Wireless Coexistence for Spectrum Sharing

Hossein-Ali Safavi-Naeini

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2016

Sumit Roy, Chair

Thomas R. Henderson

James Ritcey

Program Authorized to Offer Degree:
Electrical Engineering

University of Washington

Abstract

Wireless Coexistence for Spectrum Sharing

Hossein-Ali Safavi-Naeini

Chair of the Supervisory Committee:
Professor Sumit Roy
Electrical Engineering

Much of the spectrum licensed for usage by the regulatory authorities remains idle or heavily underutilized [28]. By allowing opportunistic access to these dormant resources, spectrum sharing promises to dramatically boost the supply of spectrum that is available for high bandwidth wireless communications. This shared access arrangement will lead to the expected coexistence of multiple wireless systems within the same frequency band giving rise to the study undertaken in this dissertation. Throughout this work, we place a high emphasis on solutions that require minimal disturbance to wireless communication standards in order to streamline their implementation and accelerate their adoption.

Our work begins by considering TV Whitespaces (TVWS) which were the first major instance of spectrum sharing to be considered. We look at adapting the 802.11 WLAN standard for operation in TVWS bands by incorporating sensing into the Wi-Fi MAC layer. We use this study to explore the potential of Software Defined Radio systems and the role they play in spectrum sharing systems while identifying the challenges and pitfalls inherent in such implementations.

Our focus then shifts to spectrum sharing in radar bands. First, we aim to shrink the exclusion regions (as defined by the NTIA in [25]) by inheriting from the techniques developed for TVWS. The key outcome of this work is to provide an analytic framework for the selection of Wi-Fi parameters than can deliver the desired radar protection performance.

This framework supports the aim of maximum spectrum utilization by reducing the areas which are deprived of shared access to radar spectrum.

The last major result in this dissertation is a detailed study into the impact of radars on communication systems. We present what is to our knowledge the first detailed look at the physical layer obstacles that hinder network throughput for devices deployed in radar bands. Looking at the two major broadband standards (IEEE 802.11 WLAN and 3GPP LTE), we identify vulnerabilities that would render networks inoperable in close proximity to radars before providing effective solutions to recover the desired performance. The line of investigation in this thesis furnishes some of the solutions that are necessary for the future success of spectrum sharing systems.

TABLE OF CONTENTS

LIST OF FIGURES

GLOSSARY

ACK: The acknowledgment message

AGC: Automatic Gain Control

AP: Access Point

AWGN: Additive White Gaussian Noise

BCC: Binary Convolutional Coding

BER: Bit Error Rate

CA: Collision Avoidance

CFO: Carrier Frequency Offset

CLT: Central Limit Theorem

CSMA: Carrier Sense Multiple Access

CW: Contention Window

DCF: Distributed Coordination Functions

DFS: Dynamic Frequency Selection

DIFS: DCF Interframe Spacing

FCC: Federal Communications Commission

FER: Frame Error Rate

INR: Interference-to-Noise Ratio

ISM: Industrial, Scientific, Medical band

LAA: License Assisted Access

LBT: Listen Before Talk

LDPC: Low Density Parity Check Code

LLR: Log-likelihood Ratio

LS: Least Squares

LTE: Long Term Evolution of the UMTS

LTF: Long Training Field

MAC: Medium Access Control

MCS: Modulation and Coding Scheme

MMSE: Minimum Mean Squared Error

MRC: Maximal Ratio Combining

MSE: Mean Squared Error

NTIA: National Telecommunications and Information Administration

OFDM: Orthogonal Frequency Division Multiplexing

OFDMA: Orthogonal Frequency Division Multiple Access

PHY: Physical Layer

PRF: Pulse Repetition Frequency

PRI: Pulse Repetition Interval

QAM: Quadrature Amplitude Modulation

QPSK: Quadrature Phase Shift Keying

SIFS: Short Interframe Spacing

SNR: Signal-to-Noise Ratio

STA: Mobile Station (Client)

STF: Short Training Field

UMTS: Universal Mobile Telecommunications System refers to the dominant cellular broadband wireless technology

U-NII: Unlicensed National Information Infrastructure

VHT: Very High Throughput

WLAN: Wireless Local Area Network

WI-FI: WLAN based on the IEEE 802.11 Standard

ACKNOWLEDGMENTS

I would like to thank all of my colleagues, friends, and teachers that have guided and supported me throughout the years.

DEDICATION

to Hamid, Reza, and Fattaneh

Chapter 1

AN INTRODUCTION TO SPECTRUM SHARING

In 1984, the term *software defined radio* was coined to refer to a programmable radio device with the flexibility to adapt to and decode a variety of broadband wireless signals. The notion of a programmable adaptive radio became a pillar in a new type of wireless networking paradigm labeled cognitive radio which was first introduced by Mitola in 1999 [46]. To understand the importance of this development, we must briefly review the evolution of wireless systems since their inception.

Spectrum is the primary resource in wireless networks. Any measure of performance, quality of service, or capacity is heavily dependent on the amount of spectrum that can be accessed by a user. Historically, in the realm of civilian wireless networks, careful management and grants of exclusive ownership have been used to prevent wireless interference from one network or device hindering the performance of another device. As demand for wireless connectivity increased, so did network deployments to meet this demand.

Slowly, it became clear that surrendering control of large swaths of spectrum without meaningful conditions on efficient usage had led to a spectrum crunch. As demand for wireless capacity was rapidly outgrowing the finite supply of spectrum, it became clear that it was time to revisit spectrum licensing practices and look for better ways to allocate this scarce resource.

The digital TV transition presented the first opportunity for this re-assessment to take place. The "Digital Transition and Public Safety Act of 2005" laid out a plan to convert all terrestrial video broadcast from analog to digital. The efficiency gains afforded by this changeover would allow the FCC to re-pack, re-assign, and re-auction the resulting freed up spectrum that had been utilized by TV transmitters. However, this time, instead of

re-licensing the spectrum for exclusive use, the FCC decided to consider unlicensed access.

As a side-effect of the repacking process, chunks of spectrum were freed in various geographical regions of the United States, but before they could be reused, it was necessary to ensure adequate protection for TV transmitters and receivers in adjacent areas. Under the moniker of TV Whitespaces (TVWS), an effort was undertaken to build cognitive radio systems with the ability to access free TV spectrum with adequate safeguards to shield neighboring TV receivers. The solution was a tiered access system with two device categories:

1. **Primary User:** The primary users were the original owners of spectrum (i.e. the TV operators/receivers) and were entitled to priority access to the spectrum. The criterion to ensure protection is simple: if a TV receiver is located within the intended TV coverage area, its quality of service should not be degraded.

2. **Secondary User:** The secondary user can freely access available spectrum subject to the protection of the primary user. This implies that it should be aware of how it can affect neighboring TV users.

This two-tier paradigm endures till this day and remains a key piece in many shared spectrum scenarios, but presented major challenges in the case of TVWS. In particular, to predict service degradation for a TV receiver (primary user), it becomes necessary to know how a secondary user's signal propagates to the primary user, and how well the signal propagates from the TV transmitter to the receiver. Hence, knowledge on the location of the primary/secondary users, detailed information about the terrain separating them, the amount of clutter and buildings in the intervening distance, and even the height of the antennas were required. In practice, such information was so hard to acquire that in order to err on the side of caution, a very conservative approach was taken. For this reason amongst others, ultimately, TVWS did not have the impact that was envisioned at the start of the effort.

Yet, the TVWS experiment did nothing to dissuade the slow march towards a more dynamic approach for spectrum access. In fact, in 2010, U.S. president Barack Obama

directed government organizations and agencies to repurpose 500MHz of government held spectrum within 10 years [54] in order to "wring abundance from scarcity, by finding ways to use spectrum more efficiently." In 2012, the President's Council of Advisors on Science and Technology (PCAST) authored a recommendation [53] with two main claims: 1) spectrum clearing and reallocation is not sustainable and 2) immediate use of federal spectrum can be obtained through sharing.

1.1 Motivation

This dissertation is is motivated by this pressing need for more spectrum. In particular, the majority of our focus will be on spectrum sharing between a wideband communication network and a pulsed radar. We aim to explore the coexistence challenges in this scenario, address how radars can be protected from undue interference, and propose mechanisms to improve communications performance in these shared channels. We will proceed along three main directions:

1. A test-bed implementation of a Wi-Fi like network incorporating sensing

2. Detecting and protecting radars through sensing

3. Physical/MAC layer impact of radars on communication links (Wi-Fi and LTE)

While the need to protect primary users was elaborated on earlier in this chapter, our focus on LTE and Wi-Fi is easily justified.

Firstly, LTE and Wi-Fi are the two dominant high data rate consumer wireless technologies in the world today. In fact, their combination spans every type of network configuration from single home Wi-Fi to nationwide cellular networks. Hence, bringing spectrum sharing to Wi-Fi and LTE is the best way to improve spectrum efficiency and meet our ever increasing demand for wireless capacity.

Secondly, as proven and mature technologies, wholesale changes to fundamental aspects of Wi-Fi and LTE are unattractive and impractical. Novel solutions that improve their coexistence capabilities with minimizing changes to the standard will accelerate the proliferation of spectrum sharing systems by taking maximum advantage of the monumental development efforts already expended on these systems.

Thirdly, while LTE and Wi-Fi are fundamentally different technologies, they have many similarities that make some of our insights applicable to both cases. By examining both technologies in detail, we will identify some key ideas that will prove important if widespread spectrum sharing is to become a reality. In the next section, we provide an outline of our main contributions towards this goal.

1.2 The Cognitive Concept and Spectrum Sharing for TVWS

The cognitive network as envisioned by Mitola incorporated a sophisticated system of learning and knowledge representation. Roughly, it consists of an algorithm that selects radio/network parameters based on environmental measurements and operating requirements. Therefore, it is not surprising that Cognitive Radio concepts lay at the foundation of spectrum sharing where operating requirements (such as protection of primary users) could be met through a combination of sensing, collaboration, mathematical modeling, and radio adaptation.

Under the primary/secondary user paradigm, a notion of an exclusion region was defined – areas in which secondary users were prohibited in order that the primary user remain adequately protected. Through empirical measurements, it became apparent that the stochastic/mathematical models for signal propagation led to pessimism in regards to the determination of exclusion regions [50] (far too much area was unavailable for secondary users). Thus, a significant research effort was focused on distributed and collaborative sensing techniques in cognitive radios as a method to improve the selection of exclusion regions.

Another line of research focused on adapting current protocols to the needs of cognitive radios or designing new protocols to meet these demands. Two major aspects of this work

were: 1) physical layer techniques to aid in cognitive use (such as NC-OFDM [61]) and 2) MAC layer protocols to allow for the incorporation of sensing [15]. It is the latter research question thats serves as the launching point for our work.

1.2.1 TVWS: A Test-bed Implementation for a Wi-Fi Cognitive Network

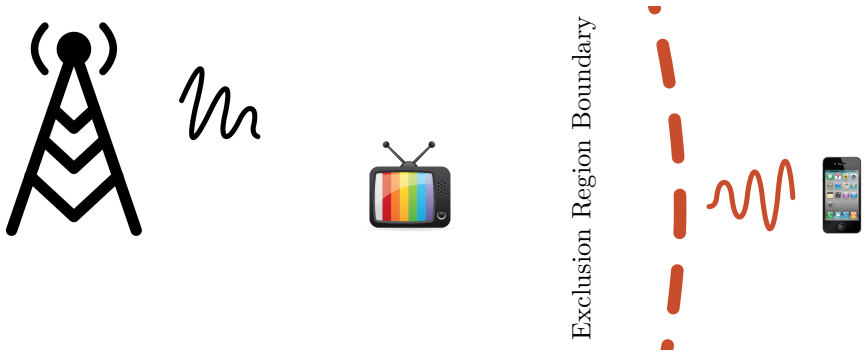


Figure 1.1: The purpose of the exclusion region is to prevent secondary users from degrading the service at a TV receiver. Note that the exclusion region is a function of receiver location as well as the received signal strength from the TV transmitter (the SNR).

In the next chapter, we begin by constructing a Software Defined Radio based cognitive network inspired by the IEEE 802.11 Wi-Fi protocol as a pre-cursor to the 802.11af standard which was ratified in 2014 [11]. This task is accomplished through a modification to the CSMA/CA medium access mechanism (dubbed QP-CSMA-CA) to incorporate sensing.

In work prior to QP-CSMA-CA, dedicated quiet periods have been defined for sensing, as a synchronized duration wherein all clients are prohibited from uplink transmissions; this interval is intended for sensing a channel's status so as to detect out-of-network transmissions. However, such dedicated periods may adversely impact system throughput as the price for coexistence.

Yet Wi-Fi's DCF mechanism already incorporates quiet intervals that could be exploited and extended for sensing purposes in lieu of a dedicate sensing period. The proposed QP-

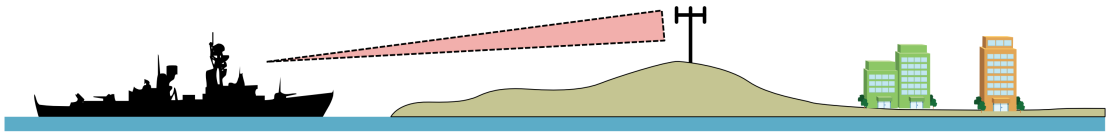


Figure 1.2: This figure illustrates an example of the radar/communication coexistence scenario as envisioned by [65].

CSMA-CA protocol is implemented on the universal software radio peripheral (USRP)-based software defined radio platform and configured in a small network for measuring throughput and latency. Experimental and simulation results show the efficacy of the proposed algorithm over the dedicated sensing-based mechanism when compared in terms of system throughput and medium access latency.

1.3 Spectrum Sharing with Radio Location Systems (Radars)

More recently, the focus of spectrum sharing has shifted to radars. A large portion of the desirable wireless spectrum is utilized by radio location systems [10] which are largely government owned and operated. Under the direction of the president's 2010 memo, the NTIA made available 150 MHz of spectrum in the 3GHz s-band for study (and future deployment) of spectrum sharing with civilian communication systems.

1.3.1 Detecting and Protecting Radars Through Sensing

The initial estimates from the NTIA (using path-loss based predictions) led to the exclusion regions shown in Figure 1.3.1. Notice that much of the coastline (coincidentally where the vast majority of the population resides) is firmly marked as an exclusion region. As was the case with TVWS, pessimism in determining exclusion regions will negate much of the benefits promised by spectrum sharing. However, unlike TVWS, radars incorporate a measure of dynamism that includes mobility and intermittent periods of inactivity. Additionally, radars have the unique characteristic that the transmitter and receiver are typically colo-

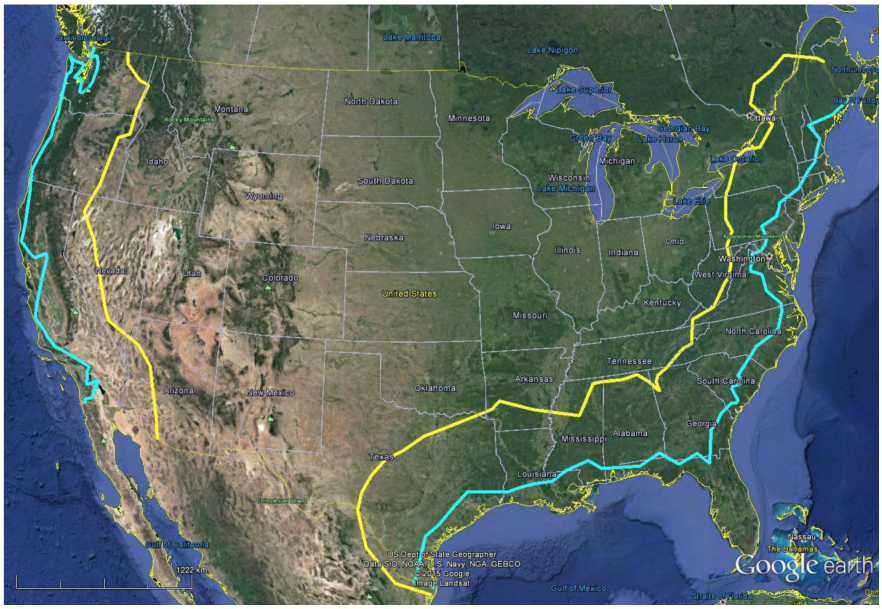


Figure 1.3: Original NTIA Exclusion Regions (Yellow) and revised exclusion regions (blue)

cated. Hence, any knowledge of the radar transmitter can be used to much greater effect for the purposes of protecting radars while simultaneously shrinking the exclusion regions (Figure 1.3).

In Chapter 3, we look at shrinking the exclusion regions by incorporating sensing into Wi-Fi. Specifically, the proposed approach to spectrum sharing is based on unilateral action by Wi-Fi networks to prevent unacceptable interference to incumbent search radars (typically operating in S-band). We will evaluate the ability of a single Wi-Fi network to *speedily detect* radar operation using spectrum sensing as a means of protecting them via subsequent dynamic frequency selection (DFS), i.e. changing to another Wi-Fi channel (typically outside the radar band with no discernible impact on radar operations). We rely on the opportunistic use of naturally occurring *random* quiet/idle periods in a Wi-Fi network employing Distributed Coordination Function (DCF) to detect the presence of a radar using energy detection. We will analytically characterize the statistical properties of the idle periods in terms of occurrence and duration in the full buffer and downlink only traffic cases, and verify

our analysis using simulations. We then suggest simple modifications to Wi-Fi parameters in order to improve radar detection performance and examine the resulting Wi-Fi throughput costs. Our key contribution will be to throughly characterize the Wi-Fi throughput vs. detection trade-off implicated by this coexistence mechanism.

1.3.2 Impact and Mitigation of Radar Interference in LTE Systems

In Chapter 4, we consider the coexistence problem in the reverse direction by investigating the impact of radar interference on LTE through direct injection of narrow-band radar waveforms into a state of the art LTE down-link simulator. We will show detailed results demonstrating the impact of interference on various parts of LTE signaling including reference symbols. Then we show how the presence of radar interference causes errors in the noise and interference estimates, impacts decoding in the LTE soft decoder, and ultimately leads to erroneously received Sub-frames. We will propose a heuristic mechanism to combat such interference and improve LTE throughput in the presence of narrow-band radar using selective erasures. Ultimately we will show that LTE can be made far more robust to bursty interference – a critical requirement prior to successful deployment in spectrum sharing scenarios.

1.3.3 Impact and Mitigation of Radar Interference in Wi-Fi Systems

In Chapter 5, we will extend the work from Chapter 4 through a comprehensive examination of Wi-Fi/radar coexistence from the perspective of a single Wi-Fi link. To our knowledge, this is the first controlled signal level study addressing the impact of radar on Wi-Fi. We will employ an array of packet error rate simulations to characterize the effect of radar interference during each phase of reception. Following this characterization, we provide a set of signal processing blocks (with accompanying analysis) to detect radar interference during packet reception and take corrective action when possible.

By capitalizing on the inherent structure of the Wi-Fi signal (in-built redundancies and pilot signals), we are able to immunize WLAN to radars and hence allow Wi-Fi networks

to operate considerably close to radar transmitters. As we will show, even in conservative deployment scenarios, the WLAN receiver can expect to see interference levels that far exceed what it can tolerate without the modifications suggested in this chapter. Solutions like those proposed in this chapter will play a key role in realizing the potential of spectrum sharing by enabling deployment of communication systems in the widest possible area.

1.3.4 The Path to Enabling Large Scale Coexistence Studies

Finally, in Appendix A, we will lay the groundwork for incorporating the signal level results obtained in Chapter 5 into the *ns-3* system simulator. The results presented in Chapters 4 and 5 have focused on the impact of radar on a single communications link. The next logical step is to consolidate the obtained results into new error tables that allow full-scale network wide coexistence studies between Wi-Fi and radar (as previewed in results presented in [21]).

Chapter 2

QP-CSMA-CA: A MODIFIED CSMA-CA-BASED COGNITIVE CHANNEL ACCESS MECHANISM WITH TESTBED IMPLEMENTATION

In this chapter, a *modified* carrier sense multiple access-collision avoidance (CSMA-CA) mechanism, termed as quiet period-CSMA-CA (QP-CSMA-CA) is proposed, for the purposes of coexistence in a cognitive networking set-up with secondary clients that seek access using 802.11. In work to date, *dedicated* quiet periods have been defined for this purpose, as a *synchronized* duration wherein all clients are prohibited from uplink transmissions; this interval is intended for sensing channel status so as to detect out-of-network transmissions. However, such dedicated periods may adversely impact system throughput as the price for coexistence. In QP-CSMA-CA, the Wi-Fi nodes perform channel sensing during an *extended back-off phase*; thereby bypassing the need for separate dedicated sensing interval. The proposed QP-CSMA-CA protocol is implemented on the universal software radio peripheral (USRP)-based software defined radio platform and configured in a small network for measuring throughput and latency. Experimental and simulation results show the efficacy of the proposed algorithm over the dedicated sensing-based mechanism when compared in terms of system throughput and medium access latency.

2.1 Introduction

The desire to improve utilization of previously licensed bands that have been shown to be under-used, has led to the new policy of allowing use of such spectrum by secondary or unlicensed users, as long as they do not interfere with the primary or licensed users [47]. The resulting proliferation of unlicensed wireless networks will increasingly lead to scenarios

where multiple such secondary networks overlap due to co-location, contributing to what is expected to become *the* major challenge in the future [32] - that of coexistence among *heterogeneous* unlicensed networks, *i.e.*, those with different PHY and MAC layers. This is already an issue in the so-called 700 MHz TV White Space (TVWS) band, where IEEE 802.22 Wireless Regional Area Networks (WRAN) will co-exist with the currently emerging IEEE 802.11af Wi-Fi networks.

IEEE 802.22 is designed for point-to-point access between a base station (that may operate upto a maximum of 4 W equivalent isotropically radiated power (EIRP)) and fixed customer premise equipment (CPE) with 1.5 Mbps/384 Kbps on downlink/uplink, respectively [69]. On the other hand, 802.11af Wi-Fi network is intended for extended range internet access of portable devices. The PHY/MAC layers of these two potentially co-located networks are thus very different by design; 802.22 has adopted orthogonal frequency division multiple access (OFDMA) and a centralized, connection-oriented MAC, where the base station controls resource allocation on the uplink among all its connected users. On the other hand, the 802.11af MAC supports the usual contention-based medium access with restrictions on operation only within channels 21 to 62 in the TVWS. Since these Wi-Fi devices will operate in the TVWS, they need to transmit with a spectral mask of -55 dBm below the maximum transmit power on channels adjacent to channels with active TV broadcasting. The PHY layer of 802.11af is based on the same principles as 802.11ac and will support multiple bandwidths, *e.g.*, 5, 10, and 20MHz. The 802.11af devices need to coexist with heterogeneous bandwidths of operation within a homogeneous Wi-Fi network, as well as with 802.22 networks, and primarily with TV broadcasting networks.

Clearly, coexistence enhancing mechanisms are desirable in all such PHY/MAC designs to protect incumbents and minimize interference, utilizing primitives such as spectrum sensing, geolocation, and frequency agility. In general, nodes within a network transmit beacons [1] that could facilitate discovery of network identity by other networks that are equipped

[1]For example, 802.22 base station transmits regular super-frame Control Header (SCH). Similarly, 802.11af APs could also transmit quiet period schedules for sensing in periodic beacon frames during

with out-of-band sensing capability [69]. In 802.22, the base station schedules *quiet periods for sensing* by all nodes during which no transmission takes place, to enable (self) network status estimation. Since 802.11af will access medium using distributed MAC, any such synchronized listening must be achieved via a different manner. The primary purpose of this work is to suggest a new MAC algorithm - Quiet period carrier sense multiple access - collision avoidance (QP-CSMA-CA) - that enables such a feature, by exploiting inherent opportunities within distributed coordination function (DCF) in 802.11. Further, we implement the QP-CSMA-CA protocol in a lab-scale universal software radio peripherals (USRPs) test-bed to validate the performance of our proposed algorithm. In summary, following are our major contributions:

- Propose QP-CSMA-CA protocol for sensing and detection of coexisting networks;
- Implementation of USRP-based heterogeneous network of secondary and primary users, where QP-CSMA-CA algorithm is applied at the secondary nodes.

The chapter is organized as follows. Section II gives a brief discussion on dedicated sensing in conventional CSMA-CA based mechanism and existing 802.22 Standard. In Section III, we provide a detailed description of our proposed QP-CSMA-CA mechanism. The USRP test-bed implementation of our proposed algorithm is detailed in Section IV while the algorithm and process flow are illustrated in Section V. The results obtained from our USRP test-bed and corresponding simulation results are presented in Section VI. Finally, Section VII draws the conclusion.

2.2 Related Work

In order to detect interfering networks, a Wi-Fi network needs to have a coordinated sensing period without activity in its own network. Currently proposed schemes [15] - [48] for

---

which the active nodes are prohibited from data transmissions.

coordinated sensing introduce periodic sensing intervals within the data transmission phase that result in reduced network performance.

The *intermittent DCF (I-DCF)* scheme [15], illustrated in Fig. 2.1, introduces dedicated and periodic sensing duration, τ in order to detect presence of incumbents. Due to these predefined durations, the authors propose to fragment data packets (Fig. 2.1(a)) in order to accommodate periodic sensing. *However, the control packets namely, RTS, CTS, and ACK packets are not fragmented.* Additionally, a successful data fragment should have a minimum of $DATA_{min}$ bits. So I-DCF scheme leads to three serious drawbacks:

- If remaining time t_r between SIFS and initiation of sensing is not sufficient for an RTS, CTS, or ACK packet, then a control packet, if scheduled, is not transmitted and can be a potential cause of inefficient spectral usage. However, a fragment of $DATA_{min}$ bits with duration less than t_r can be transmitted until the initiation of the sensing duration as depicted in Fig. 2.1(a);

- If t_r is smaller than the transmission duration of $DATA_{min}$ bits, no data fragment is sent and this t_r interval is wasted as depicted in Fig. 2.1(b);

- Significant overhead due to the need for transmitting multiple PPDU containing the packet fragments.

In [48], the base station within the IEEE 802.22 network defines specific sensing intervals namely, intra-frame sensing (IFS) and inter-frame sensing (IRFS) durations. These durations are typically around 25 and 50 ms, respectively. During these sensing periods, all the CPEs are prohibited from data transmission and are required to sense collaboratively for idle channels, not occupied by incumbents.

In a Wi-Fi basic service set (BSS), a *Quiet element* [9] is used in order to obtain measurements on occupancy of one or multiple channels, except for the one it is currently operating in. The *Quiet element* is defined by an access point (AP) in *Beacon* or *Probe Response* frame in order to request the nodes to collect and report measurements on designated channels.

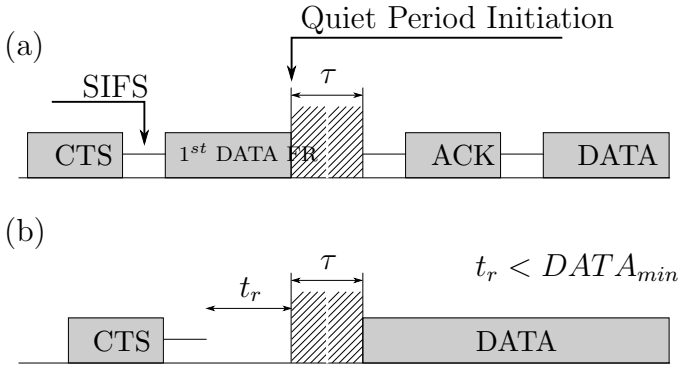


Figure 2.1: Intermittent DCF Scheme illustration

However, it should be noted that this *Quiet element* demands for a dedicated time duration of at least one time unit (TU) of 1ms during which no transmissions are permitted from the nodes in the BSS on the current channel. Multiple such *Quiet elements* can be transmitted by the AP in order to schedule various quiet intervals. These dedicated sensing intervals on multiple channels result in inefficient bandwidth utilization, since STAs are prohibited from data transmissions simultaneously.

Our proposed QP-CSMA-CA does not involve dedicated sensing since we intend to exploit existing back-off period in conventional CSMA-CA mechanism for sensing of out-of-network interference. Since carrier sensing (CS) is already performed during the back-off phase, QP-CSMA-CA extends this CS procedure to sense multiple other channels for future occupancy. By incorporating sensing within back-off, QP-CSMA-CA intends to improve short-term unfairness among network nodes and enhance aggregated throughput of the BSS as illustrated later in Section VI.

2.3 QP-CSMA-CA Mechanism

In DCF, contention-based access adopts the CSMA-CA mechanism, where the active nodes in the network perform the following actions: *(i)* sense the channel if it is idle for a fixed distributed inter frame spacing (DIFS) period, *(ii)* if the medium is still idle, the nodes

enter a *back-off phase* and choose a random value for their back-off counters between 0 and minimum contention window (CW_{min}), while sensing simultaneously its operating channel for possible occupancy, *(iii)* if medium is sensed occupied, they set their network allocation vectors (NAV) corresponding to the fixed duration specified by either an uplink or a downlink packet transmission, *(iv)* if medium is sensed idle, the nodes start decrementing their existing counter values in every time slot, and *(v)* when counter value of a single node reaches zero, and the medium is still idle, this specific node wins the contention and starts data transmissions.

In QP-CSMA-CA, we propose to introduce quiet periods within the contention period prior to gaining access to the medium. The purpose of such quiet periods is to sense and detect other coexisting network (*e.g.*, 802.22, Zigbee networks) operation either on the current channel of contention or in one its adjacent channels. Detection of such operation would either allow the Wi-Fi network to coexist using interference mitigation techniques or switch to a different channel for interference avoidance. Quiet periods ensure perfect detection of coexisting heterogeneous networks, since transmissions from the similar network are prohibited during this interval. The major difference between QP-CSMA-CA and conventional CSMA-CA (for instance, *I-DCF*) is in the scheduling of quiet periods. Dedicated sensing periods [15] are scheduled in CSMA-CA mechanism as illustrated in Fig. 2.1, while quiet periods in QP-CSMA-CA are scheduled during the contention phase.

For QP-CSMA-CA, step *(ii)* in conventional CSMA-CA illustrated above is modified to an *extended back-off* phase. This phase is initiated with the scheduled quiet period of fixed duration followed by the back-off phase as shown in Fig. 2.2. However, the quiet periods are scheduled periodically by the AP after sensing the medium to be idle for DIFS period. The reason for scheduling quiet periods within the back-off phase is two-fold:

- During back-off phase, nodes are in sensing mode and hence, not transmitting data packets (unless one of its counter value reaches zero). Therefore, quiet period is, in essence, already established.

- In back-off phase, since nodes are already in sensing mode, QP-CSMA-CA extends

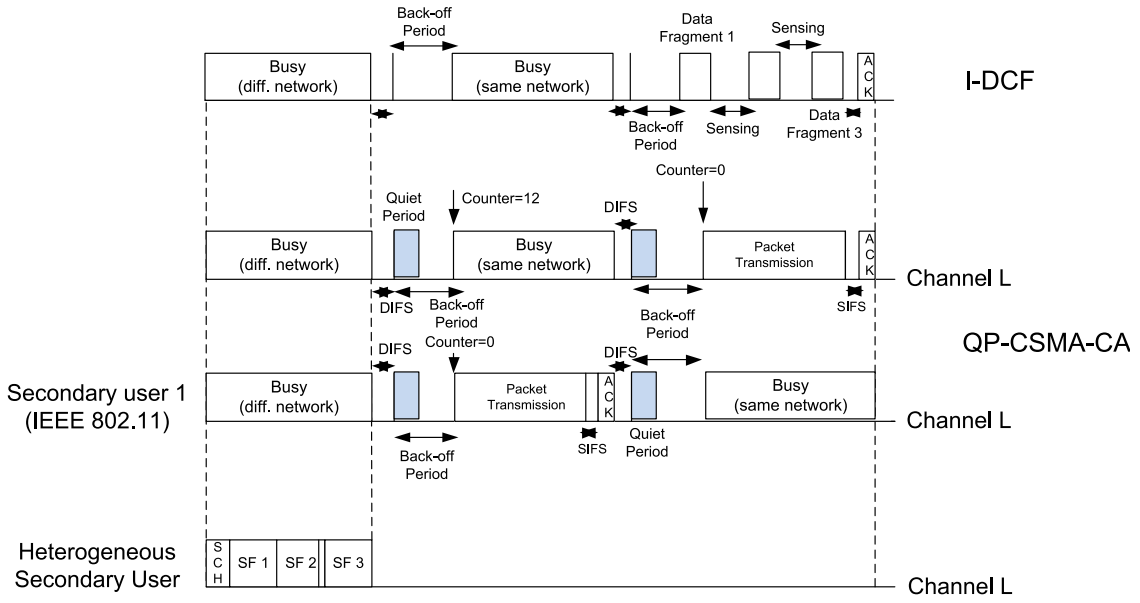


Figure 2.2: Comparison of timing diagram between QP-CSMA-CA and I-DCF

this sensing behavior not just restricting to its own channel, but also to its adjacent channels; therefore, no State change (from transmission mode to sensing mode as in dedicated sensing) is required in the transreceiving circuitry.

