEEE, Taipei, Taiwan, pp. 1-4.

Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., November 2012. Coexistence measurements and analysis of IEEE 802.15.4 with Wi-fi and Bluetooth for vehicle networks. In: 12th International Conference on ITS Telecommunications (ITST 2012). Taipei, Taiwan, pp. 785-790.

C.4 Seminars

Zacharias, S., Newe, T., 17-18 November 2010. Architectures for wireless multimedia sensor networks. In: Globe Forum. Dublin.

Zacharias, S., Newe, T., 10th & 11th November 2011. Reliable data transfer in wireless sensor networks. In: COST Action TD1001 Meeting. SG4.2, Institut für Photonische Technologien (IPHT), Jena, Germany.

C.5 Reviewer for

Mobile Robots for CyberC 2010: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2010

The Ninth International Conference on Wireless and Mobile Communications (ICWMC), 2013

Journal of Sensor and Actuator Networks, 2013

Bibliography

- Abramson, N., 1970. The aloha system: another alternative for computer communications. In: Proceedings of the November 17-19, 1970, fall joint computer conference. ACM, pp. 281–285.
- Abramson, N., 1973. Packet switching with satellites. In: Proceedings of the June 4-8, 1973, National Computer Conference and Exposition. AFIPS '73. ACM, New York, NY, USA, pp. 695–702.
URL <http://doi.acm.org/10.1145/1499586.1499751>
- Agilent, 2004. Spectrum Analysis Basics - Application Note 150.
URL <http://www.home.agilent.com/agilent/editorial.jsp?ckey=459160&id=459160&cc=IE&lc=eng>
- Ahmad, M. R., Dutkiewicz, E., Huang, X., February 2011. A survey of low duty cycle mac protocols in wireless sensor networks. In: Foerster, A., Foerster, A. (Eds.), Emerging Communications for Wireless Sensor Networks. InTech, Ch. 5, pp. 69 – 90.
- Akkaya, K., Younis, M., 2005. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks 3 (3), 325 – 349.
URL <http://www.sciencedirect.com/science/article/B7576-4B3JKH2-3/2/0baf704778ae8cf6e3651eb9f329e4c0>
- Al-Karaki, J. N., Ul-Mustafa, R., Kamal, A. E., 2004. Data aggregation in wireless sensor networks - exact and approximate algorithms. In: IEEE Workshop on High Performance Switching and Routing (HPSR). pp. 241 – 245.
- Albawicz, J., Chen, A., Zhang, L., Nov 2001. Recursive position estimation in sensor networks. In: Network Protocols, 2001. Ninth International Conference on. pp. 35–41.
- Ansari, J., Ang, T., Mähönen, P., 2011. Wispot: fast and reliable detection of wi-fi networks using IEEE 802.15. 4 radios. In: Proceedings of the 9th ACM international symposium on Mobility management and wireless access. ACM, pp. 35–44.
- Arampatzis, T., Lygeros, J., Manesis, S., June 2005. A survey of applications of wireless sensors and wireless sensor networks. In: Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation. pp. 719–724.
- Atmel, 2007. 8-bit Microcontroller with 64K/128K/256K Bytes In-System Programmable Flash ATmega640/V ATmega1280/V ATmega1281/V ATmega2560/V ATmega2561/V Preliminary Summary. Atmel.
URL http://www.atmel.com/dyn/resources/prod_documents/2549S.pdf
- Azimi-Sadjadi, B., Sexton, D., Liu, P., Mahony, M., 2006. Interference effect on ieee 802.15. 4 performance. In: Proceedings of 3rd International Conference on Networked Sensing Systems (INNS), Chicago, IL.

- Baccour, N., Kouâa, A., Mottola, L., Zamalloa, M. A. Z., Youssef, H., Boano, C. A., Alves, M., 2011a. Radio link quality estimation in wireless sensor networks: a survey. Accepted for publication on ACM Transaction on Sensor Networks.
URL <http://www.sics.se/~luca/papers/baccour11link.pdf>
- Baccour, N., Koubâa, A., Jamâa, M. B., do Rosário, D., Youssef, H., Alves, M., Becker, L. B., 2011b. Radiale: A framework for designing and assessing link quality estimators in wireless sensor networks. *Ad Hoc Networks* 9 (7), 1165 – 1185.
URL <http://www.sciencedirect.com/science/article/pii/S1570870511000217>
- Baccour, N., Puccinelli, D., Voigt, T., Koubaa, A., Noda, C., Fotouhi, H., Alves, M., Youssef, H., Zuniga, M., Boano, C., Römer, K., 2013. External radio interference. In: *Radio Link Quality Estimation in Low-Power Wireless Networks*. SpringerBriefs in Electrical and Computer Engineering. Springer International Publishing, pp. 21–63.
URL http://dx.doi.org/10.1007/978-3-319-00774-8_2
- Backof, C., June 2012. Connections: From macro to micro [from the editor]. *Vehicular Technology Magazine, IEEE* 7 (2), 3.
- Baker, N., April-May 2005. Zigbee and bluetooth strengths and weaknesses for industrial applications. *Computing Control Engineering Journal* 16 (2), 20 –25.
- Baldus, H., Klabunde, K., Muesch, G., 2004. Reliable set-up of medical body-sensor networks. In: *Wireless Sensor Networks*. Springer, pp. 353–363.
- Barkat, M., 2005. *Signal Detection and Estimation - Second Edition*. ARTECH HOUSE, INC.
- Bensky, A., 2008. *Wireless Networking - know it all*. Newnes, Ch. 4 - Radio Propagation, pp. 181 – 199.
- Bertocco, M., Gamba, G., Sona, A., June 2007. Experimental optimization of cca thresholds in wireless sensor networks in the presence of interference. In: *Proc. of IEEE Workshop on ElectroMagnetic Compatibility (IEEE EMC)*.
- Bertocco, M., Gamba, G., Sona, A., 2008. Is csma/ca really efficient against interference in a wireless control system? an experimental answer. In: *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*. IEEE, pp. 885–892.
- Biagioni, E. S., Bridges, K. W., 2002. The application of remote sensor technology to assist the recovery of rare and endangered species. *International Journal of High Performance Computing Applications* 16, 2002.
URL <http://www2.hawaii.edu/~esb/prof/pub/ijhpc02.pdf>
- Bloessl, B., Joerer, S., Mauroner, F., Dressler, F., 2012. Low-cost interferer detection and classification using telosb sensor motes. In: *Proceedings of the 18th annual international conference on Mobile computing and networking. Mobicom '12*. ACM, New York, NY, USA, pp. 403–406.
URL <http://doi.acm.org/10.1145/2348543.2348595>
- Bluetooth SIG, accessed 10 September 2010. Sig introduces bluetooth low energy wireless technology, the next generation of bluetooth wireless technology.
URL <http://www.bluetooth.com/English/Press/Pages/PressReleasesDetail.aspx?ID=4>
- Bluetooth SIG, Inc., July 2007. *Bluetooth specification version 2.1 + edr*.

