Paradigma's voor samenwerking
tussen heterogene netwerken in dezelfde draadloze omgeving

Cross-Technology Cooperation Paradigms
Supporting Co-Located Heterogeneous Wireless Networks

Lieven Tytgat

Promotoren: prof. dr. ir. I. Moerman, prof. dr. ir. S. Pollin
Proefschrift ingediend tot het behalen van de graad van
Doctor in de Ingenieurswetenschappen: Elektrotechniek

Vakgroep Informatietechnologie
Voorzitter: prof. dr. ir. D. De Zutter
Faculteit Ingenieurswetenschappen en Architectuur
Academiejaar 2013 - 2014

UNIVERSITEIT
GENT

ISBN 978-90-8578-676-4
NUR 986, 975
Wettelijk depot: D/2014/10.500/22

Universiteit Gent
Faculteit Ingenieurswetenschappen en Architectuur
Vakgroep Informatietechnologie

Promotoren: Prof. Dr. Ir. Ingrid Moerman
Prof. Dr. Ir. Sofie Pollin

Universiteit Gent
Faculteit Ingenieurswetenschappen en Architectuur

Vakgroep Informatietechnologie
Gaston Crommenlaan 8, bus 201 B-9050 Gent, België

Tel: +32 9 331 49 00
Fax: +32 9 331 48 99
Web: http://www.intec.ugent.be

Proefschrift tot het behalen van de graad van
Doctor in de Ingenieurswetenschappen:
Elektrotechniek
Academiejaar 2013-2014

Dankwoord

Had je mij 10 jaar geleden gezegd dat ik een doctoraat zou schrijven, dan had ik je waarschijnlijk voor gek verklaard. Ik wist toen waarschijnlijk nog niet eens wat dat was (Om maar te verzwijgen dat ik het nu nog maar voor de helft weet ☺). Doorheen mijn leven ben ik op basis van mensen die geloven in mij en met enig geluk hier geraakt. Laat mij dit enigszins verduidelijken.

Eigenlijk was ik in de wieg gelegd om "nen goeie metser" te worden. Mathisje, die nu 3 jaar is, kent de kleuren beter bij naam dan toen ik 5 was… Ik ben dan ook nooit een uitblinker geweest in het lager. Gelukkig heeft Frank Colle mij echter op een ander pad geplaatst door mij in het zesde in te schrijven voor de richting Industriële Wetenschappen. Na 6 jaar, waarin ik ieder jaar door het toenmalig PMS afgeraden werd om het volgende studiejaar in mijn richting aan te vangen, heb ik de stap gewaagd om de studies industrieel ingenieur aan te vangen (wat me trouwens ook afgeraden werd). Deze studies had ik hoogst waarschijnlijk niet kunnen voltooien zonder Wouter Minjauw, die me meermaals (letterlijk en figuurlijk ☺) uit het slijk gehaald heeft. Tevens ben ik door hem in contact gekomen met Bart Leenknegt, die mij aan de hand van het high-end audio project een uitdaging van jawelste voorgeschoteld heeft. Hierdoor werden mijn tekorten aan theoretische kennis zichtbaar, waardoor ik de studies burgerlijk ingenieur ben aangevat, welliswaar na een technologisch sabatjaar doorheen de studies van master in industrial management. De laatste stap richting een doctoraat werd mij tenslotte aangegeven door Prof. Jan Vandewege die me in contact bracht met Prof. Ingrid Moerman nadat ik hem had toevertrouwd dat ik iets wou doen met draadloze sensoren. Achteraf bekeken werd mijn levensloop dus bepaald door beslissingen grotendeels gestuurd door anderen. Zonder het ontmoeten van deze mensen was ik hoogst waarschijnlijk een goede metser geweest, wat niet wegneemt dat onze maatschappij evenveel baat heeft aan goeie metsers als goeie hoger opgeleiden.

Het hoeft nu ook geen verder betoog dat ik hier onmogelijk alleen geraakt was. Daarom wil ik iedereen bedanken die mij in meer of mindere mate geholpen heeft om hier te geraken.

Vooreerst wil ik Prof. Ingrid Moerman bedanken voor het mogelijk maken van mijn doctoraat. Ze heeft mij altijd gesteund, in voor of tegenspoed. Ik wil ook Prof.

Piet De Meester bedanken voor het verwezenlijken van de IBCN groep, die in zijn geheel een heel sterk motiverende en ondersteunende omgeving is.

Mijn bureaugenoten hebben mij altijd heel sterk gemotiveerd om het beste van mezelf te geven, dag in dag uit. Evy, Bart, Pieter D., Peter R, Peter DV, Pieter B, Vincent, Jono, Frank, Eli, Peter D., Ward, Mathieu, Dimitri. Ik wil jullie allemaal bedanken voor de vele gesprekken, het luisterende oor, de goede raad en de goede vriendschap die ik met jullie heb opgebouwd doorheen de jaren. Natuurlijk waren er ook buiten onze bureau nog heel wat mensen die mij geholpen hebben. Onder andere Koen, Stijn, Andy, Jeroen, … Tevens wil ik Opher bedanken voor de intensieve begeleiding die hij me heeft gegeven waardoor ik heel sterk gegroeid ben in een heel korte periode.

Mijn co-promoter, Prof. Sofie Pollin, wil ik ook bedanken voor de andere invalshoeken die je telkens opnieuw gaf. Tevens wil ik ook Michael en Jeroen bedanken voor de samenwerking die we hadden in IMEC.

Natuurlijk zijn mijn collega's maar een deel van de mensen die mij gesteund hebben. Mijn teamgenoten in handbalclub Desselgem, die mij in de voorbije jaren slechts sporadisch gezien hebben, wil ik bedanken voor de vele inspannende en ontspannende momenten. Alle leden van Jeugdhuis Jakkedoe, en de (ex) vaste beroepskrachten Stiene, Thomas, Simen, Jan en Vommie. Bedankt ook aan Inge, Wouter, Kenneth, Jan, Leen, Rik, Mathieu en nog zoveel anderen die me momenteel niet te binnen schieten om er te zijn, in goede en minder goede tijden.

Papa en Mama, ik wil jullie bedanken om er altijd te zijn voor mij, zelfs indien je zelf niet volledig akkoord gaat met wat ik doe. Davy, Andy en Bert, ik wil jullie bedanken voor alles. Niet in het minst voor de vele, volgens onze vrouwen eindeloze ☺, technische discussies zonder dewelke ik hier ooit zou zijn geraakt. Paul, Mia, Liene en Chris, Bert en Wannes wil ik danken voor o.a. hun no-nonsens manier van zijn.

Mathis die me altijd opnieuw vrolijk weet te maken als ik een zoveelste zware dag achter de rug heb en onze toekomstige spruit zijn voor mij oneindige bronnen van positieve energie.

Mijn allerliefste vrouwtje, Lies, die me door dik en dun gesteund heeft kan ik niet genoeg bedanken voor alles, gewoonweg alles.

Voor Lies, Mathis en onze toekomstige spruit

Gent, April 2014
Lieven Tytgat

Table of Contents

DANKWOORD ..... **I**

SAMENVATTING ..... **XVII**

SUMMARY ..... **XXI**

1 INTRODUCTION AND PUBLICATIONS **1**

1.1 INTRODUCTION TO WIRELESS COMMUNICATIONS 3

1.1.1 Multiplexing mechanisms *5*

1.1.2 Real-life spectrum sharing *8*

1.2 OVERVIEW OF THIS WORK 10

1.3 PUBLICATIONS 15

1.3.1 A1: Publications in International Journals referenced in the Science Citation Index *15*

1.3.2 Patent applications *16*

1.3.3 P1: Publications in International Conferences referenced in Conference Procedings Citation Index *16*

1.3.4 C1: Articles in other conference procedings *17*

1.3.5 C3: Abstracts in conference proceedings *18*

1.4 REFERENCES 18

2 ANALYSIS AND EXPERIMENTAL VERIFICATION OF FREQUENCY BASED INTERFERENCE AVOIDANCE MECHANISMS IN IEEE 802.15.4 ..... **21**

2.1 CROSS-TECHNOLOGY INTERFERENCE AVOIDANCE: WHY AND HOW? 22

2.2 FREQUENCY BASED INTERFERENCE AVOIDANCE 24

2.2.1 Home/Office Wireless Environment characteristics *25*

2.2.2 Multichannel Protocol Taxonomy *25*

2.3 TAXONOMY BASED INTERFERENCE AVOIDANCE ANALYSIS 32

2.3.1 Experiment based multichannel mechanism comparison *33*

2.4 INTERFERENCE AVOIDANCE WITH RDT 38

2.4.1 RDT runtime metric comparison *38*

2.4.2 Building a new RDT metric *40*

2.4.3 IEEE 802.15.4 transceiver based interference assessment..... 44
2.4.4 Proposed metric comparison 47
2.5 TinyOS based implementation on TMote Sky hardware 49
2.5.1 Information Dissemination Mechanism..... 49
2.5.2 Implementation Architecture..... 49
2.5.3 Packet Format Specification..... 51
2.5.4 Implementation results..... 51
2.6 Future work..... 52
2.7 Conclusion..... 53
2.8 References..... 54

3 AVOIDING COLLISIONS BETWEEN IEEE 802.11 AND IEEE 802.15.4 THROUGH COEXISTENCE AWARE CLEAR CHANNEL ASSESSMENT 59

3.1 Introduction..... 60
3.1.1 CCA operating principle..... 62
3.2 ZigBee PER under Wi-Fi interference..... 64
3.2.1 Analytical PER Model 64
3.2.2 Sensitivity analysis 68
3.2.3 Experimental model verification 70
3.3 Deployment of sensing engine based CACCA..... 72
3.3.1 Sensing engine characteristics 72
3.3.2 Case 1: ZigBee side CACCA 75
3.3.3 Case 2: Wi-Fi side CACCA 76
3.3.4 Case 3: Wi-Fi and ZigBee CACCA 79
3.3.5 Case comparisons..... 80
3.4 Future work..... 82
3.5 Conclusion..... 82
3.6 References..... 83

4 EVALUATING IEEE 802.11 AND IEEE 802.15.4 CROSS-TECHNOLOGY INTERFERENCE AVOIDANCE MECHANISMS..... 87

4.1 Introduction..... 88
4.2 ZigBee Packet loss characteristics 90
4.2.1 Space and frequency domain interference avoidance 92
4.2.2 Time domain interference avoidance..... 93
4.3 Modeling ZigBee packet loss based on Wi-Fi traffic 94
4.3.1 Building the packet loss model..... 95
4.3.2 Experiment description 97
4.3.3 Calibrating the model..... 99
4.4 Comparing interference avoidance classes 103

4.4.1 Frequency domain 103
4.4.2 Time domain 105
4.4.3 Time and frequency domain 106
4.4.4 CACCA impact on Wi-Fi 108
4.5 CONCLUSION 109
4.6 REFERENCES 110

5 COEXISTENCE AWARENESS: THE WAY FORWARD FOR WIRELESS FACTORY AUTOMATION? 113

5.1 INTRODUCTION 114
5.2 SCENARIO DESCRIPTION 115
5.3 TECHNICAL ANALYSIS 117
5.3.1 Achievable ZigBee reliability 118
5.3.2 Implementation 119
5.3.3 Power consumption 119
5.4 ECONOMIC ANALYSIS 121
5.4.1 Capital expenses 122
5.4.2 Operational Expenses 123
5.4.3 Conclusion 126
5.5 BUSINESS ECOSYSTEM ASSESSMENT OF CACCA IMPLEMENTATION 127
5.5.1 Value Proposition for Device Manufacturers 128
5.5.2 CACCA enabled product portfolio 129
5.5.3 Capital Requirements 129
5.5.4 Standardization Issues 129
5.6 CONCLUSION 131
5.7 REFERENCES 131

6 CONCLUSIONS AND PERSPECTIVES 135

6.1 CONTRIBUTION 1: SPACE - FREQUENCY BASED INTERFERENCE AVOIDANCE (RDT) 136
6.2 CONTRIBUTION 2: TIME BASED INTERFERENCE AVOIDANCE (CACCA) 136
6.3 CONTRIBUTION 3: TIME – SPACE – FREQUENCY BASED INTERFERENCE AVOIDANCE 137
6.4 CONTRIBUTION 4: TECHNO-ECONOMICAL AND BUSINESS IMPACT ASSESSMENT OF CACCA 138
6.5 OUTLOOK AND FUTURE RESEARCH OPPORTUNITIES 139
6.6 REFERENCES 141

A ENERGY AWARENESS IN SELF-GROWING SENSOR NETWORKS ... 143

A.1 INTRODUCTION 144

A.2 SAVING POWER IN WIRELESS SENSOR NODES 144
A.3 RECEIVER DIRECTED TRANSMISSION 147
A.4 COMBINING RDT WITH LPL 148
A.5 EXPERIMENTAL POWER CONSUMPTION ANALYSIS 150
A.6 FUTURE WORK 154
A.7 CONCLUSION 154
A.8 REFERENCES 154

List of Figures

Figure 1.1: US Spectrum allocation in the 300MHz to 3GHz band [1.5]. 2
Figure 1.2: Space division multiplexing. Different colours depict different frequencies 5
Figure 1.3: Frequency division multiplexing 6
Figure 1.4: Time division multiplexing 7
Figure 1.5: Code division multiplexing 7
Figure 1.6: Ideal spectrum sharing: No overhead and ideal separation 8
Figure 1.7: Real spectrum sharing with ideal separation 9
Figure 1.8: Real spectrum sharing with non-ideal separation. Typical for intra-technology spectrum sharing. 9
Figure 1.9: Real spectrum sharing with bad separation. Typical for cross-technology spectrum sharing. 10
Figure 1.10: Co-existence awareness can reduce the impact of co-located heterogeneous wireless technologies as well as shift the share of medium occupation to the desired operating point 11
Figure 1.11: The CSMA/CA operating principle 12
Figure 2.1: The 3rd floor of the iMinds w-iLab.t wireless testbed 26
Figure 2.2: Measured maximum interference levels – nighttime 27
Figure 2.3: Measured maximum interference levels – daytime 27
Figure 2.4: Multichannel protocol taxonomy focusing on cross-technology interference avoidance capabilities with typical examples 28
Figure 2.5: The Receiver Directed Transmission operating principle 31
Figure 2.6: The RDT test set-up with ZigBee nodes and Wi-Fi interferers 34
Figure 2.7: The benchmark measurement sequence 35
Figure 2.8: Average PER_Z across all nodes for all channels and different interference scenarios. X-axis = ZigBee channel, Y-axis = PER_Z (%) 36
Figure 2.9: Different interference scenarios 40
Figure 2.10: PER for 100 byte ZigBee packets 41
Figure 2.11: Physical model assumption versus real-life cross-technology interference 42
Figure 2.12: Probability density function (histogram) of the measured interference power for different ZigBee channels 44

Figure 2.13: The measured versus effective in band power..... 45
Figure 2.14: Measurement error due to the long measurement window for different Wi-Fi packet lengths for a classwidth of 2dB 46
Figure 2.15: RDT implementation architecture 50
Figure 2.16: Unicast piggyback trailer..... 51
Figure 2.17: Broadcast piggybacking trailer..... 51
Figure 3.1: Projected number of devices. Source: Morgan Stanley 3..... 61
Figure 3.2: CCA based packet transmission 62
Figure 3.3: Spectral comparison of Wi-Fi and ZigBee 63
Figure 3.4: Possible ZigBee⇔ Wi-Fi interactions..... 65
Figure 3.5: $PER_{Z,W}$ as a function of the Wi-Fi load for different Wi-Fi physical data rates 68
Figure 3.6: Sensitivity of $PER_{Z,W}$ to ZigBee packet size 68
Figure 3.7: Sensitivity of $PER_{Z,W}$ to β, and to small Wi-Fi packets..... 69
Figure 3.8: The test setup..... 70
Figure 3.9: 54 Mbps modeled and measured $PER_{Z,W}$ 71
Figure 3.10: 11 Mbps modeled and measured $PER_{Z,W}$ 71
Figure 3.11: 1 Mbps modeled and measured $PER_{Z,W}$ 72
Figure 3.12: Wi-Fi versus ZigBee sensing engine implementation 73
Figure 3.13: ZigBee timing with and without Sensing Engine 74
Figure 3.14: $PER_{ZS,W}$ as a function of the Wi-Fi load..... 75
Figure 3.15: Sensitivity of $PER_{ZS,W}$ to ZigBee packet size..... 76
Figure 3.16:Possible Wi-Fi ⇔ZigBee interactions – Wi-Fi side sensing engine..... 76
Figure 3.17: $PER_{Z,WS}$ as a function of the Wi-Fi load..... 78
Figure 3.18: $PER_{Z,WS}$ as a function of the ZigBee load 78
Figure 3.19: $PER_{ZS,WS}$ as a function of the Wi-Fi load 80
Figure 3.20: Comparison of $PER_{Z,W}$, $PER_{ZS,W}$, $PER_{Z,WS}$ and $PER_{ZS,WS}$ 81
Figure 3.21: Comparison of standard ZigBee with the three cases..... 81
Figure 4.1: The wireless scenario: blue: signal deterioration, yellow: interference 91
Figure 4.2: Space domain interference impact: measured received PER_Z across the length of the building for ZigBee channel 12..... 92
Figure 4.3: Received PER_Z for every ZigBee channel..... 93
Figure 4.4: Time domain interference impact: Received PER_Z over time of a short and a long ZigBee link 93
Figure 4.5: The used methodology enabling comparison of interference avoidance mechanisms without needing realistic, mobile and repeatable Wi-Fi interference..... 94
Figure 4.6: Four Wi-Fi channels inject interference in a single ZigBee channel..... 96
Figure 4.7: The used nodes of the iMinds w-iLab.t testbed..... 98

Figure 4.8: The ZigBee packet loss measurement sequence 99
Figure 4.9: The measured PER_Z and predicted PER_{SIR} for a single link without threshold filtering 100
Figure 4.10: The measured PER_Z and PER_{SIR} with different thresholds for a single link 101
Figure 4.11: Example measured PER_Z and predicted PER_{SIR} points 102
Figure 4.12: The PER measurements used for calibration and the predicted PER 102
Figure 4.13: Three frequency domain interference avoidance protocols compared 104
Figure 4.14: The effect on the PER of the channel selection interval 104
Figure 4.15: Comparison of regular CCA, Wi-Fi side CACCA and ZigBee + Wi-Fi side CACCA 106
Figure 4.16: Combining single channel with CACCA 107
Figure 4.17: Combining RDT with CACCA 107
Figure 4.18: Spreading the ZigBee load on multiple channels reduces the impact on Wi-Fi 108
Figure 5.1: A typical electronics production line 116
Figure 5.2: ZigBee dataloss as function of Wi-Fi load for 54Mbps Wi-Fi, 1500 bytes Wi-Fi packets and 100 byte ZigBee packets. 118
Figure 5.3: Additional hardware needed to implement CACCA on Wi-Fi and ZigBee 119
Figure 5.4: Average network lifetime for the different scenarios 121
Figure 5.5: Communication failure costs as a function of the Wi-Fi load 124
Figure 5.6: Savings for the different wireless alternatives in comparison to wired deployment. 127
Figure 5.7: Business ecosystem for CACCA Implementation in a factory scenario 128
Figure 6.1: Comparison of frequency (single channel) and space-frequency (RDT) with (CACCA) or without (regular) time based interference avoidance 137
Figure A.1: Power consumption of S-MAC and B-MAC 145
Figure A.2: The LPL operating principle 146
Figure A.3: Transmission to node with quiescent channel 3, which is unknown to the transmitter. The packet is transmitted on all channels 147
Figure A.4: a) LPL above RDT. b) RDT above LPL 148
Figure A.5: Combining RDT and LPL case 1: LPL above RDT 149
Figure A.6: Combining RDT and LPL case 2: RDT above LPL 149
Figure A.7: Comparing case 1 and case 2 with identical link throughputs. a) LPL above RDT, b) RDT above LPL 150
Figure A.8: The implemented architecture: LPL below RDT 151

Figure A.9: Power consumption of RDT without LPL 152
Figure A.10: Power consumption of RDT + LPL without transmission .. 152
Figure A.11: Power consumption of RDT + LPL with unicast transmission 153
Figure A.12: Power consumption of RDT + LPL with broadcast transmission 153

List of Tables

Table 2.1: PERZ Comparison between interference avoidance mechanisms based on the benchmark experiments. The best is highlighted 37
Table 2.2: PERZ for common channel selection metrics based on the benchmark experiments 39
Table 2.3: Default parameters used 44
Table 2.4: PERZ for newly proposed channel selection metrics based on the benchmark experiments. The best is highlighted 48
Table 2.5: PERZ of Single shot and Triggered ReSIST based on runtime implementation 52
Table 3.1: Wi-Fi and ZigBee parameters [3.2],[3.14] 63
Table 3.2: parameters used, default values are underlined 67
Table 3.3: Regular CCA versus sensing engine based CACCA timings 74
Table 3.4: Comparison of regular CCA with the three CACCA deployment alternatives 82
Table 4.1: Frequency domain PER overview 105
Table 5.1: Tmote Sky nominal characteristics 120
Table 5.2: Comparison between Wired and Wireless costs 122
Table 5.3: Capital expenses for the different deployment alternatives 123
Table 5.4: Operational expenses for the wireless alternatives as a function of the Wi-Fi load 125
Table 5.5: Total cost of ownership for all alternatives (k€) 126
Table 5.6: Synthesis - Strategic Issues (ZigBee vs. Wi-Fi Manufacturers) 130
Table A.1: Tmote Sky Typical Power Consumption 145
Table A.2: Measured energy consumption 151

List of Acronyms

3GPP	Third Generation Partnership Project
A	
AAA	Anything, Anytime, Anywhere
AAAA	Anything, Anytime, Anywhere, Anyhow
AP	Access Point
ASIC	Application Specific Integrated Circuit
B	
BER	Bit Error Rate
BG	BackGround
BW	BandWidth
C	
CA	Coexistence Aware
CapEx	Capital Expenditures
CCA	Clear Channel Assessment
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
COTS	Commercial Of The Shelf
D	
DaTD	Data Type Definition
DECT	Digital Enhanced Cordless Telecommunications
DSA	Dynamic Spectrum Access

DUT	Device Under Test

E

EDGE	Enhanced Data Rates for GSM Evolution

F

FDD	Frequency Division Duplex
FiT	Fixed Threshold

G

GPRS	General Packet Radio Service
GSM	Global System for Mobile communication

H

HERC	Heterogeneous Exclusive CCA Range
HS	Horizontal Spectrum Sharing
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HW	Hardware

I

I	Interference
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol (technology)
IPD	Inter Packet Delay
ISM	Industrial Scientific and Medical
ITU	International Telecommunication Union

L

LAN	Local Area Network
LOS	Line Of Sight
LTE	Long Term Evolution

M

MAC	Medium Access Control
MIMO	Multiple In Multiple Out
MTBF	Mean Time Between Failures

O

OFDM	Orthogonal Frequency Division Multiplexing
OpEx	Operational Expenditures
OSI	Open Systems Interconnection

P

PDF	Probability Distribution Function
PER	Packet Error Rate
PHY	Physical Layer
PIP	Physical Infrastructure Provider
PSD	Power Spectral Density
PSR	Packet Success Rate
PU	Primary User

Q

QoS	Quality of Service

R

RDT	Receiver Directed Transmission
ReSIST	Received Signal to Interference Strength based Thresholding
RF	Radio Frequency
Rx2Tx	Receive To Transmit

S

S	Signal
SDR	Software Defined Radio
SINR	Signal to Interference plus Noise Ratio
SIR	Signal to Interference Ratio
SNR	Signal to Noise Ratio
SoTA	State of The Art

T

TCP	Transmission Control Protocol
TDM	Time Division Multiplexing

U

UMTS	Universal Mobile Telecommunication System
UWB	Ultra Wide Band

V

VS	Vertical Spectrum Sharing

W

WCDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Samenvatting

Tegenwoordig verwachten draadloze toestellen continue connectiviteit om hun taak succesvol te kunnen volbrengen. Het AAAA principe – Anything, Anytime, Anywhere en Anyhow – beoogt deze visie waar te maken. Dit principe vereist echter dat verschillende draadloze technologieën gelijktijdig gebruikt kunnen worden. Maar verschillende technologieën kunnen elkaar storen, wat kan leiden tot een degradatie van de prestaties. Deze storingen, ook wel interferentie genoemd, kunnen op drie domeinen vermeden worden namelijk plaats-, tijd- en frequentiegebaseerde interferentie ontwijking.

Op plaats gebaseerde interferentieontwijking vermijdt storing tussen de transmissies van verschillende apparaten door ze ver genoeg te verwijderen van elkaar. Binnen één gebied, genaamd het botsingsdomein, is het namelijk zo dat gelijktijdige transmissies op gelijke frequenties kunnen leiden tot verstoring van deze transmissies. Op frequentie gebaseerde interferentieontwijking tracht storingen te vermijden door de werkfrequentie van de actieve apparaten zo in te stellen dat alle apparaten met een overlappend botsingsdomein op verschillende frequenties werken. Hierdoor kunnen ze het ogenblik van verzending vrij kiezen zonder dat er storingen ontstaan die een negatieve invloed op de prestatie hebben. Op tijd gebaseerde interferentieontwijking tracht storingen te vermijden door er voor te zorgen dat transmissies niet op hetzelfde ogenblik plaatsvinden. Deze aanpak laat toe dat verschillende apparaten binnen een botsingsdomein gebruik maken van dezelfde frequentie.

Binnen eenzelfde technologie wordt typisch gebruik gemaakt van de op tijd gebaseerde aanpak om interferentie te ontwijken. Het zogenaamde Medium Access Controle (MAC) mechanisme van een bepaalde technologie is zo ontwikkeld dat verschillende apparaten die data willen versturen dit niet op een hetzelfde ogenblik zullen doen indien ze zich binnen elkaars bereik bevinden. Elke technologie heeft een specifiek MAC mechanisme en het is helemaal niet evident dat de verschillende MAC schema's van verschillende technologieën die actief zijn binnen eenzelfde omgeving elkaar zullen ontwijken.

Om te garanderen dat apparaten van verschillende technologieën elkaar niet storen wordt meestal gekozen voor een op frequentie gebaseerde aanpak om interferentie te vermijden. Indien de werkfrequenties van de verschillende

technologieën niet overlappen, kunnen de apparaten nagenoeg onafhankelijk van elkaar werken. Het toekennen van de werkfrequenties aan verschillende technologieën die elk bepaalde prestatiegaranties willen bieden, is dus heel cruciaal.

Vandaar dat er regulerende instanties zijn die deze frequenties toekennen en het naleven van deze toekenningen controleren. Bij de introductie van een nieuwe technologie wordt meestal een nieuwe frequentie toegekend, waardoor er schaarste optreedt bij de praktisch bruikbare frequenties. De regulerende instanties hebben een aantal frequentiebanden vrijgegeven, de zogenaamde Industrial, Scientific en Medical (ISM) banden. Binnen de ISM banden is de technologie niet vastgelegd, waardoor meerdere technologieën deze banden tegelijkertijd kunnen gebruiken.

Verschillende draadloze technologieën kunnen een aanzienlijke impact op elkaar hebben. De interactie tussen verschillende technologieën binnen eenzelfde frequentieband is dan ook de focus van dit proefschrift. Een eerste doelstelling van dit proefschrift is het in kaart brengen van de mechanismen die leiden tot degradatie van met elkaar interagerende Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) gebaseerde technologieën, IEEE 802.11 (Wi-Fi) en IEEE 802.15.4 (ZigBee). Een tweede doelstelling is het uitwerken van mechanismen die de prestatie van deze draadloze technologieën binnen eenzelfde omgeving verbetert. Binnen dit proefschrift gaan we dieper in op de mogelijkheden om interferentie te ontwijken op drie domeinen, nl. plaats, frequentie en tijd.

In een eerste bijdrage wordt dieper ingegaan op op plaats en op frequentie gebaseerde ontwijking van botsingen. We beginnen met het analyseren van de draadloze omgeving in een typisch kantoorgebouw die deel uitmaakt van de iMinds w-iLab.t draadloze testomgeving. We stellen vast dat de ideale werkfrequentie van ieder apparaat varieert over tijd en locatie. Rekening houdend met deze observatie vergelijken we verschillende mechanismen die gebruik maken van meerdere kanalen voortbouwend op de opgestelde taxonomie voor multi-kanaal draadloze netwerkprotocollen. Deze taxonomie laat ons toe om de prestaties in te schatten binnen een realistische omgeving. Uit deze vergelijkende studie destilleren we het meest belovende mechanisme waarop we verder inzoomen. De metriek om het beste kanaal te selecteren wordt geanalyseerd en een verbetering op bestaande metrieken wordt voorgesteld. Deze nieuwe metriek wordt experimenteel geëvalueerd en vergeleken met de bestaande metrieken. Ten slotte wordt het protocol geïmplementeerd en experimenteel geëvalueerd in de testomgeving.

Bovenstaande methode laat toe dat ieder IEEE 802.15.4 apparaat op zijn locatie de frequentie om transmissies te ontvangen kiest waar de kans op botsingen het kleinst is. In dichtbezette omgevingen zal de kans op botsingen binnen elke frequentiekanaal significant zijn. Een op tijd gebaseerde oplossing laat toe om in

een dergelijke omgeving toch een evenwichtig gebruik van het spectrum tussen de verschillende technologieën te garanderen. In een tweede bijdrage gaan we daarom dieper in op de problematiek om interferentie te vermijden tussen IEEE 802.11 en IEEE 802.15.4 technologieën op basis van tijd. We bouwen een botsingsmodel tussen beide technologieën en verifiëren het model experimenteel. Vanuit dit model wordt het duidelijk dat standaard IEEE 802.11 apparaten geen rekening houden met het al dan niet bezet zijn van het medium door IEEE 802.15.4 apparaten. We stellen daarom voor om het mechanisme voor toegang tot het medium – Clear Channel Assessment (CCA) – aan te passen. Hierdoor zal een technologie wel rekening houden met de activiteit van andere technologieën. We noemen deze uitbreiding Co-existence Aware CCA (CACCA). CACCA kan toegepast worden op drie verschillende manieren, namelijk enkel in IEEE 802.11, enkel in IEEE 802.15.4 of in beide technologieën tegelijk. We stellen voor deze drie verschillende alternatieven een botsingsmodel voor, en vergelijken daarna de prestatie van de verschillende alternatieven met de prestatie zonder CACCA.

Als derde bijdrage wordt de combinatie van de voorbije twee methodieken geanalyseerd en geëvalueerd in de iMinds w-iLab.t testomgeving. Hiertoe breiden we het botsingsmodel voorgesteld in bijdrage 2 uit zodat ijking mogelijk is via referentiemetingen in de testomgeving. In deze omgeving kunnen we namelijk zowel het IEEE 802.15.4 pakketverlies als alle IEEE 802.11 trafiek tegelijk monitoren. Door deze monitoringgegevens in te brengen in het uitgebreide model kunnen we op elk ogenblik voor elke IEEE 802.15.4 link op elke frequentie het pakketverlies berekenen. Deze dataset wordt dan gebruikt om de op plaats- en op frequentie gebaseerde performantie van onze eerste bijdrage in een realistische interferentie omgeving te verifiëren. Daarna wordt de op tijd gebaseerde aanpak geanalyseerd binnen een realistische interferentie omgeving, gevolgd door de analyse van de combinatie van beide aanpakken.

Ten slotte wordt de economische haalbaarheid van de op tijd gebaseerde aanpak binnen een bedrijfsautomatisatie-context bestudeerd via een techno-economische analyse. We analyseren de impact op de betrouwbaarheid van de communicatie en de batterijlevensduur van de vier verschillende alternatieven om CACCA, uit te rollen. We bestuderen verder de technische complexiteit van het toevoegen van CACCA aan zowel IEEE 802.15.4 als IEEE 802.11. Hieruit kunnen we dan de kapitaalsuitgave en de terugkerende kosten bepalen, en vergelijken met de uitrol van een bekabelde oplossing– de referentie oplossing in bedrijfsautomatisatie. Tenslotte bestuderen we de factoren die invloed kunnen hebben op het al dan niet opnemen van CACCA in het productportfolio van chipsetfabrikanten.

Summary

Wireless devices expect ubiquitous connectivity nowadays. The AAAA principle – Anything, Anytime, Anywhere, Anyhow – promises to realize this vision. This principle requires the concurrent use of multiple heterogeneous wireless technologies within the same physical environment. However, multiple heterogeneous technologies can disrupt each other's operations, degrading their performance. These disruptions, also called interference, can be resolved in three domains namely space-, time- and frequency domain.

Space-based interference avoidance avoids interference between transmissions of multiple devices by spatially separating them from each other. Within a certain space, called the collision domain, different simultaneous wireless transmissions can interfere with each other when they use the same frequency band. Frequency-based interference avoidance aims to avoid interference by configuring the operating frequency of individual devices such that independent devices within each other's collision domain operate on different frequencies. This approach allows independent devices, even within each other's collision domain, to transmit at the same time without interfering with each other. Time-based interference avoidance aims to avoid interference by ensuring that different transmissions do not occur simultaneously. This approach allows different devices to avoid interference even when they are operating within each other's collision domain and in the same frequency band.

The most common approach for interference avoidance within a single technology is the time-based interference avoidance. The so-called Medium Access Control (MAC) mechanism is developed specifically to avoid simultaneous wireless transmissions of co-located wireless devices using the same frequency channel. However, MAC mechanisms are technology specific, and hence do not necessarily mitigate interference across heterogeneous technologies.

The frequency-based approach performs significantly better to avoid interference between multiple heterogeneous wireless technologies. Multiple technologies can operate independently by separating the operating frequencies. The allocation of the operating frequencies is hence of crucial importance, especially for technologies that need guaranteed performance,

Therefore regulatory authorities allocate and verify the correct usage of the allocated frequency bands. However, the introduction of a new technology usually requires the allocation of a new frequency band resulting in scarcity of freely usable frequency bands. For this reason the number of technologies sharing a single frequency band is increasing. The regulatory authorities have allocated a

number of frequency bands for free use by any technology. These are the so-called Industrial Scientific and Medical (ISM) frequency bands.

Cross-technology interference issues are especially apparent within the ISM bands since they are free to all. A number of technologies using the 2.4GHz ISM band employ identical Medium Access (MAC) mechanisms. However, they can still heavily interfere each other's transmissions. A first goal of this dissertation is hence to map the mechanisms resulting in degradation between two Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based technologies – IEEE 802.11 (Wi-Fi) and IEEE 802.15.4 (ZigBee). Especially ZigBee suffers severe degradation in presence of Wi-Fi. Hence within this dissertation we focus on ZigBee performance. A second goal is the analysis and evaluation of mechanisms alleviating this degradation of co-located heterogeneous CSMA/CA based wireless networks. Within this dissertation we investigate the opportunities for improving the co-existence of co-located technologies in each of the three domains – space, frequency and time.

In a first contribution we focus on the combined opportunities of space and frequency based collision avoidance. We first analyze the wireless environment in a typical office building using the iMinds w-iLab.t wireless testbed. We conclude that the ideal operating frequency of every device varies over time and location. Using this knowledge we compare a number of multichannel mechanisms utilizing a newly proposed multichannel protocol taxonomy. This taxonomy facilitates the performance assessment and comparison of each individual mechanism in a realistic environment. From this comparison we select the most promising mechanism within our office environment. Current channel selection metrics do not perform adequately in comparison to the theoretical upper bound for this mechanism. Hence we introduce a new channel selection metric, analyze it en compare it to existing metrics. We conclude this contribution by implementing the complete protocol and evaluating it on the testbed.

The first contribution allowed every IEEE 802.15.4 node to select its own optimal frequency for its location in order to minimize the collision probability with IEEE 802.11 traffic. In dense environments the optimal frequency might still suffer interference from IEEE 802.11, impeding sufficient reliability in IEEE 802.15.4. A time domain approach can efficiently share a single frequency band between both IEEE 802.15.4 and IEEE 802.11. Hence in our second contribution we focus on time domain interference avoidance between IEEE 802.15.4 and IEEE 802.11. We build a cross-technology collision model based on the properties of the CSMA/CA mechanism and verify its accuracy in a shielded wireless test environment. This model clearly shows that under most circumstances IEEE 802.11 does not adjust its channel occupation to the channel occupation of IEEE 802.15.4. Therefore we propose to make the Clear Channel Assessment (CCA) mechanism – which is used to determine if the channel is busy or free – co-existence aware, resulting in Co-existence Aware Clear Channel Assessment

(CACCA). CACCA can be enabled in IEEE 802.15.4, IEEE 802.11 or both. We conclude this contribution by comparing the performance of the three alternatives with a fourth alternative – regular CCA.

In the third contribution we analyze the combination of the two methods described in contribution 1 and 2. To reach this target we extend the collision model of contribution 2 to allow for calibration through benchmarking experiments on the testbed. The testbed experiments allow to monitor IEEE 802.15.4 reliability while at the same time monitoring all IEEE 802.11 traffic on all channels and locations across the testbed. Combining this monitoring data with the extended model gives us a dataset, which allows calculating the packet loss for every link on every channel at any time. From this dataset we analyze the behavior of space-frequency based interference avoidance, followed by time based interference avoidance and last but not least followed by time-space-frequency based interference avoidance.

Finally we assess the economic feasibility of CACCA within a factory automation scenario. In the technical analysis we study the impact on the communication reliability and the battery lifetime of four different deployment alternatives, as well as the implementation complexity of CACCA in IEEE 802.15.4 and IEEE 802.11 devices. In the economic analysis we calculate the capital expenses and the operational expenses based on the technical analysis, and we compare the four deployment alternatives with a wired rollout – the ground truth in factory automation. In the business ecosystem analysis we study the supporting and hindering factor for the uptake of CACCA into the product portfolio of IEEE 802.11 and IEEE 802.15.4 chipset manufacturers.

1
Introduction and Publications

"Real egoistic behaviour is to cooperate!"
Frank H.P. Fitzek and Marcos Katz

Communication has always been one of the cornerstones of human society. Communication allows humans to exchange ideas, thoughts, knowledge, news, etc. Internet facilitates these exchanges, and we have witnessed an incredible impact on human societies during the past decade. It is impossible to imagine a world without Internet, although the widespread adoption of Internet is still relatively young (only a few decades). And we are only at the beginning of the Internet era. Especially since Internet is now becoming mobile (and hence wireless). For example, the importance of mobile communication can hardly be ignored in large-scale events like the Arab Spring [1.1]. Festival attendees as well as organisers rely heavily on mobile communications [1.2]. Locating free parking spots, city guide apps, bike sharing, traffic rerouting, ride sharing programs, etc. are only a few of the feasible applications in Smart cities[1.3]. Smart homes, factories of the future, augmented reality, etc. will all need continuous connectivity. These examples show that huge amounts of information exchange between a huge number of widespread individuals or devices is needed, something which is only possible thanks to the widespread availability of mobile and/or wireless communications.

Maintaining connectivity is not always easy to accomplish. The basic cellular technology, GSM, is highly suited for voice communication. However, for data communication GPRS (based on GSM technology) does not offer the high throughputs required for today's mobile applications. Hence other technologies have been developed to comply with the user needs. A typical modern cellular

phone therefore contains a large number of wireless technologies (GSM [1.6], [1.7], UMTS [1.8], [1.10], HSDPA [1.11], HSUPA [1.12], LTE [1.13], Wi-Fi [1.14], IEEE 802.15.4 [1.15], Bluetooth [1.16]) in order to establish connectivity Anywhere, Anytime and Anyhow (AAA). All these different technologies are combined in a single device, and most of them are operating in different frequency bands in order to allow concurrent communications without jeopardising each other.

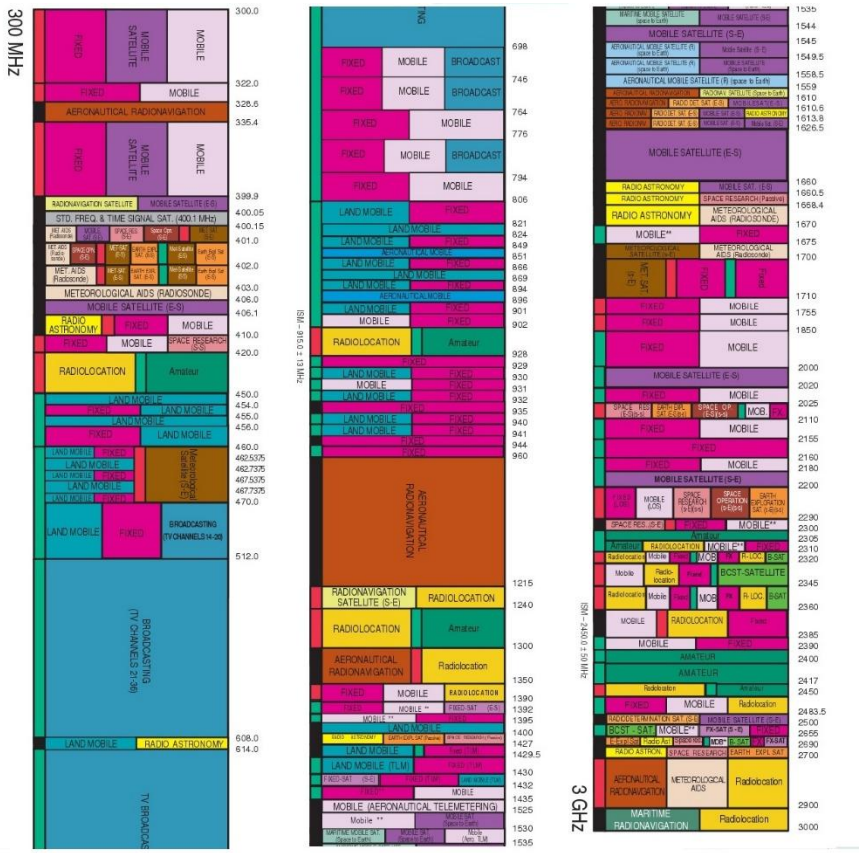

Figure 1.1: US Spectrum allocation in the 300MHz to 3GHz band [1.5].

Not only mobile phones use the wireless medium and have reserved spectral bands. Many other applications have been granted specific spectral bands. Figure 1.1 shows the current frequency allocation in the 300MHz to 3GHz frequency bands. It is clear that from a regulatory point of view the available spectrum is scarce, meaning that most spectrum is allocated (licensed) to specific wireless technologies or applications and only few spectrum is available for free use.

However, measurements indicate that large parts of allocated spectrum (also called licensed bands) are not occupied [1.17]. The spectrum scarcity in unlicensed bands on one hand and underutilization of spectrum in licensed bands necessitate a new communication paradigm to improve the utilization of the available wireless spectrum.

The Dynamic Spectrum Access (DSA) paradigm tries to improve spectrum utilization by using white spaces or spectrum holes (meaning spectrum that is not occupied in temporal, spatial or frequency domain) in licensed spectral bands by non-licensed users. It is hereby of crucial importance that non-licensed users, also called secondary users, do not degrade the performance of the licensed users or primary users. Although a lot of research efforts are spend on DSA, the practical use of DSA is hindered by regulatory and policy issues.

The situation in overcrowded unlicensed bands is different. All users in licensed bands have equal rights and can be considered as primary users that are competing for the same spectrum. Today co-located, unlicensed technologies use the same spectrum in an egoistic way, meaning that they try to achieve optimal performance for their own technology without caring about other co-located technologies. This obviously leads to collisions – an overlap in time space and frequency domains of two or more transmissions. Hence new paradigms for coexistence are needed that avoid collisions between co-located, unlicensed technologies.

This brings us to the main content of this dissertation: "Cross-technology cooperation paradigms supporting co-located heterogeneous wireless networks." Cross-technology cooperation of co-located heterogeneous wireless networks tries to minimize the negative impact different technologies have to each other leading to performance benefits for all co-located technologies.

In order to better situate this problem we start with a general introduction into wireless communications in section 1.1 followed by section 1.2 where we give an overview of this work. We finalize this introduction in section 1.3 where we give an overview of the publications of the author.

1.1 Introduction to wireless communications

Wireless communications use electromagnetic waves to send information from a sender to a receiver. The shape of the electromagnetic waves determines the information content. Hence, the receiver needs to be aware of the characteristics of the shapes used by the transmitter. The physical layer (PHY) of a technology defines the shape of the waveforms used to transport information between a sender and a receiver. The wireless transport of information from sender to receiver uses a so-called 'channel' between the sender and the receiver. The Shannon-Hartley

capacity theorem [1.1], depicted in formula (1.1), shows that each channel has an upper bound to its information capacity.

$$C = BW * \log_2\left(1 + \frac{S}{N}\right) \tag{1.1}$$

With *C* the capacity, *BW* the bandwidth (in Hz), *S* the received signal strength (in W) and *N* the noise strength (in W). Formula (1.1) shows that the maximal capacity of a channel has a linear relation with the bandwidth of the channel, and a logarithmic relation with *S/N* for sufficiently large *S/N*. In (1.1) the noise is assumed to be white noise.

In environments where multiple transmitters are active Interference (*I*) can be added on top of the noise (*N*). The available channel capacity is then reduced to (1.2)

$$C = BW * \log_2\left(1 + \frac{S}{I + N}\right) \tag{1.2}$$

With *I* the interference strength (in W) at the receiver, assuming the interference can be considered as white noise to the received signal (*S*). If we have two transmitters, the channel capacity of both is given in (1.3)

$$\begin{aligned} C_1 &= BW * \log_2\left(1 + \frac{S}{I_2 + N}\right) \\ C_2 &= BW * \log_2\left(1 + \frac{S}{I_1 + N}\right) \end{aligned} \tag{1.3}$$

In (1.3) receiver 1 and transmitter 1 are using channel 1, while receiver 2 and transmitter 2 are using channel 2.

The channel capacity of a channel is only reduced in case eg. the signal of transmitter 2 is received as interference by receiver 1. In such a case the Signal to (Interferene + Noise) Ratio (*SINR*) can be severely reduced, leading to a significantly reduced channel capacity.

The challenge is therefore to maximize channel capacity when multiple transmitters are active. This can be done by maximizing the received signal strength from the desired transmitter measured at the receiver, and by minimizing the impact of a transmission from interfering (non-desired) transmitters at the desired receiver. Within this work we do not consider mechanisms to improve received signal strength. However, we focus on mechanisms which reduce the impact of interference at a receiver. Multiplexing mechanisms intend to exploit orthogonalities between signal and interference in order to reduce the impact of this interference.

1.1.1 Multiplexing mechanisms

Multiplexing mechanisms describe how several users can share a medium with maximum medium utilization and minimum or no interference. For wireless communication, multiplexing can be carried out in four dimensions: space, time, frequency, and code. In this section we zoom in on the available multiplexing mechanisms. This section is partly based on [1.9].

1.1.1.a Space division multiplexing (SDM)

Space division multiplexing divides space into smaller spaces. This allows for spatial reuse of the spectrum. A typical example of spatial reuse is the cellular network. A spatial area is divided into cells. Each cell can operate independently. Cells can also be subdivided into sectors by the use of directional antennas increasing the spatial reuse. In Figure 1.2 cells with different frequencies (represented by different colours) are periodically reused in the network. Cells are further divided into 3 sectors, resulting in an increase of spatial reuse with a factor 3. Space division multiplexing is usually accompanied by at least one of the other multiplexing mechanisms in order to regulate the spectrum access within a cell.

In Figure 1.2 all adjacent cells are operating on a different frequency. This introduces a guard space between cells of identical frequencies, which serves to limit the cross-cell interference by exploiting Frequency Division Multiplexing. Note that introducing these guard spaces reduces the effectiveness of spatial reuse.