The potential benefits behind this new MAC proposal are the following:

- Fragmentation of data packets prior to dedicated sensing periods in *I-DCF*, while sensing during the contention phase leads to no packet fragmentation since nodes are in sensing mode after the DIFS period;

- Exploit the back-off phase that is essentially a sensing phase with inherent quiet periods;

Quiet periods, when scheduled, may initiate after synchronization at the DIFS period. The extended back-off phase starts with the quiet period, followed by back-off counter setting, and then medium access. Each of these steps are illustrated in depth in the following subsections.

Element ID	Length	Quiet Count	Quiet Period	Quiet Duration	Number of Channels	Switch Decision	Channel ID

Figure 2.3: *Quiet element* frame format in *Beacon* and *Probe Response* frames

2.3.1 Quiet Period Scheduling

In QP-CSMA-CA, as stated earlier, sensing shall be performed during the back-off phase. However, the network nodes need to be informed by the AP about scheduled sensing either in a *Beacon* or a *Probe Response* frame. We utilize the existing *Quiet element* in *Beacon* and *Probe Response* frames but with new interpretations of the fields in terms of DIFS periods. The Quiet element frame format is depicted in Fig. 2.3.

The *Element ID* is a specific value assigned for the *Quiet element*.

The *Length* field is set by the AP based on the length of the six fields namely, *Quiet Count*, *Quiet Period*, *Quiet Duration*, *Number of Channels*, *Switch Decision*, and *Channel ID*.

The *Quiet Count* field is set to the number of DIFS intervals after the current Beacon or Probe Response frame interval when the quiet period is initiated. A value of 1 indicates that the quiet interval starts immediately after the DIFS period following the current *Beacon* or *Probe Response* frame interval. Alternatively, a target time can also be advertised along with this field such that the nodes may initiate scheduled quiet period after the DIFS period following the expiration of the target time.

The *Quiet Period* field is set to the number of DIFS periods between the start of regularly scheduled quiet durations. A value of 0 indicates that no periodic quiet interval is defined. A value of 2 implies that the nodes are required to perform sensing every alternate DIFS periods. This scenario is illustrated in Fig. 2.4. The periodicity can be changed by the AP in the BSS based on measurement reports received from the nodes. Higher rate of occupancy by coexisting networks shall result in reduced periodicity (values between 1 and 3 DIFS

period) and frequent sensing schedules, while lower occupancy rates shall result in increased periodicity (values between 6 and 10 DIFS period and value 0).

The *Quiet Duration* field is set to the duration of the quiet interval required for sensing M channels. This duration is a function of the channel sensing time, T_{sen} and channel switching time, T_{sw} per channel. The parameter T_{sen} for energy detection is the time incurred in the integration of the received signal power over N samples per channel bandwidth B. It should be mentioned here that N is a function of target detection probability, P_d and false alarm probability, P_{fa}. A lower bound on sensing time T^*_{sen} for M channels is expressed in terms of received signal-to-noise ratio ζ and P_d based on [2]:

$$T^*_{sen} = M \times \frac{N}{B}\left(-Q^{-1}(P_d)\left(1+(\frac{1}{\zeta})\right)\right)^2, \tag{2.1}$$

where $Q(.)$ is the Q-function. Settling time, T_{sw}, also known as the switching time, is the time incurred by the phase locked loop circuit to switch from the current channel and lock into the next desired channel for sensing. Usually, the phased locked loop bandwidth is increased in order to reduce the settling time during the frequency switching transient. After the transient has subsided (indicated by acquisition of phase lock), the loop bandwidth is reduced. This mechanism allows fast settling with low phase noise and low power dissipation. This technique is used as an illustrative technique that can be used by the nodes for faster switching between channels to be sensed.

As evident from Eq. 2.1, the sensing time after each DIFS period is a function of the number of channels (M) to be sensed, samples per channel (N), and the current traffic load requested by the network nodes in the BSS. The AP may run an algorithm using T^*_{sen}, a fixed T_{sw}, traffic load in the BSS, P_d, and P_{fa} in order to obtain an optimal number of channels to be sensed. The detail of the algorithm is out of scope of this chapter. Based on the *Quiet Duration* field in the *Quiet element*, the recipient nodes are aware of the next quiet duration.

The *Quiet Duration* field in a *Quiet element* can be varied within a beacon interval. After initiation of contention phase after the beacon interval, the nodes perform quiet periods of durations specified in the *Quiet Duration* field in a *Beacon* frame. However, the *Channel*

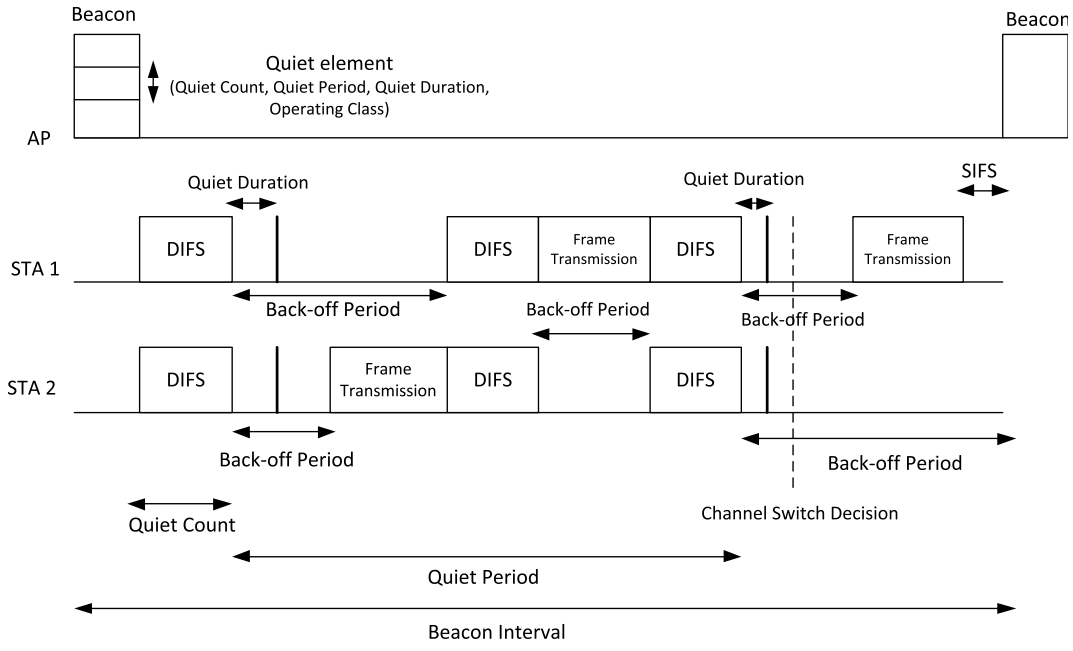


Figure 2.4: Illustration of the fields in Quiet element for sensing in back-off phase

Usage field in *Probe Request* frame can be utilized by the nodes to indicate to the AP about occupancy decisions on channels defined by the field *Number of Channels*. If no variations in sensing decisions are observed from nodes for some sensed channels, the AP uses the *Quiet Duration* field in the *Quiet element* of a *Probe Response* frame to indicate variations in quiet period scheduling for only the channels that require revised sensing durations. In such a scenario, the *Quiet Count* element is now revised and all other previous values of *Quiet Count* shall be ignored by the nodes. The reference is now based on the *Probe Response* frame, instead of the last received *Beacon* frame. The *Quiet Duration* and *Channel ID* fields are replicated for each of the channels that require modified quiet periods in QP-CSMA-CA. For the channels not mentioned in the *Probe Response* frame, the *Quiet Duration* value defined in the last *Beacon* frame shall still be maintained by the nodes. Finally, if the AP decides on no variability in sensing durations based on sensing reports from the nodes, the AP transmits an unchanged *Quiet element* in *Probe Response* or in *Beacon* frame.

The *Channel ID* field contains a variable number of octets, where each octet describes a single channel ID. Based on the algorithm executed at the AP, it should decide on the number of channels to be sensed and enlists the IDs in this field.

2.3.2 Extended Back-off Phase for Quiet Period

As Stated earlier, in order to schedule quiet periods (QPs) within the contention phase, the AP broadcasts the *Quiet element* with all the pertinent parameters. For instance, based on the fields in the *Quiet element*, the AP may schedule QPs every 5 DIFS if it detects operation from heterogeneous networks on a specific channel of interest (from measurement reports sent in regular intervals), or after 20 DIFS when no other networks are detected on this desired channel. Since the QP is scheduled in terms of DIFS intervals, it is apparent that the distributed Wi-Fi network has to synchronize at the scheduled DIFS period. Moreover, an extended back-off phase is initiated at this scheduled DIFS, where sensing shall be performed by all active (with uplink data to transmit) nodes in the network.

In order for the QP sensing to be effective, each node must enter the scheduled DIFS periods (*i.e.*, based on the *Quiet Count* field in received *Beacon* or *Probe Response* frame) simultaneously as all the other nodes. If all packets during the data transmission phase (*i.e.*, RTS, CTS, DATA, and ACK) are received successfully, then the DIFS period will be initiated by each node concurrently when the NAV expires and the medium is sensed idle. Since the hidden node problem is reduced with virtual carrier sensing, the medium is sensed idle by each node simultaneously. The NAV, being set by a successfully detected packet, also expires at the same time for each node. In case of detected errors in packet reception (*i.e.*, no ACK received from the AP after uplink data transmission), and if the following DIFS is where the QP is scheduled, then, instead of sensing the channel for ($ExtendedIFS$ - $DIFS$) period shall just sense for DIFS period in order to synchronize with the other nodes in the network. In all other scenarios of detected packet reception errors and no QP scheduling at the following DIFS, the conventional CSMA-CA protocol is executed by the nodes. *It should be emphasized here that none of the contending nodes shall be allowed to decrement*

their counters during the scheduled QP in order to ensure no packet transmission within the network.

2.3.3 NAV Setting and Medium Access

Following the extended back-off phase, the nodes resume normal operation with their existing values of back-off counters from the preceding contention period. During the preceding contention phase, the nodes contended for the channel with their respective back-off counter values. While decrementing the counter values, one of these nodes gained access to the medium when its counter value decremented to zero. When the medium is occupied by this node, all other active nodes set their NAVs to the value of RTS-NAV or CTS-NAV and freeze their counters at their respective back-off counter values. After the schedule QP, all these nodes resume their counter values from the previous contention phase.

2.4 USRP Based Experimental Set-Up for QP-CSMA-CA Evaluation

An experimental set-up to assess the performance of the QP-CSMA-CA algorithm was designed using the USRP [6] test-bed, which provides a radio front-end to a General Purpose processor (GPP) as depicted in Fig. 2.5. Basic filtering, tuning, down-sampling, and interpolation occur on the USRP; complex valued samples are streamed over Ethernet to and from the GPP, where all other signal processing necessary for demodulation are accomplished, using the open source GnuRadio software library [2]. GnuRadio blocks are connected into a flow graph that allow for data passing between blocks in a thread-safe manner. Our experiment relies heavily on the included OFDM modulation and demodulation blocks provided [1].

The performance of QP-CSMA-CA is explored with respect to three key parameters:

a) Per-channel arrival rate λ of primary user (PU) frames

b) *Quiet Period D* between sensing intervals (varying QP sensing frequency)

c) Exponent variable L that determines the *Quiet Duration*.

[2]GnuRadio includes a set of signal processing blocks that perform the digital transceiver functionalities on a host computer.

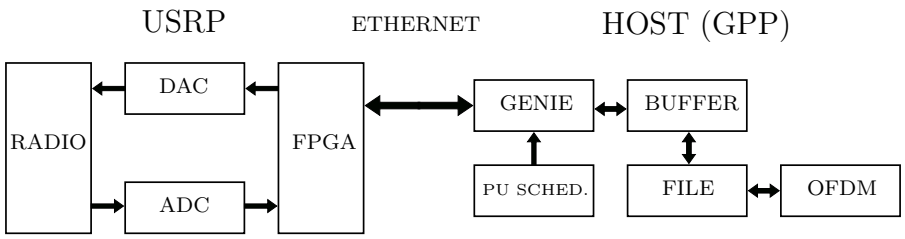


Figure 2.5: Separation of USRP and Host functions.

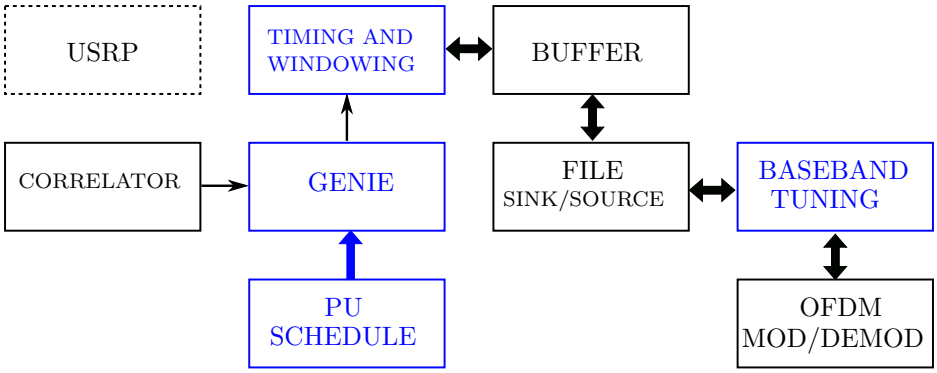


Figure 2.6: A detailed view of the GPP implementation. Blue blocks indicate custom written GnuRadio blocks used for implementation. Small arrows indicate control signals.

Prior to the start of an experiment, the values for D and L are preset at each node. After each packet is transmitted, the back-off procedure begins. If sensing is not scheduled, a random back-off between 0 and 15 ($= CW_{min}$) is selected. In the case when QP is scheduled after the completion of a packet transmission, the countdown length is selected at random in the range $[2^L, 2^{L+1} - 1]$, measured in number of slots.

Three USRPs were used in the set-up; a pair of USRP N210 devices serve as nodes in the secondary network, while a USRP2 is used to simulate the primary user (PU) [3]. The nodes used for the secondary network are synchronized through a common clock using a cable as

[3]The selection of USRP models has no significance other than availability - none of their functional differences were exploited during the experiment.

Figure 2.7: Left:PU (USRP2), Middle: Receiver (N210), Right: Transmitter (N210)

show in Fig. 2.7. The antennas used were PCB directional Log Periodic with a gain of 5-6dBi (Ettus LP0410) [6].

1. The nodes in the secondary network are set to a sample rate of 12.5 MS/s with antennas located 1 meter apart. Each node is set up as a dedicated transmitter or receiver.

2. The secondary network uses an OFDM signal with a bandwidth of 1.5MHz located in one of 5 partially overlapping 2MHz channels (Fig. 2.8).

3. A fixed packet length of 1536 bits and a preamble length of 128 is chosen for the secondary network.

4. The PU node is set to a sample rate of 7 MS/s located 10 meters away from the secondary network transmitting an OFDM modulated signal occupying 875KHz. The PU can operate in one of six non-overlapping 1 MHz channels.

5. The activity schedule for the primary, including channel dwell times and hopping sequence, are generated in advance using Matlab. The primary is modeled as a Poisson

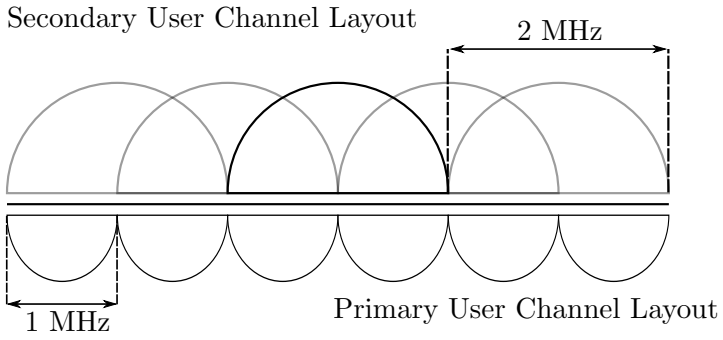


Figure 2.8: Channel layout selected to simplify detection and relocation strategy

process with arrival rate λ that dwells on a channel for an exponentially distributed duration before relocating to a uniformly distributed randomly selected channel in the range of [1,6]. A minimum dwell time of 10ms is enforced by re-generating samples that are too small.

6. Modulation and demodulation are performed off-line using the OFDM blocks included as part of the Gnuradio toolkit (Fig. 2.6).

2.4.1 Retuning

The challenge faced when the local oscillator frequency on the USRP is changed to a new channel is the lack of control on timing of the retuning. Specifically, it is not possible to ensure the USRP re-tunes at a specific time leading to uncertainties when attempting to transmit in a new channel. The timing of tuning is influenced by control signal latency that is governed by that of Ethernet [52]; often times a tuning operation can take more than 1 millisecond, orders of magnitude longer than the typical DIFS. Our solution relies on digital tuning on the GPP (Fig. 2.6). Using multiplication by a complex exponential with frequencies ranging from -2 through +2 MHz in increments of 1 MHz, data packets are pre-shifted at baseband and placed at the correct frequency offsets for each channel (Fig.

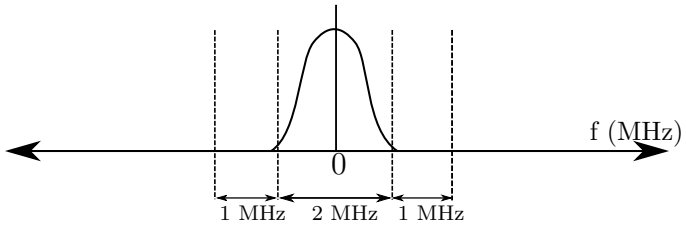


Figure 2.9: For each channel, a packet is shifted to the appropriate frequency at complex baseband.OFDM sub-carriers not shown.

2.9). Then, switching channels is simply a matter of streaming the correct data to the USRP slightly in advance of their intended transmission. Appending timing information to the samples ensures that the USRP switches to a new channel at the desired time.

2.4.2 Sensing and the Genie Block

The duration required to stream samples from the USRP to the GPP, compute energy, and make a decision regarding the presence of the PU far exceeds the allowed time proposed by QP-CSMA-CA. Therefore, in addition to the new GPP re-tuning, a Genie block is implemented (please refer to Figs. 2.5 and 2.6) to simulate sensing. The genie block has access to perfect knowledge of the PU's actions. Parameters such as P_{fa} and P_d are used to mimic real sensing as closely as possible. While the inclusion of the genie block is undoubtedly a simplification, it is justified since realistic implementations would avoid heavy latency penalties when compared to the USRP.

The Genie block maintains a running timer used to determine the timing of the sensing operations. When sensing is scheduled to occur, the Genie consults the PU activity schedule and simulates a sensing decision. The best channel is then chosen by scanning all channels and selecting the one furthest away from the location of the PU. When the genie selects the appropriate channel for transmission, it streams the baseband shifted (Fig. 2.9) packet for the channel to the USRP. In order to ensure accurate timing, a Time Tag is appended to the stream which is later used by the USRP to transmit samples at the desired time. It

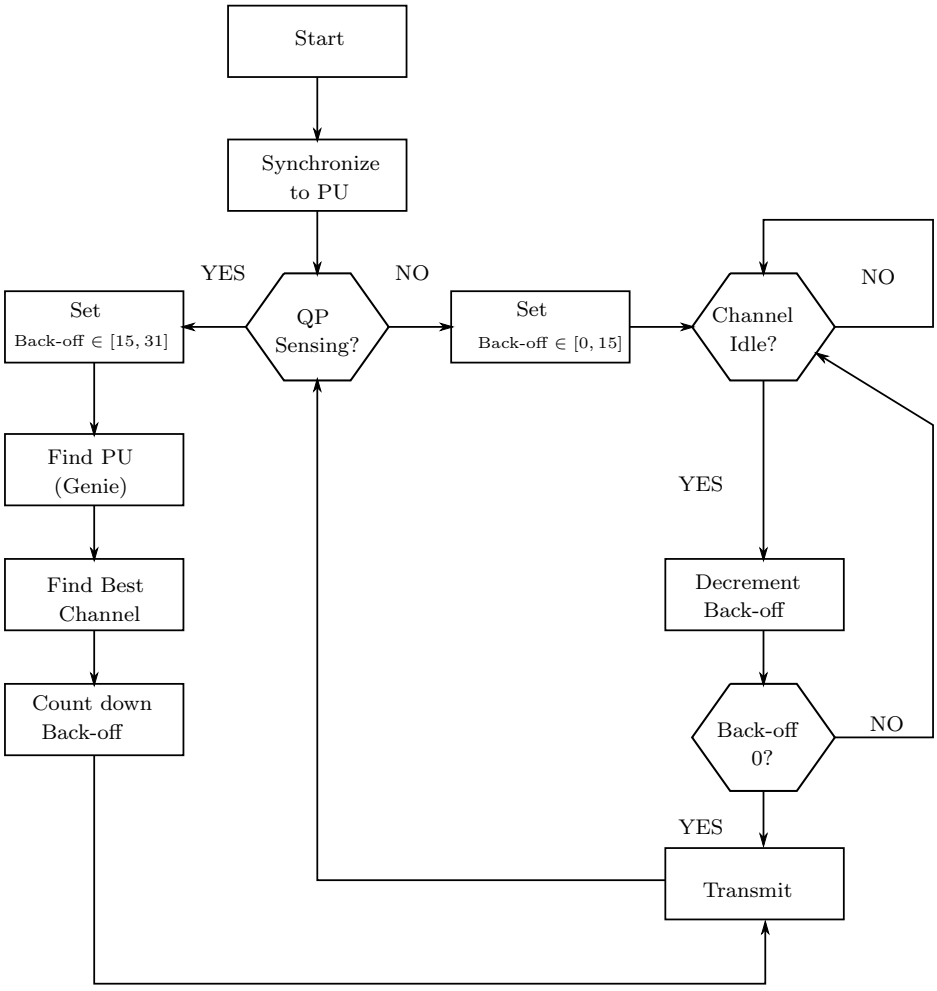


Figure 2.10: Flowchart for the QP-CSMA-CA USRP based implementation

is important to note that employing a Genie necessStates a common reference time for the primary and secondary networks.

2.5 QP-CSMA-CA Implementation

The general flow of the QP-CSMA-CA algorithm as implemented for the experiment is shown in Fig. 2.10. There are two basic flows described and the base case occurs when QP sensing is not scheduled. In such a case, the algorithm executes conventional CSMA/CA MAC.

On the other hand, when QP sensing is scheduled, the algorithm takes the opportunity to scan and locate the best available channel. Due to simulated sensing (the Genie block), synchronization between the PU and secondary networks is crucial, as such, the algorithm begins by synchronizing the networks. Thus, channel idleness and best channel decisions can be made by the Genie consulting the PU schedule.

As the algorithm executes, it maintains a count for the number of packets transmitted. The packet count is then used to establish when QP sensing takes place using the parameter D (Fig. 1, lines 1-5). If QP sensing is to occur, the extended back-off is randomly generated and counted down (each slot is $20\mu s$). At the end of the countdown, the secondary user relocates to the best channel as selected by the Genie and a packet is transmitted (Fig. 1, lines 12-13). On the other hand, if QP sensing is not scheduled, the algorithm (once again using the Genie) senses the medium until it is detected to be free. Subsequently, a random back-off between 0 and 15 is selected and counted down ultimately leading to a packet transmission. In either the QP or non QP case, once transmission is complete, the packet count is incremented and the next iteration begins. The algorithm continues the process until all packets have been transmitted. The *Quiet Period* (parameter D) is varied in each experiment while *Quiet Duration* (L) is kept constant.

2.6 Performance Evaluation of QP-CSMA-CA

Broadly, there are two sets of parameters available for modification to explore the performance of QP-CSMA-CA. The secondary network parameters govern the frequency of the extended back-off periods used for sensing (D) and the duration of sensing periods (L) while the mean dwell time of the PU (λ) are modified to evaluate the throughput of the secondary network when coexisting with varying PU activity. A simulation based on the experimental set-up is created using MATLAB in order to establish expectations for each scenario. For the purposes of the simulation, a collision channel [44] model was used.

Algorithm 1 Algorithm implementing QP-CSMA-CA on the USRP

```
1: packetcount ← 0                                   ▷ number of packets transmitted
2: period ← D                                        ▷ sensing frequency parameter
3: L ← 4                                             ▷ quiet period length
4: while more packets remain do
5:     if packetcount mod period then                ▷ QP Sensing
6:         backoff ← rand(2^L,2^(L+1) − 1)
7:         while backoff> 0 do
8:             backoff ← backoff−1
9:             wait(20 μs)
10:        end while
11:        tune_best_channel()
12:        transmit()
13:        packetcount ← packetcount+1
14:    else                                          ▷ Default Carrier Sensing
15:        if channel is idle then
16:            while backoff> 0 do
17:                backoff ← backoff−1
18:                wait(20 μs)
19:            end while
20:            transmit()
21:            packetcount ← packetcount+1
22:        else
23:            backoff ← rand(0,15)
24:            go to 17                              ▷ continue checking for idle channel
25:        end if
26:    end if
27: end while
```

2.6.1 Dedicated Sensing

As a point of comparison, measurements were made using a conventional CSMA-CA type algorithm with a dedicated sensing periodicity of 50 milliseconds and duration of 25 time slots. Packets generated just prior to the scheduled (dedicated) sensing period would be delayed till sensing is executed. In other words, the packet is not fragmented (as proposed in *I-DCF*) but delayed until sensing is complete. This modification has negligible impact given our setup.

2.6.2 Experimental Timing Diagram

At first, the node simulating the PU transmits a 13-bit barker sequence so that both networks are synchronized to a common time reference. The experiment begins 1 second after the networks have been successfully synchronized. The PU node transmits its signal as indicated by the pre-generated activity schedule. When the secondary network begins transmission, a timer is initiated. The timer is incremented based on the number of samples streamed to or from the USRP. The timer is then used by the GPP to locate the sensing windows as directed by QP-CSMA-CA. During a sensing window, the Genie makes a decision about the preferred channel to operate. The receiver simply records the complex samples provided by the USRP to a file. Once the preset experiment duration has elapsed, the experiment terminates. An off-line demodulation of the recorded data is performed to compute the number of corrupted and dropped packets. Subsequently, the nodes are re-initialized and wait for the synchronization signal from the PU node to initiate the next experiment.

2.6.3 Simulation Set-up

The Matlab based simulation is done in two steps. Firstly, the algorithm in Figure 1 is executed to generate a full trace (a fully simulated experimental time-line) of the secondary user's activities based on the QP algorithm. Next, the secondary user trace is compared to the PU activity schedule allowing detection of all packet collisions.

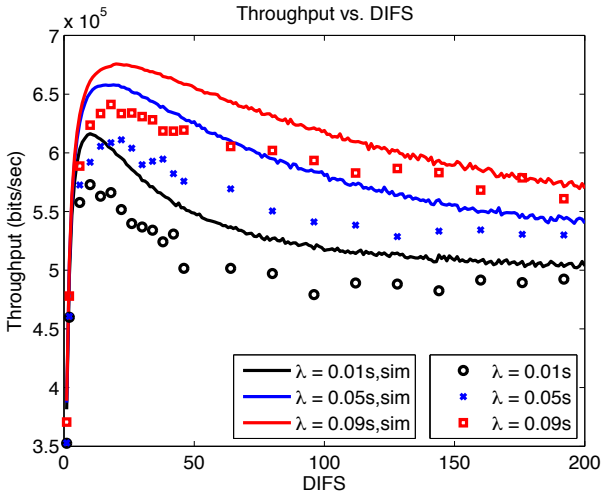


Figure 2.11: An optimal selection for number of DIFS between sensing exists

During the simulation, no detailed channel model is implemented and no samples are transmitted, instead, the collision channel model [44] is used to determine whether a packet is successfully received; once the number of collisions is tallied, it is used to compute throughput of the secondary user. Each simulation run represents a 10 second long experiment with a single PU and a pair of secondary nodes, repeated for 300 iterations. Channel set-up, packet length, and other key parameters in the simulation exactly match the experimental set-up.

2.6.4 QP-CSMA-CA Throughput

Fig. 2.11 shows that throughput increases sharply at first when sensing becomes less frequent. In the case of frequent sensing, throughput is dominated by the overhead of the newly introduced quiet periods. However, as sensing becomes more infrequent, experimental results do not match simulations as closely. In the event of a collision, the simulation assumes a packet drop. In contrast, packets are frequently successfully decoded even in the presence of interference, potentially accounting for the throughput discrepancy as the number of such events increases due to less frequent sensing.

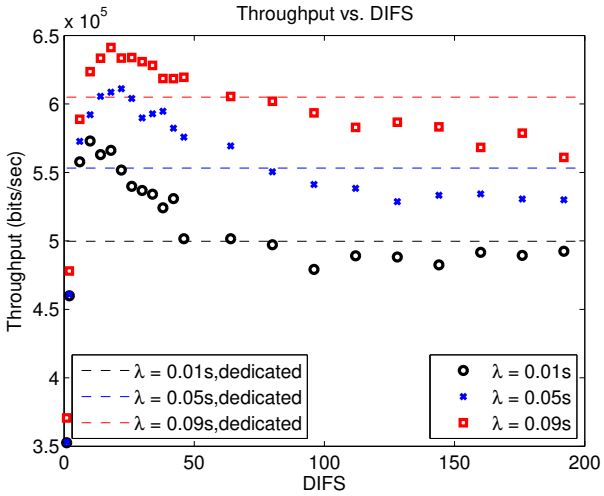


Figure 2.12: Throughput of dedicated sensing compared to QP-CSMA-CA

When evaluating the performance of QP-CSMA-CA, throughput must be compared to that of dedicated sensing. Specifically, Fig. 2.12 clearly shows the benefits of QP-CSMA-CA when compared to the dedicated sensing strategy. Dedicated sensing is comparable to QP-CSMA-CA when QP sensing is scheduled with *Quiet Period* of 75 DIFS. As a result, in cases where the PU exhibits a short mean dwell time, dedicated sensing performs significantly worse when compared with QP-CSMA-CA. On the other hand, as mean dwell time of the PU increases, the performance gap is reduced.

Regardless of the mean dwell time of the PU, optimal throughput is achieved when the secondary network is programmed to sense approximately with *Quiet Period* of 20 DIFS. Remarkably, the *Quiet Period* range of 20-40 DIFS remains close to the optimal point (Fig. 2.13) as dwell time is increased. Note that as the dwell time of the PU increases, throughput is less affected by reducing sensing frequency. As expected, frequent sensing of a slow-moving PU is a poor strategy to achieve enhanced throughput.

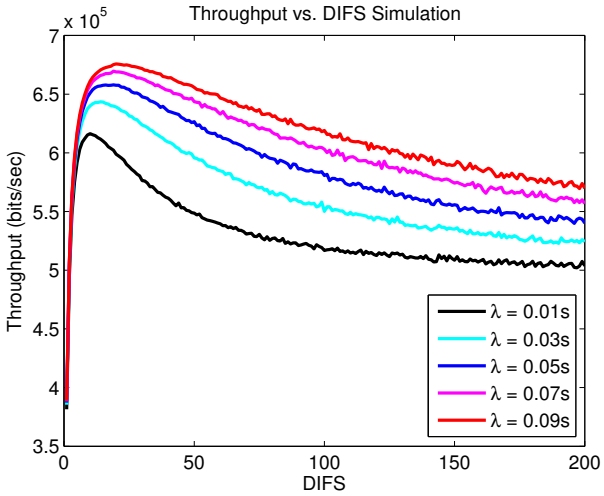


Figure 2.13: Optimal sensing frequency is stable regardless of PU dwell time

2.6.5 QP-CSMA-CA Medium Access Latency

The medium access latency results indicate that QP-CSMA-CA yields an improvement over the dedicated sensing mechanism. Fig. 2.14 illustrates the performance of QP-CSMA-CA with various values of *Quiet Periods*. Note that lowest latency does not coincide with optimal throughput, indicating a trade-off between the two performance metrics. When sensing is most frequent, the secondary network is aware of the location of the PU at all times and therefore exhibits lowest latency for medium access. Furthermore, when the PU has faster switching behavior, latency to access the medium is correspondingly higher. Once again, when compared to dedicated sensing, QP-CSMA-CA allows for significantly lower latency with *Quiet Period* values lower than 40.