- Boano, C., He, Z., Li, Y., Voigt, T., Zúñiga, M., Willig, A., October 2009a. Controllable radio interference for experimental and testing purposes in wireless sensor networks. In: The 4th IEEE International Workshop on Practical Issues In Building Sensor Network Applications (SenseApp 2009). Zürich, Switzerland, pp. 865–872.
- Boano, C., Römer, K., Österlind, F., Voigt, T., 2011a. Demo abstract: Realistic simulation of radio interference in cooja. In: Proceedings of the European Conference on Wireless Sensor Networks (EWSN).
- Boano, C., Voigt, T., Noda, C., Römer, K., Zúñiga, M., april 2011b. Jamlab: Augmenting sensornet testbeds with realistic and controlled interference generation. In: Information Processing in Sensor Networks (IPSN), 10th International Conference on. pp. 175–186.
- Boano, C. A., Brown, J., He, Z., Roedig, U., Voigt, T., sep 2009b. Low-power radio communication in industrial outdoor deployments: The impact of weather conditions and ATEX-compliance. In: Proceedings of the 1st International Conference on Sensor Networks Applications, Experimentation and Logistics (SENSAPPEAL). pp. 159–176.
- Boano, C. A., Voigt, T., Tsiftes, N., Mottola, L., Römer, K., Zúñiga, M. A., Feb 2010. Making sensornet mac protocols robust against interference. In: 7th European Conference on Wireless Sensor Networks. Coimbra, Portugal.
- Boano, C. A., Wennerström, H., Zúñiga, M. A., Brown, J., Keppitiyagama, C., Oppermann, F. J., Roedig, U., Nordén, L.-Å., Voigt, T., Römer, K., aug 2013. Hot Packets: A systematic evaluation of the effect of temperature on low power wireless transceivers. In: Proceedings of the 5th Extreme Conference on Communication (ExtremeCom).
- Boers, N., Nikolaidis, I., Gburzynski, P., dec. 2010. Patterns in the rssi traces from an indoor urban environment. In: Computer Aided Modeling, Analysis and Design of Communication Links and Networks (CAMAD), 2010 15th IEEE International Workshop on. pp. 61–65.
- Boukerche, A., Ahmad, M. Z., Turgut, D., Turgut, B., 2009a. A taxonomy of routing protocols in sensor networks. In: Boukerche, A. (Ed.), Algorithms and Protocols for Wireless Sensor Networks. John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 129–160.
- Boukerche, A., Cheng, X., Linus, J., 2003. Energy-aware data-centric routing in microsensor networks. In: MSWIM '03: Proceedings of the 6th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems. ACM, New York, NY, USA, pp. 42–49.
- Boukerche, A., Oliveira, H. A. B. F., Nakamura, E. F., Loureiro, A. A. F., 2009b. Localization systems for wireless sensor networks. In: Boukerche, A. (Ed.), Algorithms and Protocols for Wireless Sensor Networks. John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 307–340.
- Braginsky, D., Estrin, D., 2002. Rumor routing algorithm for sensor networks. In: WSNA. pp. 22–31.
- Buettner, M., Yee, G. V., Anderson, E., Han, R., 2006. X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks. In: Proceedings of the 4th international conference on Embedded networked sensor systems. ACM, pp. 307–320.
- Buracchini, E., 2000. The software radio concept. Communications Magazine, IEEE 38 (9), 138–143.
- Burrell, J., Brooke, T., Beckwith, R., jan.-march 2004. Vineyard computing: sensor networks in agricultural production. Pervasive Computing, IEEE 3 (1), 38–45.

- Butler, Z., Corke, P., Peterson, R., Rus, D., April 2004. Virtual fences for controlling cows. In: Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE International Conference on. Vol. 5. pp. 4429–4436 Vol.5.
- C. Perkins, E. Belding-Royer, S. D., 2003. rfc3561 - ad hoc on-demand distance vector (aodv) routing. Request for Comments 3561, Internet Engineering Task Force (IETF).
URL <http://tools.ietf.org/html/rfc3561>
- Carnegie-Mellon University Pittsburgh, P. D. o. C. S. (Ed.), December 1978. Proceedings of a Workshop on Distributed Sensor Nets Held at Pittsburgh, Pennsylvania on December 7-8, 1978.
URL <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA143691>
- Chen, Y., Terzis, A., February 2010. On the mechanisms and effects of calibrating rssi measurements for 802.15.4 radios. In: Proceedings of the Seventh European Conference on Wireless Sensor Networks (EWSN). pp. 256–271.
URL <http://hinrg.cs.jhu.edu/uploads/Main/calibrate.pdf>
- Chipcon, April 2002. CC1000 Single Chip Very Low Power RF Transceiver. Datasheet.
- Chipcon, June 2004. CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver. Chipcon, datasheet.
- Chong, C.-Y., Kumar, S. P., 2003. Sensor networks: evolution, opportunities, and challenges. In: Proceedings of the IEEE. pp. 1247–1256.
- Chowdhury, K., Akyildiz, I., June 2009. Interferer classification, channel selection and transmission adaptation for wireless sensor networks. In: Communications, 2009. ICC '09. IEEE International Conference on. pp. 1–5.
- Chun, N., B., Buonadonna, P., AuYoung, A., Ng, C., Parkes, D. C., Shneidman, J., Snoeren, A. C., Vahdat, A., 2005. Mirage: A microeconomic resource allocation system for sensornet testbeds. In: The Second IEEE Workshop on Embedded Networked Sensors: IEEE EmNetS-II.
- Combs, G., 2013. Wireshark - network protocol analyzer. Version 1.10.0.
URL <http://www.wireshark.org>
- Cormio, C., Chowdhury, K. R., 2009. A survey on mac protocols for cognitive radio networks. Ad Hoc Networks 7 (7), 1315–1329.
- Correll, J. T., November 2004. Igloo white. Airforce Magazine 87, 56–61.
URL <http://www.airforce-magazine.com/MagazineArchive/Pages/2004/November2004/1104igloo.aspx>
- crossbow technology, inc, 2003. MICA2 Wireless Measurement System.
- Dainotti, A., Botta, A., Pescap, A., 2012. A tool for the generation of realistic network workload for emerging networking scenarios. Computer Networks 56 (15), 3531–3547.
- De, S., Qiao, C., Wu, H., 2003. Meshed multipath routing with selective forwarding: an efficient strategy in wireless sensor networks. Computer Networks 43 (4), 481 – 497, wireless Sensor Networks.
URL <http://www.sciencedirect.com/science/article/B6VRG-4991M83-4/2/a457e3af7e3530ea8db43481817ac08d>