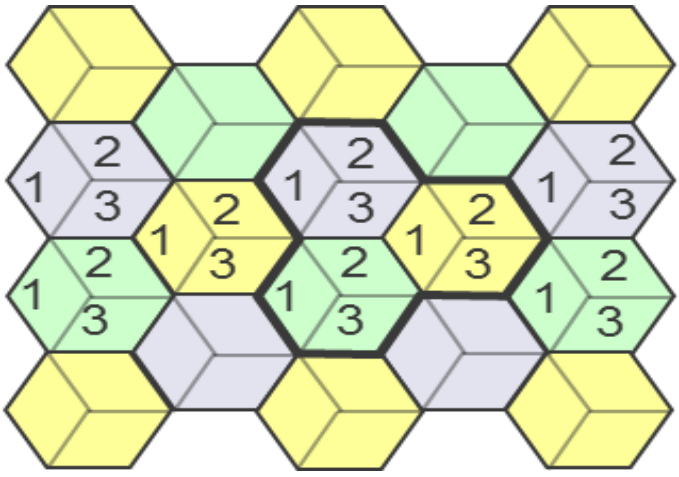

Figure 1.2: Space division multiplexing. Different colours depict different frequencies

1.1.1.b Frequency Division Multiplexing (FDM)

Figure 1.3, Figure 1.4 and Figure 1.5 show a three dimensional coordinate system with the dimensions of frequency *f*, time *t* and code *c*. Within these figures we can easily depict the three remaining multiplexing mechanisms.

Within FDM a channel gets a certain frequency band of the spectrum for the whole time, depicted in Figure 1.3. Each frequency band can be used independently without the need for coordination between channels. FDM is therefore a good candidate to separate multiple technologies. This mechanism is also applicable to analogue broadcast (AM, FM, etc.)

The allocated frequency bands need guard bands to avoid frequency band overlapping between adjacent channels. Guard bands however are a waste of capacity.

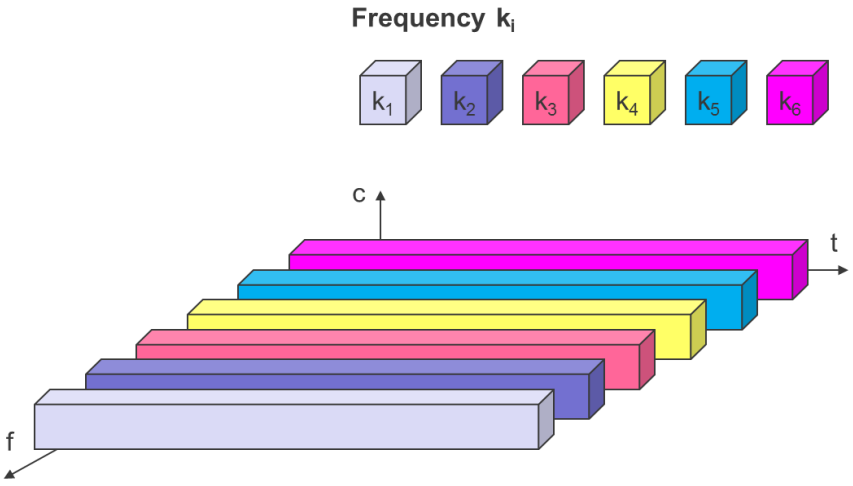

Figure 1.3: Frequency division multiplexing

1.1.1.c Time Division Multiplexing (TDM)

Time division multiplexing divides the wireless medium in timeslots. These timeslots can be static or dynamic in size and allocation to a user. Within a timeslot the complete frequency band is available to the user to which the specific timeslot has been allocated. The major advantage is that TDM is very flexible in nature, and can hence scale relatively easy with the number of users. In between timeslots there is the need for guard spaces, which represent a time gap, in order to avoid interference between adjacent time slots. The minimal size of the guard space is determined by the accuracy of the time synchronisation between different users.

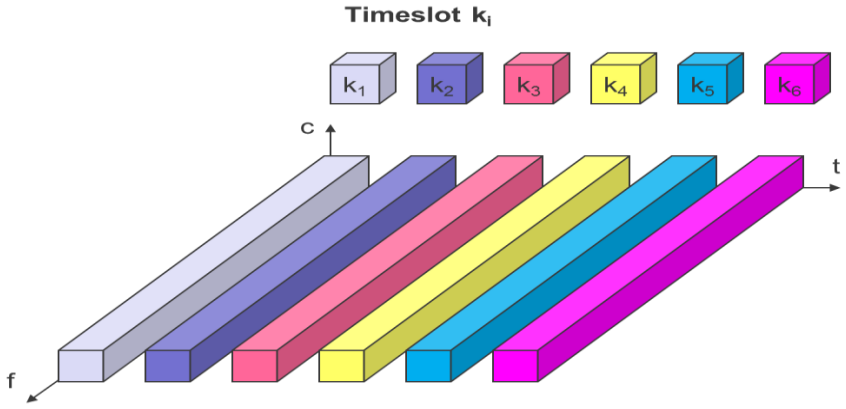

Figure 1.4: Time division multiplexing

1.1.1.d Code Division Multiplexing (CDM)

For completeness we briefly discuss CDM. However, within the remainder of this dissertation we do not consider CDM.

Code division multiplexing uses orthogonal codes to modulate their signal. It is important that there is a good separation between the signal of a desired user and the signals of other users. The separation of the signals is made by correlating the received signal with the locally generated code of the desired user. Orthogonal codes guarantee that the correlation function is high for the signal from the desired user and close to zero for other signals using other codes. This allows for multiple transmissions to occur at the same frequency and at the same time and is e.g. used in UMTS [1.8].

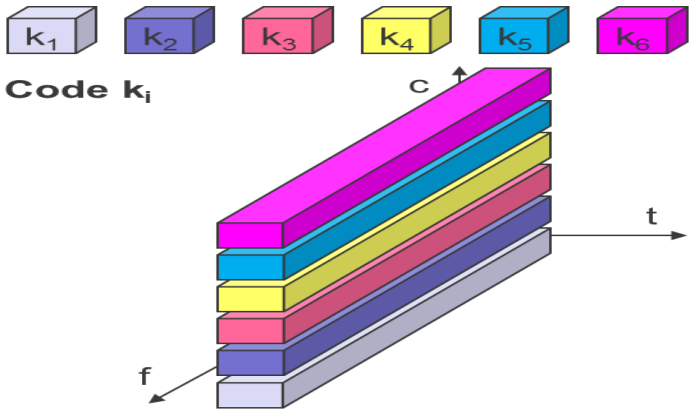

Figure 1.5: Code division multiplexing

1.1.2 Real-life spectrum sharing

In section 1.1.1 we focussed on mechanisms for efficiently sharing the wireless medium with minimum or no interference. These mechanisms allow for improved spectrum utilization in case multiple users of multiple technologies have to share the same spectrum. We now consider the available throughput when multiple users are allocated part of the wireless medium using one or more of the multiplexing mechanisms of section 1.1.1.

In an ideal sharing context there is no overhead involved for maintaining the separation between transmission channels. The separation is assumed to be ideal, i.e. transmissions can occur without having any (negative) impact on each another. Figure 1.6 shows the spectrum sharing of two ideal transmission links, where the relative throughput is normalized to the maximum throughput that can be obtained by a link, when no other links are available. On the left side link 1 is permitted to use the full available spectrum and hence achieves its optimum performance. On the right side link 2 is permitted to use the full available spectrum, resulting in the optimum performance of link 2. In between these extremes the two links have to share the wireless medium. In the ideal sharing case the wireless medium can be allocated 100% to both technologies. In this case the combined relative throughput is identical to the optimum relative throughput.

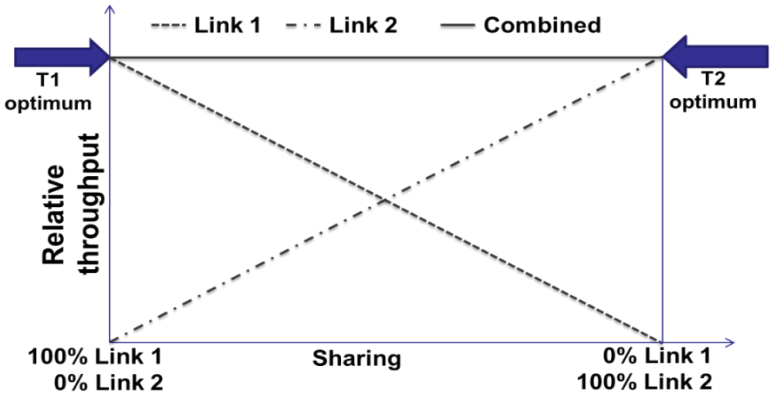

Figure 1.6: Ideal spectrum sharing: No overhead and ideal separation

Figure 1.7 show realistic medium sharing with ideal separation of channels. In this case the guard bands – whether in space, time, frequency or code – are used to guarantee non-overlapping channels. Hence, a single link can never use the medium for 100% resulting in a maximal throughput lower than the optimum link throughput. However, the throughput per link is still linear with the percentage of the medium allocated to it, since we assume ideal separation.

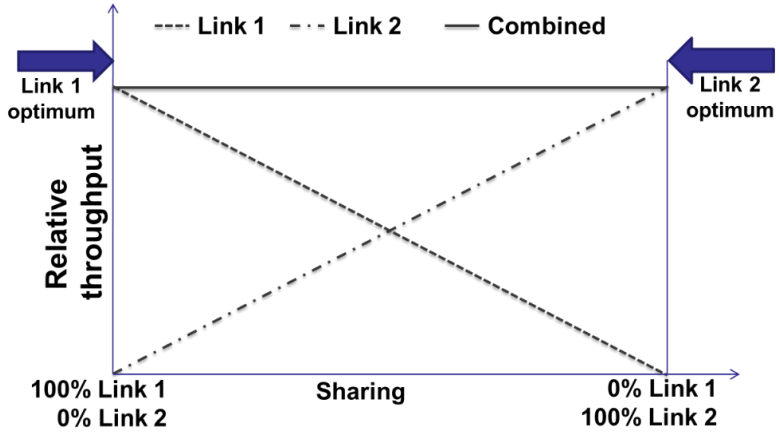

Figure 1.7: Real spectrum sharing with ideal separation

When the separation between channels is not ideal, we can no longer expect that the link throughput is linear with respect to the percentage of medium allocated to it. In this case there can be overlap (interference) between different channels, resulting in a performance degradation. This can happen in intra-technology medium sharing scenario, such as for example in Wi-Fi (IEEE 802.11), which uses a CSMA/CA (more information about CSMA/CA can be found in section 1.2) based TDM. CSMA/CA always has a probability of collision, albeit low by design, when multiple users contend for the same spectrum. Hence some throughput reduction is possible, depicted in Figure 1.8.

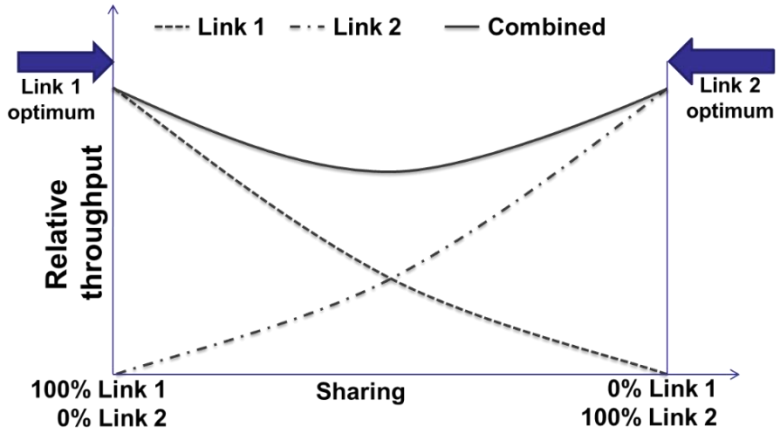

Figure 1.8: Real spectrum sharing with non-ideal separation.
Typical for intra-technology spectrum sharing.

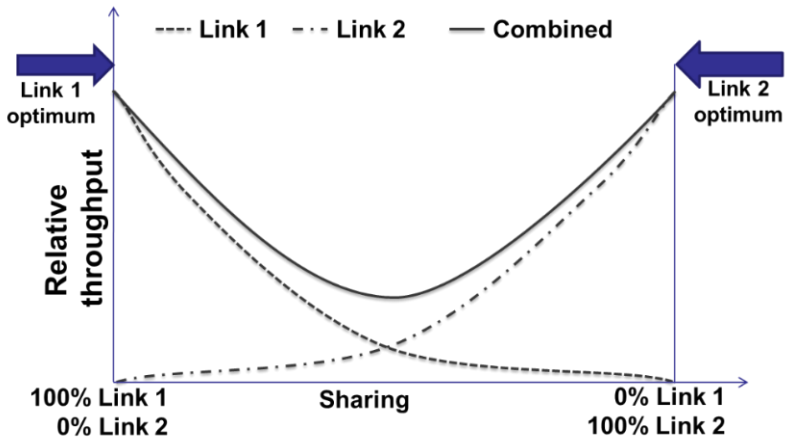

Figure 1.9: Real spectrum sharing with bad separation. Typical for cross-technology spectrum sharing.

When heterogeneous technologies share the same wireless medium, the non-ideal separation of channels is much more pronounced compared to intra-technology. Wireless technologies are generally not designed to detect and avoid other wireless technologies. As there are no guarantees that heterogeneous technologies have compatible MAC mechanisms, these MAC mechanisms may fail to create a good separation between the transmissions of co-located heterogeneous technologies. Hence the throughput is deteriorated significantly, as visualised in Figure 1.9. Additional co-existence awareness measures must be taken in order to improve medium sharing between heterogeneous technologies.

1.2 Overview of this work

The main research question addressed in this dissertation is: "How to reduce the cross-technology impact of co-located heterogeneous wireless networks sharing the same frequency band to an acceptable level". Within this dissertation we always assume that devices with different technologies cannot communicate directly with each another. We are aware that Software Defined Radio (SDR) might enable this paradigm, but we do not consider this possibility within this dissertation. We hence focus on co-existence aware mechanisms that do not rely on any cross-technology communication.

Co-existence awareness can happen on two levels. First of all, it tries to minimize the negative impact of one technology on the other, depicted by the blue arrows in Figure 1.10. Second, it tries to balance the medium occupation in order to allow both technologies to provide sufficient Quality of Service (QoS), depicted by red bar in Figure 1.10.

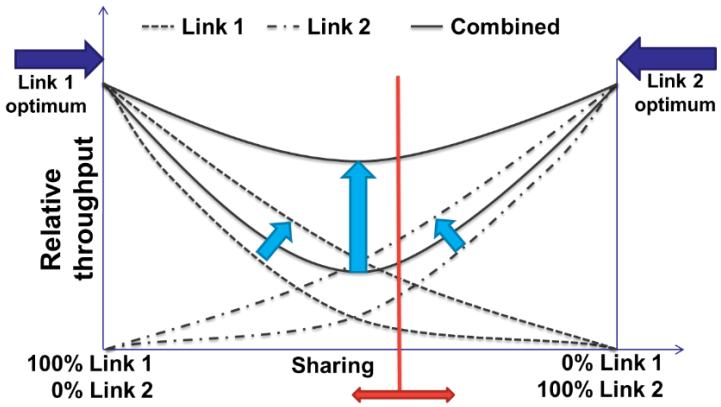

Figure 1.10: Co-existence awareness can reduce the impact of co-located heterogeneous wireless technologies as well as shift the share of medium occupation to the desired operating point

Many wireless technologies are available nowadays. However, in order to have a realistic case which can be analysed and validated both theoretically and experimentally, we have selected two readily available and widely used technologies, IEEE 802.15.4 and IEEE 802.11bg in the 2.4GHz Industrial, Scientific and Medical (ISM) band.

We refer to IEEE 802.15.4 as ZigBee within the remainder of this dissertation. Note that ZigBee defines the higher layers of the Open Systems Interconnection (OSI) model. It uses IEEE 802.15.4 as the underlying technology, which defines the two lower layers of the OSI model. Within this dissertation we solely consider these lower layers. However, in sake of readability we refer to them with the term ZigBee.

ZigBee is a technology suited for Internet of Things (IoT) applications. It is capable of very low energy consumption and has a low throughput. IEEE 802.11, better known as Wi-Fi, offers a significantly higher throughput at the cost of higher energy consumption. Wi-Fi is omnipresent nowadays, while ZigBee is emerging. Widespread adoption of ZigBee will hence result in co-location of ZigBee with Wi-Fi.

Both Wi-Fi and ZigBee technologies use the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism as Medium Access Mechanism. The basic operating principle of CSMA/CA is depicted in Figure 1.11.

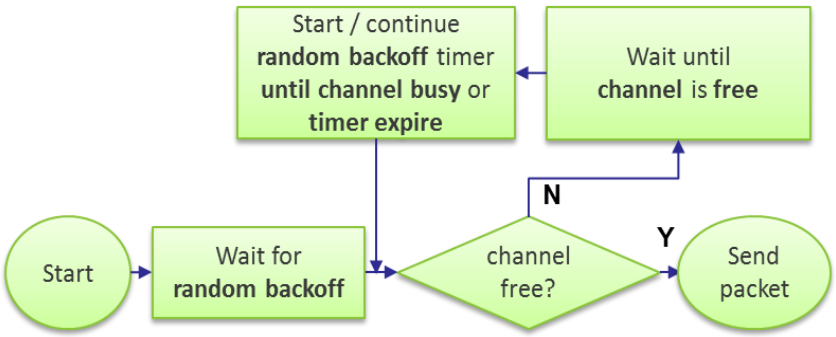

Figure 1.11: The CSMA/CA operating principle

A CSMA/CA based transmitter that wishes to transmit a packet first has wait for a random backoff time. If this timer has fired it has sense the channel to detect if another transmission is occupying the channel. This step is also called the Clear Channel Assessment (CCA). When the channel is assessed free the transmitter can start its transmission. On a busy channel the transmitter waits until the channel is free and then further waits a random period, called the random backoff period, monitored using a back-off timer. If the channel is still free when the back-off timer has expired, the packet is sent. When it is not the back-off timer is frozen until the channel is free again, at which point it continues counting down. This gives more chances to senders that were not able to send in the previous round. After packet transmission a new random period is selected for the next packet. The sequence so far is referred to as Carrier Sense Multiple Access (CSMA). What makes the sequence avoid collision – the Collision Avoidance (CA) part of CSMA/CA – is the calculation of the random backoff timeout. This timeout is a random number between a maximum and a minimum value. The maximum value is increased (typically doubled) each time a collision is detected, as it is not excluded that the back-off timers of multiple senders contending for the medium expire at the same time. This way more collisions will lead to longer average random backoff delays, resulting in a lower packet rate. In turn this results in a lower collision probability, avoiding collisions.

The channel width of ZigBee is significantly smaller (2 MHz) in comparison to the channel width of Wi-Fi (20 MHz), and the maximum transmit powers are also significantly different (0 dBm versus 20 dBm). This results in an unbalanced operation leading to severe ZigBee packet loss. The ZigBee reliability is repeatedly reported to be problematic in the presence of Wi-Fi [1.18], [1.19], [1.20].

The main research question is tackled in three different contributions, organized in different chapters of this dissertation.

- Contribution 1: Analysis and Experimental verification of frequency based interference avoidance mechanisms in IEEE 802.15.4

Contribution 1 essentially focuses on making ZigBee avoid Wi-Fi in the space-frequency domain, hence making only ZigBee coexistence-aware. Within this contribution we zoom in on optimizing the IEEE 802.15.4 performance in an office environment. Wi-Fi is omnipresent and cannot be controlled in a typical office environment. This study hence starts by analyzing the interference created by Wi-Fi. In a second step we assess the impact this interference has on all individual ZigBee links using the w-iLab.t testbed [1.21]. Furthermore we make an objective comparison of the plausible performance of a number of frequency based interference avoidance mechanisms based on a multichannel protocol taxonomy using an 'a posteriori' approach. From this comparison we select the most promising mechanism, and conclude that current metrics do not result in adequate performance for this mechanism. We therefore propose a new metric and analyze its performance in an 'a posteriori' manner based on testbed experiments. Finally we implement the full protocol and evaluate its performance using the TinyOS based TMote Sky hardware [1.22].

- Contribution 2: Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through co-existence aware clear channel assessment

. Within this contribution we look into the co-existence mechanisms of both technologies, assuming that both technologies operate on overlapping frequencies. We start by building an analytical model which predicts the ZigBee incurred Packet Error Rate (PER) under Wi-Fi interference, hereby assuming that every collision between both technologies results in packet loss. The resulting model is experimentally verified in the w-iLab.t shielded environment [1.21]. From this model we identify the key adaptations that are necessary for the Clear Channel Assessment (CCA) mechanism to turn it into a Co-existence Aware Clear Channel Assessment (CACCA). Finally we compare the three different CACCA deployment alternatives namely ZigBee enabled CACCA, Wi-Fi enabled CACCA and ZigBee as well as Wi-Fi enabled CACCA.

- Contribution 3: Evaluating IEEE 802.11 and IEEE 802.15.4 cross-technology interference avoidance mechanisms

Our third contribution combines the methodologies and results of Contribution 1 and Contribution 2. In the first contribution we focused on real-life performance of interference avoidance mechanisms (ZigBee avoiding Wi-Fi) using the wireless testbed. The second contribution focused on building a model that predicts collision probabilities based on measureable Wi-Fi and ZigBee traffic statistics, and further extended this model to include CACCA. Contribution 3 extends the real-life testbed experiments by extensive Wi-Fi sniffing across all channels spread over the full building. The Wi-Fi sniffing is used to calculate the parameters of the collision model of contribution 2. Combining this collision probability with simultaneously executed ZigBee experiments allows us to calibrate the probability that a collision between ZigBee and Wi-Fi results in packet loss on a link basis. Moreover we also predict the collision probabilities in case CACCA is deployed in all three different scenarios. We then focus on comparing space-frequency based interference avoidance, time based interference avoidance and space-time-frequency based interference avoidance in a real-life office environment. Finally we consider the CACCA impact on Wi-Fi throughput.

In addition to these three contributions tackling the main research question, we have addressed a secondary research question considering the potential economic impact CACCA can have in a wireless factory automation scenario. This results in our fourth contribution.

- Contribution 4: Coexistence Awareness: the way forward for wireless factory automation?

Wireless sensor networks can help in reducing the total cost of ownership of a complex production system in comparison to wired sensor solutions. However, the industrial wireless sensor networks like WirelessHART [1.23], ISA100.11a [1.24] are based on the IEEE 802.15.4 standard. Contribution 1 has shown that the reliability can be degraded significantly when coexisting with Wi-Fi networks while Contribution 2 shows that CACCA reduces this degradation drastically. Within this contribution we analyze the economic impact CACCA has on the total cost of ownership for a wireless sensor deployment and compare this to a wired deployment – the ground truth in assembly automation. In the technical analysis we assess the achievable reliabilities and the power consumption associated with these reliabilities. Next an economic analysis is performed to investigate the Capital Expenses (CapEx) as well as the Operational Expenses (OpEx). Economic gains for the end-user do not necessarily result in a successful uptake by manufacturers. Therefore we consider the Business ecosystem encompassing the uptake by manufacturers of CACCA enabled Wi-Fi and ZigBee devices and identify hampering as well as supporting factors for the commercialization of CACCA.

We conclude this dissertation in chapter 6 by summarizing the main conclusions of this work, and look into possible future research opportunities.

This dissertation focuses on packet loss occurring with sensor networks as a sufficiently low packet loss is a minimal requirement for most applications running on a sensor network. However, the real target is the maximization of the total quality of service of the network for a given application. The QoS does not only consider packet loss, but also considers amongst others throughput, battery lifetime, delay, robustness, etc. Within appendix A we focus on combining RDT with a low power protocol in order to combine low packet loss with long battery lifetime.

The combination of multiple protocols is in theory relatively easy, such as in previous example: one protocol selecting frequency of operation, while the other protocol decides on powering the radio on and off. However, many protocols require time-critical operations and are relatively complex. As such a typical radio driver is usually highly optimized towards a specific protocol or protocol stack, leading to a monolithic block of code hindering the flexible combination of multiple protocols. Practical implementation of a combination of protocols is therefore significantly more complex than what the theory predicts. As a response to current inflexible radio drivers, we set out to design a new radio driver architecture that completely separates radio control from MAC protocol development, while still guaranteeing the timely execution of time-critical radio functions, controlled from the higher-layer MAC protocol. This work resulted in a full implementation of a new radio driver architecture and resulted in a patent application.

1.3 Publications

The results of our work are disseminated in several papers published in international journals and presented on international conferences. Below we give an overview of all publications realized during the course of this research.

1.3.1 A1: Publications in International Journals referenced in the Science Citation Index

[1] **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, 2012:137 (pp. 1–15), doi:10.1186/1687-1499-2012-137

[2] De Mil, P., Jooris, B., **Tytgat, L.**, Catteeuw, R., Moerman, I., Demeester, P., & Kamerman, A. (2010). Design and implementation of a generic energy-harvesting framework applied to the evaluation f a large-scale electronic shelf-labeling wireless sensor network. EURASIP JOURNAL

ON WIRELESS COMMUNICATIONS AND NETWORKING., doi:10.1155/2010/343690

[3] **Tytgat, L.**, Yaron, O., Moerman, I., & Demeester, P. (2014). Analysis and experimental verification of frequency based interference avoidance mechanisms in IEEE 802.15.4. IEEE/ACM Transactions on Networking, accepted 16 dec. 2013

[4] De Mil, P., Jooris, B., **Tytgat, L.**, Hoebeke, J., Moerman, I., Demeester, P., (2014). snapMac: a Generic MAC/PHY Architecture Enabling Flexible MAC Design, accepted for publication in Ad Hoc Networks in Jan. 2014

[5] **Tytgat, L.**, Yaron, O., Pollin, S., Moerman, I., & Demeester, P. (Under Review). Evaluating IEEE 802.11 and IEEE 802.15.4 cross-technology interference avoidance mechanisms, submitted to Elsevier Computer Communications Journal, special issue on "Current and Future Architectures, Protocols, and Services for the Internet of Things"

[6] **Tytgat, L.**, Gonçalves, V., Anand, R., Yaron, O., Pollin, S., Moerman, I., & Demeester, P. (Under Review). Coexistence Awareness: The way forward for wireless factory automation?. Submitted to Emerald journal on Assembly Automation.

1.3.2 Patent applications

[1] Inventors: Jooris, B. De Mil, P., **Tytgat, L.**, (patent pending). snapMac: a Generic MAC/PHY Architecture Enabling Flexible MAC Design. Applicant: UGent/iMinds

1.3.3 P1: Publications in International Conferences referenced in Conference Procedings Citation Index

[2] Bouckaert, S., **Tytgat, L.**, Pollin, S., Van Wesemael, P., Dejonghe, A., Moerman, I., & Demeester, P. (2010). Spectrum sharing in heterogeneous wireless networks : an FP7 CREW use case. In E. Di Nitto & R. Yahyapour (Eds.), LECTURE NOTES IN COMPUTER SCIENCE (Vol. 6481, pp. 203–204). Presented at the 3rd European Conference on a Service-Based Internet, Berlin, Germany: Springer.

[3] Barrie, M., **Tytgat, L.**, Gonçalves, V., Yaron, O., Moerman, I., Demeester, P., Pollin, S., et al. (2011). Techno-economic evaluation of cognitive radio in a factory scenario. In V. Casares Giner, P. Manzoni, & A. Pont (Eds.), Lecture Notes in Computer Science (Vol. 6827, pp. 52–61). Presented at the Workshop on Performance Evaluation of Cognitive Radio Networks (PE-CRN 2011) ; 10th International IFIP TC 6 Networking Conference, Berlin, Germany: Springer.

[4] De Valck, P., **Tytgat, L.**, Moerman, I., Demeester, P., Coexistence aware clear channel assessment: from theory to practice on an FPGA SDR platform. In Proceedings of the 10th European conference on Wireless Sensor Networks (EWSN'13), Springer-Verlag, Berlin, Heidelberg, 165-178. DOI=10.1007/978-3-642-36672-7_11

1.3.4 C1: Articles in other conference procedings

[1] **Tytgat, L.**, Moerman, I., "Cross-network cooperation paradigms supporting co-located heterogeneous wireless networks", published in Proceedings of the 10th UGent-FirW PhD symposium, Ghent, Belgium, 09 December 2009, pp. 106-107

[2] Casier, K., **Tytgat, L.**, Verbrugge, S., Pickavet, M., & Moerman, I. (2011). Building the business case for wireless sensors in a factory setting. 50th FITCE congress : proceedings (pp. 238–243). Presented at the 50th FITCE International congress (FITCE 2011) : ICT : bridging an ever shifting digital divide, Brussels, Belgium: FITCE (Forum for European ICT Professionals)., doi: 10.1109/FITCE.2011.6133452

[3] **Tytgat, L.**, Yaron, O., Moerman, I., & Demeester, P. (2012). Energy awareness in self-growing sensor networks. *17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Proceedings* (pp. 241–245). Presented at the 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD - 2012), IEEE.

[4] Raju, A., Lindmark, S., Yaron, O., De Poorter, E., **Tytgat, L.**, Delaere, S., & Ballon, P. (2012). Business model assessment of Green wireless sensor ecosystems. 11th Conference of Telecommunication, Media and Internet Techno-Economics, Proceedings (pp. 1–8). Presented at the 11th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE - 2012), Ghent, Belgium: Ghent University, Department of Information technology.

[5] **Tytgat, L.** (2011). Cross-network cooperation paradigms supporting colocated heterogeneous wireless networks. FEA PhD symposium, 12th. Presented at the 12th FEA PhD Symposium, Ghent University. Faculty of Engineering and Architecture.

[6] **Tytgat, L.**, Barrie, M., Gonçalves, V., Yaron, O., Moerman, I., Demeester, P., Pollin, S., et al. (2011). Techno-economical viability of cognitive solutions for a factory scenario. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, Proceedings (pp. 254–264). Presented at the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN - 2011), IEEE.

[7] **Tytgat, L.**, Jooris, B., De Mil, P., De Poorter, E., Moerman, I., & Demeester, P. (2008). Multichannel protocol for interference avoidance in wireless sensor networks. Proceedings of 2nd Gent University and KEIO University Global COE Joint workshop (pp. 55–58). Presented at the 2nd Gent University and KEIO University Global COE Joint workshop 2008.

1.3.5 C3: Abstracts in conference proceedings

[1] Liu, W., Mehari, M., Bouckaert, S., **Tytgat, L.**, Moerman, I., & Demeester, P. (2013). Demo abstract: a proof of concept implementation for cognitive wireless sensor network on a large-scale wireless testbed. 10th European Conference on Wireless Sensor Networks, Abstracts (pp. 1–2). Presented at the 10th European Conference on Wireless Sensor Networks (EWSN - 2013).

[2] **Tytgat, L.** (2009). Cross-network cooperation paradigms supporting co-located heterogeneous wireless networks. UGent-FirW Doctoraatssymposium, 10e (pp. 106–107). Presented at the 10e FirW PhD Symposium, Gent: Universiteit Gent. Faculteit Ingenieurswetenschappen.

[3] **Tytgat, L.**, Jooris, B., De Mil, P., Latré, B., Moerman, I., & Demeester, P. (2009). Demo abstract : WiLab, a real-life wireless sensor testbed with environment emulation. EWSN 2009 adjunct poster proceedings. Presented at the 6th European conference on Wireless Sensor Networks (EWSN 2009).

[4] Moerman, I., Jooris, B., De Mil, P., Allemeersch, T., **Tytgat, L.**, & Demeester, P. (2008). WiLab : a large-scale real-life wireless test environment at IBBT. Intelligent sensor and actuator based systems for mechatronics, Presentations. Presented at the Intelligent sensor and actuator based systems for mechatronics.

1.4 References

[1.1] N. Sharif, “The ‘Arab Spring’ and the future of communications”, online: http://www.portland-communications.com/publications/quarterly-issue-3/the-arab-spring-and-the-future-of-communications/, Accessed 6 jan. 2014

[1.2] Preben Holst Mogensen and Marlene Nybro Thomsen, “New Technologies Provide Overview@aGlance at Large Music Festivals’, online: http://ercim-news.ercim.eu/en79/rd/new-technologies-provide-overviewaglance-at-large-music-festivals, Accessed 7 feb. 2014

[1.3] Lauren Drell, “25 technologies every smart city should have”, online: http://mashable.com/2012/12/26/urban-tech-wish-list/, Accessed 7 feb. 2014

[1.4] C. E. Shannon, "Communication in the presence of noise", Proceedings of the Institute of Radio Engineers, vol. 37, no.1, pp. 10-21, Jan. 1949

[1.5] Bennet, R., "The Spectrum Challenge", online: http://www.hightechforum.org/the-spectrum-challenge/, Accessed 6 jan. 2014

[1.6] European Telecommunications Standards Institute, "EN 301 502: Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements of article 3.2 of the R&TTE directive (1999/5/EC)", online: http://pda.etsi.org/pda/queryform.asp, Accessed 11 jan. 2014

[1.7] European Telecommunications Standards Institute, "EN 301 511: Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements of article 3.2 of the R&TTE directive (1999/5/EC)", online: http://pda.etsi.org/pda/queryform.asp, Accessed 11 jan. 2014

[1.8] European Telecommunications Standards Institute, "ETSI TS 125 101 : Universal Mobile Telecommunications System (UMTS); User Equipment (UE) radio transmission and reception (FDD)", online: http://www.3gpp.org/DynaReport/25101.htm, Accessed 7 feb. 2014

[1.9] Schiller, J, "Mobile Communications Second Edition", pp 69-92, ISBN: 978-0-321-12381-7

[1.10] European Telecommunications Standards Institute, "ETSI TS 125 102 : Universal Mobile Telecommunications System (UMTS); User Equipment (UE) radio transmission and reception (TDD)", online: http://www.3gpp.org/DynaReport/25102.htm, Accessed 7 feb. 2014

[1.11] European Telecommunications Standards Institute, "ETSI TS 125 308 : Universal Mobile Telecommunications System (UMTS); High Speed Downlink Packet Access (HSDPA); Overall description; Stage 2", online: http://www.3gpp.org/DynaReport/25308.htm, Accessed 7 feb. 2014

[1.12] European Telecommunications Standards Institute, "ETSI TS 125 319 : Universal Mobile Telecommunications System (UMTS); Enhanced uplink; Overall description; Stage 2", online: http://www.3gpp.org/DynaReport/25319.htm, Accessed 7 feb. 2014

[1.13] European Telecommunications Standards Institute, "ETSI TS 136 300 : LTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 ", online: http://www.3gpp.org/DynaReport/36300.htm, Accessed 7 feb. 2014

[1.14] IEEE Standards Association, "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"

[1.15] IEEE Standards Association, "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)"

[1.16] IEEE Standards Association, "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer

(PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)"

[1.17] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, Shantidev Mohanty, NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey, Computer Networks, Volume 50, Issue 13, 15 September 2006, Pages 2127-2159, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2006.05.001.

[1.18] G. Thonet, P. Allard-Jacquin, P. Colle, "ZigBee – Wi-Fi Coexistence White paper and Test Report," [online], Available: www.ZigBee.org

[1.19] Wei Yuan, Xiangyu Wang, Linnartz, J.-P.M.G. , "A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g," Communications and Vehicular Technology in the Benelux, 2007 14th IEEE Symposium on,pp.1-5, Nov. 2007, doi: 10.1109/SCVT.2007.4436237 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4436237&isnumber=4436227

[1.20] S. Pollin,I. Tan,B. Hodge,C. Chun,A. Bahai, "Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study," Cognitive Radio Oriented Wireless Networks and Communications (CrownCom) 2008 3rd International Conference on, pp.1-6, May 2008, doi: 10.1109/CROWNCOM.2008.4562460. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4562460&isnumber=4562434

[1.21] Iminds Wireless lab, [online] http://www.iminds.be/en/develop-test/ilab-t/wireless-lab, last accessed 06 Jan. 2014

[1.22] TMOTE SKY datasheet, online: http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf, Accessed 06 Jan. 2014

[1.23] HART Communication Foundation. WirelessHART Technology. [Online] http://www.hartcomm.org/protocol/wihart/wireless_technology.html

[1.24] ANSI/ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications. [Online] http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=11931, Accessed 7 feb. 2014

2

Analysis and Experimental verification of frequency based interference avoidance mechanisms in IEEE 802.15.4

This Ph.D. research focusses on improving the space-frequency-time separation of heterogeneous CSMA/CA based technologies. Within this chapter we consider IEEE 802.15.4 space-frequency domain interference avoidance protocols to lessen the Wi-Fi impact on IEEE 802.15.4. Moreover the considered protocols should be implementable using current Commercial of The Shelf (COTS) radios. Such an approach is easily incorporated in the roll-out of new sensor networks for they do not require hardware changes, not in IEEE 802.15.4 nor in IEEE 802.11.

A number of protocols exploiting space-frequency domain interference avoidance have already been proposed in literature. In search of the best performing solution the most logical first step is to quantitatively compare the performance of current State Of The Art (SoTA) solutions. This encompasses two major parts. 1) We need to identify the benchmark experiment within which the protocols should be quantitatively compared. This benchmark experiment has to be repeatable and realistic. Moreover we need an absolute optimal benchmark to compare these SoTA solutions to. This optimal benchmark helps in validating that significant improvements upon current SoTA are indeed worthwhile. 2) A large number of protocols have already been proposed in literature. As such we need to classify the existing protocols into protocol classes which showcase the packet loss reducing capabilities of each class.

The theoretical optimal solution is then selected. However, theory and practice are not always similar. Hence we take the necessary steps to go from theory to a full protocol implementation, which allows us to validate its performance, and compare it to the optimal benchmark.

Lieven Tytgat, Opher Yaron, Sofie Pollin,
Ingrid Moerman, Piet Demeester

To appear in IEEE/ACM transactions on networking
Accepted for Publication in December 2013

Abstract - *More and more wireless networks are deployed with overlapping coverage. Especially in the unlicensed bands we see an increasing density of heterogeneous solutions, with very diverse technologies and application requirements. As a consequence, interference from heterogeneous sources – also called cross-technology interference – is a major problem causing an increase of Packet Error Rate (PER) and decrease of QoS, possibly leading to application failure. This issue is apparent for example when an IEEE 802.15.4 Wireless Sensor network coexists with an IEEE 802.11 Wireless LAN which is the focus of this work. One way to alleviate cross-technology interference is to avoid it in the frequency domain by selecting different channels. Different multichannel protocols suitable for frequency domain interference avoidance have already been proposed in the literature. However, most of these protocols have only been investigated from the perspective of intra-technology interference. Within this work we create an objective comparison of different candidate channel selection mechanisms based on a new multi-channel protocol taxonomy using measurements in a real-life testbed. We assess different metrics for the most suitable mechanism using the same set of measurements as in the comparison study. Finally, we verify the operation of the best channel selection metric in a proof of concept implementation running on the testbed.*

2.1 Cross-technology Interference Avoidance: Why and How?

It is increasingly hard to imagine a world without wireless communication. Today, we experience an exciting time given the emergence of the Internet of Things, which will allow any identifiable object in the world to communicate. Most objects will connect wirelessly, for obvious reasons. Hence we can safely assume that the number of wireless devices will continue to grow exponentially [2.1]. Not only does the quantity of devices grow, but also the application domains

diversify. Different application domains impose different requirements on the network, e.g. the Quality of Service (QoS) it needs to deliver, or the limitation on power consumption of network nodes that operate on batteries. These diversifying requirements can no longer be supported by a single wireless technology. Even more, within a single environment multiple wireless technologies are being deployed in order to fulfill the applications needs. Hence coexistence of different technologies is becoming increasingly important.

The coexistence of different technologies is particularly challenging when they share the same frequency band. Representative of such situation are the unlicensed frequency bands, which are used by an increasing number of wireless technologies. As a result, different technologies which have not been designed to coexist need to operate in the same frequency bands, leading to reduced reliability of these technologies. A typical example, on which we focus in this paper, is the coexistence of IEEE 802.11 (Wi-Fi) and IEEE 802.15.4 (ZigBee) networks. These technologies have very diverse application domains, but are typically deployed in identical surroundings such as homes, offices and public buildings. It is shown in numerous studies that ZigBee suffers significant increase in packet loss rates in the presence of Wi-Fi interference [2.2], [2.3], [2.4], [2.5].

Cross-technology interference avoidance aims to avoid this interference in three domains – time, frequency and space. Space based frequency avoidance is not an option for we need all sensor nodes to operate at the location they are in, and we do not want to lower Wi-Fi transmit power for this results in decreased Wi-Fi performance. Time based interference avoidance between Wi-Fi and ZigBee has already been studied. In [2.5] they experimentally prove that Wi-Fi does not backoff at all for IEEE 802.15.4, even for very strong ZigBee signal strengths. However, In [2.6] they state that Wi-Fi can backoff within a certain range, although it still creates collisions due to the slow CCA of IEEE 802.15.4. Indeed, the Wi-Fi standard [2.11] states that Wi-Fi can implement preamble based CCA resulting in increased intra-technology detection sensitivity but removing cross-technology detection capabilities altogether, or energy based CCA which has lower intra-technology detection sensitivity but can also detect other technologies under some scenarios. Hence depending on the implementation Wi-Fi might or might not be able to backoff for IEEE 802.15.4 within a certain range. In [2.7] we have solved this issue by adjusting the Wi-Fi Clear Channel Assessment (CCA), making it sensitive for Wi-Fi as well as IEEE 802.15.4. As IEEE 802.15.4 networks cannot always rely on advanced Wi-Fi CCA capabilities, there is still a need for coexistence solutions that do not rely on such enhanced Wi-Fi capabilities. In [2.8] the authors present a method to exploit the typical bursty behavior of Wi-Fi and reduce the amount of transmissions during a Wi-Fi traffic burst. However, in case of continuous high-throughput Wi-Fi networks the throughput drops drastically. In such a scenario it is simply favorable to avoid the occupied frequencies altogether. Hence in this paper we study interference

avoidance in the frequency domain, i.e. mechanisms that attempt to direct concurrent transmissions in co-located networks to different frequencies.

More specifically, we focus on Multichannel Protocols – in which individual nodes of a single network may operate on different channels. A plethora of multichannel protocols exists in the literature. Multichannel protocols are typically used to increase throughput by exploiting frequency based parallelism. Within a cross technology interference avoidance context the maximum goodput (throughput times packet success rate) per channel is lowered due to the packet loss incurred by cross-technology interference. Typical sensor network applications require a low throughput and a long battery lifetime. Therefore within sensor networks the focus is usually on reliability and not on throughput. Hence we focus on minimizing the amount of packet loss due to the interference received from other technologies. However, the relative advantages and disadvantages of multichannel protocols with respect to packet loss rates due to cross-technology interference have not been studied so far.

Therefore in Section 2.2 we analyze the wireless environment of a typical wireless sensor network, discuss related work, propose taxonomy for multichannel protocols and compare different channel selection mechanisms defined in the taxonomy using testbed based benchmark experiments. These experiments identify the Receiver Directed Transmission (RDT) protocol [2.17] as having superior properties. Although RDT is the most promising protocol, it lacks a channel selection metric. Hence in Section 2.3 we evaluate the performance of common channel selection metrics when applied to RDT using the same testbed based benchmark experiments as in section 2.2, and show there is opportunity for improvement. For that reason we propose a new channel selection metric specific for RDT and verify its operation, again based on the same benchmark experiments. In Section 2.4 we elaborate on the proof of concept implementation and verify its runtime implementation on the testbed. Section 2.5 looks at future research while we conclude this paper in Section 2.6.

2.2 Frequency based interference avoidance

A typical Wi-Fi - ZigBee coexistence environment is an office building. ZigBee devices can be used for monitoring and control functions such as access control, HVAC monitoring and control, fire detection, etc., while Wi-Fi is used for wireless Internet connectivity. A typical ZigBee network therefore needs to maintain the needed QoS within such an environment.

2.2.1 Home/Office Wireless Environment characteristics

A thorough analysis of the time/space/frequency characteristics of the interference in a typical ZigBee environment aids in selecting the protocol that minimizes PER in the ZigBee network. We measured the interference on the third floor of the iMinds w-iLab.t testbed [2.26] using the ZigBee nodes. This testbed is located in a 20m by 80m office building, and consists of 200 nodes spread across 3 floors. Its third floor is depicted in Figure 2.1

.

Figure 2.2 and Figure 2.3 show interference measurements across the length of the building for all ZigBee channels during nighttime and daytime respectively. Figure 2.2 confirms that interference is local by nature. Moreover, there is at least one channel available with low interference levels across the building, for example channel 26. A single channel can therefore be selected that will result in relatively low perceived interference. However, Figure 2.3 shows that during daytime there is no single channel that has low interference throughout the building. Hence we conclude that the interference environment is highly dynamic.

2.2.2 Multichannel Protocol Taxonomy

A multichannel protocol must guarantee that transmitter and receiver are on the same channel at the same time so that communication can take place. Every multichannel protocol is hence composed of three major components: (1) channel selection that determines the channel at which to operate; (2) switching time scheduling, which determines when to actually switch to the selected channel; and (3) a mechanism to exchange/negotiate channel selection such as common control channel and distributed control channel, split-phase, etc.