2.7 Conclusion

Dedicated sensing intervals within DCF are introduced in Wi-Fi networks in order to detect presence of licensed users while operating on a channel opportunistically. In this chapter, we have proposed a modified CSMA-CA-based medium access mechanism termed here as QP-

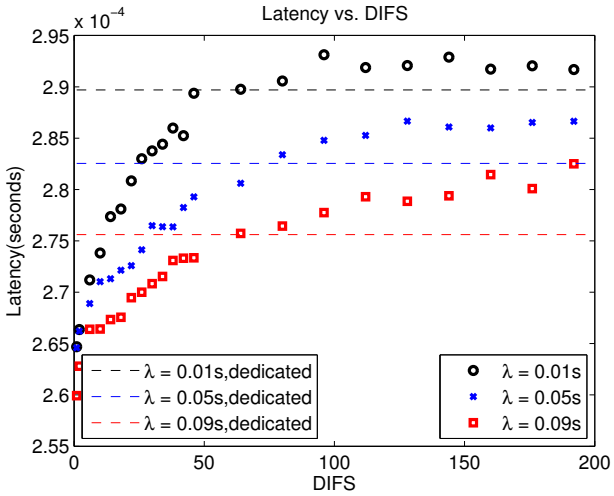


Figure 2.14: Comparison of medium access latency between conventional CSMA-CA and QP-CSMA-CA mechanisms

CSMA-CA, which enables sensing and detection of heterogeneous wireless networks during the back-off phase, while contending for the medium simultaneously. In QP-CSMA-CA, the nodes execute quiet periods during an extended back-off phase, where the nodes sense not only the operating channel but also adjacent channels in order to detect transmissions from other wireless networks. Additionally, our proposed QP-CSMA-CA mechanism is exhaustively implemented in the USRP-based SDR platform. Experimental and simulation results proved efficiency of our proposed medium access mechanism over the dedicated sensing-based CSMA-CA mechanism when compared in terms of system throughput and medium access latency.

Chapter 3

IMPACT AND MITIGATION OF NARROW-BAND RADAR INTERFERENCE IN DOWN-LINK LTE

This paper investigates the impact of radar interference on LTE by directly injecting narrow-band radar waveforms into a state of the art LTE down-link simulator. We show detailed results demonstrating the impact of interference on various parts of LTE signaling including reference symbols. Then we show how the presence of radar interference causes errors in the noise and interference estimates, impacts decoding in the LTE soft decoder, and ultimately leads to erroneously received Sub-frames. We propose a mechanism to combat such interference and improve LTE throughput in the presence of narrow-band radar using selective erasures. We simulate the proposed scheme and show that it is extremely effective in mitigating narrow-band interference and realizing the throughput expected from LTE.

3.1 Introduction

In the search for new spectrum to sustain the rapid proliferation of wireless networks, focus has recently shifted to the S-band in the 2-4 GHz range. Historically, much of these bands have been employed by civilian weather radars and military land based/shipborne radar systems. As spectrum management authorities such as the FCC and NTIA have begun to consider opening up this spectrum for shared co-channel usage by communication systems in 3.5GHz [13], a pressing question has arisen: what kind of performance can be expected from communication systems when sharing spectral resources with radars?

One such system being considered for deployment in this shared spectrum paradigm is the Long Term Evolution of the Terrestrial Radio Networks (LTE). LTE is the fourth generation 3GPP standard aimed at cellular mobile communications which was optimized for high

throughput in high mobility and interference limited scenarios. To that end, robust channel coding, frequent channel estimation, and small sub-carrier separation became cornerstones of the LTE standard.

LTE was designed to minimize in-network co-channel interference (through mechanisms such as fractional frequency re-use and frame blanking) and to be tolerant of interference/poor channel conditions through mechanisms like Hybrid ARQ (HARQ) and Interference Rejection Combining (IRC). Implicit in the design of these mechanisms was the assumption that any interference observed would largely originate from other LTE signals from adjacent cells or other users. With these assumptions, designers were able to extract the following advantages:

Timing and Predictability: The interference from adjacent LTE cells is largely synchronized in time at the victim receiver, therefore, the interference power remains roughly constant throughout a single sub-frame. In fact, the interference caused by LTE is slowly varying compared to radar interference. Since channel estimates are updated multiple times per sub-frame, it is possible for a receiver to effectively estimate the interference during reception which as we will show later in the paper is of critical importance.

Power Levels: The front-end circuitry of LTE receivers have been designed to provide a specified dynamic range through Automatic Gain Control (AGC) and Analog to Digital Conversion (ADC). These designs rely on the interference remaining within given power thresholds (i.e. no significant deviation in interference power after the AGC has been set).

Some recent work has focused on the impact of communications systems on radar receivers such as Cordil *et al* in [23], but due to the sensitive nature of information concerning radars (e.g. details of receiver structure), the public literature in the area is rather limited. A great deal more attention has focused on the reverse direction: the impact of radar interference on communication systems. In [22], Cohen *et al* show the impact of radar interference on WiMAX signaling. The authors focus on the impact of the interference on the received WiMAX constellation when the radar interference is co-channel or when the interference occurs in the guard band. In [40], Lackpour *et al* focus on various interference mitigation

mechanisms to improve WiMAX performance including spectral filtering, antenna techniques for interference cancellation, and temporal filtering. Neither of them exploit knowledge of the full receive chain to maintain link level error rates by mitigating such interference.

Recently, Sanders *et al* showed experimental results on the reduction of down-link LTE throughput due to various radar waveforms [65], however, the authors did not investigate the cause of the throughput reduction. In our work, we aim to address this gap by employing detailed link simulations to discover the ways in which LTE is affected, and thereafter propose measures for mitigation of radar interference into LTE.

The rest of the paper is organized as follows: in Section 3.2 we provide an overview of the system and simulation models used in the remainder of the paper including a brief description of LTE signaling and the soft decision turbo decoder; in Section 3.3 we examine the impact of various pulse durations and LTE MCSes in terms of codeword error; in Section 3.4 we delve deeper into the cause for codeword errors and show the impact of log-likelihood ratio (LLR) errors. Lastly, in Section 3.5 we propose a simple scheme to selectively detect and erase outlier LLRs and show large gains resulting from implementation of the scheme.

We will consider the impact of radar on LTE in following specific areas:

1. Impact on sub-frame errors;

2. Impact on the soft decision turbo decoder;

3. Impact on reference symbols;

3.2 Preliminaries & System Model

3.2.1 System Model

For the remainder of this paper, we focus on a narrow-band[1] low duty cycle radar with the parameters in Table 4.3. The radar waveforms considered have duty cycles ranging from

[1]A narrow-band waveform is chosen to avoid the need for modeling frequency selectivity from the radar transmitter to the LTE receiver since the literature on such a channel is very limited.

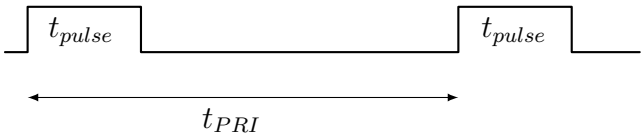


Figure 3.1: Pulse Duration and Pulse Repetition Interval for Radar

2.5-5% using a carrier wave signal with perfect windowing. We define:

t_{pulse} Pulse duration for the radar

t_{PRI} Time between pulses (pulse repetition interval)

σ_N^2 Variance of additive Gaussian noise

A Peak amplitude of the radar interference waveform

Δf Radar waveform frequency offset in relation to LTE channel center

Θ Random phase offset of radar signal distributed uniformly in $[0, 2\pi)$

$w(t)$ Windowing function

For a single pulse repetition interval (PRI), the baseband waveform of the radar interference is:

$$I(t) = A \cdot e^{j2\pi\Delta f t} \cdot e^{j\Theta} \cdot w(t) \tag{3.1}$$

$$w(t) = \begin{cases} 1 & \text{if } t < t_{pulse} \\ 0 & \text{otherwise} \end{cases} \tag{3.2}$$

We use a Δf value of 300kHz which ensures that the radar signal remains within the boundaries of the LTE channel, while it does not fall perfectly on the DC sub-carrier. In

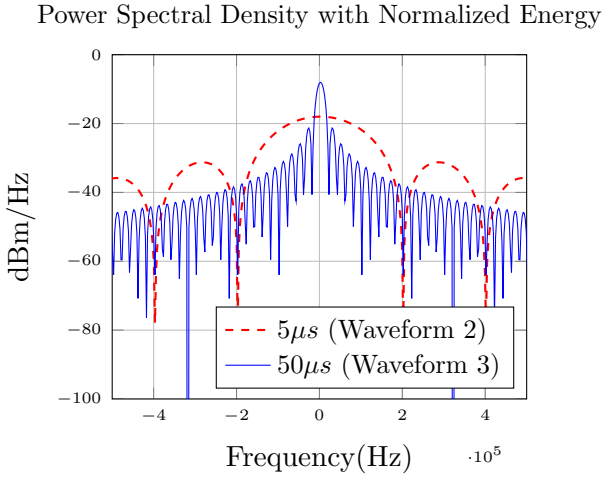


Figure 3.2: Power spectral density of two different radar Waveforms

order to vary the intensity of radar interference, we employ the Peak Interference to Noise Ratio (PINR) measure defined as:

$$\text{PINR}_{\text{dB}} = 10 \cdot \log \frac{A^2}{\sigma_N^2} \tag{3.3}$$

3.2.2 LTE Signaling

LTE uses a form of Orthogonal Frequency-Division Multiple Access (OFDMA) whereby sub-carriers and symbols are grouped into blocks of 12 sub-carriers × 14 symbols. The group of 14 symbols is termed a *sub-frame* and has a duration of $1ms$ while the 12 sub-carriers occupy 180kHz. This basic scheduling block of (12 sub-carriers for 1 sub-frame) is termed a *resource block* (RB) and is shown in Fig. 3.3. A single element in an RB (single sub-carrier for the duration of a single OFDM symbol) is labeled a *resource element*. While some OFDM symbols only carry data, others (such as symbols 1, 5, 8, and 12) also carry pilots (Fig 3.3). The pilot tones are offset in frequency and periodic in time which allows for accurate channel estimates across the entire LTE band.

Each symbol is $66.7\mu s$ in duration preceded by a $4.7\mu s$ cyclic prefix. The first symbol

Table 3.1: Radar Parameters

	Waveforms		
Parameter	**1**	**2**	**3**
Type	Carrier Wave (P0N) [65]		
Windowing	Perfect Rectangular		
Pulse	5μs	5μs	50μs
Pulse Interval	200μs	1ms	1ms
Phase	Random		

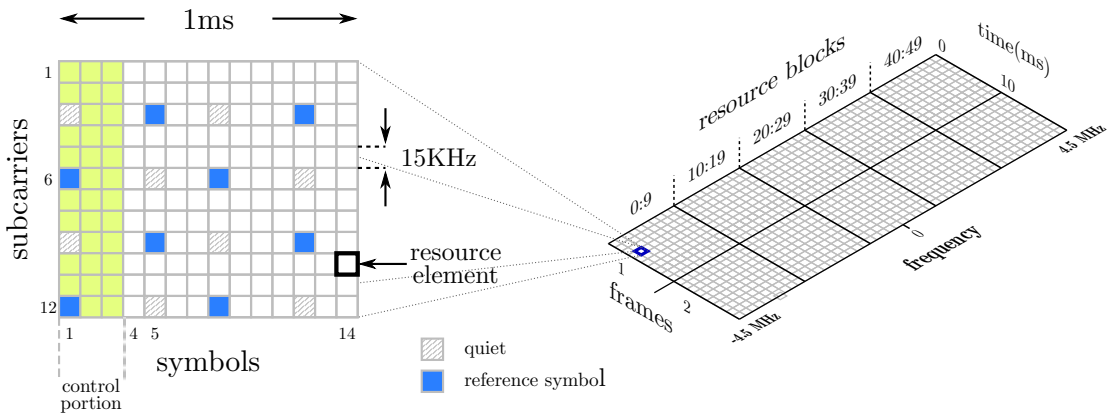


Figure 3.3: A single LTE Resource Block (left) and the LTE Resource grid for 10MHz down-link (right)

Table 3.2: LTE Parameters

Bandwidth/Type	10 MHz/FDD
Sampling Rate	15.36 MHz
Channel Model	AWGN/Pedestrian B
Antenna Config	SISO
Hybrid ARQ	Off
Rate Selection	10% Codeword Error Probability
Modulations	QPSK/16QAM/64QAM
Channel Estimation	1-D Weiner Filter, 400kHz BW
IQ Imbalance	0.5 dB Amplitude, 3 degree phase
SNR	QPSK (9dB), 16QAM (15dB)
	64QAM (19dB)

employs a slightly longer cyclic prefix ($5.2\mu s$) so the sampling rate is an integer multiple of the CDMA chip rate for legacy interoperability reasons. When injecting interference into the LTE receiver, we take care to ensure that the interference occurs outside of the cyclic prefix. We justify this choice by making the following observation: since the cyclic prefix is typically discarded, the result of interference occurring during a cyclic prefix can be thought of simply as a slightly shorter radar pulse.

3.2.3 LTE Soft Decoder

Soft decision decoders are known to provide decoding gains when used in conjunction with convolutional or turbo decoders [41] motivating their usage in LTE. However, computation of the soft information for each bit requires some knowledge of the interference/noise variance and more specifically, assumptions on the distributions of noise/interference. Typically, a common assumption is that the sum of interference and noise is Gaussian distributed.

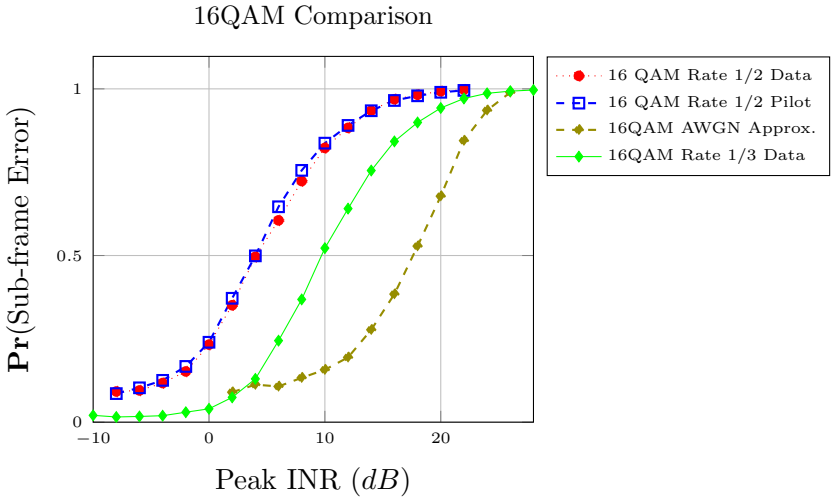
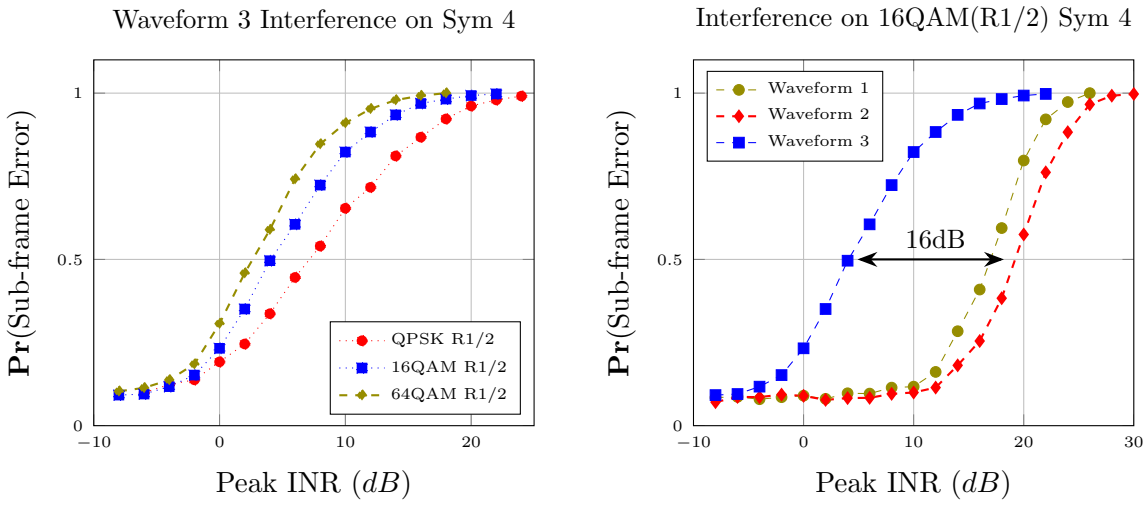


Figure 3.4: Impact of radar Waveform 3 on symbol containing pilot (LTE Symbol 5) vs. non-pilot symbol (Symbol 4)

If the noise/interference variance is known *a priori*, the log-likelihood quantity used as soft information is straightforward to compute [41]. On the other hand, most systems such as LTE rely on estimation of the variance parameters due to changing environment (e.g. number of interferers) and other time varying effects. The typical method for obtaining estimates for these quantities in LTE is to employ known pilot symbols at the receiver periodically. The noise/interference variances are estimated and used to compute the log likelihood ratios for each bit which are fed into the turbo decoder.

Large negative values of the LLR indicate high confidence in the bit being a '**0**' while large positive values indicate a high likelihood of the bit being a '**1**'; this string of LLRs is the input to the soft-decision turbo decoder. The soft-decision turbo decoder in LTE will attempt an iterative decoding of the received codeword with iterations continuing until a maximum number of iterations have been reached or the codeword is error free based on the CRC. We further explore computation of LLRs and their role in mitigating radar interference in Sections 3.4 and 3.5.



(a) (b)

Figure 3.5: (a) Frame Error Rates compared for three different modulation schemes when radar Waveform 3 is applied to LTE Symbol 4 (data only). (b) Performance impact of various waveforms on LTE (Table 4.3).

3.3 Simulation Results

The link simulator used for these simulations has been described by Papadimitriou et al in [56] and used in coexistence studies in [55]. The simulator models the LTE signal at a sample level including a fast fading channel model, channel time evolution, additive noise, effects of analog gain control, analog to digital conversion, and IQ imbalances making it a very accurate method of measuring LTE performance. Monte Carlo simulations were repeated for each data point consisting of 40 independent channel realizations evolved for 1000 sub-frames (1 second).

On the down-link, the resources in physical resource block are mapped as shown in Fig. 3.3. Some symbols (e.g. 1-3) are used for the down-link control channel. Among the symbols, some contain pilot tones on specific resource elements (e.g. symbol 5) while others use all REs for down-link data transmission (e.g. symbol 4). We will show the impact of

interference on reference as well as data symbols. Furthermore, we consider the case of multiple pulses arriving within a single sub-frame.

The results are highlighted for 3 different modulations (QPSK, 16QAM, and 64 QAM) with coding rate 1/2. SNRs for the simulation are set such that a Sub-frame Error Rate (SER) of 10% is achieved when no radar interference is present (SNRs shown in Table 3.2). The 10% error rate condition is the typical mechanism used for rate control based on CQI feedback to the transmitter. We further provide results for lower coding rates to show that coding is unable to correct the errors encountered due to radar interference. We then show how the errors manifest to gain insight into the behavior of LTE and its weakness when dealing with bursty interference.

3.3.1 AWGN Approximation

As a baseline for comparison, we replace the radar interference with Additive White Gaussian (AWGN) interference lasting the entire duration of a sub-frame. We then normalize the total energy in the interference to the energy level in a radar pulse as follows:

$$I_{AWGN}(t) = \mathcal{N}\left(0, \frac{\sigma^2_{AWGN}}{2}\right) + j \cdot \mathcal{N}\left(0, \frac{\sigma^2_{AWGN}}{2}\right) \tag{3.4}$$

$$\sigma^2_{AWGN} = \frac{t_{pulse}}{1ms} A^2 \tag{3.5}$$

We expect this approximation to be a poor one. Fig. 3.4 compares the AWGN approximation with the exact waveform which shows that for most interference intensity levels, there is a 10dB or greater difference for the same probability of sub-frame error. While the result confirms that the approximation is poor, it provides one additional piece of insight, namely, that LTE is resilient towards non-bursty interference (as it is designed to be).

The source of LTE's weakness when facing radar interference is considered in Section 3.4, but the results presented in the figure are surprising nonetheless. Given the robust coding in LTE and the short duration of the radar interference in relation to the sub-frame, we expect

that the interference will have minimal impact, an expectation that is not borne out by the presented results.

3.3.2 Waveforms, Modulations, Pilots, and Coding

Referring once again to Fig. 3.4, we highlight the fact that there is essentially no difference in LTE performance when radar interference occurs during a reference symbol vs. a data only symbol, a result which is expected. In Fig. 3.2, we observe that the energy in the pulse is largely concentrated within 300-400 kHz of bandwidth. Thus, presence of narrow-band radar will typically impact 6 pilots out of a total of 100 (there are a maximum of 2 pilots per symbol in a single RB).

Fig. 3.5a shows the impact of radar interference on various modulation orders. The trends are quite similar, but QPSK is able to sustain a 5-6 dB increase in PINR at the same error rate compared to 64QAM. This seems like a significant improvement, but as we will see in Section 3.5, far better gains can be realized.

Another method for LTE to combat poor channel conditions is to increase the redundancy in the channel code. Fig. 3.4 shows the gains when going from a coding rate of 1/2 to 1/3. The 1/3 rate is the most robust coding rate available for down-link data transmissions. This lower rate is able to sustain an additional 5dB in PINR at the same error rate, but once again, far better gains can be realized.

Fig. 3.5b shows how LTE reacts when facing different waveforms. Firstly, the separation between the curves is larger than the 10dB difference in pulse energy ($50\mu s$ is 10x longer than $5\mu s$ resulting in 10x energy). This gap due to the more spread nature of the interference energy. Sections 3.4 and 3.5 provide some explanation into why concentrated interference power has a catastrophic impact on the soft decoding process. We summarize the results presented in this section as follows:

1. The LTE down-link is more susceptible to bursty interference than expected given the sophisticated coding present

2. Adapting the coding rates and modulation orders does improve the codeword error rates

In the next section, we will delve more deeply into the exact cause of the errors and we provide a method to improve the resilience of LTE to radar interference more effectively than the built-in mechanisms explored so far.

3.4 LLR

To provide some intuition behind the errors in the LLR values, we will consider a simple BPSK constellation as shown in Fig. 3.6. This simple constellation is only used for the purposes of a simple illustration as the lowest modulation in LTE is of order 2 (QPSK) (a more detailed study of the effects of radar interference on received constellations is included in [22]). We define:

$\mathbf{y}$ The received complex symbol ($\mathbf{y} \in \mathbb{C}$)

$\mathbf{s}$ The transmitted complex symbol ($\mathbf{s} \in \mathbb{C}$)

$\mathbf{n}$ Circular symmetric complex Gaussian noise with variance σ_N^2 ($\mathbf{n} \in \mathbb{C}$)

Under the assumption of AWGN, the received constellation point is:

$$\mathbf{y} = \mathbf{s} + \mathbf{n}, \tag{3.6}$$

therefore, the Log Likelihood Ratio of the bit represented by the symbol can be computed as in (3.9).

$$\mathbf{s}_0 = -0 + 0j \qquad \text{bit } 0 \tag{3.7}$$

$$\mathbf{s}_1 = 1 + 0j \qquad \text{bit } 1 \tag{3.8}$$

$$\text{LLR} = \log \frac{exp\left\{-\frac{1}{2\sigma^2}\|\mathbf{y} - \mathbf{s}_1\|^2\right\}}{exp\left\{-\frac{1}{2\sigma^2}\|\mathbf{y} - \mathbf{s}_0\|^2\right\}} \tag{3.9}$$

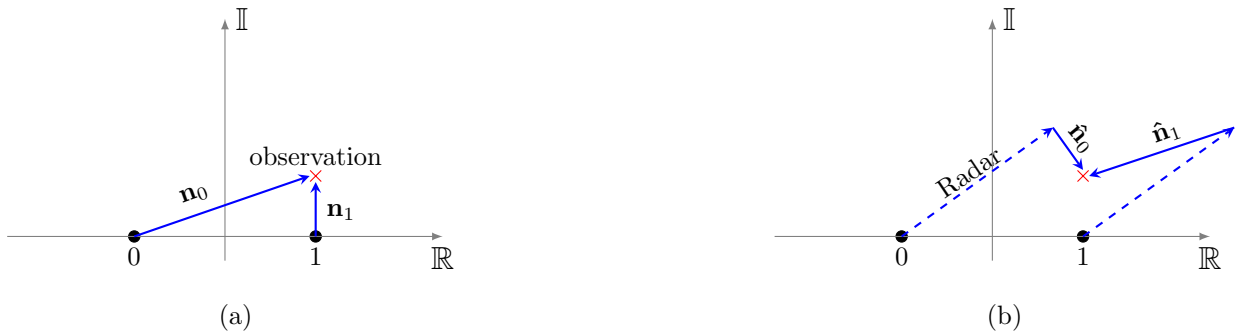


Figure 3.6: (a) High confidence due to low likelihood of the noise vector from '0' (b) Once interference is accounted for, the observed noise vector becomes far more likely reducing the confidence level

Computing the LLR in (3.10) is equivalent to computing the likelihood of having observed each of the two noise vectors drawn in Fig. 3.6a. Since the Gaussian probability density function decays rapidly away from the mean, the LLR of the observation in Fig. 3.6a will take a large positive value indicating high confidence that **1** was transmitted.

$$\text{LLR}_{\text{AWGN}} = \log \frac{\mathbf{Pr}(\mathbf{n}_1)}{\mathbf{Pr}(\mathbf{n}_0)} \tag{3.10}$$

$$\text{LLR}_{\text{RADAR}} = \log \frac{\mathbf{Pr}(\hat{\mathbf{n}}_1)}{\mathbf{Pr}(\hat{\mathbf{n}}_0)} \tag{3.11}$$

Yet the LLR computation only holds true when the parameters of the underlying noise/interference distribution have been accurately estimated and the distribution itself is well approximated by a Gaussian. With interference from a radar, these assumptions no longer hold. In fact, the observation in this case would be better explained by the sum contribution of noise as well as radar interference as shown in Fig. 3.6b. In that case, the resultant noise vector is much smaller in magnitude and the likelihood of a **0** being transmitted is significantly higher and the LLR should be computed as in (3.11).

The challenge with radar interference is that it is by its nature very bursty, therefore it is difficult to estimate and account for. Still, based on the CDF plot shown in Fig. 3.7b, it is obvious narrow-band interference from the radar tends to create extremely large LLR values.

In other words, if we detect outlying LLR values, we would be able to help the soft decoder recover by erasing those LLRs. That is the essence of the selective erasure of outliers.

3.5 Selective Erasure of Outliers

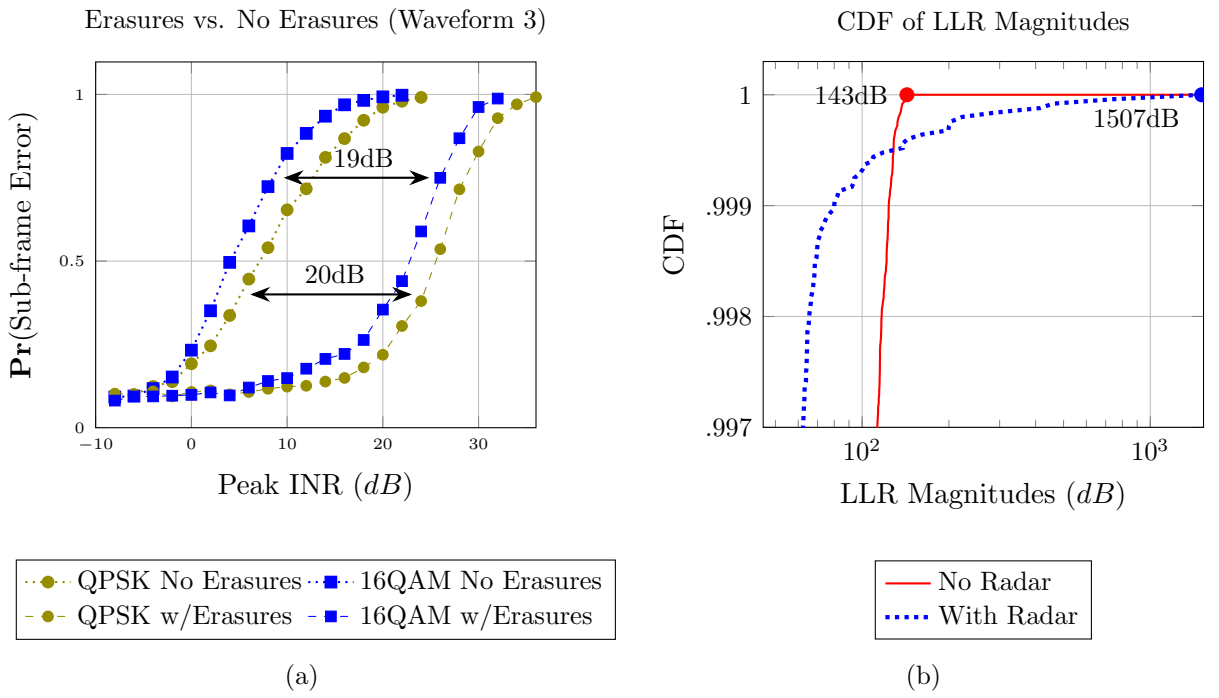


Figure 3.7: (a) Effect of selective erasures on mitigating LLR saturation. (b) CDF of LLR magnitudes with and without radar interference.

One simple way to detect outlier LLR values is to look at the LLR statistics in a given codeword.

$\mathbf{L}$ The set of LLR values for a given codeword

$\mathbf{L}_i$ The ith element in the set $\mathbf{L}$

$$\mu_{\text{LLR}} = \frac{1}{|\mathbf{L}|} \sum_{i=1}^{|\mathbf{L}|} |\mathbf{L}_i| \tag{3.12}$$

$$\sigma_{\text{LLR}} = \frac{1}{|\mathbf{L}|} \sum_{i=1}^{|\mathbf{L}|} (|\mathbf{L}_i| - \mu_{\text{LLR}})^2 \tag{3.13}$$

In other words, μ_{LLR} and σ_{LLR} are the sample mean and variance of the LLR *magnitudes* respectively. An LLR value is marked as an outlier if it meets the condition listed in (3.14):

$$\mathbf{L}_i > \mu_{\text{LLR}} + \eta \cdot \sigma_{\text{LLR}}, \tag{3.14}$$

where η is a positive design parameter used to set the outlier tolerance of the condition. We leave the task of selecting the best value for η for future work, but we have determined that a value of 5 produces very few false positives.

Once the outliers have been marked, their LLR values are erased (set to 0) which signifies a complete lack of certainty in the received bit. Thus, the soft decoder no longer relies on the LLR values of the interfered bits when attempting to decode the message. The redundancy inherent in the code will now have a chance to correct this erasure. Incidentally, the presence of such irregular LLR values can be used as a detection mechanism for radar interference which will be a topic of future work.

3.5.1 Simulation Results

Fig. 3.7b provides an important bit of insight into what currently occurs at an LTE receiver. When the radar is not present, the LLRs have magnitudes that are typically less than 150dB (which is already quite large and occurs rarely). Once the radar is switched on, we begin to see LLRs that exceed 200 dB in magnitude and can become as large as 1500dB. These high values can saturate the soft decoder making it unable to reconcile the false certainty in the interfered bits with the information from the non-interfered bits.

With $\eta = 5$, we re-run the simulations for two modulation orders: 16QAM and QPSK using Waveform 3. We immediately see a massive improvement in error rates (more than

18dB). We will leave analysis of how this method can improve operating regions for LTE as future work, suffice to say that this method can directly result in an immense expansion in areas that are suitable for LTE operation in the S-band.

3.6 Conclusion

In this paper, we examined the impact of narrow-band radar interference on the LTE down-link. We showed that there is negligible impact in interfering with reference symbols compared to data symbols, yet LTE systems are unable to cope well with narrow-band bursty interference on the down-link. We provided some insight into how the in-built LTE mechanisms perform when attempting to mitigate bursty interference through increased coding and lower modulation orders. Then, we explored the root cause of the performance impact at the LTE receiver demonstrating room for improvement in the design of LTE systems facing bursty interference (e.g. radar). Finally, we proposed a simple mechanism to mitigate such interference and showed the dramatic (order of magnitude) gains that it can achieve in resisting narrowband pulsed interference.

Chapter 4

SPECTRUM SHARING OF RADAR AND WI-FI NETWORKS: THE SENSING/THROUGHPUT TRADEOFF

The approach to spectrum sharing explored in this paper is based on unilateral action by Wi-Fi networks to prevent unacceptable interference to incumbent search radars (e.g. those operating in S-band). Specifically, we evaluate the ability of a single Wi-Fi network to *speedily detect* radar operation and to subsequently switch to a clear channel as a means of protecting them. We rely on the opportunistic use of naturally occurring *random* quiet/idle periods in a Wi-Fi network employing Distributed Coordination Function (DCF) to detect the presence of a radar using energy detection. We analytically characterize the statistical properties of the idle periods in terms of occurrence and duration in the full buffer and downlink only traffic cases, and verify our analysis using simulations. We then suggest simple modifications to Wi-Fi parameters in order to improve radar detection performance and examine the resulting Wi-Fi throughput costs. The key contribution of this work is to thoroughly characterize the Wi-Fi throughput vs. detection trade-off implicated by this coexistence mechanism.

4.1 Introduction

The fundamental challenge facing mobile network operators is the scarcity of spectrum allocated for civilian use. The demand (and hence the price) for spectrum has skyrocketed as cellular data and WLAN services have become ubiquitous in response to ever richer multimedia and interactive applications running on higher-end consumer devices. Acknowledging this recent exponential growth in data traffic on cellular networks, regulatory authorities have aimed at various strategies for systematically increasing the spectral efficiency of wireless

networks, as means for alleviating the spectrum crunch.

