Claro António Noda Diaz Quantifying, generating and mitigating radio interference in Low-Power Wireless Networks

UMinho | 2015

Universidade do Minho
Escola de Engenharia

Claro António Noda Diaz

Quantifying, generating and mitigating radio interference in Low-Power Wireless Networks

Doctoral Programme in Telecommunication – MAP-tele

universidade de aveiro

Universidade do Minho

U.PORTO

May 2015

Universidade do Minho
Escola de Engenharia

Claro António Noda Diaz

Quantifying, generating and mitigating radio interference in Low-Power Wireless Networks

Doctoral Programme in Telecommunication – MAP-tele

Supervisors:
Professor Doutor Mário Alves
Professor Doutor Adriano Moreira

May 2015

Declaration of Authorship

I, MSc. Claro António Noda-Diaz, declare that this thesis titled, 'Quantifying, generating and mitigating radio interference in Low-Power Wireless Networks' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.
- Finally, this work abides by the code of conduct and ethics of the University of Minho.

Signed: Claro A. Noda.

Date: *May 29, 2015*

“Science is a human activity, and the best way to understand it is to understand the individual human beings who practise it. Science is an art form and not a philosophical method. The great advances in science usually result from new tools rather than from new doctrines. … Every time we introduce a new tool, it always leads to new and unexpected discoveries, because Nature’s imagination is richer than ours.”

Freeman J. Dyson

Abstract

Radio interference affects the performance of low-power wireless networks (LPWN), leading to packet loss and reduced energy-efficiency, among other problems. Reliability of communications is key to expand application domains for LPWN. Since most LPWN operate in the license-free Industrial Scientific and Medical (ISM) bands and hence share the spectrum with other wireless technologies, addressing interference is an important challenge.

In this context, we present JamLab: a low-cost infrastructure to augment existing LPWN testbeds with accurate interference generation in LPWN testbeds, useful to experimentally investigate the impact of interference on LPWN protocols.

We investigate how interference in a shared wireless medium can be mitigated by performing wireless channel energy sensing in low-cost and low-power hardware. For this pupose, we introduce a novel channel quality metric—dubbed CQ—based on availability of the channel over time, which meaningfully quantifies interference. Using data collected from a number of Wi-Fi networks operating in a library building, we show that our metric has strong correlation with the Packet Reception Rate (PRR). We then explore dynamic radio resource adaptation techniques—namely packet size and error correction code overhead optimisations—based on instantaneous spectrum usage as quantified by our CQ metric.

To conclude, we study emerging fast fading in the composite channel under constructive baseband interference, which has been recently introduced in low-power wireless networks as a promising technique. We show the resulting composite signal becomes vulnerable in the presence of noise, leading to significant deterioration of the link, whenever the carriers have similar amplitudes.

Overall, our results suggest that the proposed tools and techniques have the potential to improve performance in LPWN operating in the unlicensed spectrum, improving coexistence while maintaining energy-efficiency. Future work includes implementation in next generation platforms, which provides superior computational capacity and more flexible radio chip designs.

Resumo

A interferência de rádio afeta o desempenho das redes de comunicação sem fio de baixo consumo—low-power wireless networks (LPWN), o que provoca perdas de pacotes, diminuição da eficiência energética, entre outros problemas. A confiabilidade das comunicações é importante para a expansão e adoção das LPWN nos diversos domínios de potencial aplicação. Visto que a grande maioria das LPWN partilham o espectro radioeléctrico com outras redes sem fio, a interferência torna-se um desafio importante.

Neste contexto, apresentamos o JamLab: uma infraestrutura de baixo custo para estender a funcionalidade dos ambientes laboratoriais para o estudo experimental do desempenho das LPWN sob interferência. Resultando, assim, numa ferramenta essencial para a adequada verificação dos protocolos de comunicações das LPWN.

Para além disso, a Tese introduz uma nova técnica para avaliar o ambiente radioelétrico e demostra a sua utilização para gerir recursos disponíveis no transceptor rádio, o que permite melhorar a fiabilidade das comunicações, nomeadamente nas plataformas de baixo consumo, garantindo eficiência energética. Assim, apresentamos uma nova métrica—denominada CQ—concebida especificamente para quantificar a qualidade do canal rádio, com base na sua disponibilidade temporal. Mediante dados adquiridos em várias redes sem fio Wi-Fi, instaladas no edifício de uma biblioteca universitária, demonstra-se que esta métrica tem um ótimo desempenho, evidenciando uma elevada correlação com a taxa de recepção de pacotes. Investiga-se ainda a potencialidade da nossa métrica CQ para gerir dinamicamente recursos de radio como tamanho de pacote e taxa de correção de erros dos códigos—baseado em medições instantâneas da qualidade do canal de rádio.

Posteriormente, estuda-se um modelo de canal composto, sob interferência construtiva de banda-base. A interferência construtiva de banda-base tem sido introduzida recentemente nas LPWN, evidenciando ser uma técnica prometedora no que diz respeito à baixa latência e à confiabilidade das comunicações. Na Tese investiga-se o caso crítico em que o sinal composto se torna vulnerável na presença de ruído, o que acaba por deteriorar a qualidade da ligação, no caso em que as amplitudes das distintas portadoras presentes no receptor sejam similares.

Finalmente, os resultados obtidos sugerem que as ferramentas e as técnicas propostas têm potencial para melhorar o desempenho das LPWN, num cenário de partilha do espectro radioeléctrico com outras redes, melhorando a coexistência e mantendo eficiência energética. Prevê-se como trabalho futuro a implementação das técnicas propostas em plataformas de próxima geração, com maior flexibilidade e poder computacional para o processamento dos sinais rádio.

Acknowledgements

There are two persons that stand out in my journey throughout Portugal, and this thesis sums up that adventure somehow. Prof. Adriano Moreira guided me since the first year of the MAP-Tele program at University of Minho (2008-2009) and Prof. Mário Alves welcomed me at the CISTER Research Unit in the School of Engineering of the Polytechnic Institute of Porto, as my scientific co-adviser. They have put up with my development along these years, and I am truly grateful for that.

Throughout this journey, I have had the privilege to collaborate with experienced researchers in the field. I am thankful to my co-authors: Prof. Shashi Prabh (Shiv Nadar University), for his patience, eloquent discussions and criticism. To Prof. Thiemo Voigt (University of Uppsala) for his friendliness, support and optimism, Prof. Kay Römer (Graz University of Technology) for his smooth collaboration and attention to details, and Carlo Alberto Boano for his enthusiasm and motivation for doing research work. I am also grateful to Dr. Marco Zennaro (International Centre for Theoretical Physics—ICTP), for his friendship and long-term support. Marco actually pointed me to the MAP-Tele PhD programme call and has hosted me at ICTP for multiple activities, focused on wireless communications. During the last stage of this work, I have met Balint Seeber (Ettus Research) at ICTP. Balint is a source of inspiration and friendship. His keen technical support on Software Defined Radio during the last phase of this work has made my life a little easier. I am particularly thankful to Carlos Pérez-Penichet for his friendship and unconditional availability to help in my research endeavours, for over 10 years.

I also had the pleasure to spend time with many co-workers at CISTER, including the administrative staff and secretaries who have repeatedly extended a helping hand. I am also appreciative of the sympathy and support of the members of Networked Embedded Systems group at the Swedish Institute of Computer Science (SICS), which I had the opportunity to visit during my PhD studies.

This PhD would not have been completed without the love of my family. I am especially indebted to my cousins and my brother for their affection and sustained support. The culmination of this journey is also a little tribute to my mother, who would have been happier to see the outcome.

Claro A. Noda Diaz

This work was supported by FCT (Portuguese Foundation for Science and Technology) and by ESF (European Social Fund) through POPH (Portuguese Human Potential Operational Program), under PhD grant SFRH/BD/62198/2009; also by FCT under project ref. FCOMP-01-0124-FEDER-014922 (MASQOTS), and EU through the FP7 programme, under grant FP7-ICT-224053 (CONET).

Contents

List of Figures

List of Tables

Abbreviations

AGC	**A**utomatic **G**ain **C**ontrol
AWGN	**A**dditive **W**hite **G**aussian **N**oise
CBI	**C**onstructive **B**aseband **I**nterference
CCA	**C**lear **C**hannel **A**ssessment
CMOS	**C**omplementary **M**etal-**O**xide **S**emiconductor
COTS	**C**ommercial-**O**ff-**T**he-**S**helf
CSMA	**C**arrier **S**ense **M**ultiple **A**ccess
CTI	**C**ross **T**echnology **I**nterference
DSSS	**D**irect **S**equence **S**pread **S**pectrum
FIFO	**F**irst **I**nput **F**irst **O**utput
FPGA	**F**ield **P**ogrammable **G**ate **A**rray
HSS	**H**alf **S**ine **S**haping
IDD or i.i.d.	**i**ndependent (and) **i**dentically **d**istributed
IPI	**I**nter-**P**acket **I**nterval
ISM	**I**ndustrial **S**cientific (and) **M**edical
LPWN	**L**ow-**P**ower **W**ireless **N**etwork
LR-WPAN	**L**ow-**R**ate **W**ireless **P**ersonal **A**rea **N**etwork
MAC	**M**edium **A**ccess **C**ontrol sublayer
MCU	**M**icro **C**ontroller **U**nit
OQPSK	**O**ffset **Q**uadrature **P**hase **S**hift **K**eying
PER	**P**acket **E**rror **R**ate
PDR	**P**acket **D**elivery **R**ate
PLL	**P**hase **L**ocked **L**oop
PRR	**P**acket **R**eception **R**ate
PHY	**P**hysical layer

QoS	**Q**uality **o**f **S**ervice
RSSI	**R**eceived **S**ignal **S**trenght **I**ndication
SDR	**S**oftware **D**efined **R**adio
SFD	**S**tart (of) **F**rame **D**elimiter
SIC	**S**uccessive **I**nterference **C**ancellation
SNR	**S**ignal (to) **N**oise **R**atio
SoC	**S**ystem **o**n **C**hip
SOM	**S**ervice **O**riented **M**iddleware
SPI	**S**erial **P**eripheral **I**nterface
SPOF	**S**ingle **P**oint (of) **F**ailure
USRP	**U**niversal **S**oftware **R**adio **P**eripheral
VGA	**V**ariable **G**ain **A**mplifier
WPAN	**W**ireless **P**ersonal **A**rea **N**etwork
WSS	**W**ide-**S**ense **S**tationary

Dedicated to my family in Chile, Cuba and the United States

Chapter 1

Introduction

During the last decades, communication systems have radically changed the way we live. Cellular networks are a good example, with great impact in connecting people globally. And more recently, also in connecting us to the Internet by providing data services. Making content available on the web at the users' fingertip, anywhere and any time, has changed the way we consume information and interact with each other. As the network grows with every new user, so does the value it represents for all.

The Internet has grown and evolved rapidly, yet most authors agree we are seeing its infancy. Current forecasts about the Internet next wave of grows suggest that connecting the physical world will lead to unforeseeable opportunities. The granularity at which monitoring and control is feasible within the evolving Internet is expected to drive the next computing revolution, with target domains such as critical infrastructure monitoring and control, transportation, agriculture, and healthcare among others [2]. This is already happening for some applications like integrating demand side management into the power grid, with substantial efficiency improvements in electricity consumption, distribution and generation [3].

Advances in wearable technology have also made things more intimate. As technology becomes more personal it is propitiating remote healthcare and fitness solutions with the potential to impact the scalability and the nature of care itself. The proposers of these solutions emphasise the health benefits of around the clock monitoring for our bodies with wearable computing technology, allowing to quantify our day-to-day habits and potentially helping us to improve our lifestyle.

Wearable devices are also driving the next wave of computing research. Using a smartphone today, for example, requires lots of attention and cognitive processing, since we are consuming information from a small screen and interacting through one or two fingertips. This intensive information compression and decompression into intelligible knowledge takes lots of attention, yet this is our primarily interaction with digital devices today, besides some auditory and vocal engagement.

We need new ways to access and understand information, beyond current interfaces, so that we do not need to compress and decompress all the time in these inefficient ways. Augmenting our senses is an opportunity to naturally interact with sensor data such that wearable computers could become sensory prostheses. Nevertheless, for this enormous amount of data to be meaningful to our brains, wearable technology requires to understand context and user focus. Only then such an approach to delivering digital information could mark the beginning of a fluid connection between our sensory systems and networked sensor data.

How sensor data and ubiquitous computing will change our world is impossible to predict, as the field is still in its infancy. Sensors and computers could make it possible to virtually travel to distant environments and "be" there in real time, which would have profound implications for our concepts of privacy and physical presence [4].

As networked and/or distributed computation, sensing and actuation evolve we see more feasible applications and services that rely on cyber-physical data flows. The "intelligent" systems that support these applications are increasingly dynamic and have the potential to outperform and assist humans in many rutinary tasks, while contributing to safety and comfort. Consequently, their distributed nature makes them very demanding in terms of communication performance, if humans are to depend on them (e.g. driverless cars). However, the underlying wireless techniques are intrinsically unreliable due to the use of low-power radio technology. These current techniques are intrinsically vulnerable as they rely on a shared medium for communication and are not designed from the ground up to be robust against interference or malicious attacks, like jamming.

1.1 Research Context

Research activity in low-power wireless networks has evolved during the last decade with numerous deployments of wireless sensor networks (WSN) [5], mostly comprising tracking and monitoring applications. Wireless communication in low-power networks has converged toward usage of the IEEE 802.15.4 Standard specification for the Physical layer (PHY) and Medium Access Control (MAC) sublayers of the wireless protocol stack [6]. The IEEE 802.15.4 specification envisions low-power and low data rate networks. Hardware platforms used in low-power wireless network research are based on

IEEE 802.15.4 compliant radio chips. Most of these chips perform all PHY layer functionalty internally using dedicated hardware modules. Therefore, most research efforts have concentrated on the network and application layer for sensor networks, although there has been also extensive experimentation at the MAC sublayer, see [7–9].

1.1.1 Energy Efficiency

The main design goal that defines low-power networks is energy conservation. Since most applications require the devices to operate out of limited energy sources, e.g. batteries, the system must be optimised for energy efficiency. In recent times, the energy cost of computation has dropped and continues to drop, making Micro Controller Units (MCU) increasingly energy-efficient. However, the same is not true for radio communications. The required complexity for mixed signal integrated circuits and the digital signal processing required inside the radio chip makes the energy cost of communications considerably higher than computation cost for the majority of sensor network applications [8, 10].

There are numerous techniques devised to save energy in low-power networks [10, 11]. The main policy to conserve energy consists in low-duty-cycling the wireless node's MCU and radio, introduced by Ye et al. [12]. Thus, nodes stay in a lower-power state (or sleep mode) for relatively long periods of inactivity. This duty-cycling regime implies that radios need some rendezvous mechanism to exchange packets, waking up opportunely. There are two common practices to achieve this. One common approach is to use an asynchronous Medium Access Control (MAC) protocol, which will keep nodes periodically either checking the channel for traffic or sending probes which other nodes, seeking to communicate, can detect and trigger the data exchange [13–15].

The other alternative is to use a synchronous MAC protocol, which requires to maintain time synchronisation among the network nodes. To achieve and maintain time synchronisation, nodes either use an external signal that provides a common clock [16], which is not always realisable, or use the radio to exchange packets that allow them to adjust their local clocks to maintain synchronisation. In this way, communication tasks can be performed with high energy-efficiency, turning on the radios for a minimum amount of time and yet guaranteeing that relevant nodes are turning on their radio unanimously to communicate and go back to sleep when the data exchange is concluded [17–19].

When time synchronisation is sufficiently accurate, even more sophisticated communication techniques can be used, as discussed in Chapter 5. Time synchronisation brings other benefits besides communication tasks, for example by enabling synchronous sensing which is mandatory for some applications. However, since having a common clock among nodes involves communication, which raises the baseline energy consumption, its usage has to be justified and is not the most common regime in current practices.

Some specific scenarios rely on softened energy restrictions, in an asymmetric regime where selected nodes are not energy constrained at all and therefore can maintain the radio always on, which simplifies communication protocol solutions. Typically this allows to create a beacon-enabled network where coordinator nodes are not energy constrained but low power nodes are limited to communicate through resource rich nodes, regardless of the network topology used. These beacon-enabled (also referred to as TDMA-based) networks are highly prone to failure, as clock drift leads to disastrous behaviour [20]. Also, beacons are transmitted without contention [6] which makes them vulnerable to collisions due to interference, both with other (coordinator) nodes and/or external interference sources. These scenarios are also limited to some applications and are therefore not explicitly considered in this work.

1.1.2 Unlicensed Operation

Contrary to traditional mobile networks, low-power wireless networks most often operate in the (unlicensed) industrial, scientific and medical (ISM) radio bands [21]. These bands, originally conceived for operation of non-intentional radiators, have served for intense experimentation and innovation in wireless communication technologies [22, 23].

This unlicensed operation of wireless networks incorporate new challenges, specifically due to interference [24]. Regulation on radio frequency emission under unlicensed operation mostly consists in mandatory use of modulation/coding techniques, such as spread spectrum, and/or mandatory limits on power spectral density and duration of emissions. Therefore, tranmitting devices require certification from regulatory boards. The most significant consequence of this scheme is that any radio interference must be accepted or corrected by the communication system that receives it, which typically can compromise its performance [25].

This mode of operation in a shared segment of the frequency spectrum brings about a problem referred to as the *tragedy of the common*. In general terms, the tragedy of the common consists in the lack of cooperation among contender users of a limited resource, leading to its depletion or suboptimal exploitation.

The diversity of existing solutions complicates the design for efficient usage of the wireless medium, e.g. turning simple carrier sense multiple access (CSMA) based techniques ineffective for cross-technology cooperation. The result is suboptimal performance, whenever wireless networks operating in the unlicensed spectrum are deployed and operate in radio range proximity of each other [26–29]. Although some mitigation techniques exist, sharing an uncontrolled wireless medium constitutes an important challenge for providing QoS in low-power wireless networks.

The techniques to improve coexistence in the unlicensed spectrum would benefit by signal processing in the PHY layer, to adapt to the channel condition. However, PHY signal processing requires at least some freedom to modify the radio transceiver's baseband processing modules. Available sensor network platforms are based on commercial-off-the-shelf (COTS) highly-integrated radio transceivers, which lack this flexibility and have prevented experimentation and innovation in the PHY layer for low-power wireless networks. Instead, existing platforms have limited the options to investigate MAC protocols and upper layers of the protocol stack. Additionally, signal processing in the PHY layer requires more powerful processors which need to operate at higher frequencies and offer increased performance, while maintaining energy efficiency. Only recently, sensor network platforms with relatively more powerful 32-bit MCUs, like ARM Cortex-M3 based solutions, have been developed [30, 31]. Possibly, next generation System-on-Chip (SoC) platforms will provide certain flexibility for PHY signal processing, for example see [32]. Some other very recent efforts in this direction include a novel software-defined-radio (SDR) sensor network platform [33], which leverages high power processing capacity in a field-programmable gate array (FPGA) with low-power design techniques.

1.1.3 Quality of Service

Realising the vision of augmenting our senses to naturally interact with sensor data requires significant work in defining infrastructure and network abstractions that facilitate the end user application to interact with the data in a unified and consistent way. These abstractions are needed primarily to isolate the complexity of the underlying system from the end-user application [34]. These abstractions are often referred to as service oriented middleware (SOM) and should provide standard methods to access the data of the abstracted technologies, while removing tailoring and redundant efforts.

An important application class of sensor networks is found in the industrial domains. Sensor networks can reduce the need for human presence in industrial settings, including dangerous areas, and provide added value sensory information and actuation control. In addition to all other requirements of sensor networks for less demanding application domains, industrial sensor networks are characterised by critical operation and require predictable behaviour, link reliability, low-delay communication, and interoperability with legacy systems. The reader is referred to [35] for a description of requirements and challenges in industrial sensor networks. The main challenges arrive from control loop applications, without human intervention, with hard real-time requirements for typically millisecond response times. The most significant difficulty here consist in reconciling these performance requirements with the probabilistic nature of the wireless channel. Existing wireless technologies (e.g. WirelessHART) are designed to satisfy these requirements, to certain degree and with several limitations [36, 37]. Yet the field is changing quickly. For an overview of various classes of industrial sensor networks and protocol stack component alternatives, please refer to [38].

An integrated approach to Quality of Service (QoS) support in sensor networks is rare. There are some QoS based routing protocols and (mostly) simulation based evaluations available [39, 40]. Simulation evaluations are important because they allow to find general behaviour information about the algorithms and about its suitability. However, deployments and real-world experimentation, whenever possible, permit much better assessments than simulations since performance results may vary significantly between them.

If QoS support were available, the infrastructure abstraction should classify the application required data and demand better quality for the time critical data from the abstracted sensor networks to ensure the fastest and the most reliable data delivery. Moreover, QoS in the infrastructure abstraction is an open question. The infrastructure may need to receive and process significant amount of data, and still react to alarming conditions swiftly. This problem can be seen as implementation or server infrastructure problem, but novel distributed solutions for in-network data processing and communication optimisations approaches of the infrastructure are needed [34]. Distributed solutions avoid single point of failure (SPOF), enhance security and make the network scalable.

QoS is often treated as a network level problem. In order for the network to provide QoS support, it first needs to address the unpredictable nature of the wireless channel. As previously discussed, low-power wireless networks rely in an uncontrolled shared medium. Once the network can compensate for the communication uncertainty, traditional traffic classifications can be used, similar to QoS provisions in other (wired) networks.

Proving QoS is in general a simplified form to refer to a large set of features that the infrastructure should support to one extent or another. The specific feature set characterises the entire communication stack, from application to the physical medium used for communications, as described in figure 1.1 and introduced by Chen et al. [39]. The corresponding parameters can be roughly separated in user-specified and low-level, but they are tightly interrelated. For example, user-specified parameters like periodicity, deadlines and reliability are only viable if network-level parameters like packet error rate (PER), throughput, latency and maximun delay are satisfactory. Likewise, network-level

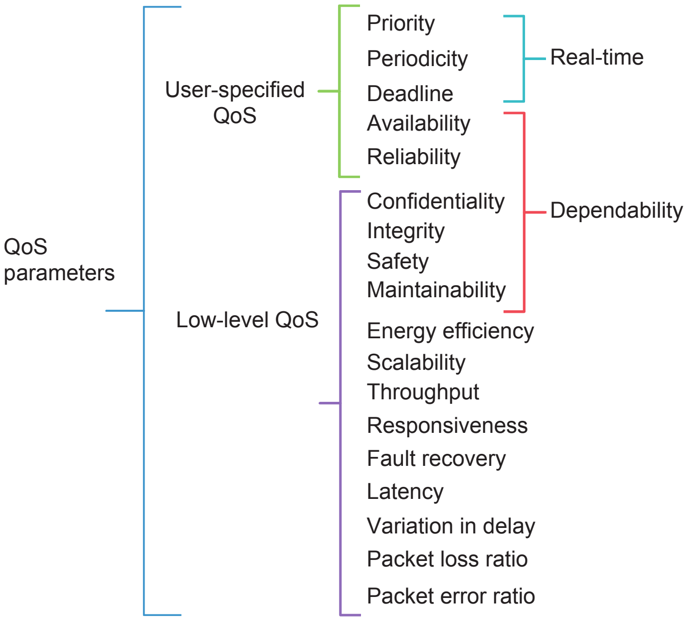


FIGURE 1.1: A comprehensive QoS parameter classification.

parameters depend on PHY and MAC performance. To guarantee that these low-level parameters are maintained in an adequate range is a challenge in any wireless network, even more so in low-power wireless networks.

There are also some sparse efforts to introduce guaranteed performances and QoS metrics in MAC protocols as well, see a survey in [39], including a comparison chart and discussion. These efforts are mostly focused on how to organise the inter-node communication in the network as to differentiate from best-effort traffic to real-time requirements. Although this is a necessary distinction, note that it is not sufficient. Under unlicensed operation, the wireless link reliability is a very fragile parameter, as the wireless signal integrity cannot be preserved under any given circumstances due to external interference. Instead, most existing work in low-power wireless networks make compromising assumptions about the nature of the wireless channel and rely on simple mechanism like multiple retransmissions to compensate for errors.

The ultimate approach to QoS provisions require to involve PHY mechanisms in a cross-layer scheme that more accurately reflect the vulnerability of the wireless channel as well as provide adequate mechanisms to mitigate interference and compensate for the probabilistic nature of the wireless channel at the lowest possible level. This is important because the PHY layer provides critical information and options about effective mitigation techniques. For example, it permits informed radio resource management and adaptation as we will discuss in Chapter 4.

Chen et al. identify the need for more QoS research [39]. In particular, the trade-off between QoS and energy efficiency in resource limited platforms, scalability, cross-layer arquitectures and QoS protocol integration. In this context, PHY is absent due to the limitations of low-power network platforms. We investigate these problems and try to break them down to the most fundamental concepts, which require to consider engineering low-power wireless network protocols from first principles.

1.2 Problem Statement and Hypothesis

We depart from the observation that in an asymmetric scenario where low-power wireless nodes operate, namely a wireless shared medium, where other contenders do not have energy constrains nor cost/performance limitations, low-power wireless nodes require agility and plasticity in its ability to use the wireless medium to avoid and/or mitigate interference, specially from cross-technology interference.

Existing low-power protocols are not in general designed to operate under interference, instead very strong assumptions are often made with regard to the wireless link. The fundamental metric used to measure link reliability is the packet reception rate (PRR). The PRR is a cumulative value that requires many iterations before it can provide any meaningful information. However, the wireless channel condition—accounting for interference—changes in a much shorter time scale.

Sensor network protocols are not systematically verified under interference conditions and yet this is a critical aspect that distinguish low-power networks operating in unlicensed spectrum from other wireless networks. Systematic performance verification could be done with sophisticated infrastructures but this is not typically aligned with sensor network deployments. Low-cost components used in sensor node platforms also affect the behaviour of the network, specially under varying climatic conditions and specific deployment characteristics that affect radio propagation. We have contributed toward performance verification in low power networks with a new tool, discussed in Chapter 2.

Moreover, the complexity of the link behaviour is exacerbated by the usage of low-power radio technology. The power of the carrier wave that reaches the receiver antenna can diminish with an accentuated non-linear dependency with the distance from the transmitter, depending on the environment characteristics. Because there is higher power attenuation (pathloss-per-distance-unit) closer to the transmitter antenna, wireless links in short range communications—using low transmission power—exhibit stronger dependency of the error rate with distance than a longer range link with the same link budget. The observation above, coupled with *small scale fading* [1, 41], explains the transitional region of low-power wireless links [42]. We briefly revisit diversity techniques used to mitigate this effect toward the end of the thesis, in Chapter 5.

The same non-linear propagation argument above makes a more powerful interference source (e.g. Wi-Fi access point) have a potentially broader spatial impact. As the pathloss-per-unit-distance will decrease away from the source, the interferer will have a larger contribution in raising the noise floor at an unintended receiver, like a low-power wireless node. The effect of multiple interferers is cumulative and we treat such cumulative interference as noise in Chapter 3, where we propose how to quantify interference.

Spectrum sensing techniques used in other systems are not suitable for resource constrained low-power nodes. But spectrum sensing is vital for dynamic mitigation strategies. At this point we pose the following questions which pave the way for the hypothesis of our work.

Given the probabilistic nature of the wireless channel, interference presence and limited node-level radio resources, is it possible to augment low-power wireless protocols with dynamic radio resource management and adaptation mechanisms that mitigate interference and improve network performance while maintaining energy efficiency?

Which spectrum sensing techniques and algorithms are viable in these resource constrained systems that permit an informed reaction to the channel condition?

Provided that instantaneous channel information exists, which radio resource allocations are possible in low-cost and resource constrained wireless nodes?

To which extent are diversity techniques effective in low-power wireless networks and how cold they be improved to compensate for the complexity of the wireless channel?

We assume that it is possible to augment low-power radio chips with power efficient channel energy sensing. The lack of this feature is not due to techical limitations but rather because the first cycles of silicon design for low-power radio technology COTS solutions did not accounted the rapid proliferation of this technology and its requirements. We also assume that next generation of low-power devices will provide increased flexibility for signal processing and larger computation capabilities.

Hypothesis: Radio resource management techniques based on adequate spectrum sensing—that captures interference in ISM bands—can improve low-power wireless network performance, namely reliability and throughput.

1.3 Research Strategy and Objectives

We follow an experimental oriented research method, using real-word data whenever possible. We employ a blend of simulation and experimentation that permits to obtain the best of both methods, simplifying implementation and experimental setup while avoiding drastic assumptions, enhancing the quality of the results and improving their validity. Moreover, we avoid designing by analogies with existing solutions and instead explore opportunities of designing from first principles, to an extent that is resonable and feasible, while dissecting implications and validity of our experimental results.

In the context described above, this dissertation addresses interference in low-power wireless networks and investigates what spectrum sensing and radio resource allocation techniques can be employed to increase network performance while operating in a shared and therefore uncontrolled wireless medium. Thus, we develop tools and propose solutions to mitigate CTI in low-power wireless networks.

Objectives:

- Provide a framework for interference generation that is repeatable, realistic and inexpensive
- Sense the wireless channel condition effectively and in an energy-efficient manner
- Adapt radio resources to boost link performance while maintaining energy efficiency
- Consider network level radio resource adaptation schemes and diversity techniques, suitable for low-power design

1.4 Research Contributions and Structure

The solutions proposed in this thesis embrace the paradigm of low-power design without limiting the options to the features offered in existing integrated radio chips but maintaining conservative expectations regarding processing capacity in low-cost radio silicon designs.

We investigate how interference in a shared wireless medium can be mitigated by performing energy-efficient channel energy sensing in low-cost and low-power hardware. Based on the information extracted from the channel, we explore radio resource allocation techniques that improve the wireless link performance. Given the constrains imposed by existing platforms, feasible sensing techniques are limited to light signal processing and are based on estimating the channel energy over time. Moreover, the radio resources are also conditioned, so we investigate packet size and error correcting codes adaptation, which has been missing or scarce in low-power wireless literature.

Firstly, we document the design of a novel sensor network testbed infrastructure augmented to generate interference in a repeatable and controlled way. This is essential for experimental validation of low-power wireless networks (LPWN) protocols under realistic and repeatable interference conditions [43]. This tool is specifically useful for studying the behaviour of LPWN under external interference [44] and to some extent the effects of simple jamming attacks, i.e., intentional interference that is devised to disrupt the network functioning.

The following contributions focus on techniques to mitigate CTI that could be implemented in future generation sensor network platforms. Specifically, a novel Channel Quality metric is designed to meaningfully quantify the channel [45].

Based on the Channel Quality metric, we investigate the feasibility of two important radio resource allocation mechanisms, packet size and erasure codes adaptation [46]. Such techniques are mostly implemented in the form of offline experiments in a computer, rather than using radio hardware. The experiments are designed to verify the wireless link performance for low-power networks in general settings which are agnostic to implementations in hardware.

Finally, this thesis includes a scalability study [47] of another form of intentionally generated interference in low-power networks. Namely, constructive baseband interference (CBI) used to increase the reliability of wireless links [48].