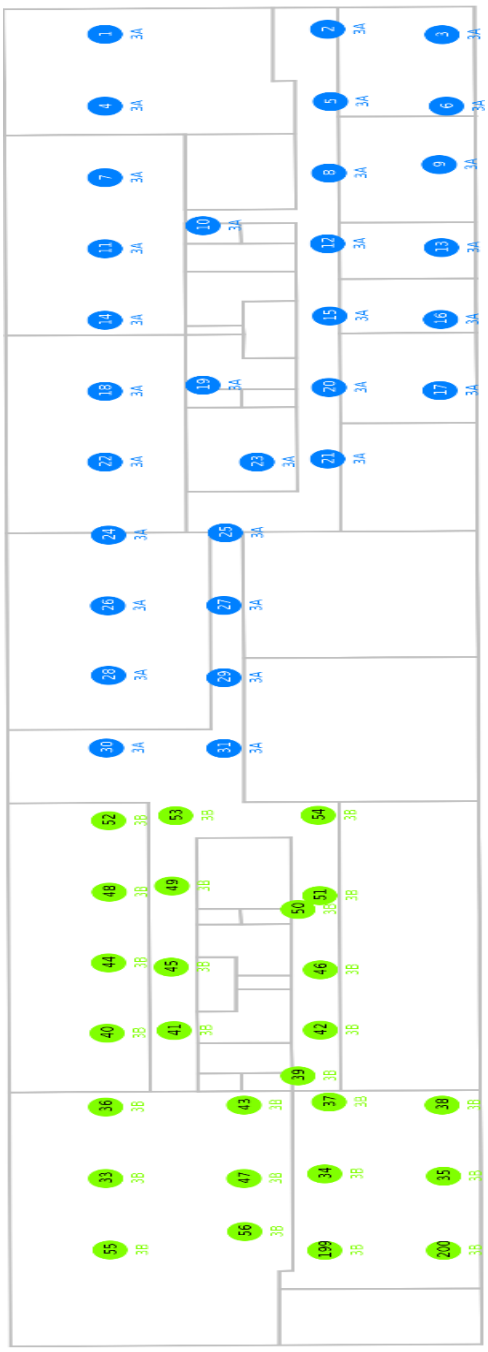

Figure 2.1: The 3rd floor of the iMinds w-iLab.t wireless testbed

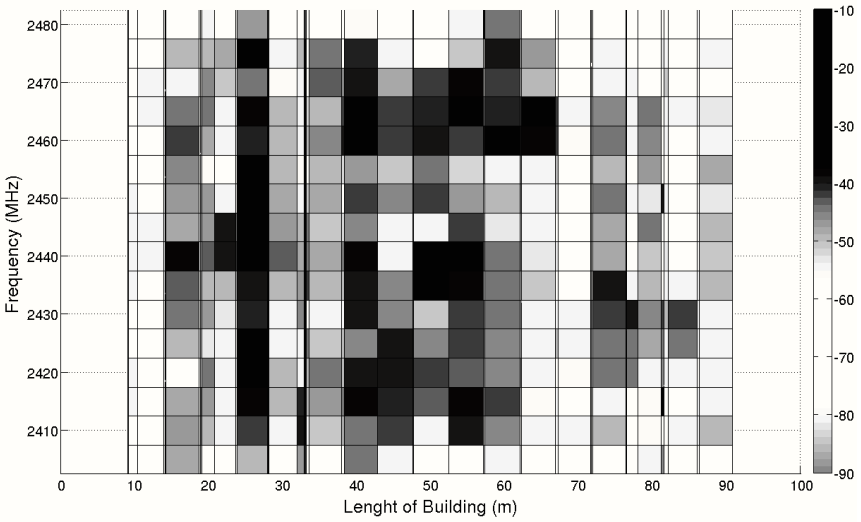

Figure 2.2: Measured maximum interference levels – nighttime

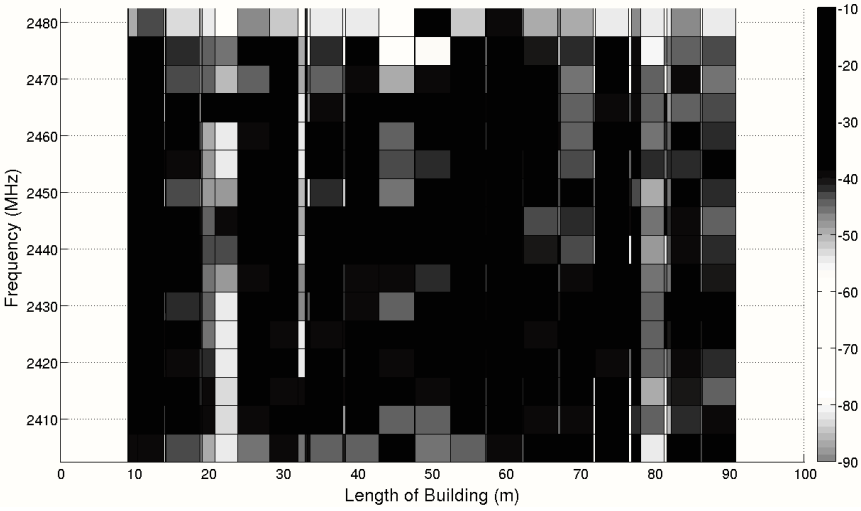

Figure 2.3: Measured maximum interference levels – daytime

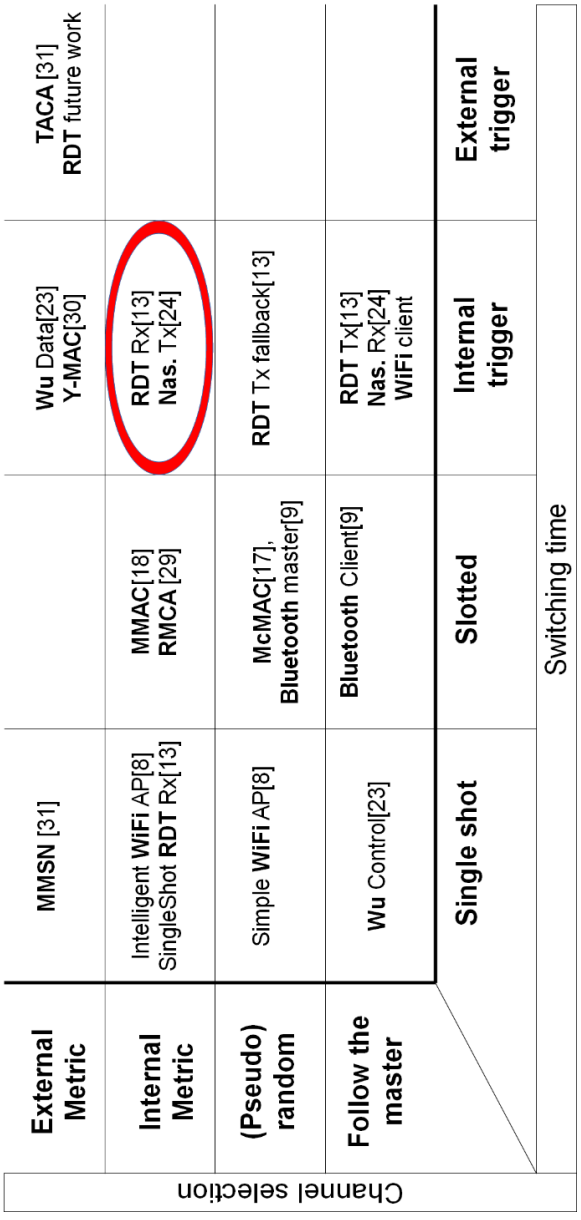

Figure 2.4: Multichannel protocol taxonomy focusing on cross-technology interference avoidance capabilities with typical examples

Soua and Minet [2.31] propose a multichannel protocol taxonomy based on four questions. 1) What is the goal? 2) At what time is channel assignment done? 3) Which channel is selected and 4) How is channel assignment done? In [2.32] Incel proposes a taxonomy based on 7 questions. 1) What is the channel assignment method, 2) Does the protocol need a control channel, 3) is it a centralized or distributed protocol, 4) Do all nodes operate on 1 frequency at a given moment in time 5) What is the type of medium access, 6) Does the protocol support broadcast and 7) What is the objective. Both works compare a number of protocols using their taxonomy. However, none of the studied multichannel protocols have cross-technology interference avoidance as goal. Even more, both taxonomies do not facilitate easy comparison of protocols within a cross-technology interference prone environment, nor does it allow prediction of protocol performance based on their classification.

Our taxonomy facilitates comparing the achievable performance under cross-technology interference by focusing only on the time and frequency behavior of protocols. In doing so we do not incorporate the specific goal nor the mechanism to exchange/negotiate protocol information – also known as control traffic – into our taxonomy. However, our taxonomy aids in predicting the suitability of a given protocol type for a specific goal. Moreover, control and data traffic both have some time – frequency behavior, which might or might not be different. Our approach allows assessing the performance of control as well as data traffic, leading to a clear insight in the strengths and weaknesses of a complete protocol in heterogeneous interference scenarios.

Figure 2.4 shows our protocol taxonomy with the frequency behavior on the vertical axis (channel selection) and the time behavior on the horizontal axis (switching time).

Within our protocol taxonomy we do not consider the used Medium Access Control (MAC) mechanism within each technology. MAC protocols typically intend to reduce intra-technology interference to an acceptable level. This might or might not result in reduced cross-technology interference. However, the multichannel protocol for optimal frequency based cross-technology interference avoidance within a given environment can still be selected using the proposed multichannel protocol taxonomy, without loss of generality. Hence a technology can still use its own medium access mechanism reducing the intra-technology collisions significantly while the usage of a multichannel protocol reduces the cross-technology collisions.

We distinguish four different approaches to channel selection mechanisms: follow the master, (pseudo) random, internal metric based and external metric based.

We define a node following the channel selection of another node – denoted the master – as a follow the master channel selection approach. In such a protocol the master has some way of informing the slave of the channel selection it needs

to adhere to. A Wi-Fi client is a typical example. It searches the channel of the Access Point, connects to it and remains on this channel. Another example is a Bluetooth slave device, which follows the hopping sequence of the master. It is informed of the hopping sequence it needs to follow by means of the master ID and a synchronization phase when joining the piconet [2.10]. A pseudo random channel selection is not based on any ranking of channels and results in a flat distribution of the selection probability of any used channel. Hence random, pseudo random, round robin, etc. channel selections all fall into this category. A Bluetooth master is a typical example of a pseudo random hopping channel selection approach, while slave devices that are part of a piconet are obliged to follow the masters channel hopping sequence. A metric based protocol is defined as a protocol which creates some form of channel ranking and therefore can select a specific channel suited to support the goal of the protocol. We denote a channel metric as an internal metric when it is calculated without needing information from another node. A typical example of an internal metric is the channel selection of a Wi-Fi AP. It selects its initial channel, based on some metric, independent of any client communication. In contrast, an external metric is a metric which can only be calculated through the usage of extra information from other nodes. Note that a distributed channel selection might use an internal (eg. RDT) or external metric (eg. Y-MAC), while a centralized channel selection by definition uses an external metric.

With regards to switching time we also distinguish four different types: single shot, slotted, internal triggered and external triggered. Single shot means that a node selects a channel at start up, and afterwards stays operating in that channel. A Wi-Fi client that can only connect to one Access Point (AP) is a typical example. In contrast, a Wi-Fi client that is able to connect to multiple APs on multiple frequencies may have a trigger causing it to switch to another AP, e.g. insufficient link quality from current AP, AP with higher received signal strength, etc. We call this approach internal triggered switching time. When the trigger is coming from another device then we call it an external trigger. A typical slotted example is Bluetooth, wherein on every slot boundary all nodes switch simultaneously to another channel.

At first glance at least one type of multichannel protocols does not fit inside this taxonomy, namely Frequency Division Duplex (FDD) based protocols, of which a typical example is a regular cellular phone. In these protocols the transmit frequency and the receive frequency are different, therefore seemingly not fitting the taxonomy. However, we simply separate the transmit and the receive channel selection, and both will again adhere to any of the time-frequency behaviors of our taxonomy. Hence a cellular phone connected to one base station has a single shot follow the master time-frequency behavior for the receiver as well as the transmitter, although they operate on different channels. Moreover, there are other protocols which use a different behavior for transmit and receive time-frequency

behavior. For example Receiver Directed Transmission (RDT) [2.17] uses a triggered follow the master behavior for transmitting packets, and a triggered metric based channel selection for receiving packets.

In [2.29] A. Nasipuri et al. propose a multichannel protocol which tries to minimize the collisions between Wi-Fi nodes. This protocol determines the communication channel by assessing channel state before transmission. It remains on the current channel when it is free or hops to another channel when it is busy. The receiving nodes do not need to know the transmit channel, for they are continuously listening on all available channels. Hence for the transmit side this is an internal triggered switching time with an internal metric based channel selection. For the receiver this approach falls into the follow the master approach with an internal trigger, since the receiver does not need any information from the transmitter. S. Wu et al.[2.28] propose to select the communication channel based on a usage list, which is updated through RTS/CTS like packets on a dedicated common control channel. Reliable communication on the control channel is guaranteed by employing two transceivers. One transceiver is dedicated to the control channel, while the other is solely used for data communication. Hence the dedicated control channel is using a single shot follow the master approach, while the data communication is using an internal triggered switching time with an external metric based channel selection.

The operating principle of RDT is illustrated in Figure 2.5. It separates the receive and transmit channel. Every node selects its own receive channel based on some metric. If it wants to transmit to another node, it does so on the receive channel of the destination. Hence it switches its channel to the receive channel of the destination, transmits a packet, and returns to its own receive channel. In [2.17], RDT is proposed as a way to improve throughput. We, on the other hand, focus on its usage as an interference avoidance mechanism. In addition, we propose concrete mechanisms for selecting channels and for exchanging channel information between nodes which are not tackled in [2.17].

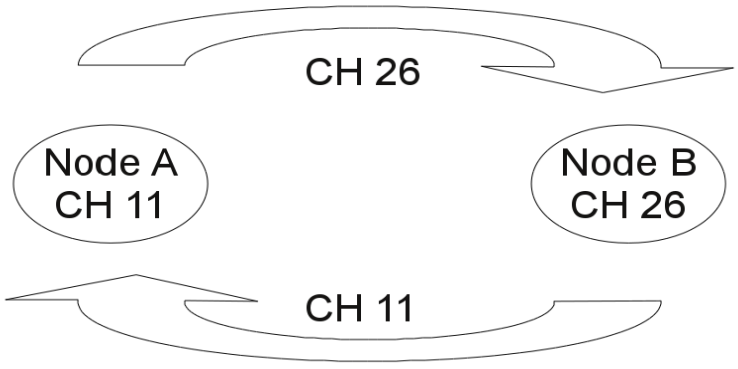

Figure 2.5: The Receiver Directed Transmission operating principle

A number of protocols depicted in Figure 2.4 are not yet discussed. However, discussing all of the available protocols is out of scope of this paper.

2.3 Taxonomy based Interference Avoidance analysis

The protocol taxonomy together with the basic understanding of the interference environment allows us to compare and predict the interference avoidance performance of the different protocol classes.

We start of by determining the most suited channel selection mechanism. Out of the interference measurements we conclude that there is no single channel available across the full length of the building. Hence we can discard protocols which make all nodes operate on a single channel, which in our taxonomy fall in the follow the master class. During the daytime experiments we can clearly see that a large amount of channels receive a significant amount of interference. Therefore a (pseudo) random approach, which essentially averages the packet loss incurred on each individual channel, will not perform as required. Protocols based on an external metric risk losing connectivity, as interference might become active, disconnecting one or more nodes from the network. In this case it might not be possible to negotiate a new operating channel since the channel selection depends on communication with one or more other nodes. An effective interference avoidance protocol must allow the nodes to select channels in a distributed fashion, according to the local conditions without the requirement to exchange data with neighboring nodes. In our Taxonomy this is called internal metric based channel selection.

We now focus on selecting the most promising switching time mechanism. Interference characteristics are dynamic over time. This conclusion is evident in the home/office environment, where people move around with their Wi-Fi enabled laptops and smartphones, and is also apparent from the comparison of daytime and nighttime measurements in Figures 3 and 4. Due to the dynamism we can predict that all single shot based protocols can result in a sudden drop in reliability. The single shot class should hence be avoided. A slotted channel selection requires a node to select a new channel every predetermined interval. It needs to select a new channel even when the interference characteristics remain optimal on the current channel, resulting in a performance drop. A slotted switching time is therefore not desirable. An effective protocol must allow nodes to determine their own switching time according to changes in their own local environmental conditions, which in our Taxonomy is referred to as triggered switching time. Moreover, nodes must be allowed to trigger a channel switch independently of other nodes and any ongoing communication with them. Hence we predict that an internal trigger based switching time will result in the most promising performance.

Hence we conclude that an internal trigger based switching time, combined with an internal metric based channel selection will most likely achieve best

performance with regards to cross-technology interference avoidance. This conclusion is marked by a red circle in Figure 2.4.

We now move on, to identify the roles of different nodes. The Signal to Interference plus Noise Ratio (SINR) at the receiver determines the Bit Error Rate of the transmission. The receiver should therefore be operating in the channel with the least interference. Hence we forecast that RDT[2.17] will most likely be the best candidate for avoiding interference.

In the following section we will experimentally compare the internal metric based channel selection mechanism with (pseudo) random hopping and single channel interference avoidance to verify the conclusions.

2.3.1 Experiment based multichannel mechanism comparison

The taxonomy presented in Figure 2.4 facilitates comparing the channel selection classes with respect to their ability to avoid interference. Within this section we experimentally compare the performance of the different channel selection mechanisms on the iMinds w-iLab.t testbed using IEEE 802.15.4 based tmote sky sensor nodes [2.9]. This testbed is located in an office building where we cannot control the Wi-Fi traffic of the regular office users. However, during night-time the office is empty and hence the level of background interference – which is primarily caused by beacons from idle Wi-Fi AP's – is relatively low.

For all tests we selected a subset of nodes in one floor of the building that are aligned along the length of the building, as depicted in Figure 2.6. This selection achieves a low average ZigBee packetloss (:=PER_Z) between all nodes when there is no interference. We also selected 3 nodes to behave as Wi-Fi interferers on different channels, in order to emulate real-life Wi-Fi network traffic. In all tests all ZigBee nodes send an equal number of packets to all nodes.

Experiments were performed in three different interference scenarios, as follows:

BackGround interference (BG): in this scenario experiments are performed at night-time, and no extra interference is generated. Hence only background interference created by the idle AP's is present

Emulated Wi-Fi interference (4.6 and 22.2Mbps): in this scenario experiments are also performed at night-time, but extra controlled Wi-Fi traffic is generated by the Wi-Fi interferers in 3 different channels, as shown in Figure 2.6. The 3 Wi-Fi interferers are 802.11g devices that operate at a physical layer speed of 54 Mbps and a MAC payload of 1240 bytes. The different scenarios represent different requested packet rates: 4.6Mbps = 471packets/s = 10% of maximum theoretical achievable throughput), 22.2 Mbps = 2220packets/s = 55 % of the maximum theoretical achievable throughput. The transmit power of these devices is 10dBm.

Real life interference (uncontrolled Wi-Fi): in this scenario experiments are performed at daytime during office hours. Real life Wi-Fi traffic is generated only

by the regular office users and interferes with the ZigBee traffic of the experiment. Hence we cannot control the loads on any of the Wi-Fi devices.

Figure 2.6: The RDT test set-up with ZigBee nodes and Wi-Fi interferers

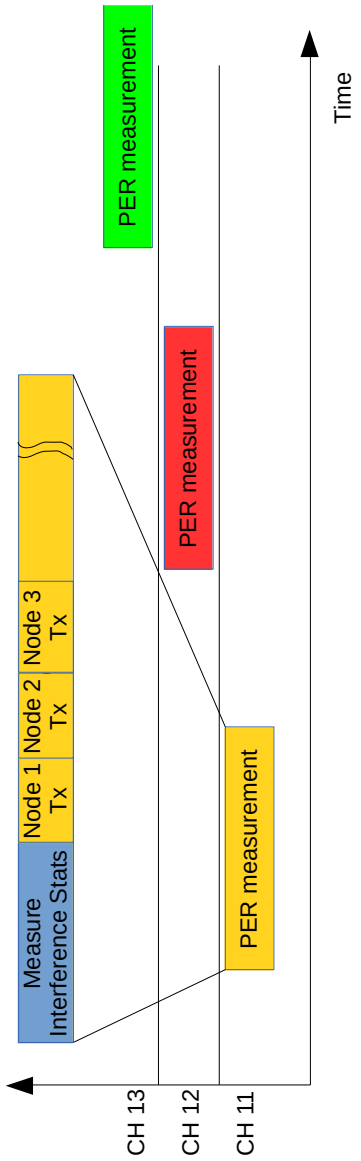

Figure 2.7: The benchmark measurement sequence

In order to compare the performance of the different channel selection mechanisms we create a benchmark of the environment, depicted in Figure 2.7. Such a benchmark experiment is executed in all different interference scenarios. We collect link characteristics like PER, received signal strength, received

interference, etc. between all nodes for all channels. This allows not only an easy comparison of the potential of the different channel selection mechanisms, but also the potential of specific metrics by emulating their operation 'a posteriori'. The benefit of this approach is that different protocols and metrics can be analyzed based on an identical underlying set of measurements, facilitating comparability of the results. The downside is that we cannot compare triggered channel selections using this approach.

At the beginning of every experiment all nodes tune to the first channel, channel 11 and measure the cross-technology interference – separating Signal and Interference in accordance to section 2.4.3 with a sample rate of 1/500µs during 10s. Statistics such as the minimum, average and maximum interference+noise levels as well as a histogram of the measured power levels with 2dB class width are collected. After the completion of this phase each node broadcasts 1000 packets of 125 bytes at intervals of 12ms, and all nodes report the Packet Error Rate (PER_Z) for that sender. Once all nodes have completed their transmissions, they all switch to the next channel, and the same sequence is repeated. This is done for all ZigBee channels (11-26).

Figure 2.8 shows the average PER_Z for a subset of channels in the different interference scenarios. It shows that real life interference results in a high amount of packet loss. The background packet loss is significantly lower, since the office space is abandoned. Table 2.1 is an aggregation of the measured statistics of the PER_Z between all pairs of nodes in all channels.

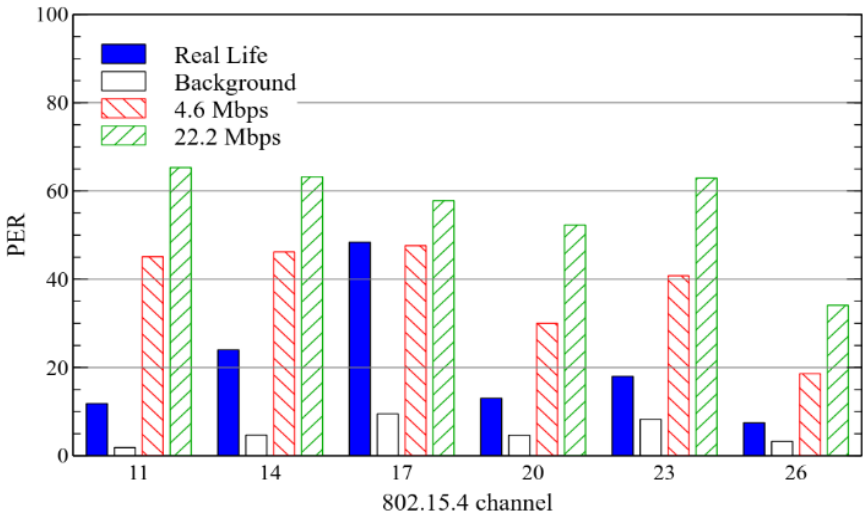

Figure 2.8: Average PER_Z across all nodes for all channels and different interference scenarios. X-axis = ZigBee channel, Y-axis = PER_Z (%)

We compare three different channel selection mechanisms namely follow the master (single channel), random (Bluetooth like) and internal metric based (RDT) with a single shot switching time. The internal metric based approach allows every node to select its receive channel individually based on a metric.

The results are summarized in Table 2.1 which shows the average PER across all nodes, as well as the average PER at the worst node. This worst node metric is important for the correct functioning of the full network. A single node with a high PER might not be able to deliver the needed QoS, resulting in application failure. A network which has a low average PER might therefore still be unable to support its application.

Protocol		Real Life	Background Interference	4.6 Mbps	22.2 Mbps
Best internal metric	Avg	6.87	0.46	16.22	24.37
	Worst	19.92	2.25	53.36	86.35
Best follow the master	Avg	7.43	1.04	18.18	33.91
	Worst	22.55	2.68	53.36	95.33
Random hopping	Avg	21.66	3.83	39.38	57.61
	Worst	30.52	7.21	71.02	94.81
Worst follow the master	Avg	54.52	7.16	47.47	67.20
	Worst	77.58	15.52	85.49	98.76
Worst internal metric	Avg	70.2	9.51	59.30	82.73
	Worst	80.6	15.52	92.95	98.76

Table 2.1: PER_Z Comparison between interference avoidance mechanisms based on the benchmark experiments. The best is highlighted

Table 2.1 shows that the lowest PER can be reached with an ideal internal metric based approach when all channel information is known. The best follow the master selection is second best. In real-life, background interference, 4.6Mbps and 22.2Mbps scenarios, there is an average increase of respectively 8%, 126%, 12% and 39% in comparison to best internal metric based. Moreover, PER at the worst node is on average 29% higher than with the best internal metric. Random hopping is an approach which is not dependent on any channel selection metric for it hops in a random fashion across all used channels. As a result it will average the PER of all used channels at every node, and hence never perform worse than the worst single channel, nor better than the best single channel. In contrast, a bad channel selection metric can potentially result in a worst case channel selection which can happen with both other protocols. Pseudo random hopping with blacklisted channels – e.g. Bluetooth 2.1 – can reduce the packet loss in comparison to regular

pseudo random hopping. However, it will never improve upon the results of the best single channel as the whole network is always operating on one channel at any given moment. The worst follow the master solution obviously performs badly, followed by the worst internal metric based channel selection which does it even worse. We can therefore conclude that a solution based on an internal metric is the most promising protocol, although the metric itself is crucial. For that reason we will go in depth on the selection of an internal metric for RDT in section 0.

2.4 Interference Avoidance with RDT

2.4.1 RDT runtime metric comparison

The metric that we want to optimize is the total average Packet Error Rate in the ZigBee network. In RDT every node selects its own receive channel, and would ideally make this selection so as to minimize the average PER across all individual nodes. This minimum is reached when each individual node selects the channel with the least average PER. Determining the best channel could hence be achieved through measuring PER on all channels and selecting the best one. However, a reliable PER assessment requires a statistically relevant number of packets per pair of nodes on all channels, incurring a high amount of overhead traffic and no timely channel ranking. For practical implementation a metric that can be measured instantaneously is preferred. Therefore instead of measuring PER we try to build a channel ranking at runtime by measuring the interference levels on the different channels. Such a measurement, further referred to as a channel scan, samples the channel power for some time and calculates metrics from the collected samples.

A number of common metrics based on channel scans exist. We compare the performance of RDT when it uses these different channel selection metrics based on the link statistics and channel scan information collected during the same experiments which resulted into Table 2.1. An overview of PER for all considered metrics in all scenarios is shown in Table 2.2.

The ‘ideal PER’ metric selects the channel with the least amount of PER, and hence results in the ideal channel selection. Hence we will always compare the performance of a metric with this metric.

The ‘min’ metric selects the channel where the minimal measured channel power is lowest as receive channel. Selecting the minimal measured channel power essentially results in measuring the radio’s noise floor. We have selected the nodes in order to have sufficient link budget. In other words the received signals are sufficiently above the noise floor of the radio and hence this is not a good metric. In the real-life scenario the resulting PER is increased by a factor 3.9 in comparison to the ideal PER metric.

The ‘max’ metric selects the channel where the maximal measured channel power is lowest. This metric will avoid channels with high measured interference levels, independent of the load this interference level has. This leads to a good channel selection in case interference load is identical across all channels. Such an environment can be found in the background interference scenario, where it achieves identical performance as the PER metric. However, in the emulated interference and especially in the real-life interference its performance drops drastically, where the average PER is increased with a factor 1.7 in comparison to the ideal PER metric.

The ‘avg’ metric selects the channel with the lowest average measured channel power. Therefore, this will combine the effect of the interference power level and its load. As a result we get fairly good performance under most circumstances. However, as can be seen in the worst node comparisons, some nodes select a less than optimal channel, which can be improved. The real-life PER is a factor 1.3 higher in comparison to the ideal PER metric.

The ‘activity’ metric is a metric proposed in [2.23]. They propose to use metric (2.1), and select the channel with the lowest ‘activity’.

$$Activity = 100 \times \frac{avg - min}{max - min} \tag{2.1}$$

With min, avg and max the minimum, average and maximum measured channel power level. This metric achieves good performance under most scenarios. It improves upon the avg metric with 7% in the real life scenario. However, the PER achieved is still a factor 1.23 higher than with the ideal PER metric.

Metric		Real Life	Background Interference	4.6 Mbps	22.2 Mbps
Ideal PER	Avg	6.87	0.46	16.22	24.37
	Worst	19.92	2.25	53.36	86.35
min	Avg	26.85	6.30	39.40	56.79
	Worst	76.35	15.52	75.89	88.76
max	Avg	11.87	2.32	25.90	32.39
	Worst	22.58	9.51	72.28	95.33
avg	Avg	9.11	2.40	23.87	36.15
	Worst	28.26	9.51	72.28	95.33
Activity [2.23]	Avg	8.48	2.45	31.62	46.12
	Worst	24.94	7.20	72.28	95.33

Table 2.2: PER_Z for common channel selection metrics based on the benchmark experiments

Out of this comparison we conclude that the Activity metric is the best metric up to now. However, this metric results in a 1.23 times higher average PER in the real-life case than the ideal PER metric. Therefore we create a new metric which comes closer to the performance of the ideal PER metric.

2.4.2 Building a new RDT metric

We assume that the link budget of all transmitters is sufficiently high to guarantee negligible packet loss if no interferer is active. Moreover, for the sake of simplicity we assume that no packet errors are caused by collisions between ZigBee packets.

In this paper we focus on the interference of Wi-Fi to ZigBee. The Clear Channel Assessment (CCA) of Wi-Fi, when configured to energy based CCA, may cause Wi-Fi to backoff for ZigBee under specific scenarios. However, typical Wi-Fi cards do not backoff for ZigBee at all because they implement preamble based CCA [2.5]. Hence the stochastic arrival processes of Wi-Fi packets from all Wi-Fi interferers are independent of any ZigBee activity, and we assume them to be identically distributed.

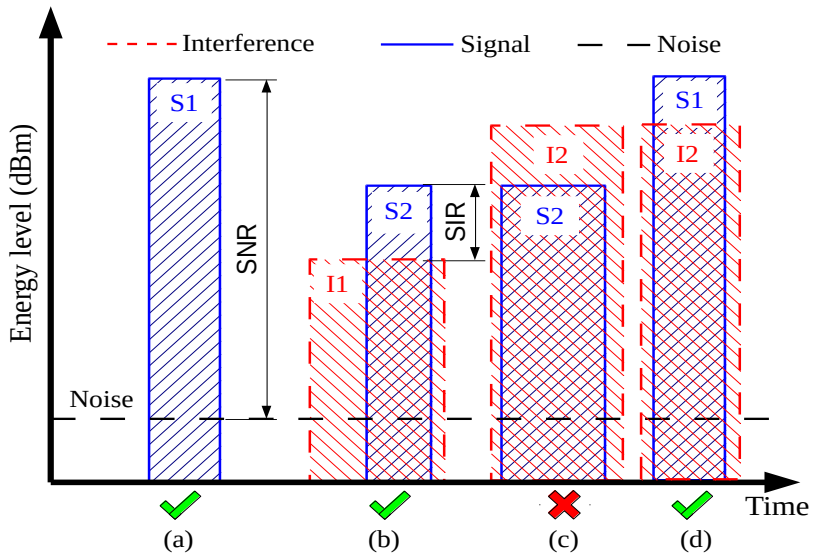

Figure 2.9: Different interference scenarios

Figure 2.9 part (a) shows that a packet that does not collide with interference is received with a sufficiently high SNR, resulting in a negligible PER. In (b), the packet is interfered by interference level I1. The BER across the full packet in this

case depends on the Signal to Interference Ratio (SIR) between received signal strength 2 (S2) and Interference signal strength 1 (I1). I1 is received at low energy, resulting in a sufficiently high SIR, which we assume allows this packet to be received correctly with high probability. Case (c) depicts a collision between S2 and the stronger received interference I2, resulting in a low SIR and hence a low probability of successfully receiving the packet. In case (d) the signal has level S1, which is sufficiently above I2 to be successfully received with high probability. We conclude that when a specific packet is interfered, its successful reception depends on the signal levels of the transmitter and the interference at the receiver.

The PER as result of a specific SIR equals the expected packet error rate given a collision with this SIR multiplied by the probability of this SIR occurring. The total expected PER of a single receiver – transmitter pair *(:=E(PER(R,T)))* can now be written as (2.2).

$$\mathrm{E}\big(PER(R,T)\big) = \int PER(s)\,\Pr(s)\,ds \qquad (2.2)$$

With s the received SIR, and Pr(s) the probability distribution of SIR.

Out of [2.10] we calculate the ZigBee PER versus SINR, depicted in Figure 2.10.

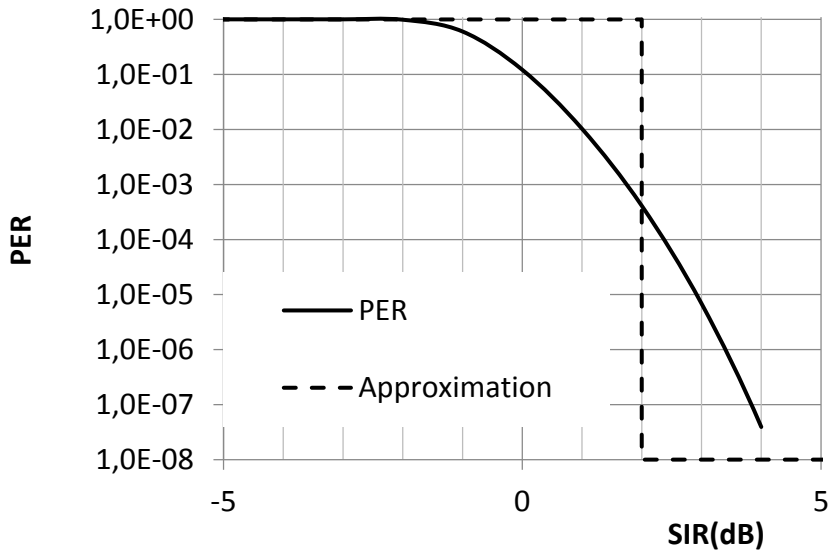

Figure 2.10: PER for 100 byte ZigBee packets

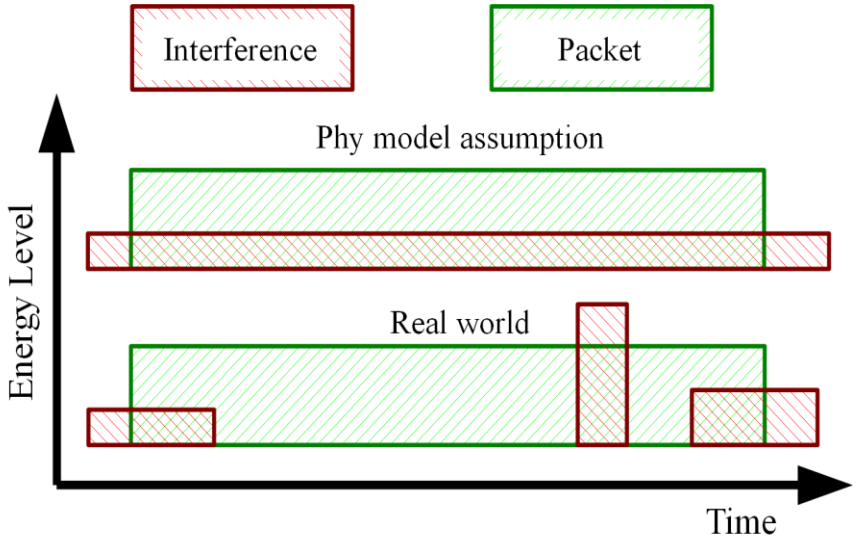

Figure 2.11: Physical model assumption versus real-life cross-technology interference

Figure 2.10 shows that the difference in SINR between 0.01% packet loss and 10% packet loss is 3dB. In order to simplify our model we neglect this 3dB and approximate PER_Z as a step function dependent on the SIR (2.3). Below the threshold which we set at 2dB, *E(err|coll)* = 1, above the threshold the *E(err|coll)* = 0. Note that in [2.13] Maheshwari et al. show that in an intra-technology interference context the usage of a full PER calculation is more accurate than a PER approximated by a threshold. The interference in both [2.10] (theoretical model) and [2.13] (empirical model) is fully overlapping with the packets. However, in a cross-technology case this assumption is not necessarily valid since the interference might only partially overlap with a packet, as depicted in Figure 2.11. Hence we cannot conclude to which extent the thresholding approximation impacts the accuracy of PER in the cross-technology case. Although the threshold-based approximation may be less accurate, it is the preferred model in view of implementation complexity since it allows a simple binary decision.

$$PER(s) = \mathrm{H}(s - Th_{SIR}) \tag{2.3}$$

With H(x) the Heaviside step function and ThSIR the SIR threshold for good reception which we set at 2dB for this results in less than 0.1% packet loss. Formula (2.2) can now be written as (2.4).

$$\mathrm{E}\big(PER(R,T)\big) \approx \int_{-\infty}^{Th_{SIR}} \Pr(s)ds \tag{2.4}$$

SIR equals to Signal strength minus Interference strength in logarithmic scale, leading to (2.5). Formula (2.5) depicts that the packet loss on a link can be estimated by assessing the probability that the interference power at the time of packet transmission is higher than the signal power minus a threshold. We want to stress that in this formula S is relatively static, while I is very dynamic. Therefore the time behavior of the sum of all interferences determines the estimated PER.

$$\begin{aligned} \mathrm{E}\big(PER(R,T)\big) &\approx \Pr(S - I \le Th_{SIR}) \\ &\approx \Pr(I \ge S - Th_{SIR}) \end{aligned} \tag{2.5}$$

We can measure the received signal strength for each transmitter. Hence creating a histogram of the interference power levels allows us to assess this probability, and thus estimate PER. Figure 2.12 depicts the histogram of the measured power levels on channels 14 and 26. From this histogram we can easily estimate PER for any values of R and T.

The best receive channel is the channel where the average weighted expected PER of all neighboring nodes is lowest (6).

$$\mathrm{E}\big(PER(R)\big) \approx \frac{\sum_{i=1}^{N} \alpha_i \times \mathrm{E}\big(PER(R,T)\big)}{\sum_{i=1}^{N} \alpha_i} \tag{2.6}$$

With α_i the weight on the estimated PER of a specific transmitter. Within the experiments we assume the weight of all transmitters to be identical. We denote *E(PER(R))* of (2.6) as the Received Signal to Interference Strength based Thresholding (ReSIST) metric.

During startup a node does not know the received signal strength of its neighboring nodes. As a consequence we cannot rely on the ReSIST metric since no received signal strengths are known. Therefore we bootstrap the channel selection by assuming a fixed received signal level from all nodes. A signal strength of 10dB above the receivers noise floor can be reached by every node within about 1/3rd of the maximum communication range. Hence we set the threshold at 10dB above noise floor as it allows a normal operation of the network in most circumstances. Within the remainder of this paper we refer to this metric as the Fixed Threshold (FiT) metric.

2.4.3 IEEE 802.15.4 transceiver based interference assessment

In the previous section we elaborated on the theory how to determine the best channel through interference power measurements. In real-life, the channel power measurements are not perfect. More specifically, 1) the power measurements include interference as well as signal and noise, while these should be separated in order to assess the resulting PER and; 2) the channel sample times are not necessarily small compared to the Wi-Fi packet length. We will now determine the effects of, and solutions to these non-ideal measurements.

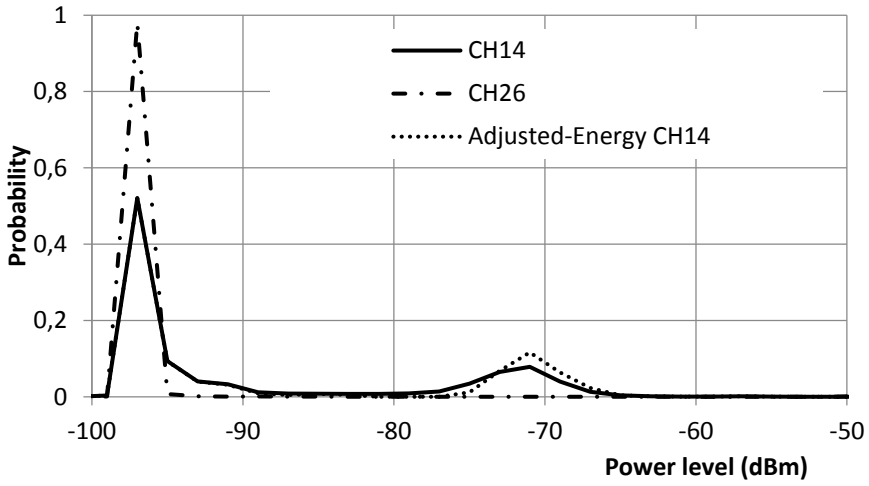

Figure 2.12: Probability density function (histogram) of the measured interference power for different ZigBee channels

	ZigBee	Wi-Fi
MAC frame size (bytes)	100	1278
Datarate	250Kbps	54Mbps
Packet-time (µs)	127b: 4256 100b: 3392 50b: 1792 5b: 352	1Mbps: 10416 11Mbps: 1121 54Mbps: 212
T_{CCA}(µs)	128	4

Table 2.3: Default parameters used

1) A regular ZigBee radio can return the power measured in the current channel in accordance with the IEEE 802.15.4 standard [2.10]. This measured power equals the sum of Signal + Interference + Noise. Within this work we neglect noise for we assume it does not result in packet loss. However, we still need to separate Signal from Interference. Two approaches can be identified. a) We can make certain that no signal is present during the power measurement. However, this implies not only that the network cannot operate during channel assessment times, but also that all 802.15.4 devices are under our control. b) We can separate signal samples from interference samples during execution of a channel scan. This can be achieved by using the preamble detection functionality of the radio. More specifically, the CC2420 radio used on the Tmote Sky can be configured to perform CCA based on either measured power level, or ZigBee preamble detection. Before starting a channel scan, we configure the CCA mode to ZigBee preamble detection. Before and after each power measurement we check if the radio assesses the channel as busy or not, and drop the measurement if any of the checks is positive. The remaining samples will predominantly contain only interference and noise.

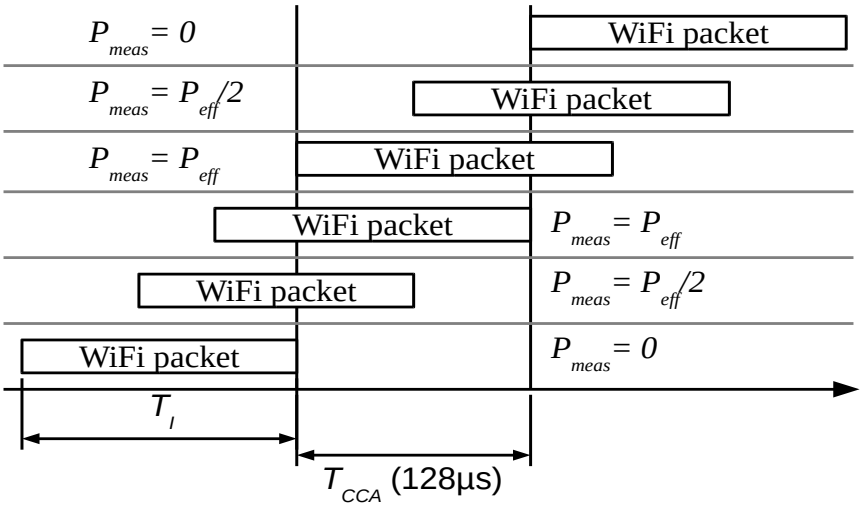

Figure 2.13: The measured versus effective in band power

2) The channel sample time of ZigBee equals 128µs (to be denoted T_{CCA}), and the measured power is averaged across this window. A Wi-Fi packet lasts between 28µs and 12.4ms. However, in sake of simplicity we initially assume all Wi-Fi packets last at least 128µs. The measured power in a sample will deviate from the effective interference power in case an interference signal starts or ends during the measurement window, as depicted in Figure 2.13. Assuming the start and end of

the interference is independent with respect to the start and end of the measurement window results in a uniform distribution of the overlap between measurement window and Wi-Fi interference.

The total timeframe where Wi-Fi packet energy is measured equals T_I+T_{CCA}. The sample will result in the effective signal power only when the CCA window fully overlaps with the Wi-Fi packet therefore removing $2*T_{CCA}$ from the total timeframe. (2.7) calculates the probability of a sample returning the effective interference power for a fixed interference length.

$$\Pr(P_{meas} = P_{eff}) = \frac{T_I - T_{CCA}}{T_I + T_{CCA}} \tag{2.7}$$

With P_{meas} the measured interference power, *Peff* the real interference power, T_I the interference packet length and T_{CCA} the measurement time.

Hence the remaining part of the measurements $(1-Pr(P_{meas}=P_{eff}))$ will result in lower measured interference power. Figure 2.14 depicts the resulting deviation of the measured power histogram with a class width of 2dB for different interference packet lengths.

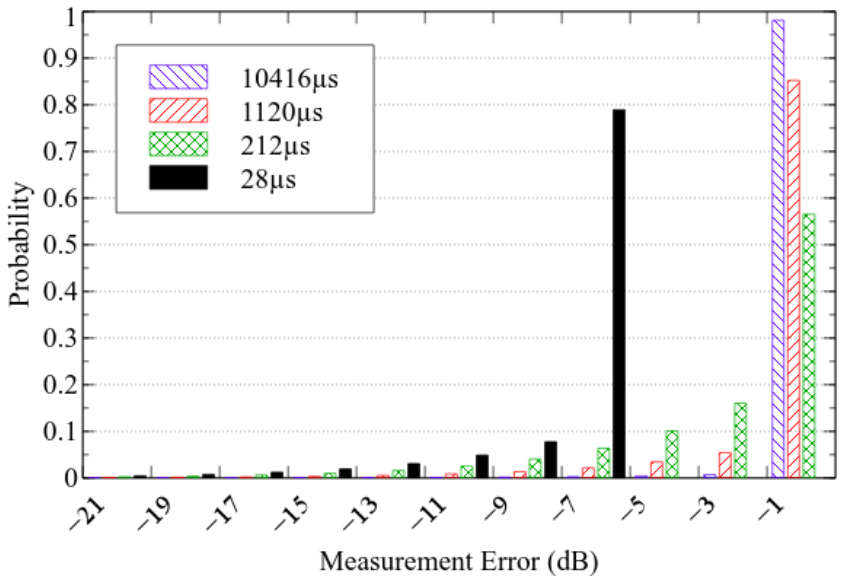

Figure 2.14: Measurement error due to the long measurement window for different Wi-Fi packet lengths for a classwidth of 2dB

For example, Figure 2.14 shows that 57% of all measurements of 212µs long interference packets will deviate less than 1dB from the effective spectral power. Hence, 57% of the measurements will be captured inside the correct class. 16% will be between -1 and -3dB – or one class lower –, 10% between -3 and -5dB, etc. For the smallest (28µs long) Wi-Fi packets, no measurement will result in effective interference power since the interference is shorter than the measurement window. In fact all measurement results are at least 6.6dB (=10*log(28µs/128µs)) lower than the effective power.

The measurement error for a specific interference packet length can now be compensated for, to determine the actual interference power histogram. Starting from the highest class, the effective amount of samples that should have been inside this class can be calculated. Eg. 57% of the effective samples for 212µs interference lengths are actually measured in this class. Therefore 1/0.57 times the number of samples measured in this class equals the effective number of samples, which an ideal measurement will measure. Now, the amount of samples that are measured in the lower classes – due to the long sample window – can be calculated, and consequently removed from the respective lower classes. This calculation can be repeated recursively for all classes. We refer to the channel selection metric that is based on these adjusted energy measurements as Adjusted Energy ReSIST (AE-ReSIST).

A plot of adjusted energy measurements of channel 14 is added in Figure 2.12. It is clearly visible that the peak around -71 dB becomes higher, and the spill out in the lower classes is reduced leading to a more accurate measurement. The downside is that we assume a specific fixed packet length, and hence introduce errors if this assumption is not correct. Moreover the interference packet lengths will in general have a certain distribution which is not accounted for. However, future work could estimate this distribution by eg. machine learning techniques, exchange of Wi-Fi packetlength statistics between Wi-Fi and ZigBee, etc.

2.4.4 Proposed metric comparison

In this section we compare the performance of the three metrics proposed in section 0 namely FiT, ReSIST and AE-ReSIST.

FiT – Fixed Threshold based interference classification (without using received signal strength information) – selects the channel with the lowest FiT cost, and improves upon all other metrics except in the background interference case. The real-life interference case results in an average PER a factor 1.13 higher than with the PER metric.

ReSIST – Received Signal and Interference Threshold based interference classification (with received signal strength information) – improves upon the performance of FiT in all scenarios. It results in a factor 1.07 higher PER than with the PER metric in the real life scenario, which is small. However, the worst case

PER is usually different from the worst case of the PER metric. This is most likely due to other effects than Wi-Fi interference significantly altering the effective link PER between nodes. More specifically we believe this is due to multipath fading, for we observed a high PER between a number of specific nodes (eg. 1 and 4 in Figure 2.6) in the background interference scenario which are physically only 5 meters separated from one another. Out of the channel scans we do not see significant Wi-Fi interference strong enough to create this high level of PER. Therefore multipath fading seems the most logical explanation, although true proof can only be found in a full electro-magnetic analysis of the environment.

Metric		Real Life	Back ground	4.6 Mbps	22.2 Mbps
Ideal PER	Avg	6.87	0.46	16.22	24.37
	Worst	19.92	2.25	53.36	86.35
FiT	Avg	7.74	2.44	23.53	35.82
	Worst	28.26	8.09	72.28	95.33
ReSIST	Avg	7.40	2.03	23.11	31.14
	worst	21.42	9.51	27.28	95.33
AE-ReSIST	Avg	7.40	2.07	23.15	31.27
	worst	21.42	9.51	72.28	97.46

Table 2.4: PER_Z for newly proposed channel selection metrics based on the benchmark experiments. The best is highlighted

AE-ReSIST – Adjusted Energy ReSIST (ReSIST with adjusted energy measurements) – performs identical to ReSIST in the real-life and background scenarios but performs worse in the emulated scenarios, where ReSIST results in the best performance. The lack of improvement is due to the contradictory effect introduced by a model error and a measurement error. The model introduces an error by assuming that the ThSIR is independent of the interferers on-time (ie. The Wi-Fi packet length). However, smaller interferer on-times result in a smaller average overlap between interference and packet (see Figure 2.11), and thus a lower packet loss than predicted. In section 0 we show that the average measured signal level of the interference reduces with smaller interference on-times. Hence the model overestimates the impact of smaller interference on-times, while the measurements, which serve as input to the model, underestimate the signal level of the interference for smaller packets, partially negating the overestimation the model makes. By reducing the measurement error we remove the overestimation of the smaller interference on-times but keep the overestimation the model makes, increasing the total error. Therefore an improvement is to be expected only when correcting the measurement error as well as the error in the packet loss model.