Looking ahead, the need for coexistence among dis-similar technologies will be a fundamental feature of wireless networks as a broad principle. For example, a significant chunk of Wi-Fi channels in the 5 GHz bands (declared U-NII, i.e. unlicensed, for North America) are utilized by various radar systems worldwide [70] [27], in fact, only 36% of 5GHz channels are unencumbered by radar protection requirements. Hence, 802.11 WLAN networks in the 5GHz band was the first significant instance of co-existence/spectrum sharing. To that end, Dynamic Frequency Selection (DFS) by Wi-Fi (based on channel sensing and radar avoidance) was the solution proposed to protect radars from WLAN systems [38].

What is more, an examination of the 225MHz-3.7GHz band assignments shows that 1700 MHz in this range has been set aside for radar and radio-location operation in the United States [10] making it a virtual certainty that issues of coexistence of radars with civilian systems will recur. In fact, the U.S. Department of Commerce has already recommended that 150 MHz of spectrum between 3550-3700 MHz be made available for wireless broadband applications [42] [14] which has led to further coexistence studies.

The reality is that spectrum usage patterns of radio-location systems (such as radars in the S-band), is very sporadic temporally, besides being spatially localized, leaving much of the spectrum heavily under-utilized in a spatio-temporal sense. As the FCC and NTIA consider spectrum sharing of parts of this band by communication networks, two critical questions must be answered:

1. What is the impact on communication systems' performance in the presence of interference from radars?

2. How can radars (deemed primary users) be protected from civilian wireless systems as required?

Answering both questions is essential to any successful spectrum sharing system. The first question is partly addressed in recent work by authors of this paper [**?**] [**?**], filings with the

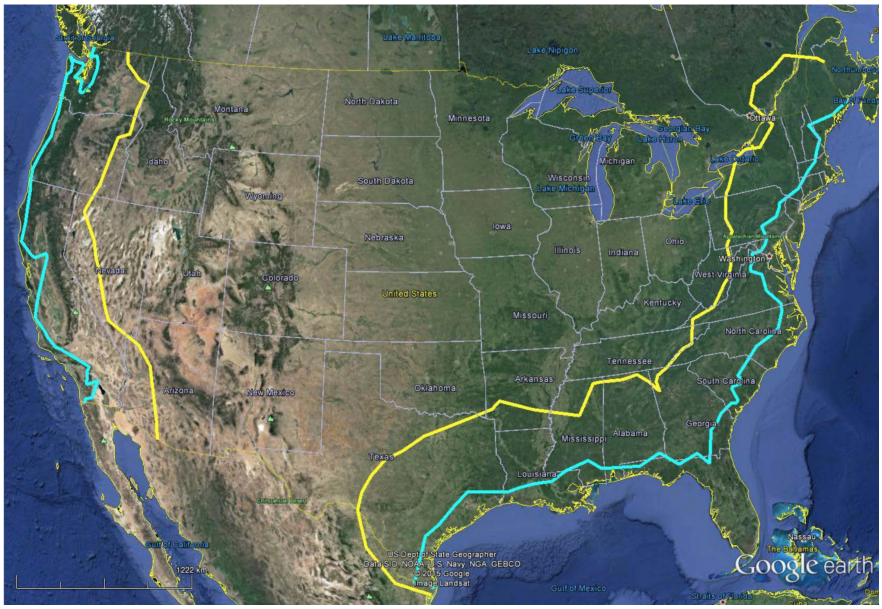


Figure 4.1: The original exclusion regions computed by the NTIA (yellow contours) were revised recently in [**?**] (blue contours). Even the revised region encompasses many of the major population centers such as Los Angeles and New York City.

U.S. Federal Communication Commission (FCC) [66], and the U.S. National Telecommunications and Information Administration (NTIA) [65] and remains a topic of active research. Additionally, there have been field and lab measurements performed by Virgina Tech and Google [12].

However, in this work we focus *exclusively* on the second question, namely the protection of the primary user. As can be readily appreciated, all coexistence design is a *balancing act* between the rights of the incumbent (to protected operation) and the secondary (to offer a new economically viable service); a point that while obvious in hindsight, has not been explored at depth in the manner presented here

Exclusion regions are spatial regions surrounding the protected primary (e.g. a monostatic radar) in which co-channel transmission by secondary users is forbidden; outside such regions, secondary operation is allowed as it is deemed to offer only harmless interference to

primary receivers (Fig. 4.1). These exclusion regions are determined by regulatory organizations (such as the NTIA) under the assumption that secondary networks (e.g. Wi-Fi) do not take any measures to mitigate interference to the radar systems [51]. In such scenarios, these no-go exclusion regions can extend for hundreds of kilometers radially from radar location, which given the proximity of radars to population centers (precisely the places where there is demand for such secondary networks), makes deployment of secondary systems un-attractive as a business proposition.

One method to minimize interference caused to radars (and hence shrink the exclusion region) relies on signal processing techniques such as multi-antenna nulling. In [68] for example, the authors consider such a technique for minimizing radar to communication system interference by employing knowledge of the interference channel matrix (presumably through reference signaling). Meanwhile, the authors in [19] consider an even deeper level of cooperation between the radar and communication systems in their joint formulation. In many cases, such broad cooperation may be difficult to achieve in practice.

A second class of methods to shrink these exclusion regions follows the *detect and switch* regime which is the focus of this paper. In such a scheme, it is crucial that communication systems detect active radars with *high reliability and speed* in order to limit interference to these incumbents due to secondary network transmissions. In our opinion, a full coexistence solution will likely employ multiple effective mechanisms, i.e. detect and switch may be employed along with other complementary approaches. This view is shared by the NTIA [**?**] which states: "NTIA's review of the public record indicates that many commenters proposed employing sensing technologies [to better enable] opportunistic access to the spectrum. NTIA agrees with these commenters and believes that sensing will help provide maximum flexibility". However, the FCC's current plans for spectrum sharing in the 3.5GHz band forgo sensing based opportunistic access (time interleaved access) and instead call for a Spectrum Access System to govern usage of the shared spectrum [14]. Hence, solutions based on detection and channel switching are a worthwhile avenue of future development for spectrum sharing between communication and radar systems although they may not be applicable in

all scenarios (i.e. for particular radars).

The inherent advantage of the detect and switch scheme is that it is easier to implement and requires minimal knowledge of the radar when compared to the aforementioned interference nulling techniques. Generally speaking, there are two broad approaches for a secondary network to implement such primary user detection; the first requires all secondary user transmissions to cease (quiet/idle periods) either via scheduling or due to inherent properties of the MAC protocol employed, while the second requires some form of primary/secondary coordination. In general, the cost and security implications of inter-network coordination between such dis-similar systems (one a secure Federal installation and the other operated by a private operator) makes it an unattractive solution. Meanwhile, inserting scheduled idle times in Wi-Fi for sensing would require significant changes and introduce additional complications to the MAC protocol and is clearly the less desirable option [33] [15]. Further, this is likely unnecessary based on the key observation that within the Distributed Coordination Function (DCF) employed by Wi-Fi, there exist natural periods of network operation whereby *all* nodes are backing off or sensing the medium, leading to randomly occurring quiet periods of random duration.

However, these naturally occurring idle periods typically comprise only a small portion of channel time on average[1]; hence the chances of detecting the short duration and low duty cycle radar pulses within such short random quiet intervals reliably is a largely open question. On the flip side, if the number or duration of such quiet intervals is increased (either via scheduling or other means) to improve radar detection probability, it will result in a commensurate loss in communication network throughput.

In this work, we study the nature of randomly occurring quiet periods in Wi-Fi networks analytically where possible, and through simulations elsewhere. We characterize the performance of a radar detection scheme relying on such idle/quiet periods for detection and illustrate the trade-offs between network throughput and improved detection performance.

---

[1]This fraction decreases as Wi-Fi node density or traffic load increases

We investigate two ways of increasing such quiet durations and compare the trade-offs associated with each method. The decisive contribution of this work is to present a method for achieving the desired radar detection performance and establishing the WLAN throughput trade-off incurred. While our work is aimed squarely at the S-band, it can easily be applied to DFS in 5GHz.

4.1.1 Related Work

Since Wi-Fi fundamentally uses Carrier Sensing (i.e. estimation of current channel state) as a key component of transmit access control (as part of DCF or CSMA/CA MAC protocol), it has been a leading candidate for cognitive network operation, particularly in scenarios with static primary user activity (e.g. TV Whitespaces) for which the 802.11af standard was ratified in 2013 [11]. In cases where the primary is more dynamic (i.e. transient), scheduling of sensing periods for detection of primary activity has seen proposed (in part, by our own earlier work). In [15], the authors consider a method of periodically scheduling idle intervals for the purposes of sensing. The scheme incurs some complication in implementation due to the increase in packet fragmentation and consequent increase in coordination overhead. In [33], we considered extending (some of) naturally occurring idle periods in the Wi-Fi DCF MAC for the purposes of channel sensing which did not suffer from the complications of [15] and was shown to detect transient out-of-network interference reliably.

In the context of radar and DFS, Zarikoff and Weldon [72] analyzed the radar detection delay in a simple Time Division Duplexed system (TDD) while also noting the absence of such analysis in the literature. The potential introduction of Wi-Fi to the S-band (3.5GHz) presents an opportunity to revisit the ideas of [33] in a more methodical setting with deeper analysis. Fundamentally, the coexistence scenario considered between Wi-Fi and pulsed search radars presents the following signal processing challenge: to reliably and speedily detect a low duty cycle pulsed signal (radar) that is highly directional due to radar beam rotation.

4.2 Coexistence Scenario

Passive detection of primary user (radar) activity by the secondary user (WiFi) in order to limit interference (by either controlling its own in-band transmission or switching to a different unoccupied channel) is measured by the obvious metric -

- **Detection Delay:** The interval from the instant the incumbent (radar) becomes active until its successful detection by the secondary network (Wi-Fi).

which is impacted by a) radar pulse duration and b) pulse repetition interval (PRI) [2].

Typically, in other applications of the shared spectrum paradigm (e.g. wireless microphones), the incumbents transmit high duty cycle signals; any Wi-Fi idle period will overlap an incumbant's transmission with high probability allowing for effective detection. In contrast, radars pose a particular challenge due to their extremely low duty cycles combined with requirement for speedy protection when they become active. In this work, we characterize the detection delay of radar by Wi-Fi systems for various Wi-Fi/radar system parameters to establish whether such a system can adequately protect radar and if the associated cost to the WLAN in terms of throughput loss is acceptable.

4.2.1 A Brief Summary of DFS in 5GHz

As already stated, DFS comprises of a radar detection and avoidance scheme by the secondary (Wi-Fi) network. The detection algorithm has two primary components:

1. **Out of Service Monitoring:** This refers to the period prior at the start (e.g. at access point start-up) when each AP must scan the channels to determine if radar is present. The scan procedure is at least 60 seconds and is required to detect radar signals above -62dBm with detection rate of 99.99%.

[2]The pulse repetition interval corresponds to the period between two consecutive radar pulses and is inversely proportional to the number of radar pulses transmitted per second (or pulse repetition frequency).

2. **In Service Monitoring:** This refers to the ability of an active Wi-Fi network to detect a radar that begins operation *after* the initial setup period of the network. DFS requires that during the regular operation, WLANs must detect a radar with a success rate of 60% for radar signals above −62dBm.

The detection rate is determined by the probability that a radar pulse *burst* is detected by a Wi-Fi network in each detection phase. Compliance with the radar protection requirements is based primarily on verifying these detection rates under the test scenarios and example radars defined in [27] or other similar requirements based on regional regulations. Once a radar has been detected, the WLAN has limited time to steer all associated devices to a different channel with no radar presence.

Clearly the DFS rules were aimed specifically at the 5GHz band and may be insufficient for protecting radars in other bands. Yet, they are the only radar detection guidelines that the authors are aware of and will be used as a design target in the rest of the paper. In practice, we expect that coordination between Wi-Fi access points (e.g. through a cloud service) will be used to improve system-wide performance.

4.2.2 Setup & Model

In this work, we consider an isolated Wi-Fi 'cell', i.e. a single access point with n connected clients, impacted by a pulsed radar. In the following sections, this will be studied for the following two cases (that produce significantly different results):

1. Downlink only traffic from the Access Point (AP) to the associated stations;

2. Full buffer at *all* nodes in the network.

The second setup corresponds to the model analyzed in [16]. It is important to note that in this model, we can represent a series of overlapping networks as a single larger network if we assume that no hidden nodes exist. Analyzing a more general setting with an arbitrary interference graph is intractable and outside the scope of this paper.

Slot durations and frame spacings conform to the 802.11 standards [9] as indicated in Table 4.2. Network time is ***slotted*** with a resolution of $t_{\text{slot}} = 1\mu s$ as baseline. Furthermore, we assume that a radar pulse that arrives during an idle Wi-Fi period is perfectly detected using a scheme such as energy detection. For example, the Wi-Fi Dynamic Frequency Selection (DFS) mechanism requires radar pulses to be detected 99.99% of the time at a received signal power level of -62dBm which is very reasonable [3].

Example parameters for radars operating in 3.5GHz and 5GHz are included in Table 4.1 based on [35] [27] [8]. The radars considered transmit a series of equally spaced pulses called a pulse *burst* in a given direction before rotating to a different direction[4]. The duration of the burst, and consequently the duration that the radar is pointed in a fixed direction is referred to as the *dwell time* and the interval between two consecutive pulses is labeled as the Pulse Repetition Interval (PRI) with duration t_{pri}. While other radar types such as pulse compression radars are also employed in the band, we leave them as a topic of future work.

The radars we will consider tend to have low duty cycles (often less than 1%) with peak transmit powers that can exceed 90dBm. Accordingly, a simple link-budget analysis using an irregular terrain path-loss model (e.g. Fig. 5 in [31]) would indicate that radar pulse power at a Wi-Fi AP can exceed -62dBm at distances of tens of kilometers from the radar. As a result, energy detection schemes such as DFS can be very effective in the vast (often densely populated) area immediately surrounding such a radar.

We also note that radar detection is conducted by a single node on behalf of the secondary network, which logically should be the AP (since subsequent to determination of radar activity, it is can trigger DFS). Finally, in this work we do not account for the impact of radar interference on Wi-Fi throughput. The extremely low duty cycle of radar interference combined with the typically robust coding available in newer generations of Wi-Fi (i.e. LDPC) makes Wi-Fi resistant to interference from radar, i.e. Wi-Fi packet losses due to a radar pulse 'hit' is a secondary effect (which we neglect) compared to the throughput costs

[3]The impact of imperfect detection is deferred for future work.

[4]Directionality could be achieved through a phased array in place of mechanical rotation

Table 4.1: Example Radar Parameters

Parameter	Values
Pulse Repitition Interval (t_{pri})	$100\mu s - 5ms$
Pulse Duration	$0.8\mu s - 50\mu s$
Pulses Per Burst	$10 - 25$
Peak Power	up to 90dBm
Antenna Main Beam Gain	up to 40dBi

incurred by the Wi-Fi network due to requirements for increased sensing/idle periods.

4.3 Characterizing Wi-Fi Quiet Periods

In this section, we characterize the stochastic properties of quiet/idle periods in Wi-Fi networks under DCF. Since WLAN networks may operate with different node configurations and traffic loads that (as we will show) have significant impact on efficient detection, we examine two distinct canonical scenarios:

1. Fully saturated uplink/downlink networks where all nodes have full outbound traffic buffer;

2. Saturated *downlink only* networks where the Access Point is the only node with outgoing traffic (corresponds to majority data 'pull' applications by clients such as web browsing).

A major reason for focusing on these two scenarios is that we are able to develop analytical models (as shown next) that provides insight and context for the more detailed simulation study. We begin by providing a basic description of the Wi-Fi DCF essentials for completeness and as prelude to our analysis.

Table 4.2: Wi-Fi Timing Parameters

Parameter	Description	Duration
t_{slot}	Timing Slot	$1\mu s$
t_{bo}	Backoff	$9 \times t_{\text{slot}}$
t_{difs}	DIFS	$34 \times t_{\text{slot}}$ (5GHz)
t_{sifs}	SIFS	$16 \times t_{\text{slot}}$ (5GHz)
t_{ack}	ACK	$48 \times t_{\text{slot}}$
t_{payload}	Payload	up to $\approx 3000 \times t_{\text{slot}}$

t_{slot} = 1 slot = 1 microsecond

4.3.1 Wi-Fi Basics

The Wi-Fi standard employs a Carrier Sensing Medium Access with Collision Avoidance (CSMA/CA) mechanism for accessing the wireless medium [9]. The specific implementation used in Wi-Fi – the Distributed Coordination Function (DCF) – is a distributed slotted medium access scheme with an exponential back-off.

The algorithm operates in the following way: each node attempting transmission must first ensure that the medium has been idle for a duration labeled the DCF Interframe Spacing period (DIFS) which is typically in the range of 28-50μs. Once the medium has remained idle for a DIFS period, the node selects a back-off counter uniformly at random in the range of $[0, 2^m W - 1]$ [5] where the value of m is initialized to 0. The node then counts down from the selected back-off value in a slotted fashion (i.e. the node decrements the counter every t_{BO} microseconds) as long as no other transmissions are detected. If during the countdown a transmission is detected, the counting is paused until the medium has once again been detected idle for a DIFS period. Once the counter hits zero, the node transmits its payload

[5] Typical W values are 16, 32.

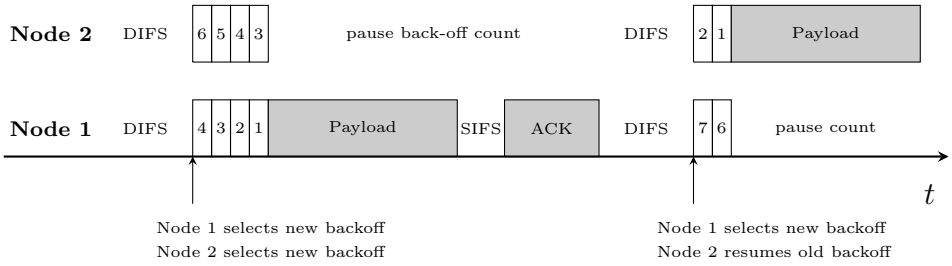


Figure 4.2: This parallel timeline for two nodes contending for access to the same channel shows the role of the random back-off in reducing collisions.

(illustrated in Fig. 4.2). Any node that did not complete its countdown to zero in the previous transmission round, resumes the countdown at the next opportunity without selecting a new back-off value.

A collision event occurs if and only if two nodes select the same back-off counter value at the end of a DIFS period. In case of a collision, the value of m (the back-off stage) is incremented by one (binary exponential backoff) such that the back-off counter is doubled for the next attempt, thereby reducing the probability that any two nodes select the same back-off counter repeatedly. Once a transmission has been completed successfully, the value of m is reset to 0. The value of m cannot exceed a maximum value $m_{\max}$ (typically values are 3-5).

4.3.2 Statistical Characterization of the DCF in the Saturated Regime

In [16], Bianchi produced an elegant performance analysis of DCF for the scenario that all nodes always have a full buffer of outgoing traffic. Following [16], we introduce the following definitions:

n The total number of nodes in the network

$m_{\mathbf{max}}$ The maximum back-off stage (max value of m)

W The minimum back-off window size

τ Probability that a generic node attempts transmission in a back-off slot

p Probability of collision for a generic packet in the network

$P_{\mathbf{tr}}$ The probability that at *least* one node attempts transmission in a back-off slot

$P_{\mathbf{s}}$ Probability of a successful packet transmission

$t_{\mathbf{s}}$ Duration of a successful transmission cycle (includes ACK)

$t_{\mathbf{c}}$ Duration of an unsuccessful (collision) transmission cycle

Accordingly, the transmission probability τ of any node can be obtained by solving the following system of non-linear equations [16]:

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1) + pW\left(1-(2p)^{m_{\max}}\right)} \tag{4.1}$$

$$p = 1 - (1-\tau)^{n-1} \tag{4.2}$$

Lastly, expressions can be obtained for the following terms:

$$P_{\mathrm{tr}} = 1 - (1-\tau)^{n} \tag{4.3}$$

$$P_{\mathrm{s}} = \frac{n\tau(1-\tau)^{n-1}}{P_{\mathrm{tr}}} \tag{4.4}$$

$$t_{\mathrm{s}} = t_{\mathrm{payload}} + t_{\mathrm{sifs}} + t_{\mathrm{ack}} + t_{\mathrm{difs}} \tag{4.5}$$

$$t_{\mathrm{c}} = t_{\mathrm{payload}} + t_{\mathrm{difs}} \tag{4.6}$$

$$\text{throughput} = \frac{t_{\mathrm{payload}}}{(1-P_{\mathrm{tr}})t_{\mathrm{bo}} + P_{\mathrm{s}}P_{\mathrm{tr}}t_{\mathrm{s}} + (1-P_{\mathrm{s}})P_{\mathrm{tr}}t_{\mathrm{c}}} \tag{4.7}$$

One important caveat is that Bianchi's analysis is known to be accurate for larger numbers of nodes (e.g. 10), in the WiFi network, and less so when the number of nodes is very small (e.g. 2-3)

Using the results summarized, we describe Wi-Fi network activity as an alternating idle/busy renewal process (Fig. 4.3) where each state encompasses multiple MAC structures:

- **Idle:** The idle period is comprised of the DCF Interframe Spacing (DIFS) and random back-off intervals. The random duration of this idle period is governed primarily by the number of idle back-off slots.

- **Busy:** The busy period is of random length based on whether the transmission is successful (necessitating an ACK message), or unsuccessful, thus characterized by the probability of a successful transmission.

Fig. 4.3 shows an example of this renewal process. We define:

B_k The *random* duration of the busy period in the k^{th} renewal cycle. Randomness is due to the success or failure of transmission.

I_k The *random* duration of the idle period in the k^{th} renewal cycle. The randomness in the idle duration is due to the random back-off

Q_k The *random* number of back-off slots during idle period I_k. $Q_k \sim \text{Geo}(P_{\text{tr}})$

For the k^{th} renewal cycle, we use B_k^{start} and B_k^{end} signify the start and end time slots for busy period B_k (similarly for I_k). Then, we can show that:

$$I_k \triangleq Q_k \cdot t_{\text{bo}} + t_{\text{difs}} \tag{4.8}$$

$$\mathbf{P}(Q_k = q_k) = P_{\text{tr}} \cdot (1 - P_{\text{tr}})^{q_k} \quad q_k = 0, 1, \ldots \tag{4.9}$$

and

$$\mathbf{P}(B_k = b) = \begin{cases} P_{\text{s}} & \text{if } b = t_{\text{payload}} + t_{\text{sifs}} + t_{\text{ack}} \\ 1 - P_{\text{s}} & \text{if } b = t_{\text{payload}} \end{cases} \tag{4.10}$$

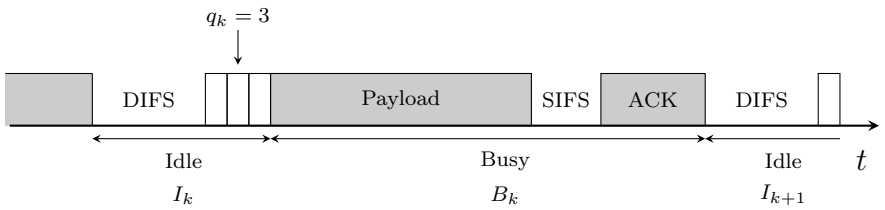


Figure 4.3: Wi-Fi operation as an alternating idle/busy renewal process: The k^{th} cycle consists of a) an idle period that equals the fixed duration DIFS and a random number of back-off slots (3 in this illustration) and b) busy period that consists of payload, SIFS, and ACK (in the case of a successful transmission) and only the payload (in case of a collision).

4.3.3 DCF with Downlink Only Traffic

A very different scenario compared to a fully saturated network is when only the Access Point's buffer is full (downlink only traffic) corresponding to exclusively data pull type applications (web browsing) by associated nodes, who have no (negligible) uplink traffic. In that case, there will be no collisions, and therefore, the success probability of any transmission equals 1. As such, we can show that:

$$\mathbf{P}(Q_k = q_k) = \frac{1}{W} \text{ for } 0 \leq q_k < W \tag{4.11}$$

Likewise, since no collisions can occur, the busy period are deterministic:

$$\mathbf{P}(B_k = t_{\text{payload}} + t_{\text{sifs}} + t_{\text{ack}}) = 1 \tag{4.12}$$

This simple characterization allows us to compare the distribution of the quiet period duration in the downlink only as well the downlink/uplink scenario. In Fig. 4.4, we show this comparison for multiple node configurations for the parameters listed in Table 4.2. Fundamentally, as the number of nodes increases, the duration of quiet periods as well as their proportion as a percentage of total channel time decreases which as we will show leads to a commensurate increase in detection delay.

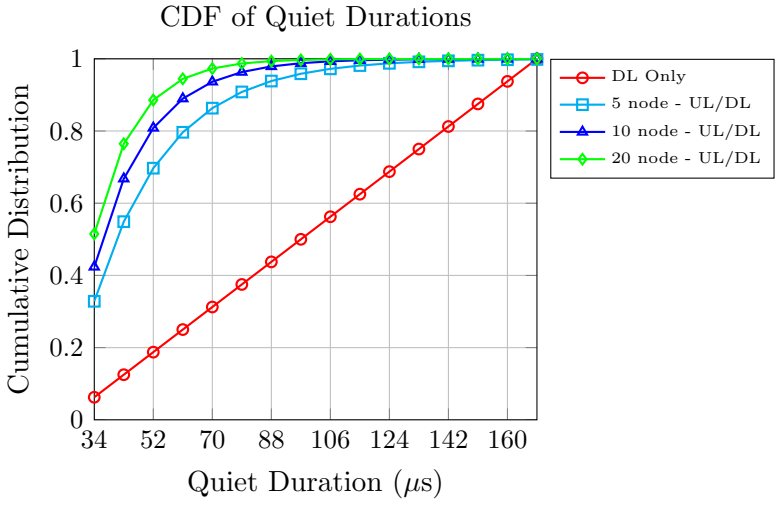
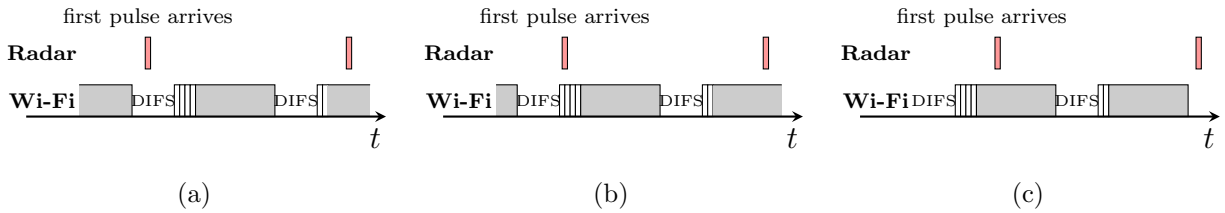


Figure 4.4: A comparison of the distributions of the quiet durations for various scenarios. Here $W = 16$ and $m = 5$.



(a) (b) (c)

Figure 4.5: (a) In this case, the first pulse arrives during a DIFS portion of the idle period. (b) In this case, the first pulse arrives during the back-off portion of the idle period. (c) In this case, the first pulse arrives during the busy period.

$$\text{throughput} = \frac{t_{\text{payload}}}{\mathbb{E}[B_k] + \mathbb{E}[I_k]} = \frac{t_{\text{payload}}}{t_{\text{s}} + \frac{W-1}{2} t_{\text{bo}}} \tag{4.13}$$

4.4 Radar Detection in Wi-Fi

Since we assume no synchronization between the radar pulses and the Wi-Fi network, once the radar becomes active, the first pulse it transmits will arrive at random in relation to the Wi-Fi network state. From the alternating renewal theorem, we can show that if a pulse arrives at a random time instant, the Wi-Fi network will be in an idle state with probability P_{idle} (Fig. 4.5a and 4.5b) and in a busy state with probability P_{busy} (Fig. 4.5c) computed as below:

$$P_{\text{busy}} = \frac{\mathbb{E}[B_k]}{\mathbb{E}[B_k] + \mathbb{E}[I_k]} \tag{4.14}$$

$$P_{\text{idle}} = 1 - P_{\text{busy}} \tag{4.15}$$

Since we assume that any radar pulse arriving during an idle period can be detected perfectly (i.e. with probability 1), the detection delay (defined in Section 4.3) is the interval measured from the first (reference) pulse, till the first time a radar pulse that arrives during a Wi-Fi idle period. Hence if the first pulse arrives during an idle period, the detection delay is said to be zero.

For the remainder of our analysis, we will treat the random variable B_k as a constant t_{busy} which is set to equal expected duration of B ($E[B]$). This is anyway reasonable since the ACK/SIFS durations are typically negligible compared to the payload duration (in the downlink only case, this approximation is exact) and does not impact any of the insights from the analysis.

$$t_{\text{busy}} \triangleq \mathbb{E}[B] = t_{\text{PAYLOAD}} + P_{\text{s}}(t_{\text{SIFS}} + t_{\text{ACK}}) \tag{4.16}$$

Next, we define:

S_i The *random* arrival time of the i^{th} radar pulse. Since all timing is *slotted*, $S_i \in \mathbb{N}$ and clearly $S_i = S_{i-1} + t_{\text{pri}}$

N_i The index of the renewal period in which pulse i arrives (e.g. in Fig. 4.6, $N_1 = N_2 = 1$ since pulses 1 and 2 arrive during busy period 1, and $N_3 = N_4 = 2$)

A_i The *random offset* of the i^{th} pulse inside the associated busy period. $A_i \in \{1, 2, \cdots, t_{\text{busy}}\}$. $A_i \triangleq S_i - B_{N_i}^{\text{start}}$

r_i The remaining time from the end of the busy period till the arrival of pulse $i+1$ as calculated in (4.18). A negative value for r_i signifies that a pair of pulses arrive in the same busy period (e.g. pulses 1,2 in Fig. 4.6)

D The random variable describing the detection delay in number of pulses where $D = 1$ signifies detection of the first arriving pulse. $D \in \{1, 2, ...\}$

$d_{\mathbf{burst}}$ The number of pulses in a radar pulse burst

For the radar to be detected with the first arriving pulse ($D = 1$), the network must be idle at arrival time which occurs with probability P_{idle} according to (4.15). For $D > 1$, our approach is to compute the detection delay distribution recursively, therefore, our derivation focuses on obtaining an expression for the following conditional probability:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) \tag{4.17}$$

which denotes the probability that pulse $i+1$ arrives at offset a_{i+1} in an upcoming busy period given that pulse i arrived at offset a_i in a busy period.

One key observation to make is that (4.17) *does not* depend on arrival values prior to i (e.g. A_{i-1}), a fact that is used to help simplify our analysis. Even so, we must consider two separate classes in the upcoming subsections:

1. $t_{\text{pri}} < t_{\text{busy}}$ (Fig. 4.6)

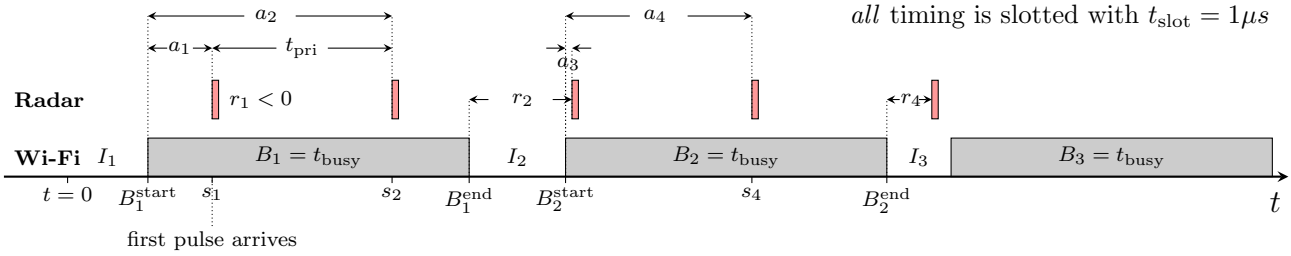


Figure 4.6: Example timeline for a detection delay of 5 ($D = 5$) for $t_{\text{pri}} < t_{\text{busy}}$. The fifth pulse is the first that arrives during an idle period. Busy periods are of fixed duration t_{busy}, while idle periods are of a random duration.

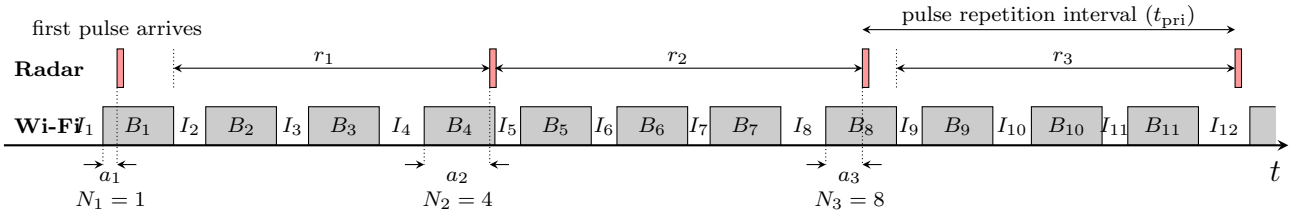


Figure 4.7: Here we show a sample time-line for a detection delay of 4 pulses (i.e. $D = 4$) for $t_{\text{pri}} > t_{\text{busy}}$. Note that $N_i = n_i$ signifies that pulse i arrives during busy period B_{n_i}.