List of author's publications

The list of peer-reviewed publications partially documenting the results obtained during the research work of this dissertation follows:

Books

Nouha Baccour, Anis Koubâa, Claro Noda, Hossein Fotouhi, Mário Alves, Habib Youssef, Marco Antonio Zúñiga, Carlo Alberto Boano, Kay Römer, Daniele Puccinelli, Thiemo Voigt, and Luca Mottola. *Radio Link Quality Estimation in Low-Power Wireless Networks.* SpringerBriefs in Electrical and Computer Engineering. Springer International Publishing, Heidelberg, 2013. ISBN 978-3-319-00773-1, 978-3-319-00774-8. URL http://link.springer.com/10.1007/978-3-319-00774-8

Academic Journals

Claro Noda, Shashi Prabh, Mário Alves, Carlo Alberto Boano, and Thiemo Voigt. Quantifying the Channel Quality for Interference-aware Wireless Sensor Networks. *SIGBED Rev.*, 8(4):43–48, December 2011. ISSN 1551-3688. doi: 10.1145/2095256.2095262. URL http://doi.acm.org/10.1145/2095256.2095262

Conferences and workshops

Carlo Alberto Boano, Thiemo Voigt, Claro Noda, Kay Römer, and Marco Zúñiga. JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation. In *Proc. of the 10th Conf. on Information Processing in Sensor Networks (IPSN)*, pages 175–186, Chicago, USA, April 2011

Claro Noda, Shashi Prabh, Mário Alves, Carlo Alberto Boano, and Thiemo Voigt. Quantifying the Channel Quality for Interference-Aware Wireless Sensor Networks. In *International Workshop on Real-Time Networks (RTN)*, June 2011

C. Noda, S. Prabh, M. Alves, and T. Voigt. On packet size and error correction optimisations in low-power wireless networks. In *2013 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 212–220, June 2013. doi: 10.1109/SAHCN.2013.6644980

Claro A Noda, Carlos Pérez-Penichet, Balint Seeber, Marco Zennaro, Mário Alves, and Adriano Moreira. On the scalability of constructive interference in Low-Power wireless networks. In *12th European Conference on Wireless Sensor Networks (EWSN'15)*, Porto, Portugal, February 2015

Posters

C. Noda, S. Prabh, C.A. Boano, T. Voigt, and M. Alves. Poster abstract: A channel quality metric for interference-aware wireless sensor networks. In *2011 10th International Conference on Information Processing in Sensor Networks (IPSN)*, pages 167–168, April 2011

Chapter 2

Experimenting with Interference

Radio interference drastically affects the performance of low-power wireless networks (LPWN), leading to packet loss and reduced energy-efficiency, among other problems. The number of wireless devices operating in ISM frequency bands continues to increase and there is a strong need for understanding and debugging the performance of existing LPWN protocols under interference. Low-power wireless links have a propensity to erratic behaviour, besides the vulnerability to interference in ISM bands. Designing protocols that are resilient to interference requires a low-cost flexible testbed infrastructure—that allows the repeatable generation of a wide range of interference patterns—for experimentation and performance verification tests. We introduce the fundamentals of low-power wireless links and address the lack of such an infrastructure by repurposing off-the-shelf hardware platforms to record and playback interference patterns as well as to generate customizable and repeatable interference in real-time. We present JamLab: a low-cost infrastructure to augment existing LPWN testbeds with accurate interference generation while limiting the overhead to a simple upload of the appropriate software. We discuss how to sidestep several hardware limitations to get an accurate measurement and regeneration of interference. We also ilustrate how to use JamLab to characterize the impact of interference on LPWN MAC protocols. The design of JamLab is documented in [43].

2.1 Introduction

LPWN are usually comprised of a collection of autonomous nodes running distributed system software. This software enable the nodes to coordinate their activities and share data, typically using low-power radio technology to create wireless links among network nodes. In this way, the network of nodes behave as a whole, a single entity. Although not all sensor network applications are necessarilly distributed in nature, the fundamental communication aspects are. Thus, the system as a whole displays some robustness with regard to the nodes malfunctioning or communication links interruptions. However, in most circumstances, poor link reliability can represent a problem. Even if the link anomaly is temporary the network latency increases, packets are lost and deadlines are missed. At the network layer, a faulty link can be sidestepped by re-routing the traffic through a different path. Nevertheless, the time and network overhead necessary for detecting a faulty link and updating the routing tables can be a problem for many aplications. Firstly, the link is typically assessed via an averaged PRR metric and secondly, the distributed algorithm that establishes the new route adds even more delay in the process.

In this chapter we provide an introduction to the ways in which interference that affects low-power wireless links can be experimented with and we make the case for the need to make protocols robust against interference. We also address some of the experimental challenges that this represents.

2.2 Complexity in the Wireless Channel

Wireless communications rely on electromagnetic waves to transport information. Radio wave propagation is ultimately described by fundamental laws of classical electrodynamics, and Maxwell's equations in particular. The interaction between a propagating wave and the environment, i.e. fields and matter, other than open space, can be very complex to be effectively described by solving the corresponding equations. Instead, statistical models are used to describe the propagation of radio waves [41, Chapter 4-5]. At the cost of sacrifying accuracy, these models are tractable and lend themselves well for most radio engineering purposes.

There are peculiarities of the electromagnetic interaction of radio waves with materials present in our environment. For example, radio waves often do not require a line-of-sight between the transmitter and receiver, as they transverse non-metallic obstacles. This versatility is the reason of the ubiquitous usage of modern radio communication systems. In contrast with dedicated mediums like transmission lines, e.g. wires or optical fibres, radio waves propagating in the wireless medium experiment high level of distortion and mix with unwanted interference, both natural and human-made, which produces errors in the information conveyed. As a consequence, radio communication protocols need to eliminate such errors from the information contained in the radio signal that reaches the receiver.

Low-power networks feature short-range wireless links and rely on multihop communication. This has some operational implications: (i) low transmission power makes links less reliable, (ii) multiple hops increase the end-to-end latency and reduce throughput, and (iii) distributed information processing in the nodes enables fast all-to-all interactions, like network-wide agreement and data aggregation. Thus, low-power networks are used in relatively low-data-rate applications and the wireless links are much more prone to introduce errors in the information received. Moreover, the low-cost hardware used in low-power wireless networks restrains the computational capacity available to combat the error-prone nature of the wireless channel. Thus, most protocols have relied in rather simple techniques, e.g. retransmissions, compared to analogous sophisticated solutions (e.g. channel coding) in mobile (cellular) networks. Such simplicity hinders the predictability and reliability of the wireless links.

Additionally, the desired simplicity of low-power wireless network protocols and the low-cost hardware involved invites to design protocols that coordinate the access to the wireless medium in a distributed way. This is often handled using a probabilistic MAC scheme in which nodes verify the absence of other ongoing transmissions in the medium prior to access the channel; this is known as carrier sense multiple access (CSMA). As a consequence, low-power network suffer from inter-node interference. That is, several wireless links operating simultaneously mutually interfere with each other. In such a CSMA scheme, inter-node interference results in nondeterministic delays in the wireless links, specially in high traffic scenarios or near a sensor network (data) sink. Although CSMA is widely used in asynchronous MAC protocols, there are other ways to coordinate medium access, for example through time multiplexing which has also been explored in synchronous MAC protocols [17–19]. Additionally, many protocols use multiple 802.15.4 channels at different nodes to increase robustness and bandwidth. In these cases, interference can be handled through design choices. In the next section, we will discuss interference that originates outside the low-power wireless network and therefore cannot be suppressed by design, but instead has to be avoided or mitigated in the low-power nodes.

2.3 Interference in ISM Bands

Low-power wireless networks, as well as mobile networks, only operate effectively in a certain range of the radio frequency spectrum. Low frequency carrier waves tend to propagate better since they suffer less absortion from the environment but they also have larger wavelength, which increases the size of electrically efficient antennas. On the contrary, high frequency waves suffer from comparatively more attenuation, reflected in the channel pathloss, but requires smaller antenas while maintaing the same antenna aperture. Moreover, simple receiver designs impose a large ratio beween the carrier frequency and the bandwidth of the baseband signal, which contains useful information to convey to the other end. Thus, the usage of higher carrier frequencies increase the wireless link information capacity while using simple receivers. As a consequence there is a range of frequencies between 300 MHz and 3 GHz which is like a sweet spot for mobile wireless communications; the reader is refered to [41] for an introduction to radio wave propagation.

The case of low-power wireless networks is further complicated by their inherent low-power wireless links. Since sensor networks are characterised by small data volumes, low-power wireless links are optimised for low data rate operation and thus use relatively narrowband PHY modulation schemes. This relatively low bandwidth and power usage make cross technology contention strategies based on carrier detection not very effective, since radio transceivers from other networks are often unlikely to detect ongoing transmissions from low-power wireless nodes [52]. Moreover, commodity hardware for Wireless Fidelity (Wi-Fi) networks based on IEEE 802.11 [53] can also be vulnerable to interference from low-power wireless nodes [54], leading to a mutually deteriorating performance and complex behaviours. This bandwidth and power asymmetry leave low-power wireless links higly vulnerable to interference from other coexisting technologies. Such interference from coexisting networks in ISM Bands is typically referred as Cross Technology Interference (CTI). Furthermore, there are popular communication systems, operating in ISM bands, which worsen interference by transmitting a permanent carrier during operation, like video and audio senders [55].

Moreover, the success of solutions sprun by innovation in the unlicensed sprectrum has created a situation in which unlicensed radio bands, contained within that sweet chunk of spectrum, are increasingly crowded [56]. This has triggered research efforts into interference mitigation and coexistence enhancement techniques. A survey of literature on experimentation, measurement, modeling and mitigation of internference in low-power networks can be found in [44].

Existing communication protocols for low-power wireless networks suffer from CTI and the results are: (i) decreased sleep time due to missing or false beacon detections on node rendezvous, (ii) corrupted packets due to packet collisions, most likely due to CTI, and thus, excessive retransmissions which affect an otherwise energy efficient behaviour [43, 57], and (iii) deadline misses in real-time schemes. Thus, in applications with stringent quality-of-service requirements, robustness against interference is crucial.

The fact that the environment has a profound impact on radio propagation has led to a remarkable preference for experimental research in testbeds by the LPWN community, since simplified simulation models of radio propagation do not capture the complexity of the real world. The same holds true for interference: testbed infrastructures need to be augmented with means to generate realistic interference patterns in a repeatable manner to develop, test, and evaluate LPWN protocols and applications under interference.

2.3.1 Generating Repeatable Interference

As an increasing number of standard communication technologies operate in ISM bands, the congestion in the radio spectrum increases while the quality of communications decreases. In QoS sensitive sensor network applications, such as industrial automation and health care, radio interference represents a major challenge.

This challenge is especially serious in the 2.4 GHz ISM band, as LPWN compete with the ongoing communications of WLAN, Bluetooth, and many other technologies. Communications in these frequencies can also be affected by several domestic appliances that are source of electromagnetic noise, such as microwave ovens, video-capture devices or baby monitors. This high number of different wireless devices sharing the same frequencies and space, raises the need for coexistence and interference mitigation techniques [58, 59].

In particular, there is a strong need for understanding the performance of existing LPWN protocols under interference, as well as designing novel protocols that can deliver high and stable performance despite changing interference patterns. This, however, requires a proper testbed infrastructure where realistic interference patterns can be easily created in a precise and repeatable way.

Wireless network testbeds with heterogeneous devices, such as diverse interference sources, are costly and inflexible. We therefore propose to augment existing LPWN testbeds with *JamLab*, a low-cost infrastructure for the creation of realistic and repeatable interference patterns. JamLab supports the recording and playback of interference traces in LPWN testbeds, as well as the customizable generation of typical interference patterns resulting from Wi-Fi, Bluetooth, microwave ovens, or any other device operating in the frequency of interest. To ensure a low-cost and hence widely applicable solution, we propose to use off-the-shelf motes. In this way, a fraction of the already deployed testbed nodes could be used for interference generation with the overhead limited to the simple uploading of the appropriate software.

However, building such a low-cost solution is challenging due to the limitations of the available hardware. In order to obtain an accurate playback, the interference-pattern levels need to be measured precisely at a high sampling rate, so that also short interference patterns (e.g., resulting from Wi-Fi traffic) can be reproduced. We discuss in the next section how to obtain accurate readings of the RSSI noise floor while achieving an adequate sampling frequency of around 60 kHz on a sensor platform.

2.3.2 Experimental Challenges

While operating the radio chip of sensor platforms to record interference signals, the radio is exposed to strong signals which are not dealt with or quantified in a sensor network normal operation. However, these signals can make the node to malfunction, since they originate from more powerful interference sources that can adversely operate in the vicinity of the sensor nodes. We show that under these circumstances, many erroneous RF channel energy readings occur, and we correct such wrong readings by properly configuring the internal automatic gain control of the CC2420 radio [60]. This radio chip is (maybe the most) widely used in sensor network research platforms in the community.

Moreover, (re)generating interference requires the patterns to be reproduced accurately in both frequency and time domains. This turns out to be hard to obtain, given the coarse output power levels available from the radio transceiver and the limited memory available on the motes. We show that to achieve an accurate regeneration, voluminous records of interference patterns need to be stored in the mote in real-time and later played back accordingly. Moreover, we provide precise and lightweight models of common interference sources in the 2.4 GHz ISM band to generate (emulate) realistic patterns.

Finally, the placement of the nodes inside the testbed is also critical and needs to be optimised, after understanding the spatial domain implications of measuring and generating interference.

2.3.3 JamLab Overview

JamLab is a *low-cost* approach to augment *existing* testbeds with a way to generate *realistic* and *repeatable* interference patterns. The key idea behind JamLab is to use off-the-shelf motes to record and playback interference patterns instead of bringing Wi-Fi access points, microwave ovens, or other equipment to the testbed. The latter approach is not only costly and hard to reproduce exactly by other researchers, but it is even difficult to exactly reproduce a given interference pattern with the same appliance. For example, the sequence and timing of the Wi-Fi frames generated by a file download may differ between repeated trials due to TCP adaptation mechanisms (e.g., timeouts, window sizes).

Furthermore, every device used to generate interference in the testbed needs to be programmed remotely. Programming several heterogeneous devices such as Wi-Fi access points or microwave ovens would create a significant overhead, whereas using JamLab the installation overhead is minimal.

Indeed, with JamLab, either a fraction of the existing nodes in a testbed are used to record and playback interference patterns, or a few additional motes are placed in the testbed area. In JamLab those motes used for interference generation are called *HandyMotes*. The HandyMotes support two modes of operation: *emulation*, where a simplified model is used to generate interference patterns that resemble those generated by a specific appliance (such as a Wi-Fi device or a microwave oven); and *regeneration*, where each HandyMote autonomously samples the actual interference, compresses and stores it locally, and regenerates the recorded patterns later. The latter mode is especially useful to record realistic interference patterns, such as in a crowded shopping center or on a lively street, by placing a few HandyMotes to record interference, and bringing them to the testbed to playback the recorded traces there.

Since the maximum RF output power of motes (0 dBm) is typically much smaller than the RF output of other typical interference sources (25 and 60 dBm for Wi-Fi and microwave ovens, respectively), a Wi-Fi transmitter or a microwave oven may disturb sensor network communications over much larger distances than a HandyMote can. In JamLab, the testbed area is subdivided into cells as depicted in Figure 2.1, such that a HandyMote placed at the center of the cell can interfere with all testbed motes contained in the cell, but the interference with motes outside of the cell is minimized. This requires a careful placement or selection of HandyMotes and control of their RF output power.

To capture short interference patterns such as those generated by Wi-Fi beacons, JamLab uses high sampling rates and data compression, due to the limited amount of available memory, see [43, Section 4.1]. For the playback of recorded interference traces, a special test mode of 802.15.4 radios to generate modulated or unmodulated carrier signals is used, as detailed in [43, Section 4.2].

Another challenge is that many interference sources emit wideband signals, i.e., they interfere with many 802.15.4 communication channels at the same time. In contrast, a mote can only transmit on a single channel at a time. Although many existing LPWN protocols use a single channel only, in JamLab multiple HandyMotes are placed in each cell, each one interfering in one 802.15.4 channel [43, Section 4.3]. The use of software defined radio (SDR) techniques using USRP devices would provide more accurate jamming signals on a wider bandwidth, but at a much higher cost which represents a considerable limitation.

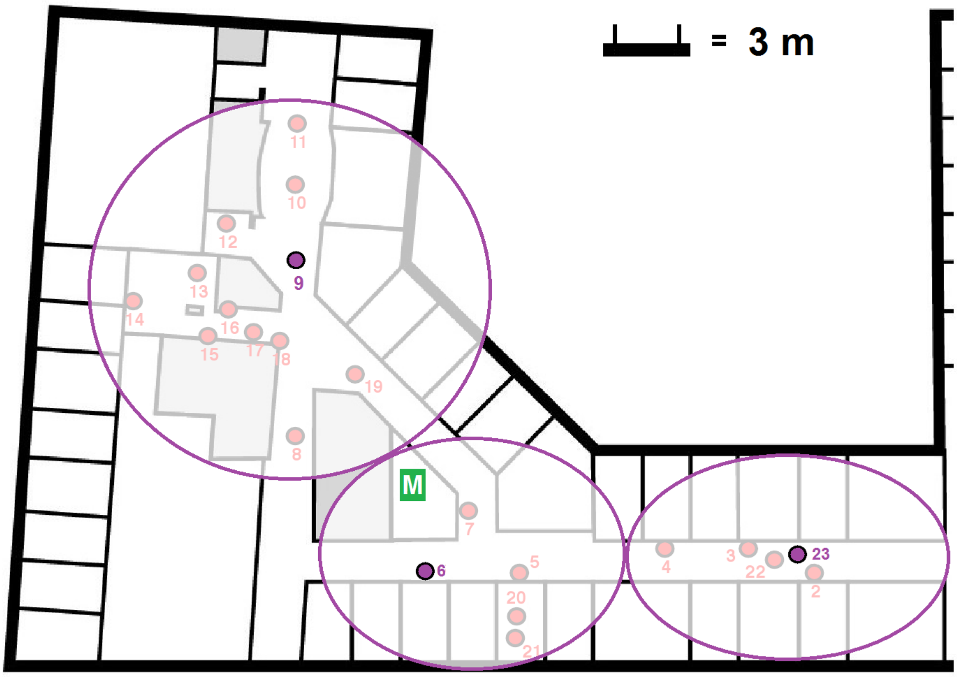


FIGURE 2.1: Testbed augmented with JamLab. Nodes 6, 9, and 23 are selected as HandyMotes, and take care of interference (re)generation in their respective cell, corresponding to the circled areas.

JamLab has been designed specifically for the Texas Instruments CC2420 radio [60], and tested on several sensor motes such as Maxfor MTM-CM5000MSP, Crossbow TelosB, and Sentilla JCreate, but the framework can be applied to any LPWN platform. Based on the analysis of the datasheets, the HandyMotes should be easily ported to similar radios such as the Ember EM2420 transceiver, and to newer radios such as the CC2520. We develop the HandyMotes based on Contiki, a lightweight and flexible operating system for tiny networked sensors [61].

2.4 Measuring Interference

Measuring interference accurately on a mote is a key functionality, for recording and later playback of interference, as well as for acquiring a deep understanding of common interference sources such as Wi-Fi or Bluetooth. We describe in this section the techniques we used in order to let a common sensor mote measure the interference accurately at a sufficiently high sampling rate.

2.4.1 Measuring at High Sampling Rates

Link quality indicators such as RSSI and LQI provide a quantitaive indication of the signal strength and quality, upon the reception of a packet. The only feasible way to assess the interference status is hence the continuous measurement of the RSSI noise floor, i.e., the RSSI in absence of packet transmissions.

In order to retrieve the spectro-temporal characteristics of different interference sources, we improve existing Contiki tools [62] and develop two applications that scan the 2.4 GHz frequency spectrum by reading the RSSI noise floor from the CC2420 radio transceiver:

- The *time scanner* scans a single predefined IEEE 802.15.4 channel at its middle frequency with a very high sampling rate, and returns the RSSI noise floor readings over time;
- The *frequency scanner* scans sequentially the whole 2.4 GHz spectrum by switching between all 802.15.4 channels.

A first requirement of both scanners is to achieve a high sampling rate, given that we need to detect short transmissions periods. After boosting the CPU speed, optimizing the SPI operations, as well as buffering and compressing the RSSI noise floor readings using Run-Length Encoding (RLE), we reached a maximum sampling rate of approximately 60.5 kHz when sampling a single channel with the *time scanner*. The highest sampling frequency reachable by the *frequency scanner* is instead 3.4 kHz, since it is constrained by the settling time of the radio when switching channels. Hence, the limitations of low-power radios do not permit to achieve a sampling rate sufficiently high to capture all Wi-Fi transmissions.

The minimum size of a Wi-Fi packet is 38 bytes (ACK and CTS frames), which would make a resolution of 60 kHz sufficient to detect all 802.11b frames, but not all 802.11g/n frames. As most Wi-Fi frames are data frames and typically contain higher layer headers, one can sample at 60 kHz frames with TCP/IP headers having a payload size higher than 27 and 227 bytes for 802.11g/n, respectively. Despite the use of large PDUs to reduce preamble overhead [63], this resolution does not guarantee to capture all the VoIP traffic over 802.11g/n [64].

Another requirement for the scanners is to accurately measure the strength of the ongoing interference in the radio spectrum by means of precise RSSI noise floor readings. The CC2420 radio specifies an accuracy of ±6 dBm, and a linearity of ±3 dB in the dynamic range $[-100, 0]$ dBm. Such accuracy and linearity has so far been acknowledged by the research community as enough to carry out operations such as Clear Channel Assessment (CCA) and low-power channel sampling for activity recognition [65]. However, our experiments show that the RSSI noise floor readings captured at high sampling rate suffer from a systematic problem in three specific scenarios, namely: (i) when a narrow unmodulated carrier is transmitted, (ii) when microwave ovens are switched on, and (iii) in the presence of Bluetooth transmissions. In these scenarios, the CC2420 radio often returns RSSI values that are significantly below the supported range and the sensitivity threshold, e.g., -110 or -115 dBm. Figure 2.2 reports examples of such wrong readings, which represent an important problem, since they also impact the correct functioning of CCA in the presence of narrow-band signals, as shown in Figure 2.2c.

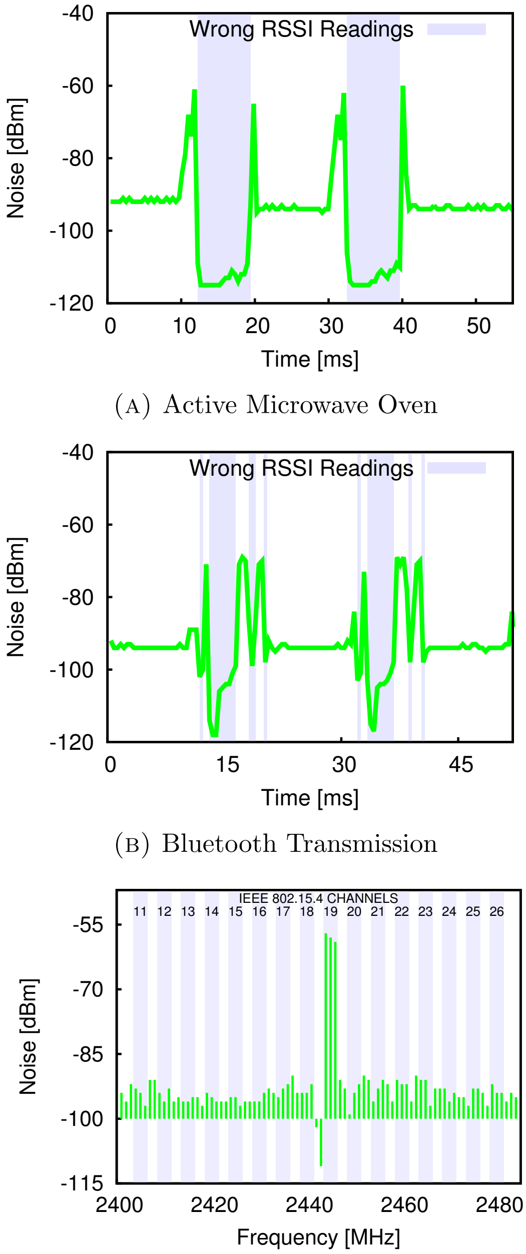
Our investigation also shows that the same problem applies to other sensornet platforms employing similar versions of the chip, such as the Ember EM2420 transceiver. We experimentally identified that the problem is due to the saturation of the Intermediate Frequency (IF) amplifier chain: we have observed that maximum gain is used in the Variable Gain Amplifier (VGA) when the incorrect RSSI readings occur.

2.4.2 Avoiding Saturation in RSSI Readings

The origin of this saturation problem can be found in the radio demodulation chain. The CC2420 chip implements part of the IF filtering in analog domain and further filtering is later performed in the digital domain. It employs an Automatic Gain Control (AGC) loop to maintain the signal amplitude close to a certain target value that guarantees the correct operation of the Analog-to-Digital Converter (ADC). More specifically, the signal is maintained within the ADC dynamic range, despite large variations in the input signal from the antenna. For this purpose, the AGC loop uses a digital sample of the final IF signal amplitude and adjusts the gain of the VGA stage accordingly (see Figure 2.3). If a narrowband signal is present near the cut-off frequency of the combined IF chain, the resulting sampled signal amplitude may be remarkably lower than the partially unfiltered one at the ADC, as a consequence of the digital filtering. Since the AGC uses the final value to set the gain of the amplifier chain, there is no guarantee that the ADC is not saturating. Upon ADC saturation, the receiver is no longer linear and the RSSI values are incorrect.

To linearize the radio response for an arbitrary noise signal and hence avoid wrong RSSI readings, we activate the peak detectors in-between the amplifier stages, so that their output is used by the AGC algorithm to compute the required gain. The latter is attained with VGA stages and the system switches in and out fixed gain stages as needed. In the CC2420, the peak detectors are controlled by the *AGCTST1* register, and can be configured as follows:

```
unsigned temp;
```



(A) Active Microwave Oven

(B) Bluetooth Transmission

(C) Unmodulated Carrier

FIGURE 2.2: Examples of wrong RSSI readings: several values are significantly below the sensitivity threshold of -100 dBm due to receiver saturation. This error is caused by an incorrect operation of the AGC loop in presence of narrow-band signals.

```
CC2420_READ_REG(CC2420_AGCTST1, temp);
CC2420_WRITE_REG(CC2420_AGCTST1,
(temp + (1 << 8) + (1 << 13)));
```

The register also includes flag bits to activate peak detectors among fixed gain stages in the IF chain and at the ADC itself [60].

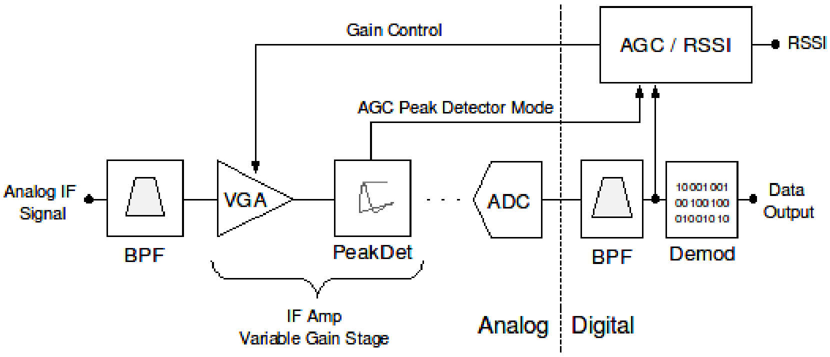


FIGURE 2.3: Simplified diagram of the CC2420 AGC loop.

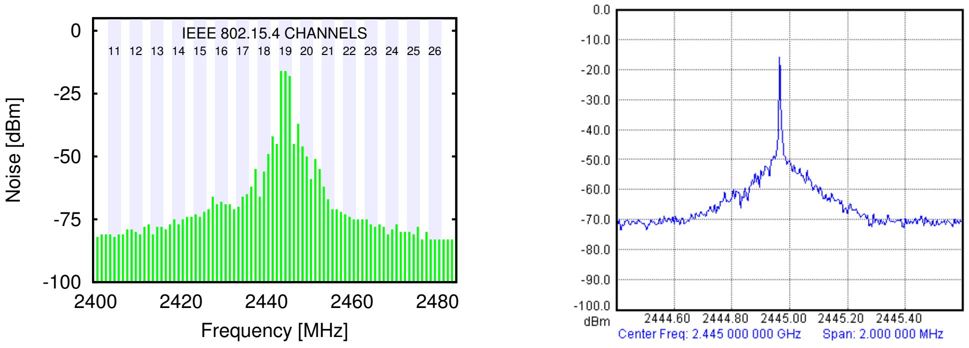
2.4.3 Validation of the Experimental Setup

We validate our RSSI noise floor measurements both in time and frequency with the help of a professional Anritsu MS2711D spectrum analyzer [66]. In these experiments, we connect the RF ports of the transceivers or the analyzer directly via a 50 Ohms matched impedance RF pigtail. This isolates the signals of interest from external noise sources and eliminates the medium pathloss, so that the amplitude of the tone and the spectral footprint can be compared.

Firstly, we verify the correctness of the *frequency scanner* readings, using the unmodulated test signal available in the CC2420 radio. In order to do this, we program another mote to transmit an unmodulated tone at 2445 MHz, the center of IEEE-802.15.4 channel 19, at maximum power. Figure 2.4a shows the correct operation of the receiver and the linearized IF amplifier chain while scanning the RSSI values across the band using the peak detectors. The same test signal can be seen in the spectrum analyzer (Figure 2.4b). This worst case scenario shows that we have linearized the receiver, thus avoiding wrong RSSI noise floor readings.

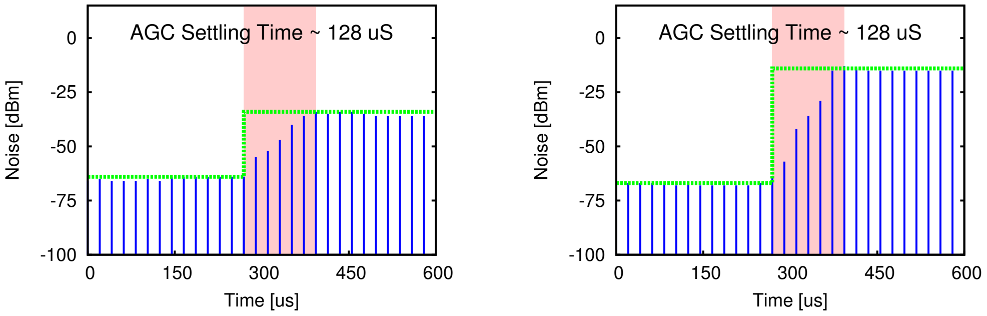
Secondly, we measure the evolution of the RSSI readings over time to an RF tone step signal, in order to evaluate the accuracy with which we can effectively measure RSSI values. We use our *time scanner* with two different power levels (-25 and 0 dBm), and obtain the results shown in Figure 2.5. The frequency of the scanner is sufficiently high to show how the CC2420 internally averages the RSSI over the last 8 received symbols, or 128 μs, as defined by the IEEE 802.15.4 standard. Such settling time is shown to be independent of the height of the step signal.

Impact on Clear Channel Assessment (CCA). Activating the peak detectors in-between the amplifier stages also improves the reliability of the CCA operation commonly used in MAC protocols [65]. Due to wrong RSSI readings, the CCA returns a



(A) Sensor Mote (B) Anritsu MS2711D

Figure 2.4: Single tone excitation obtained running the *frequency scanner* operating across the band (a), and in the Anritsu Spectrum Analyzer, with a frequency span of 2 MHz (b). Notice the correct readings despite the very narrow pulse used, as compared to Figure 2.2c.



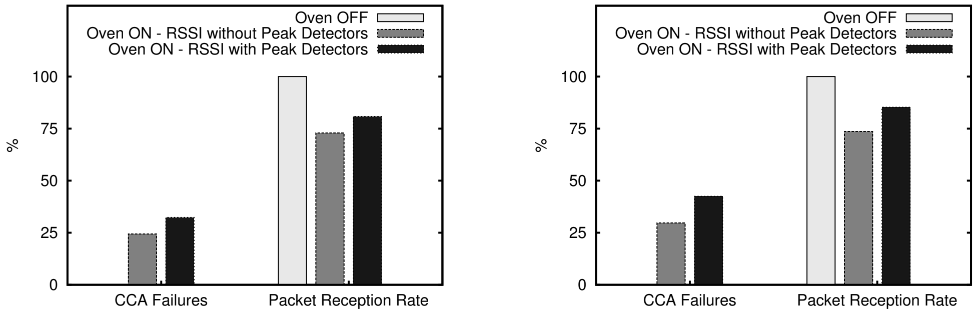
(A) -25 dBm (B) 0 dBm

Figure 2.5: Evolution of RSSI readings over time for two different RF tone step signals. The accuracy of our RSSI scanner is high enough to show the moving average used by the CC2420 to compute the RSSI over the last 8 received symbols.

clear channel when a narrow unmodulated signal is transmitted. As a result of this, the application would generate a transmission that is very likely to fail, thus wasting some of the limited energy budget.

A typical example of this would happen when transmitting packets in the presence of an active Bluetooth device or a microwave oven in the neighborhood. Our approach significantly improves the CCA accuracy, leading to a higher Packet Reception Rate (PRR).

Figure 2.6 shows the amount of ”channel busy” outcomes of CCA before and after activating the peak detectors. The absolute gain in terms of PRR depends on the microwave oven model, on the channel of interest, and on the data rate. We experimentally collect data at the receiver side of a couple of sensor nodes communicating periodically at a rate of 128 packet-per-second (packet/s) in presence of an active Lunik 200 microwave oven in the neighborhood. The nodes are placed 1 meter apart and use a transmission power



(A) Channel 23

(B) Channel 25

Figure 2.6: Avoiding wrong RSSI readings—through peak detection—improves the CCA accuracy and packet reception rate under interference.

of -25 dBm. As shown in Figure 2.6, the PRR increases by up to 12% when activating the peak detectors and avoiding wrong RSSI readings.