However, building a precise cross-technology packet loss model of which the parameters can be determined in a real-life scenario requires an in-depth study of the overlap between interference and the packet in a real-life environment, which is out of scope of this paper.

2.5 TinyOS based implementation on TMote Sky hardware

2.5.1 Information Dissemination Mechanism

A packet can be received only if it is transmitted on the quiescent channel of its destination(s). The easiest way to achieve this is to transmit the packet on all channels. However, this multiplies the needed amount of transmissions and thus wastes battery power and creates additional interference. To avoid multichannel transmissions it is necessary to inform the transmitter of the quiescent channel of the receiver.

We select two different mechanisms for distributing quiescent channel information to the surrounding nodes. The first mechanism is to periodically broadcast this information on all channels. This mechanism has the advantage of making sure that all nodes in the area are informed, and also serves as a keep alive packet with which the receiving nodes can update their neighbor database in case nodes lose connectivity. However, it is not efficient in terms of energy consumption, time incurred, and spectral usage. The second mechanism is to piggyback receive channel information on messages that are sent to neighboring nodes. This mechanism only costs a few additional bytes inside some of the transmitted packets. When a node decides to switch its receive channel while receiving a stream of packets, it can very quickly notify the sending node by piggybacking its acknowledgments. However, this mechanism cannot guarantee that all surrounding nodes know the quiescent channel.

The combination of both mechanisms overcomes both shortcomings. The periodic broadcasts make sure all surrounding nodes know the quiescent channel of the node. At the same time, piggybacking guarantees that nodes with which the transmitting node actively communicates are updated very quickly.

2.5.2 Implementation Architecture

The protocol is implemented on Tmote Sky nodes running TinyOS 2.1. It was implemented inside the radio driver as this makes it transparent to the higher layers. We have opted for a modular approach of three modules namely RDT control, Channel Assessment and a back-end database. The implementation independent settings – such as enable/disable RDT, allowable channels, channel

scan time, etc. – can be governed by an external interface. The architecture of the implementation is shown in Figure 2.15.

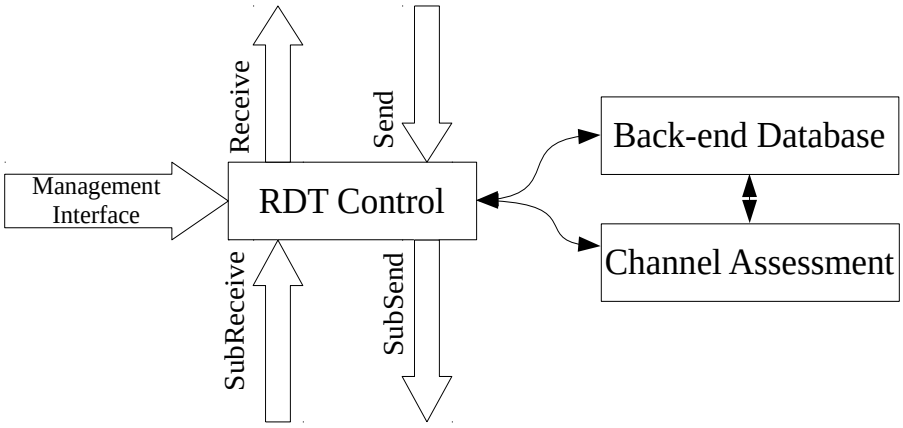

Figure 2.15: RDT implementation architecture

The RDT control module is responsible for the RDT information dissemination and the channel switching. The RDT control module piggybacks a packet with the receive channel given sufficient space is available in the packet. Periodic broadcasts are implemented by sending an empty packet with broadcast destination through the application level active message interface. This packet is then automatically piggybacked since sufficient space is certainly available. The RDT control also switches the radio's channel when a packet needs to be transmitted.

The channel assessment module is responsible for selecting the receive channel of the node and returning the destination channel(s) of a packet. To resolve the receive channel it performs the channel selection algorithm of Section 0 periodically. The channel switching module requests the destination channel(s) of a specific node to the backend-database module. If the receive channel is known, it is returned as a single destination channel. Otherwise, the packet needs to be transmitted on all channels that are in use by the system.

The backend database module stores information regarding the surrounding nodes. Typical information includes receive channel, received signal strength, PER, time since last packet received/transmitted, etc. The receive channel information is used to supply the current receive channel of a node to the channel assessment module. The received signal strength is used to calculate the ReSIST metric. Although PER itself is not used in the protocol, it is used in the executed experiments for reporting purposes. The time since the last packet received or transmitted to a node is used to support mobility of the nodes, and remove stale node data.

2.5.3 Packet Format Specification

Packets are piggybacked by adding extra trailers to the standard active messages created by TinyOS. When a packet is piggybacked, its AMType is overwritten with the RDT AMType of 255, thus allowing the receiver to distinguish between piggybacked packets and non-piggybacked packets.

Two types of piggyback trailers are specified, one for unicast packets and the other for broadcast packets. The format of the unicast piggyback trailer is depicted in Figure 2.16. The minimal trailer consists of the grey parts. These include the original AMType, the original packet length, the quiescent channel, and the transmit power of the packet. The DataType Definition (DaTD) field defines whether extra information is present in the trailer, e.g. measured pathloss. Although the pathloss is unused within this work, this can be used in future work in eg. transmit power adjustment.

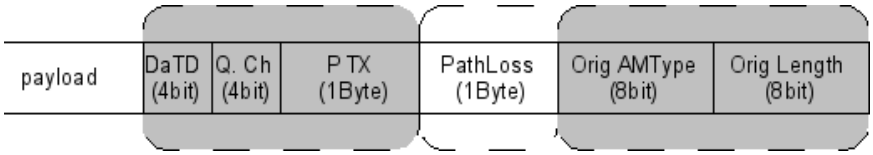

Figure 2.16: Unicast piggyback trailer

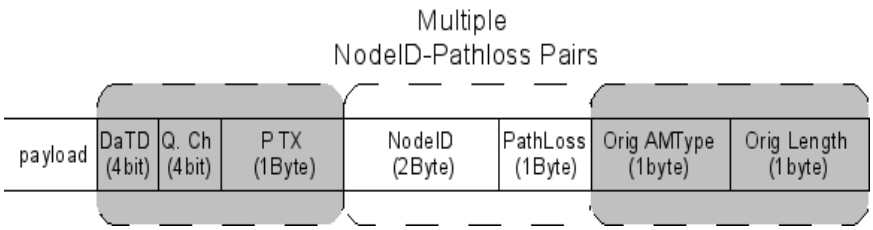

Figure 2.17: Broadcast piggybacking trailer

The format of the broadcast piggyback trailer is depicted in Figure 2.17. It consists essentially of the same information included in the unicast trailer; however since it reaches multiple destinations, specific information such as path-loss measurements for multiple nodes can be placed inside a single packet.

2.5.4 Implementation results

In the online experiments, the RDT protocol implementation is used. Two different settings are used. The first is a single shot channel selection setting. RDT

scans all channels only at the beginning of the experiment, and selects the best channel. No more channel switches are performed during the experiment. This setting allows for comparison between the RDT implementation and the RDT evaluated on the benchmark experiments. The second setting – triggered channel selection – allows RDT to dynamically switch channel selections during the experiment.

The experiments presented in the previous section do not exploit the dynamism of RDT. The benchmarking experiment that is executed lasts nearly two hours, resulting in a database which has average PER across a two hour timeframe. Hence we lose the time accuracy. The real-life implementation is set to scan the current channel every 15s, allowing it to dynamically adjust to changing channel states. In the single shot ReSIST scenario, the initial channel selection is maintained for the full experiment, while in the triggered scenario RDT is allowed to change channels dynamically at runtime.

The results of the triggered ReSIST metric – which are shown in Table 4 – are significantly better in the real-life scenario in comparison to the single shot results. The remaining scenarios are slightly worse than the benchmark based scenarios. This can be explained by the dynamic nature of RDT in a static scenario. Deviations in the measurements might make the nodes hop to a channel with a higher PER for a short time, until it performs another channel scan which is worse than the best channel and it hops back. However, in the real-life scenario the channel states change significantly in comparison to the measurement deviations, resulting in channel hops to channels with better channel states.

Metric	Real Life	Back ground	4.6 Mbps	22.2 Mbps
Single shot ReSIST	8.15	2.12	22.91	32.06
Triggered ReSIST	3.48	2.94	24.83	34.23

Table 2.5: PER_Z of Single shot and Triggered ReSIST based on runtime implementation

2.6 Future work

RDT is capable of coping with dynamic environments given it has relevant state information of all channels. However, a ZigBee node only operates on one channel at a given moment and hence only the state information of the current channel is updated. This has as effect that the state information of the other channels becomes outdated. Updating these channel states can be done by temporarily switching the quiescent channel. However, this might result in a

temporary deterioration of the PER. This trade-off between exploration and exploitation – which can be solved optimally if the problem can be formulated as a multi-armed bandit problem – needs to be considered.

Sensor networks are usually battery powered and therefore energy sensitive. The current RDT implementation does not consider energy saving mechanisms, commonly used in sensor networks. Hence combining RDT with an energy saving protocol is certainly an interesting topic. Moreover, RDT exchanges protocol information – which consumes energy – but also reduces the number of needed transmissions – which saves energy. The channel scan, combined with the pathloss information can also be used for transmit power adjustment. The channel scan information of the receiver can namely be used at the transmitter to determine the expected PER, resulting in minimal transmit power for a requested link PER. We have done an 'a posteriori' comparison of different single shot interference avoidance protocols as well as RDT metrics starting from identical benchmark experiments. Due to dynamism in the environment, a single shot channel selection might not be maintainable across the full lifetime of a sensor network. However, comparing triggered channel selection protocols and metrics is extremely hard because multiple experiments – which are done at different times – are needed. Hence extreme care needs to be taken that we compare the protocols and metrics, and not the difference in the environment. Repeatability and reproducibility of wireless experiments is a hot topic that is addressed today by many researchers. We refer for instance to [2.37]. An in-depth comparison of triggered protocols and metrics thus remains an open issue.

2.7 Conclusion

Coexistence of different wireless technologies is becoming an increasingly limiting factor in achieving the needed QoS with a certain technology. We show through measurements in an office environment that the interference created by Wi-Fi on a ZigBee network is of a dynamic, local nature.

Using our proposed multichannel protocol taxonomy, we conclude that an internal metric based channel selection combined with an internal trigger based switching time is the most suitable packet loss reducing protocol in an office environment. We experimentally verify that an internal metric based channel selection indeed performs best in real life environments. It is able to reduce the average PER with a factor 3.43 and 1.73 compared to (pseudo) random channel selection and the best single channel respectively. However, it can perform worse in case a wrong channel metric is used.

We therefore analyze the performance of commonly used metrics and show that a significant improvement is achievable. Hence, we propose a new metric – called ReSIST – and experimentally verify its operation. We show that our channel metric reduces the average PER with a factor 3.63, 1.60, 1.23 and 1.14 in

comparison to respectively min, avg, max and activity [2.23] channel metrics in real-life cases. We also verify that our channel metric degrades with 7.7% compared to the situation where we have full channel information. Therefore we proposed an improvement to ReSIST which reduces the measurement error incurred by IEEE 802.15.4 based channel assessments. However, we concluded that the performance did not improve as expected, as we reduce only one out of two contradictory errors, explained in depth in section III.D. Finally, we verified our implementation of triggered ReSIST – which is able to switch channels dynamically at runtime – and conclude that in the real-life case a PER reduction with a factor 2.34 in comparison to a single shot channel selection is achievable.

2.8 References

[2.1] M Meekers, S Devitt, L Wu, "Morgan stanley internet trends 04/12/2010", Morgan Stanley Research 2010, http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, Accessed 15 Feb. 2012

[2.2] Bin Zhen, Huan-Bang Li, Shinsuke Hara, and Ryuji Kohno, "Clear channel assessment in integrated medical environments," in EURASIP JournalOn Wireless Communication Networks 2008, Article 48 (January 2008), 8 pages.DOI=10.1155/2008/821756 http://dx.doi.org/10.1155/2008/821756

[2.3] G. Thonet, P. Allard-Jacquin, P. Colle, "ZigBee – Wi-Fi Coexistence White paper and Test Report," [online], Available: www.ZigBee.org

[2.4] Wei Yuan, Xiangyu Wang, Linnartz, J.-P.M.G. , "A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g," Communications and Vehicular Technology in the Benelux, 2007 14th IEEE Symposium on,pp.1-5, Nov. 2007, doi: 10.1109/SCVT.2007.4436237 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4436237&isnumber=4436227

[2.5] S. Pollin,I. Tan,B. Hodge,C. Chun,A. Bahai, "Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study," Cognitive Radio Oriented Wireless Networks and Communications (CrownCom) 2008 3rd International Conference on, pp.1-6, May 2008, doi: 10.1109/CROWNCOM.2008.4562460. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4562460&isnumber=4562434

[2.6] C.M. Liang, N.B. Priyantha, J. Liu, A. Terzis, "Surviving Wi-Fi interference in Low Power ZigBee Networks", in proocedings of SenSys '10, pp. 309 - 322, november 3-5, Zurich, Switzerland, 2010

[2.7] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, P. Demeester, "Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment", EURASIP Journal on Wireless Communications and Networking 2012, 2012:137 doi:10.1186/1687-1499-2012-137

[2.8] J. Huang, G. Xing, G. Zhou and R. Zhou, "Beyond co-existence: Exploiting Wi-Fi white space for ZigBee performance assurance.", In Proceedings of the The 18th IEEE International Conference on Network Protocols (ICNP '10). IEEE Computer Society, Washington, DC, USA,

305-314, 2010 DOI=10.1109/ICNP.2010.5762779 http://dx.doi.org/10.1109/ICNP.2010.5762779

[2.9] TMOTE SKY datasheet, online: http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf, Accessed 06 Aug. 2012

[2.10] IEEE Std. 802.15.4 — 2006, IEEE Standard for Information Technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), Sept. 2006.

[2.11] IEEE Std. 802.11 — 2012, 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

[2.12] IEEE Std. 802.15.1 — 2005, IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)

[2.13] R. Maheshwari, S. Jain, and S. R. Das, ”A measurement study of interference modeling and scheduling in low-power wireless networks.”, In Proceedings of the 6th ACM conference on Embedded network sensor systems (SenSys '08), New York, NY, USA, 141-154. DOI=10.1145/1460412.1460427, 2008

[2.14] L. Tytgat M. Barrie, V. Gonçalves, O. Yaron, I. Moerman, P. Demeester, S. Pollin, P. Ballon, S. Delaere, “Techno-economical Viability of Cognitive Solutions for a Factory Scenario,” 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp. 254-264, 3-6 May 2011

[2.15] M. Barrie, L. Tytgat, V. Gonçalves, O. Yaron, I. Moerman, P. Demeester, S. Pollin, P. Ballon, S. Delaere, “Techno-Economic evaluation of Cognitive Radio in a Factory Scenario,”in proceedings of Perfomance Evaluation of Cognitive Radio Networks (PE-CRN) 2011, 9-13 may 2011.

[2.16] A.W. Min, K. Kim, K. Shin, “Robust cooperative sensing via state estimation in cognitive radio networks,” in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 185 – 196, 2011

[2.17] Shacham N.,King P.: "Architectures and performance of multichannel multihop packet radio networks.", IEEE Journal on Selected Areas of Communication, JSAC-5(6):1013{1025, 1987

[2.18] R. Balamuthi, H. Joshi, C. Nguyen et al., “A TV White Space Spectrum Sensing Prototype”, in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 297 – 307, 2011

[2.19] P. Van Wesemael, S. Pollin, E. Lopez, A. Dejonghe, “Performance Evaluation of Sensing Solutions for LTE and DVB-T”, in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 531 – 537, 2011

[2.20] IMEC (2012 02 6), IMEC sensing engine development [online], Available:http://www.imec.be/ScientificReport/SR2008/HTML/1225000.html

[2.21] Y. Xiao, J. Rosdahl, “Throughput and Delay Limits of IEEE 802.11,” in IEEE communications letters VOL. 6, NO.8 august 2002, PP 355 - 357, 2002

[2.22] S. Shin, H. Park, S. Choi, W. Kwon, “Packet Error Rate Analysis of IEEE 802.15.4 under IEEE 802.11b interference”, in the Third International Conference on Wired/Wireless Internet Communications (WWIC), Xanthi, Greece, 2005

[2.23] Hossian, M.; Mahmood, A.; Jantti, R.; , "Channel ranking algorithms for cognitive coexistence of IEEE 802.15.4," Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on , vol., no., pp.112-116, 13-16 Sept. 2009, doi: 10.1109/PIMRC.2009.5449986

[2.24] Hoi-Sheung; So, W.; Walrand, J.; Jeonghoon Mo; , "McMAC: A Parallel Rendezvous Multi-Channel MAC Protocol," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE , vol., no., pp.334-339, 11-15 March 2007, doi: 10.1109/WCNC.2007.67

[2.25] J. So and N. Vaidya, “Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using a Single Transceiver,”in ACM Mobihoc, May 2004.

[2.26] CREW project – w.iLab.t portal, online: http://www.crew-project.eu/wilabt, accessed may 15, 2012

[2.27] N. Jain, S. R. Das, A. Nasipuri, A Multichannel CSMA MAC protocl with receiver-based channel selection for multihop wireless networks

[2.28] Shih-Lin Wum Chich-Yu Linm Yu-Chee Tseng and Jang-Ping Sheu, A novel MAC protocol with On-Demand Channel assignment for multi-hop mobile ad-hoc networks

[2.29] A. Nasipuri, J. Zhuang, S. R. Das, A Multichannel CSMA MAC Protocol for Multihop Wireless Networks, in Proceedings of Wireless Communications and Networking Conference 1999, p 1402 – 1406 vol. 3, 1999, DOI:10.1109/WCNC.1999.796968

[2.30] Kaigui Bian; Jung-Min Park; Ruiliang Chen; , "Control Channel Establishment in Cognitive Radio Networks using Channel Hopping," Selected Areas in Communications, IEEE Journal on , vol.29, no.4, pp.689-703, April 2011, doi: 10.1109/JSAC.2011.110403

[2.31] Soua, R.; Minet, P.; , "A survey on multichannel assignment protocols in Wireless Sensor Networks," Wireless Days (WD), 2011 IFIP , vol., no., pp.1-3, 10-12 Oct. 2011, doi: 10.1109/WD.2011.6098201

[2.32] O. D. Incel., “A survey on multi-channel communication in wireless sensor networks.”, Comput. Netw. 55, 13 (September 2011), 3081-3099. DOI=10.1016/j.comnet.2011.05.020 http://dx.doi.org/10.1016/j.comnet.2011.05.020

[2.33] Q. Yu, J. Chen, Y. Sun, Y. Fan, W. Shen, “Regret Matching Based Channel Asseignment for Wireless Sensor Networks” in Proc. IEEE ICC’10, Cape Town, South Africa, 2010

[2.34] Y. Kim, H. Shin, H. Cha., “Y-MAC: An energy efficient Multi-channel MAC Protocol for Dense Wireless Sensor Networks” In Proc. IPSN’08, St. Louis, Missouri, USA, 2008

[2.35] Y. Wu, M. Keally, G. Zhou, W. Mao, “Traffic-Aware Channel Assignment in Wireless Sensor Networks”, in Proceedings of the 4th International Conference on Wireless Algorithms, Systems, and Applications, WASA '09, Pages 479 – 488, doi: 10.1007/978-3-642-03417-6_47

[2.36] G. Zhou, C. Huang, T. Yan, T. He, J. A. Stankovic and T.F. Abdelzaher, “MMSN: Multi-Frequency Media Access Control for Wireless Sensor Networks”, In IEEE INFOCOM, 2006

[2.37] CREW project homepage, http://www.crew-project.eu/, last accessed 06/2013

3

Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment

Chapter 2 focused on space-frequency based interference avoidance protocols which are implementable on current COTS hardware.

Within this chapter we step away from these requirements and focus on developing a solution which allows IEEE 802.15.4 and IEEE 802.11 to co-exist nicely when operating within each other's frequency band. The observed performance degradation of chapter 2 shows that time based separation of transmissions is not functioning efficiently between IEEE 802.15.4 and IEEE 802.11. Co-existing on the same frequency band within each other's collision domain is therefore only possible by improving the time based separation between both technologies.

In other words, the current CSMA/CA implementations of both technologies are not compatible with each other. In order to identify the needed changes we first model the collision probability between both technologies. The needed changes to make them co-existence aware are identified. This results in a new collision model enabling performance comparison of the different roll-out scenarios of co-existence aware CSMA/CA to regular CSMA/CA.

**Lieven Tytgat, Opher Yaron, Sofie Pollin,
Ingrid Moerman, Piet Demeester**

Published in EURASIP Journal on Wireless Communication Networks
(JWCN) issue 2012:137

Abstract - More and more devices are becoming wirelessly connected. Many of these devices are operating in crowded unlicensed bands, where different wireless technologies compete for the same spectrum. A typical example is the unlicensed ISM band at 2.4 GHz, which is used by IEEE 802.11bgn, IEEE 802.15.4 and IEEE 802.15.1, among others. Each of these technologies implements appropriate Media Access Control (MAC) mechanisms to avoid packet collisions and optimize Quality of Service (QoS). Although different technologies use similar MAC mechanisms, they are not always compatible. For example, all CSMA/CA based technologies use Clear Channel Assessment (CCA) to detect when the channel is free, however in each case it is specifically designed to improve detection reliability of the specific technology. Unfortunately, this approach decreases the detection probability of other technologies, increasing the amount of cross-technology collisions. In this paper we introduce the concept of coexistence aware CCA, which enables a node operating in one technology to backoff for other coexisting technologies as well. As a proof of concept we analyze the Packet Error Rate (PER) incurred by an IEEE 802.15.4 network in the presence of IEEE 802.11bg interference, and assess the PER reduction that is achieved by using coexistence aware CCA.

3.1 Introduction

Wi-Fi has since long been the major wireless technology connecting PCs with each other. Lately, we observe an evolution from powerful wireless devices to lightweight embedded devices, while at the same time their density is increasing. The number of such wireless devices is expected to become an order of magnitude bigger than the current number of PCs, as can be seen in. In addition, new types of application areas introduce new wireless communications solutions, which employ a variety of wireless technologies.

The problem when using different wireless technologies in the same frequency band is that most of them are not designed to be compatible with each other. Even if different technologies use a similar Medium Access Control (MAC) Protocol, they might still impede each other.

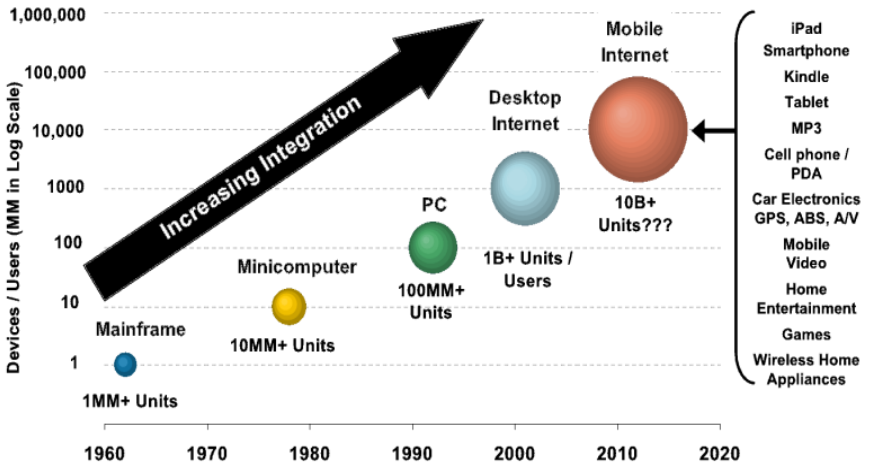

Figure 3.1: Projected number of devices.
Source: Morgan Stanley [3.1]

Within this paper we study the collisions between two heterogeneous CSMA/CA based MAC technologies. As a proof of concept we analyze the collisions between IEEE 802.11bg and IEEE 802.15.4. Throughout the paper we refer to IEEE 802.11bg with the term Wi-Fi, and to IEEE 802.15.4 with the term ZigBee. Note that IEEE 802.15.4 only defines the physical (PHY) layer and MAC layer, in contrast to ZigBee that also specifies higher layers of communication above IEEE 802.15.4. However, for the sake of simplicity we use the terms IEEE 802.15.4 and ZigBee to denote the same thing.

The co-existence behavior of Wi-Fi and ZigBee has been studied extensively. The physical layer effects of Wi-Fi and ZigBee coexistence are already considered in the IEEE 802.15.4 standard [3.2]. Zhen et al. study the cross-technology detection probability of Clear Channel Assessment (CCA) between ZigBee and Wi-Fi in [3.3]. They conclude that ZigBee is oversensitive to Wi-Fi, while Wi-Fi is insensitive to ZigBee beyond a Heterogeneous Exclusive CCA Range (HERC), which they calculate to be 25m with the free space pathloss model. In [3.4] Wei Yuan et al. study the co-existence behavior of ZigBee and saturated Wi-Fi. They conclude through a model and simulation that 5.75% of the ZigBee throughput remains under the assumption that Wi-Fi and ZigBee CCA can avoid all cross-technology collisions. They also conclude through simulation that no throughput remains in case Wi-Fi does not detect ZigBee. S. Pollin et al. measure the coexistence impact of ZigBee and Wi-Fi in [3.5]. They conclude that standard Wi-Fi devices do not backoff for ZigBee traffic, even in very close proximity. They also show that the CCA mechanism of ZigBee can reduce collisions with Wi-Fi, but it is too slow to avoid all Wi-Fi traffic. Thonet et al. measure up to 85% ZigBee packet loss due to 802.11b traffic in [3.6]. Consequently, we conclude that ZigBee

might incur severe packet loss when it coexists with Wi-Fi. However, no model predicting the performance degradation has been proposed. Out of [3.2] it is possible to determine the Packet Error Rate (PER) depending on the Signal to Interference Ratio (SIR) and the size of the collision window, given there is a collision. However, the amount of collisions is dependant on the channel access mechanism of both Wi-Fi and ZigBee. Hence, a detailed model for cross-technology collisions that considers realistic Wi-Fi and ZigBee channel access mechanisms is a key open issue. In [3.7] and [3.8] we propose such a model and focus on exploring the economic value of introducing sensing engines in one specific business scenario. In this paper we focus on a thorough theoretical study of this model, and verify it against real-life measurements in a testbed environment.

The remainder of the paper is organized as follows. In Section 3.1.1, we analyze the CCA based medium access in Wi-Fi and ZigBee. In Section 3.2, we derive the ZigBee PER model under Wi-Fi interference, look at the sensitivities it has and verify it through measurements. Out of this model, the major mechanism leading to the high ZigBee PER is identified. In Section 3.3 we analyze the different Coexistence Aware CCA (CACCA) implementation alternatives, and the implications of using a spectrum sensing engine as a CACCA agent. Section 0 gives an overview of potential topics for further research, while Section 3.5 concludes this paper.

3.1.1 CCA operating principle

The operating principle of a CCA based MAC consists of three steps, as depicted in Figure 3.2. Prior to any transmission, the radio remains in receive-mode for a time window of length T_{CCA}, during which it measures the average received power. If it is above a certain threshold, the radio assumes the channel is busy, and backs-off. Otherwise, the radio switches to transmit mode – which takes T_{Rx2Tx} – and starts to transmit the packet.

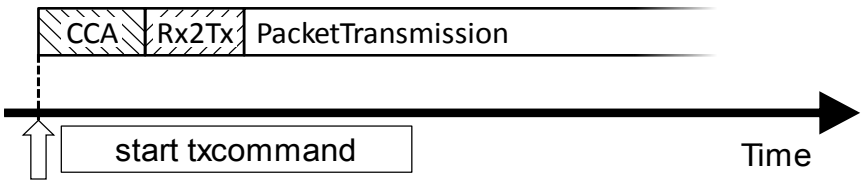

Figure 3.2: CCA based packet transmission

Both Wi-Fi and ZigBee use CCA, however their operating parameters such as Bandwidth (BW), Power Spectral Density (PSD) and timing (duration of the CCA window, packet time, etc.) differ, as can be seen in Table 3.1.

The difference in bandwidth and power – of which a spectral diagram is given in Figure 3.3 – results in a difference in detection sensitivity. With a bandwidth of 22 MHz, Wi-Fi CCA captures the full power of both Wi-Fi and ZigBee transmissions. ZigBee transmits at 0dBm, which is 20dB lower than the Wi-Fi transmission, resulting in a 20dB lower sensitivity to ZigBee than to Wi-Fi. On the other hand, with a bandwidth of only 2 MHz, ZigBee CCA captures the full power of other ZigBee transmissions in the same channel, but only $2/22^{th}$ – or -10.4dB – of the Wi-Fi transmit power, resulting in a 9.6dB higher sensitivity to Wi-Fi than to ZigBee. These simple calculations support the observations of [3.3] that we mentioned earlier.

	ZigBee	Wi-Fi
BW (MHz)	2	22
Tx power (dBm)	0	20
PSD (dBm/MHz)	-3	6.6
T_{CCA} (µs)	128	<4
T_{Rx2Tx} (µs)	192	<5
Min. packettime(µs)	320	28
Max. packettime(µs)	4256	12416

Table 3.1: Wi-Fi and ZigBee parameters [3.2],[3.14]

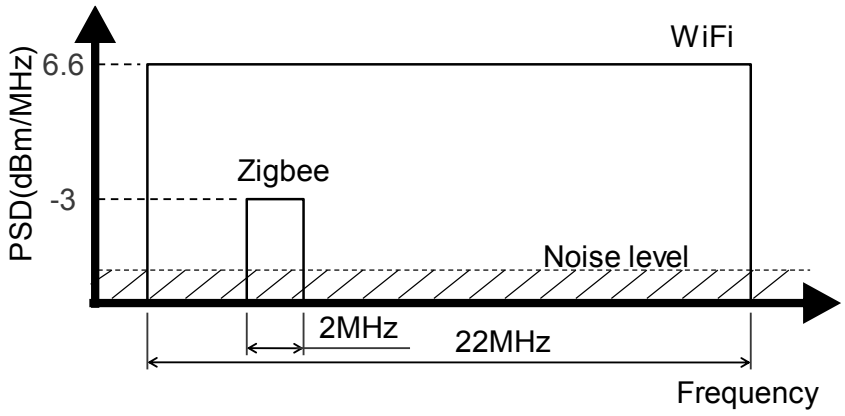

Figure 3.3: Spectral comparison of Wi-Fi and ZigBee

Both Wi-Fi and ZigBee allow preamble detection instead of energy detection as CCA. Preamble detection can improve sensitivity, but prevents cross-technology detection due to the differences in preambles between technologies. In ZigBee this is usually disabled as the sensing time defined by the standard is sufficiently long to allow adequate sensing sensitivity. However, Wi-Fi enables

this by default in order to reach the maximum sensing sensitivity within the short Wi-Fi CCA timeframe. We can therefore assume that standard Wi-Fi does not backoff at all for ZigBee traffic.

3.2 ZigBee PER under Wi-Fi interference

3.2.1 Analytical PER Model

In the following we assume that every collision between a Wi-Fi packet and a ZigBee packet results in the ZigBee packet being lost. Although this is undoubtedly an oversimplification, it allows us to clearly show the plausible PER reduction through the usage of coexistence aware CCA.

We focus on the packet loss in the ZigBee network under Wi-Fi interference. For the sake of convenience we sometimes use the Packet Success Rate (PSR), which is defined by

$$PSR := 1 - PER \tag{3.1}$$

We identify three sources for ZigBee Packet Errors. First, there is packet loss due to the received ZigBee signal being too low compared to the radio noise ($PER_{Z,SNR}$). Second, ZigBee packets can get lost because of collisions with other ZigBee packets ($PER_{Z,Z}$). Finally ZigBee packet loss can occur because of collisions between ZigBee and Wi-Fi packets ($PER_{Z,W}$). These independent events are not mutually exclusive, hence the total PER_Z is smaller than or equal to their sum. Moreover, $PER_{Z,W}$ is only one of the sources of PER_Z and thus also smaller than or equal to PER_Z. For the total ZigBee Packet Error Rate (PER_Z) we have

$$PER_{Z,W} \leq PER_Z \leq PER_{Z,W} + PER_{Z,Z} + PER_{Z,SNR} \tag{3.2}$$

$PER_{Z,SNR}$ has been studied extensively, as described for example in [3.2]. In addition, we will not discuss $PER_{Z,Z}$ in detail in this paper. Nevertheless, under normal operating conditions – which means low load in the sensor network and sufficient link budget – $PER_{Z,Z} \approx 0$ and $PER_{Z,SNR} \approx 0$. Consequently,

$$PER_Z \approx PER_{Z,W} \tag{3.3}$$

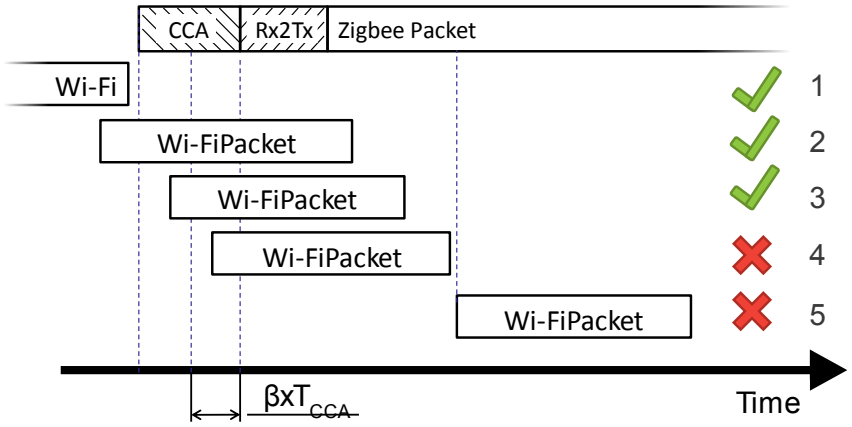

Figure 3.4: Possible ZigBee ⇔ Wi-Fi interactions

In Figure 3.4 we illustrate the possible interactions between Wi-Fi and ZigBee broadcast traffic. Remember that Wi-Fi CCA does not detect ZigBee transmissions, therefore the CCA and Rx2Tx windows of Wi-Fi are not visualized in Figure 3.4. In case 1, a Wi-Fi transmission starts and finishes without interaction with ZigBee, and thus no collision occurs. In the 2nd case, a Wi-Fi packet starts close before the ZigBee device starts its CCA. Hence the ZigBee CCA window will be completely overlapped by the Wi-Fi transmission and ZigBee will sense the channel as busy. In case 3, the Wi-Fi packet starts earlier than a certain percentage – β – of the CCA window. β is defined as the percentage a transmitted Wi-Fi packet needs to cover the ZigBee CCA window in order for the ZigBee device to assess the channel as busy. Therefore the ZigBee device will backoff, avoiding a collision. In case 4 the Wi-Fi packet starts beyond the β boundary, resulting in ZigBee assessing the channel as free. Initially we assume that all Wi-Fi packets are longer than $\beta \times T_{Z,CCA} + T_{Z,Rx2Tx}$, therefore the Wi-Fi packet will have some overlap with the actual ZigBee packet, which will result in a collision. Later on we will also examine our model with shorter Wi-Fi packets. Finally, in the 5th case, the Wi-Fi packet starts during the ZigBee packet, resulting in a collision. We conclude that a collision happens whenever a Wi-Fi transmission starts during the $\beta \times T_{Z,CCA} + T_{Z,Rx2Tx} + T_Z$ timeframe of a ZigBee transmission. We further assume that all collisions result in packet losses, and therefore the probability of not losing a packet, $PSR_{Z,W}$ equals to the probability of not having a Wi-Fi transmission starting during this time frame, which can be written as

$$PSR_{Z,W} = \Pr\left(t_{\overline{W}} > \beta \times T_{Z,CCA} + T_{Z,Rx2Tx} + T_Z\right) \tag{3.4}$$

with

$t_{\overline{W}}$:= a random variable that represents the time until the current Inter Packet Delay (IPD) of Wi-Fi terminates and a new Wi-Fi packet starts.

T_Z := The average ZigBee packet length

$T_{Z,CCA}$:= The ZigBee CCA time

$T_{Z,Rx2Tx}$:= The ZigBee Rx to Tx turnaround time

Since Wi-Fi CCA does not detect ZigBee transmissions, the instants of time at which Wi-Fi transmissions start are independent of the ZigBee transmissions. We assume that the distribution of Wi-Fi IPD can be approximated by the exponential distribution, with average $T_{\overline{W}}$. Note that it is typically assumed that the Wi-Fi IPD has a self-similar distribution (i.e. traffic bursts). However, traffic bursts can be divided into periods of intense traffic, and periods of less intense traffic. Within each period we assume the distribution of IPD can be reasonably approximated by the exponential distribution, respectively with a high and a low rate. This assumption allows to determine the $PER_{Z,W}$ during intense traffic as well as during low traffic periods, which is the major intent of this study.

Under these assumptions we can write

$$PSR_{Z,W} \approx e^{-\frac{\beta \times T_{Z,CCA} + T_{Z,Rx2Tx} + T_Z}{T_{\overline{W}}}} \tag{3.5}$$

Note that $T_{\overline{W}}$, T_Z and β are variables, while $T_{Z,CCA}$ and $T_{Z,Rx2Tx}$ are constants that are defined by the ZigBee standard [3.2] (see Table 3.1).

In the remainder of this paper we use typical default values for the various parameters, as specified in Table 3.2, unless explicitly noted otherwise. In addition, we use a default value of β=1. In Table 3.2 the MAC frame size – as well as the derived MAC load – consist of the MAC header + payload. We continue to use this MAC load throughout this paper. The packet durations are derived according to [3.2] for ZigBee and [3.13] for Wi-Fi without ACKs or RTS/CTS.

	ZigBee	Wi-Fi
MAC frame size (bytes)	127, 100, 50, 5	1278
Datarate	250Kbps	1Mbps, 11Mbps, 54Mbps
Packet-rate (packets/s)	25	10
MAC Load (Kbps)	20	102.2
Packet duration (µs)	127b: 4256 100b: 3392 50b: 1792 5b: 352	1Mbps: 10416 11Mbps: 1121 54Mbps: 212

Table 3.2: parameters used, default values are underlined

Equation (3.5) does not depend explicitly on the average Wi-Fi packet duration T_W. However, $T_{\overline{W}}$ can be written as

$$T_{\overline{W}} = \frac{1}{R} - T_W \tag{3.6}$$

with

R := The average Wi-Fi packet rate (packets/s)

T_W := The average Wi-Fi packet duration (s)

Equation (3.6) shows that the influence of T_W on $T_{\overline{W}}$ remains relatively low as long as $1/R$ remains large compared to T_W. The duration of the default Wi-Fi packet at 1Mbps is 10.4ms, so in order to limit the deviation in $T_{\overline{W}}$ to 10%, the packet rate should remain below 10 packets/s (=102.2Kbps). We can therefore expect that below this throughput the different Wi-Fi data rates will result in almost identical $PER_{Z,W}$. We will therefore use the 100Kbps point (the highlighted vertical line in Figure 3.5) as a first comparison point throughout this paper. Furthermore, we assume that a ZigBee network can cope with up to 10% packet loss. Hence we use the Wi-Fi load resulting in 10% $PER_{Z,W}$ (the highlighted horizontal line in Figure 3.5) as a second comparison point throughout this paper. Figure 3.5 plots $PER_{Z,W}$ as a function of the Wi-Fi load for a ZigBee frame size of 100 bytes. We calculate a ZigBee $PER_{Z,W}$ of 3.74% at the 100Kbps point. The load resulting in 10% $PER_{Z,W}$ point for 54Mbps Wi-Fi data rate equals 279 Kbps.

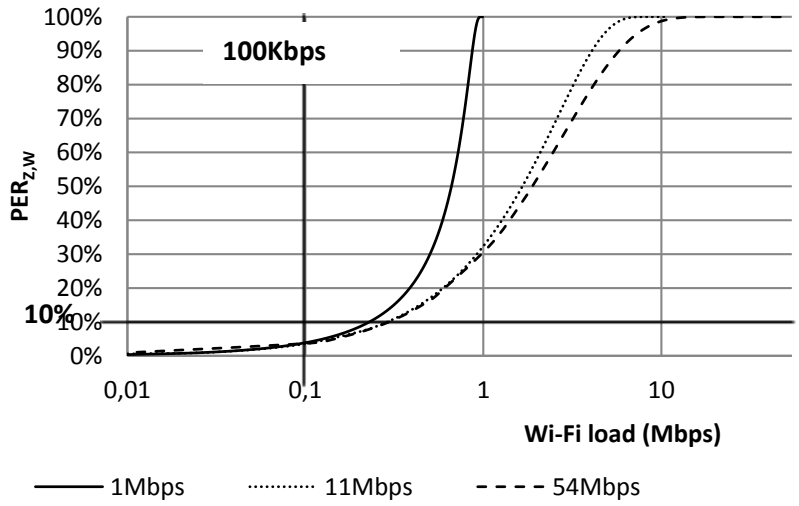

Figure 3.5: $PER_{Z,W}$ as a function of the Wi-Fi load for different Wi-Fi physical data rates

3.2.2 Sensitivity analysis

The total ZigBee packet duration T_Z can vary between 320µs and 4256µs. Figure 3.6 shows the difference in $PER_{Z,W}$ for 54Mbps Wi-Fi. There is a factor 8 difference in $PER_{Z,W}$ between the largest and smallest ZigBee packets.

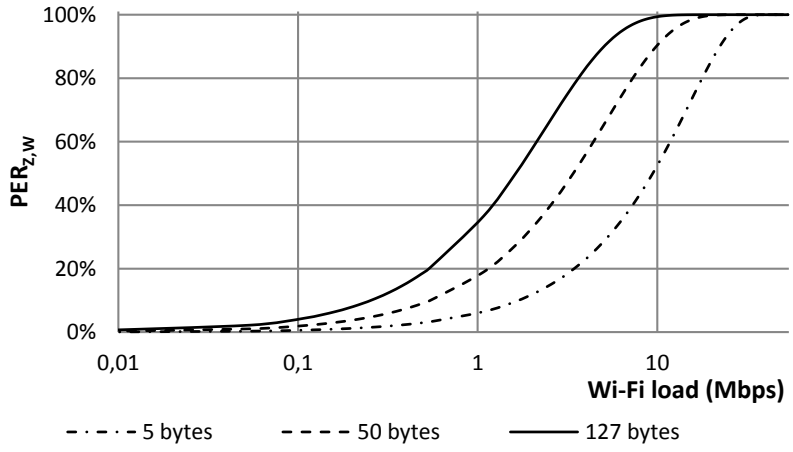

Figure 3.6: Sensitivity of $PER_{Z,W}$ to ZigBee packet size

β depends on the CCA threshold and the received signal energy. Determining the exact value of β is out of scope for this paper. However, we explore the

sensitivity of $PER_{Z,W}$ to the value of β. Equation (3.7) shows the $PSR_{Z,W}$ in the case $\beta = 0$ while Figure 3.7 compares the case of $\beta = 1$ with that of $\beta = 0$. There is a reduction of $PER_{Z,W}$ with a factor 1.23 at the 100 Kbps point, and the 10% $PER_{Z,W}$ point shifts from 279Kbps to 324Kbps.

$$PSR_{Z,W,\beta=0} \approx e^{-\frac{T_{Z,Rx2Tx} + T_Z}{T_{\overline{W}}}} \tag{3.7}$$

Recall that during the analysis we assumed the Wi-Fi packets to be longer than $T_{Z,Rx2Tx} + \beta \times T_{Z,CCA}$ (:= T_{Z0}). However, Wi-Fi can transmit smaller packets. A collision will then only occur if the actual Wi-Fi packet transmission starts less than the duration of the Wi-Fi packet before the actual ZigBee packet starts. This change has the effect of replacing the term $T_{Z,Rx2Tx} + \beta \times T_{Z,CCA}$ in (3.5) with the actual duration of the Wi-Fi packet T_W:

$$PSR_{Z,W,T_W<T_{Z0}} \approx e^{-\frac{T_Z + T_W}{T_{\overline{W}}}} \tag{3.8}$$

The largest deviation to the base model is caused with the smallest Wi-Fi packets possible (28 µs). This possibility is also visualized in Figure 3.7. There is a factor 1.8 difference for 100 Kbps Wi-Fi, and the 10% $PER_{Z,W}$ point shifts from 279Kbps to 486Kbps.

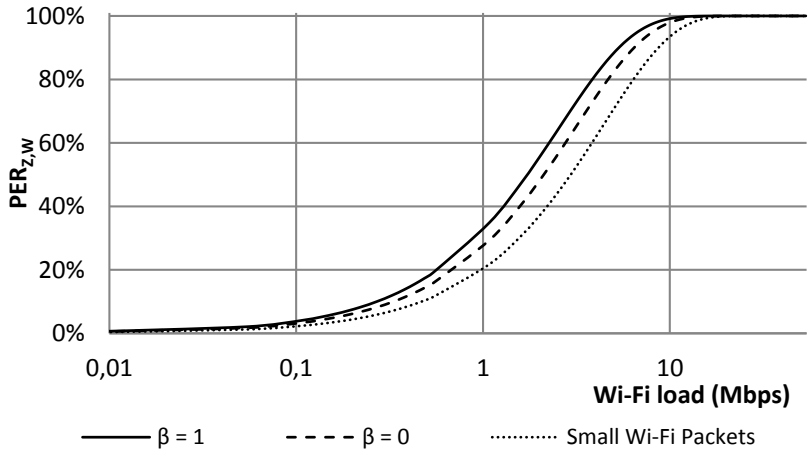

Figure 3.7: Sensitivity of $PER_{Z,W}$ to β, and to small Wi-Fi packets

3.2.3 Experimental model verification

We now turn to validate our model in practice. The experiments are conducted in the Wireless lab of the IBBT iLab.t technology centre [3.15]. iLab.t has an RF shielded environment of 4 Qosmotec shielded boxes, in which ZigBee and Wi-Fi devices are connected by coax cables. It can achieve full mesh connectivity between all four boxes through the use of a PC controlled attenuator. Hence no external interference is received, and the attenuation of each link can be set. Using this setup allows for real devices to communicate in a controlled environment. For our experiments we use three nodes with attenuation between them set as shown in Figure 3.8. The Wi-Fi transmitter broadcasts at 18dBm, the ZigBee transmitter broadcasts at 0dBm, and PER_Z is measured at the ZigBee receiver. These settings result in SNR at the ZigBee receiver of about 25dB, and SIR of -22.4dB. Hence, all ZigBee packets which do not collide with Wi-Fi are received correctly, and all packets that collide with Wi-Fi are lost.

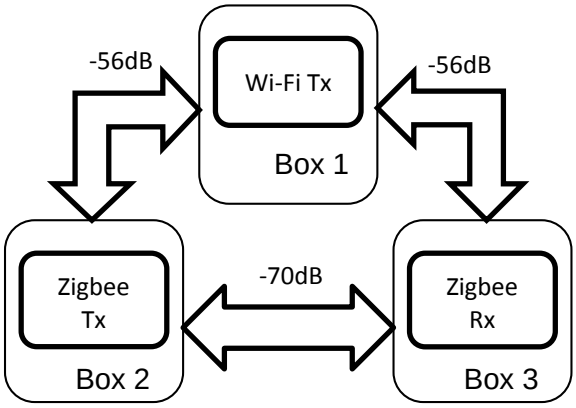

Figure 3.8: The test setup

All experiments are run with 100 byte ZigBee packets and 1278 byte Wi-Fi packets sent at bitrates of 1, 11 and 54Mbps. All packets are transmitted with a fixed IPD.