2. $t_{\text{pri}} \geq t_{\text{busy}}$ (Fig. 4.7)

Before doing so, we define:

$$r_i \triangleq a_i + t_{\text{pri}} - t_{\text{busy}} \tag{4.18}$$

4.4.1 $t_{pri} < t_{busy}$

When $t_{\text{pri}} < t_{\text{busy}}$, multiple radar pulses can arrive within a single busy period (Fig. 4.6). An example of this coexistence class is when a radar with short PRI (e.g. $200\mu s$) is sharing spectrum with an 802.11 WLAN employing $3ms$ aggregated frames. **Case 1:** $r_i < 0$

This condition is satisfied if and only if both pulses fall within he same busy period. An example of this case can be observed with pulses 1 and 2 in Fig. 4.6. As shown, a_1 and a_2 differ by exactly t_{pri}. In this case, we have the trivial (deterministic) result that:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) = \begin{cases} 1 & \text{when } a_{i+1} = a_i + t_{\text{pri}} \\ 0 & \text{otherwise} \end{cases} \tag{4.19}$$

Case 2: $r_i \geq 0$

If pulse $i+1$ falls within the next renewal cycle, we can show that:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) = \mathbf{P}(I_{N_{i+1}} = r_i - a_{i+1}) \tag{4.20}$$

Recall that according to (4.8):

$$I_{N_{i+1}} = Q_{N_{i+1}} \cdot t_{\text{bo}} + t_{\text{difs}};\ Q_{N_{i+1}} \in \mathbb{N}, \tag{4.21}$$

therefore, we can write:

$$\mathbf{P}(I_{N_{i+1}} = r_i - a_{i+1}) = \mathbf{P}\left(Q_{N_i+1} = q_{N_i+1}\right), \tag{4.22}$$

where

$$q_{N_i+1} = \frac{r_i - a_{i+1} - t_{\text{difs}}}{t_{\text{bo}}}. \tag{4.23}$$

Hence, we conclude that:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) = \begin{cases} \mathbf{P}(Q_{N_i+1} = q_{N_i+1}) & r_i \geq 0 \\ 1 & r_i < 0 \text{ and } a_{i+1} = a_i + t_{\text{pri}} \\ 0 & \text{otherwise} \end{cases} \tag{4.24}$$

where $\mathbf{P}(Q_{N_i+1} = q_{N_i+1})$ is obtained from (4.9) or (4.11) based on whether we consider the downlink only or the uplink/downlink configuration.

4.4.2 $t_{pri} \geq t_{busy}$

For this class, it is possible for multiple busy periods to occur in a single PRI as would be the case for a long PRI radar coexisting with a WLAN not using frame aggregation. An example is shown in Fig. 4.7. It is straightforward to see that given some remainder time r_i, the next pulse cannot occur any later than busy period $N_i + K$, where:

$$K = \left\lceil \frac{r_i}{t_{\text{busy}} + t_{\text{difs}}} \right\rceil \tag{4.25}$$

therefore:

$$N_i < N_{i+1} \leq N_i + K \tag{4.26}$$

Provided the value of r_i as calculated in (4.18), we have:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) = 0 \;\text{ if } r_i - t_{\text{difs}} < 0 \tag{4.27}$$

Otherwise, if $r_i \geq 0$, for each $k = 1, \ldots, K$, we can show that:

$$\begin{aligned} &\mathbf{P}\left(\sum_{j=1}^{k} I_{N_i+j} = r_i - a_{i+1} - t_{\text{busy}}(k-1) \right) \\ &= \mathbf{P}\left(\sum_{j=1}^{k} Q_{N_i+j} = \hat{q} \right) \\ &\text{where } \hat{q} = \frac{r_i - a_{i+1} - t_{\text{busy}}(k-1) - t_{\text{difs}} k}{t_{\text{bo}}} \\ &r_i - t_{\text{difs}} \geq 0 \text{ and } \hat{q} = 0, 1, \ldots \end{aligned} \tag{4.28}$$

The intuition behind this formulation is that for pulse $i+1$ to fall within busy period $N_i + k$, $k-1$ busy periods and k idle periods must have elapsed prior to B_{N_i+k}. Meanwhile, the quantity $\hat{q}$ is nothing but the sum of all back-off slots that must have remained idle for this event to occur.

Now, depending on the network configuration of interest (uplink/downlink or downlink only), the distribution of Q_k will differ as will the distribution of the sum. When considering

an uplink/downlink network, Q_k is distributed geometrically, hence the sum can be computed using a negative binomial:

$$\mathbf{P}\left(\sum_{j=1}^{k} Q_{N_i+j} = \hat{q}\right) = \binom{k-1+\hat{q}}{k-1} P_{\text{tr}}^{k}(1-P_{\text{tr}})^{\hat{q}} \tag{4.29}$$

In contrast, in the downlink only case, Q is discrete uniform and according to [18], the sum distribution can be calculated as:

$$\begin{aligned}\mathbf{P}\left(\sum_{j=1}^{k} Q_{N_i+j} = \hat{q}\right) &= \frac{k}{(W+1)^k}\times \\ &\sum_{u=0}^{\lfloor \hat{q}/W \rfloor} \frac{\Gamma(k+\hat{q}-u\cdot W)(-1)^u}{\Gamma(u+1)\Gamma(k-u+1)\Gamma(\hat{q}-u\cdot W+1)}\end{aligned} \tag{4.30}$$

where $\Gamma(.)$ is the Gamma function for integer arguments. As a final step, we must sum over all possible values of k:

$$\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i) = \sum_{k=1}^{K} \mathbf{P}\left(\sum_{j=1}^{k} Q_{N_i+j} = \hat{q}\right) \tag{4.31}$$

$$\text{where } \hat{q} = \frac{r_i - a_{i+1} - t_{\text{busy}}(k-1) - t_{\text{difs}}k}{t_{\text{bo}}}$$

$$r_i - t_{\text{difs}} \geq 0 \text{ and } \hat{q} = 0, 1, \ldots$$

4.4.3 Detection Delay

We gather and summarize the result for $\mathbf{P}(A_{i+1} = a_{i+1} | A_i = a_i)$ as follows:

$t_{\text{pri}} < t_{\text{busy}}$ and	uplink/downlink: Eq. 4.24, 4.9
$t_{\text{pri}} < t_{\text{busy}}$ and	downlink only: Eq. 4.24, 4.11
$t_{\text{pri}} \geq t_{\text{busy}}$ and	uplink/downlink: Eq. 4.29
$t_{\text{pri}} \geq t_{\text{busy}}$ and	downlink only: Eq. 4.31

With expressions in hand for the various network configurations and coexistence classes, we can compute the detection delay recursively. If the first pulse arrives at $a_1 = \alpha$, we can

write:

$$\mathbf{P}(D=2|\alpha) = 1 - \sum_{\alpha'=1}^{t_{\text{busy}}} \mathbf{P}(A_{i+1}=\alpha'|A_i=\alpha) \tag{4.32}$$

then for $d > 2$, we have:

$$\mathbf{P}(D=d|\alpha) = \sum_{\alpha'=1}^{t_{\text{busy}}} \mathbf{P}(A_{i+1}=\alpha'|A_i=\alpha)\mathbf{P}(D=d-1|\alpha') \tag{4.33}$$

and the full expression for the detection delay can be written as:

$$\mathbf{P}(D=d) = \begin{cases} 1 - P_{\text{busy}} & \text{when } d=1 \\ \frac{P_{\text{busy}}}{t_{\text{busy}}} \sum_{a_1=1}^{t_{\text{busy}}} \mathbf{P}(D=d|A_1=a_1) & \text{otherwise} \end{cases} \tag{4.34}$$

where:

$$A_1 \sim \text{Unif}(1, t_{\text{busy}}) \tag{4.35}$$

Finally, we can obtain the detection rate for a radar burst of d_{burst} pulses as:

$$P_d(d_{\text{burst}}) = \mathbf{P}(D < d_{\text{burst}}) \tag{4.36}$$

4.4.4 Simulations and Verification

Having obtained the probability distributions of the detection delay in the previous subsection, we now aim to validate our analysis through simulations. Specifically, we examine four scenarios of interest to understand the impact of various network parameters on detection delay (Table 4.3) (all Wi-Fi timing parameters are set according to Table 4.2).

Fig. 4.8 shows a comparison of analytical and simulation results for the scenarios in Table 4.3. It is immediately apparent that our analysis closely matches the results of our simulations. As the payload size decreases (approaching the size of the ACK/SIFS), we expect that our t_{busy} approximation becomes less accurate. However, even in these cases, our analysis remains very close and is a good predictor for 60^{th} and 90^{th} percentile detection delays which map directly to the *in-service monitoring* requirements of interest to DFS.

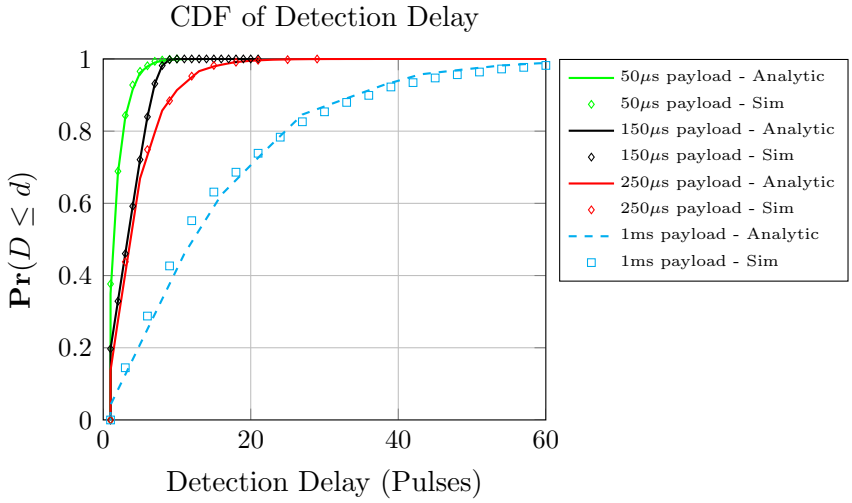


Figure 4.8: Simulations vs. Analysis for a network with 10 clients and various payload sizes and PRI = 200μs.

Clearly, increases in Wi-Fi payload duration lead to significantly higher detection delays. While undesirable, this increase in detection delay is accompanied by an increase in network throughput (Table 4.3), a trade-off that can be navigated intelligently to maximize throughput while meeting detection requirements as we will show in the next section.

An additional area that requires examination is how the analytical models match simulations when the number of nodes in the network changes. The statistical model for a saturated uplink/downlink Wi-Fi network [16] (reviewed in Section 4.3) is most accurate when the number of clients increases (e.g. $>$ 10). However, as illustrated in Fig. 4.9c, our model remains robust when the number of clients is reduced to 5. Only upon further reduction to 2 clients that simulations begin to diverge from analytical predictions (Fig. 4.9b). In the downlink only case, our analysis is exact as born out by Fig. 4.9a.

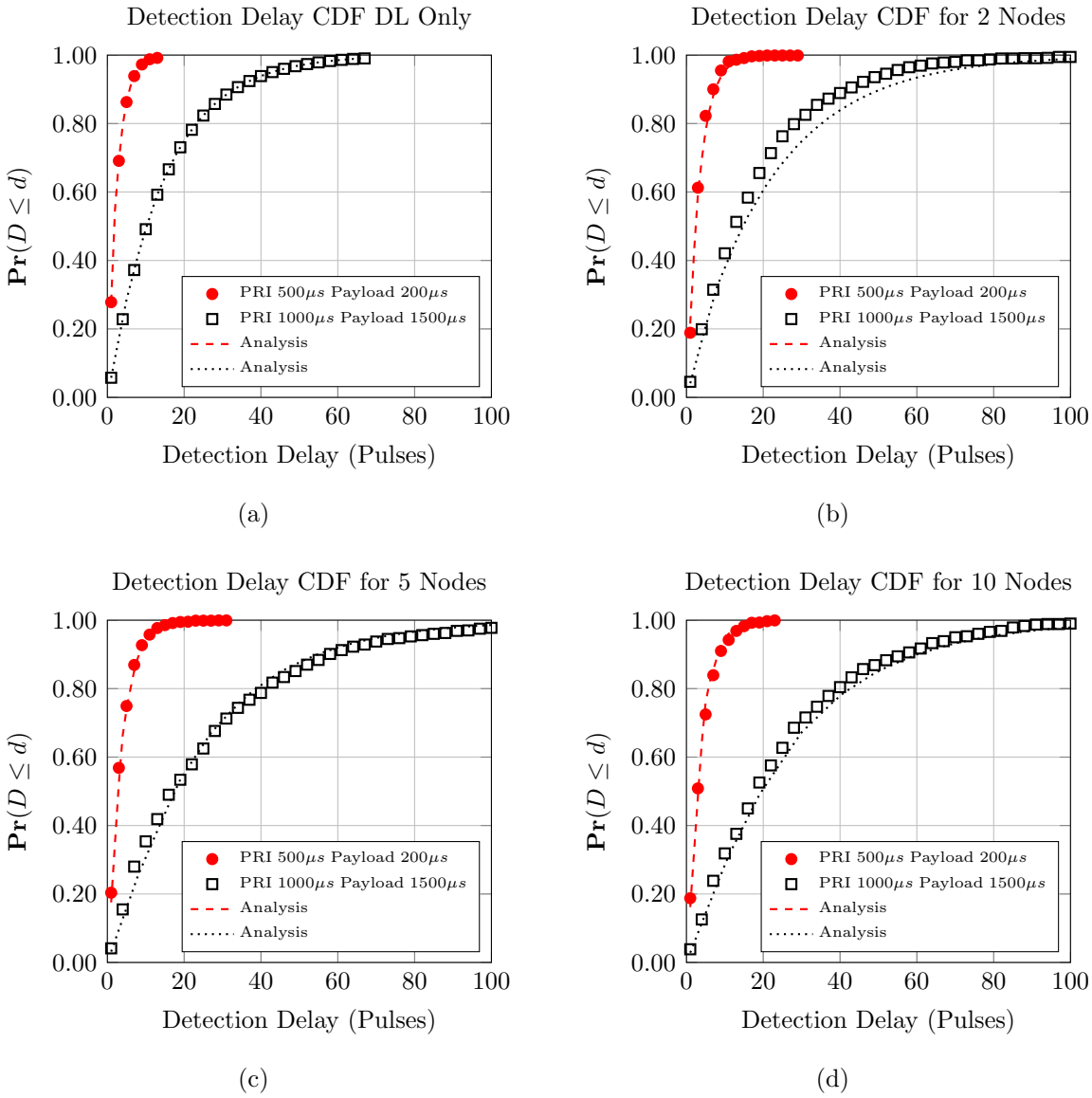


Figure 4.9: (a) In the downlink scenario, the provided analysis is exact (borne out by matching simulation results). (b) Analysis loses some accuracy in the full buffer uplink/downlink case for small number of nodes (e.g. < 5). Analysis and simulation results closely match for (c) and (d).

Table 4.3: Simulation Verification Scenarios

Scenario:	1	2	3	4	5
t_{payload}	$50\mu s$	$150\mu s$	$250\mu s$	$1ms$	$3ms$
Clients			10		
Radar Pulse			4μs		
Radar PRI			200μs		
Energy Detection			Ideal		
d_{burst} for $P_d = 0.6$	4	6	6	16	44
Throughput (Analysis)	0.299	0.571	0.599	0.718	0.7553
Throughput (Sim.)	0.3	0.58	0.61	0.725	0.75

4.5 Other Results and Discussion

So far in this work we have derived the detection delay as a function of network and radar parameters. In this section, we will examine several radar parameter sets to gain some insight into sensing/detection as a coexistence mechanism. Later, we will consider using the analysis developed within this paper as a guideline for selecting Wi-Fi parameters that allow us to achieve some desired detection requirements.

4.5.1 The Impact of Wi-Fi and Radar Parameters

As observed in the preliminary results in Section 4.4.4 (Fig. 4.8), increases in the payload duration negatively impact detection delay. The intuition behind this observation is that increased payloads both reduce the frequency with which idle periods occur, as well as the overall average idle time making it less likely for the low duty cycle radar signal to be detected.

We will examine the trade-off and design implications of these facts in the next sub-

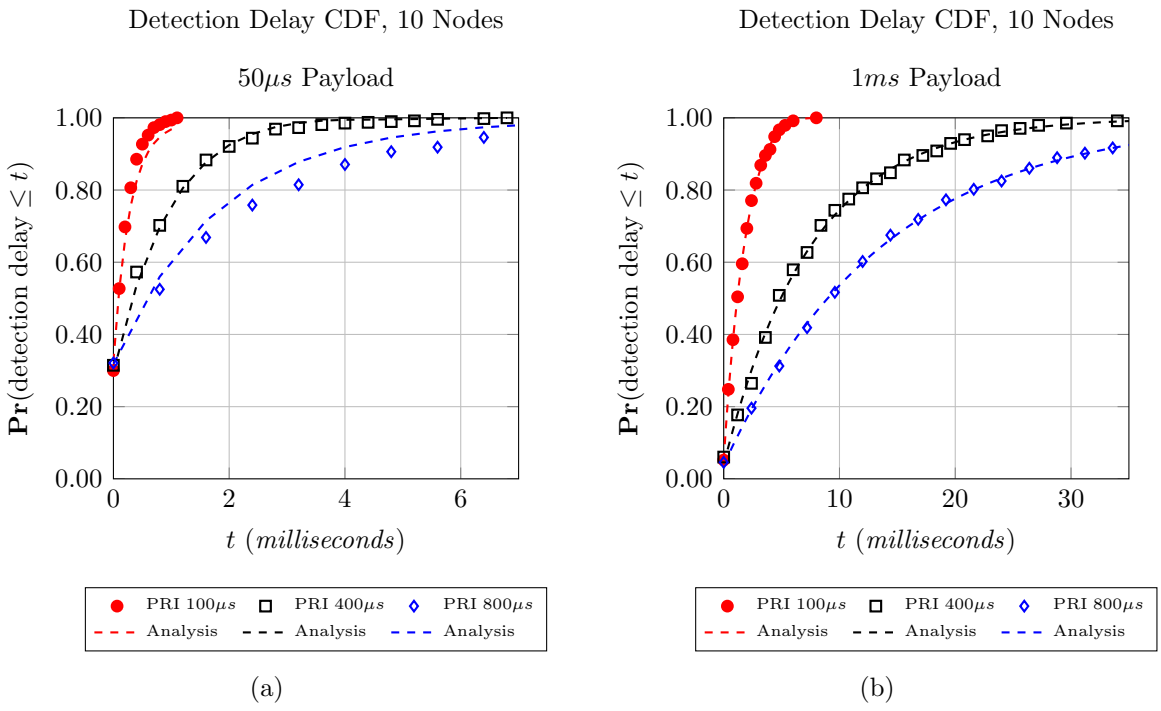


Figure 4.10: This figure shows the detection delay (in seconds) as a function of radar PRI for two fixed payloads. Aside from the PRI, all parameters match those in Table 4.3. (a) Shows a 10 node saturated network with a fixed payload size of $50\mu s$. Wi-Fi throughput at this setting is 0.299 (b) Shows the detection delay for a similar network but with a longer payload duration of $1ms$. Wi-Fi throughput at this setting is 0.725.

section, but here we consider results two Wi-Fi networks with payload durations at two extremes of the gamut. Fig. 4.10 is evidence of the dramatic affect of payload size on the detection delay when comparing corresponding results for the different payloads. In the worst case, it can take hundreds of pulses for a radar to be detected when the secondary network's channel utilization is high.

4.5.2 The Detection vs. Throughput Trade-off

What remains is to apply the framework we have developed to the underlying coexistence problem, namely, that of achieving the best network throughput subject to detection requirements. To do so, we can tune the length of the payload (busy period) and the DIFS (idle period) which will achieve two goals:

1. Modifying the proportion of network idle time,

2. Adjusting the frequency with which such idle periods occur.

Both outcomes are clearly overheads to the secondary network in terms of throughput while they will reduce detection delay. Note that we can trivially guarantee any desired detection delay $D_{\text{des}} > 1$ by imposing the following conditions:

$$I^{\min} \geq t_{\text{pri}} \implies t_{\text{difs}} \geq t_{\text{pri}} \tag{4.37}$$

which ensures that every idle period is of sufficient duration to contain at least a single pulse arrival. The second condition ensures that at least one such idle period occurs by the desired detection delay (D_{des})

$$D_{\text{des}} t_{\text{pri}} \geq I^{\min} + B^{\max} \tag{4.38}$$

While feasible, this guarantee comes at a (potentially) heavy cost. In essence, we are lengthening the inter-frame spacing which reduces throughput while simultaneously, we decrease the duration of the payload which compounds the effect. Such overheads impose

a heavy penalty that would significantly degrade Wi-Fi throughput. However, if we forgo strict requirements and adopt statistical guarantees instead, we will be able to achieve far better network performance while maintaining acceptable protection for radars. Currently, the specific detection requirements available in the public literature are those applying to the 5GHz band [27]. Hence, we use these numbers simply as a benchmark for the results in the remainder of the paper.

The derivations in the previous section show that the distribution of detection delay is a function of the distributions of I and B. However, they cannot be considered as independent 'knobs' used for tuning. Modifying either one affects both throughput and detection; in fact as we will show, adjusting the payload seems to be clearly sufficient.

Based on our calculations, we can select WLAN parameters that achieve a particular in-service detection probability given particular radar characteristics. As an example, we will consider a radar with a PRI of $200\mu s$ in line with [27]. Table 4.3 shows the parameter sets that yield a 60% detection rate for a PRI of $200\mu s$. When the payload size is $3ms$ (which is close to the maximum allowable by Wi-Fi), the throughput is maximized. Yet d_{burst} should exceed 40 pulses before it can be detected at a sufficiently high rate.

Reducing the payload size to $1ms$ deceases the number of pulses required for detection by more than one half. Evidently, this improvement results in only a minimal loss of throughput (less than 10%) though additional improvements through further reductions of the payload size come at a much greater cost. We readily conclude that we can simultaneously obtain high throughput (by using $1ms$ Wi-Fi payloads) and a 60% detection rate for bursts longer than 16 pulses; this is an indication that through careful selection of the appropriate parameters, a Wi-Fi network can achieve acceptable throughput while adequately protecting a radar primary.

Fig. 4.11 shows a complete picture of the detection vs. throughput trade-off for a radar with a PRI of $200\mu s$ as a function of payload and DIFS duration. As alluded to earlier, it is evident that for almost any desired pulse burst, the best throughput can be attained by simply adjusting the payload. By avoiding any changes to the DIFS mechanism, we eliminate

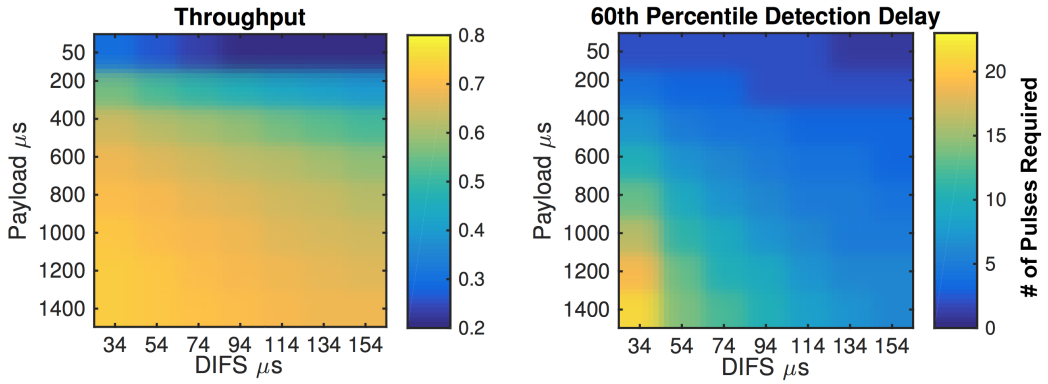


Figure 4.11: For $t_{\text{pri}} = 200\mu s$, these figures illustrate the detection delay vs. throughput trade-off for various t_{difs} and t_{payload}.

the need for intricate and costly changes to the Wi-Fi standard (Wi-Fi already allows for payloads of varying duration).

In order to complete the picture, we will also present results for a selection of other radar parameters indicated in [27], namely those listed in Table 4.4. It is easy to see that radars that transmit less frequently are more difficult to detect reliably. This is in fact not only related to the frequency of the pulses, but also the tendency for longer PRI radars to transmit a smaller number of pulses in each burst. The key insight we gain from the results presented in this section points to the advantage of optimizing the detection rates for specific radar parameter sets so that maximum throughput can be achieved for the Wi-Fi network.

4.6 Conclusion

In this paper, we examined the statistical properties of randomly occurring quiet periods in Wi-Fi networks for the purposes of radar detection using DFS in a Wi-Fi/radar co-existence scenario. Our work was motivated by system design requirements (radar incumbent protection) for the purpose of spectrum sharing between radar and Wi-Fi communication systems. For our analysis, we considered two canonical scenarios encompassing a downlink only as

Table 4.4: DFS Scenarios

PRI	$250\mu s$	$1429\mu s$	$5000\mu s$
Pulse Duration	$1\mu s$	$1\mu s$	$5\mu s$
d_{burst}	25	18	10
Target Burst P_d		0.6	
Clients		10	
Max Throughput	0.7363	0.715	0.6470
Payload Duration	$1.5ms$	$930\mu s$	$400\mu s$

well as an uplink/downlink network. Next, we confirmed our analysis through extensive simulations for various network/radar parameters.

We showed that in many circumstances, these random quiet periods occur with sufficient frequency to provide some statistical guarantees for in-service radar detection, especially in the regions close to the radar that are currently designated no-transmit zones. We provided an intelligent method to adjust Wi-Fi parameters in order to achieve the desired protection for the radar while attaining acceptable throughput, thereby providing a basis for successful deployment of wireless broadband access (using Wi-Fi) in the vicinity of radar installations. Lastly, we showed that modifying the payload duration is the most effective adjustment to speedily detect radars and provide them with adequate in-service protection.

Chapter 5

A STUDY OF WI-FI IN RADAR BANDS: ANALYSIS AND SOLUTIONS

Spectrum sharing between radar and communication systems has the potential to enable access to hundreds of MHz of new spectrum leading to dramatically increased capacity for wireless broadband. However, prior to deploying wireless systems in the same band as radars, we must examine the impact of radar interference on system throughput. In this paper, we study the impact of radar interference on WLAN (Wi-Fi) at the link level through detailed signal level simulations. We examine the consequences of interference during various stages of signal reception (e.g. synchronization and channel estimation) on the packet error rate. Finally, we propose and evaluate schemes to mitigate the impact of radar on Wi-Fi systems through radar detection via modifications to the 802.11 decode chain. Our results show potentially effective system solutions for radar/WLAN spectrum sharing in the 3.5GHz (S-band) that is of current interest.

5.1 Introduction

The WLAN 802.11 standard has been a cornerstone of wireless broadband networking for the past two decades. While it has primarily served as a key *access mechanism* for indoor (home and enterprise) users, it has been recently expanded for various new use cases, as below, attesting to the versatility of its base design:

1. High speed wideband communications for multimedia and low latency applications (e.g. 802.11ax)

2. Narrowband low power wide area IoT applications (802.11ah) in sub 1 GHz bands

3. Wide area (outdoor) opportunistic access (e.g. TV Whitespaces with 802.11af)

The above has been primarily achieved by adapting 802.11's physical and medium access layers to the specifics of these emerging applications; however, the carrier sensing feature that underpins Wi-Fi multiple access in Distributed Coordination Function (DCF) - necessitated by the shared access nature of the ISM bands with different device types such as cordless phones and Bluetooth - has remained among these changes. Therefore, a knob for wireless coexistence is inherent in WiFi, which has enabled additional capabilities such as Dynamic Frequency Selection (DFS) for 5GHz (UNII bands) [9] WLAN devices as well as database assisted coexistence within the TV spectrum (802.11af) [11]. In that vein, our work seeks to determine the potential of Wi-Fi networks in new bands being considered for shared usage such as the 3.5GHz [66]. We begin with two basic questions that must be addressed:

Can Wi-Fi networks sufficiently protect radars from undue interference?

Affording radar protection has been approached from several directions in the literature. A natural and conservative solution as in [37], is to institute an exclusion zone around the radar wherein all WLAN operation is prohibited. The computaton of such a region assumes perfect knowledge of the radar location, orientation, antenna pattern, and activity schedule as well as propagation conditions between the radar and WiFi nodes. Our own earlier work in [64] sought a more intelligent solution that would potentially allow WiFi operation at some locations in the above exclusion zone, by exploiting the WLAN carrier sensing capability to detect (and avoid) radar operation in any of its channels. In addition, work from [68] considers physical layer techniques (such as beam forming) to limit interference to radars though such techniques typically require additional coordination between the radars and the communication networks (e.g. known preambles/channel estimation).

How well can the Wi-Fi networks operate in radar bands?

There has been some experimental work done by the NTIA [65] on the subject of Wi-Fi performance when facing radar interference. However, the work is treated in broad strokes. The authors in [40] consider the effect of radar interference on a WIMAX constellation, while our own earlier work in LTE/radar coexistence [63] explored some aspects of coexistence at the physical layer for LTE systems facing pulsed interference.

This work is also distinct from our previous effort [64] that focussed largely on how 802.11 WLANs may exploit the inherent randomly occurring 'quiet periods' to reliably detect radar pulses; it explored the detection-throughput trade-off as a consequence of tuning DCF parameters so as to provide (statistical) guarantees on detectability. Here, we approach the co-existence problem from a very different perspective: occasionally, radar pulses will interfere with 802.11 frames. We undertake (to the best of our knowledge), the most detailed exploration of how 802.11 WLAN physical layer is impacted by where such pulsed interference occurs (relative the header and payload of a frame). We begin by presenting a summary of some of the effects of such interference using an 802.11ac signal level link simulator developed in MATLAB. We next consider some mitigation schemes that could be employed within the 802.11 receive chain to render it significantly more robust (i.e. WLAN packets that are hit by such pulse interferers are nevertheless decoded) and thereby dramatically improve the possible regions of operation for WLAN networks.

5.1.1 Motivation

A brief analysis here will set the stage for the distinctive contributions of this work. The authors in [37] undertook a 1st-order analysis of the level of interference that can be tolerated by a radar while maintaining reasonable target detection performance. The results therein indicated - based on the target distance to the radar, interference from secondary communication networks must remain lower than -11dB in relation to the noise floor. Given that a typical Wi-Fi transmitter emits a signal at around 20dBm, the path-loss required to

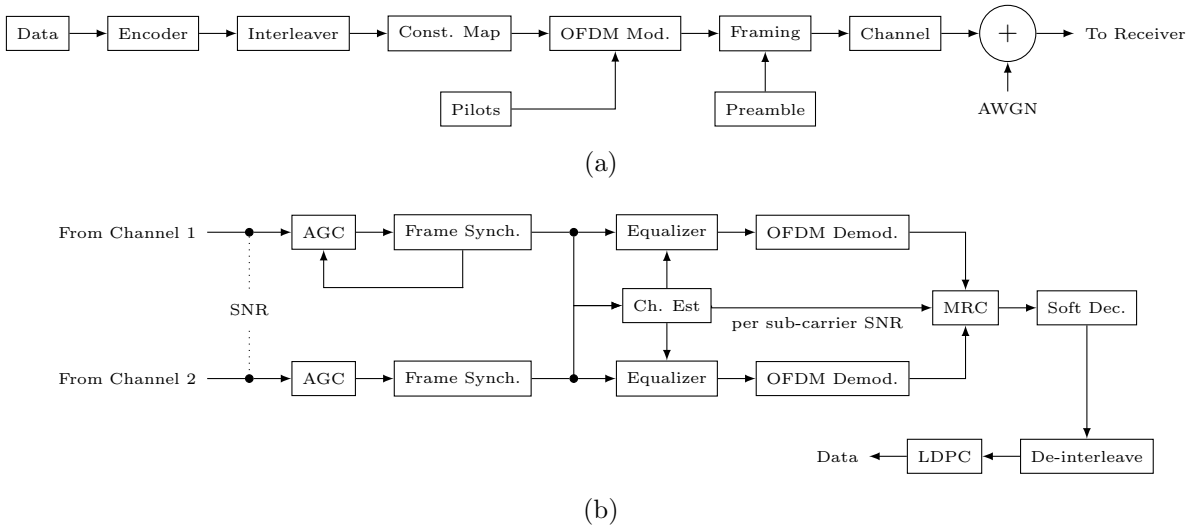


Figure 5.1: (a) Block diagram for a single antenna Wi-Fi transmitter. (b) Receiver block diagram for two-antenna receive diversity with Maximal Ratio Combining (MRC)

sufficiently attenuate the WLAN interference to the radar can easily be obtained:

$$\text{PL} \geq 20dBm + 11db + G_{\text{radar}} - \text{Noise Floor} = 141dB \tag{5.1}$$

In other words, it is feasible to envision a secondary network deployed at a location that is separated from the radar by approximately 144dB of path-loss. Now, considering the reverse, a radar transmitter can emit at levels up to 80-120 dBm (based on radar antenna pattern) in the direction of the secondary network, when the radar main beam in pointed in that direction. Hence, if we attempt to deploy a WLAN as close as possible to the radar receiver, i.e. at the 144 dB path loss range, the received interference power at the Wi-Fi network from the radar can be up to -21dBm. Mitigating this asymmetry and making Wi-Fi resilient to this low duty cycle, high power interference is the key to improved utilization of this radar spectrum.