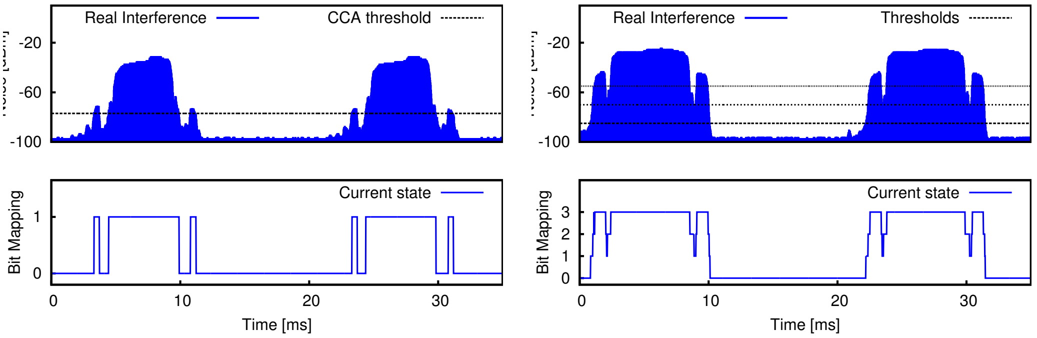
2.5 (Re)Generating Interference

With the techniques to accurately measure interference introduced in the previous section, HandyMotes record and replay interference patterns. We describe first how to compress and store traces in COTS motes and then how to playback those recordings.

2.5.1 Recording Interference Traces

When used in *regeneration* mode, HandyMote records interference traces that are later played back accordingly. Those traces can be either stored on the mote in RAM or Flash memory, or—if the HandyMote is connected to a testbed during recording—can be streamed over a wired backchannel to a base station. In any case, the data rate of 480 kbps generated by sampling RSSI with a resolution of 8 bits to hold values between 0 and -100 dBm at 60 kHz is too high to store it directly in memory or to stream it over the backchannel. The very efficient Coffee Flash file system supports a peak write bandwidth of only 376 kbps [67], the MSP430 UART supports a maximum data rate of 460 kbps for writing to the USB backchannel, and the limited 4 kB RAM of the MSP430 could just record a trace of less than 70 milliseconds duration.

While we need a high compression ratio, the compression method has to be efficient enough to allow sampling of RSSI at 60 kHz. Therefore, we use a simple Run-Length Encoding strategy and a quantisation of the samples to a few bits per sample. We store a stream of pairs (v, o), where v is a sample and o is the number of consecutive occurrences of this sample. This method is very effective, as RSSI values typically change slowly



(A) 1-bit precision

(B) 2-bit precision

FIGURE 2.7: Encoding techniques to save memory resources.

over time. The quantisation is justified by the fact that the CC2420 only supports 11 distinct output power levels in the range [-55,0] dBm by setting the PA_POWER register to the values we derived and listed in Table 2.1. To obtain the highest possible output resolution, four bits per sample with an appropriate non-linear quantisation are hence sufficient. For example, for a two-bit resolution one can use thresholds -55, -70, and -80 dBm (or register values 31, 7, and 3) with a spacing of 15 and 10 dBm, respectively, for quantizing the RSSI range into four regions.

Figure 2.7b shows how original RSSI readings (top) are mapped into 2 bits (bottom): the two-bit quantisation of a 35 ms interference recording reduces the amount of data from 2076 bytes to 84 bytes—a compression ratio of 1/25. A single bit per sample is enough to support binary interference regeneration. This corresponds to the outcome of a continuous CCA operation, in which the outcome busy/idle channel is mapped to a binary number [68]. Figure 2.7a shows the outcome of a one-bit quantisation of 35 ms of interference. The amount of data is reduced from 2076 bytes to 20 bytes – a compression ratio of less than 1/100. This reduces the raw data rate of 480 kbps to less than 5 kbps (depending of course on the values of the raw samples), a data rate that can be handled by Flash and USB, and allowing us to store several seconds of recording in RAM. In our current implementation, we store traces in RAM.

PA_POW.	dBm	PA_POW.	dBm	PA_POW.	dBm
31	0	15	-7	2	-45
27	-1	11	-10	1	-50
23	-3	7	-15	0	-55
19	-5	3	-25	-	-

TABLE 2.1: Discrete output power levels of the CC2420 radio.

Recording interference traces is energy demanding, as both CPU and radio need to be constantly active while scanning the radio medium. Using software-based on-line energy estimation [69], we obtain an average power consumption of 65.4 mW for Tmote Sky motes, which allows for a lifetime up to 4 days when powered using primary AA batteries.

2.5.2 Generating Interference Patterns

Boano et al. have shown how the CC2420 test modes can be used to generate controllable and repeatable interference [70, 71] by transmitting a modulated or unmodulated carrier signal that is stable over time. This approach is superior to common jamming techniques based on packet transmissions, as the emitted carrier signal is independent from packet sizes and inter-packet times.

In order to generate an interference pattern, the interferer has to be enabled and disabled and its output power has to be set according to the compressed recorded trace in regeneration mode or according to the output of models in emulation mode, as described in [43, Section 5]. When enabling the transmitter using the STXON command, the radio oscillator first has to stabilize before a transmission is possible, resulting in a latency of 192μs or a maximum playback frequency of only 5 kHz. Therefore, we leave the transmitter on and just change the output power level to 0 (or -55 dBm) instead of disabling the transmitter. At level 0 the RF output power is so small that even a receiver at a distance of only few centimeters can hardly notice the signal. The advantage of this approach is that the latency for changing the output power is dominated by the SPI access time. We optimized the SPI driver in Contiki, resulting in a latency of only few microseconds – allowing us to to playback at the same frequency of 60 kHz that was also used during recording.

Besides the sampling and playback rate, also the jitter during playback of the individual samples needs to be minimized in order to ensure an accurate reconstruction. At 60 kHz, the playback time between two consecutive samples is just 17μs, hence the duration of the execution of a sequence of microcontroller instructions is no longer negligible. In particular, different execution paths in the program to uncompress samples in regeneration mode lead to different execution times and jitter. Therefore, we add NOP instructions to make all execution paths equally long.

Since each node can only transmit in one of the IEEE 802.15.4 radio channels, multiple channel interference generation requires time synchronisation among HandyMotes operating in different channels. The reader is referred to [43, Section 4.3] for a discussion of how multiple channel interference generation is achieved in JamLab.

In addition to recording and replaying interference, JamLAb also emulates interference patters based on simple models of the most common interference sources, as described in [43, Section 5].

2.6 Evaluation

In this section, we first evaluate the accuracy with which a HandyMote can regenerate a previously recorded interference trace in the time domain. We then augment an existing sensornet testbed infrastructure with JamLab, and evaluate the accuracy with which the augmented testbed can regenerate a previously recorded interference trace in the spatial domain. Finally, we use JamLab to characterize the performance of MAC protocols under interference.

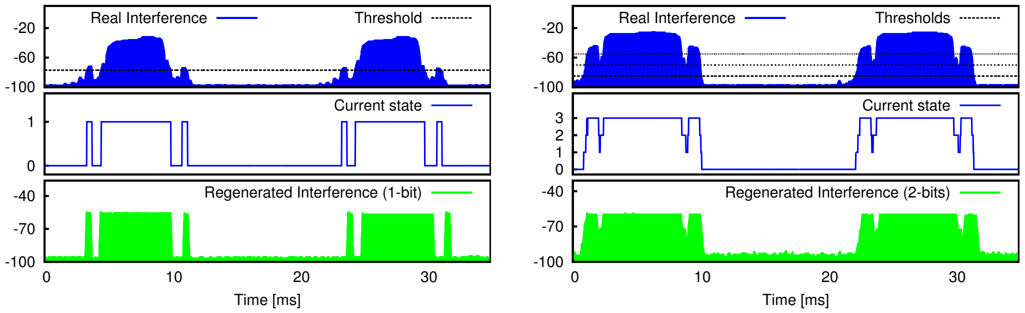
2.6.1 Temporal Accuracy

We evaluate the accuracy with which a HandyMote can regenerate a previously recorded interference in the time domain. We run a HandyMote in regeneration mode in proximity of an active Lunik 200 microwave oven warming a bowl of tea. The HandyMote is placed at 1 meter distance from the oven, and records a trace of channel 24 at a 60 kHz sampling rate. Figure 2.8a (top) shows the interference generated by the microwave as measured by the HandyMote. Next, the trace is quantized to single-bit resolution (middle). Finally, once the microwave oven stopped operating, the HandyMote plays back the recorded binary interference (bottom) using transmission power 0 dBm. As we can notice from the figure, the regeneration is quite accurate in the time domain.

We quantify the accuracy of the regenerated signal with respect to the originally recorded signal using the the *cross-correlation* coefficient (**c**). We represent original and regenerated signals by the series $x(i)$ and $y(i)$, respectively, where $i = 1, \ldots, N$. These series are binary, and take 0 (clear channel) or 1 (busy channel) values. Considering this representation, **c** is given by:

$$\mathbf{c} = \frac{\sum_{i=-\infty}^{\infty} x(i)y(k-i)}{rms(x)rms(y)} \tag{2.1}$$

where $rms()$ denotes the root mean square value of a signal. We tested eight pairs of original and regenerated samples and the maximum value of **c** was selected for each pair:



(A) 1-bit Mapping

(B) 2-bit Mapping

FIGURE 2.8: Regenerated interference of a microwave oven.

$$\mathbf{c}_{xy} = \max_{k\in[-(N-1),(N-1)]} \{\mathbf{c}\} \tag{2.2}$$

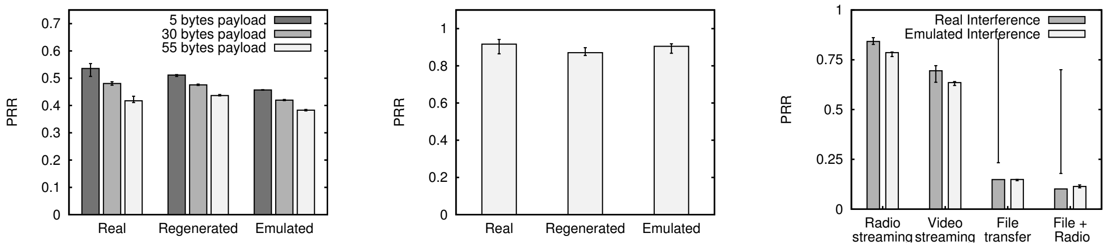
The average correlation $\mathbf{c}_{xy}$ is 0.93 with a standard deviation of 0.065. Hence, our implementation does a commendable job with respect to the cancellation of the jitter between sampled and regenerated interference and hence regenerates interference with a fairly high accuracy.

We carry out the same experiment using 2-bit quantisation with thresholds -55, -70, and -80 dBm, and we then regenerate the interference using transmission power register levels 31, 7, and 3 (i.e., 0, -10, -25 dBm), respectively. The results match the previous ones with binary interference. Figure 2.8b shows the regeneration process when using a two-bit quantisation.

2.6.2 Impact on Packet Reception Rate

In this section we experimentally study the impact of interference on Packet Reception Rate (PRR), comparing the PRR for original, emulated, and regenerated interference signals. We use the same Lunik 200 microwave oven as in the previous experiment, and collect data at the receiver side of a pair of sensor nodes at about 1 meter distance, with the sender transmitting packets at a rate of 128 packet/s. The sensor just transmits the packet without any clear channel assessments or duty cycling. We place a HandyMote between the two nodes and we run it both in emulation and regeneration mode, once the microwave oven stopped being active.

We carry out different experiments with different payload sizes, and we run the HandyMote using transmission power 0 dBm in both emulation and regeneration mode, such that the generated interference signal blocks communication between the sensor nodes. Figure 2.9(a) shows the results.



(a) Microwave Oven (b) Bluetooth (c) Wi-Fi

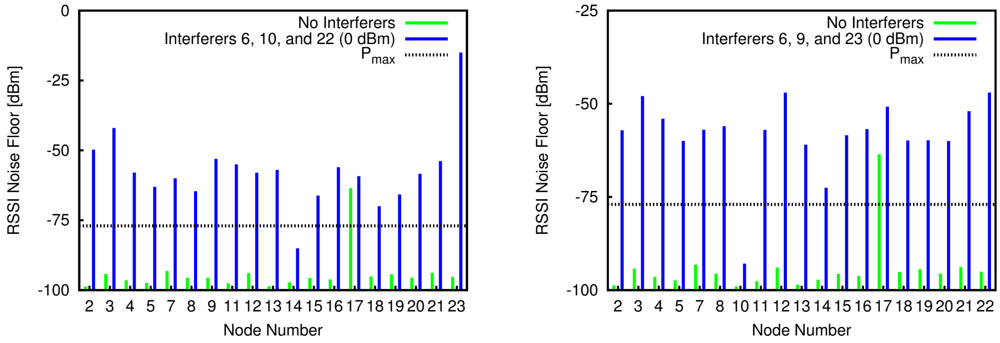
Figure 2.9: Impact of real, emulated, and regenerated interference on packet reception rate.

The PRR collected when the microwave oven is active decreases when the payload size increases as the probability of periodic microwave interference hitting a packet increases with increasing payload size. The PRR obtained for regenerated interference differs by 5.6% from the original one, hence showing a reasonable accuracy. For emulated interference, the PRR differs from the original one by 12.83%, the reason for that being the quantisation error of a fixed power microwave emulation compared to the noisy amplitude of the original interference signal, whis is occasionally too weak to block the transmission. In contrast, the emulated interference signal is binary and always blocks communication. Accuracy is improved in this case by using a random transmission power of the HandyMote [43, figure 9].

We repeat the experiments in presence of Bluetooth interference. We first measure PRR during a Bluetooth file transfer between a laptop and a mobile phone. We place the HandyMote between the two communicating motes and we measure the PRR obtained with original, emulated, and regenerated interference. We run the HandyMote in emulation mode using the models derived in [43, Section 5.2]. Figure 2.9(b) shows that the packet reception rate obtained under regenerated interference differs by 5.02% from the the original one, while in emulation mode it differs by only 1.31%.

Finally, we repeat the experiment with Wi-Fi interference. Using the same setup as above, we run the HandyMote in emulation mode using the models derived in [43, Section 5.1] while generating Wi-Fi traffic from a laptop for various traffic scenarios.

Figure 2.9(c) shows the results. Also in this case the HandyMote generates interference quite accurately, and the difference between the PRR obtained under real interference and the one obtained under emulation varies between 0.25% and 8.56%. The reason for this difference is that emulation repeats the same pattern over and over, while actual Wi-Fi interference might change in time, due, for example, to TCP adaptation mechanisms.



(A) HandyMotes 6, 10, and 22

(B) HandyMotes 6, 9, and 23

FIGURE 2.10: Testbed augmented with JamLab. In the first configuration, nodes 6, 10, and 22 are selected as HandyMotes. In the second configuration, nodes 6, 9, and 23 are selected instead.

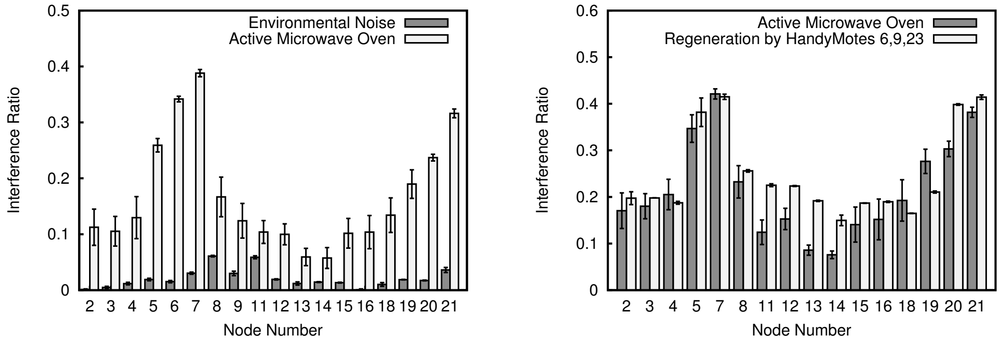
2.6.3 Spatial Accuracy

Next we want to study the accuracy of the spatial distribution of interference generated by a testbed that has been augmented with JamLab, and therefore configured as described in [43, Section 6.3]. Figure 2.1 shows the topology of the testbed used, which features 25 Tmote Sky nodes deployed in an office environment.

There is a tradeoff between the accuracy of regeneration and the cell size, as larger cell size leads to larger cross-talk regions, where motes may be interfered by multiple HandyMotes in neighboring cells, as discussed in [43, Section 6.2]. We therefore investigate a worst-case scenario with respect to accuracy, where only a few large cells with large cross-talk regions are used.

Figure 2.10a shows that, with this configuration, node 14 would not be covered as RSSI is smaller than -77 dBm due to the remote location of the node. We therefore change the selection of the HandyMotes (instead of adding more cells) to nodes 6, 9, and 23 as shown in Figure 2.1). With this configuration node 14 is covered, but node 10 is not covered by HandyMote 9 (Figure 2.10b), while in the original configuration node 10 covered node 9 (Figure 2.10a). This is an example of an asymmetric link – something the simple model in [43, Section 6.2] does not capture.

Using this testbed configuration obtained in the previous section, we now study how accurately we can regenerate the spatial distribution of interference. For this, we place a Whirlpool M440 microwave oven in the position marked as M in Figure 2.1, within the cell controlled by HandyMote 6. This case represents a worst-case scenario, as the oven can interfere over long distances due to its high (60 dBm) and highly varying output power.



(A) Impact of microwave oven

(B) Impact of regeneration

FIGURE 2.11: Comparison between the interference generated by an active microwave oven and the one regenerated by JamLab in regeneration mode throughout the whole testbed.

Our goal is to record the spatial distribution of the interference patterns generated by the microwave oven in one of the most affected channels (23) all over the testbed. We then let the HandyMotes regenerate the recorded traces while the remaining nodes record the regenerated interference and compare it with the original interference recorded while the microwave oven was active.

As we have already investigated the temporal accuracy of regeneration in Section 2.6.1, we now focus on the distribution of the intensity of interference. Instead of recording raw traces, every mote computes the *interference ratio* as the fraction of time in which interference is present (i.e., the fraction of RSSI noise floor readings higher than P_{max}).

Figures 2.11a and 2.11b show the comparison of the interference ratio during the activity of the microwave oven, and during the regeneration using JamLab (HandyMotes 6, 9, and 23). Due to their different distances from the microwave oven, node 7 recorded the highest interference ratio when the oven was active, followed by nodes 6, 21, 20, and 5, respectively (Figure 2.11a). The regeneration within this cell is based on the trace recorded by HandyMote 6, therefore nodes 21, 20, and 5 will perceive a higher interference ratio, node 7 a lower one (Figure 2.11b). A similar reasoning can be applied to all other nodes in the testbed: node 14, for example, perceives a higher interference ratio, as recorded by HandyMote 9, which is closer to the oven. If a better spatial accuracy is required, a higher number of (smaller) cells needs to be configured [43, Section 6].

It is important to remark that the environmental noise may play an important role in the quality of the interference (re)generation, as it will add-up to the interference (re)generated by the HandyMotes. Observing Figures 2.11a and 2.11b, we can see how the interference received by node 8 is higher than the one recorded by HandyMote 9 due to a high environmental noise. In order to reduce the non-determinism caused by

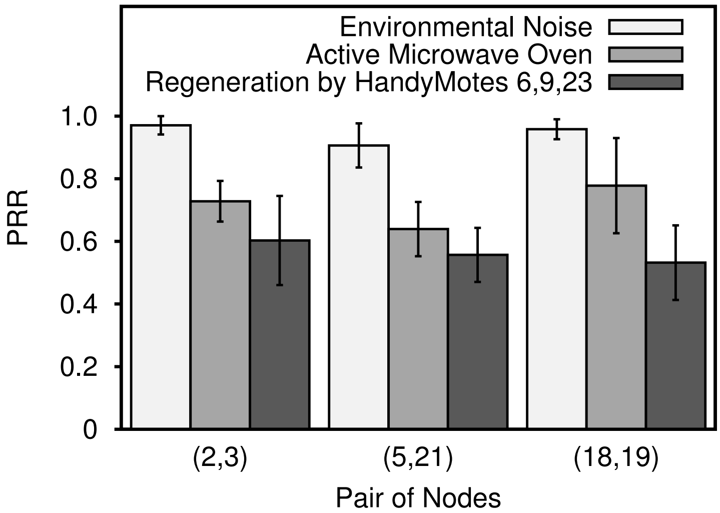


FIGURE 2.12: Comparison of the PRR obtained generating interference using a microwave oven and using JamLab.

differences in ambient interference between recording and regeneration, the experiments should be run when the background noise is low, for example in the evening or during the night.

We finally investigate the accuracy of the regeneration with respect to PRR. We repeat the above experiment while nodes pairs (2,3), (5,21), and (18,19) transmit and receive packets with a payload of 5 bytes at a rate of 64 packet/s on channel 23. Figure 2.12 shows that PRR values are similar between original and regenerated interference for the first two pairs of nodes, while there is a larger error (31.6%) for pair (18,19). This is due to nodes 18 and 19 being much closer to the microwave oven than HandyMote 9, following the discussion made for Figure 2.11.

2.6.4 Characterization of Protocol Performance

In this section we demonstrate the usability of JamLab by characterising the impact of interference on low-power MAC protocols. We show that using JamLab we can get important insights regarding protocol behaviour under *emulated but realistic* interference.

We perform our experiments in the testbed shown in Figure 2.1. Our setup consists of a sender (node 7), a receiver (node 5) and one (node 6) or two (nodes 6 and 21) HandyMotes, whose position and transmission power is carefully chosen to jam the communications between sender and receiver. The sender transmits 400 packets to the receiver at a rate of 1 packet/s. We use 3 different MAC layers: NULLMAC, a simple layer that just forwards packets between the radio driver and the network layer, X-MAC [72], and X-MACQ [73], an enhanced X-MAC with a queue and the ability to rapidly drain the queue in absence of interference.

A first HandyMote generates interference using the implementation of Garetto's 802.11 model [43, Section 6]. We use the model with the RTS/CTS access mechanism and set the minimum and maximum contention window size to 32 and 1032, respectively, as these seem to be the most widely used parameter settings. We emulate saturated traffic from 20 stations (this amount was chosen to have an interference time similar to the one of an active microwave oven), where each station sends packets with a size of 1000 bytes. A second HandyMote emulates a microwave oven as in [43, Section 6].

Table 2.2 shows our results. We depict the average results of three runs. With NULLMAC and microwave oven interference, the PRR is slightly lower than 50%, which confirms the results in Figure 2.9(a). The table also shows that under microwave oven interference, X-MAC performs better than NULLMAC with smaller payloads. As explained in [74], the reason for this is X-MAC sending strobes for a longer time than its off-time and hence the receiver has on average more than one chance to complete the handshake.

While it is known that the PRR decreases with increasing packet size, X-MAC's PRR decreases significantly, namely from almost 60% to less than 40%, as the packet size increases from 30 to 100 bytes. Also, in presence of Wi-Fi interference X-MAC performs much worse for large packet sizes. The experimental results in Figure 2.9(a) are taken using NULLMAC. Combining the results in this figure with the ones in Table 2.2, we see a very modest decrease of NULLMAC's PRR with increasing packet size.

The difference between NULLMAC and X-MAC is that in order to receive a data packet, a receiver that employs NULLMAC needs to successfully receive 1 packet only, whereas X-MAC requires the completion of the handshake, i.e., the receiver needs to receive the sender's strobe and acknowledge it, before the sender can send the data packet to the receiver. In our experiments, this data exchange must happen within one time period without interference. This means that until the data packet itself is transmitted, a substantial fraction of a time period without interference has already been used for the handshake. Note that this time period without interference is short due to the bursty interference patterns created by both microwaves and Garetto's Wi-Fi model as the latter emulates saturated traffic. This explains why the packet size is more important for X-MAC than for NULLMAC. The table also shows that X-MACQ is more robust than X-MAC against interference, hence confirming the results in [74] using more realistic interference patterns generated using JamLab.

Payload (bytes)	Oven NULL	Oven X-MAC	Wi-Fi X-MAC	Both X-MAC	Both X-MACQ
30	45.3%	59.2%	41.6%	20.9%	39.7%
100	43.6%	39.5%	23.8%	9.2%	15.6%

Table 2.2: Performance of different MAC protocols under emulated but realistic interference (average PRR in %)

2.7 Summary and Future Work

Interference has a strong impact on LPWN performance. Hence, protocols and applications need to be tested under realistic and controlled interference. We present JamLab, a tool to augment existing LPWN testbeds with a low-cost infrastructure for the creation of realistic and repeatable interference patterns. JamLab provides simple models to emulate the interference patterns generated by several devices, and a playback capability to regenerate recorded interference patterns. We demonstrate the utility of JamLab by showing its accuracy in both temporal and spatial domains.

Future work includes a further automation of the testbed configuration procedure, and an accurate study and modeling of new interference sources in the frequency bands used by LPWN.

My contributions

I am a co-author of the JamLab paper [43]. I have devised the experiments to identify the cause of the erroneous RSSI readings in the CC2420 radio chip. These experiments allowed us to verify the saturation of the amplifiers in the receiver RF chain and I proposed a (re)configuration of the automatic gain control (AGC) of the chip. I conducted experiments to verify the correct operation of the new configurations using a professional Anritsu MS2711D spectrum analyzer. During this experimentation and further familiarisation with sophisticated functionality and diagnostic/testing features of the chip, we were able to tweak them for our purposes. I was involved in the design process of JamLab. I have assisted in carrying out the experiments, and contributed to the manuscript.

I have also contributed to a bibliographic review on existing interference mitigation techniques and link quality estimation documented in [44].

Chapter 3

Channel Quality Metric

Reliability of communications is key to expand application domains for sensor networks. Since most LPWN operate in the license-free Industrial Scientific and Medical (ISM) bands and hence share the spectrum with other wireless technologies, addressing interference is an important challenge. In order to minimize its effect, nodes can dynamically adapt radio resources provided information about current spectrum usage is available.

We present a new channel quality metric—dubbed `CQ`—based on availability of the channel over time, which meaningfully quantifies interference. We discuss the optimum scanning time for capturing the channel condition while maintaining energy-efficiency. Using data collected from a number of Wi-Fi networks operating in a library building, we show that our metric has strong correlation with the Packet Reception Rate (PRR). This suggests that quantifying interference in the channel can help in adapting resources for better reliability. In this line, we present a discussion of the usage of our metric for various resource allocation and adaptation strategies, preconizing our contributions in Chapter 4. The work included in this chapter was partially documented in [45].

> *"Like sin itself, the deliberate un-licensing of spectrum began with an Apple."*
>
> Henry Goldberg

3.1 Introduction

Wireless technologies have grown exponentially during the last decade and are progressively cast around for more applications. Many standardized technologies operate in crowded license-free Industrial Scientific and Medical (ISM) frequency bands. The deployment of co-located wireless networks operating in the same band is increasingly unavoidable. Wireless networks become more and more ubiquitous in residential and office buildings as they offer great flexibility and cost benefits. These networks usually serve different purposes, use different technologies and are most often not designed to communicate with each other. However, despite the extensive research, the issue of reliability of wireless networks remains a challenge: since they operate in the same band, they suffer from performance degradation due to interference.

Medium access techniques such as TDMA and FDMA cannot be readily applied in the context of ISM bands [75], as they are not designed to tolerate inter-network interference. Instead, distributed multiple access schemes based on *carrier sense*—such as CSMA—are widely employed along with *spread spectrum* modulation techniques, which provide some robustness as well as generate lower levels of interference.

Low-power wireless networks have lead to a flurry of research and standardization processes in the last decade, with reliability and energy efficiency as the primary concerns. On the other hand, the proliferation of the IEEE 802.11 based Wi-Fi networks has been significant. This trend will further continue with the deployment of the fourth generation mobile cellular networks (LTE/4G). In order to satisfy the increasing data traffic demands, it is not uncommon for network operators to divert load to the unlicensed spectrum, avoiding spectrum licensing costs as well.

Although this bottom-up approach to unlicensed spectrum usage exacerbates the challenges to achieve reliability and predictability in low-cost wireless solutions, there are many gains for end users [76] and extensive opportunities for innovation [77]. It has also incubated new research directions, such as dynamic spectrum allocation for future wireless systems [78]. Inspired by this paradigm, we investigate mechanisms for interference avoidance within ISM bands for low-power radios.

Some wireless networks, like sensor networks, require low-power operation. In such LPWN, the Physical (PHY) and Medium Access Control (MAC) layers are typically based on the IEEE 802.15.4 standard, a standard developed for wireless low-power personal area networks (WPANs). Although sensor network protocols are designed for energy-efficiency, most of them, however, do not explicitly account for interference. Especially in the case of high sustained interference, the overall energy consumption in communications increases due to factors such as excessive retransmissions and decreased sleep times [73].

Wireless Sensor Networks (WSN) are seen as a viable alternative for monitoring, control and automation applications, provided they are made appropriately reliable and delays are bounded. To this end, interference and coexistence pose a major challenge. In this chapter, we present the *channel quality* (`CQ`) metric that provides a quick and accurate estimate of interference by capturing a channel's availability over time at a very high resolution. This metric is useful towards achieving better reliability and lower latency through dynamic radio resources allocation.

Interference in low-power wireless networks has two distinct origins. First, there is the interference that may be experienced by the cumulative effect of concurrent transmissions of nodes, which is well captured by the Signal to Interference plus Noise Ratio (SINR) model. Second, the interference produced by other networks like those based on the IEEE 802.11, operating on overlapping channels have large RF power and spectrum footprint. Even though CTI represents a well known problem [79–82] it has not been adequately addressed in LPWN. This problem is hard to resolve for two reasons: (i) efficient cooperative schemes for spectrum access are not possible with currently deployed technologies and (ii) there are large RF power and spectrum footprint asymmetries. CTI could be avoided by sophisticated communication protocols that are sensitive to instantaneous spectrum occupation. However, low-cost hardware and limited energy-budget of the nodes make the typical spectrum sensing techniques as proposed for non resource constrained systems [83] unsuitable for LPWN.

Mitigation of interference through dynamic spectrum access and opportunistic channel selection is not new in the LPWN literature. These approaches improve communication performance and energy efficiency [84–86].

Several works have investigated lightweight mechanisms for quantifying interference based on the features of existing IEEE-802.15.4 radios, such as energy detection. Musaloiou et al. [87] presented interference estimators that can be implemented using off-the-shelf radios and outlined distributed algorithms to dynamically switch frequency.

Several multichannel protocols have been proposed to maximize protocol performance in the last years [88–91]. Sharing the idea of exploiting opportunistic channel selection, we design our channel quality metric for resource-constrained wireless devices that can help systematise channel selection in such multichannel protocols.

Ansari and Mähönen [92] described the design challenges for the dynamic selection of an interference-free channel in wireless sensor networks, and described a lightweight channel selection strategy. Differently from their work, we exploit energy detection to quantify the channel quality by measuring the availability of the channel over time.

This chapter embeds the following contributions:

- A novel channel quality metric that is based on channel availability and is agnostic to the interference source.

- An analysis of the parameter space and validation of the metric's performance with real-world interference traces.

This chapter is organized as follows. Section 3.2 provides further motivation for this work and in Section 3.3 we derive the expression for our `CQ` metric. Section 3.4 describes how we use the *energy detection* (ED) feature in IEEE-802.15.4 compliant radios to measure the evolution of signal (interference) strength in 802.15.4 channels, our experimental setup and our data collection experiments. We then discuss results of our evaluations and conclude the chapter in Section 5.4.

3.2 Motivation

Any given network configuration at deployment phase, like radio channel selection, is typically not enough as the network may experience communication interruptions or simply fails at some point. We need LPWN that seamlessly adapt resources and self-organize to maintain their integrity in a changing environment. Several recent studies have addressed burstiness and interference in wireless links. Srinivasan et al. proposed a metric to quantify link burstiness and show impact on protocol performance and achievable improvements in transmission cost [93]. Also, Munir et al. investigated scheduling algorithms to improve reliability and provide latency bounds [94]. However, these solutions can not react to instantaneous changes in the channel condition. They rather select routes and channels using long-term observations.

There are aggressive techniques to deal with interference in wireless systems. Successive Interference Cancellation (SIC) has been partially demonstrated for 802.15.4 in Software Defined Radios [95]. Nevertheless, there are practical limitations to further advance with it. For example, it is known that SIC requires highly linear amplifiers in the receiver (large dynamic range) and also excellent adjacent channel suppression, because residual energy put in the front-end causes it to underperform and desensitizes the radio. Both of these requirements lead to expensive solutions. Furthermore, it is questionable whether SIC's demand for signal processing could outweigh its benefits compared to other approaches, in view of available technology, inexpensive hardware and energy budget constrains. Finally, these ideas are not trivially applied to CTI because a large heterogeneous set of possible signals to disentangle further complicate SIC-based solutions.

