THE UNIVERSITY
of EDINBURGH

Research on Efficiency and Privacy Issues in Wireless Communication

Saravana Manickam Rathinakumar

Doctor of Philosophy

Institute of Computing Systems Architecture
School of Informatics
University of Edinburgh

2018

Abstract

Wireless spectrum is a limited resource that must be used efficiently. It is also a broadcast medium, hence, additional procedures are required to maintain communication over the wireless spectrum private. In this thesis, we investigate three key issues related to efficient use and privacy of wireless spectrum use. First, we propose *GAVEL*, a truthful short-term auction mechanism that enables efficient use of the wireless spectrum through the licensed shared access model. Second, we propose *CPRecycle*, an improved Orthogonal Frequency Division Multiplexing (OFDM) receiver that retrieves useful information from the cyclic prefix for interference mitigation thus improving spectral efficiency. Third and finally, we propose *WiFi Glass*, an attack vector on home WiFi networks to infer private information about home occupants.

First we consider, spectrum auctions. Existing short-term spectrum auctions do not satisfy all the features required for a heterogeneous spectrum market. We discover that this is due to the underlying auction format, the sealed bid auction. We propose GAVEL, a truthful auction mechanism, that is based on the ascending bid auction format, that avoids the pitfalls of existing auction mechanisms that are based on the sealed bid auction format. Using extensive simulations we observe that GAVEL can achieve better performance than existing mechanisms.

Second, we study the use of cyclic prefix in Orthogonal Frequency Division Multiplexing. The cyclic prefix does contain useful information in the presence of interference. We discover that while the signal of interest is redundant in the cyclic prefix, the interference component varies significantly. We use this insight to design CPRecycle, an improved OFDM receiver that is capable of using the information in the cyclic prefix to mitigate various types of interference. It improves spectral efficiency by decoding packets in the presence of interference. CPRecycle require changes to the OFDM receiver and can be deployed in most networks today.

Finally, home WiFi networks are considered private when encryption is enabled using WPA2. However, experiments conducted in real homes, show that the wireless activity on the home network can be used to infer occupancy and activity states such as sleeping and watching television. With this insight, we propose WiFi Glass, an attack vector that can be used to infer occupancy and activity states (limited to three activity classes), using only the passively sniffed WiFi signal from the home environment. Evaluation with real data shows that in most of the cases, only about 15 minutes of sniffed WiFi signal is required to infer private information, highlighting the need for countermeasures.

Acknowledgements

My journey to pursue research in Computer Science started the day I quit Nokia Siemens Networks in 2008. Since then I have had the pleasure of working with some of the smartest people in the world and this thesis would have not been possible without them.

First and foremost, I thank my wife, Ramya, for her steadfast support through the ups and (crazy) downs of this journey for over a decade. From attempting one of the most competitive exams on the planet just to help my chance, to, staying up in the wee hours to proof read my papers, she has done it all. Thank you Jos. I thank my appuchi and ammatha (grandparents), Mr Muthusamy and Mrs Gandhimadhi, for their unwavering belief in me. Appuchi would have been very happy to see me graduate. I thank my mother and father for their support through out the years. Their unrelenting drive to provide a good life for their kids is one of the main reasons I am who I am. I thank my siblings/cousins, Prakash, Nandhini, Vichu, Harish, Vijay, Gayathri and others for their continued love and support. I am lucky to have such a loving family.

I would like to extend my gratitude to Dr Mahesh K. Marina for his support, patience and guidance during the course of my PhD studies. I am truly thankful for his encouragement to be independent and impactful. I am very grateful for the opportunity to work with Dr Bozidar Radunovic at Microsoft Research. Our work on cyclic prefix in OFDM, was instrumental in helping me gain expertise in signal processing and low-level hardware. I thank, Dr Rik Sarkar for many fruitful discussions. His guidance was crucial to the discovery of the effectiveness of the kernel density functions for recycling cyclic prefix in OFDM. I am thankful to my thesis examiners, Dr Oliver Holland and Dr Myungjin Lee for accepting to evaluate the thesis and for helpful suggestions to improve it.

I am fortunate to have worked along side some amazing collegues, Dr Arsham Farshad, Dr Sofia Pediaditaki, Dr Valentin Radu, Dr Paul Patras, Dr Lito Kriara, Dr Bharghava Rajaram, Dr Yota Katsikouli, Xenofon Foukas, Praveen Tammana, Ursula Challita, Arpit Joshi, Dr Cengis Hassan, Mohammed Kaseem, Alex Dawson, Galini Tsoukaneri, Stan Manilov, Chiara Capretti, Rajkarn Singh, and Daniel Licciardello.

Finally, I thank the good people in the Internet who have helped me out in numerous situations. The reddit community is who I turn to in moments of despair and its amazing how experts in almost any subject can be found willing to help there. I also thank the people participating in online forums such as stack exchange without whom a majority of bugs and problems will go unsolved.

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified. Some of the material used in this thesis has been published in the following papers:

Saravana Rathinakumar., Bozidar Radunovic., & Mahesh K. Marina. (2016). *CPRecycle: Recycling Cyclic Prefix for Versatile Interference Mitigation in OFDM based Wireless Systems.* In Proceedings ACM CoNEXT 2016.

Saravana Rathinakumar., & Mahesh K. Marina. (2016). *GAVEL: strategy-proof ascending bid auction for dynamic licensed shared access.* In Proceedings ACM MobiHoc 2016.

Saravana Rathinakumar., Bozidar Radunovic., & Mahesh K. Marina. (2015). *ShiftFFT: An efficient approach to mitigate adjacent channel interference in OFDM systems.* In proceedings of HotWireless workshop at ACM Mobicom 2015.

Saravana Rathinakumar., Mahesh K. Marina., Sofia Pediaditaki., & Maziar Nekovee. (2014). *An iterative and truthful multiunit auction scheme for coordinated sharing of spectrum white spaces.* In Proceedings of NetEcon Workshop at ACM Sigmetrics 2014.

Saravana Manickam Rathinakumar
10 March 2018

To

Ramya
my amazing wife
whose support
has made it possible for me to complete this work

and

Mrs Madura Devi and ***Mr Rathina Kumar***
my beloved parents
for their countless sacrifices

Table of Contents

List of Figures

List of Tables

Acronyms

AE Auto Encoder.

ANN Artificial Neural Networks.

BPSK Binary Phase Shift Keying.

CNN Convolutional Neural Networks.

CP Cyclic Prefix.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

DBL Deep Belief Network.

DL Deep Learning.

FFT Fast Fourier Transform.

ICT Information and Communication Technology.

ISI Inter-symbol Interference.

ISM Industrial Scientific Medical.

LP Linear Programming.

LSA Licensed Shared Access.

LTE Long-Term Evolution.

MAC Medium Access Control.

MCS Modulation and Coding Scheme.

MIMO Multiple Input Multiple Output.

MNO Mobile Network Operator.

OFDM Orthogonal Frequency Multiple Access.

QAM Quadrature Amplitude Modulation.

QoS Quality of Service.

QPSK Quadrature Phase Shift Keying.

ReLu Rectified Linear Unit.

RF Radio Frequency.

RNN Recurrent Neural Network.

SIR Signal to Interference Ratio.

SNR Signal to Noise Ratio.

SSID Service Set Identifier.

VCG Vickrey-Clarke-Groves.

WLAN Wireless Local Area Network.

WPA Wireless Protected Access.

Chapter 1

Introduction

Wireless communication is playing a vital part in the rapid advancement of information and communication technologies (ICT) that has a central role in improving our lives across a multitude of sectors such as healthcare, transportation, and energy efficiency to name a few. Wireless spectrum is a limited resource that needs to be managed efficiently. It is also a broadcast medium where any receiver in the range of the transmitter can receive the signals. In this thesis, we examine three issues involving efficiency and privacy of wireless spectrum use.

First, we consider access mechanisms for the licensed shared access market using short-term spectrum auctions. Auction mechanisms are known to be in use since 500 B.C [3] and are considered an effective market mechanism due to their perceived fairness and efficiency in allocating resources. However, the use of auction mechanism for dynamic short term spectrum sharing is more recent. In 2008, the first truthful auction mechanism, VERITAS [4] was proposed for dynamic short term spectrum sharing. It was based on the sealed-bid auction format where the bidders submit sealed bids to the auctioneer, who determines winners, as well as the winning prices. It was the first auction for dynamic short-term spectrum auctions that achieved truthfulness as a dominant strategy for bidders. However, since then, several problems, such as lack of channel sharing and problem with rogue auctioneers, have been uncovered [5, 6], and numerous auction mechanism have been proposed [7, 8] to solve some of these problems. Even so, a qualitative comparison of these truthful short-term spectrum auctions reveal that only some of the concerns with VERITAS have been addressed in these mechanisms that intend to replace VERITAS. A key common feature between these auction mechanisms is that, they are all based on the sealed-bid auction format.

An in-depth analysis of these auction mechanisms reveals a surprising insight.

Most of these problems associated with short-term dynamic spectrum auctions can be attributed to the underlying auction format which these auction mechanisms are based on, *the sealed-bid auction* format, and not due to the winner and price determination schemes of these auction mechanisms. Furthermore, the sealed-bid auction format is only one among many auction formats such as english auctions (also known as open ascending price auctions), dutch auctions (open descending price), and the Vickery auction format (second price auction). We find that the application of ascending-bid auction format to short-term spectrum auctions does not suffer from the same problems as existing short-term auction mechanisms that are based on the sealed-bid auction format. With this insight, we design GAVEL, a truthful short-term auction mechanism for the LSA model. Simulation results using real world data of the geo-locations of over 2000 houses, show that GAVEL has a better performance than existing mechanisms, in terms of revenue for the auctioneer, spectrum utilisation and number of winners.

Second, we consider the use of cyclic prefix in OFDM systems. Orthogonal Frequency Division Multiplexing is the most commonly used modulation scheme for wide-band communication. OFDM suffers from inter-symbol interference in a dispersive channel and a guard interval (between successive frames) equal to the dispersion time of the channel during which no energy is transmitted is the simplest solution. In 1980, Peled and Ruis [9], proposed the use of the cyclic prefix to be transmitted during the guard interval [10]. The cyclic prefix is a repetition of the last part of the transmitted frame during the interval at the beginning of that frame. At the receiver, this cyclic prefix is not used since it only contains redundant information (a copy of the last part of the frame), resulting in a significant reduction in spectrum utilisation. In WiFi, for instance, the duration of the cyclic prefix is 0.8μS from a data frame of 3.2μS, in other words, around 20% of the frame duration is allocated for the cyclic prefix, which results in a significant overhead. However, in the presence of interference, the utility of cyclic prefix increases.

We discovered that while the cyclic prefix carries only redundant information about the signal of interest, it carries unique information about the interference in the environment. In other words, we observe that the signal carried in the cyclic prefix is affected by different levels of interference when compared to the signal carried in the later part of the frame. Using this key insight, we propose CPRecycle, an improved OFDM receiver, that instead of discarding the cyclic prefix, exploits the redundant information to mitigate several types of interference that occur commonly in current popular deployment scenarios such as homes and public access points. Using USRPs

and off-the-shelf IEEE 802.11 access points, we demonstrate that CPRecycle can be used to mitigate both adjacent channel interference and co-channel interference. In contrast to several other interference mitigation schemes, the key advantage of CPRecycle is that it only requires modifications at the receiver and does not requires any changes to the protocol or the transmitter. Hence it can be supported on devices that are in use today such as smart phones and laptops.

Third, we consider the privacy of encrypted home WiFi networks. The latest IEEE 802.11ac standard can achieve about 500 Mbps per stream throughput and the latest consumer WiFi access points can support multi-input multi-output (MIMO) with up to eight spatial streams, while occupying 120 MHz of wireless spectrum. This can enable the latest WiFi routers to achieve a throughput of more than 1 Gbps [11], which can be useful to support the growing number of WiFi enabled devices that demand a high data rate such as smart 4K televisions (requires about 32 Mbps for compressed 4K video) and wireless storage (about 500 Mbps) devices used for backup. However, wireless networks are also more prone to several attacks due to the inherent broadcast nature of the medium. Traditionally, this has been solved with the use of encryption, however, not every part of the communication is encrypted, for instance the management frames. Also, the size preserving encryption mechanisms in WiFi reveal traffic characteristics of the network.

In this chapter, we explore the possibility of inferring private information from passively sniffed WiFi signal from a home environment. We observe, using manual analysis, with data collected from three homes in the UK, that private information such as occupancy status of the home and activities of home occupants can be inferred. With this insight, we propose WiFi Glass, a deep learning technique that can be used to infer private information about home occupants using passively sniffed WiFi signal data. Evaluation of WiFi Glass using real data shows that it can determine occupancy status of a home and some activities (sleeping, watching television), with high accuracy. In most cases, a rogue agent will only need to record the WiFi traffic in the home environment for about 15 minutes, highlighting the need to develop countermeasures.

Chapter 2

Short-term Spectrum Auctions

2.1 Spectrum auctions for licensed shared access

Mobile data traffic has been experiencing dramatic growth in the past several years and this growth trend is expected to continue for the foreseeable future. Making more spectrum available is an obvious mechanism to cope with this growing demand. However opportunities for clearing spectrum below 6 GHz, where most mobile networks operate currently and will continue to do so in future, to create new bands for licensed exclusive use by mobile network operators (MNOs) are dwindling. However MNOs prefer licensed spectrum as it offers interference protection and lets them develop services that provide guaranteed quality of service (QoS).

Licensed Shared Access (LSA) [12] has emerged as a new shared spectrum access model that can unlock substantial amount of licensed spectrum below 6 GHz held by incumbents not concerned with civilian wireless and mobile data communication and enable more efficient use of such spectrum bands. LSA framework allows incumbents to authorise other users (e.g., MNOs) to access all or part of the spectrum licensed to them at designated times and in designated locations as per the sharing rules agreed between them and mediated by the national regulator. From a MNO perspective, LSA model opens up new spectrum bands for use that are qualitatively similar to licensed spectrum to offer guaranteed QoS. While the current LSA use cases reflect relatively longer term authorisation of incumbent spectrum to LSA licensees in the order of a few years, it is believed that we will be heading to a future with a dynamic LSA model that features short-term and fine-grained spectrum sharing [13], and potentially involving new operators and business models [14].