5.2 WLAN Preliminaries

In preparation for our in-depth exploration of the physical layer coexistence aspects Wi-Fi/radar, we summarize the key relevant elements of the WLAN physical layer in this section (and the Radar system in the next) for the subsequent analysis.

5.2.1 OFDM and Channel Model

We focus our work on a 20 MHz single stream Wi-Fi link. The WLAN physical layer adopts a 64 subcarrier OFDM scheme resulting in a subcarrier spacing of 312.5 KHz. Each symbol has a duration of $4\mu s$ which includes a cyclic prefix of $800ns$[1]. At the left edge of the 20MHz channel, 4 subcarriers are used as a guard band while at the right edge, 3 guard subcarriers are used. Additionally, the DC subcarrier is not utilized for transmission. Of the remaining 56 subcarriers, 4 are used as equally spaced BPSK modulated sub-carriers resulting in a single pilot being present every 4.375 MHz while 52 are employed for data transmission (Fig. 5.2). From this point forward, we use the index $l \in [0, 63]$ to refer to individual sub-carriers.

Given a complex baseband WLAN signal $x(n)$ and a circularly symmetric white gaussian noise process $w(n) \sim \mathcal{CN}(0, \sigma_w^2)$, we define the *total* Signal to Noise Ratio as:

$$SNR = \frac{\sigma_x^2}{\sigma_w^2} \tag{5.2}$$

Additionally, we assume that any frequency selective channel $h(n)$ applied to the transmitted sequence $x(n)$ is normalized (without loss of generality) such that the power in $x(n) * h(n)$ remains σ_x^2, the (input) signal power . Therefore, for a given OFDM symbol, the received signal may be written as follows:

$$y(n) = x(n) * h(n) + w(n) \tag{5.3}$$

Following in the footsteps of the IEEE 802.11 taskgroup, we use the TGac channel model D to describe the channel between the WLAN transmitter and receiver. This channel model

[1]We neglect Greenfield mode in this work for the sake of brevity

Table 5.1: Wi-Fi Parameters

Bandwidth	20 MHz
N_{fft}	64
Null Carriers	0-3, 32, 61-63
Pilot Carriers	11, 25, 40, 54
N_{data}	52 (# of data carriers)
Cyclic Prefix	800ns (16 samples)
Symbol Duration	$4\mu s$ (80 samples)
Noise Power	var $w(n) = \sigma_w^2$
Signal Power	var $x(n) = \sigma_x^2$
Channel Model	TGn Channel Model D [26]
# of Antennas	TX: 1, RX: 2
Receiver	Maximal Ratio Combining [34]
MCSes	MCS 0: BPSK R1/2, MCS 4: 16QAM R3/4
	MCS 8: 256QAM R3/4

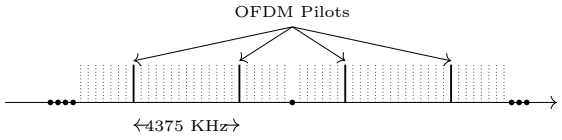


Figure 5.2: A 64 subcarrier OFDM scheme is used in a 20MHz channel with 4 pilots are evenly spaced amongst the occupied subcarriers. There are a total of 8 null subcarriers: 4 at the left edge, 3 at the right edge, and 1 at DC.

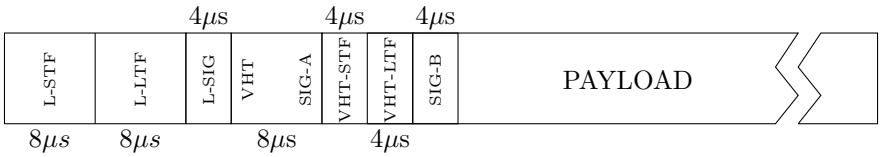


Figure 5.3: Each OFDM symbol has a duration of $4\mu s$. Some packet fields consist of multiple OFDM symbols (e.g. L-LTF is 2 symbols long).

is represented using a tapped delay line with 18 taps sampled at 100 Mhz ($10ns$ between taps). A full description of this model can be found in [26] including the requisite information to compute inter-antenna correlations in multi-antenna scenarios. To combat deep fades, the WLAN receiver in this paper uses a 2 antenna diversity scheme (maximal ratio combining [34]). The transmit/receive chain is illustrated in in Fig. 5.1. To obtain the correlations between the receiver antennas, we use the channel properties as laid out in [26] assuming an antenna separation of 0.5λ.

5.2.2 Symbols, Framing, and Error Correction

A transmitted 802.11ac Wi-Fi frame consists a series of $4\mu s$ OFDM symbols arranged as shown in Fig. 5.3. Each frame segment comprises one or more OFDM symbols and serves a different function as follows:

- L-SIG, VHT-SIG: These fields contain meta information including frame addressing,

CRC, frame size, and MCS selection.

- L-STF: The Short Training Field is used for frame detection, coarse synchronization, course frequency offset estimation, and selecting amplifier gain levels (Automatic Gain Control).

- L-LTF, VHT-LTF: The Long Training Fields are used for channel estimation. In a multi-stream transmission, each transmit antenna requires an additional VHT-LTF symbol, but we only consider single stream WLAN systems in this work

- The payload contains the encoded data. The modulation scheme and coding rate are chosen amongst a set of predefined parameters shown in Table 5.1. We do not consider multi-stream transmissions in this work.

For the purposes of error correction two options exist:

1. Binary Convolutional Code (BCC): a rate 1/2 constraint length 7 convolutional code is applied to the data followed by puncturing to achieve the desired rate. This is the baseline coding employed in the standard. In this work, BCC is *only used* for the SIG fields.

2. LDPC: LDPC coding with three codeword sizes of 648, 1248, and 1944 bits is also available within the standard. The generation of the parity matrices for the various code rates is described in [9]. Due to the fixed size of the codewords, additional steps are necessary to ensure that the code words fit within the OFDM symbols (detailed process described in [59]). Since LDPC provides improved performance, we use LDPC *exclusively* for the payload.

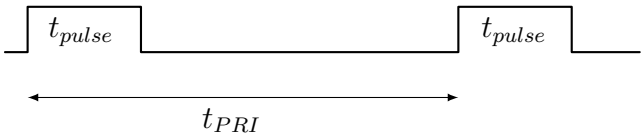


Figure 5.4: Pulse Duration and Pulse Repetition Interval for Radar

5.3 Radar System Summary

We consider a radar waveform with constant amplitude A and define the notion of *peak* Interference to Noise Ratio as follows:

$$\text{INR} = \frac{A^2}{\sigma_w^2} \tag{5.4}$$

The main relevant parameters of a radar waveform:

t_{pulse} Pulse duration for the radar

t_{PRI} Time between pulses (pulse repetition interval)

A Peak amplitude of the radar waveform

f_s The sweeping frequency of the chirp (i.e. $f_{max} - f_{min}$).

The values for these parameters in the scenario considered for this paper are shown in Table 5.2. Note that in order to simplify presentation of results, we assume that t_{pulse} is $4\mu s$ and that pulse arrivals coincide with a single WLAN OFDM symbol. This condition does not hold in general and can easily be relaxed in simulation studies and analysis but at the cost of significant additional complexity to the notation and presentation of the material.

In addition, we assume that the maximum frame duration for the WLAN is $200\mu s$ so as to limit the number of pulses arriving within a frame. Again, this condition does not hold in general but is necessary to successfully study the impact of radar interference on *individual* aspects of the receive process. Hence, when considering the arrival of radar interference, we

Table 5.2: Radar Parameters

f_s	4 MHz
Waveform	Linear FM Chirp
Pulse Duration	$4\mu s$
PRI	$200\mu s$
Duty Cycle	2%

are concerned with a single pulse arrival during a single OFDM symbol selected at random in the frame segment of interest (e.g. data symbol 5 within the payload segment or L-LTF symbol 2 within the PLCP).

Given these assumptions, the radar waveform can be written as follows:

$$u(t) = A \cdot e^{j\left(\frac{f_s}{4\mu s} + \Delta f_c\right)t},\ 0 \leq t < 4\mu s \tag{5.5}$$

$$f_s = 4 \text{ MHz} \tag{5.6}$$

where Δf_c represents the relative carrier frequency offset between the radar interferer and the Wi-Fi signal and f_s is the sweep frequency for the chirp. In this work, we focus on full overlaps between the radar and Wi-Fi signal, hence we consider $\Delta f_c \in [-4, 4]$ MHz.

In simulations, the Wi-Fi receiver samples the signal at 20 MHz and discards the first 16 samples from each $4\mu s$ OFDM symbol ($800ns$ cyclic prefix). Hence, the retained portion of the sampled interference signal is written as follows:

$$u(n) = A \cdot e^{j\left(\frac{f_s}{K} + \Delta f_c\right)(n+16)},\ 0 \leq n < N_{\text{fft}} \tag{5.7}$$

We assume a flat channel between the radar and the WLAN receiver based on the following two justifications:

1. There is not a great deal of literature addressing the appropriate channel to use when measuring radar to comm system interference

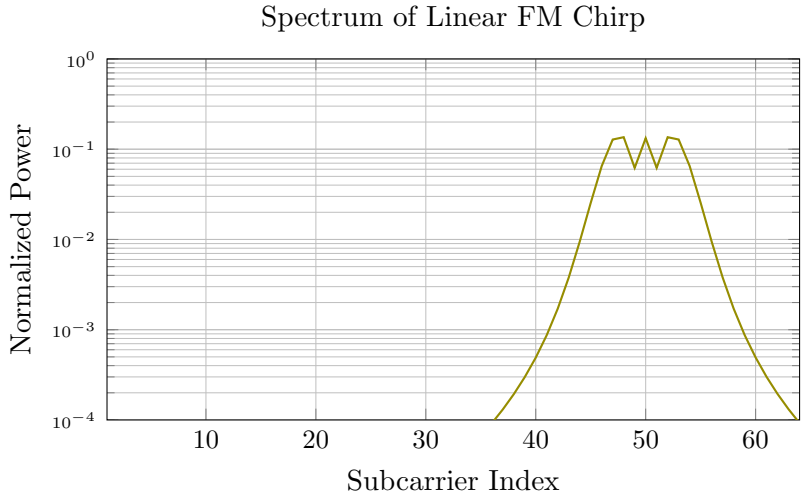


Figure 5.5: Power spectrum of a linear FM chirp. This corresponds to $3.2\mu s$ of the chirp waveform that affects the retained portion of the OFDM symbol ($800ns$ discarded in the cyclic prefix)

2. The radar antenna is highly directional, limiting the multi-path nature of the channel

Since we are considering an OFDM system, we will complete our model by translating it to the frequency domain. Specifically, the radar interference arriving on subcarrier l during a given OFDM symbol is denoted:

$$U_l \triangleq \sum_{n=0}^{N_{\text{fft}}-1} u(n) \cdot e^{-2\pi jdn/64} \tag{5.8}$$

which is simply the Discrete Fourier Transform (DFT) of the sampled radar waveform (shown in Fig. 5.5). We use similar notation to represent other components of the received signal in the frequency domain and thus, for a given receiver antenna r, the frequency domain received signal corresponding to the k^{th} OFDM symbol takes the following form depending on the presence of radar interference:

$$\mathcal{H}_0 \text{ (no radar)} \qquad : Y_{r,l}^{(k)} = X_{r,l}^{(k)} H_{r,l} + W_{r,l}^{(k)} \tag{5.9}$$

$$\mathcal{H}_1 \text{ (with radar)} \qquad : Y_{r,l}^{(k)} = X_{r,l}^{(k)} H_{r,l} + W_{r,l}^{(k)} + U_l \tag{5.10}$$

where $r \in [1, 2]$ represents the antenna number and $W_{r,d}^{(k)}$ are i.i.d. $\mathcal{CN}(0, \sigma_w^2)$. The least squares channel estimates on each antenna are:

$$\hat{H}_{1,l} = H_{1,l} + W_{1,l}^{(V)}$$
$$\hat{H}_{2,l} = H_{2,l} + W_{2,l}^{(V)} \tag{5.11}$$

where the superscript $^{(V)}$ corresponds to the index of the VHT-LTF symbol (OFDM symbol 9 from Fig. 5.3).

5.4 Simulation Results

In this section, we provide a series of results aimed at shedding light on the impact of radar interference on the various phases of reception. To do so, we inject the interference waveform described by (5.7) into both reception paths at the Wi-Fi receiver (i.e. antennas 1 and 2), then measure the packet error rate as a function of SNR and INR. At least 2000 iterations are completed for each (SNR, INR) pair to yield smooth results. The multi-path channel is reset to obtain a new realization for each iteration of the simulation.

5.4.1 L-STF

We begin by considering the impact of interference on the L-STF. Specifically, interference during this portion of the frame can lead to a failure in packet detection (i.e. packet reception is not even attempted). However, there are also additional 'soft' effects as a result of interference during this phase:

- Increased synchronization error results in higher incidence of decode errors due to a higher chance of inter-symbol interference

- Since the automatic gain control is set during this phase, high interference causes distortion due to the limited dynamic range of the Analog to Digital Converter (ADC). This effect is most prominent at very high INR values.

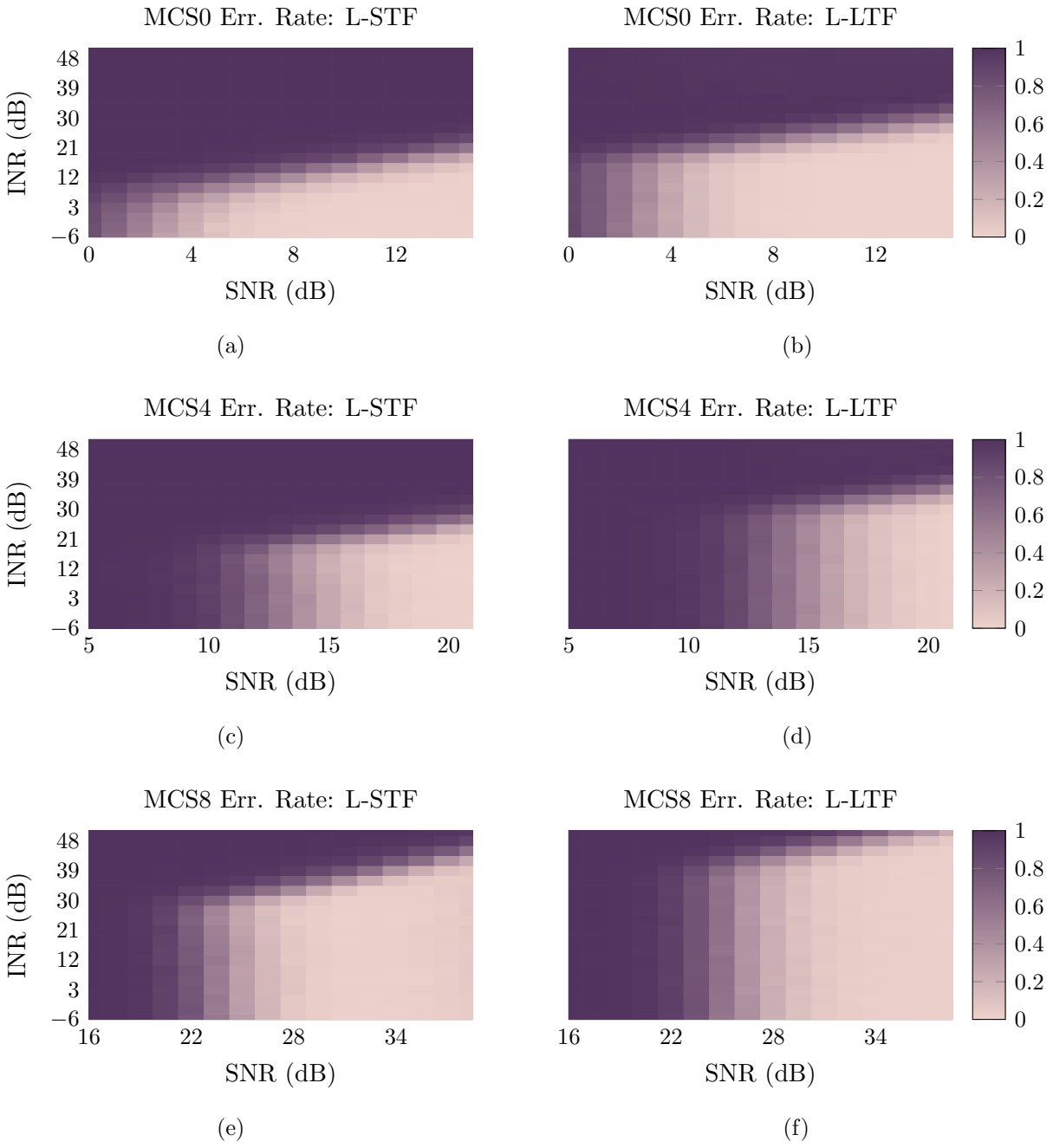


Figure 5.6: (a) (c) (e) Show frame error rate when interference occurs during the Short Training Field. (b) (d) (f) Show frame error rate when interference occurs during Legacy Long Training Field.

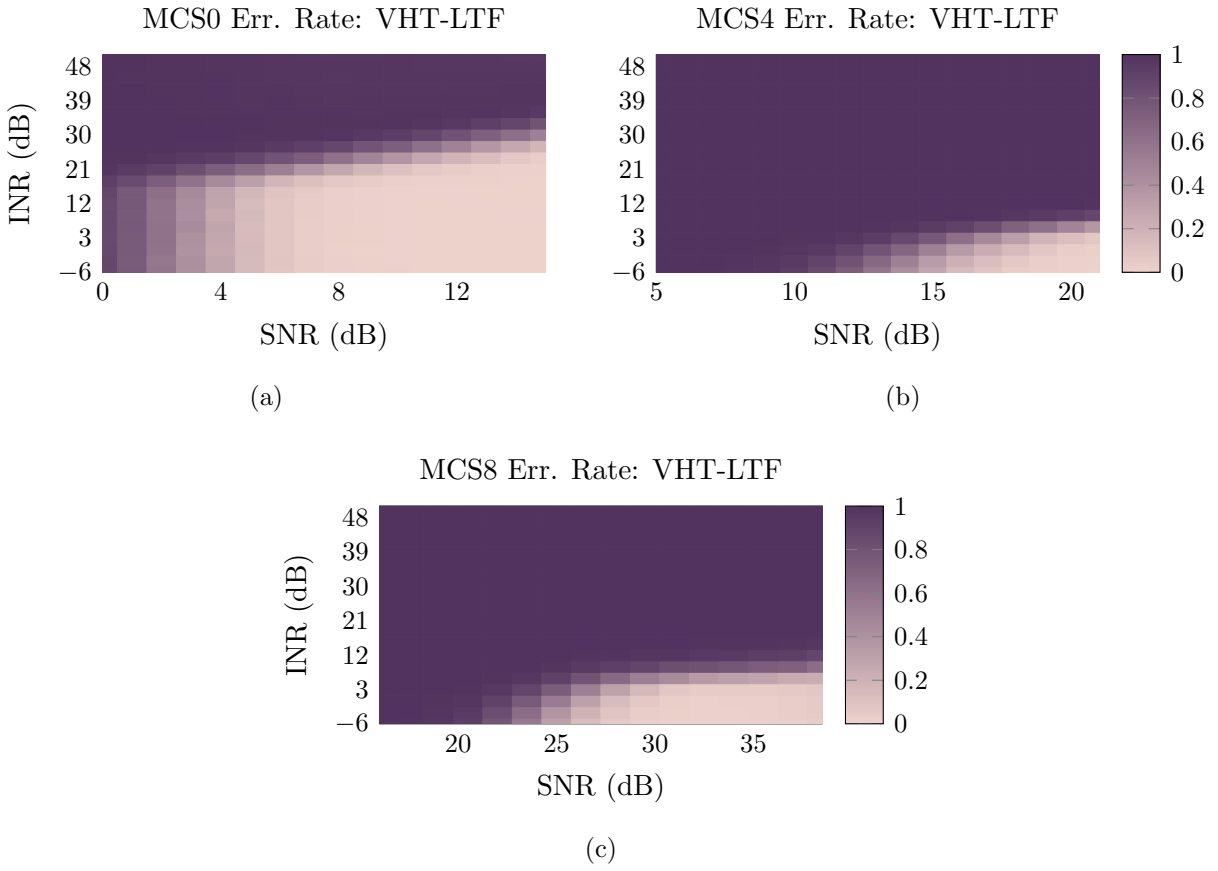


Figure 5.7: (a) - (c) Show frame error rate when interference occurs during the VHT Long Training Field.

Figures 5.6a 5.6c 5.6e catalogue the packet error rate due to L-STF interference. It is immediately apparent that the increased operating SNRs for MCS4 and MCS8 make them more resilient to interference during the L-STF. The boundary of the low error region seems to closely follow the SNR=INR line. As the INR passes the SNR, the packet error rate rapidly approaches 1.

5.4.2 L-LTF

Next, we consider interference during the L-LTF (Figures 5.6b 5.6d 5.6f). In legacy Wi-Fi networks (802.11g), the L-LTF is used for channel estimation. However, after the introduction of 802.11n, an additional LTF (the VHT-LTF) was introduced for that purpose. Hence, the primary function of the L-LTF in our simulations is to estimate noise power and compensate for carrier frequency offset between the Wi-Fi transmitter and receiver. The results indicate that the receiver is slightly less sensitive interference during this phase when compared to the L-STF.

5.4.3 VHT-STF

Since the VHT-LTF is the primary means of channel estimation, interference during this symbol propagates itself through the rest of the decode process. As shown in Figures 5.7a 5.7b 5.7c, the impact of interference on the VHT-LTF is far more pronounced than the L-STF or the L-LTF. Furthermore, higher MCSes are more sensitive to interference; note that in the case of MCS8, and INR of 10dB has a dramatic effect yielding a packet error rate of 1.

5.4.4 Payload

The last remaining piece of this evaluation is the impact of radar interference on the payload. In this work, we have elected to use the LDPC coding option provided in WLAN due to its superior error correcting capabilities. The alternate coding option (BCC) is block interleaved for each OFDM symbol which provides resistance to deep fades in the channel (through frequency diversity) but does nothing to combat bursty interference like radar. LDPC on the other hand has some measure of built-in time interleaving due to the nature of the parity matrix.

However, it seems that the LDPC decoder is unable to cope with the bursty nature of the radar interference. Figures 5.8a 5.8c 5.8e illustrate how a radar burst during a payload

symbol can drastically increase the packet error rate even at relatively low INR values. For example, MCS4 at 20dB SNR is guaranteed to be undecodable at an INR value of 20dB. More alarmingly, MCS8 shows a complete breakdown at INR levels as low as 3dB. This reality is sobering given the INR levels we expect to encounter in such Wi-Fi/radar coexistence scenarios (see Section 5.1.1).

As we will see in the coming section, all is not lost. In fact, as we observed in [63], the major source for payload errors comes from decoder saturation and can be combatted through intelligent erasures of interfered bits.

5.5 Mitigating Radar Interference

So far, we have predominantly reported on Wi-Fi's inability to cope with bursty interference. Fortunately, a closer examination of the 802.11 protocol reveals a series of tools that can effectively be used to allay these concerns. Specifically, we will endeavor to detect interference during Wi-Fi symbols and take corrective action when/if possible. In the next section, we will focus on how detection can occur and under what circumstances in can be successful, but here, we concern ourselves with what happens once interference has already been detected.

5.5.1 Channel Estimation

One area in which mitigation is possible is channel estimation. This is due to the in-built redundancy in the Wi-Fi packet whereby channel estimation pilots are sent separated by $20\mu s$ (see Fig. 5.3). In particular, the VHT-LTF and L-LTF fields are largely identical except that the VHT version contains 2 additional sub-carriers on each side which are null carriers in the L-LTF case. This legacy construct was retained for backwards compatibility but it will provide a useful in our coexistence scenario.

In essence, we are able to generate two independent estimates of the channel at two different time instants. If one is judged to be corrupted by interference, it is possible to exploit this redundancy by selecting the uncorrupted channel estimate. Fig. 5.11a, illustrates how these channel estimates can differ if one is corrupted by radar interference.

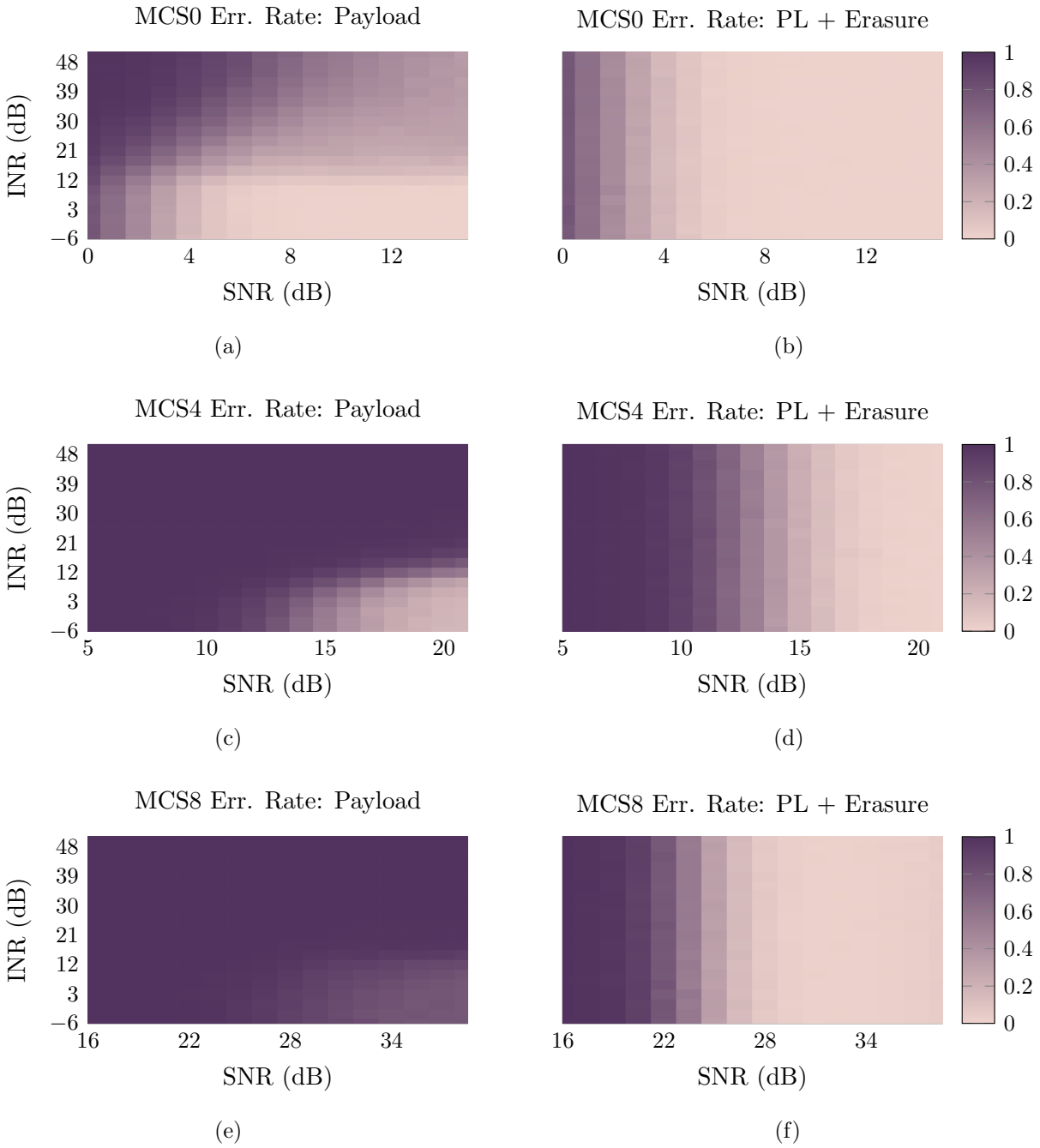


Figure 5.8: (a) (c) (e) Show the impact of radar interference on the payload. Note that MCS4 and MCS8 experience catastrophic error rates at low to moderate levels of radar interference. (b) (d) (f) In contrast, with the mitigation methods from 5.5.2 applied, the payload is practically immune to radar interference.

It turns out (as we will show in Section 5.6.3) that detecting such interference is quite straightforward. In fact, in practically all cases of interest, almost perfect detection is possible. Furthermore, a false alarm is not particularly detrimental since the false detection will simply result in replacing one uncorrupted channel estimate with another.

5.5.2 Payload

The more difficult case to tackle is that of interference during the payload. Previously [63], we showed that 'erasing' the interfered bits can lead to dramatic reductions in packet error rates. Recall that the input to an LDPC decoder is the *log-likelihood ratio*. Given an observed constellation point, the LLR is defined as follows:

$$\text{LLR} = \log \frac{\mathbf{Pr}\left(0|\text{observation}\right)}{\mathbf{Pr}\left(1|\text{observation}\right)} \tag{5.12}$$

This soft value encodes a notion of confidence in the decision of the decoder. Large positive/negative values indicate high confidence that the bit is a '0' or '1' respectively. Burst interference corrupts these LLR values in a way that cannot be reconciled by the LDPC decoder (see [63] for more details). By setting the LLR for interfered bits to 0, we remove the corrupted bits in the hopes that the error correcting code is able to recover them.

When utilizing the LDPC coding option, the data bits are split into a series of codewords. Each codeword can have a length of 648, 1248, or 1944 bits. Shortening and padding bits are added to ensure that the resulting coded bits fit within an integer number of OFDM symbols (additional details can be found in [59]). No interleaving is required since some measure of randomness is introduced through the LDPC parity matrix.

Consider a single codeword with a length of 1944 bits. At MCS0, a single OFDM symbol corresponds to 26 coded bits, while at MCS8 an OFDM symbol corresponds to 312 bits. While the LDPC decoder may be able to cope with the erasure of 26 consecutive bits within a single codeword, 312 bits being erased from a single codeword is usually unrecoverable. Fortunately, this shortcoming is easy to overcome with a simple column interleaver.

If the payload is comprised of the bits $b_1 \cdots b_M$, we form an $\frac{M}{52} \times 52$ matrix as below:

$$\begin{bmatrix} b_1 & b_{K+1} & \dots & b_{51K+1} \\ b_2 & b_{K+2} & \dots & b_{51K+2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{52} & b_{K+52} & \dots & b_{51K+52} \end{bmatrix} \tag{5.13}$$

Then, the string of input bits are transformed by transposing the matrix and reading the bits column by column such that the transmitted bits take the following form:

$$b_1 b_{K+1} b_{2K+1} \cdots b_{51K+1} b_2 b_{K+2} \cdots b_{51K+2} \cdots b_{51K+K} \tag{5.14}$$

By using the column interleaver, we can ensure that cost of erasing a single OFDM symbol is amortized over all the codewords comprising the frame and that we are not introducing a clump of consecutive erasures within a single codeword.

The result of this erasure/interleaving scheme can be seen in Figures 5.8b 5.8d 5.8f. It should be apparent that the erasures have overcome the drastic effects of payload interference. In fact, since the effects of the interference are 'erased', the error rates are no longer dependent on INR (assuming perfect detection of the interfered symbol). In reality, perfect detection may not be possible, we address this question in the following section.

5.6 Detecting Interference

As we have shown, identifying an interfered symbol followed by some simple mitigation measures can lead to a dramatic reduction in packet error rates for WLAN. These measures can be designed under the assumption that the radar interference arrival time is known (e.g. through side information), but more realistically, such interference must be detected. In this section we consider this detection problem as it relates to the various phases of Wi-Fi reception.

In order to select the detection criteria, it would be ideal to make no strong assumptions as to the nature of the radar signal. We will rely heavily on the Constant False Alarm

Rate (CFAR) criterion as a means of selecting detection thresholds that limit the false alarm rate. False alarms during payload interference detection will lead to unnecessarily discarding certain bits, therefore we select a false alarm rate of 5% as our target[2].