- Deb, B., Bhatnagar, S., Nath, B., 2003. Reinform: Reliable information forwarding using multiple paths in sensor networks. In: LCN. pp. 406–415.
URL <http://www.research.rutgers.edu/~bdeb/ReInForm.pdf>
- Demirkol, I., Ersoy, C., Alagoz, F., April 2006. Mac protocols for wireless sensor networks: a survey. *Communications Magazine, IEEE* 44 (4), 115 – 121.
- Dishongh, T. J., McGrath, M., 2010. *Wireless Sensor Networks for Healthcare Applications*. Artech House.
- Duda, A., 2008. Understanding the performance of 802.11 networks. In: *Proceedings of PIMRC*. Vol. 8.
- Dunkels, A., Grönvall, B., Voigt, T., 2004. Contiki - a lightweight and flexible operating system for tiny networked sensors. In: *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, pp. 455–462.
- Dunkels, A., Österlind, F., Eriksson, J., Boano, C. A., accessed: February 2012. Contiki projects: Frossi scanner. <http://contikiprojects.svn.sourceforge.net/viewvc/contikiprojects/sics.se/frossi-scanner/>.
- Dunkels, A., Österlind, F., He, Z., November 2007. An adaptive communication architecture for wireless sensor networks. In: *Proceedings of the Fifth ACM Conference on Networked Embedded Sensor Systems (SenSys 2007)*. Sydney, Australia.
URL <http://www.sics.se/~adam/dunkels07adaptive.pdf>
- Dunkels, A., Schmidt, O., Voigt, T., Ali, M., 2006. Protothreads: simplifying event-driven programming of memory-constrained embedded systems. In: *Proceedings of the 4th international conference on Embedded networked sensor systems*. ACM, pp. 29–42.
- Durgin, G., Rappaport, T., De Wolf, D. A., 2002. New analytical models and probability density functions for fading in wireless communications. *Communications, IEEE Transactions on* 50 (6), 1005–1015.
URL http://www.propagation.gatech.edu/Archive/PG_WA_040906_GDD/RParchive/TransCom02.pdf
- Dutra, D. A., accessed: July 2013. Tinyos tutorials: Rssi demo. <https://github.com/tinyos/tinyos-main/tree/master/apps/tutorials/RssiDemo>.
- Eriksson, J., accessed: July 2013. Contiki example: Rssi scanner. <https://github.com/contiki-os/contiki/blob/master/examples/sky/rssi-scanner.c>.
- ETSI, 2005. Digital enhanced cordless telecommunications (dect); a high level guide to the dect standardization - high level guide. Tech. Rep. TR 101 178, ETSI.
URL http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=19280http://www.etsi.org/deliver/etsi_tr/101100_101199/101178/01.05.01_60/tr_101178v010501p.pdf
- Farahani, S., 2008. *ZigBee Wireless Networks and Transceivers*. Newnes.
- Felemban, E., Lee, C.-G., Ekici, E., June 2006. Mmspeed: multipath multi-speed protocol for qos guarantee of reliability and timeliness in wireless sensor networks. *Mobile Computing, IEEE Transactions on* 5 (6), 738 – 754.

- Flowers, D., Yang, Y., November 2010. Microchip MiWi Wireless Networking Protocol Stack - AN1066. Microchip Technology Inc.
URL http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1824&appnote=en520606
- Fontán, F., Espiñeira, P., 2008. Modeling the Wireless Propagation Channel - A simulation Approach with MATLAB ®. Wiley Series on Wireless Communications and Mobile Computing. Wiley, ISBN: 978-0-470-72785-0.
- Ganesan, D., Govindan, R., Shenker, S., Estrin, D., 2001. Highly-resilient, energy-efficient multipath routing in wireless networks. *Mobile Computing and Communications Review* 1 (2), 10 – 24.
- Gast, M., August 2003. When is 54 not equal to 54? a look at 802.11a, b, and g throughput. Accessed 18 November 2013.
URL http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html
- Gawthrop, P., Sanders, F., Nebbia, K., Sell, J., March 1994. Radio spectrum measurements of individual microwave ovens (volume 1). Tech. rep., NTIA Report 94-303-1.
- Gay, D., Levis, P., von Behren, R., Welsh, M., Brewer, E., Culler, D., June 2003. The nesc language: A holistic approach to networked embedded systems. In: *Proceedings of Programming Language Design and Implementation (PLDI) 2003*.
URL <http://nesc.sourceforge.net/papers/nesc-pldi-2003.pdf>
- Gilbert, E. N., 1960. Capacity of a burst-noise channel. *Bell Syst. Tech. J* 39 (9), 1253–1265.
- Gnawali, O., Fonseca, R., Jamieson, K., Moss, D., Levis, P., 2009. Collection tree protocol. In: *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems. SenSys '09*. ACM, New York, NY, USA, pp. 1–14.
URL <http://doi.acm.org/10.1145/1644038.1644040>
- GNU Radio Members, last accessed August 2013. Gnu radio.
URL <http://gnuradio.org/>
- Golmie, N., 2006. *Coexistence in Wireless Networks*. Cambridge University Press, ISBN 0-521-85768-6.
- Golmie, N., Chevrollier, N., Rebala, O., December 2003. Bluetooth and wlan coexistence: challenges and solutions. *Wireless Communications, IEEE* 10 (6), 22–29.
- Golmie, N., Cypher, D., Rebala, O., 2005. Performance analysis of low rate wireless technologies for medical applications. *Computer Communications* 28 (10), 1266 – 1275.
URL <http://www.sciencedirect.com/science/article/pii/S0140366404002828>
- Gomez, C., Paradells, J., 2010. Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine* 48 (6), 92–101.
- Grini, D., 2006. Rf basics, rf for non-rf engineers. In: *MSP430 Advanced Technical Conference*.
URL <http://www.ti.com/lit/ml/slap127/slap127.pdf>
- Gummadi, R., Wetherall, D., Greenstein, B., Seshan, S., August 2007. Understanding and mitigating the impact of rf interference on 802.11 networks. *SIGCOMM Comput. Commun. Rev.* 37 (4), 385–396.
URL <http://doi.acm.org/10.1145/1282427.1282424>

- Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G., Nov 2011. Smart grid technologies: Communication technologies and standards. *Industrial Informatics, IEEE Transactions on* 7 (4), 529–539.
- Gutiérrez, J., Callaway, E., Barrett, R., 2004. *Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4*. IEEE Standards Wireless Networks Series. Standards Information Network, IEEE Press.
- Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., Witten, I. H., 2009. The weka data mining software: An update. *SIGKDD Explorations* 11 (1).
- Hart, B., November 2013. *Renewing 2.4 ghz*. Tech. rep., IEEE.
- HART Communication Foundation, last accessed April 2014. Hart communication protocol - wireless hart technology.
URL http://www.hartcomm.org/protocol/wihart/wireless_technology.html
- He, T., Krishnamurthy, S., Stankovic, J. A., Abdelzaher, T., Luo, L., Stoleru, R., Yan, T., Gu, L., Hui, J., Krogh, B., 2004. Energy-efficient surveillance system using wireless sensor networks. In: *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*. ACM, New York, NY, USA, pp. 270–283.
URL <http://www.cs.virginia.edu/papers/tracking-mobisys04.pdf>
- He, T., Stankovic, J., Lu, C., Abdelzaher, T., May 2003. Speed: a stateless protocol for real-time communication in sensor networks. In: *Proceedings. 23rd International Conference on Distributed Computing Systems, 2003*. pp. 46 – 55.
URL <http://www.cs.virginia.edu/papers/speed-stateless-protocol.pdf>
- Heile, C. B., last accessed July 2013. Eee 802.15 working group for wpan.
URL <http://www.ieee802.org/15/>
- Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H., 2000. Energy-efficient communication protocol for wireless microsensor networks. In: *Hawaii International Conference on System Sciences*. pp. 3005 – 3014.
- Heinzelman, W. R., Kulik, J., Balakrishnan, H., August 1999. Adaptive protocols for information dissemination in wireless sensor networks. In: *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99)*. Seattle, pp. 174 – 185.
- Hermans, F., Rensfelt, O., Larzon, L., Gunningberg, P., 2012. A lightweight approach to online detection and classification of interference in 802.15.4-based sensor networks. In: *ACM SIGBED Review, Special Issue on the Third International Workshop on Networks of Cooperating Objects*. Vol. 9.
- Hermans, F., Rensfelt, O., Voigt, T., Ngai, E., Norden, L.-A., Gunningberg, P., 2013. SoNIC: classifying interference in 802.15.4 sensor networks. In: *Proceedings of the 12th international conference on Information processing in sensor networks*. IPSN '13. ACM, New York, NY, USA, pp. 55–66.
URL <http://doi.acm.org/10.1145/2461381.2461392>
- Herrera, M., Bonastre, A., Capella, J., 2008. Performance study of non-beaconed and beacon-enabled modes in ieee 802.15.4 under bluetooth interference. In: *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBIComm '08. The Second International Conference on*. pp. 144–149.

- Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K., November 2000. System architecture directions for networked sensors. *SIGPLAN Not.* 35 (11), 93–104.
URL <http://doi.acm.org/10.1145/356989.356998>
- Holland, M., Aures, R., Heinzelman, W., 2006. Experimental investigation of radio performance in wireless sensor networks. In: *Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on.* IEEE, pp. 140–150.
- Hornig, C., 1984. rfc894 - a standard for the transmission of ip datagrams over ethernet networks. Request for Comments 894, Network Working Group.
URL <http://tools.ietf.org/html/rfc894>
- Howitt, I., Gutierrez, J., March 2003. IEEE 802.15.4 low rate - wireless personal area network coexistence issues. In: *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE.* Vol. 3. pp. 1481–1486 vol.3.
- Huang, J., Xing, G., Zhou, G., Zhou, R., October 2010. Beyond co-existence: Exploiting wifi white space for zigbee performance assurance. In: *Network Protocols (ICNP), 2010 18th IEEE International Conference on.* pp. 305–314.
- Hui, J., Levis, P., Moss, D., 2007. Tep 125 - tinys 802.15.4 frames.
URL <http://www.tinyos.net/tinyos-2.x/doc/html/tep125.html>
- Hui, J. W., Culler, D. E., 2008. Ip is dead, long live ip for wireless sensor networks. In: *SenSys '08: Proceedings of the 6th ACM conference on Embedded network sensor systems.* ACM, New York, NY, USA, pp. 15–28.
URL <http://www.cs.berkeley.edu/~jwhui/pubs/jhui-sensys08-ipv6.pdf>
- Hunn, N., 2006. An introduction to wibree. White paper, Ezurio Ltd.
URL <http://www.tdksys.com/files/00616.pdf>
- Huo, H.-W., Xu, Y.-Z., Mikael, G., Zhang, H.-K., 2010. Coexistence of 2.4 ghz sensor networks in home environment. *The Journal of China Universities of Posts and Telecommunications* 17 (1), 9–18.
URL <http://www.sciencedirect.com/science/article/pii/S1005888509604180>
- IEEE, 2003a. IEEE std 802.15.2-2003.
URL <http://standards.ieee.org/getieee802/download/802.15.2-2003.pdf>
- IEEE, 2003b. IEEE std 802.15.4-2003.
URL <http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>
- IEEE, 2005a. IEEE standard for information technology–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 8: Medium access control (mac) quality of service enhancements. IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)), 1–212.
- IEEE, 2005b. IEEE std 802.15.1-2005.
URL <http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf>
- IEEE, 2006. IEEE std 802.15.4-2006.
URL <http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>
- IEEE, 2007. IEEE std 802.11-2007.
URL <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

- IEEE, 2009. IEEE std 802.11n-2009.
- IEEE, 2011a. Ieee standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 10: Mesh networking. IEEE Std 802.11s-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, IEEE 802.11w-2009, IEEE 802.11n-2009, IEEE 802.11p-2010, IEEE 802.11z-2010, IEEE 802.11v-2011, and IEEE 802.11u-2011), 1–372.
- IEEE, 2011b. IEEE std 802.15.4-2011.
URL <http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf>
- IEEE, 2012a. Ieee standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 1: Mac sublayer. IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), 1–225.
- IEEE, 2012b. IEEE std 802.11-2012.
URL <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
- IEEE 802.15 Working Group, September 2010. Coexistence analysis of ieee std 802.15.4 with other ieee standarads and proposed standards. Tech. Rep. 0808-00, IEEE.
- IEEE 802.19 Wireless Coexistence Working Group, accessed 20th June 2013. Coexistence assurance (ca) documents.
URL <http://grouper.ieee.org/groups/802/19/pub/ca.html>
- Information Sciences Institute, 1981. rfc 791 - internet protocol, darpa internet program protocol specification. Request for Comments 791, Network Working Group.
URL <http://tools.ietf.org/html/rfc791>
- Intanagonwiwat, C., Govindan, R., Estrin., D., 2000. Directed diffusion: A scalable and robust communication paradigm for sensor networks. In: MOBICOM., pp. 56 – 57.
- ISA, 2008. The isa100 standards - overview & status. Tech. rep.
URL http://www.isa.org/source/ISA100_Overview_Oct_2008.pdf
- ISA 100 Wireless Compliance Institute, last accessed April 2014. Isa-100 wireless compliance institute.
URL <http://www.isa100wci.org/>
- Jennic, February 2008. Co-existence of IEEE 802.15.4 at 2.4 ghz. Application Note Revision 1.0, Technology for a changing world.
URL http://www.jennic.com/files/support_files/JN-AN-1079%20Coexistence%20of%20IEEE%20802.15.4%20In%20The%202.4GHz%20Band-1v0.pdf
- Johnston, G., Cobb, J., Rotvold, E., Singhal, R., March 2010. Co-existence of wirelesshart with other wireless technologies. Tech. rep., HART Communication Foundation.
- Joseph, W., Pareit, D., Vermeeren, G., Naudts, D., Verloock, L., Martens, L., Moerman, I., 2013. Determination of the duty cycle of wlan for realistic radio frequency electromagnetic field exposure assessment. Progress in Biophysics and Molecular Biology 111 (1), 30 – 36.
URL <http://www.sciencedirect.com/science/article/pii/S0079610712001083>