Figure 3.9 displays a comparison between the measurements and the model for 54Mbps Wi-Fi. The $PER_Z \approx PER_{Z,W}$ measurements are within a margin of 13% from the model for loads lower than 1 Mbps. A maximum deviation of 34% is measured at 2Mbps application load (a packet-rate of 200 packets/s), which is the point where $T_{\overline{W}}$ becomes smaller than T_Z and obviously no ZigBee packet can be

sent.

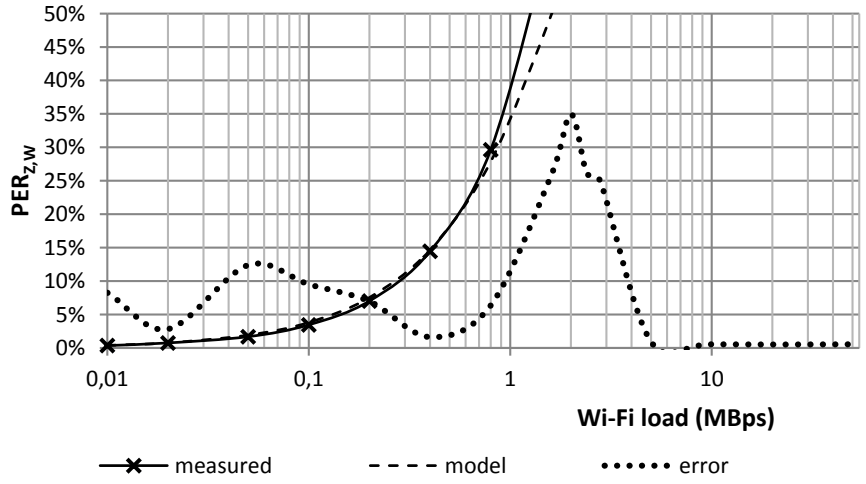

Figure 3.9: 54 Mbps modeled and measured $PER_{Z,W}$

The $PER_{Z,W}$ for 11Mbps Wi-Fi is depicted in Figure 3.10. The measurement outcome is similar to the 54Mbps case as the Wi-Fi packet durations at 54Mbps (=212µs) and 11Mbps (=1121µs) are both relatively small compared to $1/R$ (=5000 µs). The maximum deviation to the model is also situated around 2Mbps.

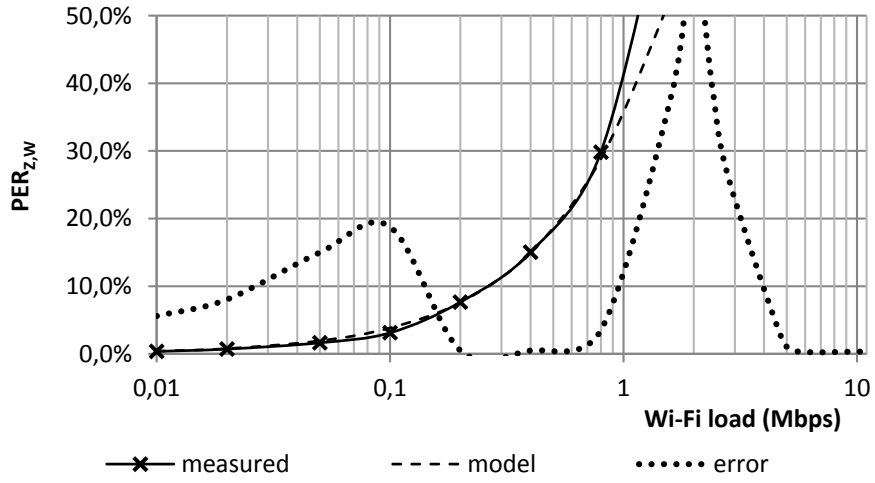

Figure 3.10: 11 Mbps modeled and measured $PER_{Z,W}$

The comparison for 1 Mbps Wi-Fi is displayed in Figure 3.11. It shows that below the 0.1Mbps load point the error remains below 13%. Beyond this point (0.1Mbps – 0.4Mbps), the model and the measured $PER_{Z,W}$ diverge. This is because the model assumes the ZigBee and Wi-Fi packet transmissions to be independent. However, due to ZigBee transmissions backing-off on the relatively long Wi-Fi packets (10ms), they tend to start their transmissions close after a Wi-Fi transmission. This results in fewer collisions than expected because in the experiments the IPD for Wi-Fi is constant. Beyond the 0.4Mbps point, $T_{\overline{W}}$ approaches T_Z, resulting in a fast increase in PER. Above 0.7Mbps, $T_{\overline{W}}$ is smaller than T_Z, resulting in 100% packet loss.

As mentioned earlier, these tests are conducted with constant IPD for both Wi-Fi and ZigBee, and still the PER measurements are rather close to our calculations. The error remains below 25% in the region where the ZigBee network stays operational ($PER_{Z,W}$<10%). This indicates that the sensitivity of our model to the probability distribution of $T_{\overline{W}}$ and $T_{\overline{Z}}$ is rather low.

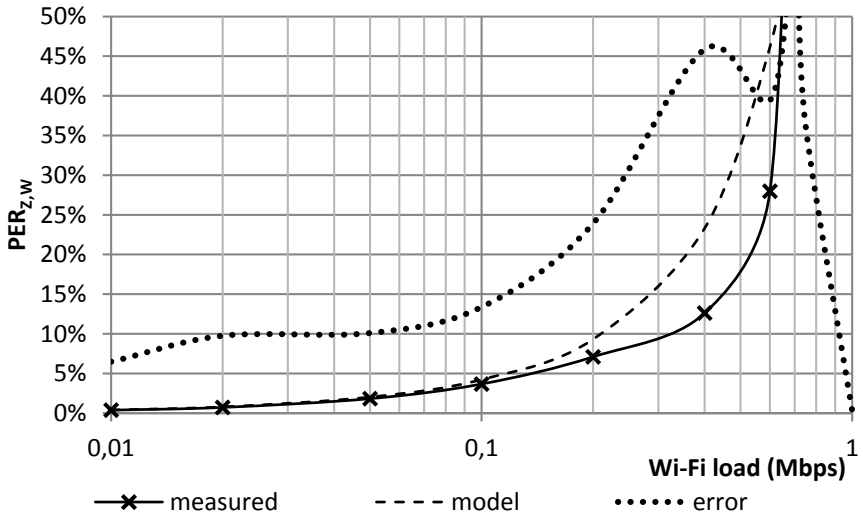

Figure 3.11: 1 Mbps modeled and measured $PER_{Z,W}$

3.3 Deployment of sensing engine based CACCA

3.3.1 Sensing engine characteristics

A spectral sensing engine is a fast and accurate device that measures spectral power density across a wide bandwidth (eg. 174MHz – 6GHz [3.12]). The internals of a sensing engine are detailed in [3.9][3.12]. A sensing engine is commonly used in space and frequency based interference avoidance within a

vertical spectrum sharing context [3.9][3.10][3.11]. However, in this paper, we use a sensing engine as a CCA agent, which is a time domain function. Hence in this work we use a sensing engine to analyze a limited bandwidth within a very short timeframe. It is focused on achieving the highest detection reliability within a very small timeframe and therefore we assume that it can detect ZigBee reliably within the Wi-Fi CCA time. Accordingly, we assume that when deploying a sensing engine the ZigBee CCA time – $T_{ZS,CCA}$ – can be reduced to 4µs, which equals the Wi-Fi CCA time, and is 32 times faster than standard ZigBee. An overview of the resulting timings is given in Table 3.3.

The power consumption of a sensing engine detecting Wi-Fi is presented in [3.16], and equals 110mW for the analog part, and 4mW for the digital part to detect Wi-Fi, totaling to 114mW. The sensing engine needs to be switched on during the 9µs long CCA + Rx2Tx window, resulting in a total energy consumption of 9µs * 114mW = 1.03µJ. The minimal power consumption of a current CC2520 ZigBee Radio in transmit mode equals 45mW, and the smallest ZigBee packet lasts 320µs, resulting in a total minimal transmit energy of 12.8µJ. Hence the total impact on the power consumption of the sensing engine equals at most 8% per transmitted packet.

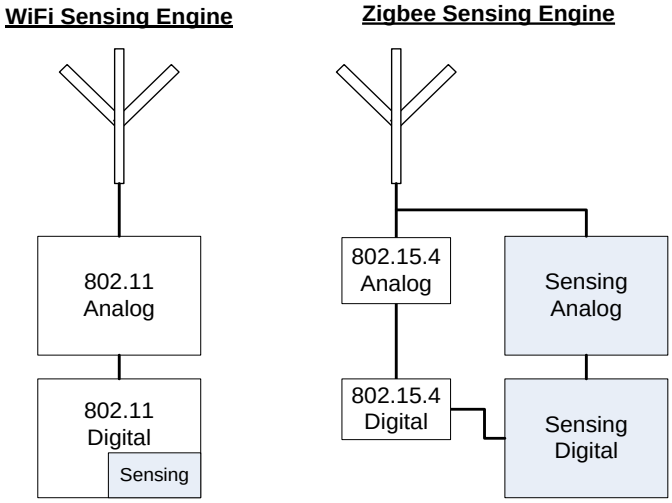

Figure 3.12: Wi-Fi versus ZigBee sensing engine implementation

When deployed in a ZigBee device, the sensing engine creates a parallel receive chain to that of the ZigBee device, as depicted in Figure 3.12. Therefore it can continue sensing the channel – and thus cancel the pending transmission – while the ZigBee device is switching towards transmit mode. Consequently, $T_{ZS,Rx2Tx}$ could in theory become negligible. To be realistic, we assume $T_{ZS,Rx2Tx}$ can

be as short as $T_{W,Rx2Tx}$. The influence of implementing a sensing engine on ZigBee devices is visualized in Figure 3.13.

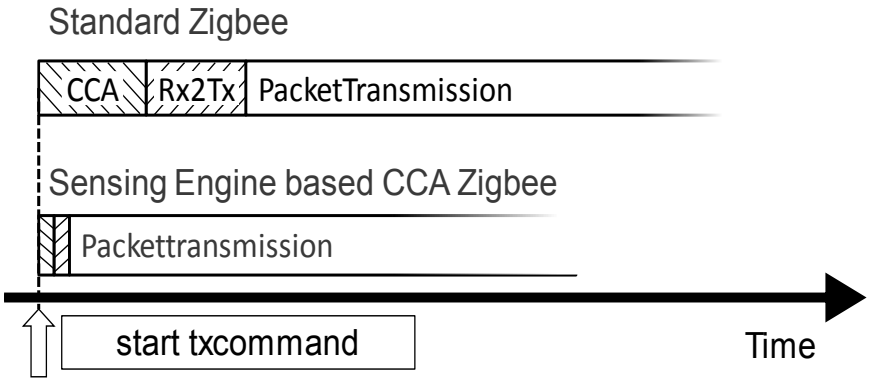

Figure 3.13: ZigBee timing with and without Sensing Engine

When deployed in a Wi-Fi device there is no need for a separate receive chain, as common Wi-Fi devices have the necessary bandwidth and sensitivity. A ZigBee packet is detected by the sensing engine within a timeframe of 4µs. The standard Wi-Fi CCA time is 4µs, hence we assume that the implementation of a sensing engine in Wi-Fi devices will not change $T_{W,CCA}$ and $T_{W,Rx2Tx}$.

Only the digital part of a sensing engine will contribute to the energy consumption in a Wi-Fi device. This 4mW is only consumed during an 8µs long timeframe, totaling to 32nJ per transmission. An 18dBm Wi-Fi transmission consumes at least 63mW, using a 100% efficient radio. The shortest packet lasts 24.5µs[3.13], resulting in an energy consumption of 1.5µJ. The sensing engine energy consumption will thus contribute to at most 2% of the energy consumption per packet transmitted at 18dBm.

	ZigBee	Wi-Fi
T_{CCA}(µs)	128	4
T_{Rx2Tx}(µs)	192	5
$Ts_{,CCA}$(µs)	4	4
$Ts_{,Rx2Tx}$(µs)	5	5

Table 3.3: Regular CCA versus sensing engine based CACCA timings

3.3.2 Case 1: ZigBee side CACCA

A standard ZigBee device can detect Wi-Fi transmissions, therefore the only effect of introducing sensing engines to ZigBee devices is that the CCA time $T_{Z,CCA}$ and the Rx2Tx transition time $T_{Z,Rx2Tx}$ are reduced to $T_{ZS,CCA}$ and $T_{ZS,Rx2Tx}$ – the resulting $PSR_{ZS,W}$ is shown in (9) and $PER_{ZS,W}$ is depicted in Figure 3.14.

$$PSR_{ZS,W} \approx e^{-\frac{\beta \times T_{ZS,CCA} + T_{ZS,Rx2Tx} + T_Z}{T_{\overline{W}}}} \tag{3.9}$$

$PER_{ZS,W}$ calculated at the 100Kbps point equals 1,05%. In other words, the inclusion of the sensing engine results in a $PER_{Z,W}$ drop of 24%. The 10% $PER_{Z,W}$ point shifts from 279 to 324 Kbps.

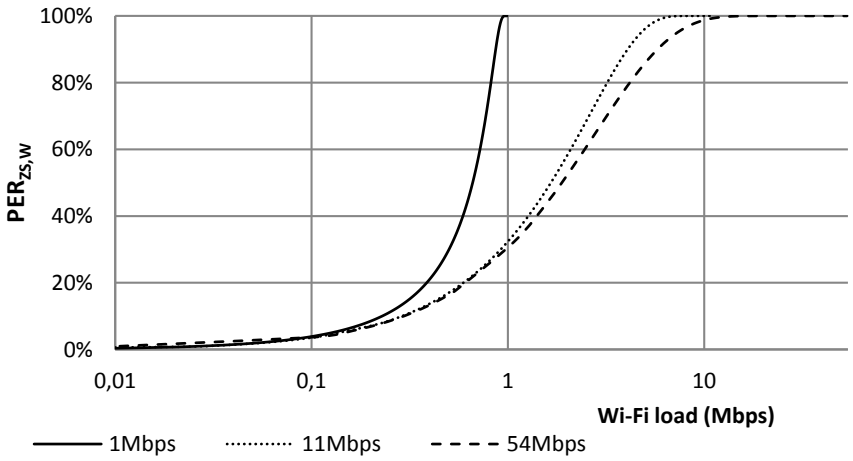

Figure 3.14: $PER_{ZS,W}$ as a function of the Wi-Fi load

Figure 3.15 depicts $PER_{ZS,W}$ for different ZigBee packet sizes. Comparing these results with the no sensing engine results of Figure 3.6 reveals the very modest difference. It is only for very small packets that a significant difference becomes noticeable. In this case $PER_{Z,W}$ at 100Kbps Wi-Fi reduces with a factor 1.9 while the 10% $PER_{Z,W}$ point shifts from 279Kbps to 580Kbps.

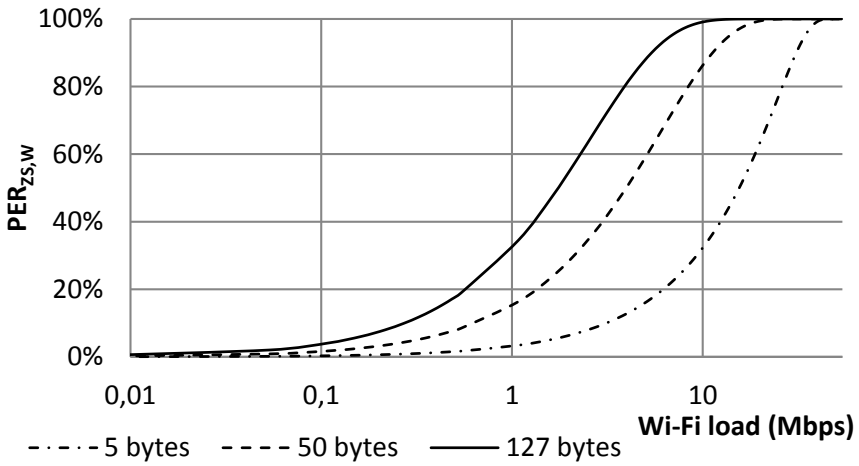

Figure 3.15: Sensitivity of $PER_{ZS,W}$ to ZigBee packet size

3.3.3 Case 2: Wi-Fi side CACCA

In section 3.2 we come to the conclusion that one of the major reasons for packet loss is the inability of Wi-Fi to detect ZigBee packets. Adding a sensing engine to the Wi-Fi devices will solve this problem. Figure 3.16 illustrates the possible collision scenarios between standard ZigBee and a sensing engine enabled Wi-Fi.

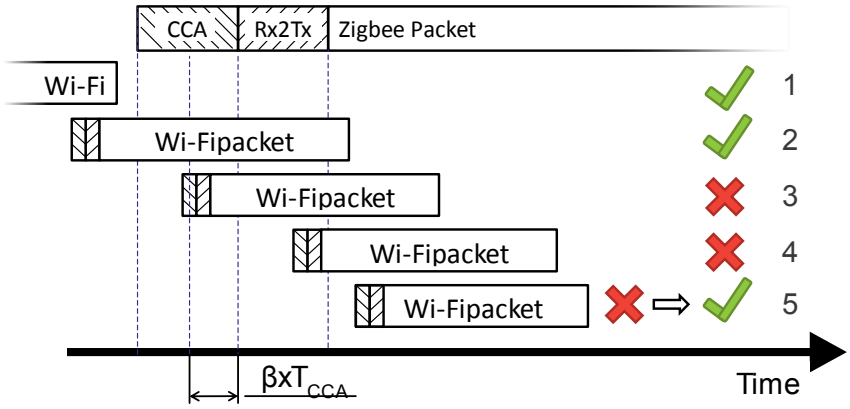

Figure 3.16:Possible Wi-Fi ⇔ZigBee interactions – Wi-Fi side sensing engine

Figure 3.16 shows two different collision possibilities. The first (case 3 in the diagram) occurs when a Wi-Fi transmission starts within the

$\beta_1 \times T_{Z,CCA} + T_{Z,Rx2Tx}$ timeframe, in which ZigBee does not detect the Wi-Fi transmission. The second (case 4) is the reverse scenario where Wi-Fi does not detect the ZigBee transmission. Combining these two mutually exclusive events results in equation (10), in which $T_{WS,CCA}$ and $T_{WS,Rx2Tx}$ equal respectively the Wi-Fi side sensing engine CCA and Rx2Tx times.

$$\begin{aligned} PER_{Z,W} = \quad & \Pr(t_{\bar{W}} < \beta_1 \times T_{Z,CCA} + T_{Z,Rx2Tx}) \\ + \quad & \Pr(t_{\bar{Z}} < \beta_2 \times T_{WS,CCA} + T_{WS,Rx2Tx}) \end{aligned} \tag{3.10}$$

Approximating $t_{\bar{W}}$ and $t_{\bar{Z}}$ as exponentially distributed random variables results in:

$$\begin{aligned} PER_{Z,WS} \approx \quad & \left(1 - e^{-\frac{\beta_1 \times T_{Z,CCA} + T_{Z,Rx2Tx}}{T_{\bar{W}}}}\right) \\ + \quad & \left(1 - e^{-\frac{\beta_2 \times T_{WS,CCA} + T_{WS,Rx2Tx}}{T_{\bar{Z}}}}\right) \end{aligned} \tag{3.11}$$

Filling in the default values from Table 3.2 and assuming $\beta_1=\beta_2=1$ gives:

$$\begin{aligned} PER_{Z,WS} \approx \quad & \left(1 - e^{-\frac{320 \times 10^{-6}}{T_{\bar{W}}}}\right) \\ + \quad & \left(1 - e^{-\frac{9 \times 10^{-6}}{T_{\bar{Z}}}}\right) \end{aligned} \tag{3.12}$$

In order to analyze the dependence on the Wi-Fi load, we assume $T_{\overline{Z}}$ sufficiently large, resulting in a negligible impact of the second part of (12). The first part of $PER_{Z,WS}$ is presented in Figure 3.17. We assess a $PER_{Z,WS}$ of 0,35% at the 100Kbps point, which is a reduction of 75% compared with $PER_{Z,W}$. The 10% $PER_{Z,W}$ point shifts from 279Kbps to 3130Kbps. Analyzing the dependence of $PER_{Z,WS}$ on the ZigBee load – the second part of formula (12) – can be achieved assuming $T_{\overline{W}}$ is sufficiently large.

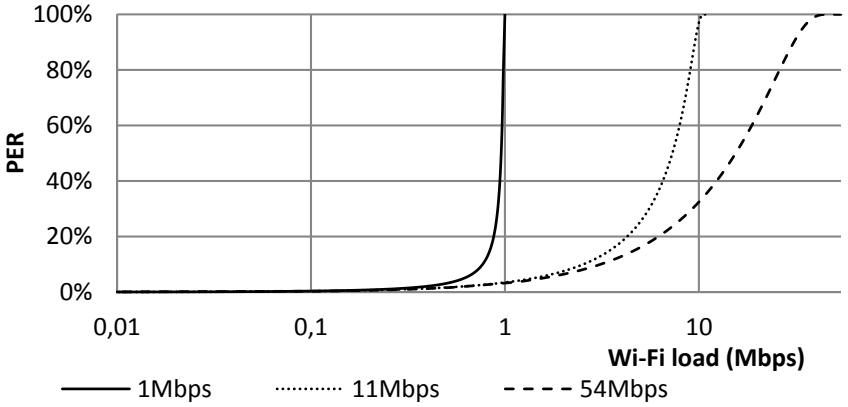

Figure 3.17: $PER_{Z,WS}$ as a function of the Wi-Fi load

Figure 3.18 shows the second part of $PER_{Z,WS}$ as a function of the ZigBee load. $PER_{Z,WS}$ stays below 1% as long as the ZigBee load remains below 200Kbps. The maximum $PER_{Z,WS}$ remains below 2,5% under all circumstances.

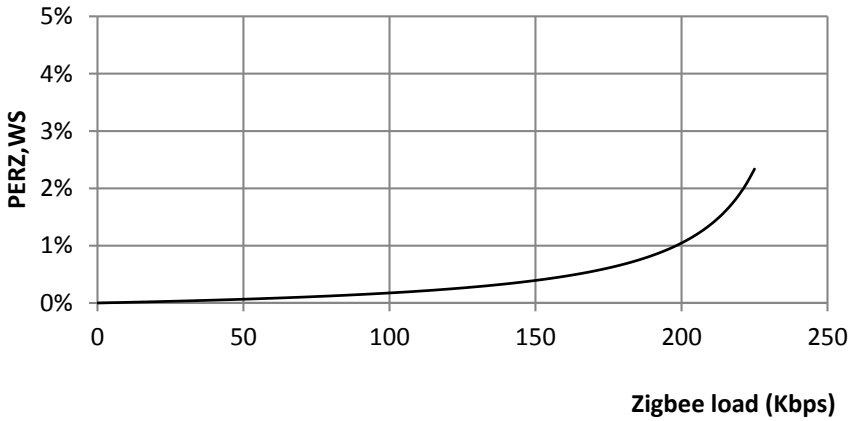

Figure 3.18: $PER_{Z,WS}$ as a function of the ZigBee load

3.3.4 Case 3: Wi-Fi and ZigBee CACCA

In typical operating conditions the ZigBee load is low, thus most of the contribution to $PER_{Z,W}$ comes from the first part of (12). This part highly depends on the ZigBee CCA+Rx2Tx time, therefore it makes sense to also examine the effect of implementing the sensing engine on both ZigBee and Wi-Fi.

The model is identical in form with the model of case 2. The difference is found in $T_{Z,CCA}$ and $T_{Z,Rx2Tx}$ which are reduced to $T_{ZS,CCA}$ and $T_{ZS,Rx2Tx}$ respectively. Equation (13) shows the model incorporating ZigBee and Wi-Fi sensing.

$$PER_{ZS,WS} \approx \left(1-e^{-\frac{\beta_1 \times T_{ZS,CCA} + T_{ZS,Rx2Tx}}{T_{\overline{W}}}}\right) + \left(1-e^{-\frac{\beta_2 \times T_{WS,CCA} + T_{WS,Rx2Tx}}{T_{\overline{Z}}}}\right) \tag{3.13}$$

Filling in the values gives us:

$$PER_{Z,W} \approx \left(1-e^{-\frac{9\times10^{-6}}{T_{\overline{W}}}}\right) + \left(1-e^{-\frac{9\times10^{-6}}{T_{\overline{Z}}}}\right) \tag{3.14}$$

Again, we look at the two parts of the formula separately. The probability of Wi-Fi starting its transmission during the $T_{ZS,CCA}+T_{ZS,Rx2Tx}$ window is significantly lower compared to case 2, as this window now only lasts for 9μs instead of 320μs. The 100Kbps point has a calculated $PER_{ZS,WS}$ of 0,01%. In comparison with Commercial Of The Shelf (COTS) hardware, this creates a drop in $PER_{Z,W}$ of 99.6%. The 10% $PER_{Z,W}$ point shifts from 279Kbps to 37Mbps.

The dependence of $PER_{ZS,WS}$ on $T_{\overline{Z}}$ (second part of the formula) is identical to case 2.

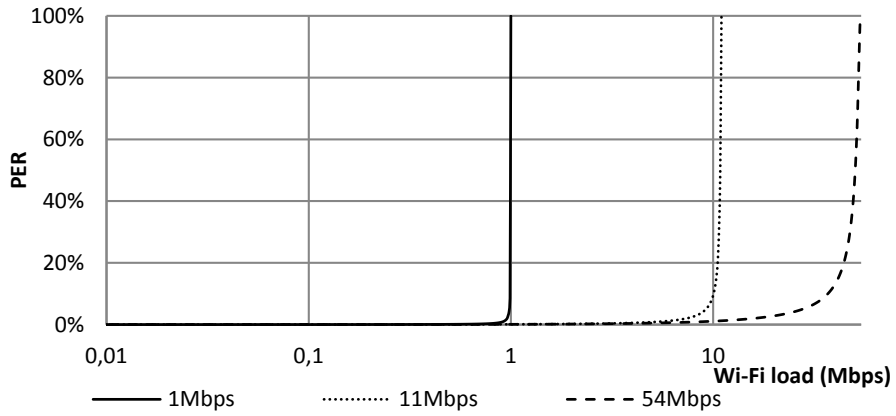

Figure 3.19: $PER_{ZS,WS}$ as a function of the Wi-Fi load

3.3.5 Case comparisons

Case 1 handles the usage of the sensing engine on the ZigBee nodes. We conclude that $PER_{Z,W}$ is highly dependent on T_Z and $T_{\overline{W}}$. The analysis shows reduction of 8% to 48% in $PER_{Z,W}$ (at 100Kbps Wi-Fi load), depending on the size of the ZigBee packets. The Wi-Fi load which leads to 10% ZigBee packet loss equals 324Kbps (for default size ZigBee packets of 100 bytes.)

Case 2 handles the inclusion of the sensing engine in the Wi-Fi devices. The model shows that the dependence on $T_{\overline{W}}$ is reduced, while the dependence on the ZigBee packet size is almost completely removed. This case reduces $PER_{Z,W}$ at 100Kbps Wi-Fi load by 75% while the Wi-Fi load which leads to 10% ZigBee packet loss becomes 3130Kbps.

Case 3 considers the implementation of the sensing engine on both ZigBee and Wi-Fi nodes. This case has the lowest dependence on $T_{\overline{W}}$. It reduces $PER_{Z,W}$ at 100Kbps Wi-Fi load by 99.6%, and achieves a Wi-Fi load resulting in a 10% ZigBee packet loss of 37Mbps.

Figure 3.20 compares all cases while Figure 3.21 zooms in on the – horizontal – 10% ZigBee PER line, and the – vertical – 100Kbps Wi-Fi load line. In addition, Table 3.4 summarizes all cases and their dependencies on packet lengths (T_Z and T_W) and IPDs ($T_{\overline{Z}}$ and $T_{\overline{W}}$)

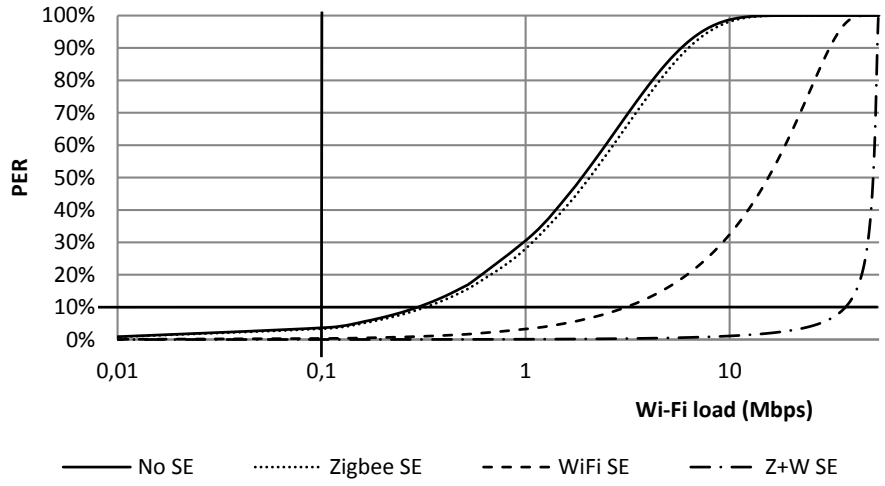

Figure 3.20: Comparison of $PER_{Z,W}$, $PER_{ZS,W}$, $PER_{Z,WS}$ and $PER_{ZS,WS}$

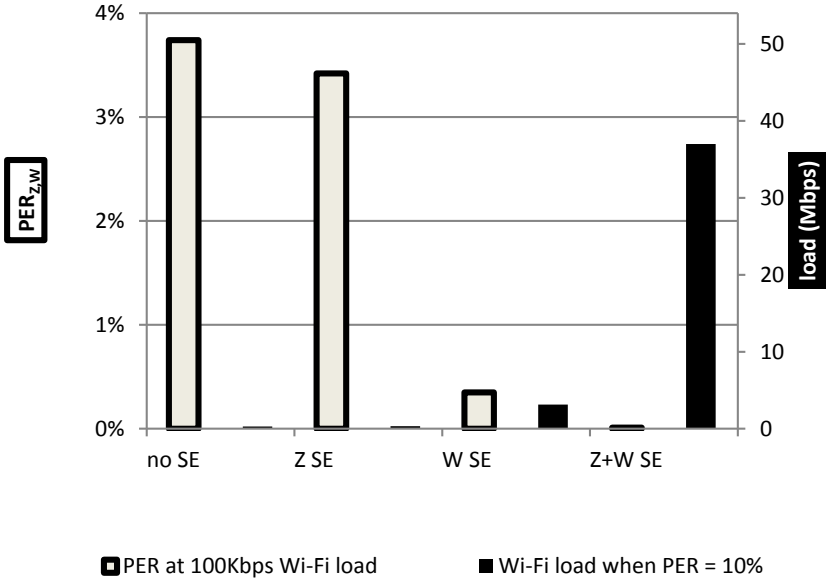

Figure 3.21: Comparison of standard ZigBee with the three cases

	reg. CCA	Z dep.	W dep.	Z+W dep.
$PER_{Z,W}$ @ 100Kbps (%)	3.74	3.42	0.35	0.01
Wi-Fi load @10% $PER_{Z,W}$ (Kbps)	297	324	3130	37000
$PER_{Z,W}$ dependence on:				
T_Z	High	High	Low	Low
$T_{\overline{Z}}$	None	None	Low	Low
T_W	None	None	Low	Low
$T_{\overline{W}}$	High	High	Med.	Low

Table 3.4: Comparison of regular CCA with the three CACCA deployment alternatives

3.4 Future work

We instantiated the CACCA analysis within a ZigBee⇔Wi-Fi context. However, similar analysis can be done in other combinations of technologies, as well as identical technologies that operate in partially overlapping bands (e.g. IEEE 802.11bgn @ 2.4 GHz).

Another aspect we did not consider is the impact the sensing engine has on the Wi-Fi side. It does not only reduce $PER_{W,Z}$ – which is a positive effect – but it also reduces the throughput of Wi-Fi – which is a negative effect. As such this remains an open issue.

This paper only considers Wi-Fi broadcast traffic, without acknowledges or request to send / clear to send. An elaboration on their impact remains for future study.

A final direction for future work is to study the combination of the time domain collision avoidance, together with frequency and/or space domain collision avoidance. This will exploit the possible benefits of a spectrum sensing engine to its fullest.

3.5 Conclusion

As more and more wireless technologies emerge, more of these technologies have to coexist with one another. One of the major open Wi-Fi⇔ZigBee coexistence issues is a model for cross-technology packet collisions. We propose a new analytical model for ZigBee packet loss due to collisions with Wi-Fi packets, analyze it theoretically and validate it experimentally. Out of this model

we conclude that the major cause of ZigBee packet loss is the inability of Wi-Fi to detect ZigBee transmissions.

In order to solve this problem, we propose the Coexistence Aware CCA (CACCA) concept. CACCA enables Wi-Fi to detect ZigBee, and can be implemented through a sensing engine. There are three different deployment alternatives namely, only ZigBee side deployment, only Wi-Fi side deployment, and ZigBee as well as Wi-Fi deployment. Deploying CACCA only on ZigBee results in 24% packet loss reduction, deploying it on Wi-Fi results in 75% packet loss reduction while deploying it on both sides reduces ZigBee packet loss by 99.6%. The maximum allowable Wi-Fi load in order to have less than 10% ZigBee packet loss rises from 279Kbps in the regular CCA case to 324Kbps in the ZigBee only deployment alternative, 3.1Mbps in the Wi-Fi only deployment alternative and 37Mbps when deploying it on both sides. The added energy consumption of a sensing engine based CACCA deployment equals to less than 8% per packet transmitted on the ZigBee side, and less than 2% on the Wi-Fi side.

We can conclude that the deployment of CACCA achieves substantial reduction of the ZigBee incurred packet loss, without needing any additional information exchange (and the incurred overhead), nor having a severe impact on the energy consumption. It can inherently cope with dynamic environments, and is backwards compatible with the IEEE 802.15.4 and IEEE 802.11 standards. Consequently, implementing CACCA increases the reliability of ZigBee while coexisting with Wi-Fi to an unprecedented level, without losing backwards compatibility with existing technologies.

As a final remark, we believe that while in the short term coexistence aware CCA presented in this paper might be seen as a quick-fix for IEEE 802.11bgn⇔IEEE 802.15.4 coexistence, it can easily be extended to allow coexistence beyond current state of the art technologies.

3.6 References

[3.1] M. Meekers, S. Devitt, L. Wu, Morgan Stanley Internet Trends 04/12/2010 (Morgan Stanley Research 2010), http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, Accessed 15 feb. 2012

[3.2] IEEE Std. 802.15.4 - 2006, IEEE Standard for Information Technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), (2006)

[3.3] Bin Zhen, Huan-Bang Li, Shinsuke Hara, and Ryuji Kohno, Clear channel assessment in integrated medical environments, EURASIP Journal On Wireless Communication Networks (2008), DOI=10.1155/2008/821756

[3.4] Wei Yuan, Xiangyu Wang, A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g, in Proceedings of 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux, pp.1-5, (2007), DOI=10.1109/SCVT.2007.4436237

[3.5] S. Pollin, I. Tan, B. Hodge, C. Chun, A. Bahai, Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study, in Proceedings of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp.1-6, (2008), DOI: 10.1109/CROWNCOM.2008.4562460.

[3.6] G. Thonet, P. Allard-Jacquin, P. Colle, ZigBee – Wi-Fi Coexistence White paper and Test Report, www.aduratech.com/pdf/ZigBee-Wi-Fi-Coexistence.pdf, Accessed 15 feb. 2012

[3.7] L. Tytgat M. Barrie, V. Gonçalves, O. Yaron, I. Moerman, P. Demeester, S. Pollin, P. Ballon, S. Delaere, Techno-economical Viability of Cognitive Solutions for a Factory Scenario, in Proceedings of 2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp. 254-264, (2011)

[3.8] M. Barrie, L. Tytgat, V. Gonçalves, O. Yaron, I. Moerman, P. Demeester, S. Pollin, P. Ballon, S. Delaere, "Techno-Economic evaluation of Cognitive Radio in a Factory Scenario,"in Proceedings of Perfomance Evaluation of Cognitive Radio Networks (PE-CRN) 2011, (2011)

[3.9] A.W. Min, K. Kim, K. Shin, Robust cooperative sensing via state estimation in cognitive radio networks, in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 185 – 196, (2011)

[3.10] R. Balamuthi, H. Joshi, C. Nguyen et al., "A TV White Space Spectrum Sensing Prototype", in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 297 – 307, (2011)

[3.11] P. Van Wesemael, S. Pollin, E. Lopez, A. Dejonghe, "Performance Evaluation of Sensing Solutions for LTE and DVB-T", in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 531 – 537, (2011)

[3.12] IMEC vzw, IMEC sensing engine development, http://www.imec.be/ScientificReport/SR2008/HTML/1225000.html, Accessed 15 feb. 2012

[3.13] Y. Xiao, J. Rosdahl, Throughput and Delay Limits of IEEE 802.11, in IEEE communications letters VOL. 6, NO.8 august 2002, PP 355 - 357, (2002)

[3.14] IEEE Std. 802.11 – 2007, 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

[3.15] IBBT, iLab.t technology centre, http://www.ibbt.be/en/develop-test/ilab-t, Accessed 15 feb. 2012

[3.16] S. Pollin, L. Hollevoet, F. Naessens, P. Van Wesemael, A. Dejonghe, and L. Van der Perre, Versatile sensing for mobile devices: cost, performance and hardware prototypes, In Proceedings of the 3rd ACM workshop on Cognitive radio networks (CoRoNet '11), pp 19-24, (ACM New York, 2011), DOI=10.1145/2030678.2030684

4

Evaluating IEEE 802.11 and IEEE 802.15.4 cross-technology interference avoidance mechanisms

In the first chapter we focused on space-frequency based interference avoidance. The second chapter focused on time based interference avoidance. Both approaches try to improve the separation between co-located IEEE 802.15.4 and IEEE 802.11. However, how do the performance gains of both approaches compare to one another? Moreover, both approaches utilize orthogonal dimensions, and can hence be combined. What does the performance of the combination of both mechanisms look like?

Within this chapter we tackle both questions. In order to do so we combine an enhanced version of the experimental testbed based approach of chapter 2 with an extended version of the analytical model of chapter 3. In chapter 2 we experimentally determine the packet loss on a link basis. This packet loss is the result of collisions. Using the model of chapter 3 and combining the measured Wi-Fi statistics of all channels overlapping with all ZigBee channels should hence predict the packet loss occurring on all ZigBee links on all channels. However, the analytical model of chapter 3 assumes all collision to result in packet loss, which is not the case in real life. This probability is dependent on the combination of Signal, Noise and Interference and can thus vary for every link. Hence a major challenge to combine both approaches is to calibrate the probability that a collision results in a packet lost on all channels and for all links. On top of this calibrated model we can incorporate the addition of CACCA, allowing to compare as well as combine the approaches of chapters 2 and 3.

**Lieven Tytgat, Opher Yaron, Sofie Pollin,
Ingrid Moerman, Piet Demeester**

Submitted to Elsevier Computer Communications Journal, special issue on "Current and Future Architectures, Protocols and Services for the Internet of Things"

Abstract - The Internet of Things paradigm requires ubiquitous wireless connectivity. A lot of these wireless connections are using a number of technologies like ZigBee, Wi-Fi, Bluetooth, etc. in the available unlicensed spectrum bands. However, the performance of these technologies tends to reduce when co-located due to cross-technology interference. A number of interference avoidance mechanisms have already been proposed which reduce the impact of one technology on another by avoiding collisions in the space, time or frequency domain. Although all of these mechanisms try to solve the same problem, comparing the impact of these mechanisms in a real-world scenario is not straightforward and still an open issue. Within this paper we assess the impact of current State of the Art interference avoidance mechanisms for a Wi-Fi – ZigBee coexistence scenario in an office environment. We analyze the achievable performance of typical frequency based ZigBee side interference avoidance mechanisms, and compare them with the achievable performance of time based interference avoidance mechanisms. Furthermore we analyze packet loss when combining time and frequency domain interference avoidance and show it reduces the average packet loss from 20% to below 1.2%.

4.1 Introduction

The Internet of Things (IoT) paradigm will make us truly aware of our world around us by connecting everyone and everything. This paradigm introduces a never seen before diversity of applications and their assorting requirements. Most of the devices used in IoT will be connected wirelessly for obvious reasons. The large application diversity requirements are currently supported though a number of different wireless technologies. E.g. Wi-Fi is currently the major technology used for wireless communication between numerous devices. However, Wi-Fi has relatively large power consumption, especially when used in battery powered devices. The longevity of these devices is typically not sufficient to be used within long running IoT applications like wireless monitoring. IEEE 802.15.4 has a power consumption which is an order of magnitude lower than Wi-Fi, enabling the needed longevity for long running applications.

Within the remainder of this paper we will refer to IEEE 802.15.4 as ZigBee. Note that IEEE 802.15.4 only defines the physical and medium access layer in the OSI model while ZigBee defines all layers of the OSI stack and are therefore not

identical. However for simplicity we will refer to all IEEE 802.15.4 based technologies as ZigBee in the remainder of this paper.

Wi-Fi and ZigBee both operate, amongst others, in the 2.4 GHz ISM band. A ZigBee network is typically co-located with Wi-Fi since Wi-Fi is omnipresent nowadays. Hence there is a severe possibility that ZigBee and Wi-Fi coexist within the same frequency band.

Wi-Fi creates a large amount of collisions with ZigBee resulting in packet loss primarily on the ZigBee side [4.1][4.2][4.3]. A number of studies have already proposed mechanisms to reduce the impact of Wi-Fi on ZigBee when both are operating in the 2.4GHz band. The usual approach taken assumes Wi-Fi is present, not under our control and unaware of other networks. Moreover protocols should preferably be backwards compatible with the standard and implementable on current hardware, excluding physical layer adjustments like code division multiple access or changes in the modulation scheme. Hence most interference avoidance approaches make ZigBee avoid Wi-Fi interference in the space, frequency and/or time domain.

Frequency and space domain interference avoidance approaches avoid Wi-Fi interference by making ZigBee devices select the channel with the lowest expected Wi-Fi impact. A number of approaches have already been proposed regarding channel selection[4.4]. In [4.5] we have classified them with respect to the expected performance under Wi-Fi interference and experimentally validated the performance of the protocol classes using a testbed. However, the analysis did not incorporate dynamic real-life interference but only focused on static interference scenarios.

Time domain interference avoidance exploits the time domain behavior of Wi-Fi to reduce the average amount of PER. A few approaches exist which do not require communication between Wi-Fi and ZigBee[4.6], [4.7],[4.8]. The first one exploits the typical bursty behavior of Wi-Fi by not sending ZigBee packets during Wi-Fi traffic burst[4.6]. A second approach, Cooperative Carrier Signaling [4.7], tries to make Wi-Fi do backoffs for ZigBee by making ZigBee devices close to all Wi-Fi devices generate secondary transmissions in sync with the primary transmission. This results in Wi-Fi detecting the channel as busy in case it is configured to use energy based Clear Channel Assessment (CCA). Finally we have presented Coexistence Aware Clear Channel Assessment (CACCA)[4.8] which makes Wi-Fi devices detect ZigBee traffic reliably.

One of the major open issues in the ZigBee-Wi-Fi coexistence context is the performance comparison of the major different approaches in a real-life environment. Hence within this paper we set out to compare the different interference avoidance mechanisms based on measurements on a real-life testbed. In section 2 we analyze ZigBee packet loss in the time, space and frequency domain using a real-life environment. In section 3 we build a generalized ZigBee packet loss model and calibrate it to predict the ZigBee packet loss for every

ZigBee link accurately, based on the measured Wi-Fi interference. We then predict the packet loss on any link for all channels at any time. This prediction allows us to compare the different interference avoidance classes based on an identical underlying set of measurement data in section 4. We also assess the impact of time based interference avoidance as well as the combination of time and frequency based interference avoidance. We conclude this paper in section 5.

4.2 ZigBee Packet loss characteristics

The performance of ZigBee is shown to deteriorate significantly when coexisting with Wi-Fi [4.3],[4.9] while under some circumstance the performance of Wi-Fi was influenced by ZigBee[4.10]. A number of interference avoidance mechanisms which try to reduce the impact of Wi-Fi on ZigBee have already been presented in literature. In all studies on Wi-Fi and ZigBee coexistence they conclude that Wi-Fi devices do not always backoff for ZigBee. In [4.3] they conclude that Wi-Fi does not consider ZigBee activity at all, while in [4.1] they conclude that in specific scenarios Wi-Fi does backoff for ZigBee. Indeed, the IEEE 802.11 standard defines two alternate mechanisms to determine when a channel is busy or free namely energy based Clear Channel Assessment or preamble detection based CCA. In energy based CCA the channel is decided to be busy or free based on all energy measured within the frequency band of the current Wi-Fi channel. A ZigBee device appropriately close to a Wi-Fi receiver can introduce a sufficient amount of energy in the Wi-Fi band, resulting in CCA deciding the channel as busy. In contrast, the preamble based CCA mechanism specifically filters the channel to detect a Wi-Fi preamble. A ZigBee packet does not match this Wi-Fi preamble. Hence Wi-Fi employing preamble based CCA will never backoff for ZigBee.

Assessing the combination of time and space-frequency domain interference avoidance requires modeling the impact of collisions not resulting in packet loss. In [4.8] we propose a practically usable model which predicts the amount of collisions occurring between Wi-Fi and ZigBee. However, not all collisions result in packet loss since the impact of a collision is dependent on the duration of the overlap between the colliding packets and the Signal to Interference Ratio (SIR) perceived during this overlap.

A wireless sensor network deployed in an office environment has to cope with the interference environment. A typical indoor wireless communication scenario is depicted in Figure 4.1. A source is sending a packet to a destination. This destination receives the packet's signal and has to decode it to retrieve the transmitted packet. However, errors in the decoded packet can occur mainly due to 1) signal deterioration and 2) the addition of interference to the signal from one or more interference sources.

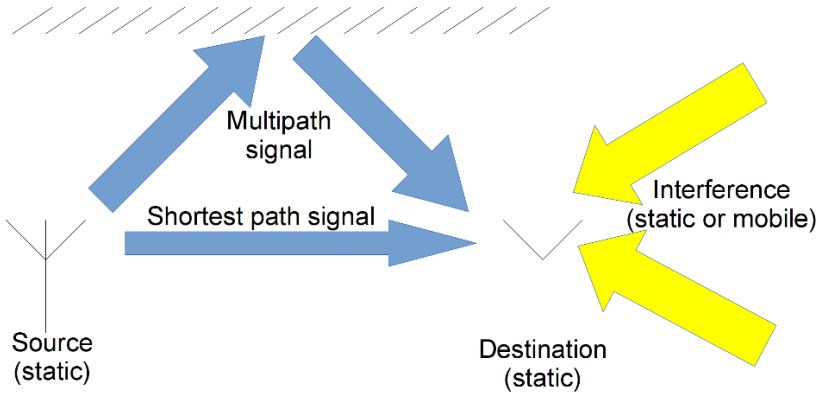

Figure 4.1: The wireless scenario: blue: signal deterioration, yellow: interference

Signal deterioration is usually accounted for by identifying the received signal strength, and comparing that with the noise floor of the radio, the so called Signal to Noise Ratio (SNR). The Bit Error Rate (BER) – and the resulting Packet Error Rate (PER) – are then calculated from this Signal to Noise Ratio (SNR). On top of this multipath fading can influence the quality of the received signal and introduce additional signal deterioration leading to a deviation off the perceived packet loss.

Packet loss due to interference can originate from other devices with the same wireless technology (intra-technology interference) and devices with other wireless technologies (cross-technology interference). Intra-technology interference is usually reduced to a minimum by design. Eg. Numerous technologies utilize the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism to avoid collisions between packets of the same technology. This mechanism tries to minimize the probability of two transmissions colliding. CSMA/CA is designed to work effectively within a single technology, denoted as intra-technology interference avoidance. However, when multiple technologies are co-located this mechanism is usually not very effective[4.3], [4.7], [4.5], [4.8].