Alternatively, we advocate that modest improvements in low-power receiver architecture can enable energy efficient spectrum sensing, which is necessary for nodes to form smart reactive networks that eliminate the need for highly complex radios. Spectrum occupation can change rapidly in time and space, yet under unfavourable channel conditions nodes adapt resources or find better channels to maintain communications. Dynamic resource adaptation can lower latency bounds and boost reliability, but in order to encompass this information into protocols one needs accurate spectrum sensing. We show that sufficiently accurate spectrum sensing is feasible with sensor nodes.

Currently, the radio transceivers in WSN nodes are mostly based on the IEEE-802.15.4 standard that is intended for low-power operation. On reception, off-the-shelf radios require around 50 mW and consume 200 – 2000 μJ per packet received. This power is drawn by the PLL synthesizer, digital demodulator, symbol decoder and RF analog blocks for signal filtering, amplification and down-conversion among other functions, typically in this order. Recent incursions in 0.18 μm CMOS process of PLL realizations [96–99], targeted for these systems, report fairly appealing figures: power consumptions below 3 mW and lock-in times smaller than 30 μs. Since the PLL synthesizer is known to be by far the most power-hungry block in the receiver, these results suggest that the next generations of LPWN radios will require, at least, one order of magnitude less chip energy per bit received.

Now, in order to support energy detection (ED) spectrum sensing, only the PLL synthesizer, analog RF blocks and AGC are necessary, while the demodulator can be turned off. Interestingly, among other optimizations, this further reduces energy consumption while the receiver is used exclusively to detect the RF energy in the channel, but we have not yet found any 802.15.4 radio chip providing this flexibility. Moreoever, ED tolerates higher phase noise from the PLL than narrow band demodulation does, which also relax the design constrains and the PLL power consumption.

3.3 Channel Quality Metric

The sources of interference in wireless networks are typically very diverse. Interference causes a decrease in the Signal-to-Noise plus Interference Ratio (SNIR) which can result in packet losses. Any device that produces RF signals with spectral components within or near the receiver passband is a potential interferer. Average energy in a channel has been used as an indicator of channel usage in the literature [86, 87, 92, 100]. Unfortunately, this metric is unable to distinguish between a channel where the traffic is bursty with large inactive periods and a channel that has very high frequency periodic traffic with the same energy profile. Clearly, the first scenario is preferable. It may well be the case that the traffic in the second case consists entirely of short-duration peaks resulting in much lower average energy but unusable channel. Motivated by this observation, we propose a metric that is based on the fine-grained availability of the channel over time and ranks in a more favourable way channels with larger inactive periods or vacancies.

Let P be channel energy sampling period and let R_{THR} be the energy threshold below which we define the channel to be idle. In our experiments, we chose R_{THR} to be the energy level required for correct decoding of packets specified by the SINR model. Therefore, the channel can be considered idle when $RSSI < R_{\text{THR}}$. For example, Figure 3.1 shows RSSI samples over time along with idle intervals, which we refer to as *channel vacancies* (CV). Let m_j denote the number of j consecutive samples where the channel was idle, which represents the duration of CV. For example, in a sample "100001001001" where 0 indicates idle channel state and 1 indicates measured energy to be larger than the threshold, $m_2 = 2, m_3 = 0$, and $m_4 = 1$. Thus, if n denotes the total number of samples, then $m_1 + m_2 + \ldots + m_n = m$ is the total number of observed CV. Notice that j consecutive clear channel samples imply that the channel was idle for at least $(j-1)P$ time units. We define the average *Channel Availability* (CA) as:

$$CA(\tau) = \frac{1}{n-1} \sum_{j|(j-1)P>\tau} jm_j \tag{3.1}$$

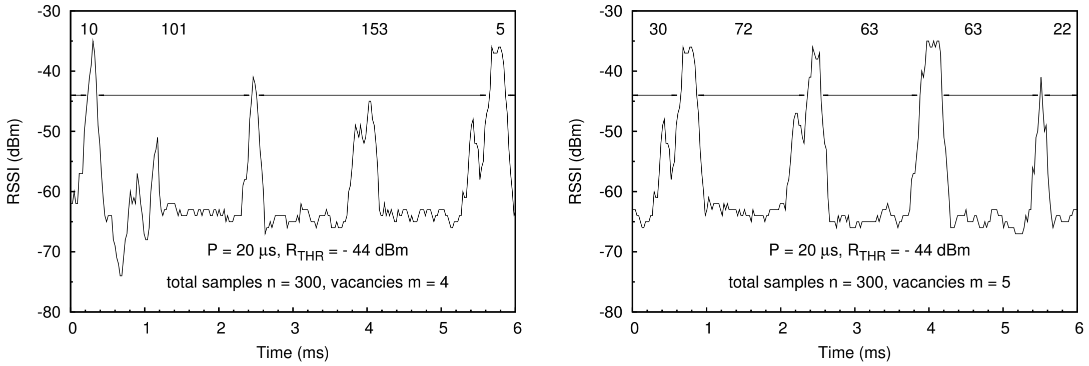
where $\tau > 2P$ is the time window of interest, which could be the duration of packets. As we argued earlier, a channel where $m_{2j} = k$ is more desirable than a channel where $m_j = 2k$, although jm_j is the same for both cases. Therefore, we want to rank a channel with larger vacancies higher even though the sum of the idle durations might be the same. Hence, we define the *Channel Quality* metric as:

$$CQ(\tau) = \frac{1}{(n-1)} \sum_{j|(j-1)P>\tau} j^{(1+\beta)} m_j \tag{3.2}$$

where $\beta > 0$ is the bias.

`CQ` in equation (3.2) take values between 0 and n^β, where the larger values indicate better channels. Observe that this expression is agnostic to the interference source.

Figure 3.1 shows the amount of channel vacancies in two scenarios with a similar channel availability ($CA_a = 0.88$ and $CA_b = 0.83$) computed with a $R_{\text{THR}} = -44$ dBm. Due to collisions, the probability of correct reception is higher in the scenario shown in Figure 3.1a than in the one depicted in Figure 3.1b.



(A) Scenario 1

(B) Scenario 2

FIGURE 3.1: Channel vacancies: two scenarios with the similar channel availability (CA).

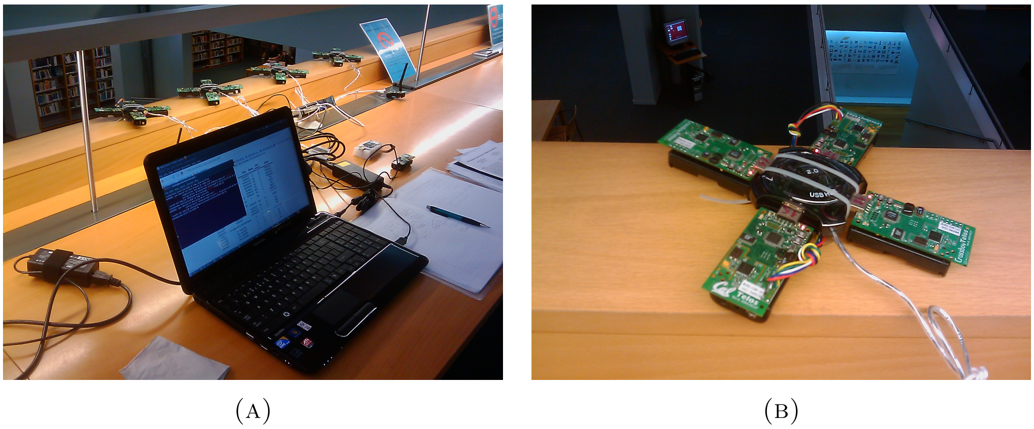
3.4 Evaluation

In this section, we first describe our experimental set-up used for data collection followed by an analysis of our metric when applied to the data. We devise off-line experiments and implement them in Python [101] scripts to be run over the traces. This has the advantage of producing a naturally controlled environment, e.g. isolating channel effects that are present in an online experiment. We show that our metric `CQ` is highly correlated with Packet Reception Rate (PRR).

3.4.1 Experimental Setup

In order to experimentally investigate our proposal we need traces of interference signals that help understand channel degradation in real-world settings. More specifically, we want to find out how our metric can help identifying a usable channel and eventually establish which alternative techniques can be applied to employ it effectively. Therefore, we have designed an experimental setup to study interference in the 2.4 GHz ISM band. This band is available globally; there are thousands of certified devices on the market that operate in it and coexistence problems are well known [79, 80], which ultimately facilitates the task of collecting interference traces. Our setup has no limitations to study any kind of interference, but given that Wi-Fi has been identified as the most critical interference source to affect LPWN [80] and it is also widely available, we report experiments with traces where interference stems solely from Wi-Fi networks.

In our setup, we employ a set of 17 TelosB sensor nodes to scan all sixteen IEEE-802.15.4 channels simultaneously. Having one node per channel enables us to increase the pace at which data is collected and makes the logging operation easier. In order to do simultaneous channel readings, we use one of the motes to transmit a scanning beacon



(a) (b)

Figure 3.2: The experimental setup used to collect energy level traces on IEEE-802.15.4 channels deployed at the Library of the Faculty of Engineering at the University of Porto (a) and detail of TelosB motes arranged in a USB hub (b)

on channel 26, which instructs all other nodes to switch to their respectively assigned channels and begin scanning. The motes are connected via USB hubs to a laptop as shown in Figure 3.2. We sample the RSSI from the CC2420 transceiver at 40 kS/s [43], and store the data in a memory buffer. After completing 5600 samples in approximately 130 ms, i.e., the largest possible amount of samples that can be stored in the limited memory of TelosB nodes, all nodes return to listen on channel 26 and wait for the next scanning beacon. Scanning beacons are sent every 8 seconds, which guarantees enough time to dump all the RSSI readings to a file.

A large density of Wi-Fi Access Points capable of producing notorious spectrum occupation is mainstream in many metropolitan areas today and particularly in university campus. However, it is the density of users and the overall volume of data been transferred that actually produces congestion and interference. Thus, we used our ensemble to collect measurements in our laboratory, which has moderate traffic on a few 802.15.4 channels. Then we conducted a measurement campaign at the Library of the Faculty of Engineering of the University of Porto, where we found very heavy traffic from 802.11 Wi-Fi networks. In our experiments, signals are well above the noise floor (10 - 70 dB), but more relevant is the time distribution of burst patterns that varies from a few microseconds to tens of milliseconds. To examine our metric proposal we then perform off-line experiments, upon a set of traces from a four hour capture.

3.4.2 Sampling Time

One of the questions we seek to answer is *how long* should we sample a channel in order to have a meaningful `CQ` value. Sampling too shortly leads to uncertainty about the near future state of the channel. Notice that the *clear channel assessment* (CCA) used in the

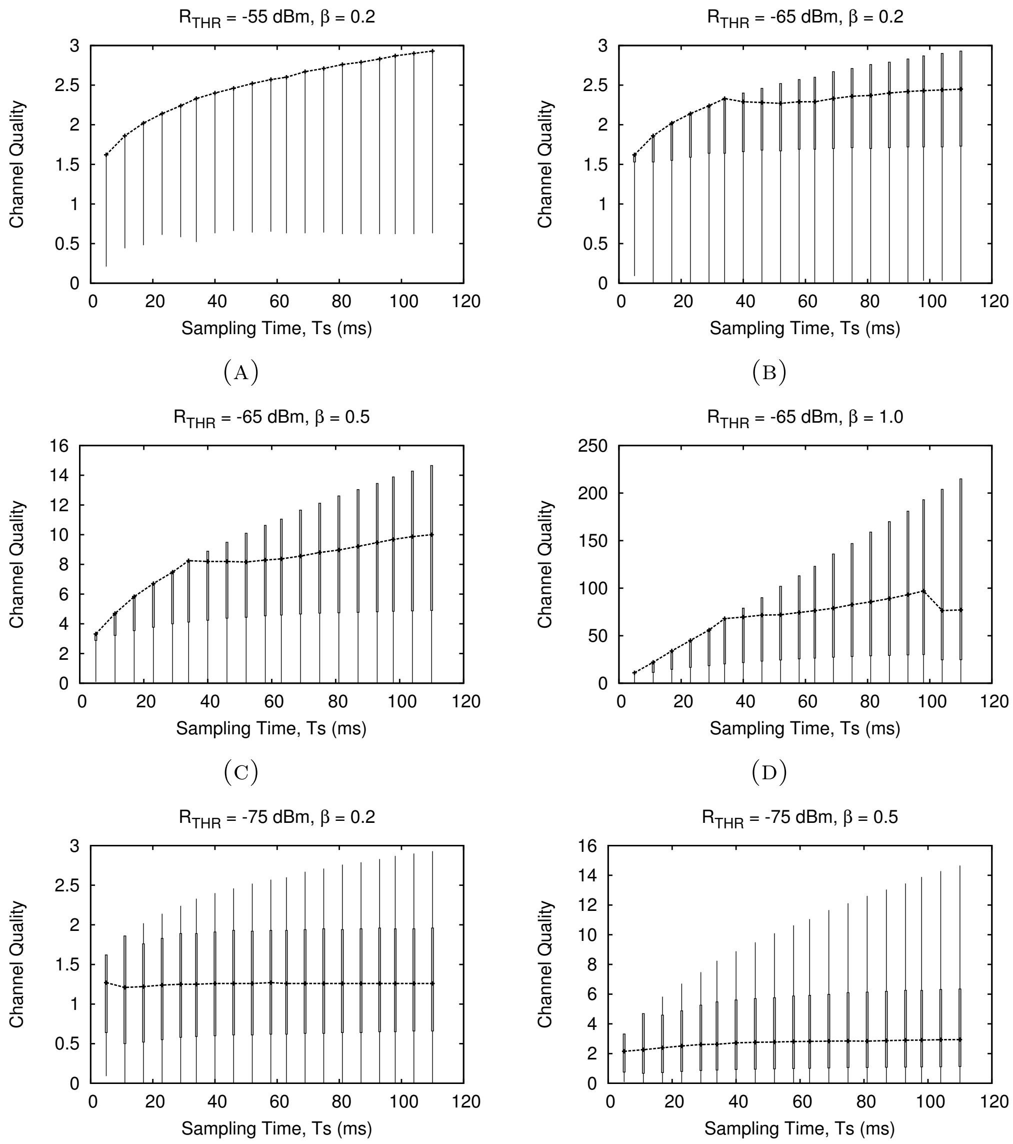
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism would not help here given the asymmetric scenario in transmission power and spectral footprint [82]. Basically, such asymmetries in the PHY layer among different radios, make the distributed coordination approach fail. LPWN nodes employ orders of magnitude less RF power than other channel contenders, which makes them more vulnerable to packet corruption since it is improbable that other nodes detect an ongoing transmission and thus defer theirs. For this reason, it is necessary to sample for longer periods, definitely larger than a CCA accounting for 8 symbol periods or 128 μs, in order to capture a sequence of events large enough to estimate the probability of successful packet reception.

On the other extreme, sampling too long introduces a cumulative effect that misses the dynamics of the channel availability and leads to poor prediction of the next state of the channel. The more distant in time the events are the more likely is that their probabilities are independent and therefore does not help to estimate the channel condition either. Furthermore, during the sampling period the radio is turned on, which consumes energy.

In practice, this means that we need to find a compromise for the sampling time that is intrinsically dependent on the system observed. In order to understand this compromise, we progressively compute the `CQ`, from 128 μs up to 120 ms, over all traces. Figure 3.3 illustrates the results. The R_{THR} threshold value is primarily chosen based on the RSSI levels of packets from other nodes we are interested in receiving.

Actually there is an SNIR margin—specific for each radio and related to the *Co-Channel Rejection Ratio* (CoCRR)—which needs to be considered here. In the CC2420 radio, this value corresponds to 3 dB for a target $PER = 10^{-3}$, and must be accounted to fine-tune R_{THR}.

Since we are not interested here in any specific packet duration, we choose $\tau = 0.2$ ms, small enough so that most CV contributions count in equation 3.2. Notice that the sum is computed over CV larger than τ only. For practical reasons, we perform data binning on all CV observations, i.e., all values which fall in a small interval, $t_{bin} = 0.5$ ms, are represented by the same value. This quantization affects the absolute values obtained in equation 3.2. Suppose an empty channel with one single vacancy of length $j = n - 1$. As mentioned in Section 3.4.1, we are sampling at approximately 40 kS/s, i.e., we take one RSSI sample every 25 μs. Therefore, we divide j by a factor $k = 20$ and thus, $CQ < ({}^{j}/_{k})^{\beta}$. This curve is the upper bound for absolute values shown in all graphs in Figure 3.3. Similarly, the values represented in the abscissas are divided by 40 to obtain the corresponding scanning time in milliseconds.



(A) (B)

(C) (D)

(E) (F)

FIGURE 3.3: CQ computed over all traces for different sampling times. Curves represent the median, boxes represent the interquartile range (IQR), and bars stand for the rest of the values.

One common trend in all graphs is that CQ stabilizes after some time, provided there is sufficient interference. This indicates that equation 3.2 converges toward a value that is proportional to an average number of vacancies during the sampling period and, clearly, also depends on β and the values of j.

Figure 3.3 shows that for lower R_{THR} values, which corresponds to heavier interference, the median of CQ stabilizes faster. On the contrary, if the channel is mostly idle, CQ grows with very high probability (e.g., if $R_{\text{THR}} = -55$ dBm as in 3.3a, CQ grows as $(2 \cdot T_s)^{0.2}$ and the IQR shrinks over the maximum). An intermediate case, as when CQ is computed for -65 dBm, see 3.3b-3.3d, demonstrates that the metric typically grows to a certain value until it finally stabilizes. Hence, these sampling times are much smaller than the timescale of the interference pattern present in the channel. Based on this behaviour, an optimum sampling time would be as long as it is necessary to have the median of `CQ` stabilized.

In a system where this metric is computed online the sampling time, represented by n in equation 3.2, could be dynamically maintained at this turning point where the median of `CQ` stabilizes, or below a certain maximum value. We defer the development of a control algorithm for this purpose to future work. For the rest of our experiments, we use a hand-picked scanning time of 40 ms.

3.4.3 Correlation with PRR

Packet Reception Rate (PRR) is a well known reliability metric. When PRR is high, the wireless channel and the link are good. However, PRR reflects all forms of signal distortion in the wireless channel combined, including interference. Thus, a medium or low PRR does not provide enough information to identify which factors are responsible for poor performance. Yet intermediate quality links, that display a medium PRR, may account for up to 50% of all links observed in LPWN testbeds [93]. Moreover, PRR and other useful metrics, such as packet's RSSI and LQI, require packet transmissions. Instead, our `CQ` metric specifically accounts for interference and has no side effect on the channel, as it relies exclusively on the receiver channel energy detection, and therefore scales with node density and channel usage.

We now investigate how the channel availability as described by our `CQ` metric is related to the probability of successful packet receptions. For this experiment we use a third of each RSSI trace, lasting 130 ms, to compute the metric and the remaining to check for the presence of interference that may lead to packet corruption. If the energy levels in the channel remain 3 dB below the RSSI of packets (CoCRR mentioned in 3.4.2), during the duration of each packet, then the packet is considered successfully received.

Multiple packets are transmitted over each trace and the average is computed to derive the PRR. Packets are transmitted periodically and transmissions are separated by an inter-packet interval time (IPI) of 2 ms. In this way, we conduct an experiment with more than 240.000 off-line packet verifications on traces obtained from the deployment at the library.

As shown in the previous section, equation 3.2 provides a range for `CQ` values that depends on n and β. However, in order to compare among `CQ` values computed with different parameter values we rewrite `CQ` as:

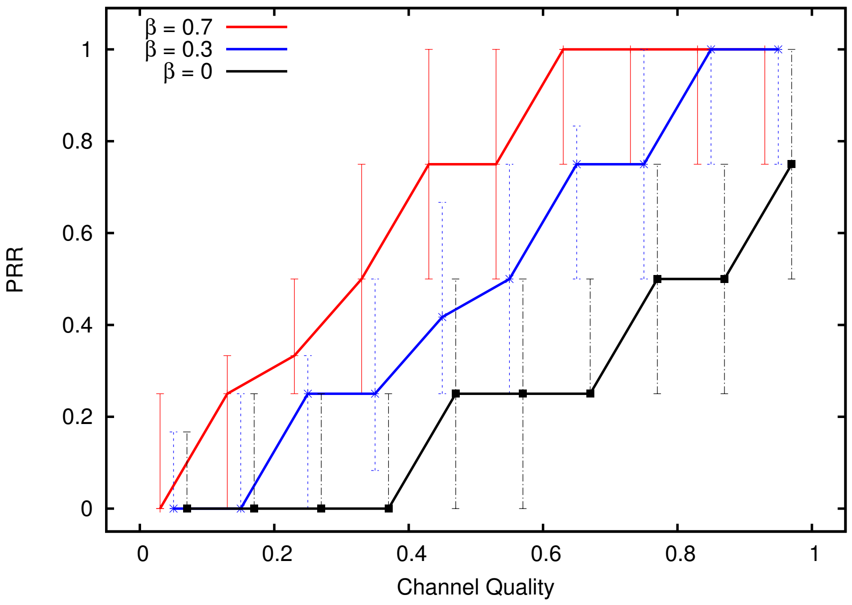


FIGURE 3.4: Dependecy of the Packet Reception Rate (PRR) and the Channel Quality (CQ) computed according to equation 3.3. This graph is obtained from over 240000 trials, using 12 packets of 5 ms in each RSSI trace. The widest range of useful CQ values is obtained for $\beta = 0.3$.

$$CQ(\tau) = \frac{1}{(n-1)^{(1+\beta)}} \sum_{j|(j-1)P>\tau} j^{(1+\beta)} m_j, \tag{3.3}$$

CQ in equation (3.3) now take values between 0 and 1, regardless of n and β values. For example, if we compute equation 3.3 with $\beta = 0.3$ for an IEEE-802.15.4 ACK frame lasting 352 μs, in the scenarios shown in Figure 3.1, we obtain $CQ_a = 0.65$ and $CQ_b = 0.50$. The difference between CQ_a and CQ_b is three times higher than the difference between CA_a and CA_b (obtained using equation 3.1 in Section 3.3), and it therefore highlights the difference in quality between the two channels.

Figure 3.4 shows the correlation between CQ and PRR. The curves correspond to the CQ median and the error bars represent the interquartile range computed over the entire set of traces, at $R_{\text{THR}} = -65$ dBm. We compute CQ for bias (β) values 0, 0.3, and 0.7 to highlight that $\beta = 0.3$ linearises the curves and better expand useful range of CQ values.

Higher values of β increase the weight of larger CV in the definition of the CQ. Therefore, having $\beta = 0.7$ will promote the selection of channels with larger CV. On the other hand, observe how for $\beta = 0$, which is equivalent to compute the average channel availability as described by equation 3.1, CQ values increase up to 0.4 but almost no packets are received, since vacancies are not large enough. In this case, CQ values grow faster than PRR which indicates that average channel availability does not capture well-enough the complexity of the channel, as we discussed in Section 3.3. Being able to tune β, as shown in the graph in Figure 3.4, helps us in maximizing the correlation among PRR and CQ. This makes our metric an accurate indicator of the channel condition, which is an interesting result. In our experiments, we find the β value that maximises the correlation among CQ and PRR to be approximately $\beta = 0.3$. Similar to the scanning time, finding the optimum β value, for an arbitrary interference scenario, is outside the scope of this work.

3.5 Summary

We introduced a new channel quality metric that is based on the availability of the channel over time. The metric is useful for interference aware protocols in LPWN. We described our experimental setup for collecting real-world interference traces in the 2.4 GHz ISM band. Using this data, we showed that our metric has strong correlation with PRR. Thus, our metric's characterization of a channel is reliable and applicable in practice. We also discussed dynamic resource allocation techniques for interference-aware protocols in WSN for which our metric can prove to be useful.

Chapter 4

Radio Resource Adaptation

In wireless networks that operate in those bands where spectrum sharing occurs across a variety of wireless technologies, such as the license-free Industrial Scientific and Medical (ISM) bands, mitigating interference becomes challenging. Addressing interference is an important aspect for the design and development of solutions intended to satisfy the demands of applications requiring QoS guarantees. In this chapter, we investigate dynamic radio resource adaptation techniques based on instantaneous spectrum usage. Using the `CQ` metric proposed in this thesis to quantify the spectrum usage, we address packet size and error correction code overhead optimisations. We also discuss interference-dependent dynamic adjustment of the correction capacity of erasure codes. The work included in this chapter was partially documented in the following conference publication [46].

4.1 Introduction

Radio resource managment and adaptation techniques are neither new in the LPWN literature. Such techniques considered in LPWN include channel frequency, trasmission power, packet size and code-rate for error correcting schemes. In this section we revisit the state of the art in resource adaptation techniques and discuss how they could be dynamically applied to leverage our `CQ` metric for interference-aware communication protocols.

Chowdhury and Akyildiz [102] presented algorithms that classify interferers and adapt transmission channels, packet scheduling times, and sleep-awake cycles accordingly. Penna et al. [100], investigated the interference detection capabilities of an IEEE 802.15.4 device in presence of Bluetooth and IEEE 802.11b/g interference and proposed a spectrum sensing strategy able to detect and discriminate different traffic conditions.

Hermans et al. [103] classify the interference source based on corrupted packets in order to use appropriate mitigating strategies. Boers et al. [104] study signal strength traces for high-level classification of interference patterns exploying decision tree classifiers, dip statistics and Lomb periodogram, adapted for constrained devices.

We share the idea of using dynamic spectrum access and opportunistic channel selection to mitigate interference, but our work is distinctly different in two aspects: (i) our `CQ` metric ranks the channel based on consecutive vacancies and is inherently agnostic to the interference source, and (ii) we go beyond the simpler goal of choosing channels and consider the alternative of actually using channels in the presence of interference.

Vuran and Akyildiz present a cross-layer solution for packet size optimization considering multi-hop routing and error control techniques [105]. They conclude that the increase in payload length decreases the MAC failure rate. In contrast, we study a point-to-point link scenario considering the overhead of packet headers and collisions due to external interference using real-world measurement data.

Huang et al. study self-similarity of Wi-Fi *white spaces*, propose a Pareto model characterize them and a control mechanism to fragment IEEE 802.15.4 frames [106]. We share the goal of adapting to the channel condition but computing `CQ` solely relies on channel energy detection by the receiver and does not require any packet transmissions. Therefore, it scales with node density and channel usage. Also, when the overhead of 6LoWPAN headers is considered, fragmented packets below 127 bytes are not energy-efficient as we demostrate in this chapter.

Hong et al. present mote-in-the-loop, an approach to optimize communication strategies such as packet size and retransmission schemes [107]. They superimpose replayed interference traces on normal communication to study the effect of interference and optimize communication strategies accordingly. Their off-line approach is orthogonal to our on-line approach. However, they can be combined by using mote-in-the-loop to determine the initial configuration and our `CQ`-based method to fine-tune the parameters online.

Sankarasubramaniam et al. [108] addressed the problem of finding the optimal packet size for data communication in a single-hop scenario with error control techniques. They use a channel model that uses the log-distance path loss model and Rayleigh fading but do not consider interference. We share their goal, but we explore the effect of packet size optimizations based on the knowledge of the channel quality as computed by our `CQ` metric.

Lin et al. demonstrated a novel pairwise transmission power control for LPWN that performs significantly better than node-level or network-level power control methods [109]. They improve PRR and energy consumption by dynamically adapting the RF transmission power to maintain the minimum level required to guarantee a good link. This approach compensate for pathloss variability but does not account for two important aspects: (i) the irreducible error floor [1, Section 6.3] produced by fading can not be removed by increasing transmission power, and (ii) it does not address external interference. A solution to both these problems is to employ additional resource adaptations, simultaneously.

FEC techniques pose a trade-off between data recovery capacity and its inherent payload and computation overhead. Liang et al. demonstrate that Reed-Solomon (RS) correcting codes performs well while recovering packets affected by 802.11 interfering signals [82]. Since interference levels may vary extensively it is interesting to see if this solution can benefit from simple `CQ`-based optimizations.

In this chapter, we explore how low-power communication protocols can benefit by dynamically adapting radio resources, based on the channel condition as quantified by a `Channel Quality` (`CQ`) metric, which we introduced in Section 3.3. Our experiments show that the packet size and erasure code optimizations provide greater energy efficiency and reliability than fragmentation and reassembly of 6LoWPAN packets. Erasure codes provide significant SINR gain margin which allows a receiver to effectively decode packets transmitted at lower power levels, well under the threshold imposed by interfering signals from the IEEE 802.11 networks (when no erasure code is used). This "equivalent SINR gain" favours spatial re-usability of the frequency and/or time slots within the low-power wireless network and increases the *practical* margin for adjustments of the transmission power.

Recent LPWN platforms with greater computation capacity provide powerful computing capabilities while maintaining low energy consumption akin to older (low-end) platforms [110, 111]. These resource-rich platforms have increased processing capabilities which make erasure code handling viable and efficient [111]. Moreover, improved radio designs [32] facilitate better spectrum sensing as well as provide hardware support for fast packet framing and assembly.

This chapter presents the following contributions:

- We provide experimental evidence that enlarging the payload of the IEEE 802.15.4 packets up to 500 bytes leads to higher energy-efficiency and higher throughput under moderate or low CTI. This finding is significant for communications among heterogeneous networks, for example, sending IPv6 packets over IEEE 802.15.4 PANs that are currently addressed in the 6LoWPAN standard.

- We provide experimental evidence that erasure codes capable of correcting 10% of the packet payload can provide an equivalent SINR gain of 25 dB with probability greater than 0.6 under heavy CTI conditions. The same erasure code increases the optimal payload sizes and boosts throughput up-to five times for a wide range of channel conditions. Furthermore, using erasure codes reduces the uncertainty in the energy cost of packet transmissions, which simplifies dynamic packet size adaptations.
- We propose a systematic approach for implementing dynamic radio resource adaptation based on wireless channel quality.

The rest of this chapter is organized as follows. Section 4.2 describes the metrics and the experimental data used. Section 4.3 presents experimental results and discusses interference dependent packet size optimizations. Section 4.4 deals with erasure code usage and code-rate optimizations. We conclude with Section 4.5.

4.2 Preliminaries

In the absence of interference, the Bit Error Rate (BER) at the Physical (PHY) layer is primarily determined by the Signal to Noise Ratio (SNR), the channel condition and the modulation scheme employed. If the bit errors are i.i.d., the Packet Error Rate (PER) can be expressed as a function of the BER and the size of the packet, namely $PER = 1 - (1 - BER)^l$, where l represents the number of bits in the packet. Yet, this PER value can be reduced with spread spectrum techniques [112].

We compute the SNR required to maintain $PER = 10^{-2}$, under *Additive White Gaussian Noise* (AWGN) and *Rayleigh* fading channel models, for three packet sizes. Table 4.1 shows the results. The largest packets (1260 B) require additional gains of 0.9 and 2.0 dB respectively, over the short ones (127 B). Note that such link margins are attained by increasing the transmission power but without changing the total chip power significantly. We chose $PER = 10^{-2}$ because this value is sufficiently small to neglect packet losses due to noise and fading. In the following, we present a simple model based on

Payload Size	127 B	512 B	1260 B
SNR (dB) *AWGN*	*1.1*	*1.7*	*2.0*
SNR (dB) *Rayleigh*	*5.9*	*7.1*	*7.9*

Table 4.1: Longer packets require larger SNR to maintain $PER = 10^{-2}$. Theoretical SNR values are computed for *AWGN* and *Rayleigh* fading channel models, using the IEEE 802.15.4 PHY parameters. We use packets larger than the maximum packet size defined by the standard to find the link budget necessary to compensate for PER.