Dynamic spectrum auctions can help address the aforementioned issues with LSA

spectrum. In general, auctions are an effective market mechanism due to their perceived fairness and efficiency in allocating resources. All the bidders have equal opportunity to win and the resources are sold to bidders who value them the most. In the LSA context, auctions have two main advantages: (i) They allow dynamic allocation of spectrum for short time periods and also even sharing at a fine-grained channel level as opposed to the static allocation of spectrum over long periods usually spanning years; (ii) They create incentives for the incumbents to participate in the auction, leading to more spectrum availability in the market. When used to coordinate spectrum sharing among LSA licensees, a suitable auction mechanism should be able to support heterogeneous spectrum bands and channels as the LSA spectrum as a whole is expected to be fragmented across different parts of the spectrum with widely different propagation characteristics. In practise, some auction scenarios may require regulatory enforcement to ensure that all bidders may have equal opportunity for the channels. For examples, in cases where the seller would value the channels based on the buyer as they may be competitors. However, for our study, we assume that all bidders would have equal opportunity to buy the channel and the valuations are buyer independent.

This chapter is organised as follows. First, an introduction to spectrum auctions is presented in Section 2.2, followed by a survey of existing spectrum auction mechanisms. We discuss the importance of the underlying auction mechanism and identify that sealed-bid auction format could be the underlying reasons for complexities in short-term spectrum auctions in Section 2.4. In Section 2.5, we propose, GAVEL, a strategy-proof short term spectrum auction based on the ascending-bid auction format. Using an example, we describe GAVEL and highlight its key properties in Section 2.5.2. The proofs for several properties of GAVEL are presented in Section 2.5.4, followed by evaluations with real life data in Section 2.6.

2.2 Introduction to Auctions

An auction is a process via which a seller (or auctioneer) offers goods to a set of buyers (or bidders), collects the bids and allocates the items based on competition. This process involves a set of trading rules for resource allocation and pricing, which, in the traditional scenarios where only a single item is offered, define four basic types of auctions [15]: the *English auction*, the *Dutch auction*, the *first-price sealed-bid auction*, and the *second-price sealed-bid auction*.

The *English auction* (also known as open, oral, or ascending-bid auction) is the

most widely used type of auction. In this type, each bid is higher than the previous one and the current highest bid is always known to the bidders. The price of the item is either announced by the auctioneer or the bidders themselves. The auction ends when no bidder wishes to bid further. The item is then sold to the buyer with the highest bid. The *Dutch auction* (also known as descending-bid auction) is the opposite of the English auction. Specifically, the auctioneer announces an initial high price and lowers the price until one bidder accepts. The winner pays the last announced price. In the *first-price sealed-bid* auction potential buyers submit sealed bids and no buyer knows the bid of its opponent. The item is sold to the buyer who places the highest bid. The winner then pays the amount she bid. Different from the English auction, in this type, buyers can only bid once, thus they cannot observe their opponents' bids and accordingly change their decisions. Similarly to the first-price sealed-bid auction, in the *second-price sealed-bid auction* (also known as Vickrey auction), each buyer places a sealed bid independently of its rivals and the winner is the buyer with the highest bid. The amount the winner pays, however, is the bid of the second highest bidder (i.e., the bidder who would win the item if the current winner had not placed a bid).

In a more complicated version, multiple items are sold simultaneously. These auctions, called *combinatorial auctions*, enable buyers to bid on bundles of items rather than individual items [16,17]. In this auction type, however, due to the large number of possible combinations, bidding and winner determination becomes a challenge. Buyers need a way to express their bids for every possible set of items and given the set of all possible bids from every bidder, the seller needs to compute the allocation that optimises some function – usually the obtained revenue. This optimisation problem, however, has been shown to be NP-complete [16].

2.3 Existing Auction Mechanisms

Existing schemes do not satisfy all the properties that are of interest to enable spectrum sharing in a dynamic LSA context. Since the first truthful short-term spectrum auction, VERITAS [4] was proposed, issues such as privacy protection, heterogeneous channels and false-name bids have been uncovered. Some of these issues have been addressed in subsequent works [5, 8, 19, 28, 29, 31], although, they require increasingly complex adaptations to the auction scheme.

The existing auctions for the short-term spectrum market, are based on the sealed

Table 2.1: GAVEL compared with existing auction schemes

Auction Scheme	Strategy-proof	Hetero Spectrum	Fine Grained Channels	Privacy Protection
VERITAS [4]	✓	✗	✗	✗
PROMISE [18]	✓	✗	✗	✗
TRUST [19]	✓	✗	✗	✗
ADAPTIVE [20]	✓	✗	✗	✗
ALETHEIA [21]	✓	✗	✗	✗
PPer [22]	✗	✗	✗	✓
DEAR [23]	✗	✗	✗	✓
PPS [24]	✓	✗	✗	✓
SPRING [25]	✓	✗	✗	✓
SATYA [26]	✓	✗	✓	✗
KAS [27]	✓	✗	✓	✗
SMASHER [8]	✓	✓	✓	✗
$\prod$ [28]	✓	✓	✗	✗
TAMES [29]	✓	✓	✗	✗
LOTUS [30]	✓	✓	✗	✗
TAHES [5]	✓	✓	✗	✗
AEGIS [31]	✓	✓	✗	✗
GAVEL (This Paper)	✓	✓	✓	✓

bid auction format. We discuss them with respect to support for the desirable properties outlined in the previous section: heterogeneous spectrum, fine-grained channels, privacy protection, rich bidding language, and false-name bids. Looking into each of these issues we observe that they can all be attributed to the behavioural characteristics of the underlying auction framework: the sealed bid auction.

Heterogeneous Spectrum: When the market has heterogeneous spectrum, it leads to additional design challenges in the auction mechanism. Bidders would have different valuations for different types of spectrum and may need to submit a different bid for these different bands of spectrum, hence the need for bid diversity. Existing auction schemes [4, 19] mostly treat spectrum as identical objects and apply the same conflict graph for different spectrum while considering spectrum reuse. Some recent works [5, 8, 28, 29, 31] have considered spectrum heterogeneity with increasingly complex winner and price determination schemes. However these mechanisms are do not protect the bid information from the auctioneer and also do not support sharing among interfering users.

In sealed bid auction format, the market clearing price determination involves identifying the critical neighbour for each channel a bidder wins. The critical neighbour is the bidder with the highest losing bid. The difficulty in providing support for heterogeneous spectrum is primarily due to the additional complexity in identifying the critical

neighbour to determine the opportunity cost for each channel independently. The conflict graph is different and hence each bidder may have a different set of interfering neighbours for each channel.

Fine-grained Channels: Most existing auction schemes preclude shared use among interfering users and the allocations ensure no interference between winners. Gandhi et al. [32] propose an auction framework to distribute spectrum based on dynamic demand in real-time. This auction scheme supports only exclusive access but can be adapted to share spectrum at a fine granularity. While it can be applied to share spectrum among neighboring users who want a portion of the spectrum, it lacks some desired properties such as truthfulness and bid diversity. The auction scheme proposed by Kasbekar et al. [27] can be adapted to enable shared use among neighbors. However, they do not support heterogeneous channels and instead of a structured bidding language, the bidders are allowed to express arbitrary externalities, making the approach intractable. Kash et al. [26] propose SATYA, a truthful auction scheme for spectrum sharing that uses bucketing and ironing of bids to maintain monotonicity for truthfulness. While this is the first scheme to support channel sharing, it has a few drawbacks. Firstly, it does not support bid diversity. Secondly, it has an exponential run time and is only polynomial under some restrictions. Finally, it does not support heterogeneous spectrum and assumes that the conflict graph is constant across the spectrum.

Similar to the heterogeneous spectrum, supporting fine-grained channels requires complex price and winner determination strategy. This is again due to the additional complexity in identifying a critical neighbour when multiple interfering bidders can win the same channel. Satya [26], for example, uses a complex scheme involving bucketing and ironing of bids to determine winners which enables fine-grained channels, but at the cost of lacking support for heterogeneous channels among other properties.

Privacy Protection: An insincere auctioneer can leverage the bid information to its own advantage [33]. Recently, a few auction schemes [22–25] that provide bid privacy have been proposed for dynamic spectrum allocation. Huang et al. [24] propose PPS, a strategy proof auction scheme that protects bid information from the auctioneer using Paillier's cryptosystem. However, it lacks in several necessary properties such as bid diversity and support for heterogeneous channels. Ming et al. [22] propose PPER, an auction scheme that guarantees bid privacy and economic-robustness using the reverse simplex method that enables the LP problem to be solved in a distributed fashion. However, the scheme is not strategy-proof and assumes that all channels are homoge-

neous. Zhu et al. [23] proposed DEAR, which protects the bid privacy with the use of cryptography tools. It is a single price auction where all the winners are expected to pay the same price. Huang et al. [25] proposed SPRING, a strategy-proof auction scheme that uses asymmetric key encryption to protect the bid information from the auctioneer. However, a bidder can bid for only one channel, which severely limits its use.

In sealed bid auction schemes, the auctioneer receives the bids from all the bidders and is the only entity in the auction to have all the information. This information bias can be avoided by encrypting the bids from the auctioneers. However, encrypting the bid information from the auctioneer also leads to the limitations in these privacy protecting auction schemes as discussed above.

False-name Bids: A rogue bidder can submit multiple bids from fictitious bidders to improve its utility and affecting the revenue for the auctioneer. This problem identified by Wang et al [21], is shown to reduce the revenue for the auctioneer by about 40% in some cases. To counter false-name bids they propose ALETHEIA [21], a false-name proof auction for short-term dynamic spectrum access. In ALETHIA, the prices of bidders are computed first, based on which the winners are then determined. For each bidder, a critical neighbour is identified such that a group of channels are priced the same as the sum of the individual channels prices. However, its designed on the basis that all channels are substitutes and hence does not support heterogeneous channels. It also does not support bid diversity, privacy protection and fine-grained channels.

In this cheating technique, a rouge bidder exploits the auctioneer's need to identify the critical neighbour for winner and clearing price determination. By creating a fictitious bidder in the neighbourhood the bidder can manipulate this critical neighbour determination process and hence this vulnerability is common to all the sealed-bid short term auctions. To prevent the manipulation of the critical neighbour identification process, ALETHIA uses a different winner and price determination strategy that only works for homogeneous spectrum.

Rich Bidding Language: The bidding language which is used by the bidders to submit their bids, should provide the ability for bidders to express their preference for substitute and complementary channels. The fundamental problem is that the existing auction mechanisms support either substitutes or complementary channels in the market but not both. Auction mechanisms for homogeneous spectrum [4, 18, 21, 22] assume all channels in the market are substitutes, while auctions for heterogeneous

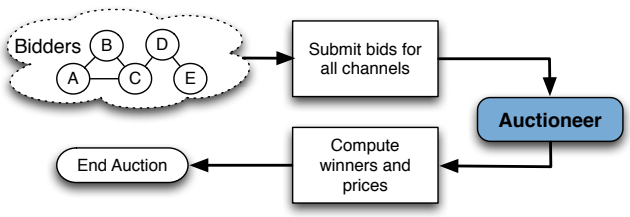

Figure 2.1: Sealed-bid auction format

spectrum [5, 29–31] assume all channels are complementary. However in a dynamic LSA context, the market for heterogeneous spectrum would consist of both substitutes and complementary channels. For example, channels in the 3.6-4.2 GHz band could be considered substitutes, where as channels in 3.6-4.2GHz are considered complementary to channels in the 2.3-2.4 GHz band.

This problem is common to sealed bid auctions where the bidders express their bids for all the channels simultaneously without being able to express package preferences. Providing such a bidding language would require a complex winner and price determination strategy, not to mention the overhead for the bidders in computing bids for all such possible combination of channels.

Table 2.1 qualitatively compares our proposed auction mechanism, GAVEL, with existing schemes in terms of being strategy-proof and satisfying the above mentioned properties.

2.4 Choice of Auction Format

The choice of the auction format is a key decision in auction design. The sealed bid and ascending bid [34] auctions are two competing auction formats that can both identify the minimum Walrasian equilibrium prices and enable truthful bidding. In the sealed bid auction format, shown in Fig. 2.1, the bidders submit their bids for channels to the auctioneer, who then computes the outcome (winners and clearing price) in one shot. In the ascending bid auction framework, shown in Fig. 2.4, the bidders (through a proxy agent) gradually submit their demand set to the auctioneer at increasing prices over multiple rounds until all the demands are met. Hence the outcome is incrementally computed in each round unlike in a sealed bid auction. While they have theoretically equivalent outcomes, these behavioural differences influence the effectiveness of the auction schemes in practice [35, 36].

In applying the sealed bid and ascending bid auction formats to short term spectrum auctions, there are two primary behavioural differences that affect the effectiveness of the auction formats, (i) Information Bias (ii) Critical Neighbour identification, as shown in Fig. 2.2.

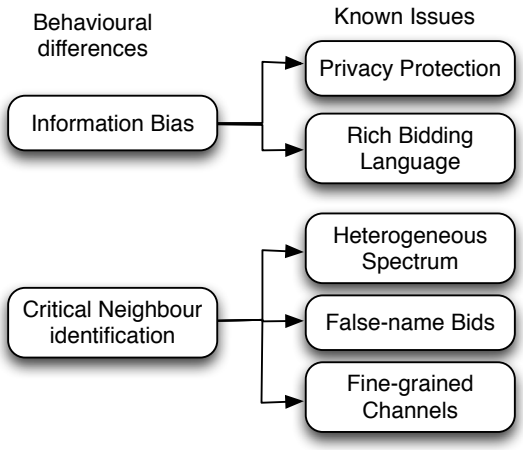

Figure 2.2: Behavioural differences and related issues

Information Bias: The information exchanged among the bidders and the auctioneer play a critical role in the effectiveness of the auction. In the sealed bid auction format, the bid information is not shared among the bidders. The auctioneer is the only entity with access to all the bids. This information bias leads to two problems. First, lack of bid privacy protection: the auction is now vulnerable to an insincere auctioneer who could create a false second highest bid to increase its revenue at the cost of the winning bidder. Second, enough information is not shared during the auction process to enable bidders to react to price changes or for market price discovery.

Whereas in the ascending bid format, the right amount of information is shared during the auction process. The demand set can be inferred by all the bidders during the auction process with increasing prices and the auction for an item ends at the market clearing price. This protects against an insincere auctioneer since the auctioneer does not have access to the highest bid as the auction ends at the second highest price. The information from the demand set can enable the bidders to react to price changes and for market price discovery. Ascending bid auctions also have the additional advantage of being transparent which can positively influence the bidding behaviour while simplifying the bidding strategy.

Critical Neighbour identification: In sealed bid auction framework, the winner and price determination involves identifying a unique critical neighbour for each win-

ner and channel in such a manner than the auction mechanism is strategy proof. This process gets increasingly complex with additional constraints such as support for heterogeneous channels, bid diversity, and fine-grained channels. Also, the need to identify a critical neighbour for determining market clearing price, can result in an auction scheme that is not strategy proof using cheating techniques such as false name bids.

In ascending bid auctions, there is no need to identify a critical neighbour since the price at which the demands can be met is the market clearing price. Hence, the complexity of winner and price determination algorithm does not increase with additional constraints. For the same reason, the auction mechanism also protects against cheating techniques such as false name bids.