- Juang, P., Oki, H., Wang, Y., Martonosi, M., Peh, L. S., Rubenstein, D., 2002. Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebrantet. In: ACM Sigplan Notices. Vol. 37. ACM, pp. 96–107.
- Kamerman, A., Erkocevic, N., sep 1997. Microwave oven interference on wireless lans operating in the 2.4 ghz ism band. In: Personal, Indoor and Mobile Radio Communications, 1997. 'Waves of the Year 2000'. PIMRC '97., The 8th IEEE International Symposium on. Vol. 3. pp. 1221–1227 vol.3.
- Kappler, C., Riegel, G., 2004. A real-world, simple wireless sensor network for monitoring electrical energy consumption. In: Karl, H., Wolisz, A., Willig, A. (Eds.), Wireless Sensor Networks. Vol. 2920 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 339–352.
URL http://dx.doi.org/10.1007/978-3-540-24606-0_23
- Karn, P., 1990. Maca-a new channel access method for packet radio. In: ARRL/CRRL Amateur radio 9th computer networking conference. Vol. 140. pp. 134–140.
- Khaleel, H., Pastrone, C., Penna, F., Spirito, M., Garello, R., 2009. Impact of wi-fi traffic on the IEEE 802.15.4 channels occupation in indoor environments. In: Electromagnetics in Advanced Applications, 2009. ICEAA'09. International Conference on. IEEE, pp. 1042–1045.
- Kleinrock, L., Tobagi, F. A., Dec 1975. Packet switching in radio channels: Part i-carrier sense multiple-access modes and their throughput-delay characteristics. Communications, IEEE Transactions on 23 (12), 1400–1416.
- Knot, T., April 2004. Smart surrogates. BP Frontiers Magazine 9, 6–10.
URL http://www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/images/fr/downloads/Frontiers_magazine_issue_09_smart_surrogates.pdf
- Krasnyansky, M., Holtmann, M., November 2002. hcidump - parse hci data.
- Kredo II, K., Mohapatra, P., 2007. Medium access control in wireless sensor networks. Computer Networks 51 (4), 961–994.
- Kumar, A., Manjunath, D., Kuri, J., 2008. Wireless Networking. The Morgan Kaufmann Series in Networking. Morgan Kaufmann, ISBN: 978-0-12-374254-4.
- Kumar, S., Shepherd, D., 2001. Sensit: Sensor information technology for the warfighter. In: Proc. 4th Int. Conf. on Information Fusion.
- Kurose, J. F., Ross, K. W., 2001. Computer Networking: A Top-Down Approach Featuring the Internet, 1st Edition. Addison Wesley.
- Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., Wolff, S. S., 1997. The past and future history of the internet. Communications of the ACM 40 (2), 102–108.
- Levis, P., 2007. Tep 116 - packet protocols.
URL <http://www.tinyos.net/tinyos-2.x/doc/html/tep116.html>
- Levis, P., Culler, D., 2002. Maté: A tiny virtual machine for sensor networks. In: ACM Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS). Vol. 37. ACM, pp. 85–95.
- Levis, P., Hui, J., Gnawali, O., Ko, J., 2011. rfc6206 - the trickle algorithm. Request for Comments 6206, Internet Engineering Task Force (IETF).
URL <http://tools.ietf.org/html/rfc6206>

- Levis, P., Patel, N., Culler, D., Shenker, S., 2004. Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks.
URL <http://www.cs.berkeley.edu/~pal/pubs/trickle-nsdi04.pdf>
- Li, A., Dong, C., Tang, X., Wang, H., Yu, W., April 2012. Identifying and analyzing wireless network protocols without demodulation. In: Wireless Communications and Networking Conference (WCNC), 2012 IEEE. pp. 2462–2467.
- Li, D., Wong, K. D., Hu, Y. H., Sayeed, A. M., March 2002. Detection, classification and tracking of targets in distributed sensor networks. IEEE Signal Processing Magazine 19, 17–29.
URL <https://eprints.kfupm.edu.sa/34714/1/34714.pdf>
- Liang, C.-J. M., Priyantha, N. B., Liu, J., Terzis, A., 2010. Surviving wi-fi interference in low power zigbee networks. In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems. SenSys '10. ACM, New York, NY, USA, pp. 309–322.
URL <http://doi.acm.org/10.1145/1869983.1870014>
- Lindsey, S., Raghavendra, C. S., 2002. Pegasus: Power-efficient gathering in sensor information. In: IEEE Aerospace Conference. pp. 1125 – 1130.
- Linnartz, J.-P. M., accessed December, 2013. Rayleigh fading. JPL's Wireless Communication Reference Website.
URL <http://www.wirelesscommunication.nl/reference/chaptr03/rayleigh.htm>
- Liu, C., Li, F., October 2004. Spectrum modelling of ofdm signals for wlan. Electronics Letters 40 (22), 1431 – 1432.
- Liu, K. J. R., Sadek, A. K., Su, W., Kwasinski, A., January 2009. Cooperative Communications and Networking. Cambridge University Press.
URL <http://www.cambridge.org/us/academic/subjects/engineering/wireless-communications/cooperative-communications-and-networking>
- Lymberopoulos, D., Lindsey, Q., Savvides, A., 2006. An empirical characterization of radio signal strength variability in 3-d IEEE 802.15.4 networks using monopole antennas. In: Römer, K., Karl, H., Mattern, F. (Eds.), Wireless Sensor Networks. Vol. 3868 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 326–341, 10.1007/11669463_24.
URL http://dx.doi.org/10.1007/11669463_24
- Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., Anderson, J., 2002. Wireless sensor networks for habitat monitoring. In: WSN'02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. ACM, New York, NY, USA, pp. 88–97.
URL <http://www.polastre.com/papers/wsna02.pdf>
- Manjeshwar, A., Agrawal, D. P., 2001. Teen: A routing protocol for enhanced efficiency in wireless sensor networks. In: IPDPS. pp. 2009 – 2015.
- Marquess, K., November 1999. Physical model sub-group discussion and questions. Tech. rep., IEEE.
URL http://grouper.ieee.org/groups/802/15/pub/1999/Nov99/99138r0P802-15_Coexistence-Study-Group-Physical-Model-Team-Report.ppt
- Martinez, K., Ong, R., Hart, J., 2004. Glacsweb: a sensor network for hostile environments. In: Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on. IEEE, pp. 81–87.