In general interference avoidance tries to minimize the effect of interference on the given technology. Within a ZigBee – Wi-Fi context interference can be avoided in three domains namely space, frequency and time. With current Consumer of the Shelf hardware it is impossible to influence the physical layer of both technologies, and as such other domains like eg. code or modulation based interference avoidance are out of scope of this work. In order to understand the potential of the different domains of interference avoidance we first consider the PER measured in each domain individually.

4.2.1 Space and frequency domain interference avoidance

Space domain interference results in nodes on certain locations having other interference characteristics than other nodes. Figure 4.2 shows a plot of the measured average ZigBee Packet Error Rate (PER_Z) received on each individual node set out across the length of the building.

We can clearly see that the average PER_Z on the left side of the building is significantly higher for channel 12. This plot is the average PER_Z of all links to each destination, hence it removes the dependency on link quality assuming that link quality is in average equal in both directions of a link. We can state that on the left side of the building interference has quite a high impact on the ZigBee PER_Z of channel 12, while on the right side of the building this impact is significantly lower. This is due to the Wi-Fi infrastructure deployed in the building, which has three access point spread across three locations on three channels. For other channels similar conclusions can be made.

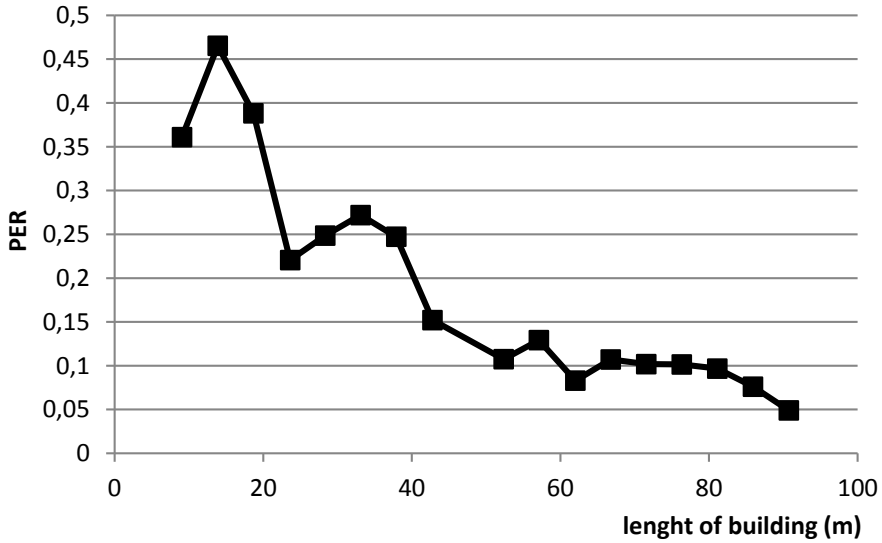

Figure 4.2: Space domain interference impact: measured received PER_Z across the length of the building for ZigBee channel 12

Figure 4.3 shows the average PER_Z across all nodes for all ZigBee channels. This figure clearly shows the difference in average PER_Z across different channels. It is typically assumed that channel 26 is the most reliable channel. During daytime this is indeed the case in our testbed. However, during nighttime channel 25 and 20 perform better.

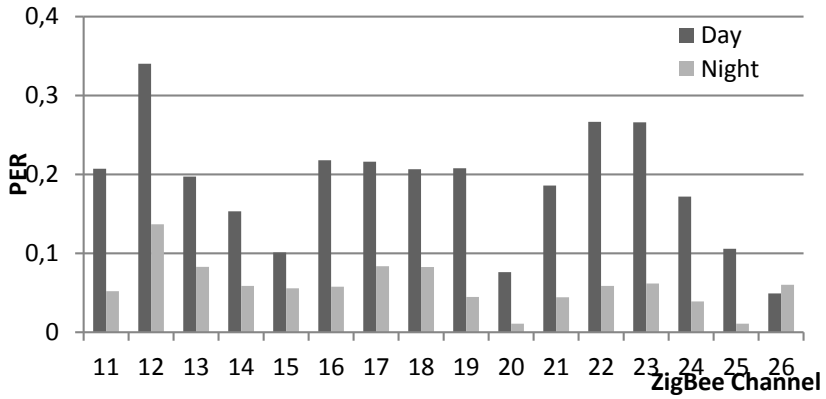

Figure 4.3: Received PER_Z for every ZigBee channel

4.2.2 Time domain interference avoidance

Wi-Fi traffic can cause temporal packet loss in ZigBee. Figure 4.4 shows the time domain PER_Z behavior of a long and a short ZigBee link on channel 16. It is clearly visible that the long link shows temporal deterioration. The nodes are on fixed locations; hence the signal quality will not alter significantly within the timeframe of the measurement. Moreover, the nighttime measurement of this link shows a significant packet loss reduction. Therefore this behavior indicates the impact interference has on this link.

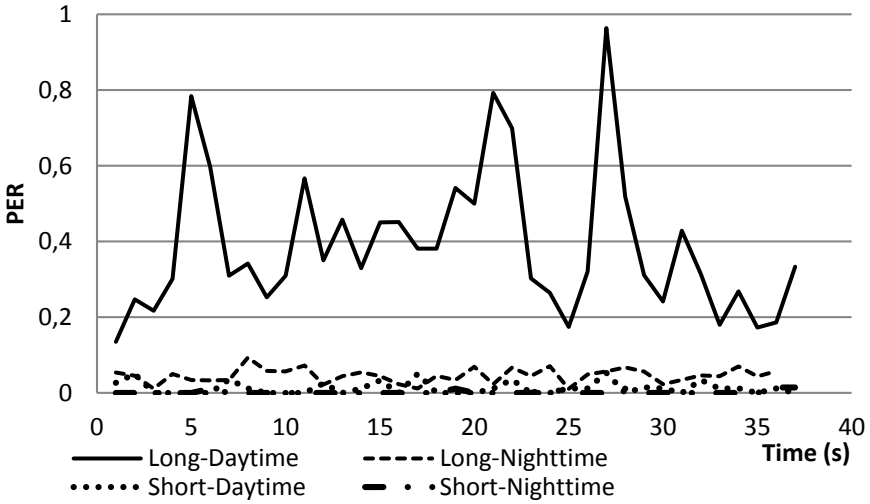

Figure 4.4: Time domain interference impact: Received PER_Z over time of a short and a long ZigBee link

4.3 Modeling ZigBee packet loss based on Wi-Fi traffic

A large number of space-frequency domain interference avoidance protocols exist and have been presented in literature [4.4], [4.9], [4.10], [4.11], [4.12], [4.13], [4.14], [4.15], [4.16], [4.17]. However, comparing the performance of these protocols with respect to one another in a real-life environment remains an open issue. There are a number of survey papers [4.18], [4.19] which intend to compare protocols with respect to their capabilities. However these survey papers compare the features of the considered protocols, and not their performance. A comparison between the performance of the implemented protocols not only requires all protocols to run within the same physical environment, but also that the interference environment is realistic and identical during all experiment runs.

A full comparison of the implemented protocols is therefore not only time consuming but has to be executed in repeatable interference environments. Moreover, these interference scenarios should behave like a real-life environment. This includes not only traffic patterns of all wireless devices but also the mobility of these devices. The generation of traffic patterns is a feasible target in current state of the art testbeds. However, the physical environment is not easily adjusted adequately to replay real-life mobility patterns. Although research is aiming at including large scale mobility within testbeds, the inclusion of realistic and repeatable mobility of a large number of devices is still problematic. Hence we cannot rely on a testbed which creates a repeatable realistic wireless interference environment.

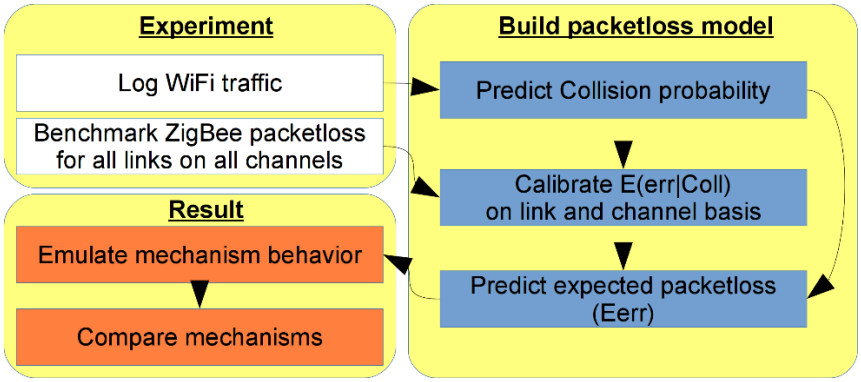

Figure 4.5: The used methodology enabling comparison of interference avoidance mechanisms without needing realistic, mobile and repeatable Wi-Fi interference.

To work around these issues we have chosen to tackle the performance assessment by building a model which predicts the expected packet loss based on

measured Wi-Fi interference traces. Therefore we extend the collision model we presented in [4.8] and calibrate it according to the methodology depicted in Figure 4.5. In the first phase we execute a benchmarking experiment where we measure the ZigBee network performance while simultaneously logging all Wi-Fi traffic on all Wi-Fi channels in 3 zones throughout the building as depicted in Figure 4.7.

The Wi-Fi logging enables estimating the collision probability between Wi-Fi and ZigBee packets (:= *Pr(Coll)*) based on the model of . Combining this with the measured ZigBee packet loss (:= PER_Z) allows us to do a regression analysis on the probability of a collision resulting in packet loss (:= *Pr(err|Coll)*), hence calibrating our model on a link basis to the real-life environment experienced on the testbed. We now predict the expected packet loss (:= *Eerr*) on a link level for all ZigBee channels at every experiment time based on real-life Wi-Fi traces by applying the calibrated model to the recorded Wi-Fi logs. On top of this prediction we emulate the behavior of space-frequency and time domain interference avoidance protocols. Last but not least we compare all interference avoidance protocol classes based on identical underlying interference.

4.3.1 Building the packet loss model

Packet loss occurring in a wireless network has essentially three major sources. The first one is insufficient Signal to Noise Ratio at the receiver, the second one is caused by signal deterioration due to multipath and frequency selective fading and the third origin of packet loss is due to interference. We assume the packet loss of all causes to be independent with respect to one another. Hence the total PER_Z in a real-life network is due to the combination of three independent events, depicted in formula (4.1).

$$PER_Z = 1 - \left((1 - PER_{SNR}) \times \left(1 - PER_{fading}\right) \times (1 - PER_{SIR})\right) \quad (4.1)$$

PER_{SNR} is solely dependent on the received signal strength and the noise floor of the receiving radio. PER_{fading} takes multipath- and frequency selective fading into account. Fading occurs when the signal transmitted is attenuated in a frequency dependent manner. This typically occurs when the signal combines with one or more reflections of itself at the receiver. Finally, PER_{SIR} is dependent on the interference generated in the environment.

PER_{SNR} and PER_{fading} are dependent on the physical environment and will therefore only change when either the location of the nodes is altered, or there are changes in the environment where the nodes are located. The nodes under test are static, and most elements within an office environment are static within the timeframe of a single experiment. Hence we can rewrite PER_Z as the combination of PER_{static} with PER_{SIR}.

$$PER_Z = 1 - \left((1 - PER_{Static}) \times (1 - PER_{SIR})\right) \quad (4.2)$$

In [4.8] we present a model which predicts the collision probability between ZigBee and WiFi. In [4.8] we validate this model by creating a test setup in which all collisions result in packetloss. However, in a real environment not all collisions result in packetloss. Within this work we extend this model to include a probability of a collision resulting in an error. Second, we only considered a single Wi-Fi channel overlapping with a ZigBee channel while in real life a single ZigBee channel is overlapped by 4 Wi-Fi channels. Third, some interference might not result into packetloss at all. In the following paragraphs we extend the model of [4.8] to include these features.

PER_{SIR} can in general be written as the probability of having a collision between interference and signal (:= *Pr(Coll)*) multiplied by the probability of a collision resulting in packet loss (:= *Pr(err|Coll)*).

$$PER_{SIR} = \Pr(Coll) \times \Pr(err|Coll) \quad (4.3)$$

In [4.8] we present a model for *Pr(Coll)* between ZigBee and a single Wi-Fi channel as follows:

$$\Pr(Coll)_{ch} \approx 1 - e^{-\frac{T_Z + T_{Z_0}}{T_{\overline{W}}}} \quad (4.4)$$

With T_Z the average ZigBee packet duration, T_{Z0} the ZigBee CCA time plus Rx to Tx turnaround time and $T_{\overline{W}}$the average Wi-Fi Inter Packet Delay (IPD). However, 4 Wi-Fi channels overlap a single ZigBee channel as depicted in Figure 4.6.

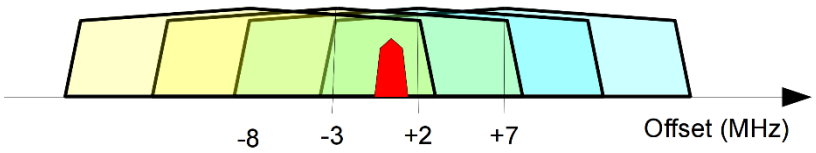

Figure 4.6: Four Wi-Fi channels inject interference in a single ZigBee channel

Hence the total *Pr(Coll)* is the combination of the $Pr(Coll)_{ch}$ of all independent but overlapping channels(4.5).

$$\Pr(Coll) = 1 - \begin{pmatrix} (1 - \Pr(Coll)_{-8}) & \times (1 - \Pr(Coll)_{-3}) \\ \times (1 - \Pr(Coll)_{+2}) & \times (1 - \Pr(Coll)_{+7}) \end{pmatrix} \quad (4.5)$$

The expected error given there is a collision is dependent on the total combined impact of all interferences during the receiving of the packet. It is a function of the received signal to interference ratio. Each signal to interference ratio (:=R) can therefore have a different *Pr(err|Coll).* We now write (4.2) as (4.6).

$$PER_{SIR} = \int \Pr(Coll, R) \times dR \quad (4.6)$$

The received signal strength is dependent on the pathloss between sender and receiver and the transmit power of the signal at the sender. The devices under test (DUT) are part of the testbed and therefore we can safely assume the received signal strength is static. This allows us to rewrite (4.6) into (4.7).

$$PER_{SIR} = \int \Pr(Coll, I) \times \Pr(err|Coll, I) dI \quad (4.7)$$

With I the measured interference strength. Below a certain interference level the probability of packetloss given collision is as good as zero. We approximate this by introducing an interference threshold below which Pr(*err*|*Coll,I*) is zero. (4.9) can therefore be limited to the range where packetloss might occur (4.8).

$$PER_{SIR} = \int_{I=Th}^{+\infty} \Pr(Coll, I) \times \Pr(err|Coll, I) dI \quad (4.8)$$

(4.8) shows that the measured Wi-Fi traces will consist out of two major types of interference. Interference which might result in packetloss and interference which will not result in packetloss.

4.3.2 Experiment description

The executed experiments have two purposes. First of all *Pr(err|Coll)* is to be determined. Hence the experiments are designed in order to fill in the needed parameters of formulae (4.3), (4.4) and (4.5). Second, the experiments must enable the prediction of packetloss (:=*Pr(err)*) based solely on the calibrated model and the recorded Wi-Fi traces with a one second time granularity.

The experiments are run on the iMinds w-iLab.t testbed, depicted in Figure 4.7. This testbed consists of 200 ZigBee and Wi-Fi enabled nodes spread across three floors. Each node has a Tmote Sky [4.20] and two Wi-Fi$_{B/G}$ interfaces. Within the building there are no Wi-Fi$_N$ access points, hence we assume no Wi-Fi$_N$ activity is present. We use a single floor of this testbed where we have a

sufficient amount of Wi-Fi sniffers available closely located to the used sensor nodes.

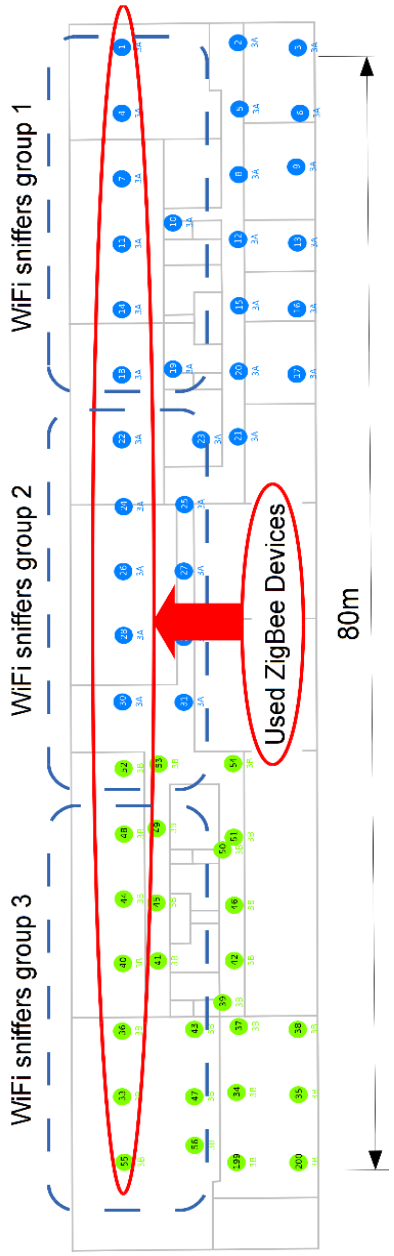

Figure 4.7: The used nodes of the iMinds w-iLab.t testbed

We have established three Wi-Fi sniffer groups. Each group of nodes logs all traffic on all Wi-Fi channels. This grouping allows to spatially differentiate the Wi-Fi traffic on the left side, middle and right side of the building as depicted in Figure 4.7. The Wi-Fi sniffers log for each received packet the time of arrival, the physical rate and the MAC payload size. This allows us to calculate $T_{\overline{W}}$ in formula (4.4) on a per second basis. On the ZigBee side we control T_Z and T_{Z_0} hence we can calculate *Pr(Coll)* on every channel for 3 locations in the building.

The benchmark experiment run on the ZigBee nodes assesses the packet loss for all links on all channels sequentially as depicted in Figure 4.8. We start an experiment by tuning all ZigBee nodes to channel 11. On this channel we let each node send 3000 broadcast transmissions. Inside each transmitted packet is a sequence number, allowing receiving nodes to log lost packets. Hence we have a full overview of all packet loss on channel 11 once all nodes have finished their transmissions, albeit measured at different time instances. However, we also have a timestamp on all transmissions allowing us to time-align the Wi-Fi and ZigBee logs.

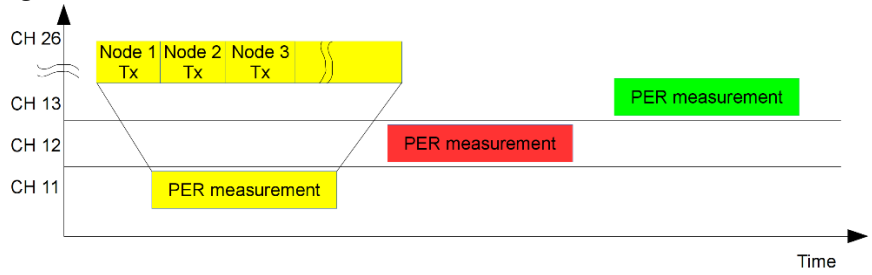

Figure 4.8: The ZigBee packet loss measurement sequence

4.3.3 Calibrating the model

We have already established that the major cause of packet loss variation on a link equals PER_{SIR}. Formula (4.8) shows that PER_{SIR} is dependent on the Interference strengths received. We log the signal strength of the received ZigBee packets. Ideally we should also log the Wi-Fi interference strength using the same antenna and location of the ZigBee receiver. However, we cannot achieve this ideal situation and we approximate this ideal situation by logging the received Wi-Fi interference on the Wi-Fi sniffers. A plot of the measured PER_Z and the *Pr(Coll)* is visualized in Figure 4.9.

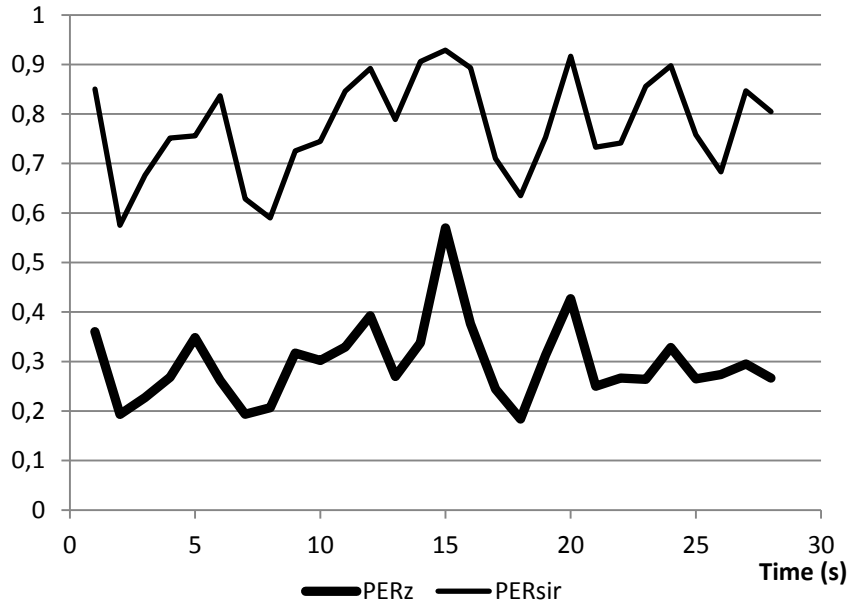

Figure 4.9: The measured PER_Z and predicted PER_{SIR} for a single link without threshold filtering

Figure 4.9 shows that for this specific link there is some correlation between the calculated *Pr(Coll)* and the measured PER_Z. There are however some artifacts which do not match. First it can be seen that *Pr(Coll)* is too high. Based on (4.8) we can conclude that a lot of Wi-Fi traffic is incorporated in the calculation of *Pr*(*Coll*) which does not influence PER_Z at all. Hence we filter the measured Wi-Fi traffic based on a threshold to only include packets with Wi-Fi signal strengths above the threshold. A higher threshold removes more low energy Wi-Fi packets from being incorporated in the model, and brings PER_{SIR} closer to *PER* as visualised in Figure 4.10. We can conclude that in this case the *Pr(err|Coll)* is as good as 1 when we incorporate a threshold of 30 or 35.

There are also links – even to the same destination as in Figure 4.9 – which have a very low average PER. However, the *Pr(Coll)* for a given destination is always identical, independent of the link quality between the ZigBee nodes. For such links the *Pr(err|Coll)* will be significantly lower, nearing to 0. Hence we need to determine three independent variables for every link namely the threshold, PER_{Static} and *Pr(err|Coll)*.

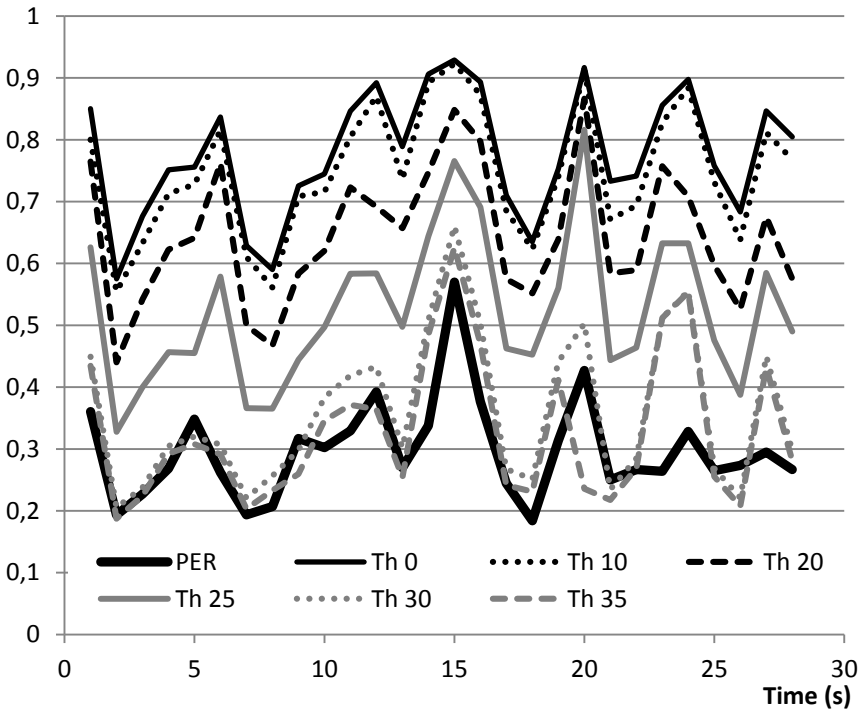

Figure 4.10: The measured PER_Z and PER_{SIR} with different thresholds for a single link

Figure 4.11 shows the model we try to fit. *Pr(err|Coll)* can be calculated from a correlation analysis between PER_{SIR} and PER_Z. However, this did produce a number of negative *Pr(err|Coll)* due to outliers in the data. In order to include all points of the measurement data while reducing the impact of outliers, especially high PER outliers, we opted to use (4.9). Moreover, the minimal values of PER_Z and PER_{SIR} are relatively stable for a link due to Wi-Fi background traffic (eg. Periodic broadcasts of APs), also visible in Figure 4.10.

$$E(err|Coll) = \frac{avg(PER_Z) - \min(PER_Z)}{avg(\Pr(Coll)) - \min(\Pr(Coll))} \tag{4.9}$$

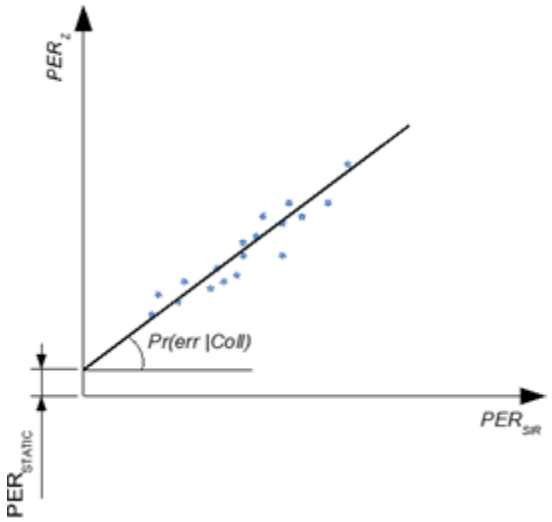

Figure 4.11: Example measured PER_Z and predicted PER_{SIR} points

Finally we determine PER_{Static} using

$$PER_{Static} = \min(PER_Z) - \Pr(err|Coll) * \min(PER_{SIR}) \qquad (4.10)$$

Out of these parameters we can now predict all packetloss based on the recorded Wi-Fi traces on a link basis as depicted in Figure 4.12. Therefore we now have a full view of all expected packet loss at any point in time for every link on every channel, calibrated on measurements sequentially executed on all channels.

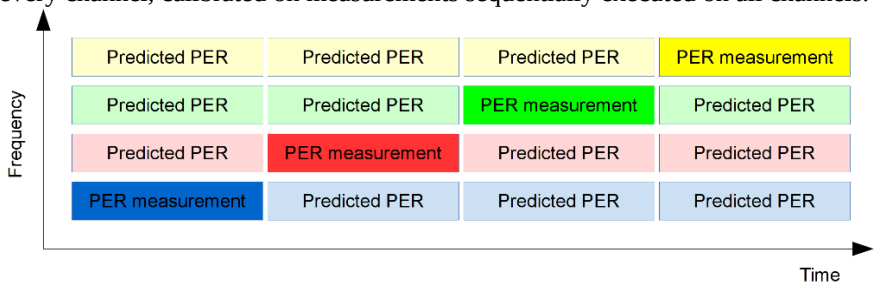

Figure 4.12: The PER measurements used for calibration and the predicted PER

This full time – space – frequency view allows us to emulate the behaviour of any given protocol on an identical basis, allowing full comparability of the results.

4.4 Comparing interference avoidance classes

In the previous section we have built and calibrated a model which allows to predict packetloss (:=*Pr(err))* for every link, channel and time based on measured Wi-Fi traces. Within this section we work on top of this model and predict the packetloss of specific interference avoidance mechanisms.

The average packet loss of a multichannel protocol is highly dependent on the channel selection executed by it. In [4.5] we have proposed a classification based on two domains, namely the channel selection mechanism, and the time at which a channel is switched. We have analyzed the impact of the channel selection class, but solely in a single shot channel selection. A single shot channel selection only selects a channel at the start of the experiment, and remains on that channel. We were unable to include slotted channel selections due to the lack of repeatable real-life experiments. However, in section 4.3 we built a full predictive model on top of which we can now emulate protocols.

4.4.1 Frequency domain

The protocol classes we identified in [4.5] for the channel selection a node can use are: 1) Follow the master, 2) pseudo random hopping, 3) internal triggered and 4) external triggered. A Follow the master channel selection essentially leads to all nodes operating on the channel decided by the master. In other words this is a single channel protocol. A typical example of pseudo random hopping is Bluetooth. Each node follows a dedicated hopping pattern. Once two nodes are synchronized they can communicate by calculating the current channel of the other node. An internal triggered approach allows any node to select its own optimal channel. RDT [4.17] is a protocol which allows such behavior, while still allowing full mesh communication with all neighboring nodes. Within this work the objective is to minimize PER_Z. In [4.5] we have concluded that the external triggered class is to be avoided for bad temporal connectivity can disable the selection of a new channel. Therefore we will focus on the first three classes. The emulated protocols all select the channel with the least amount of packet loss in an ‘a posteriori’ manner. This has as effect that the results are in fact the best results possible with this protocol class and is not dependent on a real-time channel selection.

ZigBee channel 26 is commonly referred to as the channel with the least amount of packet loss for ZigBee due to no overlapping Wi-Fi within the US. However, in Europe , amongst others, Wi-Fi may be deployed on channels 12 and 13. Within the w-iLab.t office building channels 12 and 13 are used, albeit rarely. However, ZigBee channel 26 might deteriorate significantly in case they are used. Therefore we also show results without incorporating channel 26, emulating a situation where all ZigBee channels are potentially overlapped by at least one Wi-Fi channel.

Figure 4.13 shows a comparison of the best achievable channel selection for each protocol. Random hopping results in the worst performance of 21.36% including channel 26 and 21.84% without the inclusion of channel 26. The best single channel solution results in a packet loss of 6.64% including channel 26 and 9.79% excluding channel 26. Hence we can indeed conclude that channel 26 is the best channel. RDT with a single shot channel selection performs best with a packet loss of 4.49% including channel 26 and a packet loss of 9.16% excluding channel 26.

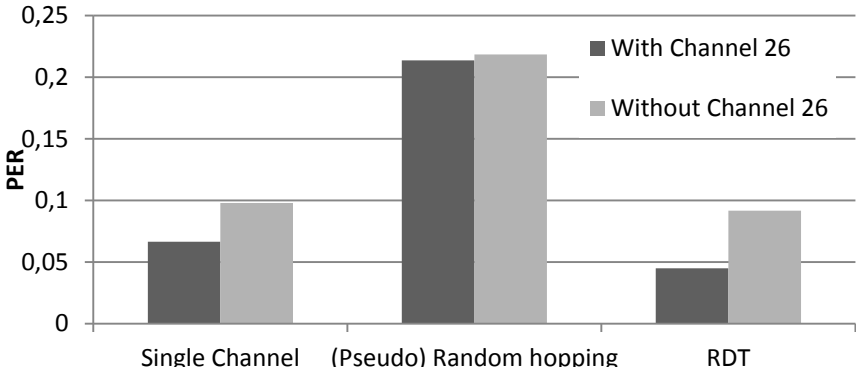

Figure 4.13: Three frequency domain interference avoidance protocols compared

Moving away from the single shot channel selection we now include slotted channel selection. Note that we do not include random hopping, for this already hops constantly across all channels.

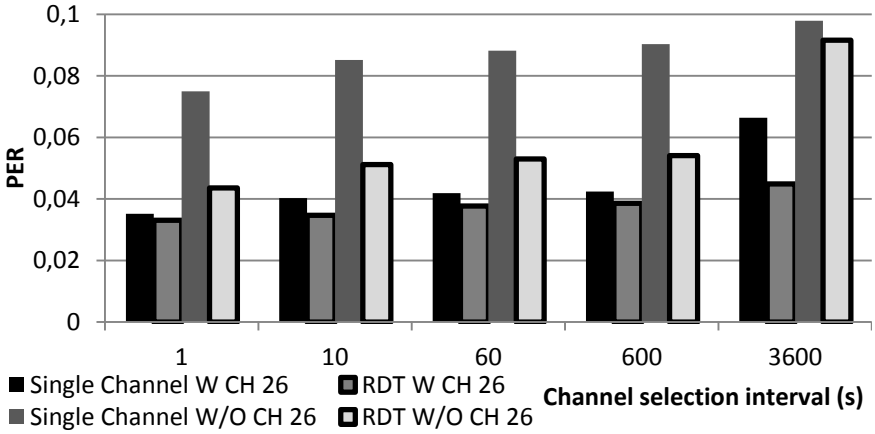

Figure 4.14: The effect on the PER of the channel selection interval

In case we include channel 26 we observe a close call between single channel and RDT performance. It is only for the largest interval (3600s) that a significant difference between RDT and single channel is to be noted. However, in case channel 26 is excluded the performance is significantly different. The single channel solution has a packet loss of at least 7.5%, while for RDT this is 4.36%. Looking at the impact of the different channel selection intervals we conclude that the performance drops significantly in case the interval is larger than 10 minutes. The performance of the 1 and 10 minute selection intervals is almost identical. Lower channel selection intervals improve upon these. However, we fear that practical feasibility of doing a good channel selection within a timeframe of 10s or even 1s might be unfeasible. Table 4.1 gives a comparison of all results in the space-frequency domain with all channel selection intervals.

Interval	**Single Channel**		**Random hopping**		**RDT**	
	With CH 26	W/O CH 26	With CH 26	W/O CH 26	With CH 26	W/O CH 26
1 s	0.0352	0.075	0.2136	0.2184	0.0331	0.0436
10 s	0.0403	0.0852			0.03468	0.0512
1 m	0.0419	0.0882			0.0377	0.053
10 m	0.0424	0.0903			0.0386	0.0541
1 h	0.0664	0.0979			0.0449	0.0916

Table 4.1: Frequency domain PER overview

4.4.2 Time domain

Within this section we analyze the implementation of CACCA in Wi-Fi and the implementation of CACCA in Wi-Fi as well as ZigBee. The cooperative carrier signaling approach presented in [4.7] makes Wi-Fi do backoffs for ZigBee, and should therefore in best case result in similar packet loss behavior to CACCA. Hence we only consider CACCA. Do note that the communication needed to execute the secondary transmission will not necessarily be safeguarded leading to reduced performance. In [4.8] we present the model for *Pr(Coll)* for all three scenarios considered here. We have concluded in [4.8] that implementing CACCA only in ZigBee does not gain significantly, which is why we do not consider ZigBee only CACCA.

We clearly see a significant reduction in PER_Z between CACCA enabled Wi-Fi and regular Wi-Fi. However, the results in [4.8] indicate a significantly larger PER_Z reduction for Wi-Fi + ZigBee CACCA in comparison to Wi-Fi only CACCA. Therefore we believe the calibration of our model will most likely contribute a large part of the packet loss due to PER_{Static}. However this packet loss is clearly dependent on the Wi-Fi traffic since it is concentrated around channels

12 and 22, two channels which suffer from a high Wi-Fi load. Hence our model most likely overestimates PER_{Static}, resulting in a lower performance improvement for the ZigBee + Wi-Fi CACCA case than expected. The average PER_Z across all channels for regular, Wi-Fi CACCA and Wi-Fi + ZigBee CACCA equal 20.5%, 4.2% and 3.38% respectively.

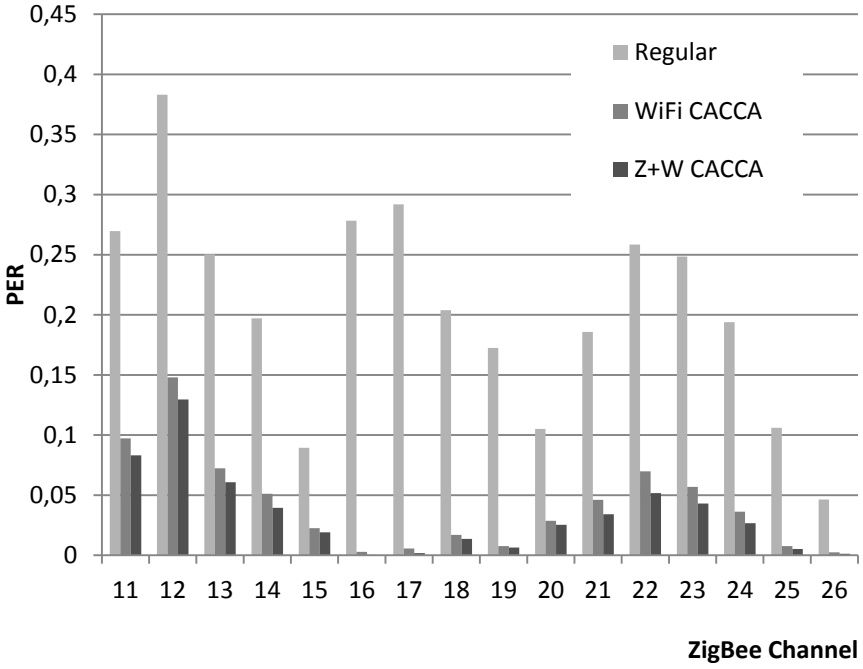

Figure 4.15: Comparison of regular CCA, Wi-Fi side CACCA and ZigBee + Wi-Fi side CACCA

4.4.3 Time and frequency domain

Last but not least we combine the time and frequency behavior of both previous sections. The results of a (pseudo) random hopping channel selection equal the average PER over all channels. Pseudo random hopping for regular Wi-Fi, Wi-Fi CACCA and Z+W CACCA this results in 20.5%, 4.2% and 3.38% packet loss respectively. In the remainder of this section we will only consider Single channel and RDT.

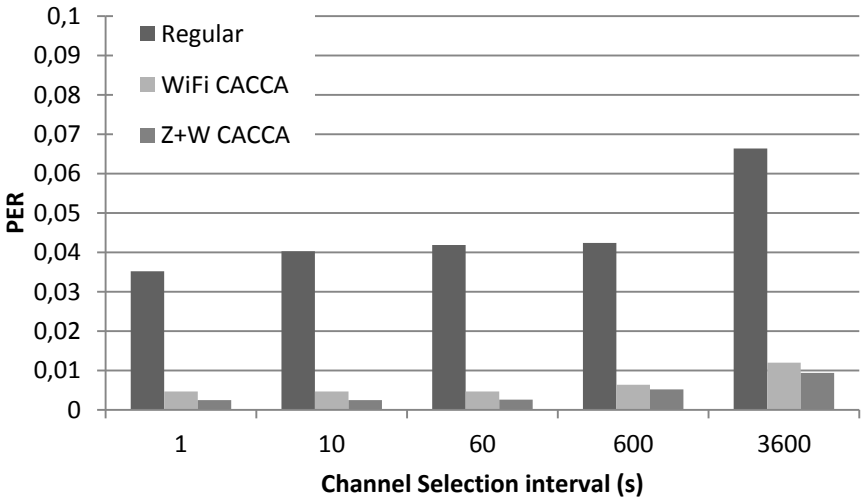

Figure 4.16: Combining single channel with CACCA

In the single channel case the remaining PER_Z crosses the 1% boundary only in the Wi-Fi CACCA case with a channel selection interval of 1h. In all other cases PER_Z remains below 1%. The average PER_z is reduced with a factor 6.96 in the Wi-Fi CACCA case and a factor 10.19 in the Z+W CACCA case.

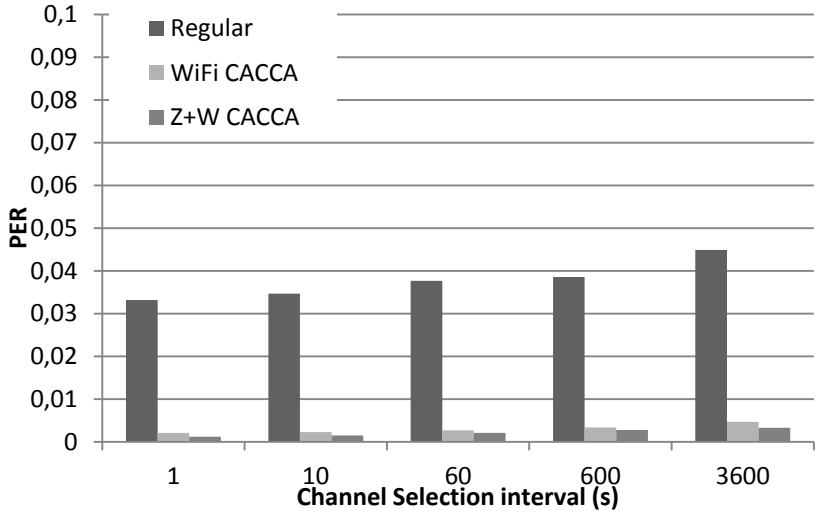

Figure 4.17: Combining RDT with CACCA

RDT already performs well in comparison to single channel. This trend is further found when combined with CACCA. In the worst scenario – Wi-Fi

CACCA with a one hour channel selection interval – PER_Z equals 0.47%. The average PER_Z for Wi-Fi CACCA equals 0.3% and for Z+W CACCA 0.22%, a reduction with a factor 12.44 for Wi-Fi CACCA and a factor 17.34 for the ZigBee and Wi-Fi CACCA case.

4.4.4 CACCA impact on Wi-Fi

Under most circumstances Wi-Fi does not backoff for ZigBee. Hence the throughput achieved by Wi-Fi is usually not influenced by ZigBee traffic. However, the goodput might be influenced due to increased packet loss [4.3]. The impact of implementing CACCA can therefore be twofold. On the one hand it will reduce the amount of collisions between ZigBee and Wi-Fi, potentially increasing the goodput. On the other hand it will reduce the achievable throughput since it will backoff in case of ZigBee activity within the Wi-Fi band. We want to minimize the impact of CACCA on Wi-Fi. Therefore we propose that Wi-Fi does not increase its collision window when it does a backoff for ZigBee. This has as effect that the only impact ZigBee activity has on CACCA enabled Wi-Fi is the reduction of the available air time. It does not influence the MAC behavior in any other way.

Note that this approach is not possible when employing the cooperative carrier signaling approach [4.7]. Thus the impact in [4.7] will not only be due to reduced air time, but also due to the higher collision window of the Wi-Fi MAC mechanism.

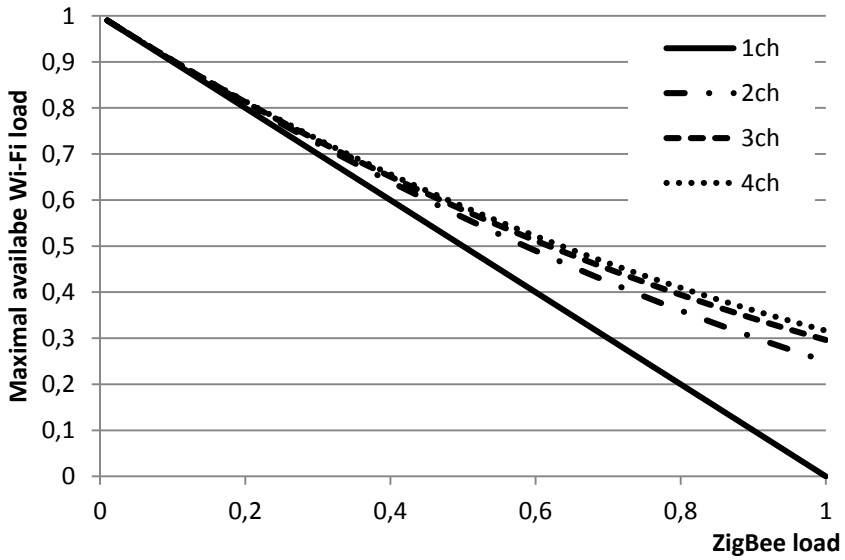

Figure 4.18: Spreading the ZigBee load on multiple channels reduces the impact on Wi-Fi

Four ZigBee channels are within the band of a single Wi-Fi channel. Each channel supports a single network which we assume has an average channel occupation denoted by δ. These four channels are independent w.r.t. one another. Hence the total percentage of time the Wi-Fi channel is free equals the combination of all four channel occupations and thus becomes formula (4.11).

$$\delta_W \approx (1-\delta_{Z1}) \times (1-\delta_{Z2}) \times (1-\delta_{Z3}) \times (1-\delta_{Z4}) \quad (4.11)$$

With δ_W the percentage of time the Wi-Fi channel is available and δ_{Zx} each ZigBee channels average occupation.

Hence the total remaining air time for Wi-Fi reduces by the combination of the ZigBee traffic in the four overlapping ZigBee channels. In contrast, the available Wi-Fi air time will increase if a protocol is spreading its load over multiple channels instead of one as shown in Figure 4.18.

This negative effect on Wi-Fi does not necessarily result in a worse experience to the Wi-Fi end-user. There might indeed be a drop in maximum Wi-Fi throughput when using CACCA. However, Wi-Fi can always decide not to care about the ZigBee activity in case its performance is not sufficient anymore. We conclude by stating that CACCA enabled Wi-Fi increases the reliability significantly, while the impact on Wi-Fi performance can be safeguarded.

4.5 Conclusion

Cross-technology packet loss between ZigBee and Wi-Fi is a major issue in wireless sensor networks used within the internet of things. Earlier work has already studied different mechanisms to reduce the impact of Wi-Fi on ZigBee. However, one of the key open issues is a comparative study of the performance of these cross-technology packet loss reducing mechanisms within a real-life environment.

Within this work we do a comparative study based on a real-life testbed environment. In order to circumvent the problem of repeatable and mobile experiments within a real-life office environment we model the ZigBee packet loss based on the combination of a collision model and testbed experiments. We calibrate the collision model to the real environment by logging the Wi-Fi traffic while doing a ZigBee benchmark experiment. This calibrated model can then predict the packet loss of every ZigBee link on every channel at every time instance based on the recorded Wi-Fi logs.

We use the calibrated model to compare the performance of three frequency based interference avoidance classes and one time based interference avoidance class. We show that RDT has an average packet loss of 4.49%, followed by a

single channel approach which has 6.64% packet loss and finally a (pseudo) random hopping approach which has 21.36% packet loss. Moreover we conclude that a dynamic channel selection should be executed minimally every 10 minutes since a significant performance drop occurs with a 1 hour channel selection timeout. With regards to the time based interference avoidance we conclude that a Wi-Fi side CACCA implementation reduces the average packet loss across all channels from 20.5% to 4.2% (a factor 4.88) and a ZigBee + Wi-Fi side CACCA reduces the packet loss to 3.38% (a factor 6.07). Finally the packet loss when combining time and frequency domain interference avoidance remains below 0.47% in the RDT case and below 1.2% in the single channel case.

4.6 References

[4.1] Yuan Wei, Wang Xiangyu, and J-P M.G. Linnartz, "A coexistence mofel of IEEE 802.15.4 and IEEE 802.11b/g," in 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux, 2007.

[4.2] Zhen Bin, Li Huan-Bang, Hara Shinsuke, and Kohno Ryuji, "Clear Channel Assessment in intergrated medical environments," EURASIP Journal on Wireless Communication Networks, p. 8, 2008.

[4.3] S Pollin, I Tan, B Hodge, C Chunand, and A Bahai, "Harmful Coexistence Between 802.15.4 and 802.11: A measurement-based study," in Proc. Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), 2008, pp. 1-6.

[4.4] M Hossian, A Mahmood, and R Jantti, "Channel ranking algorithms for cognitive coexistence of IEEE 802.15.4," in 20th IEEE international symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Tokyo, Japan, 2009, pp. 112-116.

[4.5] Lieven Tytgat, Opher Yaron, Ingrid Moerman, and Piet Demeester, "Analysis and experimental verification of frequency based interference avoidance mechanisms in IEEE 802.15.4," IEEE/ACM transactions on networking, 2013.