Considering these behavioural differences and as an alternative to the existing auction schemes we propose, GAVEL, a truthful auction mechanism that is based on the ascending bid format for a dynamic short-term spectrum auctions.

2.4.1 Design Objectives

We discuss the set of design properties we aim to achieve in the proposed auction scheme.

(i) *Individual Rationality*: The clearing price for the bidder should not be more than its bid, (ii) *Strategy-proof*: The best strategy for a bidder should be to bid truthfully. This eliminates the possibility of bidding strategies that can affect the outcome of the auction, to prevent market manipulations and ensure fairness.

(iii) *Privacy preserving*: Protect the highest bid information from the auctioneer. This is to prevent the auctioneer from exploiting the bid information to its advantage.

(iv) *Computationally efficient*: The outcome of the auction can be computed in polynomial time. This is essential for short term online auctions.

(v) *Social Welfare*: The sum of valuations of the auction winners. This is the primary objective of the auction scheme.

(vi) *Revenue*: The total payment from all the winners of the auction. While this is not our primary goal, revenue generation serves as an incentive for the incumbents to share their spectrum with the LSA licensees.

(vii) *Spectrum Utilisation*: A unique feature in spectrum auctions, the spectrum reuse should be maximised by selling it to as many bidders as possible while satisfying their requirements (proportion of channel share).

(viii) *Shared Use and Exclusive Use*: Bidders should be able to bid for a percentage

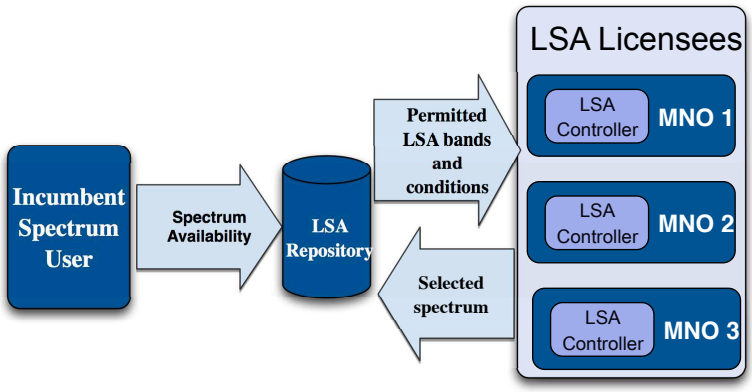

Figure 2.3: Licensed Shared Access (LSA) Framework Illustrated.

of time to use a spectrum as well as for exclusive use. This reduces the entry barrier and improves efficiency of spectrum use among users with bursty traffic.

(ix) *Spectrum Heterogeneity*: This comes from both spatial and frequency heterogeneity. With frequency heterogeneity, the conflict graph varies between spectrum bands due to varying propagation characteristics. Hence, the set of bidders who are allowed to reuse the channel changes with every band. Due to spatial heterogeneity, the same set of channels are not available for all the bidders.

(x) *Bid Diversity*: An operator may bid for different spectrum for more than one communication device or have multiple radios and should be able to express diverse demands

2.5 GAVEL

2.5.1 LSA Model

Licensed Shared Access (LSA) [12] is a new shared spectrum access framework that allows one or more LSA licensees to access the spectrum that has already been allocated to an incumbent. This framework has been designed to serve the short-term to mid-term needs through a quasi-static allocation of shared spectrum to LSA licensees. Each licensees conform to certain sharing rules included in their rights to use the spectrum. During the period when the license is active, the incumbent forfeits the spectrum access right to the LSA licensees. This enables both the incumbent and LSA licensees to guarantee a certain QoS since the resources are now guaranteed.

The LSA framework consists of four main entities, *the incumbents, LSA reposi-*

Table 2.2: Notations used in this chapter

Notation	Description
t	round index
C_k	Channel k
$p_t^{C_k}$	Price for channel C_k at round t
$V_i^{C_k}$	Valuation for channel C_k by bidder i
$d_i^{C_k}$	Demand from bidder i for channel C_k
$e_i^{C_k}$	Portion of channel C_k available for bidder i
$a_i^{C_k}$	Portion of channel C_k allocated to bidder i

tory, LSA controller and the *LSA licensees* shown in Fig. 2.3. The *incumbent* is the spectrum owner, who own long term licenses for exclusive access to a spectrum band (e.g., 3.5GHz band in US and 2.3GHz band in Europe). Incumbents propose sharing agreements that could define, temporal, geographical, and power level constraints, so as to protect themselves from interference. The *LSA repository* is a database which receives from the incumbents the pieces of spectrum in terms of space, time and frequency that are available for sharing along with the conditions they are subject to. The *LSA Controller* is responsible for managing access to the shared spectrum that has been made available to the *LSA licensees* based on the sharing rules and incumbent usage provided by the LSA repository. While the LSA framework has a broader scope, where each LSA controller can interface with more than one LSA repository as well as with multiple LSA licensee networks that use different technologies, we focus on a simpler and concrete scenario where there exists one LSA controller per licensee (a MNO). *LTE-A* supports carrier aggregation and can aggregate spectrum across different bands. It is conceivable that LTE can use carrier aggregation to leverage the spectrum available under LSA.

The basis for our proposal, `GAVEL`, is the ascending-bid auction mechanism proposed by Ausubel [37], that is shown to be efficient and also replicates the outcome of a VCG auction. But Ausubel's mechanism [37] is not intended for dynamic spectrum sharing. As such they do not account for any of the unique characteristics associated with the dynamic spectrum allocation in general and the LSA model in particular. Spatial reuse, which allows multiple users to be allocated the same channel provided they do not interfere with each other, is one such characteristic. Heterogeneous spectrum discussed in Section. 2.3 is another characteristic. Fine-grained channel sharing among interfering neighbours is yet another characteristic that needs to be supported. The overall architecture of the system based on our proposed auction mechanism `GAVEL` is

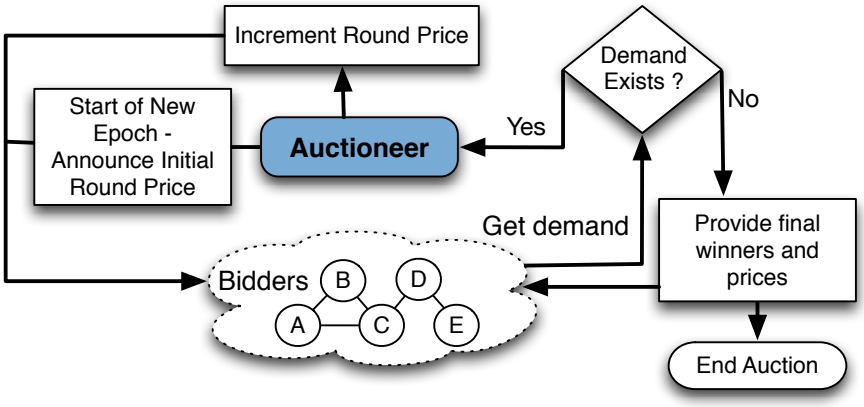

Figure 2.4: System architecture with GAVEL

Table 2.3: GAVEL Illustration: Price and Demand Vector over different rounds

Round	**Price Vector**	**A**	**B**	**C**	**D**	E	Action
1	(1,1,1)	(0.6,1,0.5)	(0.3,0.4,0)	(1,0.4,0.2)	(0,0.2,1)	(0,1,0.5)	Ch 3 credited to A
2	(4,6,3)	(0.6,1,0.5)	(0.3,0.4,0)	(0,0.4,0.2)	(0,0,1)	(0,1,0.5)	Ch 1 to A and B, Ch 2 to E
3	(4,8,8)	(0.6,0,0)	(0.3,0.4,0)	(0,0.4,0)	(0,0,1)	(0,1,0.5)	Ch 2 credited to bidders B and C
4	(4,8,10)	(0.6,0,0)	(0.3,0.4,0)	(0,0.4,0)	(0,0,1)	(0,1,0)	Ch 3 credited to bidder D

shown in Fig. 2.4.

The timeline for the system in operation is seen as a sequence of *epochs*, each consisting of a short *Auction Phase* followed by a much longer *Spectrum Use Phase*. The definition of an epoch is typically a few hours depending on the use case. Each *Auction Phase* consists of one or more *rounds* involving interaction between the auctioneer (LSA Repository) and bidders (could be multiple per LSA Licensee) as part of the auction to meet the spectrum demand of the bidders subject to their valuations, spectrum availability and mutual conflicts. The bidders interaction with the auctioneer can be managed using a proxy agent.

At the beginning of auction phase, the auctioneer announces the initial price, i.e. the *reserve price*. It then waits for a *bidding period* to receive demands from the bidders at that price. Depending on the demands, the auctioneer may allocate one or more channels to some of the bidders at the current round price. The auction then may also proceed to another round by increasing the reserve price to bring down excess demand. This process may continue over several rounds until there there is no more demand to be fulfilled. At the end of the auction phase, bidders whose bids are successful, pro-

ceed to use the spectrum they won in the following Spectrum Use phase subject to the sharing conditions, until the end of that epoch. This process repeats in the next epoch and so on.

We now describe GAVEL. Referring to Fig. 2.4, at the beginning of an epoch (round $t = 1$), the auctioneer announces a reserve price vector $p_1 = (p_1^{C_1}, p_1^{C_2}, \ldots, p_1^{C_m})$ for the channels, and the bidders respond with the demand vector $D_i(t) = (d_i^{C_1}(t), d_i^{C_2}(t), \ldots, d_i^{C_m}(t))$ where $0 < d_i^{C_k}(t) \leq e_i^{C_k}$ is the portion of channel C_k that bidder i desires at price $p_1^{C_1}$ from what is available for use $e_i^{C_k}$. If a bidder desires exclusive use of a channel then its demand would be 1. The round price controls the demand from each bidder in the sense that the decision to bid for a channel is determined by the number of channels within its private valuations. Only the channels that have higher valuations than the current round price would be in demand from the bidder. This channel has to be available for the bidder to use which is determined by the LSA Controller with information from the LSA Repository.

$$\forall i \in \mathbb{N},\ \forall C_k \in \mathbb{C} \quad \forall t \geq 1 \quad d_i^{C_k}(t) \in \{0, d_i^{C_k}(1)\} \tag{2.1}$$

At each round t with price vector p_t, for channel $C_k \in \mathbb{C}$, the auctioneer determines if for any bidder i the aggregate demand of bidder i's neighbours in the conflict graph $\mathcal{G}_{C_k}$ is low enough to satisfy i demand. If so, $d_i^{C_k}$ the portion of channel C_k demanded by bidder i is credited to the bidder. Otherwise, any portion of channel C_k allocated to bidder i is debited from the bidder, which can be written as,

$$a_i^{C_k} = \begin{cases} d_i^{C_k}, & \text{if } \sum\limits_{j \in N_i \cup i} d_j^{C_k}(t) < 1. \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

Appropriately, the current round price $p_t^{C_k}$ for channel C_k is added or subtracted from $W_i^{C_k}$, the total price to be paid by the bidder at the end of the auction.

The above process repeats with increasing round prices until there is no demand from the bidders. The channels won by the bidders are now assigned to them and removed from their list of available spectrum. In order to prevent the neighbours from rebidding for the channels that they cannot use (because one of its neighbours already won the channel), we remove these channels from the neighbours availability list as well. All the bidders that won channel C_k are no longer treated as active players in the auction scheme for channel C_k. The round price is now reset to the spectrum reserve price and the multi-round auction process is repeated until there is no demand for

channels at the reserve price.

Note that to allow for spatial reuse, we view only the neighbours of a node in the conflict graph as its competing bidders. For example in the conflict graph shown in Fig. 2.5 A competes with B and C in the auction; C competes with A, B and D; and E competes only with D. This is unlike the classical VCG auction or Ausubel's mechanism where all bidders compete with each other.

2.5.2 An Example

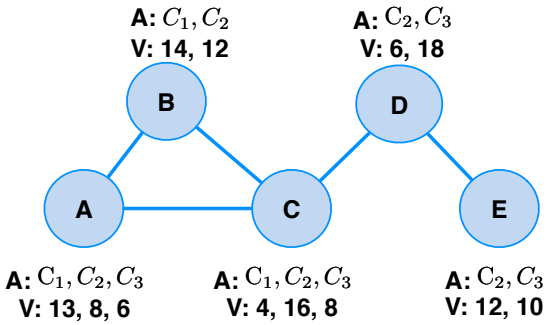

Figure 2.5: Auction Example: Graph showing conflict between five bidders with the channels available for use (A:) and private values of those channels (V:)

We now illustrate the working of the GAVEL auction mechanism for the example in Fig. 2.5. For simplicity we assume the bidders demand for channels are independent and static, i.e. their demand for one channel does not influence their demand for another. Note that in Fig. 2.5(a), the set of channels available at each LSA licensee with "A:". As a specific example, bidder A has three channels available (1, 2 and 3). A fraction of the channel is assigned to a bidder only if the LSA controller identifies if its available for use to the bidder. In this particular scenario, the demand is high with all the bidders desiring for (a fraction of) every channel available to them. The price vector announced by the auctioneer at different rounds and demand vector of bidders at different rounds in the auction scheme are shown in Table 2.3. The demand vector of bidders shown at round 1, are the fractions of channels required by the bidders.

In the first round of the auction with price $p_1 = (1, 1, 1)$, the auctioneer sets a reserve price of 1 for channels 1, 2, and 3. The five bidders A, B, C, D, and E bid for fractions of channels based on their demand (as they have higher valuations than the current round price). For instance, bidder A has a demand of 60% of channel C_1, exclusive use of channel C_2 and 50% of channel C_3. Note that at bidder A,

$$\sum_{j \in N_A \cup A} d_j^{C_3}(p_1) = d_A^{C_3} + d_B^{C_3} + d_C^{C_3} = 0.7 < 1,$$

so bidder A is credited with channel 3. Since there is excess demand, the auction proceeds to subsequent rounds with the price getting incremented at each round. At price vector $p = (4,6,3)$, at bidder E,

$$\sum_{j \in N_E \cup E} d_j^{C_2}(p_2) = d_E^{C_2} + d_D^{C_2} = 1 \leq 1.$$

Since the cumulative demand from E's neighbours show no competition, ie, at this point in the auction, E is guaranteed to win channel 2. Similarly, bidder C does not have demand for channel C_1 anymore, so bidders A and B win channel 1 to be shared between them at 60% and 30% respectively. At price vector $p = (4,8,8)$, bidder A loses interest in channel C_2, and bidder C has no more demand for C_3. So, B and C are credited channel 2 at price 8. Finally, at $p = (4,8,10)$, the market clears with bidder A winning channels C_1 and C_3, bidder B winning C_1 and C_2, bidders C, D, and E winning channels C_2, C_3 and C_2 respectively.