- MATLAB, 2009. version 7.9.0.529 (R2009b). The MathWorks Inc., Natick, Massachusetts.
- Matolak, D., Frolik, J., 2011. Worse-than-rayleigh fading: Experimental results and theoretical models. *Communications Magazine*, IEEE 49 (4), 140–146.
- Meesookho, C., Narayanan, S., Raghavendra, C., 2002. Collaborative classification applications in sensor networks. In: *Proc. of Second IEEE Multichannel and Sensor array signal processing workshop*. Arlington, VA.
URL http://sail.usc.edu/publications/Sam2002_paper.pdf
- MEMSIC Inc., 2010a. Iris Wireless Measurement System. Formerly Crossbow.
- MEMSIC Inc., 2010b. TelosB Mote Platform Datasheet. Formerly Crossbow.
- MEMSIC Inc., 2011. MICAz Wireless Measurement System. Formerly Crossbow.
- Merrill, W., Newberg, F., Sohrabi, K., Kaiser, W., Pottie, G., March 2003. Collaborative networking requirements for unattended ground sensor systems. In: *Aerospace Conference, 2003. Proceedings. 2003 IEEE*. Vol. 5. pp. 2153–2165.
- metageek, 2011. wi-spy 2.4x - 2.4 GHz Spectrum Analysis. Data sheet.
URL http://files.metageek.net/marketing/Wi-Spy_2.4x/MetaGeek_Wi-Spy_24x_datasheet.pdf
- Michahelles, F., Matter, P., Schmidt, A., Schiele, B., 2003. Applying wearable sensors to avalanche rescue. *Computers & Graphics* 27 (6), 839 – 847.
URL <http://www.sciencedirect.com/science/article/pii/S0097849303001638>
- Microchip Inc., last accessed July 2013. Miwi protocol.
URL <http://www.microchip.com/pagehandler/en-us/technology/personalareanetworks/technology/home.html>
- Microsoft, 2010. Network monitor. Version 3.4.
URL <http://www.microsoft.com/en-ie/download/details.aspx?id=4865>
- Mittag, J., August 2012. Characterization, avoidance and repair of packet collisions in inter-vehicle communication networks. Ph.D. thesis, Institut fr Telematik (TM), Steinbuch Centre for Computing (SCC) (SCC), Karlsruher Institut fr Technologie.
URL <http://digbib.ubka.uni-karlsruhe.de/volltexte/1000028815>
- Mohapatra, P., Gui, C., Li, J., Feb 2004. Group communications in mobile ad hoc networks. *Computer* 37 (2), 52–59.
- Montenegro, G., Kushalnagar, N., Hui, J., Culler, D., 2007. rfc4944 - transmission of ipv6 packets over ieee 802.15.4 networks. Request for Comments 4944, Network Working Group.
URL <http://tools.ietf.org/html/rfc4944>
- Moss, D., Hui, J., Klues, K., last accessed April 2014. Tep 105 -low power listening.
URL <http://www.tinyos.net/tinyos-2.x/doc/html/tep105.html>
- Moteiv Corporation, 2006. Tmote Sky - Ultra low power IEEE 802.15.4 compliant wireless sensor module.
- Musaloiu-E., R., Liang, C.-J. M., Terzis, A., 2008. Koala: Ultra-low power data retrieval in wireless sensor networks. In: *Proceedings of the 7th international conference on Information processing in sensor networks*. IPSN '08. IEEE Computer Society, Washington, DC, USA, pp. 421–432.
URL <http://dx.doi.org/10.1109/IPSN.2008.10>

- Nicolas, C., Marot, M., June 2012. Dynamic link adaptation based on coexistence-fingerprint detection for wsn. In: Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean. pp. 90–97.
- Niculescu, D., Nath, B., 2001. Ad hoc positioning system (aps). In: Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE. Vol. 5. pp. 2926–2931 vol.5.
- Penna, F., Pastrone, C., Spirito, M., Garello, R., April 2009. Measurement-based analysis of spectrum sensing in adaptive wsns under wi-fi and bluetooth interference. In: Vehicular Technology Conference, 2009. IEEE 69th. pp. 1–5.
- Perahia, E., 2008. Ieee 802.11n development: History, process, and technology. Communications Magazine, IEEE 46 (7), 48–55.
- Perkins, C. E., Royer, E. M., 1999. Ad-hoc on-demand distance vector routing. In: Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, pp. 90–100.
- Petrova, M., Riihijarvi, J., Mahonen, P., Labella, S., april 2006. Performance study of IEEE 802.15.4 using measurements and simulations. In: Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE. Vol. 1. pp. 487–492.
- Petrova, M., Wu, L., Mahonen, P., Riihijarvi, J., 2007. Interference measurements on performance degradation between colocated ieee 802.11 g/n and ieee 802.15. 4 networks. In: Networking, 2007. ICN'07. Sixth International Conference on. IEEE, pp. 93–93.
- Polastre, J., Szewczyk, R., Culler, D., April 2005. Telos: enabling ultra-low power wireless research. In: Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on. pp. 364 – 369.
- Priyantha, N. B., Chakraborty, A., Balakrishnan, H., 2000. The cricket location-support system. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. MobiCom '00. ACM, New York, NY, USA, pp. 32–43.
URL <http://doi.acm.org/10.1145/345910.345917>
- Raad, M. W., Yang, L. T., 2009. A ubiquitous smart home for elderly. Inf Syst Front 11, 529 – 536.
- Rabaey, J., Ammer, M., da Silva, J.L., J., Patel, D., Roundy, S., Jul 2000. Picoradio supports ad hoc ultra-low power wireless networking. Computer 33 (7), 42–48.
- Ramachandran, I., Roy, S., June 2007. Clear channel assessment in energy-constrained wideband wireless networks. Wireless Communications, IEEE 14 (3), 70–78.
- Rao, A., Ratnasamy, S., Papadimitriou, C., Shenker, S., Stoica, I., 2003. Geographic routing without location information. In: ACM MOBICOM.
- Rappaport, T. S., 1996. Wireless Communication - Principles And Practice. Prentice Hall communications engineering and emerging technologies series. Prentice Hall.
- Rashid, R., Julin, D., Orr, D., Sanzi, R., Baron, R., Forin, A., Golub, D., Jones, M., Feb 1989. Mach: a system software kernel. In: COMPCON Spring '89. Thirty-Fourth IEEE Computer Society International Conference: Intellectual Leverage, Digest of Papers. pp. 176–178.
- Rayanchu, S., Patro, A., Banerjee, S., November 2011. Airshark: Detecting non-wifi rf devices using commodity wifi hardware. In: Internet Measurement Conference (IMC). Berlin, Germany.
URL <http://pages.cs.wisc.edu/~suman/pubs/airshark.pdf>