[4.6] Huang Jun, Xing Guoliang, Zhou Gang, and Zhou Ruogu, "Beyond co-existence: Exploiting Wi-Fi white space for ZigBee performance assurance," in 18th IEEE International Conference on Network Protocols (ICNP), Kyoto, Japan, 2010.

[4.7] Xinyu Zhang and G. Kang Shin, "Cooperative carrier signaling: harmonizing coexisting WPAN and WLAN devices," IEEE/ACM transactions on networking, pp. 426-439, april 2013.

[4.8] Lieven Tytgat, Opher Yaron, Sofie Pollin, Ingrid Moerman, and Piet Demeester, "Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment," EURASIP Journal on Wireless Communications and Networking, no. 2012-137, 2012.

[4.9] HART Communication Foundation. WirelessHART Technology. [Online]. http://www.hartcomm.org/protocol/wihart/wireless_technology.html

[4.10] K J Muoung, S Y Shin, H S Park, and W H Kwon, "802.11b Performance Analysis in the Presence of IEEE 802.15.4 Interference," IEICE Transactions on Communications, vol. B, no. 90, pp. 176-179, 2007.

[4.11] S W Hoi-Sheung, J Walrand, and Mo Jeonghoon, "McMAC: A parallel rendezvous multi-channel MAC protocol," in IEEE Wireless Communications and Networking Conference (WCNC), Hong Kong, 2007, pp. 334-339.

[4.12] R Balamuthi et al., "A TV whitespace spectrum sensing prototype," in New frontiers in Dynamic Spectrum Access Networks (DySPAN), Aachen, Germany, 2011, pp. 297-307.

[4.13] International Society of Automation. ANSI/ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications. [Online]. http://www.isa.org/ISA100-11a

[4.14] B Kaigui, P Jung-Min, and C Ruiliang, "Control Channel Establishment in Cognitive Radio Networks using Channel Hopping," IEEE journal on Selected Areas in Communications (JSAC), vol. 29, no. 4, pp. 689-703, 2011.

[4.15] R Maheshwari, S Jain, and S R Das, "A measurement study of interference modeling and scheduling in low-power wireless networks," in Proceedings of the 6th ACM conference on Embedded network sensors systems (SenSys '08), New York, USA, 2008, pp. 141-154.

[4.16] A Nasipuri, J Zhuang, and S R Das, "A multichannel CSMA MAC protocol for Multihop Wireless Networks," in Proceedings of Wireless Communications and Networking Conference (WCNC), New Orleans, USA, 1999, pp. 1402-1406.

[4.17] N Shacham and P King, "Architectures and performance of multichannel multihop packet radio networks," IEEE Journal on Selected Areas of Communications (JSAC), vol. 5, no. 6, pp. 1013-1025, 1987.

[4.18] R Soua and P Minet, "A survey on multichannel assignment protocols in Wireless Sensor Networks," in Wireless Days (WD), IFIP, Niagara Falls, Canada, 2011.

[4.19] O D Incel, "A survey on multi-channel communication in wireless sensor networks," Computer Networks (Elsevier), vol. 55, no. 13, pp. 3081-3099, 2011.

[4.20] TMote Sky datasheet. [Online]. http://www.snm.ethz.ch/snmwiki/pub/uploads/Projects/tmote_sky_datasheet.pdf

[4.21] ZigBee Alliance. ZigBee Technical Documents. [Online]. http://www.zigbee.org/Standards/Downloads.aspx

[4.22] Intech Web Exclusive. (2012, Oct.) Industrial Wireless Sensor Networks: Trends and developments october 2012. [Online].

http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=90824

[4.23] J Jangeun, P Peddabachagari, and M Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications," in Second IEEE International Symposium on Network Computing and Applications (NCA), 2003, pp. 249-256.

[4.24] Lieven Tytgat et al., "Techno-economical Viability of Cognitive Solutions for a Factory Scenario," in New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on , Aachen, 2011, pp. 254-264.

[4.25] (2013) Conrad battery cost. [Online]. http://www.conrad.be/ce/nl/product/658011/Conrad-Energy-alkaline-penlitebatterij-15-V-LR06-AA-LR6-AAB4E-AM3-M-MN1500-815-E91-LR6N-15A-KAA-R6-R06-BA;jsessionid=7F6CF9A094B3268060466962C9425FDA.ASTPCEN28

[4.26] J F Moore, "Predators and prey: A new ecology of competition," Harvard Business Review, vol. III, no. 71, pp. 75-86, May 1993.

[4.27] IMEC. Cognitive solutions using imec's spectrum sensing pave the way towards cognitive radios. [Online]. http://www.imec.be/ScientificReport/SR2010/2010/1159118.html

[4.28] ZigBee Alliance. (2011, July) 100 ZigBee Smart Energy Products Now ZigBee Certified. [Online]. http://www.zigbee.org/News/AlliancePressReleases.aspx?1=1&moduleID=778&Contenttype=ArticleDet&ArticleID=324

[4.29] ABI Research. (2011, May) 850 Million IEEE 802.15.4 Chipsets to Ship in 2016, Despite Strong Competition from Bluetooth, Says ABI Research. [Online]. http://www.businesswire.com/news/home/20120511005889/en/850-Million-IEEE-802.15.4-Chipsets-Ship-2016

[4.30] (2009, Jan.) Typical profit margins on electronic sales. [Online]. http://www.answerbag.com/q_view/51115

[4.31] K Casier et al., "Extending operational models to perform micro optimizations," in Proceedings of ECOC2007, the 33rd european Conference and Exhibition on Optical Communication, Berlin, 2007.

[4.32] Farnell. FTP wire cost. [Online]. http://be.farnell.com/pro-power/cbbr6332/cable-cat5e-ftp-305m/dp/3787977

[4.33] (2013) ZigBee module cost. [Online]. http://be.farnell.com/jsp/search/browse.jsp?N=2002+202652+110143547&Ns=P_PRICE_FARNELL_BE|0&Ntk=gensearch&Ntt=zigbee&Ntx=mode+matchallpartial&locale=nl_BE&appliedparametrics=true&getResults=true&suppressRedirect=true&isRedirect=&originalQueryURL=/jsp/sear

5

Coexistence Awareness: the way forward for wireless factory automation?

The three previous chapters considered the technical possibilities to improve the performance of an IEEE 802.15.4 based sensor network within an IEEE 802.11 prone interference environment. However, technological advances do not necessarily result in adoption of these advances in real devices. Technological advances are typically only adopted in case 1) the end-user is willing to pay for a solution including this technological advancement and 2) there is a viable business case for device manufacturers

In trying to answer the first question we assess the total cost of ownership of an IEEE 802.15.4 based wireless factory automation scenario. We compare the different CACCA deployment alternatives with a wired deployment, the ground truth in factory automation.

With regards to the second question we analyze the business ecosystem involved in supplying the end-user with CACCA enabled devices. CACCA is a technology which needs to be incorporated into the radio's regular CCA mechanism. As such device manufacturers need a viable CACCA business case for its incorporation. The ecosystem analysis investigates the factors which might hamper or foster the uptake of CACCA by device manufacturers.

Lieven Tytgat, Vânia Gonçalves, Opher Yaron, Sofie Pollin, Anand Raju, Ingrid Moerman, Piet Demeester

Submitted to Internation journal of Assembly Technology and Management

Abstract - Wireless sensor networks can help in reducing the total cost of ownership of a complex production system in comparison to wired sensor solutions. However, the reliability of wireless sensor networks like wirelessHART, ISA100.11a, ZigBee, etc. – all based on the IEEE 802.15.4 standard – can be degraded significantly when coexisting with Wi-Fi networks. Hence current wireless sensors can pose a huge economic risk when used in monitoring and control of assembly automation. Coexistence Aware Clear Channel Assessment (CACCA), an interference avoidance mechanism developed earlier by iMinds, reduces this degradation drastically. We analyze the economic impact CACCA has on the total cost of ownership for a wireless sensor deployment, and compare this to a wired deployment – the ground truth in assembly automation. Furthermore we study the business ecosystem in order to determine the factors potentially influencing manufacturer's uptake of CACCA.

5.1 Introduction

Industrial production systems continuously aim to produce cheaper, faster with less scrap and increased flexibility. As result an increasing amount of sensors and actuators are used in a production system. All of these sensors need to get installed and wired up. Therefore, the total sensor wiring cost is ever increasing. Even more, supporting flexible placement or mobility of sensors is not easily handled with wired connectivity, resulting in a push towards wireless sensors.

Wireless technologies like ZigBee[5.1], Wireless HART[5.1], ISA 100.11a [5.3], etc. – all based on the IEEE 802.15.4 standard – are perfectly suited to support wireless monitoring and control since it targets low cost, low energy consumption and low throughput applications. These technologies support a large range of wireless and mobile sensors and are gaining quite some momentum [5.4][5.5]. However, IEEE 802.15.4 based wireless technologies – for simplicity further referred to as ZigBee – experience problematic reliability when deployed in a dense Wi-Fi environment due to high impact of interference from Wi-Fi on ZigBee [5.6][5.7] and is seen as one of the main inhibitors of WSN uptake in industrial automation[5.8]. Although ISA 100.11a and Wireless HART have mechanisms to reduce this impact, they still suffer from a severe drop in communication reliability under high Wi-Fi interference[5.9]. We hence conclude that current wireless solutions based on IEEE 802.15.4 are not yet able to deliver the reliability that is needed for industrial control.

Coexistence Aware Clear Channel Assessment (CACCA) holds great promise in mitigating interference between Wi-Fi and ZigBee based networks allowing ZigBee to support higher reliability cases needed for wireless assembly automation. However, increased reliability is not necessarily sufficient to guarantee economic viability of wireless communication within a factory

automation scenario. Therefore we analyse a specific assembly scenario, which we elaborate on in section 2. Section 3 then assesses the impact of Wi-Fi on ZigBee communication reliability and energy consumption with and without the usage of CACCA. It is then possible to assess the economic impact of the different deployment alternatives within the factory scenario, and compare them to a wired deployment, which is done in section 4. Section 5 highlights the factors that may facilitate or hinder the actual incorporation of CACCA into Wi-Fi and ZigBee devices. Conclusions are given in section 6.

5.2 Scenario Description

In order to gain meaningful insight into the use of CACCA we look at a realistic scenario for which we can identify accurate data. We make viable assumptions when such data is not available. More specifically, we consider a modern electronics contract manufacturer that operates multiple Surface Mount Technology (SMT) assembly lines. A mid-size manufacturer may operate a production floor with 15 assembly lines in parallel, depicted in Figure 5.1. Each line makes 300 € profit per hour and has a turnover of 700 € per hour.

Each line includes 3-4 robots and one oven, and is constantly monitored by 2 human operators on the production floor. Each robot contains 2 Wi-Fi cameras and 7-8 different ZigBee sensors, while the ovens contain 10 ZigBee sensors each, bringing the total number of sensors throughout the production floor to 600. They monitor the temperature and other parameters of machinery and processes on the assembly line, and transmit it periodically to a central control and monitoring system. This system alerts human operators of various types of malfunctions, e.g. component-feed problems and overheating, which typically happens multiple times a day.

The wireless LAN in the factory is composed of 100 Wi-Fi devices including Wi-Fi cameras, access points, laptops, portable terminals and smartphones. For example, each of the operators of the assembly lines has a portable terminal that he uses for downloading control software to the assembly machinery, verify that proper material is loaded in the robots, etc. Each production line has a dedicated Wi-Fi AP and a central ZigBee controller to guarantee single hop connectivity. Due to the dense environment these APs are using multiple frequencies within the 2.4GHz bands. They are operating on 4 orthogonal channels – channels 1, 5, 9 and 13 – which are assigned to each line in a round robin manner. Hence the ZigBee and Wi-Fi devices will need to coexist on the same frequency.

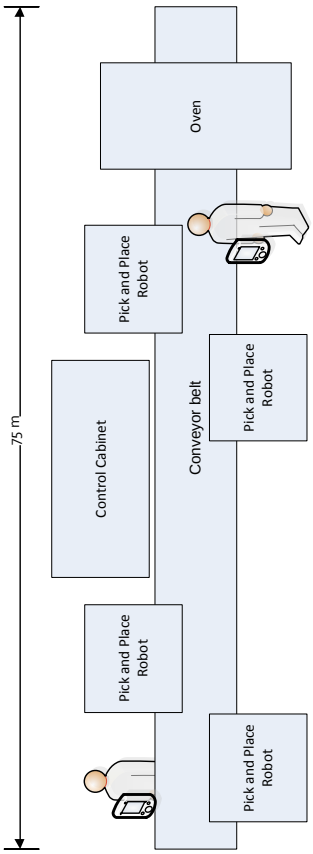

Figure 5.1: A typical electronics production line

We assume that every assembly line develops conditions that cause production failures if not reported on time. We divide these failures into two groups, major and minor failures. Major failures result in an immediate stop of the assembly line and occur in average once a year on each line when no monitoring sensors are deployed. Major failures involve 10.000 € damage to machinery, which costs 10.000 € * 1 occurrence/year * 15 lines * 5 y = 750 k€ in repairs over a 5 year period, and cause 300 €/h * 24 h * 15 lines * 5 y = 540 k€ profit loss. With a total cost of 1.290 k€ over 5 years, major failures represent a very large potential loss for the factory. Minor failures would occur on average once an hour on each line in case no monitoring sensors are deployed. Minor failures involve assembly of defective products for 30s, which over a 5 year period cost 700 €/h / 3600 s/h * 30 s * 24 occurrences/day * 365 days/y * 15 lines * 5 y= 3832.5 k€ in lost material,

and cause 300 €/h / 3600 s/h * 30 s * 24 occurrences/day * 365 days/year * 15 lines * 5 y= 1642.5 k€ profit loss. With a total cost of 5.475 k€ over 5 years, Minor failures represent an even larger potential loss than the Major failures. In summary, the potential total cost of failures in a 5 year timeframe amounts up to 6.765 k€. This significant figure is the reason why monitoring sensors are indeed deployed in assembly lines and other industrial plants.

Due to these substantial production losses and repair costs, it is clear that the factory owner is interested in installing monitoring sensors in order to avoid failure conditions from happening.

5.3 Technical Analysis

Wi-Fi as well as ZigBee use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the mechanism for gaining access to the wireless channel. CSMA/CA operates by doing at least one Clear Channel Assessments (CCA) before each transmit, which results in the channel being assessed as busy or free. Depending on the outcome it will then either commence the transmission (free channel) or do a backoff and retry later (busy channel). A regular CCA tries to assess the channel as busy or free for its own technology in order to minimize the amount of intra-technology collisions. However, in the case of co-location of multiple heterogeneous technologies CCA does not necessarily avoid inter-technology collisions since regular CCA is designed only with its own technology in mind.

Coexistence Aware CCA is an extension to regular CCA. CACCA extends regular CCA with one or more parallel CCA paths that are focused on detecting other technologies occupying the same channel. In our case it allows a ZigBee device to detect Wi-Fi activity reliably, or it allows a Wi-Fi device to detect ZigBee activity reliably. As a result technologies not only backoff for their own technology, but also for other co-located heterogeneous technologies, allowing joint operation on identical frequency bands with significantly reduced collision probabilities.

CACCA is a mechanism which is implemented in one technology to detect other technologies. Hence it does not necessarily need to be deployed in all co-located technologies. Within this paper we therefore differentiate four different deployment alternatives. The first corresponds to the status quo, thus the standard Wi-Fi and ZigBee without CACCA. The second deployment alternative consists of deploying CACCA on ZigBee only. In the third alternative CACCA is deployed only in Wi-Fi while in the fourth CACCA is deployed in both ZigBee and Wi-Fi. The reliability of a wireless link is determined by the Packet Error Rate (PER), which is the average amount of packet-loss incurred on a link. In this paper we focus on the PER occurring in the ZigBee network (PER_Z), as this network is used

for factory automation and a change in the delivered reliability can have a significant economic impact due to malfunctioning of the machinery.

5.3.1 Achievable ZigBee reliability

In [5.10] we have evaluated PER_Z in the different scenarios. However, we did not incorporate the effect of retransmits. Since it is common to use retransmissions to overcome transmission failures, we assume up to 4 retransmissions for each packet. We compare the ZigBee dataloss of these four different deployment alternatives, thus including the effect of retransmissions, in Figure 5.2. The maximum achievable MAC throughput by a Wi-Fi device without using CSMA/CA equals 42.3MBps [5.11] (54Mbps datarate, broadcast of 1500 byte MAC payload packets). The maximal achievable throughput is displayed in all figures.

It can be seen that the difference in PER_Z between alternative 1 (regular CCA) and alternative 2 (only ZigBee CACCA) is very modest. PER_Z for alternative 3 (only Wi-Fi CACCA) is significantly reduced under most Wi-Fi loads while in alternative 4 (both ZigBee and Wi-Fi CACCA) PER_Z is reduced under all Wi-Fi loads. Most applications cannot tolerate more than a certain amount of PER, which we assume to be 10%. An important measure is therefore the allowable Wi-Fi load which results in 10% PER_Z. For alternatives 1 and 2 this equals respectively 2.81 and 3.02 Mbps, alternative 3 allows up to 25.6 Mbps while the fourth alternative never reaches more than 10% PER_Z. The maximal PER_Z in this case equals 0.10%.

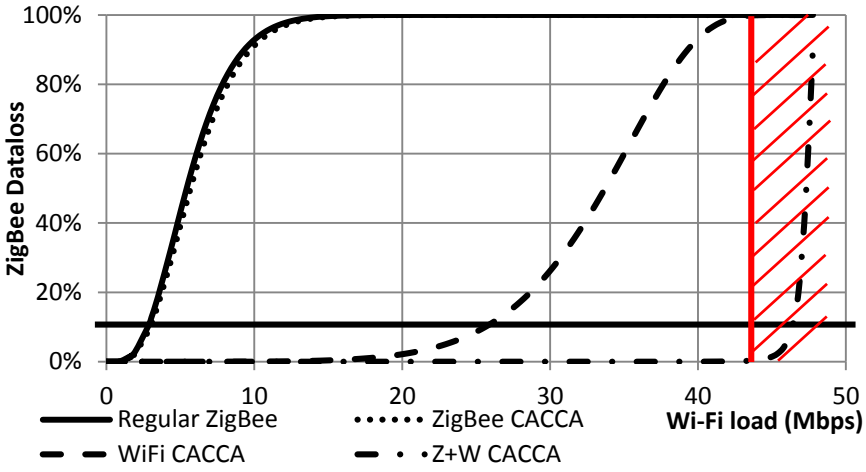

Figure 5.2: ZigBee dataloss as function of Wi-Fi load for 54Mbps Wi-Fi, 1500 bytes Wi-Fi packets and 100 byte ZigBee packets.

5.3.2 Implementation

Implementing CACCA on ZigBee allows it to detect Wi-Fi activity reliably. However, the amount of extra hardware needed – which is depicted in Figure 5.3– is large, since the analog as well as the digital parts are not able to accommodate the larger bandwidth needed for capturing a Wi-Fi transmission.

The amount of extra hardware needed to implement CACCA on Wi-Fi is small, as standard Wi-Fi analog and digital parts can be used for detecting ZigBee. Only the actual CACCA functionality – which is a small digital part as depicted in Figure 5.3 – needs to be added.

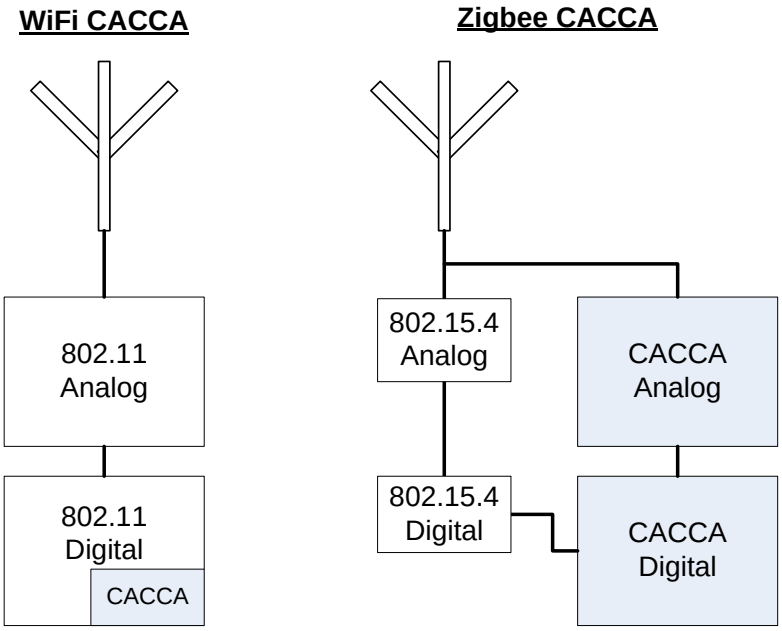

Figure 5.3: Additional hardware needed to implement CACCA on Wi-Fi and ZigBee

5.3.3 Power consumption

The power consumption of the wireless sensor nodes determines the battery replacement time. We use a Tmote Sky [5.12] powered at 3V as reference platform. Table 5.1 shows the nominal power consumption.

	Receive mode	Transmit mode	Standby mode
Current Consumption	21.8mA	19.5mA	5.1µA
Power Consumption	65.4mW	58.5mW	15.3µW

Table 5.1: Tmote Sky nominal characteristics

We assume every sensor needs to report its value and thus send a packet every second. The average duration of radio activation for the transmission of one packet, including waiting for and reception of acknowledgement, is 1.6ms. The wireless sensor does not need to remain in receive mode constantly, but can minimize the time it needs to spend in receive mode. We assume a wireless sensor node to receive configuration data once every 10s. With perfect synchronization the sensor node only needs to stay awake for 1.6ms, identical to the transmitter. The average node power consumption is the average of the power consumption due to 1) transmission of the sensor values to the central controller, 2) the receiving of the settings from the central controller and 3) the idle power consumption. The average power consumption over a 10s period thus becomes (5.1).

$$P_Z = \frac{16\text{ms} * 58.5\text{mW} + 1.6\text{ms} * 65.4\text{mW} + (10\text{s} - 16\text{ms} - 1.6\text{ms}) * 15.3\mu\text{W}}{10\text{s}} = 119.3\mu\text{W} \quad (5.1)$$

We now calculate the added power consumption due to the usage of CACCA on ZigBee devices. We assume the average power consumption of ZigBee side CACCA when active to be 100mW which is based on the power consumption of a spectrum sensing engine developed by IMEC[5.13]. CACCA is activated only during 4µs – the CCA time defined by the Wi-Fi standard – prior to the transmission of every packet. However, due to the need for external added hardware we assume that the hardware will need to be powered on during 100µs. Consequently, the average power consumed by CACCA when sending one packet per second equals 100mW * 100µs = 10µJ. The added power consumption because of CACCA contributes to 8.3% of the consumed transmit energy. The total power consumption for sensors equipped with CACCA equals 129.3µW. Above calculations do not include the power consumption due to retransmits.

Figure 5.4 gives an overview of the network lifetime as function of the Wi-Fi load. The maximal network lifetime when no Wi-Fi interference is present for regular ZigBee equals 2.43y. However, this drops quickly with growing Wi-Fi interference until it reaches the minimum of 0.51y at 8.2Mbps Wi-Fi rate. It does not go any lower due to the limited amount of retransmits allowed. Note that from this point onward the probability of having a successful data communication are very low. Adding CACCA to the ZigBee devices results in a lower maximum

network lifetime equal to 2.35y, and drops down to 0.49y at 8.2 Mbps Wi-Fi rate. Hence there is a small deterioration with respect to regular ZigBee. The Wi-Fi CACCA alternative has a maximal network lifetime equal to regular ZigBee. However a 10% drop in lifetime only occurs when the average Wi-Fi load reaches 26.8 Mbps and it results in the minimal network lifetime when the Wi-Fi load reaches 38.1Mbps. The ZigBee + Wi-Fi CACCA alternative remains at a constant 2.35y network lifetime for all Wi-Fi loads, hence there is no impact of the Wi-Fi load in this scenario.

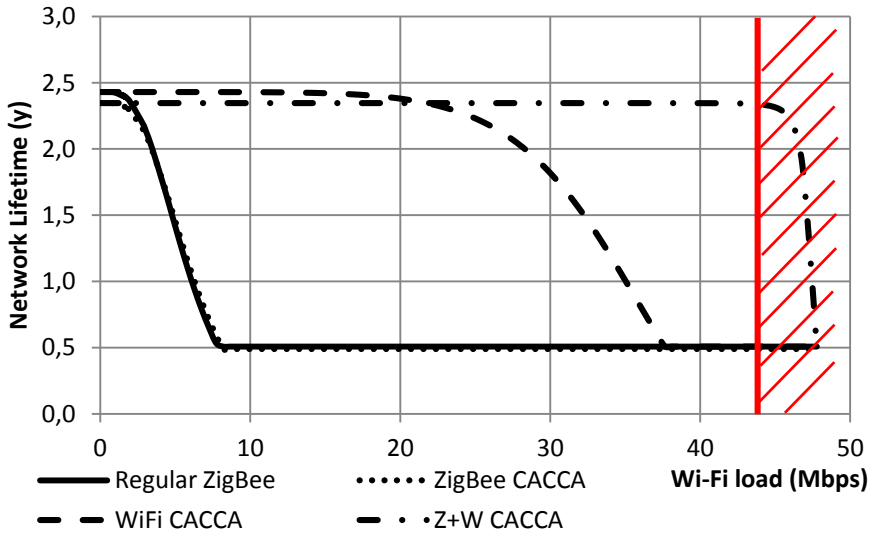

Figure 5.4: Average network lifetime for the different scenarios

5.4 Economic analysis

The economic analysis considers two major expenses, namely the operational expenses and the capital expenses. With regards to the capital expenses we solely look at the marginal deployment costs between a wired deployment and the four different wireless deployment alternatives. The wired operational expenses are a combination of the consequences of wire breakage – a minor failure with a downtime of 24h – and the wire repair expenses. For a wireless installation there are the consequences of communication errors combined with the expenses related to battery replacements during the 5 year period of operation. A summary is given in Table 5.2.

	Wired	Wireless
Capital Expenses	Planning of Wiring Wire cost Wire deployment cost	Wireless transceivers
Operational Expenses	Wire breakage consequences Repair of broken wires	Comm. error consequences Battery replacement

Table 5.2: Comparison between Wired and Wireless costs

5.4.1 Capital expenses

The Capex of the wired and wireless alternatives have a number of similarities and differences, depicted in Table 5.3. The sensor planning and placement costs are identical in all alternatives – wired and wireless – as the number and location of the sensors is identical in all cases. We will not consider these costs and only focus on the differences in investment costs.

In the wired scenario the wire placement needs to be planned and executed. We assume the total time per meter installation of wiring, including planning, at 6 minutes per meter with an installation cost of 60 € per hour[5.14]. The cost of the wires itself is estimated at 0.43 € per meter[5.15]. One production line has a total wire length of 17.25km, resulting in a total wiring installation cost for all lines of 103.5 k€ + 7.5 k€ = 111 k€.

The wireless investment cost differentiates with the wired in that is does not include wiring, but it needs wireless IEEE 802.15.4 transceivers. The pricing of wireless ZigBee modules ranges from 16.5 to 40 €[5.16]. For that reason we use an average additional wireless transceiver cost of 30 €.

The additional investment cost for nodes equipped with CACCA comes down to the extra price of a node that is equipped with CACCA. We will assess this price by first analyzing the marginal production cost associated with introducing CACCA in the Wi-Fi and/or ZigBee devices, and then estimating the retail price based on typical profit margins. In section 5.3.2 Figure 5.3 we have shown the difference in ZigBee and Wi-Fi CACCA implementation. The core of this engine is an Application Specific Integrated Circuit (ASIC) of which the production cost is estimated at 1€. Within a Wi-Fi device, no additional components need to be added and therefore we estimate the marginal production cost of incorporating CACCA in a Wi-Fi device at 1€. For ZigBee sensors it is necessary to add additional components. We approximate the marginal production cost of ZigBee CACCA at €10. We estimate the profit margins for electronics production at 60%, wholesale margins at 40% and retail margins at 20%[5.17]. These values should represent overestimations of the profit margins. We therefore estimate the marginal retail price at 5.21 times the marginal production cost. The marginal

CACCA investment cost therefore becomes 5.21€ for Wi-Fi and 52.1€ for ZigBee devices.

There are 600 ZigBee nodes and 100 Wi-Fi devices throughout the factory. The total additional investment in Alternative 2 therefore equals 31.2 k€, in Alternative 3 521 € and in Alternative 4 – 31.7 k€.

Cost allocation	Wired	ZigBee (Regular)	ZigBee CACCA	Wi-Fi CACCA	Z+W CACCA
Wire installation	X				
ZigBee module		X	X	X	X
ZigBee CACCA			X		X
Wi-Fi CACCA				X	X
Total CapEx (k€)	111	18	49.2	18.5	49.7

Table 5.3: Capital expenses for the different deployment alternatives

5.4.2 Operational Expenses

The operational expenses of a monitoring system are divided in expenses due to failures of the monitoring system and expenses to keep the monitoring system up and running. We will tackle the wired and wireless cases independently since the failure modes and the costs to keep the system up and running are drastically different.

Wired communications are assumed 100% reliable unless wires break. We assume a wire break once a year for every 20km of wire, which is 10 times higher than in case of an access network[5.18]. Moreover we assume a wire break to result in a minor line failure, but with a downtime of 24h since an electrician has to come and repair the wire. An average wire break therefore results in 300 €/h * 24 h = 7.2 k€ of profit loss. The average distance from monitoring cabinet – located in the middle of an assembly line – to sensor equals 75m / 4 = 18.75m. We add an additional 10m due to wiring not taking the straight path but following wire gutters, resulting in an average wire length of 28.75m. The failure rate for all lines due to wire breakage now equals 600 * 28.75 / 20000 = 0.86 per year, multiplied by 5 year this results in 4.31 breakdowns. The wired communication failure cost thus becomes 31 k€. The expenses to keep a wired monitoring system up and running equals the cost for repairing the broken wires. We assume a total cost of 1 k€ to fix a wire break, including the wire cost as well as the labor costs. Hence

the wire repair costs add 4310 € to the OpEx for a 5y timespan. The total OpEx for wired thus becomes 35.3 k€.

In wireless communications data gets lost with a certain probability, which is calculated in section 5.3. This has as effect that specific sensor signals will not reach the central controller, which will lead to a minor or major failure in case the sensor signal was issued to avoid a minor or major failure. Hence the average time between failures divided by the probability of losing this information in the communication path results in the mean time between failures (MTBF). The expenses due to communication failures are presented in Figure 5.5. We assume that the wireless sensors are battery powered. Depending on the estimated lifetime – calculated in section 5.3.3 – these batteries need to be replaced a number of times during the operational timespan. One sensor device needs 2 AA type batteries. A bulk price for AA batteries is assumed to be 0.93 € each[5.19]. We assume 5 minutes of labor per sensor at a labor cost of 60 € per hour. We assume the replacement of the batteries does not cause production downtime as this can be planned in advance. The total cost for installing batteries on all sensors then becomes 4.1 k€. We need at least 3 battery installments to cover a lifespan of 5y, thus the minimal battery cost equals 12.3 k€. However, depending on the amount of Wi-Fi traffic and the deployment alternative the battery cost increases. The total operational costs (OpEx) are the combination of the battery cost and the communication failure cost, presented in Table 5.4.

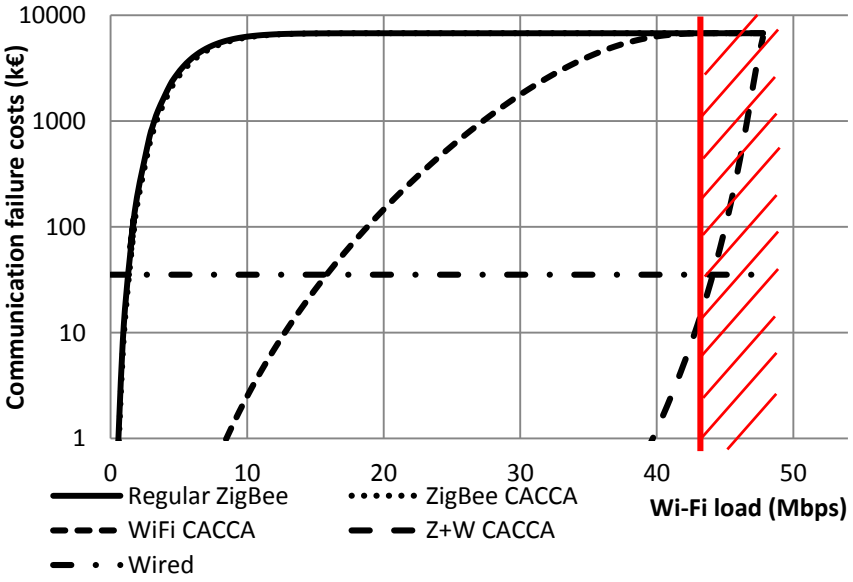

Figure 5.5: Communication failure costs as a function of the Wi-Fi load

Avg. Wi-Fi Load		No CACCA	ZigBee CACCA	Wi-Fi CACCA	Z+W CACCA
500 Kbps	Battery cost	12.3 K	12.3K	12.3K	12.3K
	Comm Fail	0.5 K	0.4 K	0	0
	Total OpEx	**12.8 K**	**12.7 K**	**12.3 K**	**12.3 K**
1 Mbps	Battery cost	12.3 K	12.3K	12.3K	12.3K
	Comm Fail	11.8 K	9.4 K	0 K	0 K
	Total OpEx	**24.1 K**	**21.7 K**	**12.3 K**	**12.3 K**
10 Mbps	Battery cost	41.2 K	45.3 K	12.3 K	12.3 K
	Comm Fail	6314.8 K	6205.8 K	2.7 K	0 K
	Total OpEx	**6366.0 K**	**6251.1 K**	**15 K**	**12.3 K**
20 Mbps	Battery cost	41.2 K	45.3 K	12.3 K	12.3 K
	Comm Fail	6764.7 K	6764.4 K	158.5 K	0.00 K
	Total OpEx	**6805.9 K**	**6809.7 K**	**170.8 K**	**12.3 K**
40 Mbps	Battery cost	41.2 K	45.3 K	41.2 K	12.3 K
	Comm Fail	6765.0 K	6765.0 K	6321.0 K	1.2 K
	Total OpEx	**6806.2 K**	**6810.3 K**	**6362.2 K**	**13.5 K**
42.3 Mbps	Battery cost	41.2 K	45.3 K	41.2 K	12.3 K
	Comm Fail	6765.0 K	6765.0 K	6696.8 K	6.3 K
	Total OpEx	**6806.2 K**	**6810.3 K**	**6738.0 K**	**18.6 K**

Table 5.4: Operational expenses for the wireless alternatives as a function of the Wi-Fi load

5.4.3 Conclusion

The total expenses which allow the monitoring sensor to communicate their data to the central line controller can now be calculated based on the CapEx and OpEx of the previous 2 sections and are shown in Table 5.5. Figure 5.6 shows the savings of the 4 wireless alternatives compared to a wired installation. The total expenses for a wired installation equal 188.0 k€. This is of course independent of the amount of Wi-Fi traffic in the factory. A regular ZigBee installation only performs satisfactory in case there is as good as no Wi-Fi traffic. The tipping point – the Wi-Fi load after which this alternative results in higher costs than wired – is at 1.9Mbps. Mediocre or high traffic loads cause a regular ZigBee network to have very bad reliability, resulting in enormous costs. The tipping point when only ZigBee is equipped with CACCA functionality is identical to regular ZigBee. Moreover, this scenario performs worse for low ZigBee loads due to the higher CapEx needs. In contrast only Wi-Fi side CACCA performs very good for low and mediocre Wi-Fi loads. This is due to the low CapEx needs as well as the significantly increased reliability under these circumstances. However, the reliability still suffers in case of Wi-Fi loads higher than 20 Mbps – the Wi-Fi CACCA tipping point – resulting in excessive expenses for these Wi-Fi loads. Finally, the Wi-Fi + ZigBee CACCA alternative present high savings under all real-world Wi-Fi loads and are limited to €68.3 k€ for all Wi-Fi loads. When compared to a wired installation we save 77 k€. The only Wi-Fi CACCA alternative outperforms the ZigBee + Wi-Fi CACCA alternative for low and medium Wi-Fi loads. However, the ZigBee + Wi-Fi CACCA alternative effectively limits the costs, removing the risk of high expenses due to communication failures.

Wi-Fi load	Wired	ZigBee (Regular)	ZigBee CACCA	Wi-Fi CACCA	Z+W CACCA
Low (500Kbps)	145.3	30.8	61.9	30.8	62.0
Medium (10 Mbps)	145.3	6382.0	6300.3	33.5	62.0
High (42.3 Mbps)	145.3	6824.2	6859.5	6756.5	68.3

Table 5.5: Total cost of ownership for all alternatives (k€)

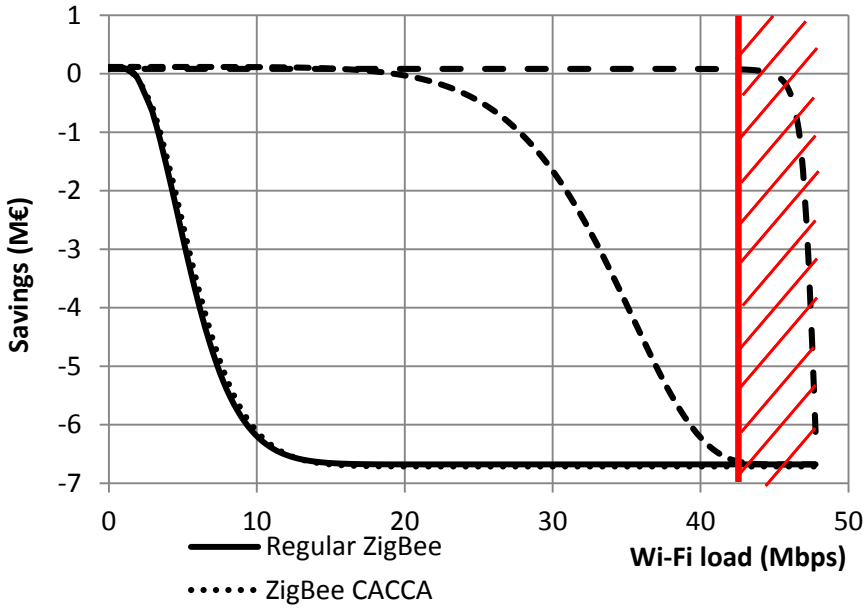

Figure 5.6: Savings for the different wireless alternatives in comparison to wired deployment.

5.5 Business Ecosystem Assessment of CACCA Implementation

Business ecosystem is defined in [5.20] as a "community supported by a foundation of interacting organizations and individuals – the organisms of the business world. This economic community produces goods and services of value to customers, who are themselves members of the ecosystem". For the purpose of this paper, we adapt the definition of the business ecosystem as an interconnected network of business stakeholders that are mutually dependent for their existence. The overall strength and sustainability of an ecosystem depends mainly on how each stakeholder contributes (adds value) to the ecosystem. Figure 5.7 represents such an ecosystem for Wi-Fi and ZigBee devices equipped with CACCA functionalities.

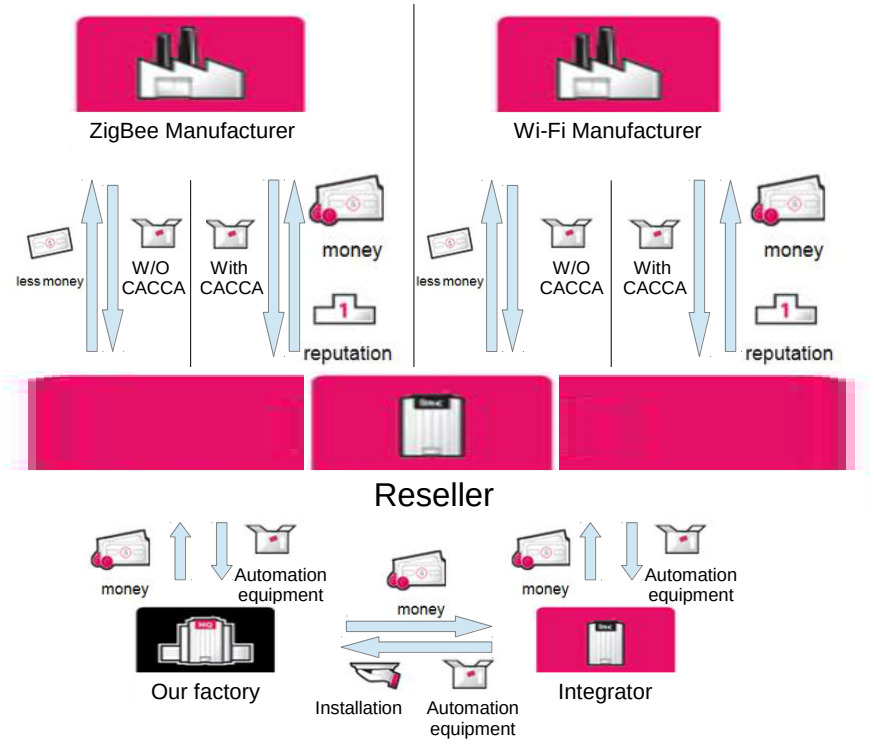

Figure 5.7: Business ecosystem for CACCA Implementation in a factory scenario

In section 5.4 we have shown that the highest savings are guaranteed when CACCA is deployed both on Wi-Fi and ZigBee devices, while reasonable savings are achieved when they are deployed only on Wi-Fi devices. However ZigBee and Wi-Fi Device Manufacturers need to absorb and promote CACCA mechanisms in their product portfolios. Analysis below elaborates strategic issues that Device Manufacturers could face hindering the rollout of CACCA enabled devices in the marketplace. Table 5.6 presents a summary of the major factors influencing possible rollout of CACCA enabled devices

5.5.1 Value Proposition for Device Manufacturers

The value proposition of developing and promoting CACCA enabled devices is currently not clear for Device Manufacturers. In section 5.4, we show that the factory can achieve a profit of 77.0 k€ in comparison to a wired deployment when Wi-Fi and ZigBee are CACCA enabled. Hence this can yield relatively high profit margins for Device Manufacturers. Wi-Fi and ZigBee manufacturers could

therefore initially target the industrial market where the need for those devices justifies higher sales price.

5.5.2 CACCA enabled product portfolio

The implementation of CACCA in a ZigBee device is more expensive and complex compared to its implementation in a Wi-Fi device. However, a single sensor manufacturer might be able to create a full product portfolio of ZigBee based sensors including CACCA functionality. In contrast, the range of Wi-Fi device types available in the market is significantly wider (access points, laptops, portable terminals, smartphones, etc.), making it almost impossible for a single manufacturer to create the full CACCA enabled product portfolio used in a typical factory. A single device manufacturer is thus more probable to create a full portfolio of ZigBee devices than creating a full product portfolio for Wi-Fi devices.

5.5.3 Capital Requirements

Costs involved in development, production, and implementation of CACCA in ZigBee and Wi-Fi devices could be an issue given the current economic conditions. However, ZigBee and Wi-Fi device manufacturers could be incentivized to co-develop and cooperate with each other in order to guarantee availability of CACCA enabled Wi-Fi as well as ZigBee devices, thus significantly reducing their risk. Moreover typical Wi-Fi traffic is mainly downstream. Hence only deploying CACCA enabled Wi-Fi APs, without making other devices CACCA enabled will already result in a significant increase in ZigBee reliability. As a result it might not be necessary for a Wi-Fi device manufacturer to build a full product portfolio of CACCA enabled Wi-Fi devices in one time, reducing the needed capital requirements.

5.5.4 Standardization Issues

Standardization bodies can have a key role in the adoption of new technologies by end-users. A standard creates well-known expectations for end-users and improves inter-vendor compatibility, hence reducing the risk arising with the investment in new technologies. On the manufacturers' side, standardization is somewhat double. On the one hand, device manufacturers tend to create lock-ins through the creation of non-standard extensions for their customers by which they hope to increase their revenues. Such a lock-in usually results in higher investment risk for the end-user, which in turn usually hampers technology adoption. For ZigBee CACCA adoption a single device manufacturer can provide the full portfolio of devices used within a company, hence the lack of standardization will not necessarily hamper the usability of the solution. However, the high number of different Wi-Fi chipsets used in a multitude of different devices, all used within a

single factory makes it very hard for a single Wi-Fi device manufacturer to span a full product portfolio used within a single company. Therefore multiple Wi-Fi device manufacturers should include CACCA functionality in their chipsets. Hence although standardization is usually needed to get a widespread technology adoption, a ZigBee manufacturer's business case might be viable without standardization while a Wi-Fi manufacturer's business case will most likely prove a lot more difficult without standardization.

Table 5.6: Synthesis - Strategic Issues (ZigBee vs. Wi-Fi Manufacturers)

Device Manufacturer (ZigBee)	**Device Manufacturer (Wi-Fi)**
✓ An 'industrial grade' ZigBee device opens additional revenue streams (due to higher sales price of CACCA enabled ZigBee devices) ✓ By adopting CACCA, ZigBee Device Manufacturers will be able to differentiate themselves from their competitors in the market ✓ CACCA enables control as well as monitoring applications, hence opens up new market opportunities for ZigBee devices ✓ Almost no added energy consumption ✓ A single chipset can be used to equip a full range of wireless automation devices ✓ No standardization will not necessarily hamper a single DM's uptake	✓ An 'industrial grade' Wi-Fi device will also fetch additional revenues due to higher sales price ✓ By adopting CACCA, Wi-Fi Device Manufacturers will be able to differentiate themselves from their competitors in the market place ✓ No added energy consumption ✓ Very low additional Capital requirements for development, no added production costs ✓ 'Industrial grade' Wi-Fi product portfolio will be highly marketable
× Only feasible when CACCA enabled Wi-Fi is used × High implementation complexity × High Capital requirements for development, production, and implementation of CACCA solutions	× The lack of standardization might hinder CACCA adoption by multiple device manufacturers, in turn hampering the creation of a full product portfolio of CACCA enabled devices × It is problematic to incentivize Wi-Fi Device Manufacturers as the reliability gains are in the ZigBee network.

5.6 Conclusion

Within this paper we have analyzed the deployment of a wireless sensor network in a factory automation scenario for four different implementation alternatives. The first alternative is the status-quo, in which no CACCA is used. The second one deploys only CACCA enabled ZigBee nodes. The third alternative deploys CACCA enabled Wi-Fi devices and the fourth alternative deploys both CACCA enabled ZigBee and Wi-Fi devices. We conclude that from a technical point of view CACCA needs to be adopted either in Wi-Fi only to reach good sensor network reliability when coexisting with moderate Wi-Fi loads, or in both Wi-Fi and ZigBee to result in excellent sensor network reliability independent of the Wi-Fi load.

In the economic analysis we conclude that the first and second implementation alternative result in huge losses due to production disruption, the creation of scrap products and machine repairs. However, the third implementation alternative (only Wi-Fi CACCA) shows better results with savings of 158 k€, equaling a 77.9% reduction in comparison to a wired rollout for Wi-Fi loads up to 12.5Mbps. Unfortunately there are no more savings when the average Wi-Fi load goes above 20Mbps and results into huge losses for higher Wi-Fi loads. Finally, the fourth implementation alternative (both ZigBee and Wi-Fi CACCA) results in savings between 77 k€ and 83.3 k€ or between 53% and 57.3% across all Wi-Fi loads.

Although our technical analysis shows that incorporation of CACCA in a Wi-Fi device is more cost effective than in a ZigBee device, the Wi-Fi incorporation holds some risk due to the high variety of Wi-Fi products used within a single factory. CACCA standardization in Wi-Fi can therefore significantly increase its adoption since at least a number of Wi-Fi manufacturers are needed to create a full CACCA enabled Wi-Fi portfolio.

In summary, CACCA has the potential to open up a new market segment of high-reliability wireless assembly automation use cases from a technical as well as an economic perspective. Moreover reliable wireless sensor networks offer significantly more flexibility compared to wired sensor networks offering additional benefits in assembly automation.