It can be clearly seen from the above example that the result of the auction is efficient: the auction has allocated the channels to the bidders who value them the most. The formal proof is provided in section 2.5.4. It can also be seen that the resultant pricing for channels won is equivalent to that of a VCG auction. For example, bidder A wins channel C_3 at the reserve price and channel C_1 at the opportunity cost ($p^{C_1} = 4$) of bidder C. Similarly, bidder B wins C_2 channel at the highest losing bid ($p = 8$) amongst its neighbours and so on.

It can be easily seen from the auction design that GAVEL satisfies the final three objectives. *Shared Use and Exclusive Use*: bidders can submit a demand $0 < d_i^{C_k} < 1$ for shared use and $d_i^{C_k} = 1$ for exclusive use. *Spectrum Heterogeneity*: GAVEL maintains a graph $\mathcal{G}_{C_k}$ for each channel C_k and the winners are computed independently for each channel. *Bid Diversity*: GAVEL allows demands $d_i^{C_k}$ for all channel $C_k \in \mathbb{C}$ and computes clearing prices for each channel independently.

2.5.3 GAVEL algorithm

Computation Complexity: `GAVEL` runs in O(NMR), where, N, M and R are the number of bidders, number of channels, and the number of rounds respectively. In each auction round, the neighbourhood demand is checked for each bidder and for each channel to enable the channel credit/debit process (NM). In practise, the values of both M and R are also quite small, further enabling the use of GAVEL in an online scenario.

Input: $\forall C_k \in \mathbb{C}$ $\mathcal{G}_{C_k}$, $\mathcal{E}_{C_k}$, Price Vector P

Output: $\forall i \in \mathbb{N}$ Channel allocation A_i

and Price to be paid W_i

$t \leftarrow 1$

while *True* **do**

  $D(t) \leftarrow$ GetDemandsFromBidders($P(t)$)

  for $i \in N$ **do**

    for $(C_k \in \mathbb{C})$ **do**

      Otherwise

      if $\sum_{j \in N_i \cup i} d_j^{C_k}(t) \leq 1$ **then**

        If channel C_k is newly allocated in this round then it is credited to bidder i and the price is adjusted

        if $a_i^{C_k} = 0$ **then**

          $a_i^{C_k} \leftarrow d_i^{C_k}(t)$; $W_i^{C_k} \leftarrow p_i^{C_k}(t)$

        end

      end

      If bidder i's demand for channel C_k cannot be satisfied anymore then it is debited from bidder i

      if $\sum_{j \in N_i \cup i} d_j^{C_k}(t) > 1$ **then**

        If channel C_k is not available for bidder i in this round then its debited and the price is adjusted

        if $a_i^{C_k} > 0$ **then**

          $a_i^{C_k} \leftarrow 0$; $W_i^{C_k} \leftarrow 0$

        end

      end

    end

    $t \leftarrow t + 1$

    if $(\forall i \in \mathbb{N} \quad D_i(t) = 0)$ **then**

      if $(t = 1)$ **then**

        Exit Auction

      end

      if $(t > 1)$ **then**

        Debit $a_i^{C_k}$ from existence vector $\mathcal{E}$ of winning bidders and their neighbours i, for all channels $C_k \in \mathbb{C}$

        $t \leftarrow 1$

      end

    end

  end

end

Algorithm 1: GAVEL Auction Scheme

2.5.4 Proof of Auction Properties

THEOREM 2.5.1. *GAVEL is truthful.*

Proof. In order to prove that an auction mechanism is truthful, we need to show: (i) the pricing function does not depend on the bid of the winning bidder; and (ii) it is monotonic, i.e. if bidder i wins a channel at bid p then he will win the channel at any bid $p^* > p$.

It is indeed the case that pricing function in GAVEL does not depend on the bid of the winning bidder. In any given round, whether a channel is won by a bidder i is not dependant on i's demand but instead on the cumulative demand of i's conflicting neighbours. Even more crucially, the price that i needs to pay for the channels it is credited in round t is the round price p_t, which does not have any relation with i's bid.

Now to the monotonicity. Assume bidder i wins a channel at price p_t at round t and at any of its subsequent rounds $t* > t$, the cumulative demand of i's neighbours $\sum_{j \in N_{-i}} d_j^{C_k}(t) \geq \sum_{j \in N_{-i}} d_j^{C_k}(t*)$. The only way bidder i cannot win the channel at higher price p^* is if the aggregate demand of i's neighbours increases with the bid p^*. This is not possible since we have assumed that the demand vectors are weakly decreasing with higher round prices, which results in a monotonically non-increasing demand for each channel with each new round. Thus i will always win the channel at any bid $p^* > p$.

Therefore, GAVEL is a truthful mechanism.

□

THEOREM 2.5.2. *GAVEL protects against the frauds of an insincere auctioneer.*

Proof. The auction should be able to protect the bidder from the auctioneer overcharging winners and colluding with other greedy bidders.

Overcharging Winners: In order to overcharge the winners the auctioneer must have the knowledge of the winning bidder's valuation. In GAVEL, the bidder never have to reveal its demand curve beyond the winning price. Once a channel is won by a bidder, it is not a player in the auction for that channel anymore.

Collusion with greedy bidders: For this trick to work, the greedy bidder must bid above its own valuation but less than the winning bidder's valuation to generate spoils. In GAVEL, it is impossible for the greedy bidder to do this without risking winning the channel at a price higher than its valuation. In which case the auctioneer may lose all of its revenue and the greedy bidder will suffer a negative utility or loss. □

THEOREM 2.5.3. *GAVEL protects against False-name bids.*

Proof. To show that GAVEL protects against False-name bids, we need to show that a bidder cannot increase his utility with false-name bids, given that the other bidders and their bids remain the same.

This is a proof by contradiction. Suppose bidder i wins x fraction of channel C_k at price p_t and with a fictitious bidder i' it wins x' fraction of channel C_k where $x \neq x'$. In GAVEL, x fraction of channel C_k can be won by bidder i at price p_t if and only if at round t, $\sum_{j \in N_i} d_j^{C_k}(t) \leq 1 - x$. With a fictitious bidder, if it wins x' fraction of channel C_k then it means $\sum_{j \in N_{i'}} d_j^{C_k}(t) \leq 1 - x'$. Since i and i' has the same set of neighbours ($N_i = N_{i'}$) , this can only happen if the demand from the neighbours change, which is a contradiction.

□

THEOREM 2.5.4. *GAVEL is individually rational.*

Proof. If bidder i wins channel C_k at round t with price $p_t^{C_k}$, then it means it has positive demand at round t for channel C_k, ie., $d_i^{C_k}(t) > 0$ which means $p_t^{C_k} < V_i^{C_k}$.

Therefore, GAVEL is individually rational for all bidders.

□

2.5.5 Application with signal exchanges

In practise, we envision the auction mechanism occurs every few hours depending on the model. As illustrated in Fig. 2.6, the LSA auctioneer broadcasts the auction parameters along with the spectrum availability vector, at the beginning of the auction epoch. This communication occurs over a secondary channel, most likely using licensed spectrum that guarantees availability. The auction parameters and the availability vector is used by the MNO agents to compute their value for each available channel.

The valuation function in the agents are directly used to compute the demand vector and is transmitted to the LSA auctioneer before the deadline set during the initial broadcast. This process is repeated until the demands are satisfied and the LSA auctioneer is able to determine the final allocations. The final channel allocations along with the constraints associated with each of the channel use including transmit power and duration are communicated to the LSA licensees.

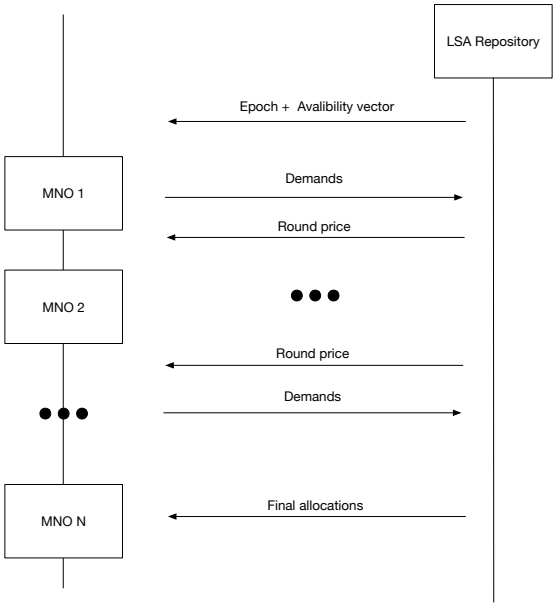

Figure 2.6: Communication signalling during the auction process

2.6 Evaluation

For our evaluation, we follow the auctioning based LSA framework described in section 2.3 with the LSA controller as the auctioneer and the LSA licensees with non-zero demand as bidders. The bidders act as their own proxy agent with access to channel valuations. We compare the results obtained with different auction mechanisms. Specifically, we compare GAVEL against two recently proposed truthful combinatorial auction schemes, AEGIS-MP [38] and SMASHER-GR [8], which supports heterogeneous spectrum. AEGIS-MP is based on the English Clock auction format in which losing bidders are allowed to increase their bids or shrink their bundles until the auction ends. It uses a greedy mechanism for channel allocation and identifies critical neighbours to enable truthful bidding. However, it does not support fine-grained channels. SMASHER-GR is a sealed bid auction that uses the notion of virtual channels to supports fine-grained channels. The bidders are expected to have uniform valuations for any channel bundles they are interested in. Note that both these scheme do not provide bid privacy protection.

To model an urban environment, we consider an area with a realistic distribution of about 2000 houses per square kilometre. We also set the number of channels in the market to 21 modelling after the TVWS bands. To simulate heterogeneous spectrum in the market, we divide these 21 channels into three bands, 700 MHz, 2.4 GHz and

3.5 GHz with 80m, 30m, and 10m interference range respectively. For each of these three bands, the average number of neighbours within the interference range is about 20, 12 and 6 respectively.

`Methodology`: The auction schemes take as input the (i) conflict graph for each channel in the market (ii) the valuation of channels for all bidders and (iii) the price vector. For AEGIS-MP the demand from bidders are only for exclusive channel use, since they do not support fine-grained channels. We adapt demand in the market by changing the bidders' channel valuations. For SMASHER-GR we use uniform valuations for all channel bundles. We rerun these auction schemes 10 times for increasing demand in the market. We evaluate the performance of GAVEL on the following metrics while varying demand in the market, (i) Revenue (ii) Social Welfare (iii) Percentage of winners (iv) Spectrum utilisation. To benchmark auction mechanisms with respect to the optimum, we use the following LP formulations that maximises each of these four metrics individually.

$$\textbf{Social Welfare}: \max_{a} \sum_{i \in \mathbb{N}} \sum_{C_k \in \mathbb{C}} V_i^{C_k} a_i^{C_k} \tag{2.3}$$

$$\textbf{Revenue}: \max_{a} \sum_{i \in \mathbb{N}} \sum_{C_k \in \mathbb{C}} p_i^{C_k} a_i^{C_k} \tag{2.4}$$

$$\textbf{Number of Winners}: \max_{a} \sum_{i \in \mathbb{N}} Y_i \tag{2.5}$$

$$\textbf{Spectrum Utilisation}: \max_{a} \sum_{i \in \mathbb{N}} \sum_{C_k \in \mathbb{C}} a_i^{C_k} \tag{2.6}$$

$$\textit{Subject to,} \sum_{j \in N(i) \cup i} a_i^{C_k} \leq 1$$

$$\mathcal{E}_i^{C_k} a_i^{C_k} \leq 1, \quad \forall i \in \mathbb{N}, \forall k \in \mathbb{C}$$

$$0 \leq a_i^{C_k} \geq 1$$

$$\textit{where,}$$

$$Y_i = 0 \textit{ if } \sum_{C_k \in \mathbb{C}} a_i^{C_k} = 0$$

$$Y_i = 1 \textit{ if } \sum_{C_k \in \mathbb{C}} a_i^{C_k} > 0$$

Results shown for optimal solution are obtained by solving the LP using the GUROBI solver.

Social Welfare: The social welfare achieved in the market for different auction schemes are compared against the optimal solution in Fig 2.7. As the demand in the

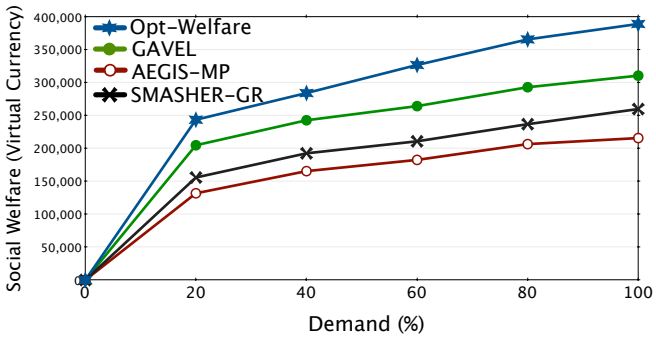

Figure 2.7: Social Welfare vs Demand

market increases, the social welfare in the market also increases, as more bidders' demands are being satisfied. It can be seen from Fig. 2.7 that GAVEL outperforms both AEGIS-MP and SMASHER-GR. This performance improvement is due to three main factors. First, GAVEL does not limit any channel assignment opportunities in order to retain the strategy-proof nature of the scheme. Second, the use of fine-grained channels enables GAVEL to satisfy a significantly larger number bidders' demand when compared to AEGIS-MP. Finally, the use of channel bundles in AEGIS-MP and SMASHER-GR results in additional channels being allocated to a bidder who has no use for them, but still pays for those channels.

When compared to the optimal solution, the social welfare achieved in GAVEL is lower primarily due to the lack of complete information of channel demands in the market at each bidder. For every bidder any direct competition for channels is only from its own neighbours. This leads to scenarios where maximising the social welfare in a local neighbourhood may not be the best allocation to maximise the total social welfare in the market.

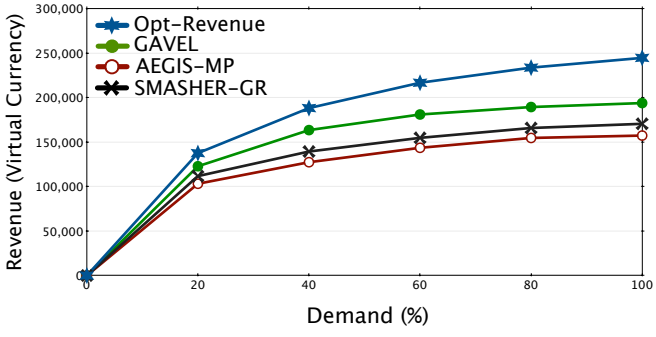

Figure 2.8: Revenue vs Demand

Revenue: The revenue generated in the market with varying demand is shown in Fig. 2.8. It can be seen GAVEL achieves higher revenue than the other two schemes. There are two major contributing factor to this increase in revenue. First, the ability to allocate fine-grained channels increases competition in the network, thereby increasing the total revenue generated. While SMASHER-GR also supports fine-grained channels it only allows uniform valuation for channel bundles which results in significant loss of revenue. Second, unlike the other auction schemes, GAVEL does not group bidders into groups to identify and charge a critical price from the winning bidders. Instead, each winning bidder pays the exact opportunity cost in the network for his access to the channel.