- Rensfelt, O., Hermans, F., Voigt, T., Ngai, E., Nordén, L.-Å., Gunningberg, P., Aug 2012. SoNIC: Classifying and surviving interference in 802.15.4-based sensor networks. Tech. Rep. 2012-022, Department of Information Technology, Uppsala University.
- Rice, S. O., July 1944. Mathematical analysis of random noise. *Bell Systems Tech. J.*, Volume 23, p. 282-332.
- Rice, S. O., January 1945. Mathematical analysis of random noise-conclusion. *Bell Systems Tech. J.*, Volume 24, p. 46-156.
- Richasse, N., accessed January, 2013. Jperf 2.0.2, graphical frontend for iperf written in java. URL <http://code.google.com/p/xjperf/>
- Riem-Vis, R., 2004. Cold chain management using an ultra low power wireless sensor network. WAMES 2004.
- Rodrig, M., Reis, C., Mahajan, R., Wetherall, D., Zahorjan, J., 2005. Measurement-based characterization of 802.11 in a hotspot setting. In: *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis. E-WIND '05.* ACM, New York, NY, USA, pp. 5–10. URL <http://doi.acm.org/10.1145/1080148.1080150>
- Römer, K., Mattern, F., dec. 2004. The design space of wireless sensor networks. *Wireless Communications, IEEE* 11 (6), 54 – 61. URL <http://www.vs.inf.ethz.ch/publ/papers/wsn-designspace.pdf>
- Roy, A., Sarma, N., 2010. Energy saving in mac layer of wireless sensor networks: a survey. In: *National Workshop in Design and Analysis of Algorithm (NWDAA).* Tezpur University, India. URL <http://alakroy.ueuo.com/mac/alakmac.pdf>
- Schmidt, F., Ceriotti, M., Wehrle, K., 2013. Bit error distribution and mutation patterns of corrupted packets in low-power wireless networks. In: *Proceedings of the 8th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization. WiNTECH '13.* ACM, New York, NY, USA, pp. 49–56. URL <http://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-schmidt-wintech-errors.pdf>
- Schmitt, H., Butz, J., January 2011. RSI03: Generation and Analysis of ZigBee™ IEEE 802.15.4 signals in the 2.4 GHz band. Rohde & Schwarz. URL http://www.rohde-schwarz.de/de/service_support/downloads/application_notes/?query=RSI03
- Seada, K., Zúñiga, M., Helmy, A., Krishnamachari, B., 2004. Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In: *SenSys.* pp. 108–121.
- Shin, S. Y., Park, H. S., Kwon, W. H., 2007. Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b. *Computer Networks* 51 (12), 3338 – 3353. URL <http://www.sciencedirect.com/science/article/pii/S1389128607000473>
- Shuaib, K., Boulmalf, M., Sallabi, F., Lakas, A., April 2006. Co-existence of zigbee and wlan, a performance study. In: *Wireless Telecommunications Symposium, 2006. WTS '06.* pp. 1–6.
- Sichitiu, M., Ramadurai, V., Oct 2004. Localization of wireless sensor networks with a mobile beacon. In: *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on.* pp. 174–183.

- Sidhu, B., Singh, H., Chhabra, A., 2007. Emerging wireless standards - wifi, zigbee and wimax. In: World Academy of Science, Engineering and Technology. Vol. 25. pp. 308 – 313.
URL <http://www.waset.ac.nz/journals/waset/v25/v25-58.pdf>
- Sikora, A., September 2004. Compatibility of IEEE802.15.4 (zigbee) with IEEE802.11 (wlan), bluetooth, and microwave ovens in 2.4 ghz ism-band. Test report, Steinbeis Transfer Centre for Embedded Design and Networking University of Cooperative Education Loerrach.
URL <http://www.ba-loerrach.de/stzedn>
- Sikora, A., Groza, V., may 2005. Coexistence of IEEE802.15.4 with other systems in the 2.4 ghz-ism-band. In: Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE. Vol. 3. pp. 1786 –1791.
- Simek, M., Fuchs, M., Mraz, L., Moravek, P., Botta, M., 2011. Measurement of lowpan network coexistence with home microwave appliances in laboratory and home environments. In: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on. pp. 292–299.
- Simon, G., Maróti, M., Lédeczi, A., Balogh, G., Kusy, B., Nádas, A., Pap, G., Sallai, J., Frampton, K., 2004. Sensor network-based countersniper system. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. SenSys '04. ACM, New York, NY, USA, pp. 1–12.
URL <http://doi.acm.org/10.1145/1031495.1031497>
- Sohraby, K., Minoli, D., Znati, T., 2007. Wireless Sensor Networks - Technology, Protocols, and Applications.
- Soltanian, A., Dyck, R. E. V., 2001. Physical layer performance for coexistence of bluetooth and IEEE 802.11b. In: Virginia Tech. Symposium on Wireless Personal Communications.
- Sproull, R., Cohen, D., Nov 1978. High-level protocols. Proceedings of the IEEE 66 (11), 1371–1386.
- Srinivasan, K., Kazandjieva, M. A., Agarwal, S., Levis, P., 2008. The β -factor: measuring wireless link burstiness. In: Proceedings of the 6th ACM conference on Embedded network sensor systems. SenSys '08. ACM, New York, NY, USA, pp. 29–42.
URL <http://doi.acm.org/10.1145/1460412.1460416>
- Srinivasan, K., Levis, P., 2006. Rssi is under appreciated. In: In Proceedings of the Third Workshop on Embedded Networked Sensors (EmNets).
- Srivastava, M., Muntz, R., Potkonjak, M., 2001. Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving environments. In: MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking. ACM, New York, NY, USA, pp. 132–138.
- Stephens, A. P., last accessed November 2013. Quick guide to ieee 802.11 activities.
URL http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm
- Suarez, P., Renmarker, C.-G., Dunkels, A., Voigt, T., 2008. Increasing zigbee network lifetime with x-mac. In: Proceedings of the workshop on Real-world wireless sensor networks. REALWSN '08. ACM, New York, NY, USA, pp. 26–30.
URL <http://doi.acm.org/10.1145/1435473.1435481>
- Subramanian, S., Shakkottai, S., 2005. Geographic routing with limited information in sensor networks. In: IPSN. pp. 269 – 276.

- Sun Labs, May 2007. Sun Small Programmable Object Technology (Sun SPOT) Theory of Operation. Sun Labs.
- Tan, W. L., Hu, P., Portmann, M., 2012. Experimental evaluation of measurement-based sinr interference models. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a. IEEE, pp. 1–9.
- Tanenbaum, A. S., Wetherall, D. J., 2011. Computer Networks, fifth edition Edition. Prentice Hall, Pearson Education, Inc.
- Texas Instruments, 2010. MSP430 Ultra-Low-Power Microcontrollers Product Brochure. Texas Instruments.
URL <http://focus.ti.com/lit/sg/slab034r/slab034r.pdf>
- Thonet, G., Allard-Jacquins, P., Colle, P., April 2008. Zigbee - wifi coexistence (white paper and test report). Tech. rep., Schneider Electric Innovation Department, 37 Quai Paul Louis Merlin 38000 Grenoble, France.
URL <https://docs.zigbee.org/zigbee-docs/dcn/08-4846.pdf>
- Tobagi, F. A., Kleinrock, L., Dec 1975. Packet switching in radio channels: Part ii—the hidden terminal problem in carrier sense multiple-access and the busy-tone solution. Communications, IEEE Transactions on 23 (12), 1417–1433.
- Tytgat, L., Yaron, O., Pollin, S., Moerman, I., Demeester, P., 2012. Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment. EURASIP Journal on Wireless Communications and Networking, 137.
- Vanheel, F., Verhaevert, J., Moerman, I., October 2008. Study on distance of interference sources on wireless sensor network. In: Microwave Conference, 2008. EuMC 2008. 38th European. pp. 175–178.
- von Eicken, T., Culler, D. E., Goldstein, S. C., Schauer, K. E., Apr. 1992. Active messages: a mechanism for integrated communication and computation. SIGARCH Comput. Archit. News 20 (2), 256–266.
URL <http://doi.acm.org/10.1145/146628.140382>
- Wang, B., Liu, K., Feb 2011. Advances in cognitive radio networks: A survey. Selected Topics in Signal Processing, IEEE Journal of 5 (1), 5–23.
- Wang, H., Elson, J., Girod, L., Estrin, D., Yao, K., 2003a. Target classification and localization in habitat monitoring. In: In ICASSP.
URL <http://lecs.cs.ucla.edu/Publications/papers/Wang03Target.pdf>
- Wang, H., Estrin, D., Girod, L., 2003b. Preprocessing in a tiered sensor network for habitat monitoring. EURASIP J. Appl. Signal Process. 2003, 392–401.
URL <http://lecs.cs.ucla.edu/Publications/papers/tier.pdf>
- Warneke, B., Last, M., Liebowitz, B., Pister, K., Jan 2001. Smart dust: communicating with a cubic-millimeter computer. Computer 34 (1), 44–51.
- Whitepaper, July 7 2009. Logitech advanced 2.4 ghz technology with unifying technology. Tech. Rep. 070709, Logitech for Business.
URL http://www.logitech.com/images/pdf/roem/Advanced_24_Unifying_FINAL070709.pdf