5.7 References

[5.1] ZigBee Alliance. ZigBee Technical Documents. [Online]. http://www.zigbee.org/Standards/Downloads.aspx

[5.2] HART Communication Foundation. WirelessHART Technology. [Online]. http://www.hartcomm.org/protocol/wihart/wireless_technology.html

[5.3] International Society of Automation. ANSI/ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications. [Online]. http://www.isa.org/ISA100-11a

[5.4] ZigBee Alliance. (2011, July) 100 ZigBee Smart Energy Products Now ZigBee Certified. [Online]. http://www.zigbee.org/News/AlliancePressReleases.aspx?1=1&moduleID=778&Contenttype=ArticleDet&ArticleID=324

[5.5] ABI Research. (2011, May) 850 Million IEEE 802.15.4 Chipsets to Ship in 2016, Despite Strong Competition from Bluetooth, Says ABI Research. [Online]. http://www.businesswire.com/news/home/20120511005889/en/850-Million-IEEE-802.15.4-Chipsets-Ship-2016

[5.6] K J Muoung, S Y Shin, H S Park, and W H Kwon, "802.11b Performance Analysis in the Presence of IEEE 802.15.4 Interference," IEICE Transactions on Communications, vol. B, no. 90, pp. 176-179, 2007.

[5.7] S Pollin, I Tan, B Hodge, C Chunand, and A Bahai, "Harmful Coexistence Between 802.15.4 and 802.11: A measurement-based study," in Proc. Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), 2008, pp. 1-6.

[5.8] Intech Web Exclusive. (2012, Oct.) Industrial Wireless Sensor Networks: Trends and developments october 2012. [Online]. http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=90824

[5.9] Lieven Tytgat, Opher Yaron, Ingrid Moerman, and Piet Demeester, "Analysis and experimental verification of frequency based interference avoidance mechanisms in IEEE 802.15.4," IEEE/ACM transactions on networking, 2013.

[5.10] Lieven Tytgat, Opher Yaron, Sofie Pollin, Ingrid Moerman, and Piet Demeester, "Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment," EURASIP Journal on Wireless Communications and Networking, no. 2012-137, 2012.

[5.11] J Jangeun, P Peddabachagari, and M Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications," in Second IEEE International Symposium on Network Computing and Applications (NCA), 2003, pp. 249-256.

[5.12] TMote Sky datasheet. [Online]. http://www.snm.ethz.ch/snmwiki/pub/uploads/Projects/tmote_sky_datasheet.pdf

[5.13] IMEC. Cognitive solutions using imec's spectrum sensing pave the way towards cognitive radios. [Online]. http://www.imec.be/ScientificReport/SR2010/2010/1159118.html

[5.14] K Casier et al., "Extending operational models to perform micro optimizations," in Proceedings of ECOC2007, the 33rd european Conference and Exhibition on Optical Communication, Berlin, 2007.

[5.15] Farnell. FTP wire cost. [Online]. http://be.farnell.com/pro-power/cbbr6332/cable-cat5e-ftp-305m/dp/3787977

[5.16] (2013) ZigBee module cost. [Online]. http://be.farnell.com/jsp/search/browse.jsp?N=2002+202652+110143547&Ns=P_PRICE_FARNELL_BE|0&Ntk=gensearch&Ntt=zigbee&Ntx=mode+matchallpartial&locale=nl_BE&appliedparametrics=true&getResults=true&suppressRedirect=true&isRedirect=&originalQueryURL=/jsp/sear

[5.17] (2009, Jan.) Typical profit margins on electronic sales. [Online]. http://www.answerbag.com/q_view/51115

[5.18] Lieven Tytgat et al., "Techno-economical Viability of Cognitive Solutions for a Factory Scenario," in New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on , Aachen, 2011, pp. 254-264.

[5.19] (2013) Conrad battery cost. [Online]. http://www.conrad.be/ce/nl/product/658011/Conrad-Energy-alkaline-penlitebatterij-15-V-LR06-AA-LR6-AAB4E-AM3-M-MN1500-815-E91-LR6N-15A-KAA-R6-R06-BA;jsessionid=7F6CF9A094B3268060466962C9425FDA.ASTPCEN28

[5.20] J F Moore, "Predators and prey: A new ecology of competition," Harvard Business Review, vol. III, no. 71, pp. 75-86, May 1993.

6

Conclusions and Perspectives

The main research question addressed in this dissertation is: "*How to minimize the cross-technology impact of co-located heterogeneous wireless network utilizing a single shared frequency band*". The focus point of this dissertation is on CSMA/CA based technologies, and more specifically on the coexistence of IEEE 802.11 and IEEE 802.15.4. The main research question resulted in three major contributions as follows:

- Space-frequency interference avoidance (receiver directed transmission or RDT);
- Time-based interference avoidance (co-existence aware CCA or CACCA);
- Time-space-frequency based interference avoidance.

Following these three contributions we have addressed a secondary question considering the potential economic impact CACCA can have in a realistic wireless factory automation scenario, which results in our fourth contribution:

- Techno-Economic and Business viability of CACCA.

Within this chapter we highlight the most important aspects of each contribution. We finalize this chapter by showing opportunities for future research.

6.1 Contribution 1: Space - Frequency based interference avoidance (RDT)

Within this contribution we have selected, implemented and experimentally validated an IEEE 802.15.4 side space-frequency protocol resulting in the lowest negative impact from Wi-Fi on ZigBee.

We analyzed time-space-frequency domain characteristics of interference in an office environment. In nighttime there are specific frequencies and locations with only limited interference. However, during daytime there are hardly such frequencies and locations. We conclude that the interference in an office environment is of a local and dynamic nature.

We have proposed a taxonomy for quantitative comparison of available IEEE 802.15.4 space-frequency interference avoidance mechanisms. We conclude that the follow the master approach can result in a relatively good channel for a period of time within a specific geographical area, but might as well result in a bad channel selection at other times and/or geographical areas. Pseudo random hopping results in average packet loss at all times and locations. The metric based approach results in the best performance.

RDT is metric based protocol which allows every node within a network to select its own optimal channel. We proposed an enhanced metric for RDT, ReSIST, and conclude that the average PER is 14% lower than the second best metric, and is only 7.7% below the ideal metric.

Finally we verify the operation of the full RDT implementation using the ReSIST metric and show it benefits significantly from the space-frequency interference characteristics in a real-life office scenario.

6.2 Contribution 2: Time based interference avoidance (CACCA)

Within this contribution we have enhanced ZigBee and Wi-Fi co-existence awareness in the time domain.

We have shown that the major reason for collisions between Wi-Fi and ZigBee is due to Wi-Fi not detecting ZigBee transmission reliably. We proposed CACCA, which enhances regular CCA to also detect transmissions of other technologies.

We have shown that out of the four different deployment alternatives two deployment alternatives gain significantly namely CACCA enabled Wi-Fi and CACCA enabled Wi-Fi and ZigBee. Moreover we show that CACCA enabled ZigBee + Wi-Fi has the potential to reduce the ZigBee packet loss to below 10%, even under severe Wi-Fi interference.

We also show that the implementation of CACCA in ZigBee devices contributes at most 8% to its radio transmit energy consumption, while Wi-Fi CACCA implementation adds less than 2% to the energy consumption.

6.3 Contribution 3: Time – Space – Frequency based interference avoidance

This contribution compares and combines the mechanisms elaborated on in Contribution 1 and Contribution 2 by applying them on top of an extended set of measurements carried out on the iMinds w-iLab.t wireless testbed.

We extended the model of contribution 2 so it can be used to predict PER_Z based on real-life measured Wi-Fi traces. Using our three-tier methodology we calibrated this model so it can predict PER_Z for every link and every channel at every time instant.

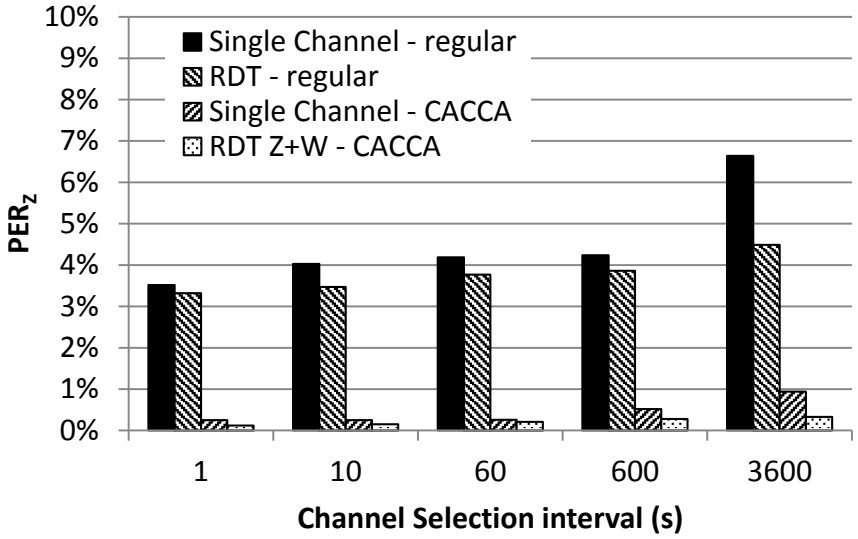

Figure 6.1: Comparison of frequency (single channel) and space-frequency (RDT) with (CACCA) or without (regular) time based interference avoidance

We have combined space-frequency domain interference avoidance with time domain interference avoidance of which the results are depicted in Figure 6.. We conclude that selecting the optimal channel every second is the best, followed by a channel selection every 10s. The channel selections every minute and every 10 minutes perform almost identical, while an hourly channel selection performs significantly worse. Using the RDT implementation of contribution 1 we need at least 20s to select a channel. Hence we conclude that a good channel selection

period equals 10 min. A longer period will result in worse performance while the performance gain for a shorter period does is only minor, but the additional energy cost is substantial.

We show that a single channel for the whole ZigBee network without the usage of CACCA performs worst. RDT without CACCA performs better, especially when there is a long time between channel selections. When CACCA is employed PER_Z drops significantly for single channel as well as RDT. PER_Z remains below 1% when CACCA is combined with a single channel solution, and it remains below 0.47% when it is combined with RDT.

Finally we conclude that Wi-Fi might have a negative impact on its throughput when enabling CACCA. This negative impact can be reduced by spreading the ZigBee load across multiple channels. Moreover, Wi-Fi always has the option to disable CACCA temporarily in case Wi-Fi performance needs to be safeguarded.

6.4 Contribution 4: Techno-Economical and Business impact assessment of CACCA

Within this contribution we have assessed the techno-economic and business impact of CACCA using a single channel ZigBee network overlapped by Wi-Fi based on the model of Contribution 2.

Within the technical analysis we conclude that out of the four different deployment alternatives – regular, CACCA enabled ZigBee, CACCA enabled Wi-Fi and CACCA enabled ZigBee + Wi-Fi – only CACCA enabled Wi-Fi and CACCA enabled ZigBee + Wi-Fi introduce significant gains in reliability as well as battery lifetime.

In the economic analysis we conclude that the CapEx of the wired deployment is the largest, followed by the rollout of CACCA enabled ZigBee + Wi-Fi, CACCA enable ZigBee and CACCA enabled Wi-Fi respectively. The OpEx of regular CCA, CACCA enable ZigBee and CACCA enabled Wi-Fi deployments is huge due to insufficient network reliability under low to medium Wi-Fi interference. In contrast, CACCA enabled ZigBee + Wi-Fi results in a lower OpEx than the wired deployment, even under severe Wi-Fi interference. We conclude that the total cost of ownership in the worst-case interference scenario is lowest for the CACCA enable ZigBee + Wi-Fi scenario, followed by the wired deployment. The other alternatives are not able to cope sufficiently with severe Wi-Fi interference and result in a huge total cost of ownership.

In the business ecosystem analysis we have shown that the CACCA enabled ZigBee business case is highly dependent on the widespread availability of CACCA enabled Wi-Fi. The introduction of CACCA enabled Wi-Fi devices may be slow due to the large diversity of Wi-Fi enabled devices deployed in a factory. The uptake of CACCA enabled Wi-Fi might be significantly accelerated through standardization. Moreover, an ‘industrial grade’ ZigBee and Wi-Fi might open

additional revenue for manufacturers due to higher sales prices and opening up ZigBee to be used in new market segments.

In summary we state that CACCA has the potential to open up a new market segment of high-reliability wireless assembly automation use cases from a technical as well as an economic perspective. Moreover reliable wireless sensor networks offer significantly more flexibility compared to wired sensor networks offering additional flexibility in assembly automation.

6.5 Outlook and future research opportunities

Within this work we have extensively evaluated the potential impact CACCA can have in a Wi-Fi – ZigBee scenario. For the evaluation we have always assumed that CACCA has a 100% detection probability. In the meantime, we have experimentally validated the ZigBee detection reliability when Wi-Fi is CACCA enabled on the WARP SDR platform [6.5]. However, this detection reliability will vary for every Wi-Fi device since it is dependent on the received interference strength. Hence it should be calibrated at every Wi-Fi node, which is not feasible. Hence extending the model to include a realistic CACCA detection probability remains future work.

This work does not explicitly measure the cross-technology impact a wireless transmission using a specific technology imposes on other technologies. Each technology tries to optimize its own 'cost' (i.e. packet loss, battery lifetime, spectrum usage, etc.), but does not explicitly assess the 'cost' it introduces on its environment. However, without an overall 'cost' function it is not feasible to analyze a tradeoff between the 'profit' and the 'cost' of wireless communication utilizing a specific technology. Such a global cost function can be used to balance the spectrum use between technologies, map applications to the available technologies, etcetera.

As mentioned in the introduction the goal of co-existence awareness is twofold: 1) reduce the impact of one technology on another, and 2) shifting the operating points of different technologies towards globally optimal horizontal spectrum sharing. However, the exact operating points can be shifted depending on the needs of the applications. E.g. A fire detection system using ZigBee in a Wi-Fi prone environment needs higher reliability in case of fire than in case of regular operation. Hence some form of negotiation between technologies might result in the optimal operation of both technologies for a given context.

Cross-technology interference issues are only starting to emerge. At this moment the 2.4GHz ISM band is the band used by a number of widespread and standardized technologies. Hence this is the most logical starting point for introducing cross-technology interference avoidance mechanisms, as the ones proposed in this dissertation. In the near future we foresee that cross-technology

interference will expand to other frequency bands. IEEE 802.11n [6.6], not considered within this dissertation, already allows a 40 MHz bandwidth mode. This mode reduces the available spectrum for IEEE 802.15.4 drastically in the 2.4GHz band. Moreover, in the 5GHz band IEEE 802.11n is co-located with IEEE 802.11a. IEEE 802.11ac, in the process of being ratified at the time of writing, allows even broader bands up to 160 MHz. In such a scenario a single 160 MHz transmission can be overlapping with up to 8 regular IEEE 802.11a channels. Therefore IEEE 802.11ac has extended the RTS/CTS mechanism to remain backwards compatible with the 20 MHz IEEE 802.11a standard. It is therefore important that all technologies occupying a broad spectrum consider backwards compatibility with technologies occupying a smaller spectrum. Software Defined Radio (SDR) and Cognitive Radio (CR) allow for a device to adapt vigorously to its environment. When using such devices it might become opportune to let the devices negotiate on the most suited communication settings to maintain the required QoS level at the minimal 'cost'. This cost can be defined as cost for the own technology, like battery life, percentage remaining throughput, reliability, etc., but might also include costs incurred in other technologies. Hence a more generalized approach towards cross-technology interference impact assessment, avoidance and negotiation seems a viable opportunity for future research.

As mentioned in the introduction a sidetrack of this work was the implementation of a combination of RDT and LPL. This implementation was significantly more complex than expected due to the high degree of integration of the radio driver with a specific MAC protocol. Other researchers within our research group also encountered this problem, and hence we have proposed a new sensor network MAC radio driver architecture [6.8], for which we applied for a patent [6.9]. Although this architecture has proven to increase the flexibility of MAC design considerably, there is still room for future research. Especially towards SDR and CR a number of opportunities remain. Current SDR and CR hardware designs are becoming extremely flexible. The hardware can in principle switch very quickly between standards. 'All' that needs to be done to receive a packet correctly is to set the correct settings in the registers so it demodulates the correct bandwidth in the correct mode for a certain timeframe. However, in practice this means that multiple MACs, potentially running independently, need to get access to the same hardware. Nowadays a single radio driver is optimized for its MAC protocol. In case multiple MACs run on the same hardware a careful design is needed in order to achieve the required time accuracy. Hence, the radio driver architecture needs to be further extended to support multiple MACs sharing the same radio. In SDR not only the MAC, but also the PHY can be managed. For example distributed MIMO systems can benefit from coherent sending and receiving. Mobile applications might also like to change PHY layer parameters at runtime with symbol granularity when changes in the channel occur. Especially

the emergence of full-duplex wireless, currently investigated in research [6.10], [6.11], might open up a lot of future work in this area.

6.6 References

[6.1] iMinds Wireless lab, [online] http://www.iminds.be/en/develop-test/ilab-t/wireless-lab

[6.2] Shacham N.,King P.: "Architectures and performance of multichannel multihop packet radio networks.", IEEE Journal on Selected Areas of Communication, JSAC-5(6):1013{1025, 1987

[6.3] A.W. Min, K. Kim, K. Shin, Robust cooperative sensing via state estimation in cognitive radio networks, in 2011 IEEE international symposium on Dynamic Spectrum Access Networks (DySPAN), pp 185 – 196, (2011)

[6.4] IMEC vzw, IMEC sensing engine development, http://www.imec.be/ScientificReport/SR2008/HTML/1225000.html, Accessed 15 feb. 2012

[6.5] De Valck, P., Tytgat, L., Moerman, I., Demeester, P., Coexistence aware clear channel assessment: from theory to practice on an FPGA SDR platform. In Proceedings of the 10th European conference on Wireless Sensor Networks (EWSN'13), Springer-Verlag, Berlin, Heidelberg, 165-178. DOI=10.1007/978-3-642-36672-7_11

[6.6] IEEE Std. 802.11 - 2012, 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, (2012)

[6.7] IEEE 802.11ac, [online] http://en.wikipedia.org/wiki/IEEE_802.11ac, Accessed 6 Jan. 2014

[6.8] De Mil, P., Jooris, B., Tytgat, L., Hoebeke, J., Moerman, I., Demeester, P., (2014). snapMac: a Generic MAC/PHY Architecture Enabling Flexible MAC Design, accepted for publication in Ad Hoc Networks in Jan. 2014

[6.9] Inventors: Jooris, B. De Mil, P., Tytgat, L., (patent pending). snapMac: a Generic MAC/PHY Architecture Enabling Flexible MAC Design. Applicant: UGent/iMinds

[6.10] Sanghoon, K., Stark, W.E., "On the performance of full duplex wireless networks," Information Sciences and Systems (CISS), 2013 47th Annual Conference on , vol., no., pp.1,6, 20-22 March 2013doi: 10.1109/CISS.2013.6552332

[6.11] Ahmed, E., Eltawil, A.M., Sabharwal, A., "Rate Gain Region and Design Tradeoffs for Full-Duplex Wireless Communications," Wireless Communications, IEEE Transactions on , vol.12, no.7, pp.3556,3565, July 2013 doi: 10.1109/TWC.2013.060413.121871

A
Energy Awareness in Self-Growing Sensor Networks

Lieven Tytgat, Opher Yaron, Ingrid Moerman and Piet Demeester

Published in the proceedings of 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks

***Abstract*—An ever increasing variety of applications are being addressed by wireless sensor networks, resulting in a continuous proliferation of their deployments, which are in many cases co-located. This development is mostly hindered by the operational complexity involved with management and maintenance of large numbers of small, battery powered wireless sensor devices. The paradigm of energy aware self-growing networks addresses these difficulties. It focuses on power saving which reduces the major maintenance complexity of replacing batteries, and on automatic cooperation between networks which reduces the management complexity. However, cross-network cooperation requires cross-network communication, which is not straightforward as they typically operate on different frequencies. Receiver Directed Transmission is a MAC layer protocol which can bridge this gap, while also minimizing interference and thus reducing the number of transmissions. In this work we study how Receiver Directed Transmission can be combined with Low Power Listening in order to take advantage of the reduced number of transmissions to improve power consumption. We then implement the selected approach on TinyOS and verify its operation experimentally.**

***Index Terms*— Energy awareness, IEEE 802.15.4, MAC, Media Access Control, Power Saving, RDT, Receiver Directed Transmission, Wireless sensor networks**

A.1 Introduction

One of the major obstacles to large scale adoption of wireless sensor networks remains its relatively high operating expense (OPEX). This cost is strongly influenced by the need to manage and maintain, and particularly replace batteries periodically, in a large number of (sometimes hard-to-reach) devices. In order to reduce OPEX to an acceptable level there is a need to address these two sources of cost.

Except for using batteries with higher capacity, which are of course more expensive, the only way to reduce the cost of battery replacement is to increase the period at which it is needed, i.e. to reduce the power consumption of the nodes. In wireless sensor nodes the single most power consuming component is the radio module. Hence a major contribution to power saving can be achieved by putting the radio in sleep-mode when it is not needed, which is typically the responsibility of the MAC layer. A variety of well known MAC protocols support sleep-mode, and in most cases there is a direct relation between the average rate of packet transmissions and the percentage of time the node spends in sleep-mode.

It remains, then, to identify a suitable protocol that can reduce the average rate of packet transmissions, and to combine it with a suitable MAC layer protocol that will put the radio to sleep mode when it is not needed. Receiver Directed Transmission (RDT) [1] is a perfect candidate. It is a MAC layer protocol which enables the nodes of a single network to operate on multiple frequencies. In a previous study [2] we use RDT to avoid interference, thus reducing the amount of retransmissions due to reception errors. In this work we elaborate on the combination of RDT with a MAC layer protocol that supports sleep mode, with the purpose of reducing power consumption. RDT makes a perfect candidate in this case, as it is also an enabler of automated management and self-growing [3], thus facilitating further reduction of OPEX. By allowing network nodes to operate on multiple frequencies, RDT in essence also allows separate networks that operate on different frequencies to communicate with each other, thus enabling cross-network communication, which is a prerequisite for cross-network cooperation and self-growing.

In Section A.2 we elaborate on the power consumption of a sensor node and explore possible MAC mechanisms for power saving and cooperation of co-located sensor networks. Section A.3 describes the operating principle of RDT, and Section A.4 explains the different ways it can be combined with a Low Power Listening (LPL) protocol. In Section A.5 we detail our experimental results and analyze the potential power savings with our combined RDT + LPL implementation. We conclude this paper in section A.7.

A.2 Saving Power in Wireless Sensor Nodes

Wireless sensor nodes can typically be in one of three modes of operation at any given time – transmitting, receiving and sleeping (radio module Off). The power

TABLE A.1: Tmote Sky Typical Power Consumption

Parameter	Spec. Nominal (mW)	Spec. Max (mW)	Measured (Mw)
P_{TX}	64	69	62.8
P_{RX}	72	76	65.0
P_{sleep}	6	8	5.3

consumption when transmitting (P_{TX}) or receiving (P_{RX}) is typically significantly higher than when sleeping (P_{sleep}). For example, Table A.1 details specified and measured values for the popular Tmote Sky wireless sensor node [4] when operating at a supply voltage of 3.3 Volts. Consequently, the most effective way to save power is to maximize the time the node spends in sleep-mode.

The mode at any given time is determined by the MAC protocol that the wireless sensor node employs. A variety of MAC protocols that periodically go into sleep-mode exist in the literature. Naturally, the lower the throughput in a wireless sensor network, the longer will the nodes be able to spend in sleep-mode, and consequently the lower will their power consumption be. A typical example is illustrated in Figure A.1, which compares the power consumption of the popular S-MAC and B-MAC protocols in a specific scenario [6].

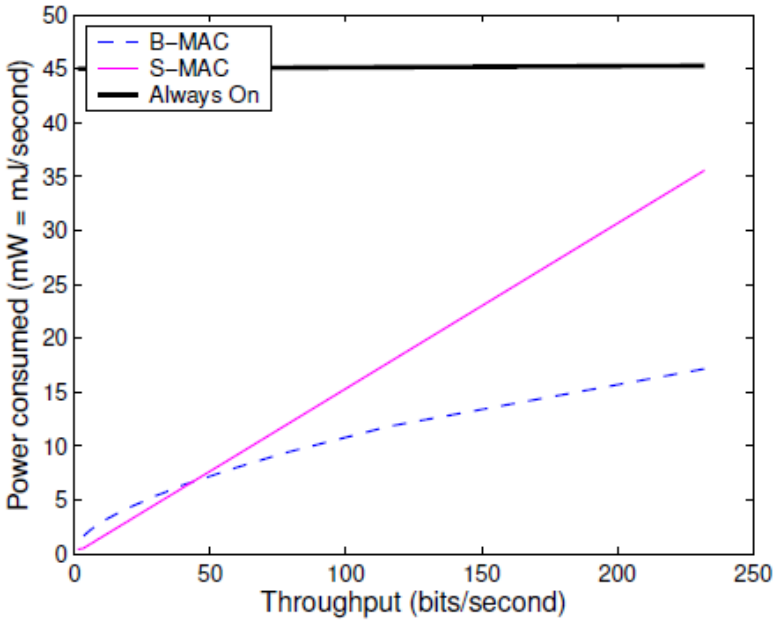

Figure A.1: Power consumption of S-MAC and B-MAC

At low throughputs S-MAC outperforms B-MAC with a small margin (up to 25% in this case), but as the throughput grows B-MAC outperforms S-MAC by growing margins. This difference in behavior is typical, as S-MAC and B-MAC belong to two different classes. S-MAC is a representative of the class of synchronized protocols, where the sleep periods of all nodes in a network are synchronized. Such protocols are more efficient when the throughput is low, as they can use long sleep periods with no penalty, but as the throughput grows the overhead of keeping synchronization between the nodes grows linearly. B-MAC, on the other hand, is a representative of the class of non-synchronized protocols. In this class a node that has a packet to send must transmit for at least the complete duration of the sleep period, to guarantee the destination node wakes-up and learns there is a packet for him. When the throughput is low, this brings to higher power consumption due to the tradeoff between longer sleep periods and the resulting longer transmission times necessary. When the throughput grows, however, the sleep periods get shorter, and the relative penalty of transmission length decreases. Moreover, in this work we also focus on cross-network communication, which is an important enabler for self-growing. The need for synchronization severely increases the complexity of enabling cross-network communication, therefore we select the non-synchronized approach. More specifically, we use the Low Power Listening (LPL) protocol implemented in TinyOS [5], which is a variant of B-MAC.

The basic idea in LPL is to minimize the time a node is in receive mode. An LPL receiver has a cycle time *T* during which it sleeps as much as possible, and only wakes up once to listen if a transmitter is sending it a packet. When a node has a packet to send, it transmits it repeatedly for at least one complete cycle time *T*, making sure that the receiver will have woken up at least once in the meantime. The receiver will therefore wake up for at least one packet time + the time between two consecutive packets, denoted as t. This operating principle is illustrated in Figure A.2.

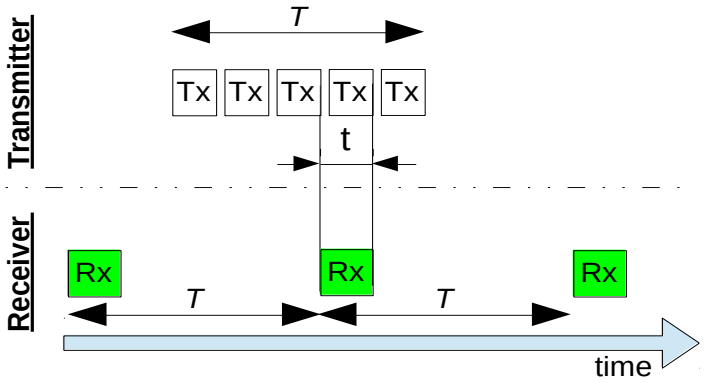

Figure A.2: The LPL operating principle

A.3 Receiver Directed Transmission

In order to minimize power consumption, it still remains to reduce the throughput at the MAC layer as much as possible. One way to do this is to reduce retransmissions of packets, by avoiding interference and resulting unsuccessful packet receptions. We propose to achieve this by utilizing Receiver Directed Transmission (RDT). RDT was studied in [1] as a mechanism to improve network throughput by using multiple frequency channels concurrently. In RDT, each node employs a single radio transceiver, and is assigned a channel to which it is listening whenever it does not transmit – its *quiescent* channel. To send a packet, the node tunes its radio to the quiescent channel of the intended receiver, transmits the packet, and then retunes to its own quiescent channel.

If the transmitter does not know the quiescent channel of the destination, or there is more than one destination (e.g. broadcast traffic), then the packet needs to be transmitted on all possible channels, as illustrated in Figure A.3. The total transmit time – denoted as the transmit cycle time – will obviously be increased by a factor of the total number of channels.

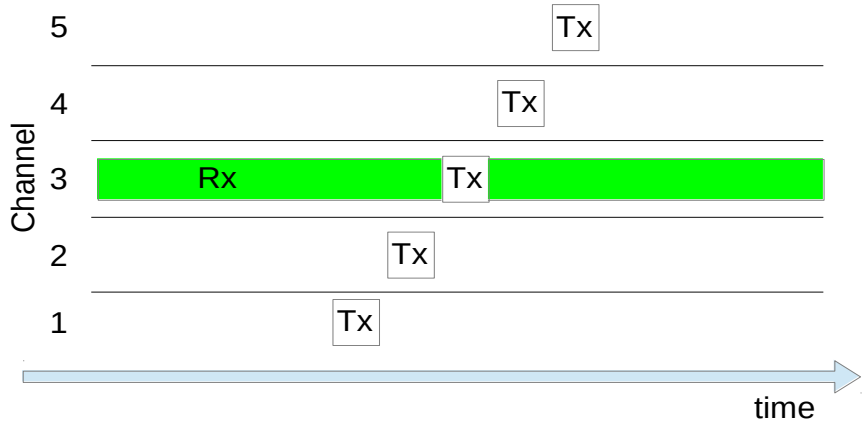

Figure A.3: Transmission to node with quiescent channel 3, which is unknown to the transmitter. The packet is transmitted on all channels.

In an earlier work we already studied RDT as a distributed mechanism for avoiding localized interference [2]. In this paper we leverage on the capability of RDT to reduce interference (and resulting packet retransmissions), but also emphasize its advantage as a cross-network communication enabler. By enabling devices on different channels to communicate with each other, RDT facilitates cross-network communication, which, as mentioned earlier, is an important enabler for self-growing.

A.4 Combining RDT with LPL

The two possible approaches for combining RDT with LPL are depicted in Figure A.4. RDT can either be implemented as a communication protocol layer below LPL (Figure A.4a) or above it (Figure A.4b). Within this section we assume broadcast traffic, resulting in RDT multiplying the packet on all used frequencies, denoted *k*. In sake of simplicity we assume the use of 3 channels within this paper, thus *k*=3.

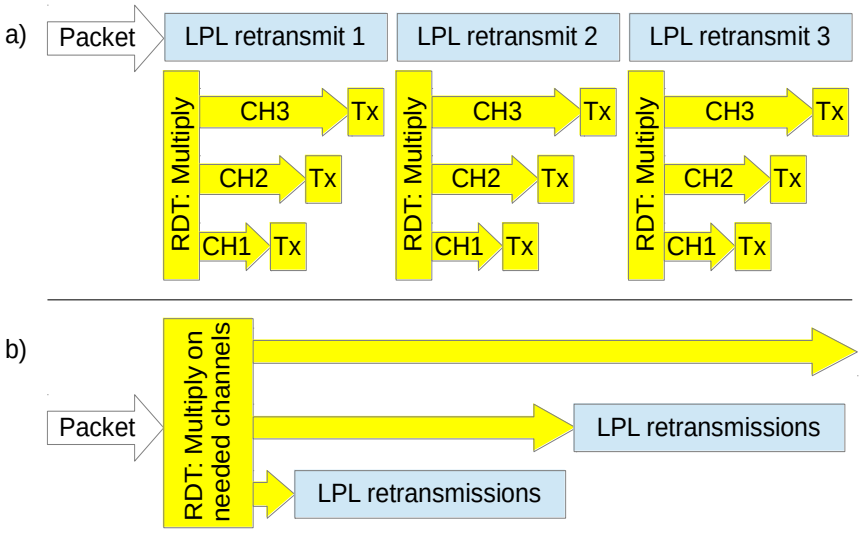

Figure A.4: a) LPL above RDT. b) RDT above LPL

In the first alternative, LPL receives a packet from the higher layer. It then delivers this packet to RDT multiple times. Each time RDT receives the packet from LPL, it transmits it in all necessary channel(s). For example, a broadcast packet results in every LPL delivery being transmitted on all channels, as illustrated in Figure A.5.

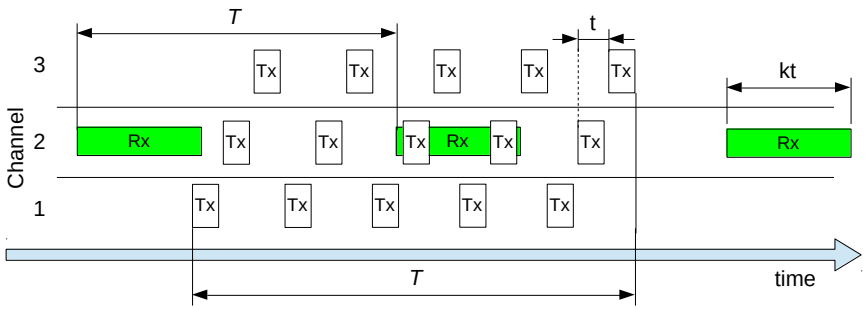

Figure A.5: Combining RDT and LPL case 1: LPL above RDT

Hence, the listen window of the receiver needs to be at least as long as it takes for RDT to transmit a single packet on all channels, which is *k* times longer than the original LPL. The transmit cycle time can remain identical to the original LPL cycle time *T*.

In the second alternative, RDT receives a packet from the higher layer. It delivers the packet to LPL multiple times, each time for a different channel. Whenever LPL receives a packet from RDT for a specific channel, it transmits it on this channel multiple times, identically to the original LPL operating on this channel. This operation is depicted in Figure A.6.

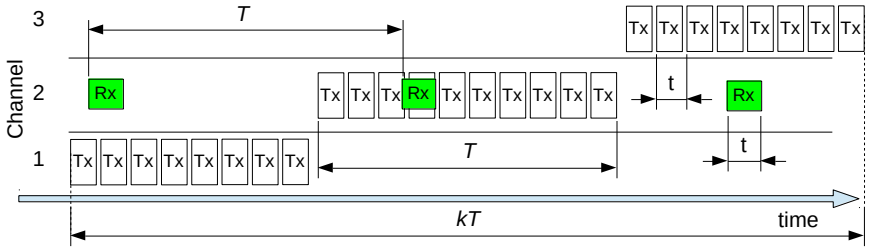

Figure A.6: Combining RDT and LPL case 2: RDT above LPL

The listen window of the receiver is identical to that of the original LPL, but the transmit cycle time is *k* times longer, i.e. *kT*.

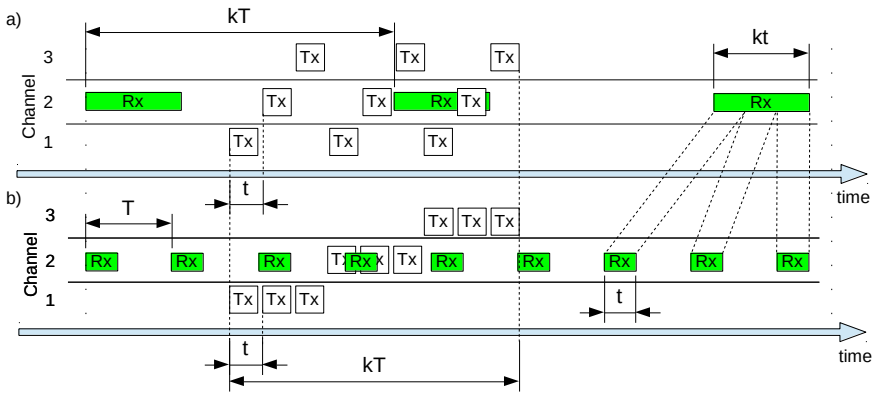

Figure A.7: Comparing case 1 and case 2 with identical link throughputs. a) LPL above RDT, b) RDT above LPL

Comparing the two alternatives with respect to transmitter energy consumption seems advantageous to LPL above RDT. The receiver's energy consumption seems to be in favor of RDT above LPL. However, there is a big difference between the two alternatives with respect to maximum throughput. When we start with the same cycle time *T* in both cases, the resulting maximum link throughput of the 'LPL above RDT' alternative is *k* times higher than that of the 'RDT above LPL' alternative, because in the latter the necessary transmit time of a packet is *k* times longer. To do a fair comparison, we need to compare both cases with identical maximum throughput. We can realize identical maximum throughput by increasing the cycle time of the 'LPL above RDT' alternative to *kT*, in contrast to a cycle time of T in the 'RDT above LPL' case, as shown inFigure A.7. Now in both alternatives the ratio of time a receiving node is in receive mode is *t/T* with *t* the transmission time of one packet; and the transmit cycle time of one packet is *kT*. Consequently, the two alternatives are practically identical in terms of power consumption.

A.5 Experimental Power consumption analysis

We chose the 'RDT above LPL' alternative, and implemented it in TinyOS on tmote sky nodes [4]. The implementation – which is illustrated in Figure A.8– is running inside the default CC2420 radio stack of TinyOS, making it invisible to higher layer protocols.

When RDT receives a packet from the higher layer protocols, it first looks up the destination's channel(s). It switches the radio channel through the setChannel call, and passes the packet on to the LPL layer, which then takes care of the needed retransmissions. LPL notifies RDT when the transmission is completed. RDT will then either switch to the next transmission channel if needed, or it will revert back to the receive channel.

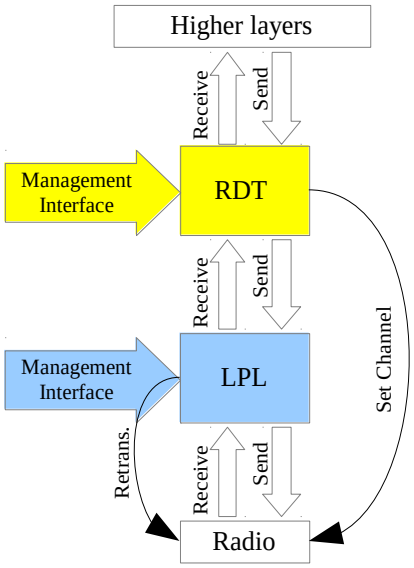

Figure A.8: The implemented architecture: LPL below RDT

TABLE A.2: MEASURED ENERGY CONSUMPTION

Test set-up	Power Consumption (mW)	Relative Power use
RDT without LPL	65.0	100%
RDT+LPL without transmission	6.1	9.4%
RDT+LPL unicast	18.3	28.2%
RDT+LPL broadcast	41.3	63.5%

We measure the power saving this implementation achieves on the w-iLab.t testbed of IBBT [7]. This testbed is deployed in an office environment and among others features power consumption measurements on all nodes. Within the experiments we use a 3.3V supply voltage. We transmit a packet every 5s, and use an LPL cycle time of 1s in all tests, unless explicitly noted otherwise. Table A.2 summarizes the measurement results and the relative power savings achieved.

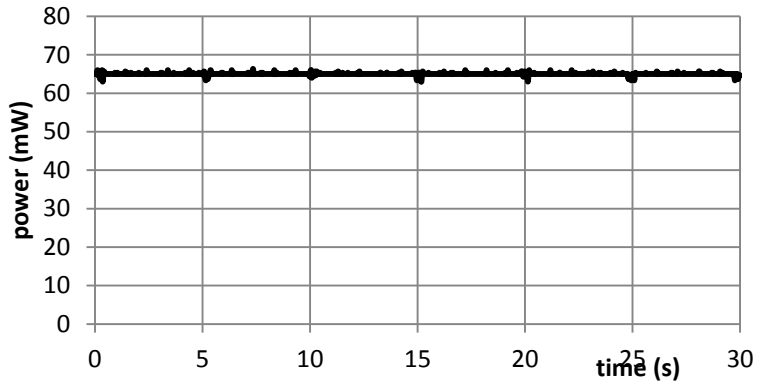

Figure A.9: Power consumption of RDT without LPL

The power consumption of RDT without LPL is depicted in Figure A.9. Without LPL the node never goes into sleep mode, therefore the power consumption is relatively constant. Packet transmissions are visible as small glitches around 0s, 5s, 10s, etc. The effect of transmissions on the average power consumption is clearly very limited. We measure an average power consumption of 65 mW.

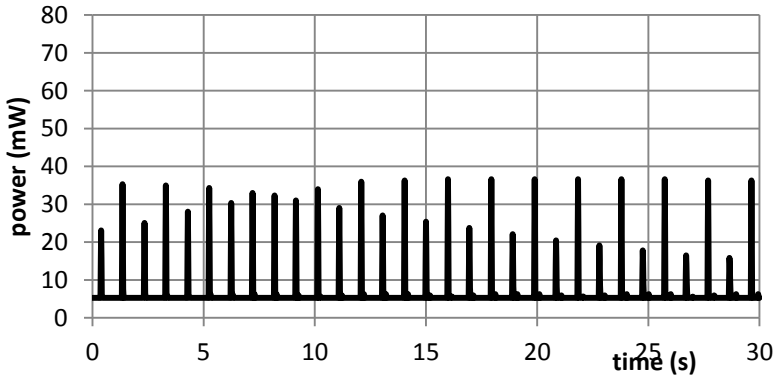

Figure A.10: Power consumption of RDT + LPL without transmission

When we add LPL the node periodically goes into sleep mode, and the power consumption is reduced significantly. Figure A.10 shows the energy consumption of a node that runs RDT + LPL when it is not transmitting packets. Every peak in the diagram is the result of the radio waking up. The average power consumption in this case is 6.1 mW. The differences in the heights of the peaks are measurement artifacts due to the nonzero time it takes to perform reliable current measurements. The actual power consumed during these peaks equals the power consumption of receive mode, i.e. 65 mW. The average cycle time T is 1008 ms.

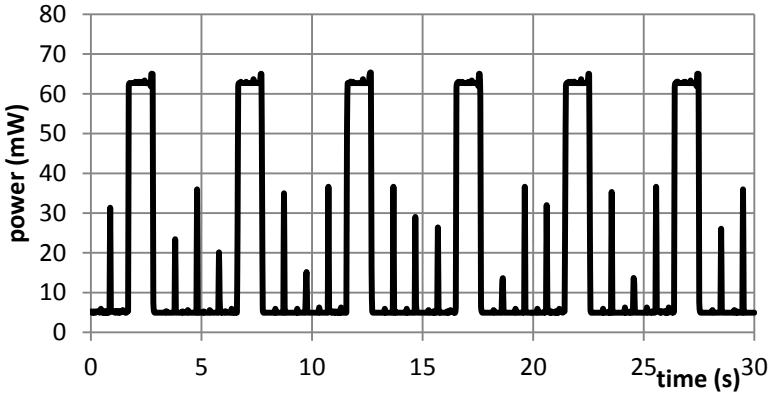

Figure A.11: Power consumption of RDT + LPL with unicast transmission

The power consumption of the RDT+LPL combination when one packet is transmitted every 5 seconds is shown in Figure A.11. We distinguish the receive peaks, also seen in Figure A.12, and the power consumption during transmission. The power consumption of the node during transmission equals 62.8 mW. A transmission lasts in average 1096 ms, which is 88 ms longer than the LPL cycle time. Hence there is sufficient overlap to guarantee the receiver has woken up during the LPL transmit window.

A broadcast packet needs to be transmitted on all channels. In this experiment there are 3 channels configured for RDT, therefore each broadcast transmission lasts 3 times longer than unicast, as shown in Figure A.12.

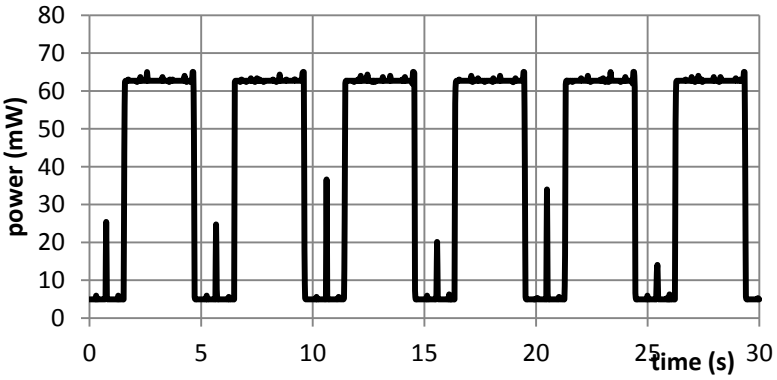

Figure A.12: Power consumption of RDT + LPL with broadcast transmission

A.6 Future work

Within this paper we have studied the energy consumption of a single node. However, we have not studied the energy consumption of a complete network. Especially the exchange of quiescent channel information to neighboring nodes will determine the final energy gains. We will elaborate on this in future work.

LPL reduces the average power consumption in receive mode. However, the time a node spends in transmit mode increases with this approach. Therefore the transmit power consumption becomes more important. Using transmit power adjustment can reduce the transmit power, but remains future work.

A.7 Conclusion

Sensor networks are deployed worldwide, resulting in more and more co-located sensor networks. Operational costs can be significantly reduced in such cases by self-growing, due to reduced management costs and power consumption. Within this paper we propose to use RDT as a self-growing enabler, as well as a mechanism to reduce the amount of packet loss resulting from interference. However, with current state-of-the-art RDT implementations the radio is always on, incurring unnecessarily high power consumption. We propose to reduce the power consumption by combining RDT with LPL.

Both RDT and LPL are MAC layer protocols, and will therefore interact with each other. We investigate the different plausible combinations, and compare the two alternatives of RDT running above LPL and LPL running above RDT. We show that for identical maximal link throughputs the two alternatives have identical power consumptions.

We selected to implement RDT above LPL, as it does not require any modification of the standard LPL implemented in TinyOS. We measured the power consumption on the IBBT w-iLab.t wireless testbed, and conclude that the power consumption of a receiver running RDT+LPL with a 1s cycle time brings power saving of 90.6%. An RDT+LPL transmitter sending unicast packets at 5 second intervals results in power saving of 71.8%; and a transmitter sending broadcast packets to three different channels achieves a 36.5% power saving.

A.8 References

[1] Shacham N.,King P.: "Architectures and performance of multichannel multihop packet radio networks.", IEEE Journal on Selected Areas of Communication, JSAC-5(6):1013{1025, 1987

[2] L. Tytgat, O. Yaron, S. Pollin, I. Moerman P. Demeester, "Analysis and experimental verification of interference avoidance mechanisms in IEEE 802.15.4", submitted to IEEE/ACM Transactions on Networking, aug. 2012

[3] Koudouridis, G.P.; Hedby, G.; Chin, W.H.; Merentitis, A.; Stamatelatos, M.; Alonistioti, N.; Yaron, O.; , "Enablers for Energy-Aware Cooperative

Decision and Control in Wireless Networks," Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd , vol., no., pp.1-5, 15-18 May 2011, doi: 10.1109/VETECS.2011.5956575

[4] Moteiv Tmote Sky data sheet, online: http://www.snm.ethz.ch/pub/uploads/Projects/tmote_sky_datasheet.pdf, accessed may 15, 2012

[5] D. Moss, P. Levis, “BoX-MACs: Exploiting Physical and Link Layer Boundaries in Low-Power Networking”, Stanford Information Networks Group Technical Report SING-08-00, 2008

[6] Polastre, J., Hill, J., And Culler, D., “Versatile low power media access for wireless sensor networks”, In Proceedings of the 2nd International Conference on Embedded Networked Sensor System (SenSys), 2004

[7] w.iLab.t portal – CREW project, online: http://www.crew-project.eu/wilabt, accessed may 15, 2012