The higher revenue in the optimal allocation is due to better spectrum reusability at the cost of economic robustness where channels are allocated to bidders without the highest valuation in order to improve the overall revenue.

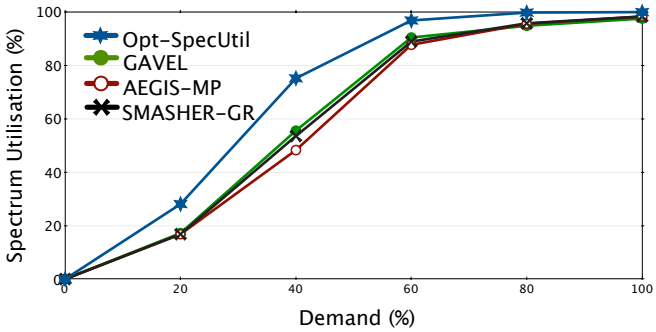

Figure 2.9: Spectrum Utilisation vs Demand

Spectrum Utilisation: The percentage of spectrum utilised with varying demand in the market is shown in Fig. 2.9. The optimal solution shows the amount of possible spectrum utilisation in the scenario. As demand in the market increases, spectrum utilisation also increases. When there is about 60% demand in the network, the spectrum utilisation achieved is more than 90% for all the auction mechanisms. This is due to the limited number of channels in the market. AEGIS-MP has a lower spectrum utilisation since it does not support fine-grained channels. Also considering that it over allocates channels to bidders who may not end up using these channels, the effective spectrum utilisation should be even lower.

Percentage of Winners: Fig. 2.10, shows the percentage of winners in the auction. The optimal scheme shows the maximum number of winners possible in this scenario. It can be seen that for the auction mechanisms as the demand in the market increases,

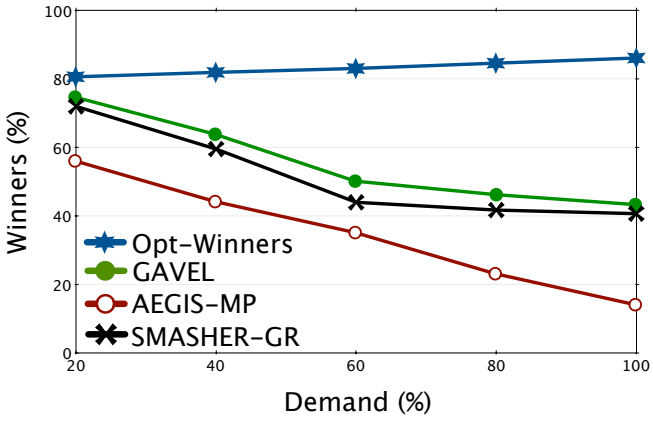

Figure 2.10: Percentage of Winners vs Demand

there is a lower number of winners, due to the increase in competition. Unlike the auction schemes, the optimal solution is able to generate more winners with increasing demand as it increases the opportunity for a bidder to win. GAVEL has a significant increase in the percentage of winners when compared to AEGIS-MP due to the use of fine-grained channels. Without the ability to allocate fine-grained channels, only one bidder can win the channel in a neighbourhood. Whereas GAVEL supports both fine-grained channels and whole channels, resulting in about 20% increase in winners. On the other hand, SMASHER-GR has a high percentage of winners since it uses a greedy scheme to allocate channels and support fine-grained channels. However even with a high number of winners SMASHER-GR achieves a lower social welfare and revenue due to the simplicity of the supported valuations, where all the channel bundles a bidder desires has the same valuation.

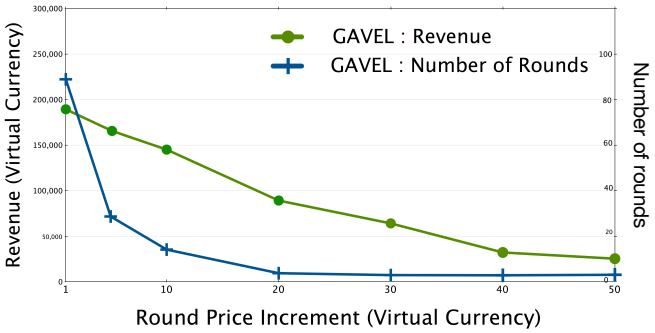

Figure 2.11: Revenue and Number of Rounds vs Price Increment Step Size

Round Price Increment: Unlike sealed bid auction schemes, GAVEL is an iterative

mechanism that spans several rounds. The number of rounds is determined by the step size of the price increment in each round. To analyse the effect of this price increment, we fix the demand in the market to 60% to compute revenue and number of rounds for different price increment values shown in Fig. 2.11. As expected, the highest revenue is obtained with the smallest step size. On the other hand, the auction takes most number of rounds to complete. Increasing the step size decreases the revenue because a higher step size drives out demand quickly and gets the auction to a point when effectively all the bidders have zero demand even though there are still unallocated channels, explaining the drop in revenue. Clearly, a higher step size leads to auction completing in fewer rounds. Interesting point to note is about how reduction in revenue with increasing step size relates to the reduction in number of rounds. It can be seen from Fig. 2.11 that increasing the step size from 1 to 5 results in about 15% loss of revenue but reduces the number of rounds by about 70%, suggesting a value for step size that keeps the duration and overhead of auction minimal without hurting the revenue much.

To summarise, GAVEL generates higher revenues for the incumbents by enabling fine-grained channels while efficiently using opportunities for channel reuse. This is an incentive for the incumbents to share more spectrum in the market, which can in turn benefit bidders. GAVEL achieves higher social welfare which means a higher number of bidders are satisfied, while protecting the bid privacy from the auctioneer. This is an incentive for the bidders to participate in the auction leading to more competition and efficient use of the wireless spectrum.

2.7 Summary and Conclusion

In this chapter, we considered auction mechanisms for short-term dynamic spectrum access. Existing auction mechanisms fail to satisfy all the requirements of a short-term spectrum market. We analyse these auction mechanisms and argue that the problems with these auction mechanisms are not due to the winner and price determination strategy, rather due to the underlying auction format, the sealed-bid auction format. Based on this insight, we proposed GAVEL, a truthful auction mechanism for short-term spectrum auctions. Using geographical information of over 2000 houses in the UK, we evaluated the performance of GAVEL against existing comparable auction mechanisms. GAVEL achieves better performance than existing mechanisms and is well suited for the short-term dynamic spectrum market.

Chapter 3

Recycling the Cyclic Prefix to Mitigate Interference in OFDM

3.1 Introduction

Orthogonal Frequency Division Multiplexing (OFDM) is a spectrally efficient digital modulation method that is at the heart of almost all modern wireless systems. In OFDM, the stream of symbols (that represent the digitally modulated form of user data) are multiplexed over closely spaced sub-carriers and transmitted as parallel sub-streams. Orthogonality of sub-carriers makes them non-interfering with each other and in turn leads to other benefits including robustness to frequency-selective fading, flexible/dynamic channel-aware allocation of sub-carriers to users and ease of spectrum aggregation. For these reasons, Wi-Fi (WLANs based on IEEE 802.11) standards since 802.11a/g have adopted OFDM as the physical layer underlying a CSMA/CA multiple access scheme. 4G LTE mobile networks take this further by incorporating a multiple access scheme called OFDMA that allocates different users to different subsets of subcarriers[1]. The most recent digital audio/video broadcasting standards are also based on OFDM.

In order to maintain orthogonality between consecutive OFDM symbols, an OFDM transmitter adds a cyclic prefix in front of each symbol. This prefix is a copy of the end of each OFDM symbol whose purpose is to maintain orthogonality. The length of the prefix is adjusted to match the worst case delay spread that can occur in any deployment. This value is typically over-provisioned. The first OFDM-based Wi-

[1]More precisely, LTE uses OFDMA in the downlink direction. A variant called SC-FDMA is used for the uplink to suit lower cost and battery operated mobile transmitters with non-linear amplifiers.

Fi standard, 802.11a/g, specified 0.8μs long cyclic prefixes which corresponded to a signal path of 240m. Newer versions allowed the cyclic prefix to be halved, which is still hugely over-provisioned, give that the range of most of the Wi-Fi links is only few tens of meters. Similarly, standard LTE cyclic prefix lasts about 5μs and covers a signal path of 1.5 km.

In this chapter, we present a novel receiver design called CPRecycle that leverages the over-provisioned cyclic prefix to mitigate the interference from concurrent wireless transmissions. The key observation underlying CPRecycle design is that when the receiver performs FFT with different starting points in the redundant portion of the cyclic prefix, the resulting signal component remains the same across the different FFTs but interference can vary by as much as 40dB, as we demonstrate in our measurements.

The main design challenge is how to find the optimal starting point for the FFT as it depends on the content of the interfering packet and it varies across subcarriers. This is very difficult as we cannot observe the interference signal in isolation. Instead, we create an empirical model of the interference as a function of the starting position of the FFT transformation. We then use this model to perform a maximum likelihood detection using the decoding outputs of all starting positions.

We implement CPRecycle on USRPs. An attractive aspect of CPRecycle is that it is local to the receiver and does not require any modification of the existing protocols nor changes at the transmitter, thus it can work with legacy devices. It is applicable to any OFDM/OFDMA based PHY with overprovisioned cyclic prefix. The computation complexity of CPRecycle can be tuned and it gracefully degrades to a standard OFDM receiver in the worst case.

In our evaluation we show that CPRecycle is useful in two important scenarios. The first scenario, *co-channel interference*, is a common case in todays Wi-Fi deployments where multiple nodes access the same Wi-Fi channel at the same time. This can cause interference and packet losses, in particular in hidden-node scenarios. In the co-channel interference case we observe up to 15dB reduction in interference through the use of CPRecycle , even in case of the highest modulation rate (64QAM) and lowest coding rate (3/4).

The second important scenario is the adjacent channel interference scenario. All wireless transmitters experience RF leakage and cause interference even outside of their own channel. OFDM is able to maintain orthogonality between carriers only in perfectly synchronised systems, which rarely occurs [39]. In practice, there is a non negligible out-of-band interference and a guard-band is reserved to prevent interfer-

ence between adjacent channels. We study the performance of CPRecycle interference mitigation in the adjacent channel interference scenario where we remove the guard-band and tightly pack channels together. We observe that CPRecycle can remove up to 25dB of interference.

Through extensive simulation and experimental evaluations using USRP and commodity Wi-Fi hardware, we demonstrate the effectiveness of CPRecycle in significantly improving receiver side decoding in presence of interference, thereby also enabling efficient spectrum use. The network level benefits are significant due to the sharp drop in the average number of interfering neighbors in the network. In summary,

- We propose CPRecycle , a novel receiver design that improves performance of existing OFDM-based wireless systems through an improved signal processing at the receiver, leveraging commonly overprovisioned OFDM cycle prefixes.
- As a part of CPRecycle , we propose a novel decoding algorithm that improves decoding performance by jointly processing received signal over multiple FFT window positions.
- In our evaluation we show that we can reduce the effects of co-channel interference on a Wi-Fi receiver by up to 15dB and the effects of adjacent channel interference by up to 25dB by implementing only local modifications at the receiver.

3.2 Background

This sections gives a brief overview of interference in OFDM based systems and the use of cyclic prefix for inter-symbol interference avoidance.

3.2.1 Interference in OFDM

Adjacent channel interference [40–45] occurs when an interferer while transmitting in its own channels, leaks part of its power into the adjacent channels, corrupting the signal received by a receiver in those adjacent channels. This can be due to intermodulation of signals. Zubow et al, [43], analyse the effects of adjacent channel interference on 802.11 WLANs and observe that adjacent channel interference causes severe problems with the carrier sensing mechanism in 802.11. It was found that the carrier sensing mechanism can be too restrictive in some cases, leading the node to mistakingly

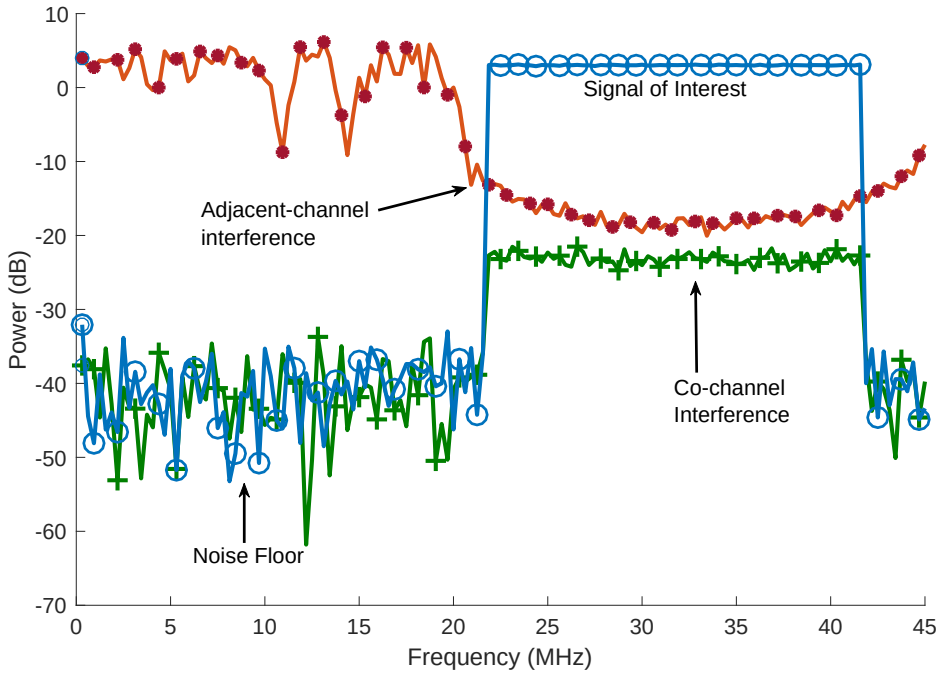

Figure 3.1: Illustration of Adjacent Channel Interference and Co-channel Interference.

defer its transmission, and too optimistic in some cases resulting in packet losses. An illustration of adjacent channel interference is shown in Fig. 3.1. In this example, the sender is assigned a 20MHz channel (from 24 to 44MHz) in which it transmits the signal of interest. The interferer although assigned an adjacent non-overlapping 20MHz channel (1 to 21MHz in Fig. 3.1) leaks energy into the adjacent band interfering with the signal of interest leading to a drop in SINR by about 15dB.