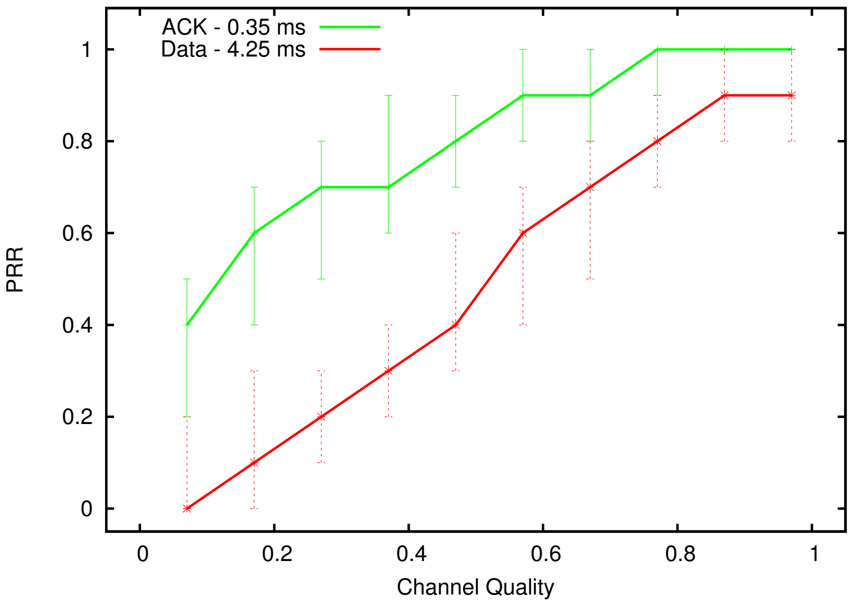


FIGURE 4.1: Correlation of channel quality indicated by CQ with PRR. Vertical bars represent the inter-quartile range (IQR).

Packet Reception Rate (PRR, defined as 1 - PER) statistics to estimate energy-per-useful-bit and link throughput. Our model accounts for packet losses due to collisions in a point-to-point link, where transmitters do not use any contention resolution.

4.2.1 Channel Quality (CQ) Metric

We quantify the wireless channel quality with the CQ metric [113], defined as in equation 3.3. Where $\beta > 0$ is a bias parameter that gives (polynomially) larger weights to longer channel vacancies and $\tau > 2P$ is the time-scale of interest, which can be the duration of packet transmission. CQ takes values in the range $[0, 1]$, where larger values indicate better channel quality. Moreover, as discussed in Chapter 3, this metric exhibits strong correlation with PRR. Nevertheless, CQ differs from PRR in that it only accounts for interference and does not consider packet transmissions. Because CQ relies on the receiver channel energy detection, it scales well with node density and channel usage.

On channel energy traces collected by a sensor network deployed in a library building [114], CQ exhibits a strong correlation with PRR shown in Figure 4.1. In this figure, for the same channel quality, the PRR is higher for the shorter ACK frames than for 100-byte data frames. Observe that lower energy thresholds, E_{THR}, tend to produce lower CQ values and vice versa. Further details can be found in [113].

4.2.2 Utility Metrics

The energy-per-useful-bit [115] is a key metric for low-power radios and our objective is to minimize it. Although sensor networks typically operate at relatively low data rates, throughput is often an issue. This issue arises, for example, in order to provide QoS to bursty traffic. Even with very low data rates, the throughput requirement for convergecasts in the neighborhood of a sink node tends to remain high. Interference affects throughput adversely, and its impact on end-to-end performance metrics usually increases with increasing hop-count.

We now define total energy-per-useful-bit and throughput, adapted from the literature. Let E_p denote the minimum total energy required to transfer a packet over the channel, PL denote the size of the packet's payload and L_p denote the latency of packets, which accounts for packet transmission time plus the inter-packet interval (IPI).

Definition 1. Energy-per-useful-bit:

$$E_{bit} = \frac{E_p}{PL \cdot PRR}. \tag{4.1}$$

Definition 2. Packet throughput:

$$U_{put} = \frac{PL \cdot PRR}{L_p}. \tag{4.2}$$

Our total energy-per-useful-bit differs from that in [115] in that we refer to useful bits as those in the data payload, excluding the ones in protocol headers, in order to capture the protocol overhead as well. We estimated E_p based on 80 mW target power, which includes chip power for both receiver and transmitter modules [60].

4.2.3 Measurement Data

In this study, we base our analysis on channel energy measurements collected by a LPWN deployed in a library building [114]. The network passively monitored all sixteen IEEE 802.15.4 channels, with a sampling period of 23 μs. These traces contain continuous sampling segments of 130 ms, spaced by intervals of around 8 s. The major (and perhaps the only) users of the channels were several IEEE 802.11 based Wi-Fi networks under normal operation. Over 500 MAC addresses were registered in two measuring campaigns which were carried out in two different days, with a duration of 3 and 4 hours, respectively. Detailed description of the traces as well as code for experiments in this chapter are available online [114].

The duration of packets in IEEE 802.15.4 based sensor networks is $512 - 4256$ μs and they can accommodate a maximum payload of 127 octets [6]; the corresponding duration in the IEEE 802.11 based networks is $202 - 1,906$ μs and $194 - 542$ μs for the versions IEEE 802.11b and IEEE 802.11g, respectively [116]. The transmission power employed by the IEEE 802.11 nodes is typically two orders of magnitude larger than the IEEE 802.15.4 node platforms. It is known that such high power signals affect sensornode receivers by producing erasures scattered across a frame, significant enough to corrupt the frames received [117]. Erasure codes allow recovery of corrupted frames while keeping the required transmission power in sensornodes low. The commodity IEEE 802.11 equipment is also affected by certain patterns of weak and narrow-band interference produced by low-power node transmissions [118]. Therefore, usage of erasure codes in LPWN nodes, which allows to keep the transmission power low, improves coexistence, also benefiting the IEEE 802.11-based networks.

4.3 Packet Size Optimisation

Various studies have shown that packet size has a significant influence on the packet reception rate [105, 108, 119]. Shorter packets are less likely to experience collisions (consequently reducing retransmissions); however, shorter packets also imply higher overheads, e.g., due to packet headers.

4.3.1 Short vs. Large Packets

The PRR comparison of ACK and data frames obtained from over 1.20×10^5 packet transmissions, shown in Figure 4.1, illustrates a clearly increasing gap among the curves, as `CQ` diminishes. This gap stems from the ACK and data frame duration, i.e., 352 μs and 4.256 ms, respectively. It confirms that on average, larger data frames undergo more frequent collisions. Observe the ordinates represent the median of PRR values corresponding to a `CQ` interval. This `CQ` quantisation is responsible for the 10% packet losses observed for $CQ = 0.95$, centred in the interval]0.9, 1.0]. We choose `CQ` sampling time of 50 ms corresponding to $n = 2170$ samples, $\beta = 0.3$, $\tau = 5$ ms and $R_{\text{THR}} = -65$ dBm. This value of R_{THR} produces a balanced distribution of `CQ` values across our trace set. We maintain these parameter values for all experiments, with the exception of τ.

Due to the trade-offs mentioned earlier, it is expected that for a given interference level, a certain packet size maximizes the throughput and minimizes the total energy-per-useful-bit. To investigate this, we conducted off-line experiments to compute the utility metrics introduced in Section 4.2.2.

4.3.2 Payload Size Optimisation Experiment

The IEEE 802.15.4 data frame contains a 6-byte PHY header and a 23-byte MAC header that includes an address field, followed by a payload of up to 102 bytes, and a 2-byte frame control sequence in the trailer [6]. Together, these headers account for around 25% of the maximum specified packet size. At a data rate of 250 kbps and 4 bits per symbol, as is commonly used in the IEEE 802.15.4-compliant radios operating in the 2.4 GHz band, each byte takes 32 μs in the air. Thus, the PHY layer header lasts 192 μs and a MAC header lasts from 224 to 736 μs, depending on the address format. After the payload, the trailer lasts 64 μs. In this experiment, we used a header duration of 1024 μs, in order to analyse implications for 6LowPANs. This extended header accounts for 22 bytes of 802.15.4 PHY-MAC, including 64-byte addresses, and 10 bytes of compressed 6LowPAN header.

In this study, we explore our objective functions for packets with payloads in the range 1 to 1500 bytes, with varying channel quality quantified by `CQ`. Table 4.2 lists the payload sizes and the corresponding number of packets used per trace. In order to avoid fragmentation of packets whose size is larger than 127 bytes, the IEEE 802.15.4 standard requires increasing the 7-bit PHY frame length field by another 4 bits.

When actual data is transmitted over the channel, often an error control technique such as Automatic Repeat reQuest (*ARQ*) manages retransmissions of corrupted packets. In these off-line experiments, PRR accounts for the cost of retransmissions of packets with any single symbol altered due to interference. We refer to them as *ARQ only* to distinguish from those in which error correction is combined with *ARQ*.

4.3.3 Experiment Results

Using the measurement data described in the previous section, we computed the PRR by checking whether collisions can occur due to the interference level exceeding the SINR threshold during a packet transmission. The outcome for same packet size, over traces whose `CQ` values fall within the same bin (bin-width = 0.1), are aggregated to compute the corresponding PRR value. This PRR value is then used in Equations 4.1 and 4.2.

Packet Payload	NoP
$\leq$ 300 *bytes*	*7*
500 bytes	*5*
1000 bytes	*3*
1500 bytes	*2*

TABLE 4.2: Payload sizes and number of packets (NoP) used per trace

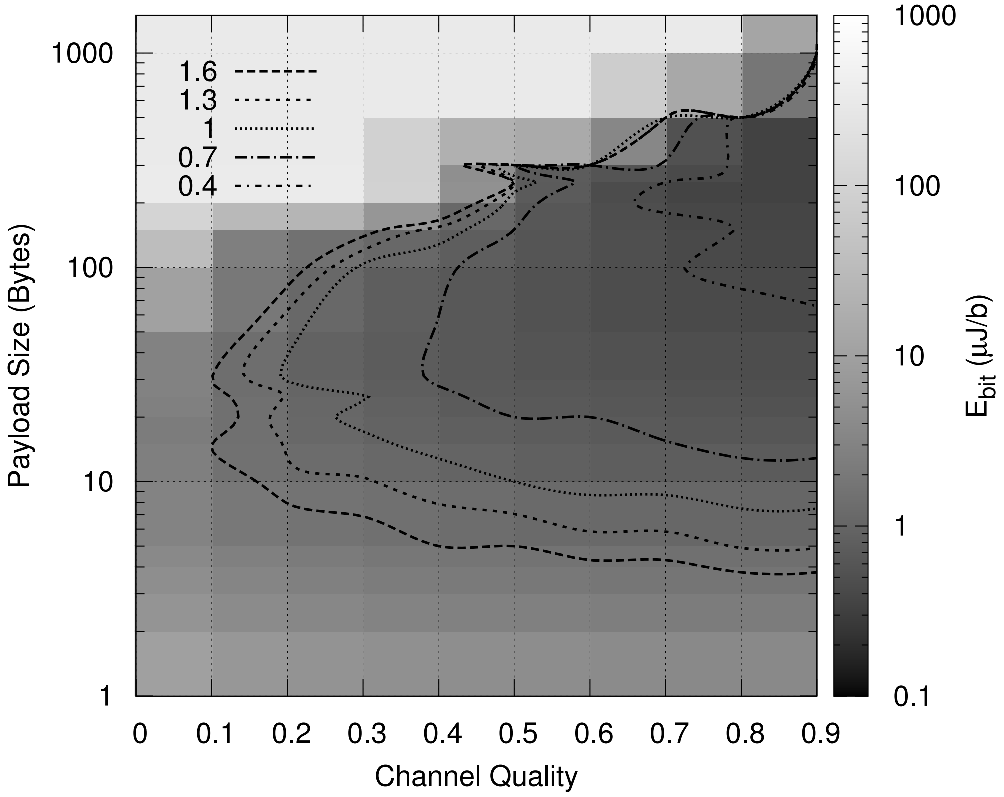


FIGURE 4.2: Effects of packet size on energy-per-useful-bit E_{bit}, defined in Eq. 4.1. Outside the isogram the energy grows abruptly, specially on the upper side due to the higher number of collisions. The contour lines converge for large packet sizes and good channel qualities, i.e., in the upper right corner. As the channel quality gets close to 1 (i.e. perfectly idle channel), the optimal packet size diverges.

Packets are scheduled with a fixed inter-packet interval, $IPI = 7$ ms. We compute CQ over a trace segment of 50 ms and then run a PRR check over the entire trace.

Figure 4.2 shows that very small payloads lead to high E_{bit}. For highly interfered channels ($0.3 < CQ < 0.6$), we find that there is a range of payload lengths from 20 to 100 bytes that provide low energy costs, 1 $\mu J/bit$ or less. The figure also shows that for congested channels, the energy required per useful bit (E_{bit}) for large packets is prohibitively high. We also find that the throughput is inversely correlated with the energy cost.

Payload sizes for the minimisation of E_{bit} are shown in Figure 4.3. A payload of around 100 bytes leads to good performance for all CQ values, which implies that a payload of this size is a good choice when no packet size adaptation is performed. This plot illustrates the energy improvements achievable by tuning the packet size for $CQ \geq$

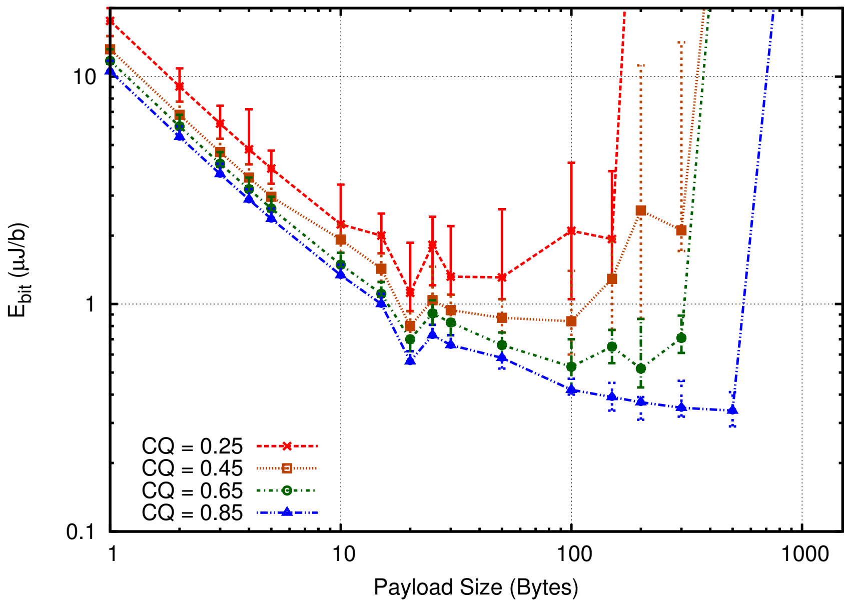


FIGURE 4.3: Energy-per-useful-bit collected from over 2.40×10^5 packets (ARQ only). Large packets provide more energy efficiency up to certain critical sizes, depending on `CQ`, above which the collision probability grows drastically and leads to very high E_{bit}.

0.6. However, the large inter-quartile ranges (IQR) for $CQ \leq 0.6$ indicate large energy cost uncertainties, thereby limiting the effectiveness of packet size tuning. Thus, delay performance and effectiveness of retransmission schemes, when packet size adaptation is used, should be evaluated online.

When the channel quality is high ($CQ \geq 0.85$), larger packets imply higher energy-efficiency and higher throughput. We encounter up to 20% increase in energy-efficiency and 240% gain in throughput for payload sizes up to 500 bytes compared to 100-byte payloads.

Vuran and Akyildiz proposed a packet size optimization framework for a multi-hop scenario, with an ARQ scheme, and found energy optimal packet sizes up-to 2×10^4 bytes, under SNR of 15 dB [105]. However, our experiment shows that in a low data-rate low-power PHY layer, under CTI, up-to 500-byte payloads can be accommodated with cost benefits, provided adecuate SNR exist—see table 4.1. These larger packets greatly increase throughput and by dynamically adjusting the packet size to the channel condition, energy-efficiency is maintained.

4.3.4 Implications for 6LoWPAN

These results are particularly relevant for 6LoWPAN networks. IPv6 requires the maximum transmission unit (MTU) to be at least 1280 bytes. In contrast, maximum packet size in the IEEE 802.15.4 standard is 127 octets. In the worst case, the maximum size available for transmitting IP packets over an IEEE 802.15.4 frame is 81 octets. The IPv6 header is 40 octets long (without optional headers), which leaves only 41 octets for the upper-layer protocols.

In order to cope with this constraint, RFC 4944 [120] proposes LoWPAN encapsulated IPv6 datagrams and header compression, which requires fragmentation and reassembly. However, increasing the IEEE 802.15.4 maximum packet size reduces header overhead, enhances link performance and boosts energy-efficiency. We have seen that it is beneficial in low interference scenarios. In the next section, we will discuss the use of erasure codes to enable large payload transmissions also in high interference scenarios. For an introduction to the design challenges related to 6LowPAN and 802.15.4, the reader is referred to RFC 4919 [121] and RFC 4964 [120].

4.4 Error Correction Optimisation

Erasure codes are commonly used in storage and communication systems as an alternative and also as a complement to data redundancy and packet retransmissions. Proper use of erasure codes provides greater efficiency and fine-tunable levels of error protection, but at the cost of greater complexity.

In communication systems, error correcting codes are used as a Forward Error Correction (FEC) technique. Provided the receiver demodulator maintains synchronization, erasure codes can help recover packets despite collisions. In the presence of short duration interfering signals, as we show next, a small level of erasure code redundancy can lead to sizeable gains in terms of energy efficiency and performance.

We explore generic erasure codes and do not account for the computation cost of any particular realization of the coding and decoding modules. Instead, our energy estimations are centred on radio chip power consumption and account for the consumption in both sender and receiver nodes. This is a reasonable approximation for next generation LPWN platforms [32, 110, 111].

4.4.1 Equivalent SINR Gain

In order to understand the impact that FEC can have in the design of LPWN protocols, we investigate the equivalent SINR gain on the measurement data set discussed in Section 4.2.3. We compute the equivalent SINR gains as follows. With respect to a sliding window whose size corresponds to a fixed packet transmission duration, we compute:

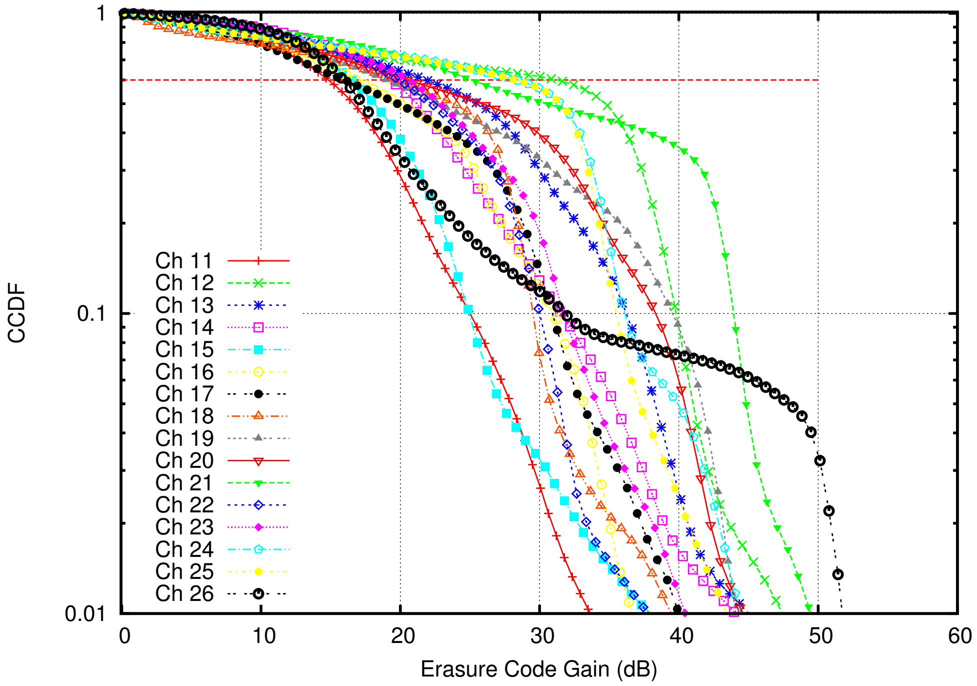


FIGURE 4.4: Effective SINR gain due to erasure codes. An erasure code, capable of recovering 10% of the packet payload, provides an effective SINR gain up to 25 dB with more than 0.6 probability for a heavily interfered channel, like channels 12 and 21. There is also considerable gain, near 15 dB, for channels 11 and 15 which are much less interfered.

(a) the maximum level that the interference signal reaches inside the window and (b) the minimum possible signal level (according to the SINR) at which the total length of erasures do not exceed the maximum correcting capacity of the erasure code being considered. The difference between these two signal values gives the equivalent SINR gain.

For each channel, the number of data points obtained by the sliding window samples is over 9.70×10^6, shown in Figure 4.4. The figure displays the Complementary Cumulative Distribution Function (CCDF) curves for four IEEE 802.15.4 channels, computed for a code capable of correcting 10% of the frame length. The values on the Y-axis represent the probability that the signal remains above a given power level, represented on the X-axis. As the figure shows, an erasure code capable of recovering 10% of the packet payload provides an equivalent SINR gain of 25 dB with probability greater than 0.6 for a heavily interfered channel, like channels 12 and 21. There is also a significant gain of over 15 dB at the same probability for channels 11 and 15 which are much less interfered.

Observe the curves in Figure 4.4 corresponding to the IEEE 802.15.4 channels 11 and 21 have a prominently distant downswing point in the x-axis (10 and 40 dB, respectively), indicating that nodes in these channels are exposed to significantly different levels of interference from the IEEE 802.11 networks. Highly frequent spiky interfering signals shift the curves further to the right, corresponding to a larger power gain due to the erasure code. At small gain values, all curves exhibit similar slopes. In the absence of interfering signals, the code provides gains owing to the presence of noise. Therefore, all CCDF curves are similar for low gain values.

The CCDF curves are also very robust with respect to the size of the *sliding window*. Our experiments consistently reveal no difference between curves computed for intervals between 3 and 60 ms, when at least 10% payload is recoverable.

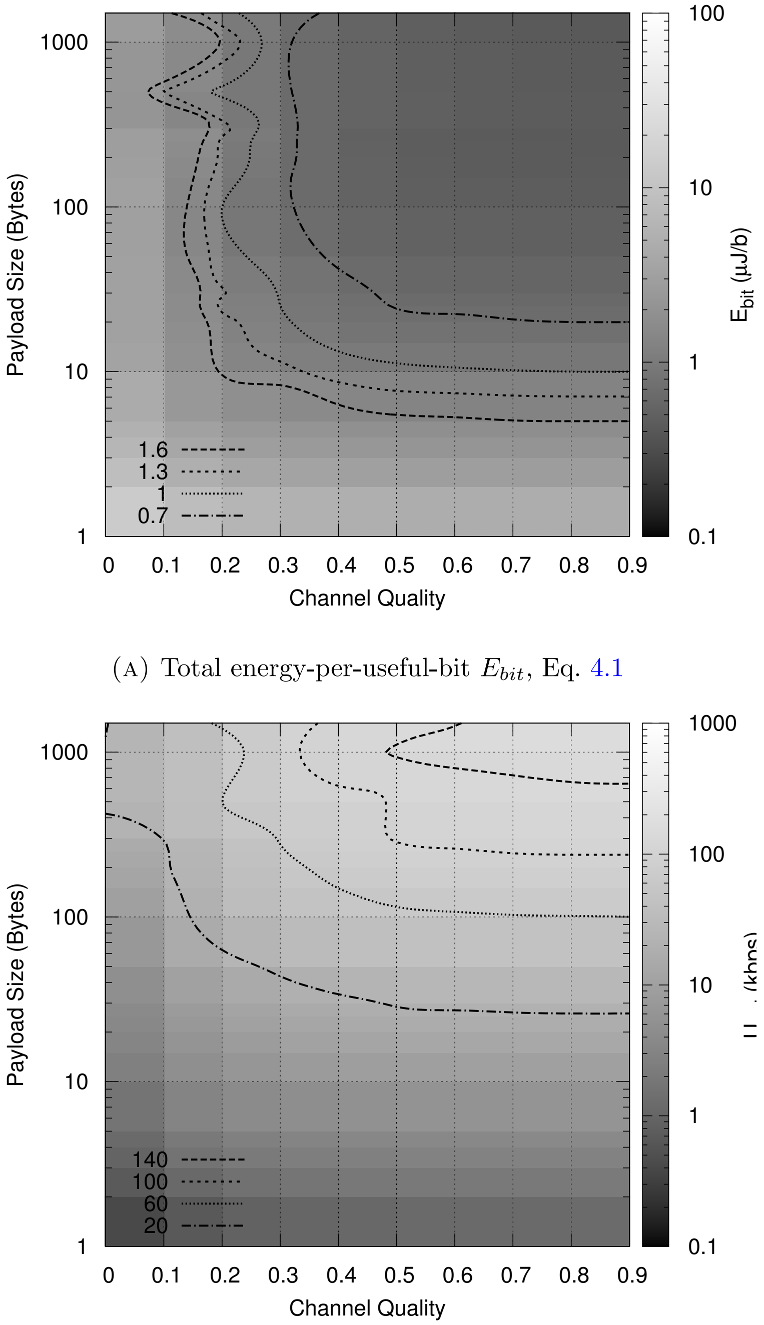
4.4.2 Erasure Codes

Consider an optimal erasure code (n, k, t), where n represents the length of the codewords, k the information bits to be mapped into the codewords, and t the code correcting capacity. This code permits to recover the original message out of any k of the n codeword symbols. The worst case recoverable erasure of the optimal code is determined by the *Reiger bound* [122] and is given by $t = 0.5(n - k)$. Moreover, the code-rate $r = {}^{k}/_{n}$ indicates the level of communication overhead the code introduces. We will further refer to this optimal erasure code as $EC[r]$. For a formal introduction to Erasure Codes (also called Burst-Error-Correcting Codes) please refer to [123, Ch. 20].

In the following study we use an erasure code $EC[r]$ to partially encode frames and conduct a similar study to the one described in Section 5.3.3. In this case, the interference level may exceed the signal level leading to the SINR fall below the threshold during a frame reception. We mark the symbols erased whenever the SINR falls below the threshold. If the amount of erased symbols remains below the level that the code can correct, the frame counts as successfully received.

PHY and MAC headers are typically added by dedicated hardware in the radio, after the transmission buffer is filled up with the rest of the frame. The checksum is computed prior to the inclusion of these headers, which leaves this part of the frame without error correction protection. First we consider this common scenario where PHY and MAC headers are not protected by a checksum and later on we consider the case for protecting the entire packet when the level of interference is extremely high.

Figure 4.5 shows the behaviour of utility metrics using a code $EC[r = 0.8]$. Similarly to the previous section, packet sizes below 10 bytes lead to high energy cost and low throughput, regardless of the channel condition. However, a new result is that packet sizes up-to 1500 bytes lead to higher energy-efficiency. Energy values are below 0.7 $\mu J/bit$ and the surface is now flat for a wide range of packet sizes and channel conditions ($CQ \geq 0.4$ and payloads ≥ 30 bytes) as shown in Figure 4.5a. The throughput surface



(A) Total energy-per-useful-bit E_{bit}, Eq. 4.1

(B) Throughput U_{put}, Eq. 4.2

FIGURE 4.5: Utility metrics with error correction ($r = 0.8$)

in Figure 4.5b also shows significant improvements, as large packets provide nearly the maximum attainable throughput for low to moderate interference scenarios.

The impact of erasure codes is even more visible by comparing Figures 4.3 and 4.6. Despite that heavy interference still doubles the energy cost, the overall energy-per-useful-bit remains nearly flat even for low channel qualities. In the experiments discussed earlier in Section 5.3.3, packets contain vulnerable frames with headers lasting 1024 μs

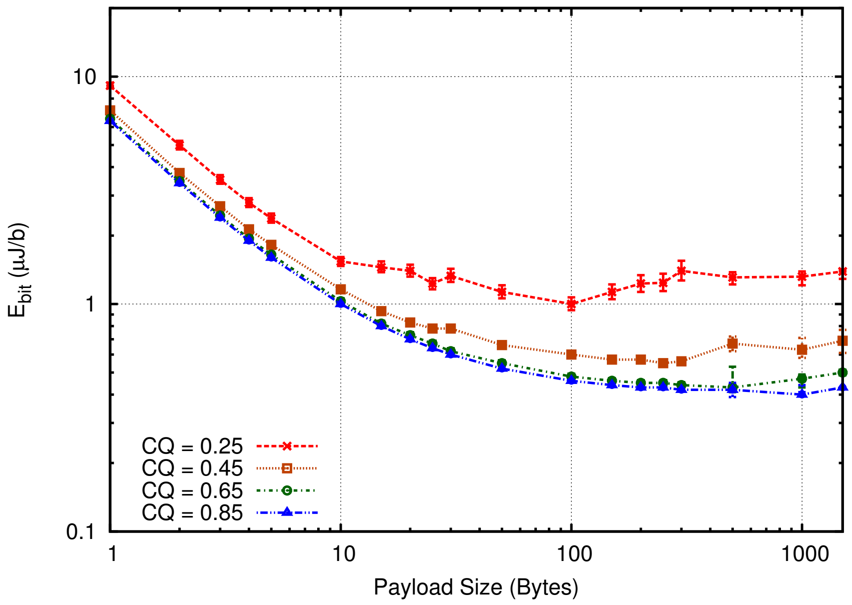


FIGURE 4.6: Energy optimization with error correction $EC[r = 0.8]$: Payload size vs. energy-per-useful-bit.

followed by the payload. The header contains 22 bytes of 802.15.4 PHY-MAC (64-byte addresses) and 10 bytes of compressed 6LoWPAN header. In contrast, in these FEC experiments, the vulnerable frame section lasts 480 μs and the rest is protected by the code. As a consequence, there is lower probability of frame errors due to collisions. Comparing the origin of the curves (negligible payload size) in Figures 4.3 and 4.6, shorter vulnerable headers cut the energy-per-useful-bit by nearly 50%.

Furthermore, the large IQR bars for $CQ \leq 0.6$ observed in Figure 4.3 are shrunk by the erasure code. The erasure code introduces tolerance for changes in the interference situation between the instant `CQ` is computed and when the frame arrives. In other words, in the experiments in Section 5.3.3, small changes in interfering energy spikes may create collisions that change the PRR values for the same `CQ` values. With the erasure code, it requires a much larger change in the interference scenario to make an equivalent difference in the PRR.

In Figure 4.7, we present a comparison of optimal payload sizes and the maximum throughput obtained using erasure codes and those obtained using ARQ (as in Section 5.3.3). The payload size and the throughput increase by almost 5 times in high interference scenarios using erasure codes. The improvements continue to hold for the wide range of `CQ`, except for very high quality channels. For perfectly idle channels, the code introduces an unnecessary overhead.

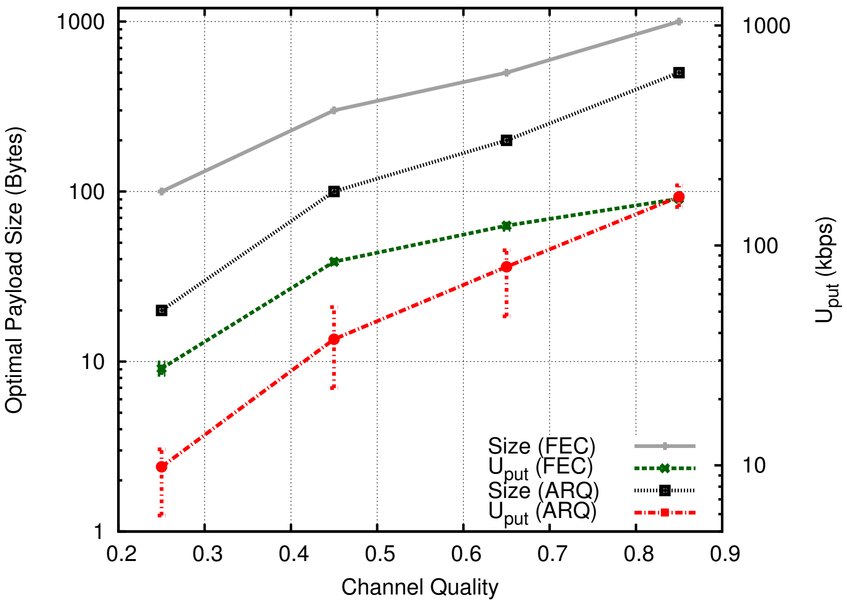


Figure 4.7: Optimal payload size and the corresponding throughput for ARQ and $EC[r = 0.8]$. Error correction increases the optimal payload and throughput nearly 5 times under heavy interference.

We explore the effects of various code-rates on the utility metrics. We found that for $r \leq 0.6$ there is no significant improvement. The added correction capacity provided by $EC[r = 0.6]$ is useless without also adding protection to all headers. We discuss this in more detail in the next section.