- Yang, D., Xu, Y., Gidlund, M., 2011. Wireless coexistence between IEEE 802.11- and IEEE 802.15.4-based networks: A survey. *International Journal of Distributed Sensor Networks* Article ID 912152, 17 pages.
URL <http://www.hindawi.com/journals/ijdsn/2011/912152/cta/>
- Ye, F., Chen, A., Lu, S., Zhang, L., 2001. A scalable solution to minimum cost forwarding in large sensor networks. pp. 304–309.
- Ye, F., Zhong, G., Lu, S., Zhang, L., Zhong, F. Y. G., 2005. Gradient broadcast: A robust data delivery protocol for large scale sensor networks. *ACM Wireless Networks (WINET)* 11, 285 – 298.
- Yoon, D. G., Shin, S. Y., Kwon, W.-H., Park, H. S., 2006. Packet error rate analysis of IEEE 802.11b under IEEE 802.15.4 interference. In: *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd. Vol. 3.* pp. 1186–1190.
- Youssef, M. A., Younis, M. F., Arisha, K. A., 2002. A constrained shortest-path energy-aware routing algorithm for wireless sensor networks. In: *Wireless Commun. and Networking Conference.* pp. 794–799.
- Yuan, W., September 2011. Coexistence of IEEE 802.11b/g wlans and IEEE 802.15.4 wsns: Modeling and protocol enhancements. Ph.D. thesis, Technische Universiteit Delft.
- Yuan, W., Linnartz, J. P. M. G., Niemegeers, I. G. M. M., 2010a. Adaptive cca for IEEE 802.15.4 wireless sensor networks to mitigate interference. In: *Wireless Communications and Networking Conference (WCNC), 2010 IEEE.* pp. 1–5.
- Yuan, W., Wang, X., Linnartz, J., 2007. A coexistence model of IEEE 802.15.4 and IEEE 802.11 b/g. In: *Communications and Vehicular Technology in the Benelux, 2007 14th IEEE Symposium on.* IEEE, pp. 1–5.
- Yuan, W., Wang, X., Linnartz, J.-P. M. G., Niemegeers, I. G. M. M., 2010b. Experimental validation of a coexistence model of IEEE 802.15.4 and IEEE 802.11b/g networks. *International Journal of Distributed Sensor Networks* Article ID 581081, 6.
- Zacharias, S., Newe, T., 2011a. Competition at the wireless sensor network mac layer: Low power probing interfering with x-mac. *Journal of Physics: Conference Series* 307 (1), 012038.
URL <http://stacks.iop.org/1742-6596/307/i=1/a=012038>
- Zacharias, S., Newe, T., December 2011b. Robustness against interference in wireless sensor networks. *Simulation Notes Europe - Journal on Developments and Trends in Modelling and Simulation* Volume 21 Number 3-4, 171–175.
URL <http://www.sne-journal.org>
- Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., October 2012a. 2.4 GHz IEEE 802.15.4 channel interference classification algorithm running live on a sensor node. In: *IEEE Sensors.* IEEE, Taipei, Taiwan, pp. 1–4.
URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6411279
- Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., February 2012b. Coexistence of different wireless sensor networks - mac protocol interference between x-mac and low power probing. In: *1st international Conference on Sensor Networks.* Rome, Italy.
- Zacharias, S., Newe, T., O’Keeffe, S., Lewis, E., June 2012c. Identifying sources of interference in RSSI traces of a single IEEE 802.15.4 channel. In: *The Eighth International Conference on*

Wireless and Mobile Communications (ICWMC). IARIA, Venice, Italy, pp. 408–414.

URL http://www.thinkmind.org/index.php?view=article&articleid=icwmc_2012_18_10_20270

Zheng, J., Jamalipour, A., 2009. Introduction to wireless sensor networks. In: Zheng, J., Jamalipour, A. (Eds.), *Wireless sensor networks: a networking perspective*. John Wiley & Sons, Ch. 1, pp. 1–18.

Zhou, G., He, T., Krishnamurthy, S., Stankovic, J. A., May 2006a. Models and solutions for radio irregularity in wireless sensor networks. *ACM Trans. Sen. Netw.* 2 (2), 221–262.

URL <http://doi.acm.org/10.1145/1149283.1149287>

Zhou, G., He, T., Stankovic, J. A., Abdelzaher, T., March 2005. Rid: Radio interference detection in wireless sensor networks. In: *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*.

Zhou, G., Stankovic, J. A., Son, S. H., 2006b. Crowded spectrum in wireless sensor networks. In: *Proceedings of Third Workshop on Embedded Networked Sensors (EmNets)*. Citeseer.

Zhou, R., Xiong, Y., Xing, G., Sun, L., Ma, J., 2010. Zifi: Wireless lan discovery via zigbee interference signatures. In: *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, pp. 49–60.

ZigBee Alliance, June 2007. Zigbee and wireless radio frequency coexistence. Whitepaper.

URL <https://docs.zigbee.org/zigbee-docs/dcn/07-5219.PDF>

ZigBee Alliance, June 2008a. Zigbee document 08006r03.

ZigBee Alliance, January 2008b. Zigbee specification (document 053474r17).

ZigBee Alliance, accessed 10 September 2010.

URL <http://www.zigbee.org/>

Zimmermann, H., apr 1980. Osi reference model—the iso model of architecture for open systems interconnection. *Communications, IEEE Transactions on* 28 (4), 425 – 432.

Zuniga, M., Krishnamachari, B., 2004. Analyzing the transitional region in low power wireless links. In: *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*. pp. 517–526.