Another scenario where adjacent channel interference might occur is when two neighboring transmitters use partially overlapping channels, a very common scenario in IEEE 802.11 networks due the limited number of non-overlapping channels. In this scenario, there are three main problems caused due to adjacent channel interference. (i) Incorrect determination of a busy medium: when a transmitter performs carrier sensing before transmitting a packet, it may detect a high energy level due to an interferer leaking energy into its adjacent bands. This leads the transmitter to incorrectly assume that the medium is in use and defer its transmission. (ii) Signal corruption due to power heterogeneity: a weak signal received by a receiver can be corrupted a high power interferer located close by leaking energy into the adjacent bands. (iii) Hidden terminals and exposed terminals that cause signal corruption due to adjacent channel

interference cannot be handled through RTS/CTS, since the nodes are operating on a different channel, even though they are overlapping channels. One of the defining features of adjacent channel interference is the effect of interference power heterogeneity. The subcarriers closer to the channels occupied by the interferer are affected by a stronger interfering signal in relative to the other subcarriers, leading to a varying effect in different subcarriers.

Co-channel interference [46, 47] occurs when multiple transmitters use the same subset of frequencies for communication. In IEEE 802.11 standards, co-channel interference is mitigated with the use of CSMA/CA, where transmitters would scan for an idle medium before transmissions. However, in dense IEEE 802.11 WLAN deployments, this situation cannot be avoided due to the limited number of non-overlapping channels in the 2.4GHz ISM band and overcrowding [48]. Gummadi et al [49], in their study of the effects of co-channel interference on 802.11 networks show how an interfering signal that is orders of times weaker can cause significant packet losses in a WLAN.

The presence of co-channel interference can have other indirect effects on the network performance as well. Using CSMA/CA, 802.11 nodes must scan the medium (for 4μs for 20MHz channel) and perform a clear channel assessment to determine if the channel is busy before transmission. The clear channel assessment can result in a busy medium when one of two following conditions are satisfied. (i) Carrier Sense; It is able to detect and decode an 802.11 preamble (ii) Energy Detection; The energy detected in the channel is atleast 20dB greater than the minimum modulation and coding rate sensitivity. In the presence of co-channel interference, the transmitter would perform an exponential back-off which reduces the achievable throughput. Significant improvements in throughput [50] can be achieved by reducing this energy detection threshold.

In cellular networks, the use of femto cells can cause co-channel interference when deployed in a co-channel or hybrid configuration. In these configurations, a macrocell is overlaid with OFDM based femto cells assigned an overlapping set of channels. This can cause co-channel interference between neighboring femto cells sharing the same set of channels (co-tier interference) or between a femto cell and a macro cell (cross-tier interference) [51]. While co-tier interference can be managed through an efficient allocation of subcarriers, it is far more difficult to manage cross-tier interference due to limited availability of the wireless spectrum.

3.3 Related Work

Adjacent Channel Interference: OFDM systems are known to suffer from high levels of out-of-band emissions. Several techniques have been proposed to reduce this out-of-band radiation. Windowing is a time domain technique [52], where the signal is multiplied with a windowing function before transmission to reduce the energy in the side lobes. Techniques such as Subcarrier weighing [53], Multiple-choice sequences [54], Cancellation carriers [55], constellation Expansion [56], and Adaptive symbol transition [57] are some of the techniques that manipulate the frequency domain signal at the transmitter to enable out of band reduction. A comprehensive comparison of these side lobe reduction has been presented in [58]. One of the defining features of adjacent channel interference is that only the subcarriers the band assigned to a transmitter is affected. The schemes that suppress ACI are designed to mitigate the interference in the edge subcarriers and hence are not suitable to suppress other types of interference such as co-channel interference.

In LTE, fractional frequency reuse and adaptive power management is used to reduce the level of interference in the network. Active interference mitigation schemes such as interference rejection combining [59], co-ordinated multipoint transmission (COMP) [60], and channel coding are being used to mitigate co-channel interference.

Windowing is a time domain technique [52], where the signal is multiplied with a windowing function before transmission to reduce the energy in the side lobes. However, it expands the signal in the time domain resulting in wastage of bandwidth. Techniques such as Subcarrier weighing [53], Multiple-choice sequences [54], Cancellation carriers [55], Extended Active Interference cancellation [61], Constellation Expansion [56], and Adaptive symbol transition [57] are some of the techniques that manipulate the frequency domain signal at the transmitter to enable out of band reduction. An excellent comparison of these techniques has been presented in [58]. All of these techniques require high computational complexity and some techniques [52, 54] result in lower throughput due to the use of some subcarriers for control. Since these techniques are designed to reduce OOB emissions from OFDM transmitters, they either dont use the edge subcarriers for data or use them to transmit data that would minimise the spurious emissions. Hence they cannot be used in cases where the ACI is due to intentional use of partially overlapping channels. **Co-channel Interference**: Co-channel interference management techniques can be grouped into two categories (i) schemes that mitigate interference by modifying the transmitted signal (ii) schemes

that decode the signal of interest in the presence of interference.

In 802.11 [62], co-channel interference is prevented using CSMA/CA, where a transmitter would sense the channel and only transmit if the energy detected in the channel is less than a threshold. This ensures that nodes using the same channel does not cause co-channel interference. However, this leads to the exposed terminals problem, where nodes are made to unnecessarily defer their transmission even though simultaneous transmission would have been successful.

In LTE, fractional frequency reuse and adaptive power management is used to reduce the level of interference in the network. Active interference mitigation schemes such as interference rejection combining [59], co-ordinated multipoint transmission (COMP) [60], and channel coding are being used to mitigate co-channel interference. Co-ordinated multipoint transmission is a well known technique to mitigate inter-cell interference in 3GPP networks. It involves the coordination of multiple transmitters with in a cell, where certain transmitters can be muted to improve the overall SINR.

Interference mitigation schemes such as [63,64], adapt the transmissions to be more resilient to interference. Their application is limited to niche scenarios and moreover they require changes to the existing standards and are not backward compatible. Interference alignment [65–67] is a recently proposed technique that in this category. However, they require communication over the wired backbone and are not backward compatible. Similarly, Swarun et al, propose OpenRF [68] a cross-layer architecture for interference management that enables access points to cancel their interference at the clients significantly improving the network capacity and is applicable only to multiple antenna systems.

Several schemes have been proposed to decode the signal of interest in the presence of co-channel interference. Kong et al [69] propose MZig, a physical layer technique to decode simultaneous transmissions from multiple ZigBee devices to provide an m-fold increase in throughput. Gollakota et al, propose TIMO [70], an IEEE 802.11n receiver that can decode the packets in the presence of cross-technology interference. While TIMO can work even when the interference is persistent and lasts over a few seconds, unlike, CPRecycle , it can only be applied to receivers with multiple antennas. Yan et al, propose WizBee, [71], a ZigBee receiver that can decode ZigBee packets in the presence of strong interference from 802.11 nodes limiting its application.

In contrast to the interference management schemes discussed above, CPRecycle can mitigate different types of interference on single antenna systems and is also backward compatible with legacy OFDM systems.

Partial Packet Recovery: Partial packet recovery is a class of techniques that attempt to recover corrupt packets instead of retransmitting them. Several approaches [72–77] have been proposed to address this inefficiency in retransmitting an entire packet due to a few bit errors. They can broadly be categorised into (i) co-operative packet recovery and (ii) cross-layer packet recovery.

In co-operative packet recovery schemes such as [72–74, 78] multiple access points coordinate with each other to recover partially corrupted packets by exploiting receiver diversity. SOFT and MRD use PHY layer information to identify corrupt blocks of bits that needs to be transmitted. ZipTx uses adaptive FEC codes to improve probability of repairing bit errors in co-operation with other APs in the vicinity. However, co-operative packet recovery techniques (including MRD and SOFT) demand additional constraints such as multiple coordinating APs, hardware changes, incompatible with IEEE 802.11, and hence are not useful in scenarios where CPRecycle is applicable. These techniques are useful in 802.11 mesh networks, where only the correct bits of a packet are forwarded on and the receiver combines multiple such copies to recover the entire packet, and in scenarios where these multiple APs coordinate through a wired backbone to share partial packets with the receiver.

Cross-layer partial packet recovery techniques such as [75, 77] attempt to recover partially corrupt retransmissions of the same packet and are in an way extensions of the chase combining decoder (where multiple noisy copies of a packet are combined to recover the packet). These techniques however require modification at both the transmitter and receiver to use additional parity bits to identify corrupt blocks for re-transmission.

Furthermore, both categories of partial packet recovery techniques are complementary to CPRecycle and can be used in combination to improve the packet reception rate further. For example, SOFT and PPR use a confidence measure on decoding a bit as '0' or '1' cooperatively with multiple APs to improve decoding accuracy. When used in combination with CPRecycle, it would receive higher confidence measures on the decoding decision since CPRecycle exploits multiple copies of the signal in the cyclic prefix to select the FFT window with the signal that is closest to the correct lattice point.

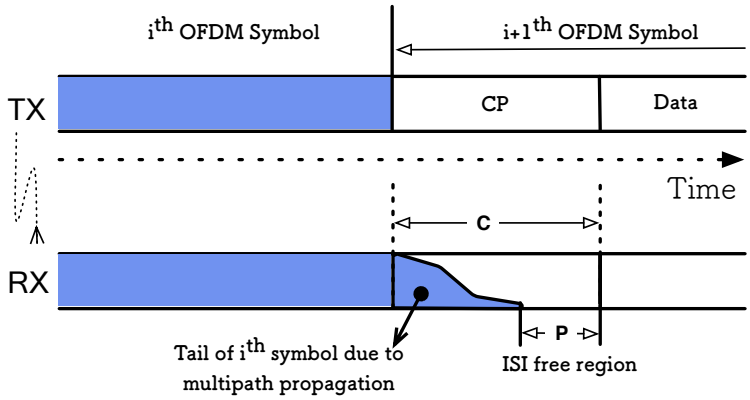

Figure 3.2: Illustration of Cyclic Prefix (CP) or guard interval.

3.3.1 Cyclic Prefix

In OFDM based systems, the cyclic prefix (CP) or guard interval, illustrated in Fig. 3.2, is used primarily to prevent inter-symbol interference (ISI). ISI is a type of signal distortion that is caused when consecutively transmitted symbols interfere with each other at the receiver. This is due to the multi-path propagation characteristics of the wireless channel, where a transmitted signal may take multiple paths from the transmitter to the receiver with different propagation delays and the multiple copies of the signal may interfere with itself. The cyclic prefix acts as a guard period between successive OFDM symbols, thereby completely eliminating the ISI. The duration of the cyclic prefix is chosen to be greater than the largest delay spread expected by any user in the target environment. It is usually defined in the communication standards and cannot be changed adaptively based on the environment due to interoperability issues.

In practice, cyclic prefix is a copy of a portion of the OFDM symbol towards its end, and it is inserted before the actual OFDM symbol. Because of the way cyclic prefix is constructed, only one symbol from the intended transmitter is received at any point in time during the whole course of duration spanning the cyclic prefix and actual OFDM symbol.

The downside of using cyclic prefix is that it lowers the spectral efficiency since no additional information is transferred during the cyclic prefix period. Note that cyclic prefix duration is chosen based on the maximum delay spread which can result in substantial portion of the overall symbol period being consumed by the cyclic prefix. For example, in 802.11 systems about 20% of the symbol duration is allocated for the cyclic prefix.

Standard	Bandwidth	FFT Size	CP Size	Duration
802.11a/g	20 MHz	64	16	0.8 μs
802.11n/ac	40 MHz	128	32 (16)	1.6 (0.8) μs
802.11n/ac	80 MHz	256	64 (32)	3.2 (1.6) μs
802.11n/ac	160 MHz	512	128 (64)	6.4 (3.2) μs

Table 3.1: Cyclic Prefix in 802.11 standards

Table 3.1 lists size and duration of cyclic prefix specified in different 802.11 standards with the default long guard interval as well as the short guard interval (in parentheses). In LTE, the normal cyclic prefix length is 4.7μs, an overhead about 7% in a OFDM symbol with actual data portion of about 66.7μs. There is also an extended cyclic prefix of length 16.7μs specified in LTE for broadcast services and environments with long delay spreads, increasing the cyclic prefix related overhead to 25% in this case.

Studies that model the indoor propagation characteristics [79–81] of wireless signals, however, show that in most of the cases the multi-path delay spread is in the order of nano-seconds, suggesting that cyclic prefix in practice is usually over-provisioned by a significant amount. In these measurement based studies, the power delay profile, which is the strength of the received signal plotted against time, is used to characterise the multipath channel. The time delay between the multipath arrivals is used to determine the maximum delay spread in the environment, which is in the order of nano-seconds for various environments [79–81]. Since the inter-symbol interference from an OFDM symbol on the following OFDM symbol is limited to the maximum delay spread, this suggests that the cyclic prefix is over-provisioned significantly in several environments.

Furthermore, the latest standards such as IEEE 802.11n/ac, support wider channel widths of upto 160MHz. With wider channels, as shown in Table 3.1, the duration of the cyclic prefix increases due to the increase in number of subcarriers. However, since the multipath delay spread is independent of the channel width, the number of samples that are not affected by ISI (which is the portion of over-provisioned cyclic prefix) only increases with channel width.

Table 3.2: Notations used in this chapter

Notation	Description
X_s	Frequency domain signal to be transmitted
x_s	Time domain signal to be transmitted
$\hat{X}_s$	Frequency domain signal received
P	Number of samples unaffected by ISI
C	Number of samples in cyclic prefix
F	Number of subcarriers
L	Alphabets of the IQ constellation
R_A	Amplitude variation
R_ϕ	Phase variation
f_m	density function
B_a	amplitude smoothing parameter
B_ϕ	phase smoothing parameter

3.4 Opportunities in Cyclic Prefix

In a standard OFDM system (illustrated in Fig. 3.3), the receiver discards the cyclic prefix before decoding the OFDM symbol. In this section we discuss the opportunities in retaining the cyclic prefix and using it to improve symbol decoding. We start by analyzing the effect of choosing different FFT windows on an OFDM symbol.

3.4.1 Sliding FFT Windows

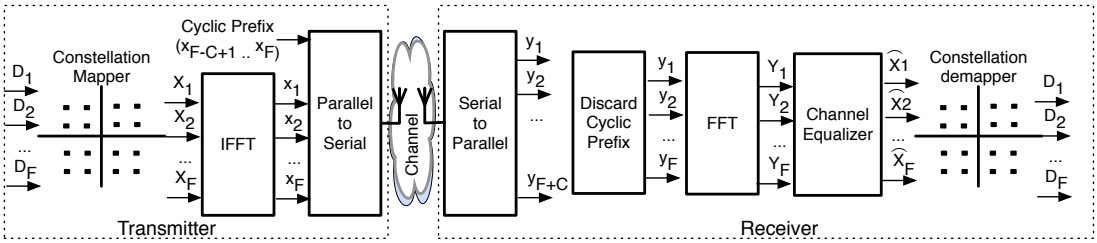

Figure 3.3: Schematic of a standard OFDM system.