This experiment shows that erasure codes further extend optimal packet sizes up-to 1500-byte payloads. These large packets boost performance and energy-efficiency under heavy interference from Wi-Fi networks. These results agree with previous findings by Vuran and Akyildiz [105] and point toward sizeable cost benefits in extending the maximum packet size in the low-power low-datarate PHY. Furthermore, large packet sizes may not be a limitation for future LPWN platforms [32].

4.4.3 CQ-based FEC Optimisation

We now discuss the use of the wireless channel quality metric (CQ) to dynamically adapt the payload size and FEC overheads.

We compare the performance gains of erasure codes $EC[r = 0.6]$ and $EC[r = 0.8]$ for low channel qualities, and find little or no difference. Moreover, the number of unrecoverable packets is independent of their sizes. This is due to the fact that the errors are located in the unprotected headers. Thus, to investigate the effectiveness of $EC[r = 0.6]$, we leave only the PHY header vulnerable, which is 6-byte long and hence lasts 192 μs. In this case, we find performance improvements for $CQ \leq 0.3$.

We study these two codes, $EC[r = 0.6]$ and $EC[r = 0.8]$, and ARQ on frames containing 100-byte payloads. The result is shown in Figure 4.8. In the figure, we can identify three regions based on the behaviour of the code. Each region corresponds to a range of CQ values, which we simply refer to as *low*, *medium* and *high* channel qualities. In each of these regions there is one code-rate that provides the optimum results for both utility metrics, energy as well as throughput. These new results indicate that there are between 20 to 60% improvements in both energy-per-bit and throughput, over the entire CQ range. Moreover, we find that both utility metrics favour larger payloads.

From these evaluations, we make the following observations: (a) optimal payload sizes increase with CQ, for all code-rates, (b) lower code-rates lead to larger optimal payload sizes, (c) for each channel quality range (*low*, *medium* and *high*), there is a code-rate that improves the utility metrics regardless of the payload sizes, and for a given CQ larger payloads perform better on the utility metrics. This can be seen in Figures 4.7 and 4.8.

Based on these experimental results, we propose the following algorithm, RR-ADAPT, to dynamically adapt radio resources in a receiver initiated MAC protocol, e.g., A-MAC [124]. RR-ADAPT determines the optimal settings for data transfer on channels affected with interference including CTI. This algorithm takes as inputs the energy level of the frame's signal reaching the receiver (R_{THR}) and the data volume to be transferred from the sender. It then provides the optimal payload sizes and code-rate as follows: it computes CQ based on E_{THR} and finds the optimal code-rate from off-line results, such as the one in Figure 4.8. It then finds the optimal payload based on CQ and r, from the curves in Figure 4.7. The receiver computes the CQ, and then inserts the CQ value in the MAC probe, sent periodically at the end of each sleep cycle. The sender prepares packets accordingly before transmitting.

To the best of our knowledge, there are no IEEE 802.15.4 transceivers that can be adapted to handle very large ($\sim$ 1000 bytes) packets. Therefore, we leave validating these ideas in online experiments as a future work.

4.5 Summary

We addressed the issue of co-existence of low-power wireless networks in the presence of cross-technology interference from uncontrollable sources, which may operate at high power levels. Using the CQ metric (introduced in Chapter 3), we studied dynamic packet

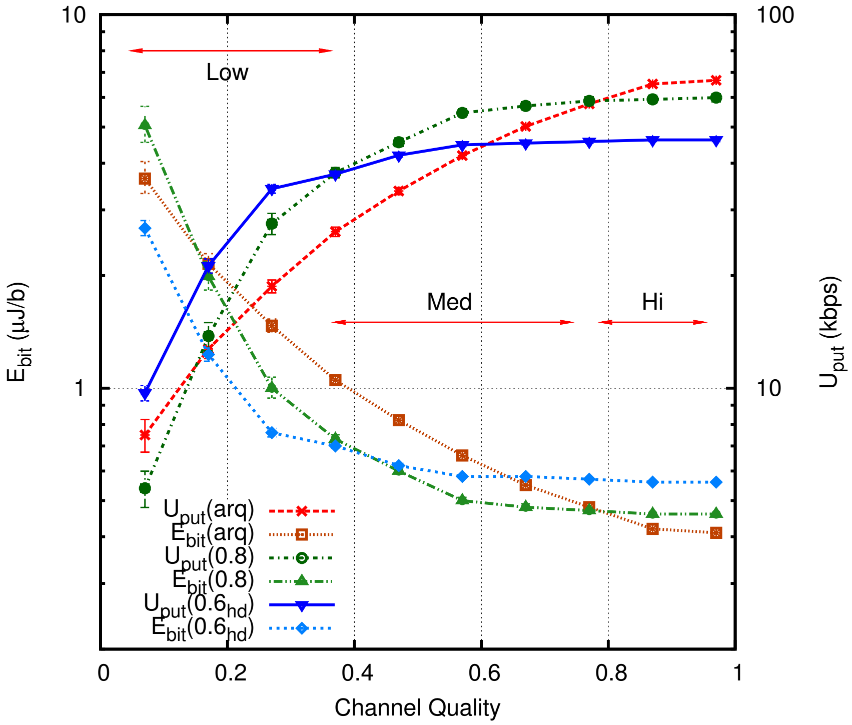


FIGURE 4.8: Optimal error control for three channel quality regions: *Low CQ-FEC(0.6)*, *Medium CQ-FEC(0.8)* and *High CQ-ARQ*.

size adaptation and the application of erasure codes for optimizing reliability, energy consumption and throughput.

Based on measurement data collected from a building containing several Wi-Fi networks, we found that payload size in the neighbourhood of 100 bytes leads to near-optimal performance in general in the IEEE 802.15.4 networks. We find that for moderate and low interference levels, increasing the packet size to a few hundred bytes, i.e. beyond the limit specified in the IEEE 802.15.4 standard, can lead to significant improvements in network performance.

Our data also shows that for very high interference scenarios, erasure codes capable of correcting 10% of the packet payload can provide an equivalent signal to interference plus noise ratio (SINR) gain of 25 dB with probability greater than 0.6. This is significant for interference management and for increasing spatial re-use by employing lower transmission power and suggests that erasure codes drastically improve energy-efficiency and throughput of low-power wireless links. We show that the payload size and the throughput increase by almost fivefold in high interference scenarios using erasure codes. In this heavy interference regime, even though interference doubles the energy-per-usable-bit cost, erasure codes remain cost-effective for very large payload sizes, up-to 1500 bytes.

Chapter 5

On the Scalability of Constructive Baseband Interference

Constructive baseband interference has been recently introduced in low-power wireless networks as a promising technique enabling low-latency network flooding and sub-µs time synchronisation among network nodes. The scalability of this technique has been questioned in regards to the maximum temporal misalignment among baseband signals, due to the variety of path delays in the network. By contrast, we find that the scalability is compromised, in the first place, by emerging fast fading in the composite channel, which originates in the carrier frequency disparity of the participating repeaters nodes. We investigate the multisource wave problem and show the resulting signal becomes vulnerable in the presence of noise, leading to significant deterioration of the link whenever the carriers have similar amplitudes. The work included in this chapter was partially documented in a short-paper publication [47].

5.1 Introduction

Radio wave propagation, other than in open space, is characterised by producing an interference pattern within wavelength distance granularity that leads to irregular radio coverage. Thus, given a uniform antenna radiation pattern, there is a remarkable irregularity in spatial power distribution of the wave. This interference among the original signal and its reflected components in the surrounding environment are to some extent captured by indoor wireless channel models and it is known as multipath small scale fading.

The power of the radio signal relative to the power of the electromagnetic noise in the wireless channel determines the signal to noise ratio (SNR). When the radio wave is used as a carrier, its parameters are altered by the modulation process in the transmitter and then used to convey information to a radio receiver. The level of errors in the information decoded by the receiver is a function of the SNR in the receiver. Therefore, the location of the radios becomes critical, since in general a strong SNR is needed to maintain low-error levels.

The most obvious way to increase SNR is by increasing the power of the transmitter. However, large transmission power values reduce the spatial capacity of the network, generate disruptive interference to collocated systems and it is not energy-efficient. An alternative way is to use some form of redundancy, for example, antenna diversity in the receiver is a practical technique, as far as the antennas can be feasibly separated for at least a quarter of the wavelength. Another approach is to use sender diversity to simultaneously radiate multiple waves from different locations. The resulting radio coverage is the superposition of all participating waves, effectively weaving a tapestry of signal coverage much more homogeneous and regular that what can be achieved with a single emitter. Such a system is known as a single frequency network and is widely used in modern wireless communication networks. The basic technique for single frequency networks is constructive baseband interference (CBI), which is used to transmit identical baseband information from several senders simultaneously. We will discuss CBI in detail in this chapter and will examine the scalability of this technique in low-power wireless networks.

CBI exploits the spatial, temporal and spectral diversity exhibited by the wireless channel to introduce link redundancy and increase reliability [125, 126]. This diversity of the wireless channel manifests itself as a given symbol stream traverse different wireless channels simultaneously and each symbol is unlikely to suffer the same level of distortion, small-scale multipath fading and attenuation in all channels at the same time. Therefore, concurrent transmission of identical packets from several senders can increase the quality of the wireless link towards a receiver.

CBI has been recently introduced in wireless networks by Rahul et al. [125]. Dutta et al. employed CBI to alleviate the acknowledgement implosion problem, using simultaneous transmissions of short acknowledgement packets, in a receiver-initiated low-power Medium Access Control (MAC) protocol [127]. Ferrari et al. devised a communication primitive for low-latency network flooding and sub-µs time synchronization for low-power wireless nodes [126]. In subsequent works, they also proposed an infrastructure (analogous to a shared bus), which supports mobile nodes in a multihop low-power wireless network [128]. Doddavenkatappa et al. further optimise network flooding, enabling a multichannel packet pipeline across the network [129, 130].

However, some limitations in the efficacy and scalability of CBI have been studied by Wang et al. [131]. They investigate the worst case scenario in a multihop network showing that cumulative non-deterministic delays in the network cause the temporal displacement between concurrent transmissions to exceed the symbol boundaries, leading to poor packet reception rate. We take a different perspective on this matter by analysing the superposition of carrier waves. Our main contribution is that we demonstrate that the scalability of CBI is not only limited by the variety of temporal delays as investigated by Wang et al. but, firstly, by specific properties of the composite signal.

We present the multisource wave problem (Section 5.2) and investigate the error rate and the envelope of the composite signal, which results from the superposition of all repeater signals. Our experiments (described in Section 5.3) show an acute signal vulnerability in the presence of noise and the consequent deterioration of the link quality for a power imbalance among two or more repeater signals smaller than 5 dB (Section 5.3.4). We discuss the results and draw some conclusions in Section 5.4.

5.2 Constructive Baseband Interference: a Snapshot

CBI occurs when multiple-source carriers, modulated with identical information and adequate time synchronisation, add up in the receiver antenna. Figure 5.1 shows a simple model that abstracts CBI. The signal generated in each of the senders are carriers modulated with the exact same information and time synchronised. The time synchronisation error plus the wave propagation delay difference among these signals must remain within symbol boundaries, to avoid intersymbol interference [132]. In the case of the IEEE 802.15.4 PHY, operating at 250 kbps, half the symbol time corresponds to 0.5 µs [126**?**].

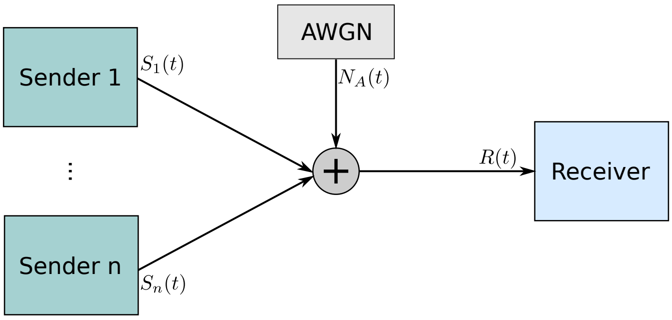


FIGURE 5.1: Simple model for CBI.

Since the modulated carrier of each transmitter traverses distinct wireless channels towards the receiver, we refer to them as *individual channels* as they are, in general, statistically independent. Furthermore, the composite signal that results from the superposition of waves can be interpreted as if it traverses a *composite channel* characterised by the resulting sum of multisource carriers, in addition to the overall multipath effect of the individual channels. Equation 5.1 represents the composite signal in the receiver plus noise, modelled as a Additive White Gaussian Noise (AWGN). We will examine the properties of the composite channel in Section 5.3.2.

$$R\,(t) = h_1\ S_1\,(t) + h_2\ S_2\,(t) + ... + h_n\ S_n\,(t) + N_A\,(t) \tag{5.1}$$

The channel state information CSI for channel i is represented as h_i, which is a complex number and represents the wireless channel instantaneous transfer function. We are particularly interested in the case of highly correlated wireless channels, as a worst case scenario, where h_i values are very similar for all channels involved in CBI. This is a realistic scenario in low-power wireless network applications as a simple example in our experiments demonstrates (Section 5.3.4).

Most communication models currently used in LPWN fall into two categories: data collection and data dissemination. The latter benefits from CBI when it is used for network flooding, as the traffic generated in the network is one-to-many. Collection (many-to-one) and other communication patterns, such as one-to-one, have been implemented using a network primitive based on CBI and shown to be more energy-efficient and reliable than more traditional low-power wireless network stacks, where an asynchronous MAC protocol is coupled with a routing protocol [128].

5.2.1 Baseband Synchronisation

In order to generate CBI, participating sender nodes must concurrently send the same information within a time synchronisation accuracy substantially better than half symbol period. As the wave can propagate along different distances from participating repeater nodes toward a receiver, the corresponding time shift introduced must also remain low to avoid intersymbol interference.

In order to obtain such time synchronisation, the network needs a bootstrapping phase in which nodes acquire a common clock. Then, repeater nodes can retransmit frames while introducing the minimum possible non-deterministic delays in the process. Nodes can only repeat correctly received frames and the start of frame delimiter (SFD) symbols are decoded by the radio chip and attended by an interrupt service in the microcontroller.

During reception, this SFD signalling event serves as a common time reference for all nodes in the radio range of a repeater. Moreover, information about the number of retransmission the frame has undergone serves as a reference time relative to the initiator (which transmitted the original frame). By processing and updating these values periodically it is possible compensate the MCU's clock drift, to maintain a time error among clocks up to several order of magnitude below the IEEE 802.15.4 symbols time, depending on the implementation and the hardware used.

Provided the nodes have a common clock, the radio transceivers can initiate a synchronous transmission with the same information. We will discuss the modulation and the characteristics of the baseband signal in the next section.

5.2.2 Modulation

Let us first analyse the baseband signal and carrier modulation. We focus on Offset-Quadrature-Phase-Shift-Keying with half-sine-shaping (OQPSK-HSS), which is used by IEEE 802.15.4 compliant radios operating at 2.4 GHz. Figure 5.2 depicts an example of the baseband signal, a stream of bits split in two branches of odd and even bits, as described by equations 5.2 and 5.3 respectively. Each one is used to alter the phase of a sine wave, according to the corresponding information bit value. The resulting baseband components are represented by equations 5.4 and 5.5. It is worth mentioning that in the IEEE 802.15.4 PHY these bit streams are not the frame payload but instead the result of an intermediate coding for spread spectrum modulation, known as Direct Sequence Spread Spectrum (DSSS) [6].

Under CBI, provided that each repeater node receives and correctly decodes the frame content, a new frame payload is fed to the radio chip transmitter FIFO buffers with as tight synchronisation as possible. This may require to resolve intricate timing issues, depending on the hardware platform used. For example, when the radio and the MCU

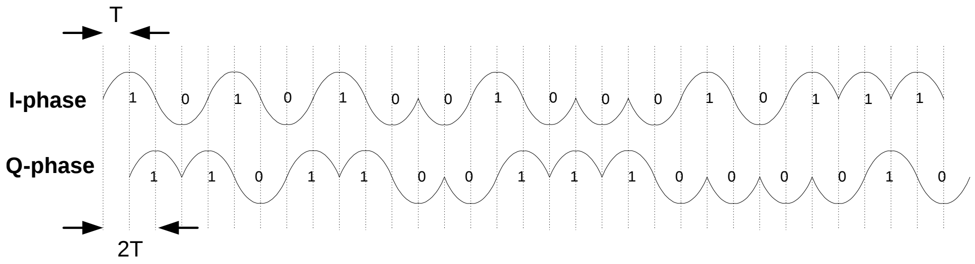


Figure 5.2: Offset-Quadrature-Phase-Shift-Keying with half-sine-shaping (OQPSK-HSS). The in-phase and out-of-phase components are shifted by $\pi/2$ in order limit valid symbol transitions. Under CBI, the half symbol period (represented by T in the graph) corresponds to the maximum possible misalignment before intersymbol interference occurs.

are packaged separately and the chips are connected through a serial bus, the solution calls for careful low-level programming [126].

$$a_I\left(t\right) = \sum_{k=-\infty}^{\infty} \alpha_k^I \Pi\left(\frac{t-2kT}{2T}\right) \tag{5.2}$$

$$a_Q\left(t\right) = \sum_{k=-\infty}^{\infty} \alpha_k^Q \Pi\left(\frac{t-\left(2k+1\right)T}{2T}\right) \tag{5.3}$$

$$\text{I-phase}\left(t\right) = a_I(t)\cos\left(\frac{\pi t}{2T}\right) \tag{5.4}$$

$$\text{Q-phase}\left(t\right) = a_Q\left(t\right)\sin\left(\frac{\pi t}{2T}\right) \tag{5.5}$$

These two baseband signal components are used in the transmitter section of the chip to modulate linearly independent components of the carrier, as described by equation 5.6. This modulation process is carried out concurrently in each repeater node; the result are equal symbols transmitted from each node at any given time.

The direct conversion radio transceiver uses a frequency synthesiser to generate the carrier frequency from a time-base typically provided by an external quartz crystal. The frequency accuracy of the quartz crystal is specified in IEEE 802.15.4 to remain below ±40 *ppm* [6]. Given this accuracy, the relative error of the carrier is preserved and produces an absolute frequency error smaller than ±100 kHz in the 2.4 GHz carrier, which is a small frequency offset to tolerate in the receiver, provided that the spectral footprint of the DSSS modulated carrier is approximately 2 MHz wide. Note the carrier frequency is represented in equation 5.6 by ω_c.

$$S\left(t\right) = a_I\left(t\right)\cos\left(\frac{\pi t}{2T}\right) \; A\cos\left(\omega_c t\right) + a_Q\left(t\right)\sin\left(\frac{\pi t}{2T}\right) \; A\sin\left(\omega_c t\right) \tag{5.6}$$

Figure 5.3 shows the internal block diagram of the TI CC2420 radio chip. Within the transmitter signal path (lower side), the RF mixers produce a carrier-suppressed amplitude modulation. Note that this 2.4 GHz carrier, modulated with the baseband signal discussed previously, carries information only through its phase variations. The resulting signal to reach the sender's antenna is expressed in equation 5.6. We will analyse the implication of this frequency offset for CBI in the next sections.

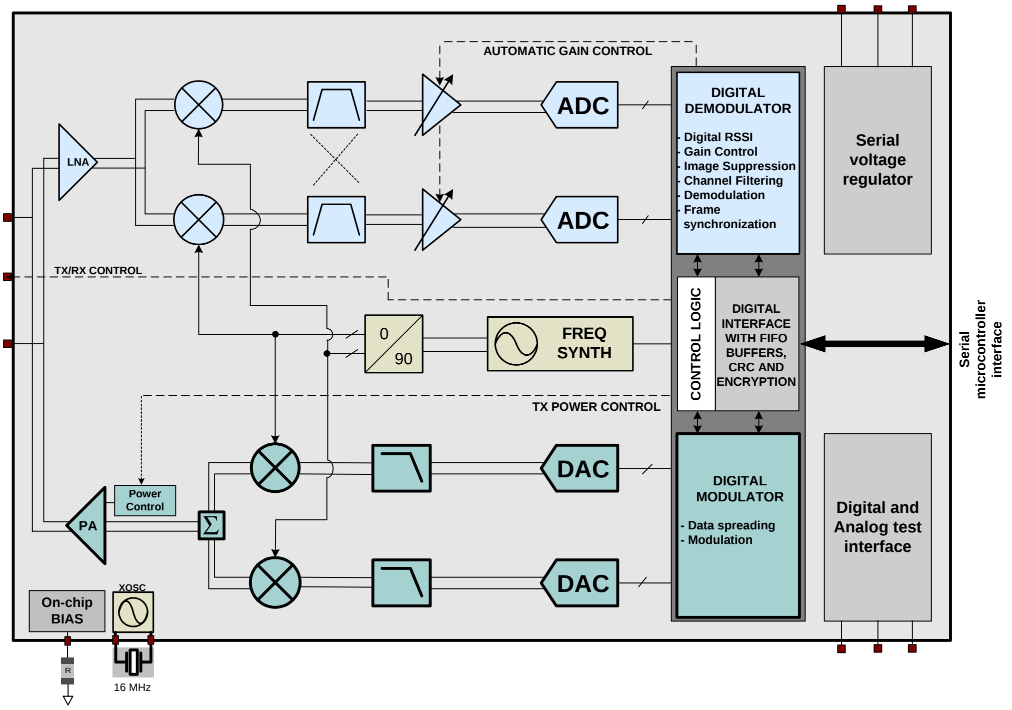


FIGURE 5.3: Block diagram of the internal design of a generic radio transceiver chip, with the antenna port on the left side. Note the frequency synthesizer block of the transceiver, in the center. Above it, the receiver RF chain and below it, the transmitter RF chain. Both path use a symmetrical architecture for the respective in-phase and out-of-phase components. The image is taken from the TI CC2420 datasheet.

5.2.3 Carrier Waves

The signal from multiple repeaters reaches the receiver nodes within radio range as a composite signal, which is the superposition of the participating repeater signals. We can also describe the composite signal based on the in-phase and out-of-phase components of the individual carriers that add up in the wireless channel as expressed as follows:

$$R\left(t\right) = R_I\left(t\right) + R_Q\left(t\right) + N_A\left(t\right) \tag{5.7}$$

Moreover, each of the respective components in equation 5.7 can be further expressed in terms of the individual carriers. Note that if we consider accurate enough time synchronisation, then the baseband signal remains identical and can be extracted as a common factor, as expressed by equations 5.8 and 5.9. We also assume for simplicity that the channel state information (CSI) for the respective wireless channels are identical, which is reasonable approximation for highly correlated channels. Hence, we represent the carrier amplitude simply by A_i.

$$R_I(t) = a_I(t)\cos\left(\frac{\pi t}{2T}\right)\sum_{i=1}^{n} A_i \cos\left(\omega_{c_i} t + \theta_{c_i}\right) + N_A(t) \tag{5.8}$$

$$R_Q(t) = a_Q(t)\sin\left(\frac{\pi t}{2T}\right)\sum_{i=1}^{n} A_i \sin\left(\omega_{c_i} t + \varphi_{c_i}\right) + N_A(t) \tag{5.9}$$

Each of the above components is separated from the composite carrier signal in the quadrature RF mixer stage in the receiver, by multiplying by another signal whose frequency is very close to the original carriers. This effectively transports back the signal to near baseband frequencies, while preserving the corresponding absolute frequency disparity existing among participating repeaters. Note that this frequency disparity is the absolute frequency value resulting from the multiplication of the quartz crystals resonance frequencies (±100 kHz), with the indicated error tolerance of ±40 *ppm*. Figure 5.3 shows the involved modules in the upper side of the block diagram of the TI CC2420 radio chip.

Let us now look into the wave properties to understand CBI from that perspective. Let the composite unmodulated signal A_c from n sources be expressed as:

$$A_c = \sum_{i=1}^{n} A_i \sin(w_i t + \phi_i) \tag{5.10}$$

Also let A_i, w_i and ϕ_i represent the amplitude, angular frequency and phase of the individual sources respectively. Note that the multisource problem in equation (5.10) is similar to the multipath problem, where all frequencies are equal since they originate at a single source. On the other hand, multiple sources implies small disparities in the carrier frequencies, as there is always a limit in the frequency accuracy of the quartz-crystal based oscillators used to synthesize the carrier. Section 5.3.1 elaborates on this.

The properties of the probability density function (*pdf*) of the resultant amplitude or envelope of equation (5.10) are important for the performance evaluation of wireless systems. The modelling of fading and shadowing in the multipath problem (all w_i are equal) has been widely studied and an expression for the *pdf* can be found in [133].

To the best of our knowledge, an exact expression for the *pdf* of the envelope in equation (5.10) remains an open mathematical problem. Thus, for the sake of simplicity, let us consider the case of two sources ($n = 2$). Let the envelope E_c of equation (5.10) be:

$$E_c = \left[A_1^2 + A_2^2 + 2A_1A_2\cos\left(\left(\omega_1 - \omega_2\right)t + \varphi\right)\right]^{1/2} \tag{5.11}$$

Equation (5.11) reveals a harmonic function with angular frequency $w_c = w_1 - w_2$ which leads to periodic depressions in the amplitude of the composite signal. This is known as the *beating effect*. It is important to note that these depressions can be quite numerous during the packet duration, depending on w_c. As the amplitude decreases, the signal which is blurred by noise in the wireless channel gets closer to the decision boundary, making it increasingly vulnerable. With more sources, the peak to average ratio of the composite signal envelope increases and the problem gets worse, as we will see in Section 5.3.4.

5.3 Scalability of CBI: an Experimental Study

The scalability of CBI is relevant because the disposition of wireless sensor nodes in a deployment should follow application needs. Consider the plausible scenario where a large number of fixed sensor nodes may be required in a given location, while sparse nodes suffice in other areas. Also mobile sensors attached to humans, animals or robots impose a dynamic spatial density. In such scenarios, bulk data transfer with high-throughput, low-latency and low-power may be important system features. For example, the time window to transfer data might be limited in railway-bridge monitoring, as data is uploaded to passing trains [134]. CBI enhances link performance, radio coverage and enables node mobility, while maintaining good link quality. Nevertheless, in our experiments we observe a critical lack of link quality scalability as the number of concurrent repeaters grow, as we explore in the remaining of this chapter.

In this section, we discuss specific aspects of low-power networks based on the IEEE 802.15.4 PHY that are relevant to the scalability of CBI.

5.3.1 Hardware-related features of the IEEE 802.15.4 PHY

As mentioned previously, the oscillator's frequency accuracy of IEEE 802.15.4 compliant radios is mandated below ±40 ppm [6]. This accuracy ensures tight bounds on the transmitter carrier frequency and allows the receiver to use a narrow channel filter to attenuate out-of-band noise power. However, a frequency discrepancy of up to 200 kHz is possible between two radios operating in the same channel of the 2.4 GHz band. We examine the carrier frequency dispersion for TelosB sensor nodes [135] employing a Software Defined Radio (SDR) from Ettus Research [136] for spectrum analysis, and an Agilent 8648C Signal Generator as a reference (10 Hz accuracy and time-base stability below ±0.1 ppm typical). We verify such a frequency offset among nodes and observe no perceptible time variation in the frequencies, provided a constant room temperature is

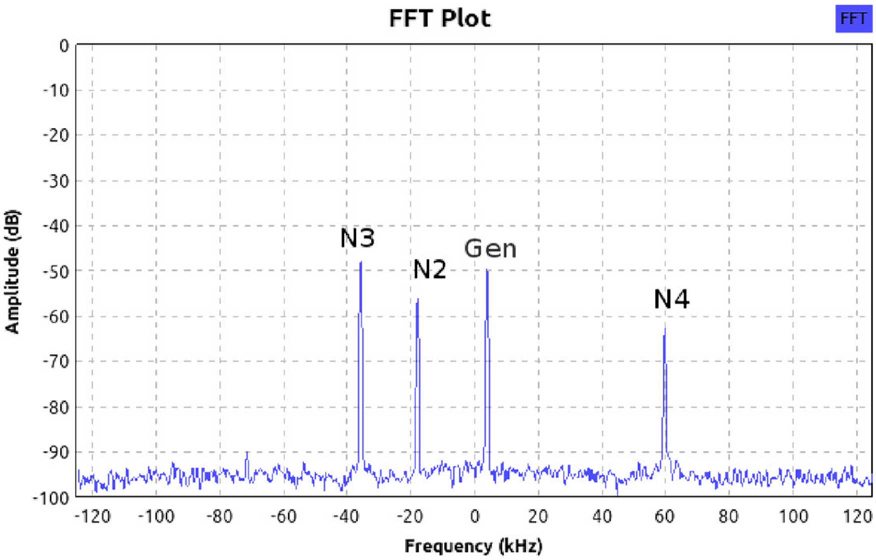


FIGURE 5.4: FFT of the CC2420 unmodulated carriers from nodes N3, N2 and N4, together with the Agilent 8648C Signal Generator tuned to the center frequency of Channel 26. The B210 here actually tunes to 2479.99643 MHz.

maintained. The corresponding carrier frequencies for several TelosB nodes are shown in the frequency domain in figure 5.4 and the precise frequency values are listed in table 5.1, as a curiosity.

The IEEE 802.15.4 standard also specifies that the receiver sensitivity must be measured at a packet error rate (PER) of 1% for 52-symbol packets [6]. Thus, the required symbol error rate (SER) results near 10^{-4}, which we use as the reference threshold for minimal link performance. Note that a corresponding chip error rate (CER) value, assuming chip errors are i.i.d., is not applicable since errors are more probable during envelope depressions. Hence, we design our experiments to measure both CER and SER. We will discuss in Section 5.3.3 the necessary experimental setup for these measurements.

Node ID	Frequency (MHz)
N1	*2480.00682*
N2	*2479.97831*
N3	*2479.96013*
N4	*2480.05641*

TABLE 5.1: Unmodulated carrier frequencies for a few TelosB nodes measured with a spectrum analyser and the Agilent 8648C Signal Generator.

5.3.2 Composite Channel

The signals traversing the wireless channel reach the receiver with amplitudes that depend on the path loss of the individual channels. Since the baseband signals are time

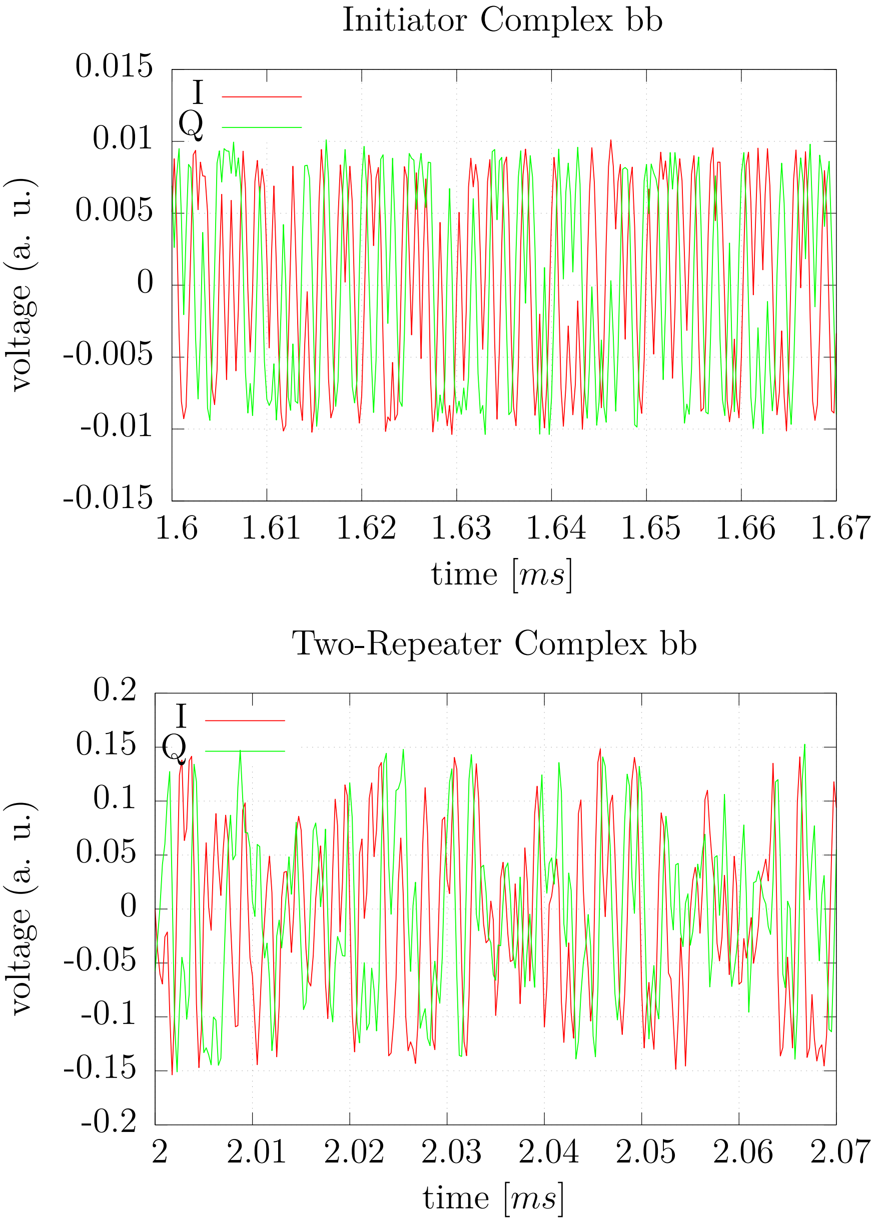


Figure 5.5: Time domain representation of the (complex) baseband signal voltage in arbitrary units. The graph to the left represents the original signal received from a single repeater (the initiator) while the one to the right shows the beating among carriers of two repeaters. The fading effect in the composite signal is clearly visible in the graph to the right.

synchronised, the receiver always locks[1] with the preamble of the strongest signal (to decode the symbols). Therefore, when the amplitude imbalance is sufficiently large there is always *capture* [137]. However, when the magnitudes of the carriers are similar, intrinsic properties of the composite channel emerge.