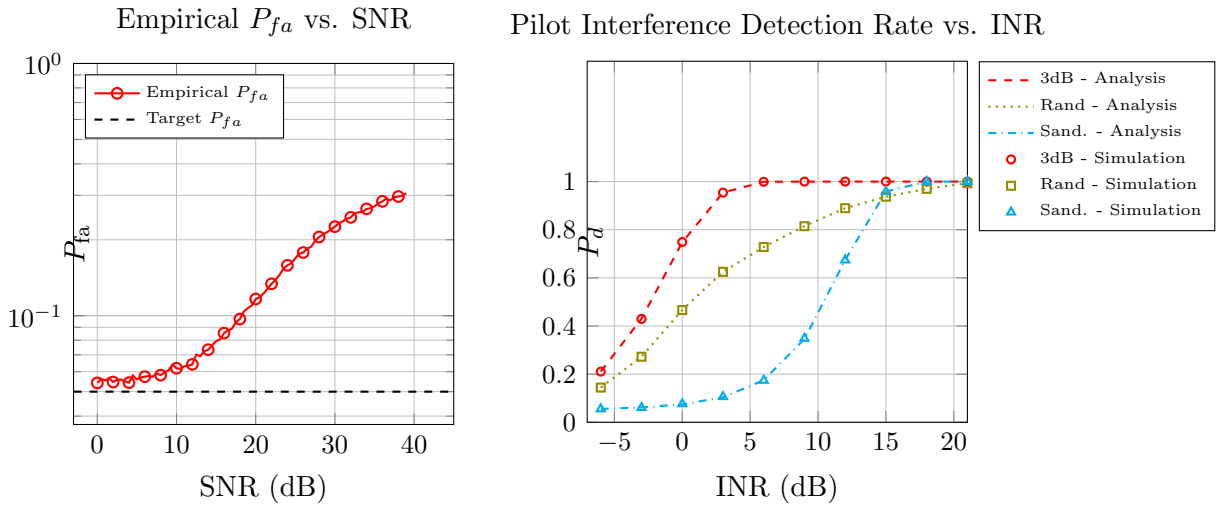


Figure 5.9: (a) The accuracy of the CLT approximation from (5.18) and (5.19) is shown here. The approximation proves to be poor above an SNR of 10dB the analytic approach to threshold selection ineffective. (b) Results are shown for three cases: 1) when the radar waveform's 3dB bandwidth overlaps a pilot, 2) when the radar waveform is located completely at random in relation to the pilots and 3) when the radar waveform is sandwiched perfectly between two pilots (e.g. 11, 25).

5.6.1 Payload Interference Detection Using Aggregate Energy

Without any prior knowledge of the radar signal, the simplest way to detect interference is through energy detection. With a target P_{fa} in mind, we formulate the two hypotheses as

[2]The target false alarm is in itself a possible subject of future study. For the sake of brevity, we only consider $P_{fa} = 5\%$ in this work.

follows:

$$\mathcal{H}_0 \text{ (no radar)} \qquad : y(n) = x(n) * h(n) + w(n) \tag{5.15}$$

$$\mathcal{H}_1 \text{ (with radar)} \qquad : y(n) = x(n) * h(n) + w(n) + u(n) \tag{5.16}$$

In order to decide between the two hypotheses, we are interested in the quantity below which represents the average energy for the duration of a single OFDM symbol:

$$\mathcal{E} = \frac{1}{N_{\text{fft}}} \sum_{n=0}^{N_{\text{fft}}-1} |y(n)|^2 \tag{5.17}$$

Under the null hypothesis $\mathcal{H}_0$, the literature suggests that this quantity can be suitably approximated using the central limit theorem [57] (we will examine the accuracy of this approximation momentarily). The parameters used for this CLT approximation are summarized as follows:

$$\text{mean} : \mu_{\mathcal{E}} = \sigma_x^2 + \sigma_w^2 \tag{5.18}$$

$$\text{variance} : \sigma_{\mathcal{E}}^2 = \frac{1}{N_{\text{fft}}} \left[\sigma_x^4 + 2\sigma_w^2 - (\sigma_x^2 - \sigma_w^2)^2\right] \tag{5.19}$$

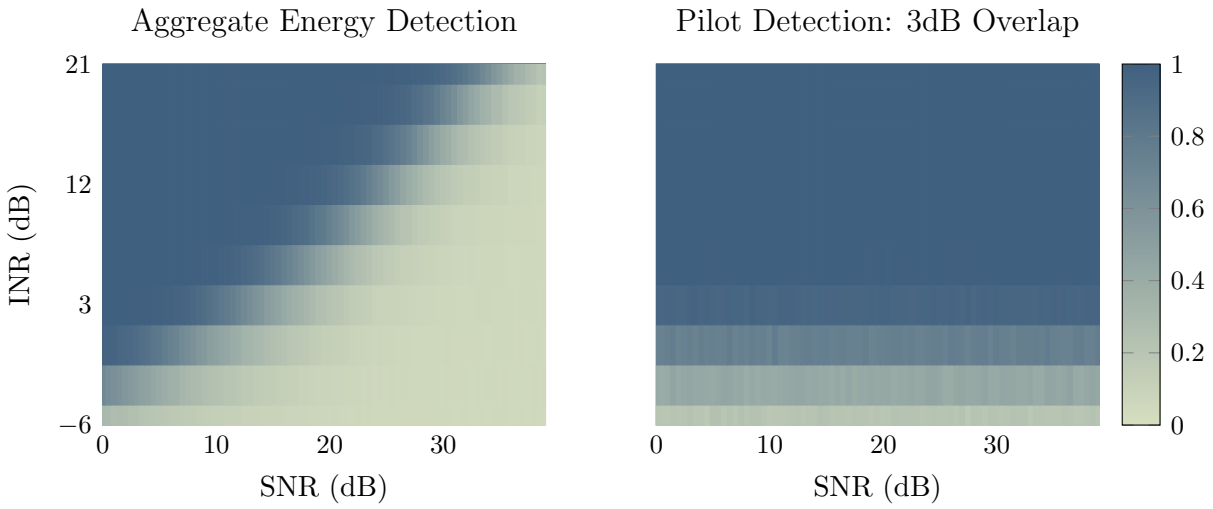
Given a target false alarm rate P_{fa}, we can arrive at the detection threshold γ_{cfar}:

$$\gamma_{cfar} = \sigma_{\mathcal{E}} \cdot Q(P_{fa}) + \mu_{\mathcal{E}} \tag{5.20}$$

where $Q(.)$ is the complimentary CDF of the standard normal random variable.

Fig. 5.9a shows how the analytic γ_{cfar} performs in simulations. Observe that at lower SNRs (0-10dB), P_{fa} remains close to the target rate, yet at higher SNRs, it does poorly. Although this statistical model for the OFDM signal is widely used in the literature, it is not accurate enough for determining a suitable threshold.

As an alternative to this analytic approach, simulations can be used to tabulate suitable energy detection thresholds γ_{emp} as a function of SNR. Then the question remains: what is the detection probability given these suitable thresholds? Fig. 5.10a shows P_d as a function of SNR and INR.



(a) (b)

Figure 5.10: (a) The aggregate energy detection method can work under some circumstances, but at higher SNRs, the signal variation masks the radar interference limiting the application of this method. (b) On the other hand, the pilot based detection method works extremely well regardless of the SNR.

Interestingly, we observe that increased SNR also necessitates a higher INR for successful detection of the radar pulse. Intuitively, this indicates that the energy variation in the WLAN signal at high SNRs masks the ability of aggregate energy statistic to detect radar interference. In summary, we conclude that aggregate energy is suitable in some scenarios but with important limitations (specifically high SNR low INR cases). We also emphasize that there are significant shortcomings in the analytical models that demand additional effort for accurate threshold selection.

5.6.2 Payload Interference Detection Using Pilots

Recall from Fig. 5.2 that a series of known pilot symbols are interspersed amongst the OFDM sub-carriers. If the radar waveform overlaps a pilot in the frequency domain, the fact can be used for detection. Recall from (5.11) that the least squares channel estimates for a subcarrier l on antennas $1, 2$ are respectively:

$$\hat{H}_{1,l} = H_{1,l} + W_{1,l}^{(V)} \tag{5.21}$$

$$\hat{H}_{2,l} = H_{2,l} + W_{2,l}^{(V)} \tag{5.22}$$

In order to detect interference during the k^{th} OFDM symbol on the pilot subcarriers ($l \in \{11, 25, 40, 54\}$) we use the following decision statistic:

$$\mathcal{V}_l^{(k)} = \frac{1}{2}\left\{X_l \cdot (H_{1,l} + H_{2,1}) - X_l \cdot (\hat{H}_{1,l} + \hat{H}_{2,1}) + W_{1,l}^{(k)} + W_{2,l}^{(k)}\right\} \tag{5.23}$$

According to the Wi-Fi standard, $X_l \in \{-1, +1\}$ which leads to the following relationship:

$$\mathcal{V}_l^{(k)} = \frac{1}{2}\left\{W_{1,l}^{(V)} + W_{2,l}^{(V)} + W_{1,l}^{(k)} + W_{2,l}^{(k)}\right\} \tag{5.24}$$

The null hypothesis $\mathcal{H}_0$ then yields:

$$\mathcal{H}_0 : \ \mathcal{V}_l^{(k)} \sim \mathcal{CN}\left(0, \sigma_w^2\right) \implies |\mathcal{V}_l| \sim \text{Rayleigh}\left(\frac{\sigma_w^2}{2}\right) \tag{5.25}$$

Since $\mathcal{V}_l^{(k)}$ are iid (in k), the false alarms occur independently on each of the four pilot subcarriers. Hence the target per-pilot false alarm rate $\hat{P_{fa}}$ can readily be obtained:

$$\hat{P_{fa}} = 1 - (1 - P_{fa})^{\frac{1}{4}} \tag{5.26}$$

and the threshold η_l follows:

$$\hat{P_{fa}} = \mathbf{Pr}\left(|\mathcal{V}_l|_{\mathcal{H}_0} > \eta_l\right) \tag{5.27}$$

$$\eta_l = \sqrt{-\sigma_w^2 \log \hat{P_{fa}}} \tag{5.28}$$

Similarly, we can approach calculation of the probability of detection P_d. We define the per-subcarrier INR:

$$\mathrm{INR}_l = \frac{|U_l|^2}{\sigma_W^2} \tag{5.29}$$

Recall that under hypothesis $\mathcal{H}_1$, $\mathcal{V}_l$ has the following description:

$$\mathcal{H}_1 : \ \mathcal{V}_l^{(k)} = \frac{1}{2}\left\{W_{1,l}^{(V)} + W_{2,l}^{(V)} + W_{1,l}^{(k)} + W_{2,l}^{(k)}\right\} + U_l \tag{5.30}$$

and hence, $\mathcal{V}_l^{(k)}$ is distributed as a Rician random variable:

$$\mathcal{H}_1 : |\mathcal{V}_l| \sim \text{Rician}\left(\sigma_w\sqrt{\mathrm{INR}_l}\ , \frac{\sigma_w^2}{2}\right) \tag{5.31}$$

The probability of detection on a given pilot is then simply:

$$P_{d,l} = Q_1\left(\sqrt{2 \cdot \mathrm{INR}_l}\ , \frac{\sqrt{2}\eta}{\sigma_w}\right) \tag{5.32}$$

where $Q_1(.)$ is the Marcum Q-function. Finally, the overall probability of detection is:

$$P_d = 1 - \prod_{\substack{l=11,25,\\ 40,54}} (1 - P_{d,l}) \tag{5.33}$$

Fig. 5.9b shows a comparison of simulation results to those obtained from the analysis in this section. Specifically, we consider three separate cases:

1. When the radar waveform's 3dB bandwidth overlaps that of a pilot, the threshold η_l is extremely effective at detecting the radar interferer. In fact, for almost any INR of interest (above 5dB), detection is virtually guaranteed. This result is significant as we will demonstrate in the next section when we employ mitigation schemes for radar interference.

2. When the radar waveform is randomly positioned in relation to the pilots, detection suffers. Still, an 80% detection rate is possible at 8dB while detection is virtually guaranteed above 18dB INR.

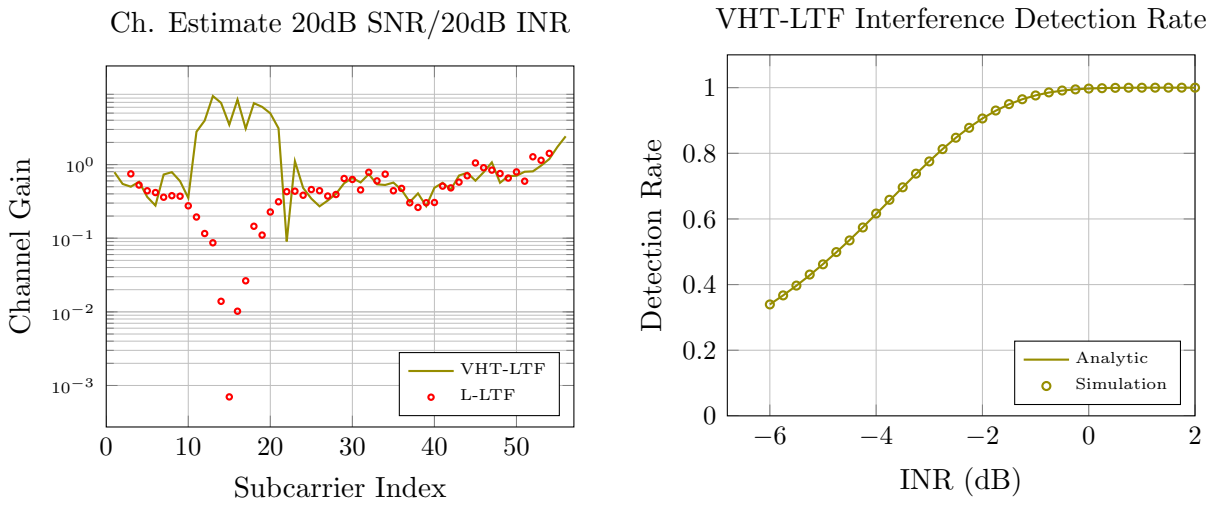
3. When the radar waveform is guaranteed to be 'sandwiched' between pilots, the detection rate is worst as a function of INR. Nevertheless, a reasonable detection rate is achieved by 13dB and a virtual guarantee of detection by 18dB.

Notice that compared to the detection scheme described in Section 5.6.1, pilot aided detection enjoys a higher detection rate as well as a better method for setting detection thresholds. Under some circumstances (e.g. between 0-10dB SNR and no significant radar overlap with pilots) the pure energy detection method may still be suitable. Lastly, narrowband radar signals may be more difficult to detect using pilots due to the large pilot spacing (14 subcarriers) necessitating a fallback to aggregate energy detection. By carefully planning the frequency alignment of the radar and Wi-Fi (in practice this is likely to occur purely at the Wi-Fi side), an overlap with the pilot can become more likely leading to a better chance for detection.

5.6.3 Interference During LTF

In the case of interference arriving during the VHT-LTF, we can take advantage of the in-built redundancy due to the L-LTF. Specifically, the L-LTF is almost identical to VHT-LTF with the exception that in VHT, an additional 2 subcarriers are used on either side of the band (i.e. using L-LTF we obtain a channel estimate for 52 subcarriers instead of 56). When interference is detected during the VHT-LTF, the channel estimates for the center 52 sub-carriers can be replaced with those from the L-LTF (see Fig 5.11a).

An interesting side-effect of this duplicate LTF is that a false detection of interference carries with it a very low penalty. Consider that in the worst case, a false alarm will simply replace one realization of the channel estimation noise with another.



(a) (b)

Figure 5.11: (a) When radar interference arrives during the VHT-LTF, the channel estimate is significantly impacted. The VHT-LTF and L-LTF based estimate are largely identical, except for the two additional subcarriers on each side of the band that are present for VHT-LTF. In this simulation, the radar's signal is concentrated around Wi-Fi subcarrier 15. (b) Detecting interference by comparing estimates from the VHT-LTF to that of the L-LTF is highly accurate with $P_d = 1$ at $0dB$ INR.

Using the least squares channel estimates (5.11), the difference between two subsequent channel estimates (assuming coherence time is $\gg$ than the interval separating L-LTF and VHT-LTF [26]) can be written as follows:

$$\kappa_l = \hat{H}_l^{(L)} - \hat{H}_l^{(V)} = W_l^{(L)} - W_l^{(V)} \tag{5.34}$$

where the superscripts $^{(L)}$ and $^{(V)}$ are used to signify the channel estimates obtained from the L-LTF and VHT-LTF respectively. Since $W_l^{(L)}$ and $W_l^{(V)}$ are iid gaussian random variables with variance σ_w^2, then $\kappa_l \sim \mathcal{CN}(0, 2\sigma_w^2)$. Again, assuming no additional knowledge of the radar interference, we must once again rely on the CFAR criterion for detecting interference during the channel estimate. Note that the $\hat{H}_l^{(L)}$ is only defined for $l \notin \{[0,5] \cup 32 \cup [59,63]\}$

since the L-LTF does not transmit pilots on subcarriers $l \in \{4, 5, 59, 60\}$.

We can borrow heavily from the analysis in the previous sections (recall that the total number of unoccupied subcarriers is 52). Specifically, we select a CFAR threshold ζ under hypothesis $\mathcal{H}_0$:

$$\mathcal{H}_0 : \ \kappa_l \sim \text{Rayleigh}(\sigma_w^2) \tag{5.35}$$

$$\hat{P_{fa}} = 1 - (1 - P_{fa})^{\frac{1}{52}} \tag{5.36}$$

$$\zeta = \sqrt{-2\sigma_w^2 \log \hat{P_{fa}}} \tag{5.37}$$

To obtain the probability of detection, we note that under hypothesis $\mathcal{H}_1$, the following holds:

$$\mathcal{H}_1 : \ \kappa_l \sim \text{Rician}\left(\sigma_w \sqrt{\text{INR}_l}, \sigma_w^2\right) \tag{5.38}$$

$$P_{d,l} = Q_1\left(\sqrt{\text{INR}_l}\ , \frac{\zeta}{\sigma_w}\right) \tag{5.39}$$

$$P_d = 1 - \prod_l (1 - P_{d,l}) \tag{5.40}$$

Fig. 5.11b compares the analytical detection results with those obtained through simulation. Again, even more so than before, radar interference is easily detectable if it occurs during the VHT-LTF. $P_d = 1$ is achieved at 0dB SNR.

5.7 Evaluating the Solution

We now revisit the motivation behind this work as outlined in Section 5.1.1. Maximizing utilization and re-use of radar spectrum entails the protection of radars combined with efficient usage of the shared spectrum. The means to deploy Wi-Fi networks in the largest proportion of allowed locations is a critical component in increasing the efficiency of this shared spectrum arrangement.

Path-loss models are notoriously inaccurate for predicting signal strength propagation in complex environments [60] , yet they are instructive as a method of comparison. In [37], the authors performed an exponential fit to the Longley Rice path-loss model [43] and arrived at

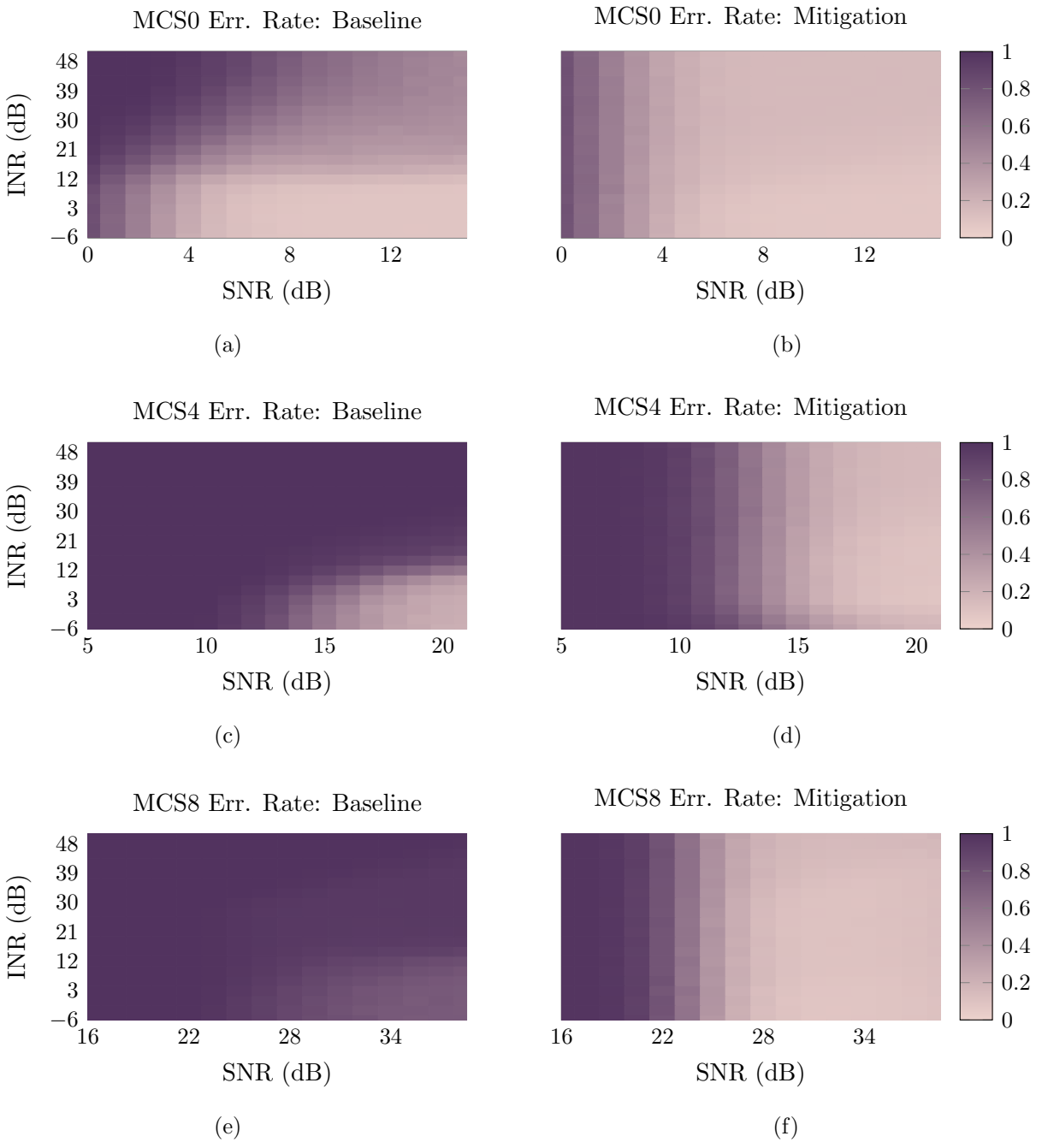


Figure 5.12: (a) (c) (e) The overall error rate for a Wi-Fi packet incorporating all stages of reception is shown for the various MCSes. (b) (d) (f) After the application of the proposed mitigation schemes, the resulting error rates are dramatically improved to the point of insensitivity to radar INR.

a path-loss exponent of -3.97 as a suitable approximation yielding the following path-loss formula:

$$\mathrm{PL}(d) = 24.133dB - 39.7\log_{10}(d) \tag{5.41}$$

The maximum allowable interference to the radar mandated a path-loss of 141dB (Section 5.1.1) corresponding to a minimum distance d_{min} of separation between the radar and the WLAN:

$$d_{min} = 10^{\frac{141+24.133}{39.7}} \approx 13.5KM \tag{5.42}$$

Assuming a noise floor of $-90dBm$, radar transmit power $80dBm$ (a conservative estimate), and an antenna gain of $10dB$ (e.g in the back lobe), a WLAN receiver located at d_{min} can expect to see large values for INR:

$$\mathrm{INR}_{max} = 80dBm + 10dB - 141dB = 39dB \tag{5.43}$$

Without mitigation mechanisms proposed in this work, INR levels above 10dB would significantly impact all but the lowest MCS. Even an intermediate MCS such as MCS4 is unable to cope with INR levels above $5dB$ (Fig. 5.12c), an INR level that requires a distance $103KM$ to achieve.

$$10^{(175+24.133)/39.7} \approx 103KM \tag{5.44}$$

The disparity between these distances would negate much of the sought after gains driving efforts towards shared access to radar spectrum. By implementing the minimal fixes proposed in this work, a Wi-Fi network can be deployed as close as possible to d_{min} while still obtaining satisfactory throughput.

5.8 Conclusion

In this work, we presented a detailed link level study of WLAN and radar coexistence using a signal level link simulator. We showed the impact of interference on various stages of

reception that would render WLAN networks inoperable under expected levels of radar interference. We showed that by detecting radar interference, we are able to provide a pair of mitigation mechanisms to combat interference during the payload and channel estimation phases. Then, we provide analysis and simulations to prove that radar interference detection is not only possible, but can be done efficiently and with minimal impact to the Wi-Fi network. Finally, putting all of these pieces together, we compared the packet error rate for a standard WLAN receiver compared to one employing the novel methods described within this work showing dramatic improvements that make WLAN operable in a vast array of scenarios of interest.

Appendix A

INVESTIGATION AND IMPROVEMENTS TO THE OFDM WI-FI PHYSICAL LAYER ABSTRACTION IN NS-3

This work presents results based on a critical re-examination of the current physical layer abstractions for IEEE 802.11 OFDM WLAN in the ns-3 network simulator motivated by a) the need to improve fidelity of the Layer-1 abstraction essential for a network level simulator, and b) setting the stage for desired new features (not currently implemented) in the future. We implement a *multi-stage packet reception* that addresses a shortcoming in the current WLAN receiver model, making it closer to existing hardware, and lays the groundwork for improvements such as packet capture. Next, we consider the frame error rate (FER) model in ns-3 which relies on analytical bounds on the bit error probability (BER) at the output of the convolutional decoder. We demonstrate key issues with the current approach through detailed link level simulations using a newly developed Wi-Fi link simulator and look forward to forthcoming fixes being considered.

A.1 Introduction

In recent years, simulation tools have played a critical role in wireless research and development. Standards organizations such as the 3rd Generation Partnership Project (3GPP) and the IEEE have relied heavily on simulation scenarios to guide the development of cellular and Wi-Fi standards and evaluate ideas proposed for inclusion. Likewise, the research community has made extensive use of simulation tools to accompany mathematical analysis. In fact, in many cases, mathematical analysis is intractable or otherwise cumbersome and simulation tools such as ns-3 have become the primary method for evaluating new designs and performance in specified use-case scenarios. To that end, ensuring the accuracy and

performance of these tools is crucial to their credibility and ultimately, wider acceptability. One such tool widely used in academia is the network simulator 3 (ns-3) [3]. ns-3 is an open source packet level simulator, with the intent to support a growing number of wireless and wired network stacks. In this paper, we focus exclusively on the current Layer-1 error model abstractions for ns-3 OFDM Wi-Fi (802.11n); based on a critical examination, highlight some shortcomings.We first propose some architecture modifications that are consistent as a foundation for future extensions. We then implement a new *multi-stage packet reception* framework and evaluate its impact.

A.1.1 The Simulation Workflow

Network simulation integrates two categories of simulation tools:

1. **Link Simulators** These signal level simulators (typically built in MATLAB) are designed to closely mimic the physical layer operation of a wireless modem incorporating all details of the digital baseband sections - modulation, demodulation, coding, channel emulation/estimation, and the effect of analog components such as gain control and digitization. The goal is to evaluate receiver algorithms (typically as a function of SNR) to derive bit and ultimately, frame error rates in a single Wi-Fi link. The run-time complexities of these simulators limit their suitability to single link simulations.

2. **System Simulators** System level simulators are designed to abstract away the effects of the physical layer into simple quantities such as frame error rate as a function of SNR. By design, these operate at Layer-2 (frame-in/frame out) and thus require the Link Simulator to provide a frame/packet based link abstraction (i.e. a table look-up for the FER as a function of all relevant system parameters, including SNR). By operating at this level of abstraction, system simulators offer the ability to simulate networks with hundreds of nodes with reasonable run-time. Hence, they are an excellent tool for evaluating the full protocol stack including the effect of application, transport and network layers as well as network topologies.

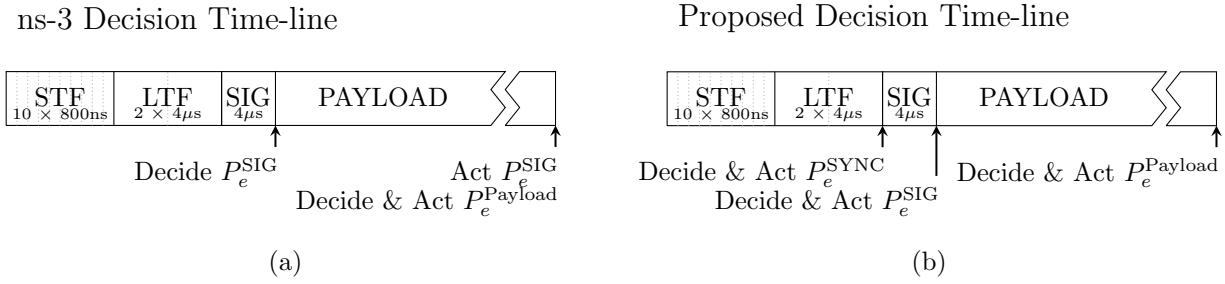


Figure A.1: (a)The current implementation of Wi-Fi in ns-3 uses a single action point at the end of the frame. (b)Our newly proposed decision process makes the appropriate decisions at the relevant intermediate points.

One important aspect in the usage of system simulators is the choice of the physical layer abstractions (also referred to as the link-to-system mapping). The accuracy of this mapping (and hence the credibility of the system simulator) reflect how closely the simulator models effects that occur in real networks. In the case on ns-3, the Wi-Fi model at present lacks the ability to accurately depict packet capture [29]. Also, concerns have been raised over the validity of the two error models in use; the YANS error model [39] has been found to be too optimistic for AWGN channels, while the NIST error model [58] has been found to be too conservative [36, 58]. These concerns motivate detailed look at the current physical layer abstraction employed in ns-3.

A.1.2 Preliminaries

We begin by describing the structure of a Wi-Fi packet as it pertains to the reception process. In this paper, we consider a Wi-Fi system with a channel width of 20MHz according to the 802.11 standard [9]. Since the 802.11g release of Wi-Fi, OFDM has served as the underlying air interface technology for a multitude of reasons pertaining to favorable performance characteristics (e.g. resistance to multi-path delay spread, ease of equalization, etc.) At the

physical layer, a Wi-Fi frame consists of four major portions[1] (Figure A.1):

Short Training Field (STF): This portion of the frame consists of an 800ns signal repeated 10 times. The periodic nature of the signal is meant to assist in frame synchronization and detection using a delayed autocorrelation method [71]. At the start of the frame, correlating the incoming signal with a version of itself delayed by 800ns presents strong peaks that allow the receiver to locate the start of the frame. In addition, during the STF, the Automatic Gain Control (AGC) at the receiver is adjusted in order to obtain good quantization performance (dynamic range) for the remainder of the frame.

Long Training Field (LTF): This portion of the frame consists of a $4\mu s$ OFDM symbol repeated twice. The purpose of this portion of the frame is to assist in channel estimation, coarse carrier frequency offset estimation, IQ imbalance estimation and other signal processing tasks requiring a reference signal. Errors in the estimate can dramatically impact decoding of the payload. Typical estimators such as MMSE or DFT are employed [20].

L-SIG Field: This portion of the frame is modulated as BPSK with a rate 1/2 convolutional code. It is responsible for carrying information on how the data field can be decoded including the modulation scheme, the coding rate, and the duration of the data. The BPSK symbols are converted into OFDM symbols with the same properties as the data portion.

Payload: The data field is transmitted using 64 sub-carriers with a carrier separation of 312.5 kHz. Some sub-carriers are unused (e.g. DC sub-carrier, 6 on the left and 5 on the right due to the guard bands) and 4 of the modulated sub-carriers are allocated as pilots. The remaining 48 data sub-carriers all use the same modulation which can range from BPSK/QPSK through 64-QAM (802.11a/n) or 256-QAM (802.11ac or later). The data is encoded using a convolutional encoder and decoded at the receiver using a Viterbi decoder. Each OFDM symbol used for data transmission is of duration $4\mu s$ (which includes an $800ns$ cyclic prefix). For Modulation Coding Schemes (MCSes) addressed in this work, Wi-Fi employs a constraint length 7 convolutional encoder with rate 1/2 which can be punctured to

[1]We omit specifically addressing additional header fields introduced in the HT modes in this work and leave it as a subject of future work

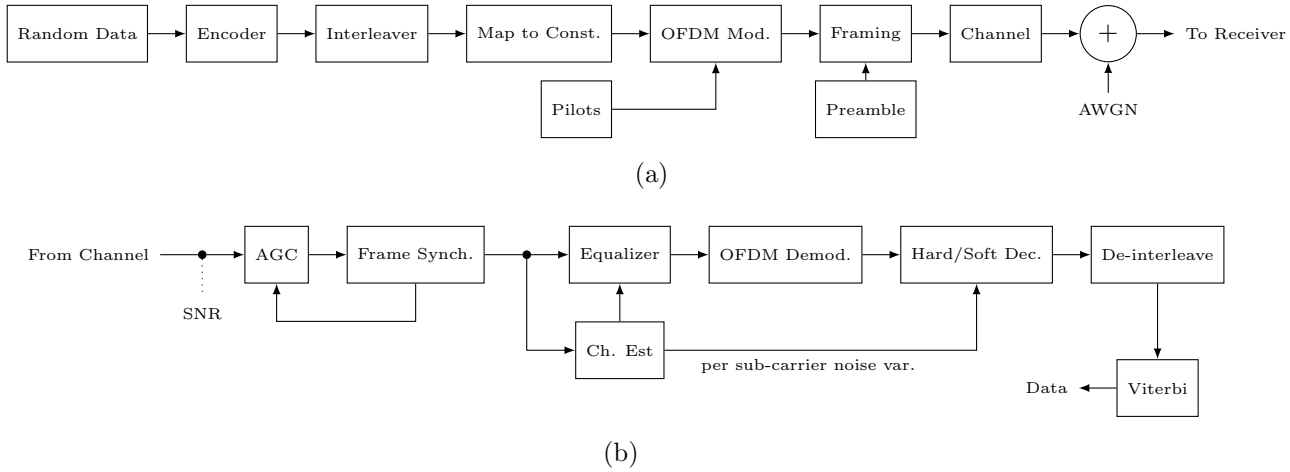


Figure A.2: (a) Block diagram for a single antenna Wi-Fi transmitter. (b) Receiver block diagram for single-antenna Wi-Fi receiver link simulations.

achieve other desired rates [**?**].