Let us consider a discrete-time OFDM system, illustrated in Fig. 3.3. The system consists of F subcarriers onto which complex data symbols D_s are modulated using an inverse discrete Fourier transform (IDFT). Let vector

$$X_s = (X_s[0], \cdots, X_s[F-1])$$
$$\text{where,} \quad X_s[f] \in \mathcal{L} = \{l_1, l_2, \cdots, l_k\}$$

denote, in frequency domain, a complex vector representing the s^{th} OFDM symbol transmitted by the n^{th} user, and $\mathcal{L}$ denotes the finite set of alphabet from the transmitter's codebook, each corresponding to a lattice point. The time-domain representation of the OFDM symbol s transmitted by the n^{th} user is given by

$$x_s = (x_s[0], \cdots, x_s[F-1])$$

where,

$$x_s[t] = \frac{1}{F} \sum_{f=0}^{F-1} X_s[f] e^{i2\pi ft/F}, \quad 0 \leq t < F$$

To eliminate the effects of dispersed channel distortion a cyclic prefix, which is a copy of a portion of the symbol, is prepended to each OFDM symbol. The time-domain signal with a cyclic prefix of size C transmitted by node n can be written as follows,

$$x'_s[t] = x_s[t \bmod F], \qquad -C \leq t \leq F-1$$

The received signal y_s for OFDM symbol s, contains $F+C$ samples, including the cyclic prefix of C samples. To perform DFT on the received signal, a segment of size F must be chosen with the rest of the C samples disregarded from y_s. Since there are P samples in the cyclic prefix that are not affected by ISI, as shown in Fig. 3.2, there are P valid sampling windows which can be used to decode the data transmitted in symbol s. We refer to each of these P sampling windows as segments. After channel equalization, since these P segments are not affected by ISI, the signal received from the j^{th} segment at subcarrier f in OFDM symbol s can be written as,

$$\hat{X}_s^j[f] = \frac{1}{\hat{H}} \sum_{t=0}^{F-1} y_s^j[f] e^{-i2\pi(C-P+j)f/F} + \mathcal{E}_s^i[f] \tag{3.1}$$

where, $\hat{H}$ is the estimated channel matrix and $\mathcal{E}_s^i[f]$ is the cumulative noise on that subcarrier from the environment and other interferers.

In the time domain, these different segments correspond to different cyclic shifts of the data transmitted in the OFDM symbol. However, this translates to a frequency dependant phase rotation in the frequency domain which can be computed (and easily corrected) for the segment j and subcarrier f as,

$$\theta^j[f] = e^{-i2\pi(C-P+j)f/F} \tag{3.2}$$

Hence, this predictable phase shift can be easily corrected to obtain P copies of the transmitted symbol.

PROPOSITION 3.4.1. *Choosing different FFT segments of an OFDM symbol does not affect the symbol except for a multiplicative phase shift due to the rotation in the time domain.*

3.4.2 Opportunities for Interference Mitigation

To understand the effects of interference in different FFT segments, we conduct real life experiments with USRPs and implement the OFDM system illustrated in Fig. 3.3. We consider the communication between an 802.11g access point and client in the presence of (adjacent/co-channel) interference. The transmitter is assigned a total of 64 subcarriers of 312.5KHz width and the duration of the cyclic prefix is fixed at 0.8 μs with 16 samples. To create a scenario with adjacent channel interference, contiguous subcarriers are assigned to the sender and interferer with 4 subcarriers as guardband in between. The interferer transmits the signal with a temporal offset that is greater than 0.8 μs, the duration of the cyclic prefix to create adjacent channel interference. To create co-channel interference, the interferer is assigned the same set of subcarriers used by the sender. *The key insight from analyzing the interference at the receiver is*

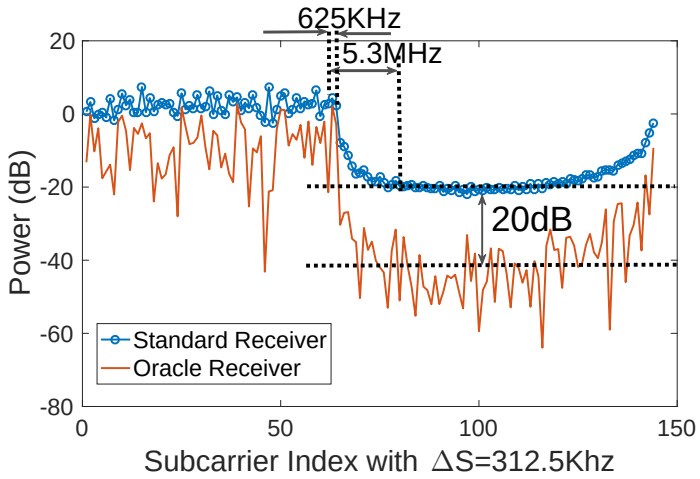

Figure 3.4: Almost 20dB reduction in interference by choosing best FFT segment for each subcarrier

that the effect of interference varies significantly across the different FFT segments of the same OFDM symbol. For instance, an OFDM symbol received with -20dB SIR,

is shown in Fig. 3.4. In this scenario, the interferer occupies the subcarriers (68-132) adjacent to the sender (1 to 64) and due to a temporal offset greater than the duration of cyclic prefix, leaks energy into the adjacent bands distorting the sender's signal. The normalised interference power (obtained by muting the sender) at subcarrier 63 as seen by the receiver for different levels of SIR, over all 16 possible FFT segments of an OFDM symbol is shown in Fig. 3.5. It can be seen that the interference power varies significantly across the FFT segments. For instance, in the presence of adjacent channel interference with -30dB SIR, the interference power varies by almost 40dB, with the lowest at FFT segment 6.

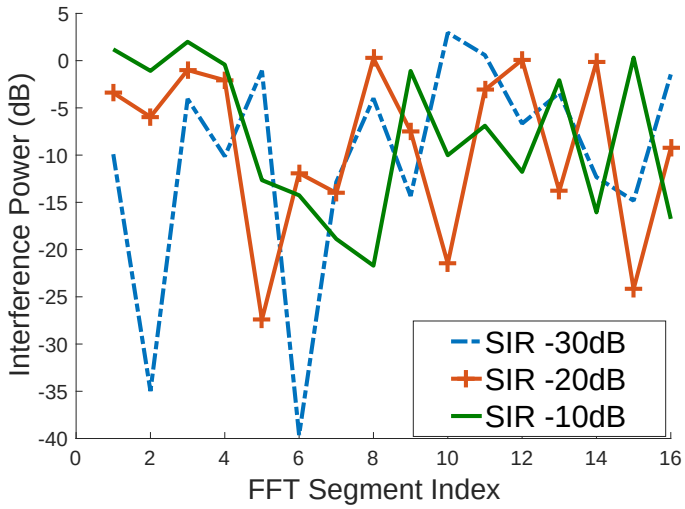

Figure 3.5: Interference power in a subcarrier at different FFT segments showing significant variation

Combining this insight with the fact that these P values for each subcarrier f have the same signal component as stated in Proposition 3.4.1, but are affected by a different interference component as shown in Eq. 3.1, it is clear that identifying the best FFT segments for each subcarrier can have significant benefits over discarding the cyclic prefix as done in existing OFDM based wireless systems.

First, minimizing interference power in each subcarrier would reduce the overall effects of interference, enabling signal decoding even in the presence of interference and it can be effective for different types of interference. In the example discussed above in Fig. 3.5 with SIR -30dB, a standard OFDM receiver would have discarded the cyclic prefix and selected the 16th FFT segment where the interference is almost 35dB stronger than in FFT segment 6. We refer to a scheme identifying the FFT seg-

ment yielding the lowest interference power as the Oracle scheme, which assumes perfect knowledge of the interference at the receiver. The interference power in different subcarriers with a standard OFDM receiver and an Oracle receiver are shown in Fig. 3.4. The oracle scheme is able to reduce the effects of interference in the channel used by the sender by about 20dB as illustrated.

Second, the sharp spectrum mask realized by choosing the best FFT windows can reduce the number of subcarriers used as guard-band between contiguous bands assigned to neighboring transmitters. This means cognitive users can be allocated frequencies that are much closer to incumbents, improving efficiency of spectrum use. For instance, from Fig. 3.4, the spectrum mask realized using the oracle scheme (shown in red with empty circle as key) is very sharp compared to the vanilla case of not using any adjacent channel interference mitigation mechanism (shown in blue with filled in circle as key). And the required guard band is significantly reduced from 5.3MHz to just 625KHz for an adjacent channel interference threshold of about -20dB, enabling efficient use of the spectrum.

However to exploit these opportunities, we need to be able to decode the received symbol in the presence of P redundant copies of the signal and there are several challenges that must be overcome first.

3.4.3 Challenges with Decoding

It is not practical to possess perfect knowledge of interference at the receiver, without which the FFT segments with the minimum interference power cannot be identified. The Oracle scheme while it provides a clear picture of the opportunities for mitigating interference, is thus impractical.

Using simple statistical metrics to decode OFDM symbols using P redundant copies is not effective and as a result underlying opportunities for mitigating interference may be squandered using them. To understand this, we define a naive decoder to identify the closest lattice point around which the signal received in different FFT segments is scattered. For each subcarrier we compute the average deviation of the received complex vector from the various possible lattice points for the modulation scheme used, over all the FFT segments. Then the lattice point with the minimum average deviation is assumed to be the correct one [82]:

$$l* = \arg\min_{l \in \mathcal{L}} \sum_{i=1}^{P} |\hat{X}_s^i[f] - l| \tag{3.3}$$

To evaluate the naive decoder, we use USRPs and the same WiFi settings described above for the experiments. We vary the SIR for different modulation schemes and the packet error rates for QPSK modulation are shown in Fig. 3.6, 3.7, and 3.8 for different guardband sizes. As expected, the metric performs well at lower interference power. When the SIR is about -10dB, both the Oracle scheme and the naive decoder are able to eliminate the packet errors. However, at SIR -20dB, while the Oracle scheme is able to decode all the packets successfully, using the naive decoder only results in marginal improvements. In the presence of strong interference (with SIR less than -10dB), the shortcomings of the naive decoder are apparent. The performance of the oracle scheme with strong interference shows that there are FFT segments where the received signal can be successfully decoded, however, the naive decoder is unable to find the right lattice points. In analyzing the scenarios where the naive decoder fails, we identify three main sources for these errors.

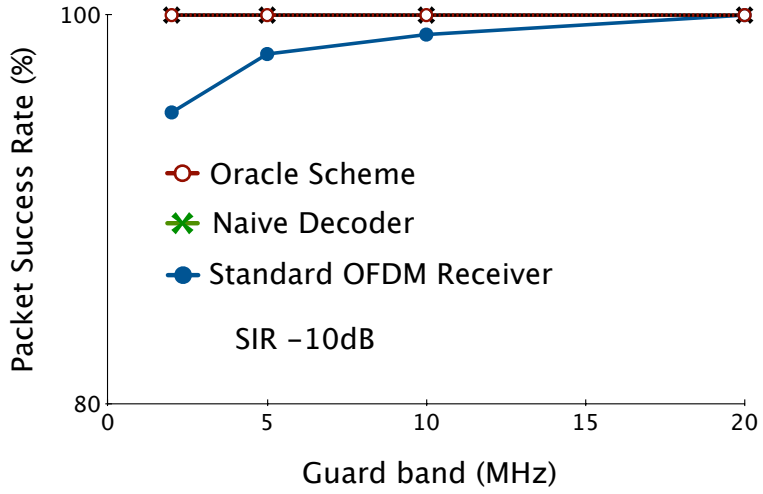

Figure 3.6: Packet success rate using Oracle scheme and the naive decoder showing deteriorating performance when interference increases; experiment settings: single adjacent channel interferer, QPSK with 3/4 coding rate, varying guard band and SIR values = 10 dB

To illustrate this, we use an example scenario shown in Fig. 3.9, with the set of possible lattice points of the transmitted signal (blue plus marker) and the signal received in different FFT segments (red cross marker). For simplicity, we consider only two lattice points (BPSK) and $P = 5$ (five FFT segments are used for decoding). In this instance, the transmitted signal corresponds to lattice point 1, and due to varying interference in different FFT segments, the received signal is scattered around the

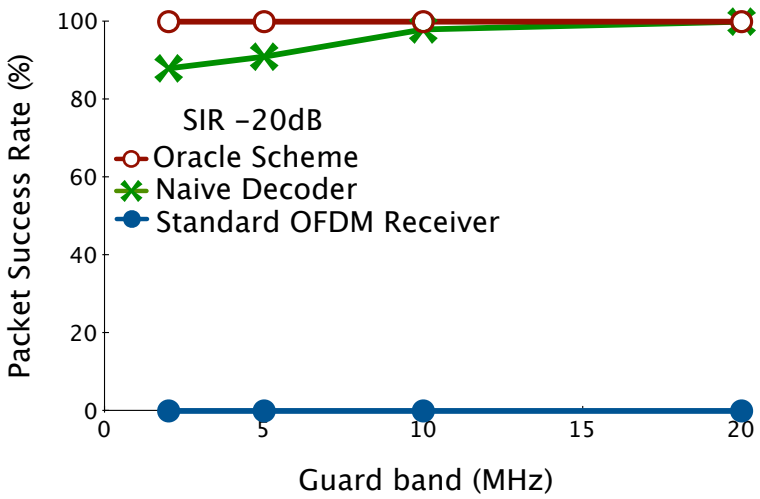

Figure 3.7: Packet success rate using Oracle scheme and the naive decoder showing deteriorating performance when interference increases; experiment settings: single adjacent channel interferer, QPSK with 3/4 coding rate, varying guard band and SIR = 20dB

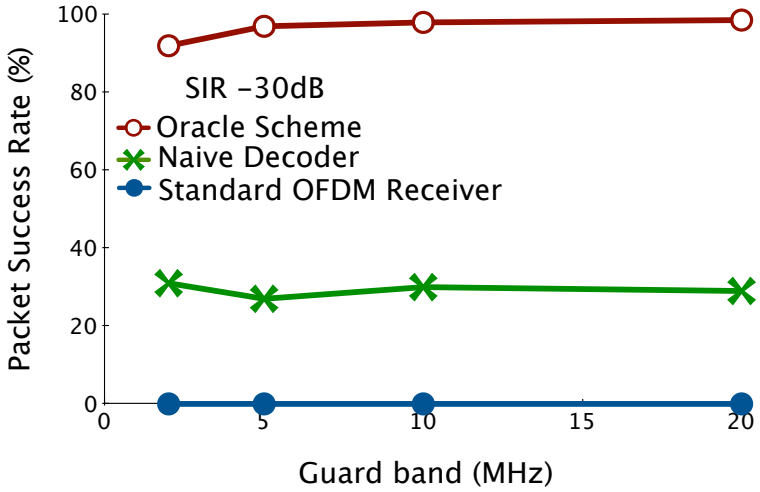

Figure 3.8: Packet success rate using Oracle scheme and the naive decoder showing deteriorating performance when interference increases; experiment settings: single adjacent channel interferer, QPSK with 3/4 coding rate, varying guard band and SIR = 30dB

transmitted lattice point. To illustrate different scenarios where errors occur, we consider that one of the FFT segments suffers from strong interference and the received signal is close to lattice point 0 even though the transmitted signal corresponds to lat-

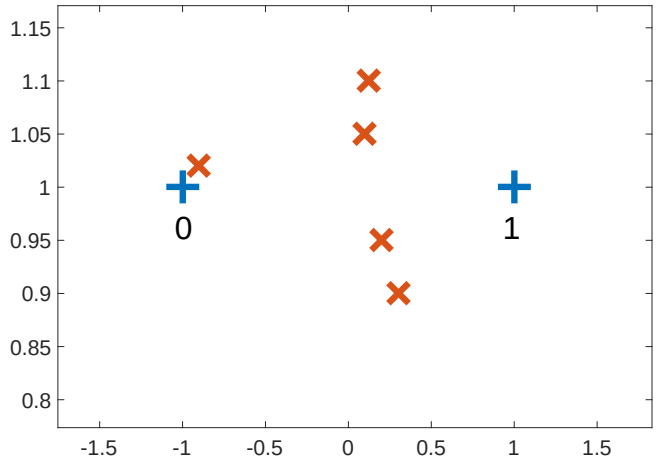

Figure 3.9: Constellation plot showing two lattice points and received signal in 5 FFT segments illustrating problems with a simple metric

tice point 1.