[1] If the two signals were not time synchronised, the receiver will detect the first preamble and lock to that chip stream. Once the second signal arrives, depending on their relative intensity there might be capture (stronger arrives first) or a collision (stronger arrives later) resulting in the lost of both packets.

The indoor multipath wireless channel is a time-invariant channel whose Channel Impulse Response (CIR) is considered quasistationary with a typical *rms delay spread* $\sigma_\tau < 100$ ns (see Saleh and Valenzuela [138]). Thus, the time dispersive nature of the channel is minimal and the coherence bandwidth is larger than the IEEE 802.15.4 Direct Sequence Spread Spectrum (DSSS) signal bandwidth. Also the individual channel is very slow time varying [138], with a coherence time much larger than the symbol duration, $T_{ci} \gg T_s$. This regime is known as *flat* and *slow* fading [1, 41].

On the other hand, according to equation 5.11, the worst-case coherence time of the composite channel can be expressed as $T_{cc} = {}^{\pi}/_{2w_c}$ and results in $1\,\mathrm{ms} \geq T_{cc} \geq 1\,\mu\mathrm{s}$ with high probability, which is orders of magnitude shorter than what would be observed due to the Doppler spread. Thus, the composite channel one observes under CBI displays *fast* fading, which originates in the carrier frequency disparity of the participating repeater nodes. Figure 5.5 illustrates the deterioration of the signal for a two-repeater experiment, with a (50 %) $T_{cc} \approx 5$ µs. Thus, we see the corresponding frequency disparity among the two repeater 2.4 GHz carriers is close to 40 kHz in the referred experiment. Note that depressions do not incur in a signal null value, since there was a certain power imbalance among the nodes.

5.3.3 Experimental Setup

We design our experiments to analyse IEEE 802.15.4 PHY signals. This analysis benefits from an SDR platform as one can tap into the digital signal processing chain with ease. Our setup is designed around the Ettus USRP B210 board [136] and an SDR transceiver implementation in GNU Radio by Bloessl et al., which interoperates with IEEE 802.15.4 radios [139].

We employ a set of TelosB sensor nodes running Glossy [126] in a one-hop network composed of the initiator and up to eight repeaters. We then record low-noise complex baseband signals, at least 40 dB over the noise floor. We use an example application (`rx_sample_to_file`) from the USRP Hardware Driver (UHD) package running in an overdimensioned Linux workstation to avoid buffer overflows when recording the signal at 4 Msps. The initiator sends 15 packets per second, which are retransmitted 16 and 8 times for the wired and wireless experiments, respectively. Our 480-second-long baseband traces contain at least 1.6×10^5 symbols for our error-rate study. Note that failure to detect the PHY header invalidates the packet, thus we use payloads smaller than 16 byte to maintain robust statistics under high noise levels.

We use two configurations: a wired one and a wireless one. The former is intended to replace the wireless channel with an isolated and controlled signal path provided by an

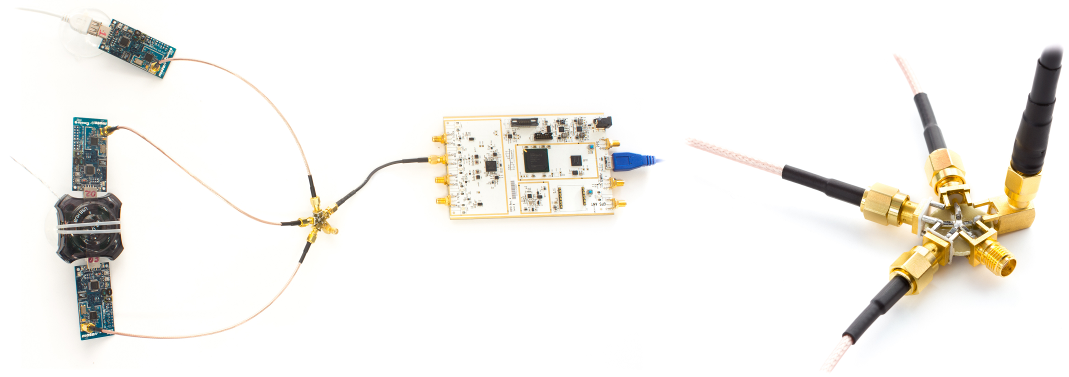


FIGURE 5.6: Photo of the hardware component arrangement used in our wired experimental setup (left) and the power combiner we built (right). The power combiner is built from a resistive T-Network, it provides fixed power attenuation of 40 dB regardless of the number of ports in use. The resistive loads are calculated to minimise power reflection through accurate impedance matching for the 50 Ohms ports.

RF power combiner. This power combiner introduces constant signal attenuation instead of the wireless pathloss, with virtually no signal distortion or delays. Thus, allowing us to experiment with similar power levels in an accurate and controlled way. It also allows us to limit the level of noise at the SDR input. On the other hand, the wireless configuration, uses a real wireless channel to explore CBI in a more realistic scenario. However, we use a disposition of the nodes where there is line-of-sight between all the repeaters and the SDR, providing highly correlated wireless channels which emphasize a worst-case scenario for the scalability of CBI.

Our first (wired) configuration requires all antenna ports (nodes and SDR) be wired through a 5-port 40 dB T-Network resistive power attenuator and combiner which emulates an ideal wireless channel without multipath distortions nor external interference. One node behaves as the flooding initiator, transmitting at an RF power of

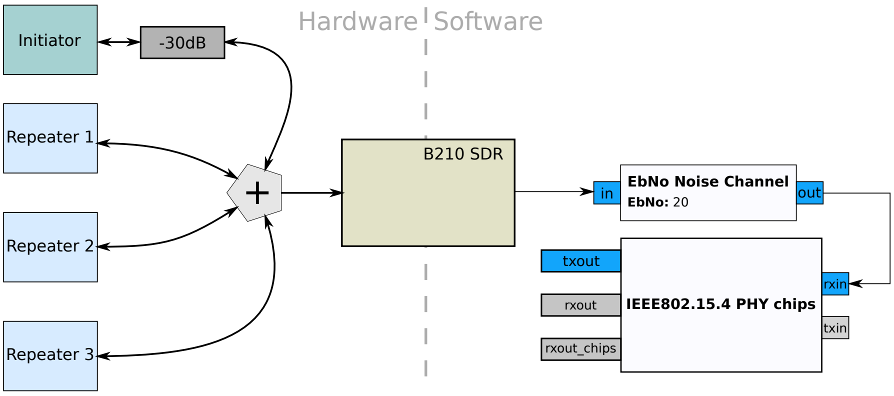


FIGURE 5.7: Block diagram of the functional component setup used in our wired experiments.

$P_{RF} = -15$ dBm. Its signal runs through an additional 30-dB attenuator, thus reaching the SDR at -85 dBm. The repeater operates up to $P_{RF} = -5$ dBm, hence it reaches the SDR at -45 dBm. This power allocation choice is intended to guarantee that the repeaters get the initiator packets with high probability but also forces its signal below the noise floor at the SDR. The hardware components setup is illustrated in figure 5.6, incluiding a closeup image of the power combiner, on the right side. Moreover, the block diagram in figure 5.7 represents the functional components, including both hardware and software, we use for the wired configuration experiments.

Our second (wireless) configuration involves a setup of sensor nodes fastened to an external glass wall, and the B210 SDR board with a 12-dBi YAGI antenna (ANT2400Y12WRU) fixed to a mast on the other end of the office, approximately 7 meters apart. The block diagram in figure 5.8 illustrates all the components involved in our wireless experiments. In this case, the initiator antenna is replaced with a dummy load to attenuate its signal. This is a practical way to preclude the initiator signal from appearing in the SDR traces and affecting the statistic error study where only repeater's signal is desired.

The rest of our experiments are conducted off-line, in the computer, employing the rich component tool set in GNU Radio [140]. Using predefined payloads in Glossy, which are not altered by repeaters, we compute CER and SER by comparing the received frame content from the traces with the expected payload.

In order to compute CER, we need frames whose content is the chip sequences corresponding to the payload's symbols. Thus, we extend the SDR transceiver by Bloessl et al. to also export frames containing received chips, prior to decoding DSSS symbols. We generate two separate *packet capture* (pcap) files with frames containing chips and symbols, respectively. In order to study link performance, we develop a channel module suitable to add controlled noise quantities to match a desired SNR value. This module requires specifying the energy-per-bit (E_b) to spectral noise density (N_0) ratio $^{Eb}/_{No}$ (in

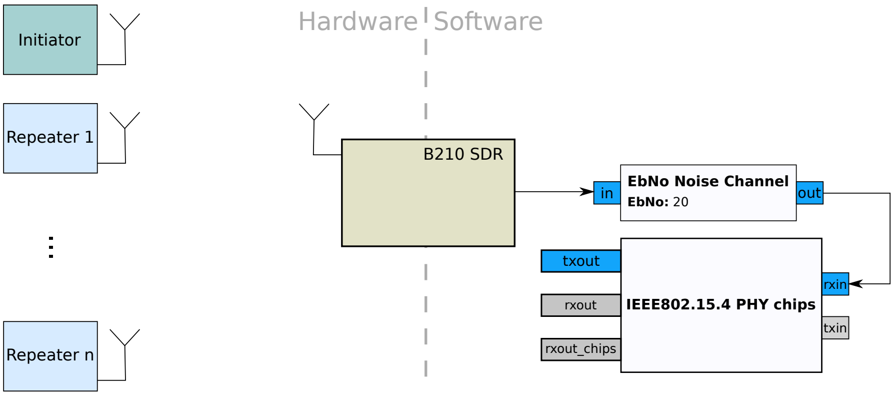


Figure 5.8: Block diagram of the functional component setup used in our wireless experiments.

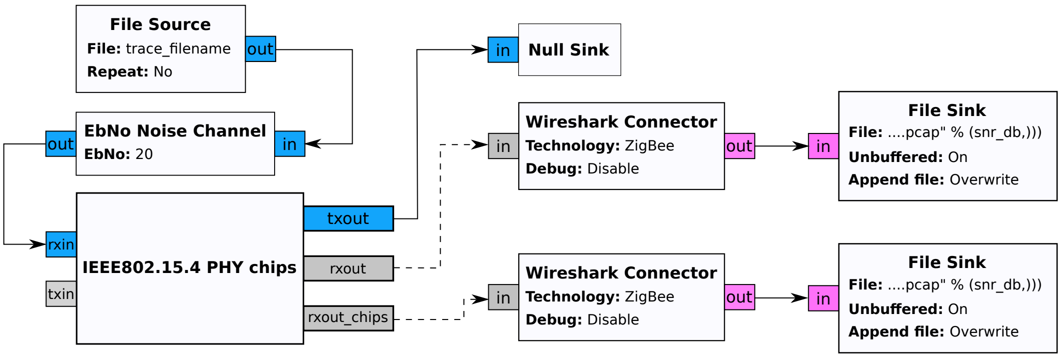


FIGURE 5.9: GNU Radio flow graph used to measure SER and CER in the composite channel by adding synthetic noise in an AWGN channel.

dB) and simulates an Additive White Gaussian Noise (AWGN) channel. The variance values σ^2 are internally computed based on the signal's peak amplitude, the bandwidth of the IEEE 802.15.4 channel and the specified $^{Eb}/_{No}$. A step-by-step derivation of σ can be found in Appendix A. By adding synthetic noise we can study a wide range of SNR ratios in a controlled and repeatable experiment. The GNU Radio flow graph used for the error-rate study is shown in figure 5.9. The flow graph consists of a file source, containing the complex baseband signal, our channel module to add Gaussian noise, and the extended transceiver. Frames containing decoded chips and symbols are stored in their respective pcap files for further processing.

5.3.4 Results and discussion

The IEEE 802.15.4 PHY coding scheme for the 2.4 GHz band uses pseudo-orthogonal codes where $k = 4$ bits are encoded together into an $n = 32$ chip sequence. As discussed in Section 5.2.2, the raw signalling is carried out using Offset-Quadrature-Phase-Shift-Keying with half-sine-shaping (OQPSK-HSS) at a rate of 2 $^{\text{Mchip}}/_{\text{s}}$. The code rate $r = {}^{k}/_{n} = {}^{1}/_{8}$ then results in a throughput of 250 kbps. Thus, the DSSS processing gain is $P_G = 10\log(\frac{1}{r}) \approx 9\,\text{dB}$.

Since symbols are encoded in phase, magnitude variations of the signal do not directly impact detection reliability. However, as intersymbol distances in the constellation diagram diminish with the carrier amplitude, the envelope depressions lead to errors (Section 5.2.3). A brief summary of the most significant experimental results we have accumulated follows, illustrating the limits of the link performance under CBI.

Wired Configuration

We use a combination of up to three nodes directly *wired* to the SDR. This guarantees controlled and repeatable settings, as well as channel-independent power levels from repeaters that reach the receiver. In our setup there are two receivers: the initiator and the SDR. Only if the initiator decodes the repeaters packet correctly can the Glossy cycle be completed, until the defined number of retransmissions [126]. Additionally, the power combiner introduces a constant power loss across the signal bandwidth and its proper impedance matching avoids reflections.

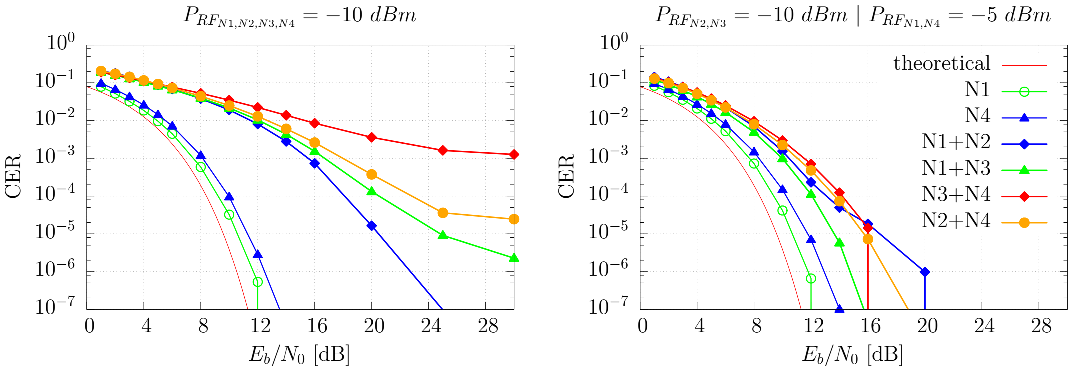


Figure 5.10: CER curves for single and two-node repeater combinations. The CER for pairs of nodes decreases for a 5-dB RF power imbalance. Each point in the graph is computed from 9.4×10^4 frames, 16 byte each. A 40-dB power attenuator fixes path loss to resemble a non-delay and non-multipath channel. Some curves were removed for clarity.

Figure 5.10 shows CER curves for single- and two-repeater combinations. All three-node combinations produce error rates well above 10^{-1} and are not shown. For pairs of nodes, we obtain a family of curves with varied and generally poor link performance. We observe a correlation between error rate and power (P_{RF}) imbalance. We show two power configurations: (i) all repeaters use $P_{RF} = -5$ dBm and (ii) decrease one repeater to $P_{RF} = -10$ dBm. As we raise the power imbalance by 5 dB, the link performance increases. Note that 5 dBm is the minimum power step the nodes allow.

The figure also shows that power imbalance moves the curves towards the minimum theoretically attainable error rate and near the single-repeater curve. We can relate this result with the ameliorated beating effect brought about by a larger power imbalance. Note that having different amplitudes in equation (5.11) is better than having similar ones, as the depth of the undulations in the composite signal corresponds to such amplitude imbalance. The smaller the amplitude imbalance the deeper the signal's envelope depression.

Wireless Configuration

We assess to what extent channel diversity could help reduce error rates. Figure 5.11 shows CER and SER for up to eight repeaters. For the two-node curve an E_b/N_0 of 16 dB is needed to maintain a minimum SER of 10^{-4}, a 12 dB difference relative to one repeater. For the cases of four and eight repeaters, both error rates remain above 10^{-1}. This experimental result indicates the channel diversity gain is limited for highly correlated indoor wireless channels. Unfortunately, these are very common settings for wireless sensor network deployments.

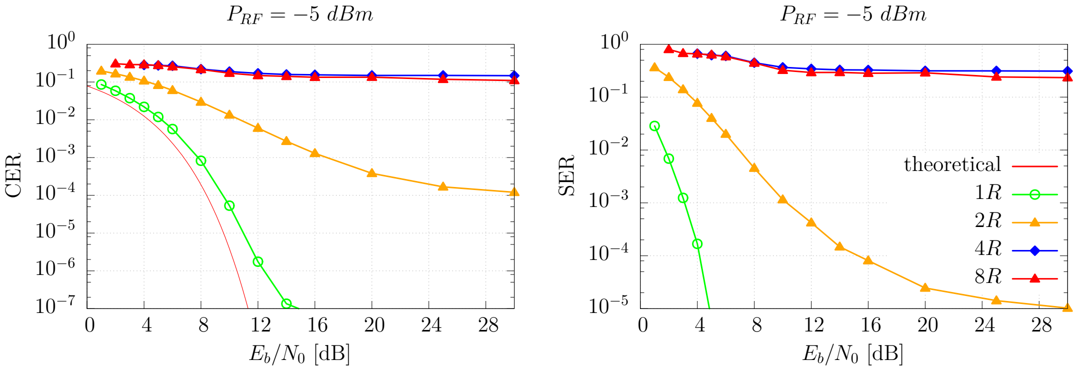


FIGURE 5.11: CBI among up to eight repeater nodes after symbols traverse a highly correlated indoor wireless channel. Each point in the graph is computed from 4.8×10^4 frames, 8 byte each. The theoretical curve, as derived in [1, Section 6.1.2], is shown for CER only.

Furthermore, we estimate the *pdf* of the baseband signal's envelope. The results are shown in figure 5.12. As the number of repeaters increases, the envelope's histogram spreads, showing a large range of amplitude observations. Besides making the signal vulnerable to noise as previously discussed, the composite signal demands a high dynamic range on the receiver. As there is not an automatic gain control (AGC) on the B210 board, signal clipping may occur as more repeaters are added. We make sure the SDR operates in linear mode, hence the large error rates in figure 5.11 are exclusively due to the depressions in the composite signal. Note that the two-repeater curve in figure 5.12 recreates the behaviour described by equation (5.11). The rate of change of the cosine function that describes the envelope's undulations is lower on the extreme values, which explains the two peaks in the histogram.

5.4 Summary

CBI is a useful technique to boost link reliability in low-power networks and constitutes a key technique toward enabling deterministic low-power network operation. However,

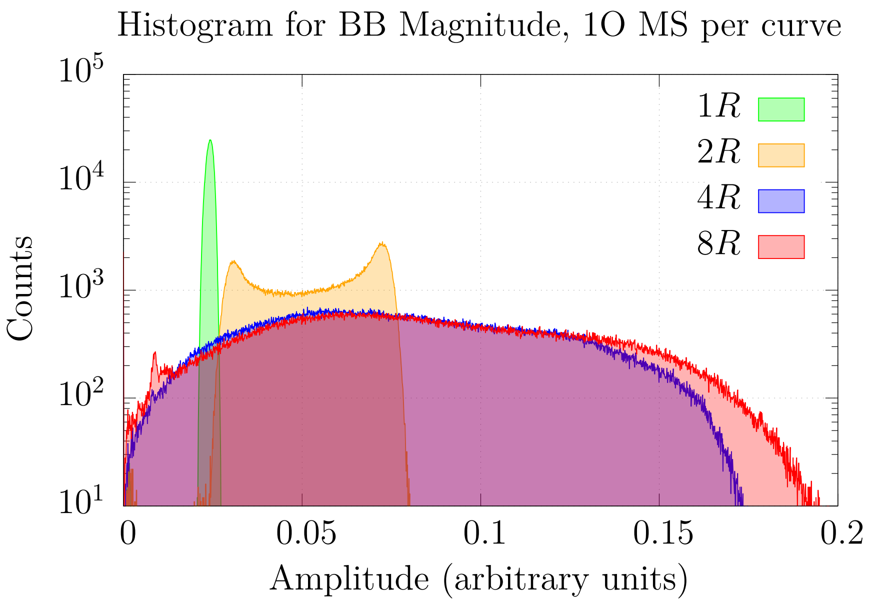


FIGURE 5.12: Amplitude observations in the magnitude of the signal spread as the number of repeaters increases. Although the magnitude contains no information, the lower-end observations become vulnerable to noise, compromising link quality.

we have shown that link quality under CBI does not scale with the number of repeaters due to lack of coherence among multisource carriers. Specifically, the link layer reliability is affected by emerging fast fading in the composite channel, wherever capture effect is absent. Thus, we find a fundamental limitation that potentially impacts all concurrent transmissions and puts a high demand for dynamic range in the receivers. Commercial transceiver chip implementations feature greater receiver sensitivity than the SDR board used in these experiments, and use an AGC that reacts to (not very fast) envelope depressions by increasing the gain in the receiver's signal chain. Combined, these attributes can improve the link quality, e.g. as reported by Ferrari et al. in [126, figure 12]. However, we suspect this is effective for a low-noise channel only, since amplification cannot improve SNR. Further experimentation is needed to understand the interaction between the composite signal and the AGC response in existing radio transeivers. Even in the absence of noise, a relatively large AGC's response time may prevent correct reception for a small enough coherence times in the composite channel.

Doddavenkatappa et al. orchestrate multichannel transmissions to sustain a packet pipeline while flooding the network [129, 130]. Multichannel operation expands the degrees of freedom and time diversity increases probability of reception, but open questions remain in regard to suitable repeater selection for effective network flooding, i.e., guaranteeing power imbalance in all receivers, for enhanced performance. A power allocation optimization framework to enhance the RF power imbalance in all nodes across the network is an interesting approach whose feasibility is yet to be investigated. It may also be relevant to look into the security benefits of a power allocation that include jamming nodes inside the network to make eavesdropping difficult or impossible far from the intended spatial destination.

An alternative solution to the composite signal depressions is to introduce channel diversity gain in the PHY layer, using space-time codes [141], which would be suitable for low-power design. However, its usage requires access to the PHY layer for precoding the baseband signal, what is not possible if the radio transceiver's baseband processing modules are implemented in hardware, as in most COTS radio transceivers chips existing in the market. The space-time code implementation requires either an SDR platform or low-power radio chips with flexible baseband processing in software. Unfortunately, the chips were introduced only recently by companies like Nordic Semiconductors (e.g. the SoftDevices for nRF51XXX series SoC) and Silicon Labs (the promising EFR32 series SoC, which at the time of writing have not been yet released to the market) [32].

Chapter 6

Conclusions

This dissertation focuses on radio interference in low-power wireless networks, it presents four interrelated topics and details several aspects of our contributions in each.

Firstly, repeatable interference generation is addressed in order to experiment with low-power wireless networks (LPWN) protocols, measure its impact on protocols performance, benchmark protocols under realistic and controlled interference as well as assist in the design of new ones. Thus, we present JamLab, a low-cost solution to augment testbeds with interference generation capabilities.

Secondly, we propose a novel quality metric for the wireless channel—dubbed CQ—which meaningfully quantifies the channel condition under interference to assist in mitigation strategies. Our metric has a strong correlation with packet reception rate (PRR) but accounts for interference only, its based on channel availability over time and is agnostic to the interference source. Moreover, there is no need for packet transmissions as our metric relies exclusively on energy detection in the channel. Therefore, measuring/computing CQ has no side effect on the channel and scales well with node density.

Thirdly, we use our CQ metric to study dynamic packet size adaptation and the application of erasure codes for optimizing reliability, energy consumption and throughput. Based on measurement data collected from a building containing several Wi-Fi networks, we showed that for moderate and low interference levels, increasing the packet size to a few hundred bytes, i.e. beyond the limit specified in the IEEE 802.15.4 standard, can lead to significant improvements in network performance. We also show that erasure codes drastically improve energy-efficiency and throughput of low-power wireless links, remaining cost-effective for large payload sizes, e.g., 1000–1500 bytes.

Fourthly, we investigate constructive baseband interference CBI—a useful technique to boost link reliability in low-power networks—a key technique recently introduced to provide deterministic low-power network operation. We show that link quality under CBI does not scale with the number of repeaters due to lack of coherence among multisource carriers. Thus, we find a fundamental limitation that potentially impacts concurrent transmissions under CBI, which requires further experimentation to understand the extent at which the composite signal remains readable in existing radio transceivers and possible solutions for the worst-case scenarios. Even more critical, interference from other networks may prevent correct reception due to the vulnerability of the composite signal and small coherence times in the composite channel. It may also be relevant to look into the security benefits of a power allocation that include jamming nodes inside the network to make eavesdropping difficult or impossible far from the intended spatial destination.

Contrary to other wireless networks, LPWN put emphasis in energy efficiency and nodes use low-cost hardware. These constrains posse additional challenges to maintain reliability and predictability in the network performance. While sophisticated signal processing is often used in other networks, it requires richer computation resources than what is typical in LPWN nodes. Thus, there is a need for innovation in new techniques that provides necessary performance metrics to extend the application of LPWN into critical infrastructure monitoring and control within the evolving Internet. Permitting the next wave of grows of the Internet to connect the physical world and reach domains such as sustainable transportation, agriculture, healthcare among others. New research directions consider energy harvesting techniques and novel radio interfaces which suits some of these scenarions.

Future work include: (i) online evaluation of our channel quality metric (CQ) metric for resource allocation techniques and performance trade-off in next generation low-power radio designs and (ii) effect of external interference on the composite signal under CBI. Both constitute revant use cases for JamLab and can contribute to better understand the requirements for future low-end spectrum sensing and radio adaptation techniques for interference-aware protocols operating in unlicensed spectrum.

Appendix A

Noise Generation

The study of noise and its effects on communication systems is based on the mathematical theory of random processes. What we observe physically is a noise waveform $X(t)$, which can be model as collection of random variables, one for each time instant t. This collection of random variables is called a *random process*.

Noise in the wireless channel is often modelled as an additive white Gaussian noise (AWGN). Although white noise implies an infinite bandwidth—i.e. including all frequency components in the spectrum—, in any practical scenario the channel is bandwidth limited. Moreover, the amplitude in the time domain has a *normal distribution*. Therefore, noise does not have a maximum amplitude. Instead, the noise amplitude is probabilistic in nature and can take any arbitrary value, with the corresponding probabilities.

In this appendix, we derive an expression for the noise variance σ^2 of the associated normal distribution required to obtain a range of normalised (${}^{Eb}\!/_{No}$) signal-to-noise ratios (SNR) desired for our experiments. The resulting σ^2 is then used in a GNU Radio [140] channel module developed for this purpose, which is described in Chapter 5. Thus, we need to express noise variance σ^2 as a function of the given signal's peak amplitude, the bandwidth of the IEEE 802.15.4 channel and the desired ${}^{Eb}\!/_{No}$.

Let the normalised SNR be expressed as a function of the energy corresponding to one data bit (E_b) and the noise spectral density N_o:

$$SNR = {}^{E_b}\!/_{N_o} \tag{A.1}$$

This energy-per-bit E_b can be expressed for the OQFSK-HSS (or MSK) signal in terms of its peak amplitude (A) and its frequency (f_c) as follows:

$$E_b = {}^{A^2}\!/_{4f_c} \tag{A.2}$$

Let noise be modelled as a zero-mean Wide-Sense Stationary (WSS) random processes $X(t)$, assumed to exist in the input of a linear time-invariant system (impulse response $h(t)$ and transfer function $H(f)$), with power spectral density proportional to $|H(f)|^2$ and constant of proportionality ${}^{N_o}\!/_2$—the two-sided power spectral density of the white noise—, which is the value of the power spectral density of the white noise process for all frequencies, $-\infty < f < \infty$. Then, it can be shown the following relation holds:

$$\sigma^2_{X(t)} = \frac{N_o}{2}\int_{-\infty}^{\infty} |h(t)|^2 \mathrm{d}t = \frac{N_o}{2}\int_{-\infty}^{\infty} |H(t)|^2 \mathrm{d}f \tag{A.3}$$

The reader is invited to see a formal treatment of WSS random processes by Pramod Viswanath in [142, Appendix A].

In the case of white noise in a flat frequency response systems, with finite bandwidth B, the transfer function is $|H(t)| = 1$ and, thus, the integral in equation A.3 results in:

$$\sigma = \sqrt{{}^{N_o B}\!/_2} \tag{A.4}$$

Now, substituting equation A.2 into equation A.1, replacing the resulting N_o into equation A.4, we obtain the following expression, where SNR is expressed in dB:

$$\sigma = \sqrt{{}^{A^2 B}\!/_{8 f_c 10^{(SNR_{dB}/10)}}} \tag{A.5}$$

The baseband carrier frequency for IEEE 802.15.4 [6] corresponds to $f_c = 500$ kHz or equivalently the chip duration is $T_c = 10^{-6}$ s. While we are sampling the baseband signal at a sampling rate of 4 Msps, we limit the noise bandwidth to the 802.15.4 system. The spectral footprint of the OQFSK-HSS signal falls off about $(0.75 f_c T_c)$, resulting in $B = 1.5 * 500$ kHz $= 750$ kHz. The power spectra for OQFSK-HSS (or MSK) signal can be found in [143, figure 6.9].

Thus, the required value of σ for our channel module can be obtained as follows:

$$\sigma = {}^{A}\!/\!\sqrt{({}^{16}\!/_{3})10^{-(SNR_{dB}/10)}} \tag{A.6}$$

Our module emulates an AWGN wireless channel adding the necessary level of noise power to satisfy the input parameter SNR, based on the signal's magnitude peak values which is dynamically measured internally.

A radio receiver's AGC adjusts gain to avoid non-linearities and maintain high resolution sampling across the amplifier chain, prior to the ADC stage. We consider that the AGC treat signals and noise equally, if they are changing faster than the AGC's response time.

A phase modulated signal has average-to-peak magnitude ratio near one. However, signals whose magnitude average-to-peak ratios are lower—e.g. due to carrier beating—will lend themselves to more errors, regardless of their (average or peak) magnitudes.

Therefore, using the signal's magnitude peak values as the reference to sinthetise noise is conducive to a fair comparison among different signals in our experiments.

Bibliography

[1] Andrea Goldsmith. *Wireless Communications.* Cambridge Univ. Press, NY, USA, 2005.

[2] Jean-Philippe Vasseur and Adam Dunkels. *Interconnecting Smart Objects with IP: The Next Internet.* Morgan Kaufmann, Burlington, MA, 1 edition, June 2010. ISBN 9780123751652.

[3] The Internet of Things. *MIT Technology Review - Business Report*, August 2014. URL http://www.technologyreview.com/businessreport/the-internet-of-things/free/.

[4] Gershon Dublon and Joseph A. Paradiso. Extra sensory perception. *Scientific American*, 311(1):36–41, July 2014. ISSN 0036-8733. doi: 10.1038/scientificamerican0714-36. URL http://www.nature.com/scientificamerican/journal/v311/n1/full/scientificamerican0714-36.html.

[5] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless Sensor Network Survey. *Comput. Netw.*, 52(12):2292–2330, August 2008. ISSN 1389-1286. doi: 10.1016/j.comnet.2008.04.002. URL http://dx.doi.org/10.1016/j.comnet.2008.04.002.

[6] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).* IEEE 802.15.4 Working Group, rev. 802.15.4-2006 edition, September 2006.

[7] Koen Langendoen. Medium access control in wireless sensor networks. *Medium access control in wireless networks*, 2:535–560, 2008. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7952&rep=rep1&type=pdf.