A.1.3 Motivation

The current ns-3 error model for payload reception is based on analytical results for bit error probabilities (note that the L-SIG is nothing but a short duration payload). Specifically, once an expression for P_b (the bit error rate) as a function of SNR is obtained [45], the payload error rate P_e is computed as follows:

$$P_e = 1 - (1 - P_b)^N, \tag{A.1}$$

where N is the number of data bits in the payload.

In examining the current physical layer abstraction and error model in ns-3, we will consider two aspects:

1. Sources of packet/frame error

2. Accuracy of error probabilities as a function of SNR and payload length

To address the first aspect, we note that in the current implementation of ns-3, a successful packet entails a computation at the end of the L-SIG for correct reception of the header, followed by an error rate computation at the end of the frame to decide on correct reception of the payload. Although failure of the L-SIG is considered at the end of the L-SIG field, the model defers any change of state notification (i.e. the receiver remains in an RX state) until the end of the frame. This does not conform to existing hardware Wi-Fi systems. Lastly, errors during STF/LTF are not even considered.

But first, we begin our examination with the second facet of the abstraction by considering the analytical bit/packet error rates used within ns-3. In the next section, using the published results from 802.11 standardization as a guide [49], we take a closer look at these error rates and consider any factors that may explain the large discrepancies.

A.2 AWGN Phy Layer Simulations

In order to take a critical look at the ns-3 physical layer error model, we employ a MATLAB based link simulator [7] and focus on a SISO Wi-Fi system as a natural first step. Figure A.2 shows a block diagram describing operations carried out in our link simulator. Additionally, the current incarnation of ns-3 operates under the assumption of an AWGN channel exclusively, hence the results we produce make the same assumption (we hope to address frequency selective channel models such as TGn Channel D in the future).

On the transmitter side, after the application of a convolutional error correcting code [**?**], the bits are interleaved and modulated according to the desired constellation (BPSK through 64QAM) before being transmitted through the channel. The parameters used for the link simulations are shown in Table A.1. We emphasize that *noise figure* is set to 0dB for all the results in this section ensuring a fair comparison. Non-zero noise figure can easily be accounted for as a simple additive SNR shift for all results.

The currently employed ns-3 model for frame errors is described in A.1.3 and in particular in (A.1). The two issues with this approach which we aim to study in this section:

Table A.1: Link Simulation Parameters.

Antenna	1x1 (SISO)
Sampling Rate	100 MHz
AGC	Logarithmic Loop
ADC	Ideal 12bit
Synchronization	Delayed Auto-correlation
Channel Estimation	Ideal (AWGN)
Demodulator	Soft Decision (8bit quantization)
Decoder	Viterbi (128 Traceback)
Noise Figure	0dB
Iterations	> 2048

1. The bit error rate bounds are accurate at higher SNRs, yet the lower MCSes are typically used at lower SNRs (where the bound is loose).

2. Computing the frame error rate using (A.1) makes the *critical* assumption that bit errors occur independently

There are two other discrepancies when comparing ns-3 to our simulations as well as those from IEEE Task Group n (TGn). Firstly, modern WLAN receivers typically use soft decoding in place of hard decoding due to the 1-2dB gain[2] afforded as a result. The 802.11 standard does not require any specific decoding mechanism, though usage of soft decoders has become standard practice.

Another contributing factor in mismatch between ns-3 and simulations lies in the computation of the SNR (Figure A.2b shows where SNR is measured in the system). Currently, ns-3 considers noise power over 20MHz while in reality the noise of interest is limited to the

[2]The real system gain is less than the theoretical one due to quantization and truncation of the log-likelihood ratios

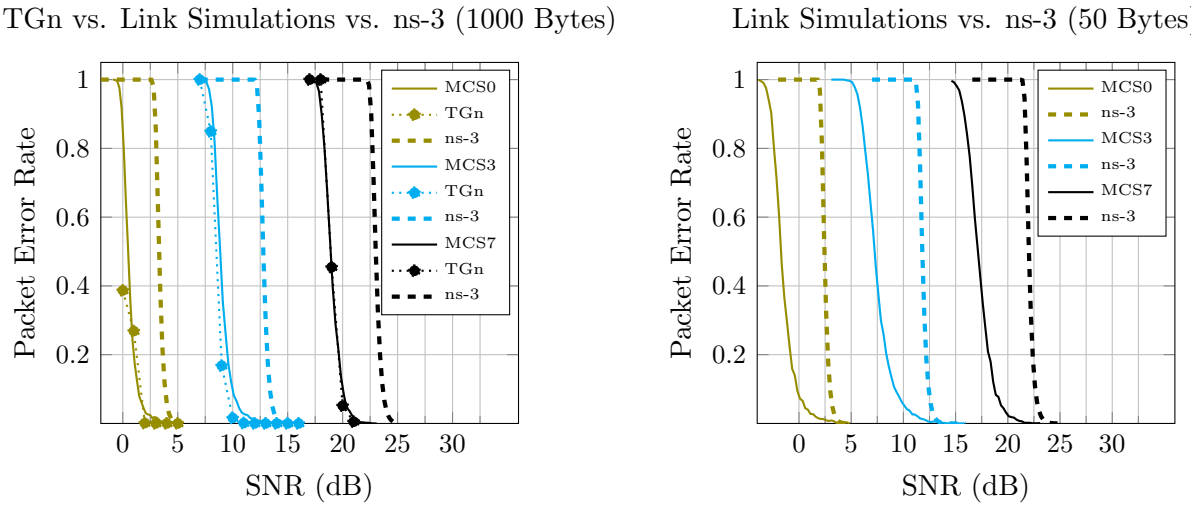


Figure A.3: (a) Comparing simulation and TGn results (see [49] Figure 2-1) to ns-3 reveals a large gap. The transition is also more rapid in the case of ns-3. (b) The SNR gap between ns-3 results and those of the link simulator widens for smaller payloads. No TGn results exist for this payload size.

occupied sub-carriers (i.e. 52/64), hence an additional SNR shift must be accounted for:

$$SNR_{\text{dB}} = 10\log_{10}\frac{P_{TX}}{N_0 20\text{MHz}} + 10\log_{10}\frac{52}{64} \tag{A.2}$$

In Figure A.3a, we compare our link simulation results to those produced by the IEEE's 802.11n task group [49] during standardization for MCS0, NCS3 and MCS7 (selected for simplicity, though all MCSes exhibit the same behavior). While our link simulation results for frame errors closely match those of IEEE TGn, ns-3 displays a far more pessimistic error rate. We can observe that this disparity is not merely an SNR shift since the slope of the graphs also differs (ns-3 exhibits a sharper transition).

Even if we were to adjust for the SNR offset described by (A.2), ns-3 retains a 2-3dB gap across the range. This can be attributed in part to the assumption of independence regarding bit errors which in effect spreads errors amongst multiple frames when they are actually more concentrated/localized. In our opinion, this intrinsic assumption makes models that rely on bit errors less suitable for use in ns-3.

A.2.1 Packet Error Rates in ns-3: Issues

A possible remedy is for the ns-3 physical layer to move to a packet error based model that uses link simulation results to decide on packet errors directly. In deriving frame errors from analytical bounds on bit error rates for coded bits, we encounter complicating factors that warrant a thorough examination of mappings from SNR to error rates:

- Effect of frame length on error rates
- The impact of coding on isolated bit errors

It is this second shortcoming which is most problematic. It is well known within the literature that bit errors occur in bursts at the output of the Viterbi decoder [24]. Hence, using the Viterbi bit error rate under the iid assumption (A.1) results in a very loose upper bound. While this equality holds for an uncoded packet, for coded bits, a tighter *upper bound* can be

obtained by using the first error probability P_e in (A.1) instead of the *bit error* probability [62].

Figure A.3b compares the error rates for a shorter frame duration (50 bytes) that could represent something like a TCP acknowledgment message. Clearly, the gap has increased and the slope has diverged even more in comparison to the 1000 byte packets examined in A.3a. Likewise, in the case of the L-SIG (a 3 byte payload at MCS0), the difference is even more stark. In Table A.2, we show the required SNR to decode the L-SIG with various success rates. To achieve a 50% success rate in decoding the L-SIG, ns-3 error models indicate a required SNR of 1.7dB while our link simulator can do so at -3.5dB, a difference of more than 5dB.

Then, we must also consider the effect of varying SNR during a frame which is currently tackled in ns-3 by arbitrarily splitting the frame across bit boundaries (not accounting for the underlying timing of the OFDM symbols). And finally, we note that ns-3's current treatment of interference via a unified SINR (whereby interference is treated as additive noise) has it's own limitations; but changes to this is deferred to future. We conclude this section by stating that the need for an improved physical layer abstraction is clear, and through the proposed improvements, we set the stage for subsequent improvements in ns-3 WLAN/OFDM Phy abstractions in future. Recent work in the IEEE 802.11ax standards committee has emphasized the importance of a accurate computations of error rates. To that end, we believe that a similar approach incorporating a frequency selective effective SINR model (such as MIESM or RBIR) would be a necessary first step.

A.3 Wi-Fi Reception Process in ns-3

The existing Wi-Fi reception process in ns-3 works based on the received SNR at the physical layer [2] and frame length. We propose to modify the existing decision process to the one shown in Figure A.1b, with the ability to "drop" a frame at any of the decision stages, bringing it closer to actual WLAN implementations [17]. The motivation behind this modification is two fold: i) helping to account for the lack of capture effect in existing ns-3 reception, and

Table A.2: Required SNR to achieve given success rates for SYNC and L-SIG.

	ns-3 (SNR)		LinkSim (SNR)	
Success Rate	50%	95%	50%	95%
SYNC		-	-10 dB	0.21 dB
SIG	1.7 dB	2.4 dB	-3.5 dB	0.3 dB

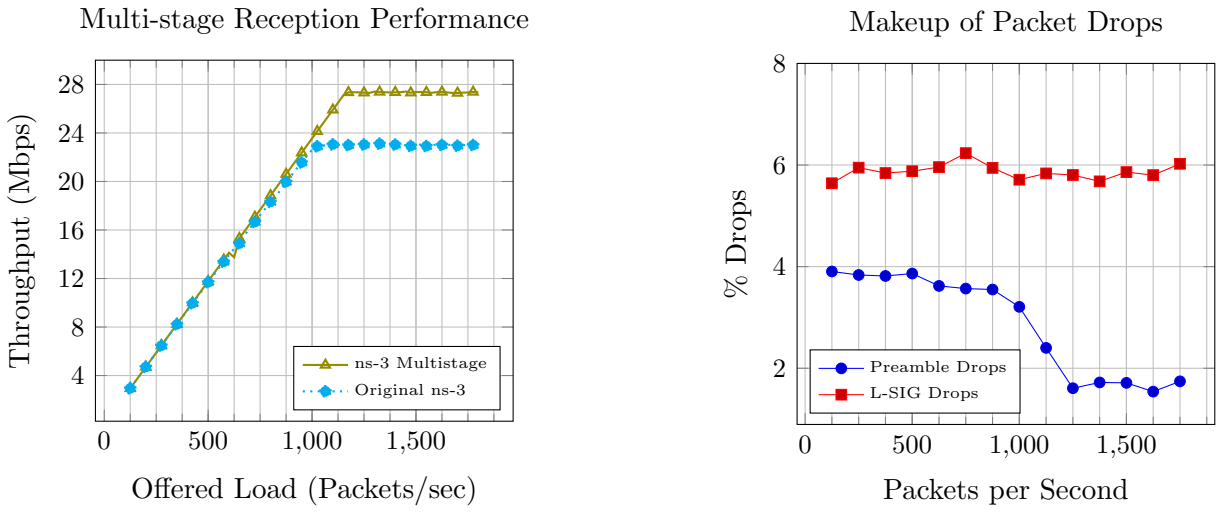


Figure A.4: (a) Throughput increase in the hidden node scenario due to multi-stage reception (b) Percentage of frame drops occurring before the payload captured by multistage reception.

ii) anticipated low SINR scenarios in future co-existence simulations within ns-3. Splitting up the reception process requires error results for the STF/LTF preamble sync, which we generate from link simulations.

A selection of results for sync are tabulated in Table A.2. A natural question to ask is: what is the significance of the added stages? At SNRs higher than 5dB, synchronization is almost always successful, however, keep in mind that ns-3 uses SNR in lieu of SINR, hence it incorporates interference. While periodically low SINRs at the start of the frame are expected to occur more frequently in co-existence studies, they can occur even in the current Wi-Fi only simulations when accounting for high node densities or hidden nodes (see Table A.3).

As an example, accounting for drops at the LTF/STF stage can lead to a 5.5% drop in throughput in the case of 10 flows on the network. Conversely, if we consider a hidden node scenario (described in [4]), we observe that partial collisions within the STF/LTF occur frequently. If the receiver is locked onto a weak signal through the end of a frame, other subsequent stronger frames will be ignored. By dropping a weak packet early, running the same simulation scenarios yields a throughput gain of up to 16% at high offered loads.

Given this motivation, we modify the Wi-Fi reception in ns-3. It is pertinent to mention here that inclusion of accurate sync error models adds to the fidelity of the reception process as opposed to relying only on the L-SIG error rates and assuming perfect synchronization based only on *received power*. This will have a greater impact in the case of multiple possibly heterogeneous interference sources.

We now go on to describe the simulations used to obtain the synchronization error rates, and the impact of the multistage reception on existing ns-3 Wi-Fi only simulations.

A.3.1 Multistage Reception

We use link simulations to provide a synchronization failure rate (P_e^{SYNC}) for the newly added stage in ns-3. Aside from the trivial case of not detecting the start of a frame altogether, any timing error in the synchronization can propagate through the remainder of the reception

Table A.3: Likelihood of Low SNR During Synchronization for 25 Node Ad-Hoc Network [5].

	Frequency of Occurrence			
Flows	$< 2dB$ *SINR*		$< 5dB$ *SINR*	
2	1.5%		2.4%	
5	2.47%		4.04%	
10	3.56%		5.71%	

process (so called "soft effects"). In particular, the effective SNR loss due to synchronization error has some impact on payload demodulation especially for higher modulation orders (e.g. 64QAM).

We do not propose keeping track of such soft effects at this time due to the added implementation complexity that it would entail (though we are considering them for inclusion in the future). Instead, in order to arrive at a number for P_e^{SYNC}, we set an acceptable synchronization error threshold of less than 1 cyclic prefix (i.e. $800ns$) within the LinkSim. If the initial synchronization estimate is within this window, we consider the timing acquisition (and frame detection) to have been successful[3]. Table A.2 shows some synchronization results as a function of SNR for the AWGN channel. Note that if there is significant SNR variation between the synchronization stage and the payload, the soft effects of synchronization will become more apparent, however, we leave this case for future work.

The implementation has been modified to separate the preamble and header reception process, with the ability to drop the packet at either of these stages and, potentially, commit to another incoming packet. The preamble reception is compliant with the standard [9, 15.3.6.2]. At the start of reception, if the PHY is either IDLE or CCA_BUSY, and there is currently no SYNC being attempted, an end of preamble event is scheduled. At the LTF, the success rate of the preamble sync is looked up from LinkSim based results, and an event for L-SIG header reception is scheduled. If the preamble has synced successfully, the reception

[3]For higher MCSes, a fine grained timing synchronization step can follow the initial coarse estimate [67].

process moves onto header decode, otherwise the frame is dropped and the PHY reverts from the reception state. If the header is decoded successfully, this is followed by payload decode. Again, if the header fails, the frame is dropped with a corresponding change in the PHY state. This model necessitates the addition of a state to indicate whether there is a preamble sync being attempted, and to ensure that a header decode is preceded by a successful preamble sync.

A.4 ns-3 Simulation Results

To study the impact of multi-stage reception on Wi-Fi simulations, a canonical hidden node scenario was studied, both with and without RTC/CTS enabled [4]. Two nodes, hidden from each other, transmit to a common access point placed in the center. The L-SIG was transmitted at MCS0, with the payload at MCS7 for 1472 byte frames. Constant bit rate traffic was generated, and the number of frames per second ranged from 125 ($1.47Mbps$) to 1800 ($21.19Mbps$) for *each* transmitting station. The default NIST error rate model was used for both cases, with SYNC results from LinkSim incorporated for the multi-stage reception.

The original reception process gives lower throughput, since incoming frames with a high (average) SNR can be dropped due to the AP's commitment to receive a frame from the other station that partially overlaps the incoming frame. With modified reception, the throughput improves, with increased effect at higher traffic loads as seen in Figure A.4a. To further illustrate the impact of frame drops at the preamble and header stages, the percentage of total drops occurring at these two stages were tabulated A.4b. In the hidden node scenario, 8-10% of the total drops happen before the payload stage. For these cases, the AP is now free to receive the next incoming frame, instead of being tied to an erroneous frame that a real implementation would have given up on. In both implementations we observe that the throughput levels off at increasing offered load due to built-in MAC layer overheads.

The same experiment was repeated with RTC/CTS enabled. Since the data packet collisions decrease significantly, the throughput for both the multi-stage and original reception line up. There is still a small difference in the throughput ($0.3Mbps$) at the maximum offered

load (1800 packets per second), due to the collision of RTS frames.

When the same simulation scenario is repeated with both stations visible to each other, the throughput is identical for both cases. For simulations with multiple flows with no hidden nodes, the throughput with multi-stage reception was lower than the original ns-3 implementation. One example scenario was an ad-hoc grid [5], where the throughput for multistage is 0.3% lower for 2 flows, and decreases by 5.5% for 10 $4Mbps$ flows. This difference results from an overall greater number of frame drops, a direct consequence of the newly added sync stage.

The results indicate that in current scenarios, multistage reception has an impact on the simulation results, albeit in a limited fashion. However, while our current work does not explicitly model frame capture, the additional stages we have introduced set the stage for inclusion of capture effect in the future which will lead to even greater changes in throughput (see [30]).

A.5 Conclusion and Future Work

In this paper, we evaluate the ns-3 physical layer abstraction to improve fidelity and accuracy. We developed a link simulation tool and show that its results closely match those published by the IEEE task group charged with Wi-Fi standardization. We then used our link simulator to examine possible sources of error in the ns-3 physical layer error model that support a move away from the default analytical model. Then, with a eye towards future inclusion of capture effects in ns-3 as well conforming to existing hardware implementation, we used results from our link simulator to introduce a multi-stage reception model for ns-3 with inclusion of preamble sync error rates. Finally, we studied the effect of our modifications in some canonical scenarios (hidden nodes and RTS/CTS) to ensure that the behavior conforms to expectations. In this context, we are validating and developing both analytical error models, and link-sim results, as well as changes to the physical layer abstraction to augment the fidelity and range of applicability of ns-3.

Although not finalized yet for submission to the ns-3 main tree, we have developed

modifications to the YansWifiPhy class to enable the third stage of reception and to provide a link simulation-based error model for the PLCP preamble fields. We have also developed a framework that permits the loading of link simulation-based error models that are expressed as text files, to replace the analytical error models. We plan to investigate further with our link simulator how best to handle situations in which the SNR varies during the duration of the received frame, including occurrences of Wi-Fi signal overlap.

BIBLIOGRAPHY

[1] GNU Radio Software.

[2] ns-3 Design Documentation: Wi-Fi Module.

[3] ns-3 Network Simulator.

[4] ns-3 Wi-Fi Example: wifi-hidden-terminal.

[5] ns-3 Wi-Fi Example: wifi-simple-adhoc-grid.

[6] Universal software radio peripheral (USRP).

[7] University of Washington Wi-Fi Link Simulator.

[8] Characteristics of radiolocation radars, and characteristics and protection criteria for sharing studies for aeronautical radionavigation and meteorological radars in the radiodetermination service operating in the frequency band 2700-2900 MHz. Technical report, International Telecommunication Union, 2000-2003.

[9] Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specification, 2009.

[10] Presentation: Spectrum with Significant Federal Commitments, 225 mhz - 3.7 ghz. Technical report, US National Telecommunications and Information Administration, 2009.

[11] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation, 2013.

[12] Presentation: Radar/Small-Cell Compatibility Lab and Field Tests. Technical report, Virginia Polytechnic Institute, 2014.

[13] Proposal to Create a Citizens Broadband Service in the 3550-3650 MHz Band. Technical report, FCC, Apr 2014.

[14] Amendment of the Commissions Rules with Regard to Commercial Operations in the 3550-3650 MHz Band. In *FCC Report and Order 15-47A1*. FCC, 2015.

[15] Athanassios V. Adamis and Philip Constantinou. Intermittent DCF: a MAC protocol for Cognitive Radios in Overlay Access Networks. In Wei Wang, editor, *Cognitive Radio Systems*. InTech, 2009.

[16] Giuseppe Bianchi. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, 2000.

[17] Broadcom. *WLAN Chipset BCM2050*.

[18] Camila C.S. Caiado and Pushpa N. Rathie. Polynomial Coefficients and Distribution of the Sum of Discrete Uniform Variables.

[19] Alex R Chiriyath, Bryan Paul, Garry M Jacyna, and Daniel W Bliss. Inner bounds on performance of radar and communications co-existence. *Signal Processing, IEEE Transactions on*, 64(2):464–474, 2016.

[20] Yong Soo CHo, Jaekwon Kim, Won Young Yang, and Chung-Gu Kang. *MIMO-OFDM Wireless Communications with MATLAB*. Wiley, 1st edition, 2010.

[21] Benjamin Cizdziel. Spectral Coexistence of Wi-Fi Networks with Radar Systems. Master's thesis, University of Washington, Seattle, WA, 2015.

[22] L. Cohen, E. Daly, J. DeGraaf, and K. Scheff. Mitigation of Radar Interference with WiMAX Systems. In *Waveform Diversity and Design Conference (WDD), 2010 International*, pages 159–164, Aug 2010.

[23] B.D. Cordill, S.A Seguin, and L. Cohen. Electromagnetic Interference to Radar Receivers Due to In-Band OFDM Communications Systems. In *Electromagnetic Compatibility (EMC), 2013 IEEE International Symposium on*, pages 72–75, Aug 2013.

[24] L.J. Deutsch and R.L. Miller. Burst Statistics of Viterbi Decoding. Technical Report TDA Progress Report 42-64, NASA, May 1981.

[25] E. Drocella, J. Richards, R. Sole, F. Najmy, A. Lundy, and P. McKenna. 3.5 GHz Exclusion Zone Analyses and Methodology. Technical Report TR-15-517, NTIA, June 2015.

[26] Vinko Erceg, Laurent Schumacher, , and Persefoni Kyritsi. TGn Channel Models. Technical Report IEEE 802.11-03/940r4, IEEE, May 2004.

[27] ETSI. EN 301 893. pages 1–26, 2012.

[28] FCC Spectrum Policy Task Force. Report of the spectrum efficiency working group. http://transition.fcc.gov/sptf/reports.html, 2002.

[29] P. Fuxjaeger and S. Ruehrup. Validation of the NS-3 Interference Model for IEEE 802.11 Networks. In *Wireless and Mobile Networking Conference (WMNC), 2015 8th IFIP*, October 2015.

[30] Xiaohu Ge, Dongyan, and Yaoting Zhu. Throughput Model of IEEE 802.11 Networks with Capture Effect. In *Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006.International Conference on*, pages 1–4, Sept 2006.

[31] Mo Ghorbanzadeh, Eugene Visotsky, Weidong Yang, Prakash Moorut, and Charles Clancy. Radar In-Band and Out-of-Band Interference into LTE Macro and Small Cell Uplinks in the 3.5 GHz Band, 2014.

[32] C. Ghosh, S. Roy, and D. Cavalcanti. Coexistence Challenges for Heterogeneous Cognitive Wireless Networks in TV White Spaces. *Wireless Communications, IEEE*, 18(4):22–31, August 2011.

[33] C. Ghosh, H.A. Safavi-Naeini, S. Roy, K. Doppler, and J. Stahl. QP-CSMA-CA: A Modified CSMA-CA-Based Cognitive Channel Access Mechanism with Testbed Implementation. In *Dynamic Spectrum Access Networks (DYSPAN), 2012 IEEE International Symposium on*, pages 501–509, Oct 2012.

[34] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005.

[35] Hugh Griffiths, Lawrence Cohen, Simon Watts, Eric Mokole, Chris Baker, Mike Wicks, and Shannon Blunt. Radar Spectrum Engineering and Management: Technical and Regulatory Issues. *Proceedings of the IEEE*, 103(1):85–102, 2015.

[36] Christopher Hepner, Arthur Witt, and Roland Muenzner. In Depth Analysis of the ns-3 Physical Layer Abstraction for WLAN Systems and Evaluation of its Influences on Network Simulation Results. *SINCOM 2015*, page 46, 2015.

[37] Farzad Hessar and Sumit Roy. Spectrum sharing between a surveillance radar and secondary wi-fi networks. *arXiv preprint arXiv:1602.00802*, 2016.

[38] Jan Kruys, Edgard Vangeel, Bruce Kraemer, Vijay Auluck, Rich Kennedy, Jim Raab, and Rob Kubik. Spectrum Sharing in the 5 GHz Band - DFS Best Practices. Technical report, Wi-Fi Alliance, 2007.

[39] Mathieu Lacage and Thomas R Henderson. Yet Another Network Simulator. In *Proceeding from the 2006 workshop on ns-2: the IP network simulator*, page 12. ACM, 2006.

[40] A Lackpour, M. Luddy, and J. Winters. Overview of Interference Mitigation Techniques Between WiMAX Networks and Ground Based Radar. In *Wireless and Optical Communications Conference (WOCC), 2011 20th Annual*, pages 1–5, April 2011.

[41] S. Le Goff, A Glavieux, and C. Berrou. Turbo-codes and High Spectral Efficiency Modulation. In *Communications, 1994. ICC '94, SUPERCOMM/ICC '94, Conference Record, 'Serving Humanity Through Communications.' IEEE International Conference on*, pages 645–649 vol.2, May 1994.

[42] Gary Locke and Lawrence E Strickling. An Assessment of the Near-Term Viability of Accommodating Wireless Broadband Systems in the 1675-1710 MHz , 1755-1780 MHz , 3500-3650 MHz , and 4200-4220 MHz , 4380-4400 MHz Bands. Technical report, U.S. Department of Commerce, 2010.

[43] A. G. Longley and P. L. Rice. Prediction of tropospheric radio transmission loss over irregular terrain. a computer method-1968. Technical Report AD0676874, 1968.

[44] J. Massey and P. Mathys. The Collision Channel Without Feedback. *IEEE Trans. Inf. Theor.*, 31(2):192–204, March 1985.

[45] LE Miller. Validation of 802.11 a/uwb coexistence simulation. Technical report, national institute of standards and technology (NIST), WCTG white paper, 2003.

[46] J. Mitola and G. Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, Aug 1999.

[47] J. Mitola and Jr. Maguire, G.Q. Cognitive Radio: Making Software Radios More Personal. *Personal Communications, IEEE*, 6(4):13–18, Aug 1999.

[48] Apurva Mody, Ranga Reddy, Matthew J. Sherman, and Tom Kierman. Resource Allocation for Improved Self-coexistence. IEEE Workingroup Report 802.22-08/0092r06, August 2008.

[49] Syed Aon Mujtaba. TGnSync Proposal PHY Results. Technical Report IEEE 802.11-04/891r5, Agere Systems, July 2005.

[50] Rohan Murty, Ranveer Chandra, Thomas Moscibroda, and Paramvir (Victor) Bahl. Senseless: A database-driven white spaces network. *IEEE Transactions on Mobile Computing*, 11(2):189–203, February 2012.

[51] NTIA. 3.5 GHz Exclusion Zone Analyses and Methodology. Technical Report 15-517, June 2015.

[52] George Nychis, Thibaud Hottelier, Zhuocheng Yang, Srinivasan Seshan, and Peter Steenkiste. Enabling MAC Protocol Implementations on Software-defined Radios. In *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation*, NSDI'09, pages 91–105, Berkeley, CA, USA, 2009. USENIX Association.

[53] President's Council of Advisors on Science and Technology (U.S.). *Report to the President: Realizing the Full Potential of Government-held Spectrum to Spur Economic Growth*. 2012.

[54] Office of the Press Secretary. Presidential memorandum: Unleashing the wireless broadband revolution, June 2010.

[55] R.C.D. Paiva, P. Papadimitriou, and S. Choudhury. A Physical Layer Framework for Interference Analysis of LTE and Wi-Fi Operating in the Same Band. In *Signals, Systems and Computers, 2013 Asilomar Conference on*, pages 1204–1209, Nov 2013.

[56] Panayiotis Papadimitriou, Tero Ihalainen, Heikki Berg, and Klaus Hugl. Link-level Performance of an LTE UE Receiver in Synchronous and Asynchronous Networks. In *WCNC*, pages 3861–3866, 2013.

[57] E. Peh and Y. C. Liang. Optimization for cooperative sensing in cognitive radio networks. In *2007 IEEE Wireless Communications and Networking Conference*, pages 27–32, March 2007.

[58] Guangyu Pei and Thomas R Henderson. Validation of ofdm error rate model in ns-3. Technical report, 2010.

[59] Eldad Perahia and Robert Stacey. *Next Generation Wireless LANs: 802.11N and 802.11Ac*. Cambridge University Press, New York, NY, USA, 2nd edition, 2013.

[60] C. Phillips, D. Sicker, and D. Grunwald. Bounding the error of path loss models. In *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, pages 71–82, May 2011.

[61] J. D. Poston and W. D. Horne. Discontiguous ofdm considerations for dynamic spectrum access in idle tv channels. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pages 607–610, Nov 2005.

[62] John G Proakis and Massoud Salehi. Digital conununicarions, 2007.

[63] H. A. Safavi-Naeini, C. Ghosh, E. Visotsky, R. Ratasuk, and S. Roy. Impact and mitigation of narrow-band radar interference in down-link lte. In *2015 IEEE International Conference on Communications (ICC)*, pages 2644–2649, June 2015.

[64] H. A. Safavi-Naeini, S. Roy, and S. Ashrafi. Spectrum sharing of radar and wi-fi networks: The sensing/throughput tradeoff. *IEEE Transactions on Cognitive Communications and Networking*, 1(4):372–382, Dec 2015.

[65] Frank H. Sanders, John E. Carroll, Geoffrey A. Sanders, and Robert L. Sole. Effects of Radar Interference on LTE Base Station Receiver Performance. Technical Report TR-14-499, NTIA, December 2013.

[66] Austin C Schlick, Aparna Sridhar, Paul Margie, S. Roberts Carter, William B Sullivan, and Danielle J Piñeres. REPLY COMMENTS OF GOOGLE INC. ON THE FURTHER NOTICE OF PROPOSED RULEMAKING, 2014.

[67] Timothy M Schmidl and Donald C Cox. Robust Frequency and Timing Synchronization for OFDM. *Communications, IEEE Transactions on*, 45(12):1613–1621, 1997.

[68] Shabnam Sodagari, Awais Khawar, T Charles Clancy, and Robert McGwier. A Projection Based Approach for Radar and Telecommunication Systems Coexistence. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 5010–5014. IEEE, 2012.

[69] C. Stevenson, G. Chouinard, Zhongding Lei, Wendong Hu, S.J. Shellhammer, and W. Caldwell. IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard. *Communications Magazine, IEEE*, 47(1):130–138, January 2009.

[70] U.S. Department of Commerce. Fast Track Evaluation of the 5350-5470 MHz and 5850-5925 MHz Bands Pursuant to Section 6406(b) of The Middle Class Tax Relief and Job Creation Act of 2012. Technical report, January 2013.

[71] K Wang, M Faulkner, J Singh, and I Tolochko. Timing synchronization for 802.11a wlans under multipath channels. In *Proc. ATNAC*, volume 2004, 2003.

[72] Brad W. Zarikoff and David Weldon. Detection of pulsed radar in a time division duplexed system. In *73rd IEEE Vehicular Technology Conference*, pages 1–5, 2011.