[8] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung. MAC Essentials for Wireless Sensor Networks. *IEEE Communications Surveys Tutorials*, 12(2):222–248, 2010. ISSN 1553-877X. doi: 10.1109/SURV.2010.020510.00058.

[9] Pardeep Kumar. *Medium access control protocols for energy and delay efficient applications of wireless sensor networks.* PhD thesis, Freie Universität Berlin, Germany, 2012. URL http://www.diss.fu-berlin.de/diss/receive/FUDISS_thesis_000000037320?lang=en.

[10] Vibhav KumarSachan, Syed Akhtar Imam, and M. T. Beg. Energy-Efficient Communication Methods in Wireless Sensor Networks: A Critical Review. *International Journal of Computer Applications*, 39(17):35–48, February 2012. ISSN 09758887. doi: 10.5120/4915-7484. URL http://research.ijcaonline.org/volume39/number17/pxc3877484.pdf.

[11] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3):537–568, 2009. URL http://www.sciencedirect.com/science/article/pii/S1570870508000954.

[12] Wei Ye, J. Heidemann, and D. Estrin. An energy-efficient MAC protocol for wireless sensor networks. In *IEEE INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*, volume 3, pages 1567–1576 vol.3, 2002. doi: 10.1109/INFCOM.2002.1019408.

[13] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 95–107, New York, NY, USA, 2004. ACM. ISBN 1-58113-879-2. doi: 10.1145/1031495.1031508. URL http://doi.acm.org/10.1145/1031495.1031508.

[14] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard Han. X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, SenSys '06, pages 307–320, New York, NY, USA, 2006. ACM. ISBN 1-59593-343-3. doi: 10.1145/1182807.1182838. URL http://doi.acm.org/10.1145/1182807.1182838.

[15] David Moss and Philip Levis. BoX-MACs: Exploiting physical and link layer boundaries in low-power networking. *Stanford, Tech. Rep.*, 2008. URL http://coronet2010.stanford.edu/pubs/sing-08-00.pdf.

[16] Anthony Rowe, Vikram Gupta, and Ragunathan (Raj) Rajkumar. Low-power clock synchronization using electromagnetic energy radiating from AC power lines. In *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, SenSys '09, pages 211–224, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-519-2. doi: 10.1145/1644038.1644060. URL http://doi.acm.org/10.1145/1644038.1644060.

[17] Tijs van Dam and Koen Langendoen. An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03, pages 171–180, New York, NY, USA, 2003. ACM. ISBN 1-58113-707-9. doi: 10.1145/958491.958512. URL http://doi.acm.org/10.1145/958491.958512.

[18] Wei Ye, J. Heidemann, and D. Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 12(3):493–506, June 2004. ISSN 1063-6692. doi: 10.1109/TNET.2004.828953.

[19] G. Lu, B. Krishnamachari, and C.S. Raghavendra. An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*, pages 224–, April 2004. doi: 10.1109/IPDPS.2004.1303264.

[20] P.P. Czapski. A Survey: MAC Protocols For Applications Of Wireless Sensor Networks. In *TENCON 2006. 2006 IEEE Region 10 Conference*, pages 1–4, November 2006. doi: 10.1109/TENCON.2006.343847.

[21] Henry Goldberg. Grazing on the commons: the emergence of part 15. *info*, 11 (5):72–75, August 2009. ISSN 1463-6697. doi: 10.1108/14636690910989351. URL http://www.emeraldinsight.com/doi/abs/10.1108/14636690910989351.

[22] Kevin J. Negus and Al Petrick. History of wireless local area networks (WLANs) in the unlicensed bands. *info*, 11(5):36–56, August 2009. ISSN 1463-6697. doi: 10.1108/14636690910989324. URL http://www.emeraldinsight.com/doi/abs/10.1108/14636690910989324.

[23] Vic Hayes and Wolter Lemstra. Licence-exempt: the emergence of wi-fi. *INFO*, 11 (5):57–71, August 2009. ISSN 1463-6697. doi: 10.1108/14636690910989333. URL http://www.emeraldinsight.com/doi/full/10.1108/14636690910989333.

[24] Charles Jackson, Raymond Pickholtz, and Dale Hatfield. Spread spectrum is good-but it does not obsolete NBC v. US. *Fed. Comm. LJ*, 58: 245, 2006. URL http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/fedcom58&section=16.

[25] Kenneth R. Carter. Unlicensed to kill: a brief history of the part 15 rules. *info*, 11 (5):8–18, August 2009. ISSN 1463-6697. doi: 10.1108/14636690910989306. URL http://www.emeraldinsight.com/doi/abs/10.1108/14636690910989306.

[26] A. Sikora and V.F. Groza. Coexistence of IEEE802.15.4 with other systems in the 2.4 GHz-ISM-band. In *Proceedings of the IEEE Instrumentation and Measurement*

Technology Conference, 2005. IMTC 2005, volume 3, pages 1786–1791, May 2005. doi: 10.1109/IMTC.2005.1604479.

[27] M. Petrova, Lili Wu, P. Mahonen, and J. Riihijarvi. Interference measurements on performance degradation between colocated IEEE 802.11g/n and IEEE 802.15.4 networks. In *Sixth International Conference on Networking, 2007. ICN '07*, pages 93–93, April 2007. doi: 10.1109/ICN.2007.53.

[28] G. Thonet, P. Allard-Jacquin, and P. Colle. ZigBee-WiFi coexistence. Technical report, 37 Quai Paul Louis Merlin, Grenoble, France, April 2008.

[29] H. Khaleel, C. Pastrone, F. Penna, M.A. Spirito, and R. Garello. Impact of wi-fi traffic on the IEEE 802.15.4 channels occupation in indoor environments. In *International Conference on Electromagnetics in Advanced Applications, 2009. ICEAA '09*, pages 1042–1045, September 2009. doi: 10.1109/ICEAA.2009.5297781.

[30] Raja Jurdak, Kevin Klues, Brano Kusy, Christian Richter, Koen Langendoen, and Michael Brunig. Opal: A multiradio platform for high throughput wireless sensor networks. *Embedded Systems Letters, IEEE*, 3(4):121–124, 2011. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6086565.

[31] JeongGil Ko, Kevin Klues, Christian Richter, Wanja Hofer, Branislav Kusy, Michael Bruenig, Thomas Schmid, Qiang Wang, Prabal Dutta, and Andreas Terzis. Low power or high performance? a tradeoff whose time has come (and nearly gone). In *Wireless Sensor Networks*, pages 98–114. Springer, 2012. URL http://link.springer.com/chapter/10.1007/978-3-642-28169-3_7.

[32] Energy Micro. Energy Friendly Radios: EFR4D2090 Datasheet. http://www.energymicro.com/draco, June 2012. Confidential/Preliminary, Provided as Registered Copy.

[33] Sándor Szilvási, Benjámin Babják, Péter Völgyesi, and Ákos Lédeczi. Marmote SDR: Experimental platform for low-power wireless protocol stack research. *Journal of Sensor and Actuator Networks*, 2(3):631–652, September 2013. doi: 10.3390/jsan2030631. URL http://www.mdpi.com/2224-2708/2/3/631.

[34] Teemu Laukkarinen, Jukka Suhonen, and Marko Hännikäinen. A Survey of Wireless Sensor Network Abstraction for Application Development. *International Journal of Distributed Sensor Networks*, 2012:e740268, December 2012. ISSN 1550-1329. doi: 10.1155/2012/740268. URL http://www.hindawi.com/journals/ijdsn/2012/740268/abs/.

[35] V.C. Gungor and G.P. Hancke. Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches. *IEEE Transactions on Industrial*

Electronics, 56(10):4258–4265, October 2009. ISSN 0278-0046. doi: 10.1109/TIE.2009.2015754.

[36] O. Chipara, Chengjie Wu, Chenyang Lu, and W. Griswold. Interference-Aware Real-Time Flow Scheduling for Wireless Sensor Networks. In *2011 23rd Euromicro Conference on Real-Time Systems (ECRTS)*, pages 67–77, July 2011. doi: 10.1109/ECRTS.2011.15.

[37] A. Saifullah, You Xu, Chenyang Lu, and Yixin Chen. Priority Assignment for Real-Time Flows in WirelessHART Networks. In *2011 23rd Euromicro Conference on Real-Time Systems (ECRTS)*, pages 35–44, July 2011. doi: 10.1109/ECRTS.2011.12.

[38] A.A. Kumar Somappa, K. Øvsthus, and L.M. Kristensen. An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges. *IEEE Communications Surveys Tutorials*, 16(3):1391–1412, 2014. ISSN 1553-877X. doi: 10.1109/SURV.2014.012114.00058.

[39] Jaime Chen, Manuel Díaz, Luis Llopis, Bartolomé Rubio, and José M. Troya. A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection. *Journal of Network and Computer Applications*, 34(4):1225–1239, July 2011. ISSN 1084-8045. doi: 10.1016/j.jnca.2011.01.008. URL http://www.sciencedirect.com/science/article/pii/S1084804511000257.

[40] R. Sumathi and M.G. Srinivas. A Survey of QoS Based Routing Protocols for Wireless Sensor Networks. *Journal of Information Processing Systems*, 8(4):589–602, December 2012. ISSN 1976-913X. doi: 10.3745/JIPS.2012.8.4.589. URL http://koreascience.or.kr/journal/view.jsp?kj=E1JBB0&py=2012&vnc=v8n4&sp=589.

[41] Theodore Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2nd edition, 2001. ISBN 0130422320.

[42] M. Zuniga and B. Krishnamachari. Analyzing the transitional region in low power wireless links. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004*, pages 517–526, October 2004.

[43] Carlo Alberto Boano, Thiemo Voigt, Claro Noda, Kay Römer, and Marco Zúñiga. JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation. In *Proc. of the 10th Conf. on Information Processing in Sensor Networks (IPSN)*, pages 175–186, Chicago, USA, April 2011.

[44] Nouha Baccour, Daniele Puccinelli, Thiemo Voigt, Anis Koubaa, Claro Noda, Hossein Fotouhi, Mario Alves, Habib Youssef, Marco Antonio Zuniga, Carlo Alberto Boano, and Kay Römer. External radio interference. In *Radio Link Quality Estimation in Low-Power Wireless Networks*, SpringerBriefs in Electrical and Computer Engineering, pages 21–63. Springer International Publishing, January 2013. ISBN 978-3-319-00773-1, 978-3-319-00774-8. URL http://link.springer.com/chapter/10.1007/978-3-319-00774-8_2.

[45] Claro Noda, Shashi Prabh, Mário Alves, Carlo Alberto Boano, and Thiemo Voigt. Quantifying the Channel Quality for Interference-Aware Wireless Sensor Networks. In *International Workshop on Real-Time Networks (RTN)*, June 2011.

[46] C. Noda, S. Prabh, M. Alves, and T. Voigt. On packet size and error correction optimisations in low-power wireless networks. In *2013 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 212–220, June 2013. doi: 10.1109/SAHCN.2013.6644980.

[47] Claro A Noda, Carlos Pérez-Penichet, Balint Seeber, Marco Zennaro, Mário Alves, and Adriano Moreira. On the scalability of constructive interference in Low-Power wireless networks. In *12th European Conference on Wireless Sensor Networks (EWSN'15)*, Porto, Portugal, February 2015.

[48] F. Ferrari, M. Zimmerling, L. Thiele, and O. Saukh. Efficient network flooding and time synchronization with glossy. In *2011 10th International Conference on Information Processing in Sensor Networks (IPSN)*, pages 73–84, April 2011.

[49] Nouha Baccour, Anis Koubâa, Claro Noda, Hossein Fotouhi, Mário Alves, Habib Youssef, Marco Antonio Zúñiga, Carlo Alberto Boano, Kay Römer, Daniele Puccinelli, Thiemo Voigt, and Luca Mottola. *Radio Link Quality Estimation in Low-Power Wireless Networks.* SpringerBriefs in Electrical and Computer Engineering. Springer International Publishing, Heidelberg, 2013. ISBN 978-3-319-00773-1, 978-3-319-00774-8. URL http://link.springer.com/10.1007/978-3-319-00774-8.

[50] Claro Noda, Shashi Prabh, Mário Alves, Carlo Alberto Boano, and Thiemo Voigt. Quantifying the Channel Quality for Interference-aware Wireless Sensor Networks. *SIGBED Rev.*, 8(4):43–48, December 2011. ISSN 1551-3688. doi: 10.1145/2095256.2095262. URL http://doi.acm.org/10.1145/2095256.2095262.

[51] C. Noda, S. Prabh, C.A. Boano, T. Voigt, and M. Alves. Poster abstract: A channel quality metric for interference-aware wireless sensor networks. In *2011 10th*

International Conference on Information Processing in Sensor Networks (IPSN), pages 167–168, April 2011.

[52] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. Surviving wi-fi interference in low power ZigBee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, SenSys '10, pages 309–322, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0344-6. doi: 10.1145/1869983.1870014. URL http://doi.acm.org/10.1145/1869983.1870014.

[53] *Wireless LAN MAC and PHY Specifications*. IEEE 802.11 Working Group, IEEE std 802.11-2007 edition, June 2007.

[54] Ramakrishna Gummadi, David Wetherall, Ben Greenstein, and Srinivasan Seshan. Understanding and mitigating the impact of RF interference on 802.11 networks. In *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '07, pages 385–396, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-713-1. doi: 10.1145/1282380.1282424. URL http://doi.acm.org/10.1145/1282380.1282424.

[55] Shyamnath Gollakota, Fadel Adib, Dina Katabi, and Srinivasan Seshan. Clearing the RF smog: Making 802.11n robust to cross-technology interference. In *Proceedings of the ACM SIGCOMM 2011 Conference*, SIGCOMM '11, pages 170–181, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0797-0. doi: 10.1145/2018436.2018456. URL http://doi.acm.org/10.1145/2018436.2018456.

[56] Gang Zhou, John A. Stankovic, and Sang H. Son. Crowded Spectrum in Wireless Sensor Networks. In *in Proceedings of Third Workshop on Embedded Networked Sensors (EmNets)*, 2006.

[57] Carlo Alberto Boano, Thiemo Voigt, Nicolas Tsiftes, Luca Mottola, Kay Römer, and Marco Antonio Zúñiga. Making sensornet MAC protocols robust against interference. In *Wireless Sensor Networks*, pages 272–288. Springer, 2010. URL http://link.springer.com/chapter/10.1007/978-3-642-11917-0_18.

[58] M. Petrova et al. Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks. In *International Conference on Networking 2007*, .

[59] A. Sikora and V.F. Groza. Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-Band. In *IEEE Instrumentation and Measurement Technology*, May 2005.

[60] *Smart RF CC2420 datasheet - 2.4 GHz IEEE 802.15.4 / ZigBee-Ready RF Transceiver*. Texas Instruments, March 2007.

[61] A. Dunkels and B. Grönvall and T. Voigt. Contiki - a Lightweight and Flexible OS for Tiny Networked Sensors. In *EmNetS'04*.

[62] The Contiki Projects Community. http://sourceforge.net/projects/contikiprojects.

[63] Y. Liu et al. IEEE 802.11 WLANs WG Group Information doc. no. 802.11-10/1079r0, September 2010.

[64] P. Verkaik, Y. Agarwal, R. Gupta, and A. Snoeren. SoftSpeak: Making VoIP Play Fair in Existing 802.11 Deployments. In *NSDI'09*.

[65] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *2nd International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 95–107, Baltimore, MD, USA, November 2004.

[66] Anritsu MS2711D Spectr. Analyzer. http://www.anritsu.com.

[67] N. Tsiftes, A. Dunkels, Z. He, and T. Voigt. Enabling Large-Scale Storage in Sensor Networks with the Coffee File System. In *IPSN'09*.

[68] Q. Wang and T. Zhang. Source Traffic Modeling in WSN for Target Tracking. In *Proc. of the 5th ACM PE-WASUN*, 2008.

[69] A. Dunkels, F. Österlind, N. Tsiftes, and Z. He. Software-based on-line energy estimation for sensor nodes. In *Proc. of EmNets'07*.

[70] C.A. Boano et al. Controllable Radio Interference for Experimental and Testing Purposes in WSN. In *IEEE SenseApp 2009*, .

[71] C.A. Boano, K. Römer, Z. He, T. Voigt, M. Zuniga, and A. Willig. Generation of Controllable Radio Interference for Protocol Testing in Wireless Sensor Networks. In *SenSys'09, demo session*, .

[72] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard Han. X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Boulder, Colorado, USA, November 2006.

[73] Carlo Alberto Boano, Thiemo Voigt, Nicolas Tsiftes, Luca Mottola, Kay Römer, and Marco Zuniga. Making Sensornet MAC Protocols Robust Against Interference. In *Proceedings of the Seventh European Conference on Wireless Sensor Networks (EWSN), LNCS 5970*, pages 272–288, Coimbra, Portugal, February 2010. Springer Berlin Heidelberg.

[74] C.A. Boano, T. Voigt, N. Tsiftes, L. Mottola, K. Römer, and M. Zuniga. Making Sensornet MAC Protocols Robust Against Interference. In *EWSN'10*, .

[75] Kenneth R. Carter. Unlicensed to kill: a brief history of the Part 15 rules. *Info*, 11(5):8–18, 2009.

[76] Henry Goldberg. Grazing on the commons: the emergence of Part 15. *Info - The journal of policy, regulation and strategy for telecommunications*, 11(5):72–75, 2009.

[77] Vic Hayes and Wolter Lemstra. Licence-exempt: the emergence of Wi-Fi. *Info - The journal of policy, regulation and strategy for telecommunications*, 11(5):57–71, 2009.

[78] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50(13):2127 – 2159, 2006.

[79] Axel Sikora and Voicu F. Groza. Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-Band. In *IEEE Instrumentation and Measurement Technology*, pages 1786–1791, Ottawa, Canada, May 2005.

[80] Marina Petrova, Lili Wu, Petri Mahonen, and Janne Riihijarvi. Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks. In *International Conference on Networking (ICN)*, Sainte-Luce, Martinique, April 2007.

[81] Jan-Hinrich Hauer, Andreas Willig, and Adam Wolisz. Mitigating the Effects of RF Interference through RSSI-Based Error Recovery. In *Proc. of the 7th European Conference on Wireless Sensor Networks (EWSN)*, pages 224–239, Coimbra, Portugal, February 2010.

[82] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. Surviving Wi-Fi Interference in Low Power ZigBee Networks. In *Proceedings of the 8th Conference on Embedded Networked Sensor Systems (SenSys)*, Zurich, Switzerland, November 2010.

[83] T. Yucek and H. Arslan. A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications. *IEEE Communications Surveys Tutorials*, 11(1), 2009.

[84] Lance Doherty, William Lindsay, and Jonathan Simon. Channel-Specific Wireless Sensor Network Path Data. In *Proc. of the 16th Conf. on Computer Communications and Networks (ICCCN)*, pages 89–94, Honolulu, HI, USA, August 2007.

[85] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Channel surfing: defending wireless sensor networks from interference. In *Proc. of the 6th Conf. on Information*

Processing in Sensor Networks (IPSN), pages 499–508, Cambridge, MA, USA, April 2007.

[86] Luca Stabellini and Jens Zander. Energy-efficient detection of intermittent interference in wireless sensor networks. *International Journal of Sensor Networks*, 8 (1):27–40, 2010.

[87] R. Musaloiu-E. and A. Terzis. Minimising the effect of wifi interference in 802.15.4 wireless sensor networks. *International Journal of Sensor Networks (IJSNet)*, 3 (1):43–54, December 2007.

[88] K. Pister and L. Doherty. TSMP: Time synchronized mesh protocol. In T. F. Gonzalez, editor, *Proceedings of the 20th IASTED International Conference on Parallel and Distributed Computing and Systems*, Orlando, FL, USA, November 2008. ACTA Press.

[89] Youngmin Kim, Hyojeong Shin, and Hojung Cha. Y-MAC: An Energy-Efficient Multi-channel MAC Protocol for Dense Wireless Sensor Networks. In *Proceedings of the 7th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, St. Louis, Missouri, USA, April 2008.

[90] Joris Borms, Kris Steenhaut, and Bart Lemmens. Low-Overhead Dynamic Multichannel MAC for Wireless Sensor Networks. In *Proc. of the 7th European Conf. on Wireless Sensor Networks (EWSN)*, Coimbra, Portugal, February 2010.

[91] Mo Sha, Gregory Hackmann, and Chenyang Lu. ARCH: Practical Channel Hopping for Reliable Home-Area Sensor Networks. In *Proc. of the 17th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, Chicago, IL, USA, April 2011.

[92] Junaid Ansari and Petri Mähönen. Channel Selection in Spectrum Agile and Cognitive MAC Protocols for Wireless Sensor Networks. In *Proc. of the 8th Workshop on Mobility Management and Wireless Access (MobiWac)*, Bodrum, Turkey, October 2010.

[93] Kannan Srinivasan, Maria A. Kazandjieva, Saatvik Agarwal, and Philip Levis. The beta-factor: measuring wireless link burstiness. In *Proc. of the 6th Conference on Embedded Networked Sensor Systems (SenSys)*, pages 29–42, Raleigh, NC, USA, November 2008.

[94] S. Munir, S. Lin, E. Hoque, S. Nirjon, J. Stankovic, and K. Whitehouse. Addressing Burstiness for Reliable Communication and Latency Bound Generation in Wireless Sensor Networks. In *Proceedings of the 9th ACM/IEEE International Conference*

on Information Processing in Sensor Networks (IPSN), Stockholm, Sweden, April 2010.

[95] Daniel Halperin, Thomas Anderson, and David Wetherall. Taking the sting out of carrier sense: interference cancellation for wireless LANs. In *Proc. of the 14th International Conference on Mobile Computing and networking (MobiCom)*, pages 339–350, San Francisco, CA, USA, 2008.

[96] M. Vamshi Krishna, Xie Juan, M.A. Do, K.S. Yeo, and C.C. Boon. A low power fully programmable 1 MHz resolution 2.4 GHz CMOS PLL frequency synthesizer. In *Proc. of the 2nd IEEE Conference on Biomedical Circuits and Systems (BIOCAS)*, pages 187–190, Marrakech, Morocco, November 2007.

[97] Louis-François Tanguay and Mohamad Sawan. An ultra-low power ISM-band integer-n frequency synthesizer dedicated to implantable medical microsystems. *Analog Integr. Circuits Signal Process.*, 58:205–214, March 2009.

[98] Wu Xiushan, Wang Zhigong, Li Zhiqun, Xia Jun, and Li Qing. Design and realization of an ultra-low-power low-phase-noise CMOS LC-VCO. *Journal of Semiconductors*, 31(8):085007, 2010.

[99] Geng Zhiqing, Yan Xiaozhou, Lou Wenfeng, Feng Peng, and Wu Nanjian. A low power fast-settling frequency-presetting PLL frequency synthesizer. *Journal of Semiconductors*, 31(8):085002, 2010.

[100] Federico Penna, Claudio Pastrone, Maurizio Spirito, and Roberto Garello. Measurement-based Analysis of Spectrum Sensing in Adaptive WSNs under Wi-Fi and Bluetooth Interference. In *Proc. of the 69th Vehicular Technology Conference (VTC)*, Barcelona, Spain, April 2009.

[101] Guido Van Rossum. Python for Unix/C Programmers. In *Proc. of the NLUUG najaarsconferentie. Dutch UNIX users group*, 1993.

[102] Kaushik R. Chowdhury and Ian F. Akyildiz. Interferer Classification, Channel Selection and Transmission Adaptation for Wireless Sensor Networks. In *Proc. of the Conference on Communications (ICC)*, Dresden, Germany, June 2009.

[103] F. Hermans, O. Rensfelt, T. Voigt, E. Ngai, L. Larzon, and P. Gunningberg. SoNIC: Classifying Interference in 802.15.4 Sensor Networks. In *Proc. of the 12th ACM IPSN*, pages 55–66, Philadelphia, USA, April 2013.

[104] Nicholas M. Boers, Ioanis Nikolaidis, and Pawel Gburzynski. Sampling and Classifying Interference Patterns in a Wireless Sensor Network. *ACM Trans. Sen. Netw.*, 9(1):2:1–2:19, November 2012. ISSN 1550-4859.

[105] Mehmet C. Vuran and I. F. Akyildiz. Cross-layer Packet Size Optimization for Wireless Terrestrial, Underwater, and Underground Sensor Networks. In *Proc. of the 27th IEEE Conference on Computer Communications (INFOCOM)*, pages 226–230, Phoeniz, AZ, USA, April 2008.

[106] Jun Huang, Guoliang Xing, Gang Zhou, and Ruogu Zhou. Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance. In *Proc. of the The 18th IEEE ICNP*, Washington, DC, USA, 2010.

[107] Minyan Hong, Erik Björnemo, and Thiemo Voigt. Exploring sensor network communication strategies with the mote-in-the-loop approach. In *Proc. of the 14th WPMC*, October 2011.

[108] Y. Sankarasubramaniam, I. F. Akyildiz, and S. W. McLaughlin. Energy Efficiency Based Packet Size Optimization in Wireless Sensor Networks. In *Proc. of the 1st Workshop on Sensor Network Protocols and Applications*, June 2003.

[109] Shan Lin, Jingbin Zhang, Gang Zhou, Lin Gu, John A. Stankovic, and Tian He. ATPC: adaptive transmission power control for wireless sensor networks. In *Proc. of the 4th Conference on Embedded Networked Sensor Systems (SenSys)*, pages 223–236, Bolder, Colorado, USA, November 2006.

[110] Raja Jurdak, Kevin Klues, Brano Kusy, Christian Richter, Koen Langendoen, and Michael Brünig. Opal: A Multiradio Platform for High Throughput Wireless Sensor Networks. *Embedded Systems Letters*, pages 121–124, 2011.

[111] JeongGil Ko, Kevin Klues, Christian Richter, Wanja Hofer, Branislav Kusy, Michael Brünig, Thomas Schmid, Qiang Wang, Prabal Dutta, and Andreas Terzis. Low Power or High Performance? A Tradeoff Whose Time Has Come (and Nearly Gone). In *EWSN*, 2012.

[112] M. Goyal, S. Prakash, W. Xie, Y. Bashir, H. Hosseini, and A. Durresi. Evaluating the Impact of Signal to Noise Ratio on IEEE 802.15.4 PHY-Level Packet Loss Rate. In *Proc. of the 13th NBiS*, pages 279–284, Los Alamitos, CA, USA, 2010.

[113] Claro Noda, Shashi Prabh, Mário Alves, Carlo Alberto Boano, and Thiemo Voigt. Quantifying the Channel Quality for Interference-aware Wireless Sensor Networks. *ACM SIGBED Rev.*, 8:43–48, December 2011. ISSN 1551-3688.

[114] Claro Noda, Shashi Prabh, Mário Alves, Thiemo Voigt, and Carlo Alberto Boano. CRAWDAD data set cister/rssi (v. 2012-05-17). Downloaded from http://crawdad.cs.dartmouth.edu/cister/rssi, May 2012.

[115] J. Ammer and J. Rabacy. The energy-per-useful-bit metric for evaluating and optimizing sensor network physical layers. In *Proc. of the 3rd Annual IEEE SECON*, volume 2, sept. 2006.

[116] *Wireless LAN MAC and PHY Specifications*. IEEE 802.11 Working Group, ieee std 802.11-2007 edition, June 2007.

[117] C. Liang, N. Priyantha, J. Liu, and A. Terzis. Surviving Wi-Fi Interference in Low Power ZigBee Networks. In *SenSys'10*.

[118] Ramakrishna Gummadi, David Wetherall, Ben Greenstein, and Srinivasan Seshan. Understanding and mitigating the impact of RF interference on 802.11 networks. In *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 385–396, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-713-1. doi: http://doi.acm.org/10.1145/1282380.1282424.

[119] C. A. Boano, T. Voigt, C. Noda, K. Römer, and M. Zúñiga. JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation. In *Proc. of the 10th IPSN*, pages 175–186, Chicago, USA, April 2011.

[120] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), September 2007. URL http://www.ietf.org/rfc/rfc4944.txt. Updated by RFC 6282.

[121] N. Kushalnagar, G. Montenegro, and C. Schumacher. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919 (Informational), August 2007. URL http://www.ietf.org/rfc/rfc4919.txt.

[122] S. Reiger. Codes for the Correction of 'Clustered' Errors. *Information Theory, IRE Transactions on*, 6(1):16 –21, march 1960. ISSN 0096-1000.

[123] Shu Lin and Daniel J. Costello. *Error Control Coding, Second Edition*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2004. ISBN 0130426725.

[124] Prabal Dutta, Stephen Dawson-Haggerty, Yin Chen, Chieh-Jan Mike Liang, and Andreas Terzis. Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless. In *ACM SenSys*, Zurich, Switzerland, 2010.

[125] Hariharan Rahul, Haitham Hassanieh, and Dina Katabi. SourceSync: A Distributed Wireless Architecture for Exploiting Sender Diversity. In *ACM SIGCOMM 2010*, New Delhi, India, August 2010.

[126] Federico Ferrari, Marco Zimmerling, Lothar Thiele, and Olga Saukh. Efficient Network Flooding and Time Synchronization with Glossy. In *ACM/IEEE IPSN*, Chicago, IL, USA, April 2011.

[127] Prabal Dutta, Stephen Dawson-Haggerty, Yin Chen, Chieh-Jan Mike Liang, and Andreas Terzis. Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless. In Jan Beutel, Deepak Ganesan, and Jack A. Stankovic, editors, *SenSys*, pages 1–14. ACM, 2010. ISBN 978-1-4503-0344-6.

[128] Federico Ferrari, Marco Zimmerling, Luca Mottola, and Lothar Thiele. Low-power wireless bus. SenSys, New York, NY, USA, 2012. ACM.

[129] Manjunath Doddavenkatappa, Mun Choon Chan, and Ben Leong. Splash: Fast data dissemination with constructive interference in wireless sensor networks. In *USENIX NSDI'13*, Lombard, IL, 2013.

[130] Manjunath Doddavenkatappa and Mun Choon. P3: A practical packet pipeline using synchronous transmissions for sensor networks. In *ACM/IEEE IPSN*, 2014.

[131] Yin Wang, Yuan He, XuFei Mao, Yunhao Liu, Zhiyu Huang, and Xiang-Yang Li. Exploiting Constructive Interference for Scalable Flooding in Wireless Networks. In *IEEE INFOCOM*, Orlando, FL, USA, 2012.

[132] Aveek Dutta, Dola Saha, Dirk Grunwald, and Douglas Sicker. SMACK: A SMart ACKnowledgment scheme for broadcast messages in WLANs. In *ACM SIGCOMM*, NY, USA, 2009.

[133] Scinance Analytics Y Maghsoodi. Exact amplitude distributions of sums of stochastic sinusoidals. 2008.

[134] Kameswari Chebrolu, Bhaskaran Raman, Nilesh Mishra, Phani Kumar Valiveti, and Raj Kumar. Brimon: A sensor network system for railway bridge monitoring. ACM MobiSys, NY, USA, 2008.

[135] Joseph Polastre, Robert Szewczyk, and David Culler. Telos: Enabling ultra-low power wireless research. In *ACM/IEEE IPSN*, Piscataway, NJ, USA, 2005.

[136] Ettus Research. USRP B200/B210 Bus Series Product Overview. URL `http://goo.gl/WOYLmQ`. (Accessed: 22.09.2014).

[137] K. Leentvaar and J. Flint. The Capture Effect in FM Receivers. *IEEE Transactions on Communications*, 24(5):531–539, May 1976. ISSN 0090-6778. doi: 10.1109/TCOM.1976.1093327.

[138] A A M Saleh and R.A Valenzuela. A statistical model for indoor multipath propagation. *IEEE Journal on Selected Areas in Communications*, 5(2):128–137, February 1987. ISSN 0733-8716.

[139] Bastian Bloessl, Christoph Leitner, Falko Dressler, and Christoph Sommer. A GNU Radio-based IEEE 802.15. 4 Testbed. *12. GI/ITG FACHGESPRÄCH SENSORNETZE*, 2013.

[140] GNU Radio Website, accessed September 2014. URL http://www.gnuradio.org.

[141] Hamid Jafarkhani. A quasi-orthogonal space-time block code. *IEEE Transactions on Communications*, 49(1), January 2001.

[142] Pramod Viswanath. *ECE 361: Lecture 3*. University of Illinois, 2011. URL https://goo.gl/be3v15. Accessed: 2015-05-25.

[143] Simon Haykin. *Communication Systems*. Wiley Publishing, 5th edition, 2009. ISBN 0471697907, 9780471697909.