The first source of the error is the use of arithmetic mean in the naive decoder to determine the central tendency of the signal received in different FFT segments. It is well known that arithmetic mean is susceptible to outliers making it ineffective either due to a small sample size or if the underlying distribution is skewed. In the example discussed above, the received signal in four of the five FFT segments are closer to lattice point 1. However, due to a single outlier, on an average the five points are closer to lattice point 0 and hence are incorrectly identified. The small number of ISI free FFT segments further increase the proportion of these outliers.

Second the naive decoder assumes that the received signal from different FFT segments are on the correct lattice point. At the receiver, the signal corresponding to a lattice point would have been affected by fading and AWGN noise due to the wireless medium. The constellation decoders work under the assumption that of the received signal with the effects due to fading and noise perfectly removed would be exactly one of the lattice codes. However, this is not true in the presence of interference. With interference affecting each of the FFT segments apart from fading effects and channel noise, the received signal would be at a certain distance from the correct lattice point. In the example discussed above, four of the five points are at a similar distance away from the lattice point. Instead, if the received signal is expected to be at a certain distance from lattice point 1 then the decoder has a better chance of identifying the

outlier.

Finally, the naive decoder completely ignores the phase errors due to interference. It only takes into account the amplitude effects of interference by computing the Euclidian distance between the lattice points. Phase noise can be introduced due to the fluctuation of the oscillators in the transmitters and the performance degradation [83–85] of OFDM systems in the presence of phase noise has been well studied. The example discussed above shows such a case, where the same phase error on the outlier would have a much larger change in the euclidean distance between the outlier and the lattice points.

3.5 CPRecycle

Considering the aforementioned issues with using simple statistical metrics for decoding, we design CPRecycle , a novel OFDM receiver that creates an interference model from the preambles to effectively utilize the opportunities provided by the redundant samples in the cyclic prefix.

3.5.1 Modeling the effect of interference

In OFDM based systems, the symbols with data is usually preceded by one or more training symbols of known data called preambles for channel estimation and synchronization. These preambles typically use a robust modulation scheme that can be decoded even at low SNR values. In CPRecycle receiver, using the P ISI free segments of each of the preambles, P complex values are generated for each subcarrier with every preamble symbol. These P complex values can be used to create a model of the interference effects. We now discuss the various issues that needs to be addressed in generating such a model.

The first hurdle with using the preambles to generate a model is that the modulation schemes in preambles and the data symbols could be different. Lattice codes are generated by selecting a finite number of points from a two dimensional Euclidean space $\mathcal{R}^n$ depending on the modulation scheme. Hence the received signal in the preambles cannot be directly used to create a model for the data symbols to use. To facilitate this, we compute the variations of the received signal in different FFT segments relative to the lattice point being considered. It can now be applied to a signal corresponding to any lattice point and hence used across different modulation schemes.

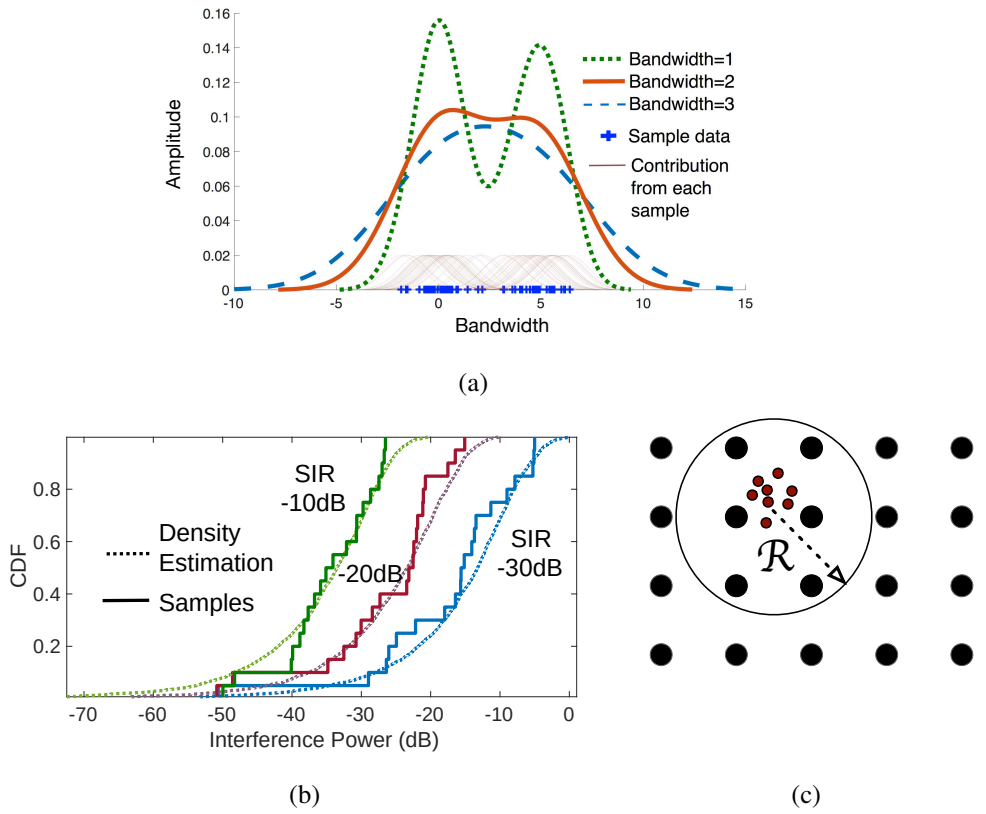

Figure 3.10: (a) Kernel density estimation with varying bandwidth; (b) Density estimates and samples of amplitude variations showing accurate modeling for different SIR scenarios; (c) Illustration of lattice points with a sphere of radius $\mathcal{R}$ centered at the centroid of signal received in 7 FFT segments.

Another issue is the limited number of samples that are available to create and use the interference model. Most of the OFDM standards use utmost two preambles for channel estimation and in each preamble the maximum number of samples for each subcarrier is the number of samples in the cyclic prefix. Furthermore, since the receiver does not possess any information about the interference, it is not accurate [86] to assume a standard probability distribution (e.g., gaussian). Hence care has to be taken to design a non standard probability distribution that works well with a small sample size.

Finally, there is the need to decouple the amplitude and phase effects of interference in different FFT segments, mainly because there is no correlation between them. In scenarios with strong interference, it is reasonable to expect that the interfering signal is carrying data that either amplitude or phase modulated. In such cases too it is beneficial to consider phase errors independently. Also, with amplitude and phase er-

rors decoupled, a weighted function can be used to tune the impact of these errors to improve the accuracy of the interference model.

Based on the issues discussed above, to effectively utilize the opportunities provided by the redundant samples in the cyclic prefix, we need a non-parametric density estimation from the amplitude and phase changes in the different FFT segments that works well with a small sample set.

The simplest method to estimate the probability density of the interference is to use bins of constant or variable width in phase and amplitude and construct a bivariate histogram. However, there are two main problems with using bivariate histograms to model the effect of interference in our context: (i) with a small sample set there are discontinuities in the estimated density due to empty bins (ii) it assumes that there is no relation between the data in adjacent bins.

So we instead employ a more effective alternative called kernel density functions [87–89] to generate a non parametric density. Unlike histograms, kernel density functions does not have discontinuities and can produce a smooth distribution with a small sample set. Furthermore, the amplitude and phase changes can be integrated using a bivariate product kernel density function where the weight for amplitude and phase variations can be tuned.

In order to generate a probability density function with the preamble data in each subcarrier, we use a bivariate gaussian product kernel density estimation function with a variable bandwidth. Let $R_A^j[f]$ and $R_\phi^j[f]$ denote the set of amplitude and phase variation values observed on a subcarrier f, $1 \leq j \leq P$, from the preambles, which can be computed as:

$$R_A^j[f] = \mathcal{A}(\hat{X}_s^j[f] - X_s[f]), \quad 1 \leq s \leq N_p, \quad 1 \leq j \leq P$$
$$R_\phi^j[f] = \Phi(\hat{X}_s^j[f] - X_s[f]), \quad 1 \leq s \leq N_p, \quad 1 \leq j \leq P$$

where N_p is the number of preambles used in modeling the interference. Then the

probability density function can be written as:

$$f_m(a_{obs},\phi_{obs}) = \frac{1}{P*N_p}\sum_{j=1}^{P*N_p}\left[K_a(\frac{a_{obs}-R_A^j[f]}{B_a}) \times K_\phi(\frac{p_{obs}-R_\phi^j[f]}{B_\phi})\right]$$

where,

$$K_a(a) = \frac{1}{2\pi}e^{-a^2/2} \text{ and } K_\phi(p) = \frac{1}{2\pi}e^{-p^2/2} \tag{3.4}$$

B_a and B_ϕ are the kernel-bandwidths which are smoothing parameters that determine the range of amplitude and phase over which the sample points are averaged to generate the probability density.

It is well known that the choice of the kernel-bandwidths has a significant impact [90] on the accuracy of density estimation and it is crucial to identify right value. To illustrate this consider an example of a set of amplitude variations along with the kernel density function with three different bandwidths shown in Fig. 3.10(a). Larger bandwidths result in over smoothing of the density estimate and smaller bandwidths introduce large errors between the data points. In general, it is beneficial to have a larger bandwidth at low densities and a smaller bandwidth at high densities of data.

In CPRecycle , we use the data driven approach to determine the best bandwidth which is possible in the presence of at least two preambles. The Gaussian kernel density function shown above generates a smooth bivariate density function and the probability density function is recomputed each time a new set of preambles are received.

The density estimation of amplitude variations and the variations observed in the data symbols, for different SIR values are shown in Fig. 3.10(b). The kernel density functions accurately predict a density that is applicable for the amplitude variations in the data symbol.

3.5.2 Maximum likelihood decoding

To decode the received symbols $\hat{X}_s[f]$ to the correct lattice point, we use a maximum likelihood decoder that identifies the lattice point with the maximum probability of the received symbol corresponding to that point. When only one FFT segment is used, the maximum likelihood decoder reduces to a minimum Euclidean distance decoder that

identifies the codeword that is closest to the received symbol. However, with CPRecycle receiver, each symbol transmitted on a subcarrier results in P received symbols, one per FFT segment.

Let the transmitted symbols $X_s[f]$ be drawn from a known finite alphabet $\mathbb{L} = \{l_1, l_2, \cdots, l_k\}$ each corresponding to a point in the lattice. The maximum likelihood decoder can be defined as:

$$l^* \triangleq \underset{X_s[f] \in \mathbb{L}}{\text{argmax}} \quad \mathcal{P}(X_s[f]|\hat{X}_s[f]) \tag{3.5}$$

where

$$\mathcal{P}(X_s[f]|\hat{X}_s[f]) = \prod_{j=1}^{P} \frac{\mathcal{P}(\hat{X}_s^j[f]|X_s[f])}{\mathcal{P}(X_s[f])}$$

where $\mathcal{P}(X_s[f])$ sent is constant and $\mathcal{P}(\hat{X}_s^j[f]|X_s[f])$ can be computed from the probability density function defined in Eq. 3.4 as follows:

$$\mathcal{P}(\hat{X}_s^j[f]|X_s[f]) = f_{X_s[f]}(\mathcal{A}(\hat{X}_s^j[f] - X_s[f]), \Phi(\hat{X}_s^j[f] - X_s[f]))$$

With higher modulation schemes the search space for the decoder increases exponentially with the number of lattice points (as 2, 4, 16, 64, 256 for BPSK, QPSK, 16QAM, 64QAM, and 256QAM respectively). Hence it is essential to reduce the number of possible lattice points for comparision. In CPRecycle , to select a subset of possible lattice points we use the concept of a fixed sphere decoder.

The concept of a fixed sphere has been shown to be effective [91–93] to reduce the search space in identifying the closest lattice point. For single antenna receivers, the decoder searches through the lattice points that are located within a sphere of radius $\mathcal{R}$ centered at the received signal. However, a slight variation is required in our case since the decoder receives P signal values from which the lattice points need to be identified, instead of one.

In CPRecycle , to identify the point around which the sphere is centered, we compute the centroid of the cluster of P complex signal values. The centroid is simply the average of the real and imaginary values of all the P values. Only the subset of lattice points that fall in the sphere of radius $\mathcal{R}$ from the centroid of the P samples constitute the search space for the decoder. The choice of lattice points for a sphere decoder is illustrated in Fig. 3.10(c). In this instance, only the six lattice points that fall within the

sphere are considered as possible transmitted codes by the decoder. This significantly reduces the number of operations required in decoding the received symbol.

3.5.3 Putting It All Together

Input: B_a,B_ϕ,$\mathcal{R}$,$\hat{X}_s$,P
Output: X_s
if *OFDM Symbol s is a preamble* **then**
  for *each segment* $j \in \{1,2,\cdots,P\}$ **do**
    $Y_s^j = FFT(y_s^j)$ $R_A^j[f] = \mathcal{A}(Y_s^j[f] - X_s[f])$, $\forall f \in \mathcal{F}$ $R_\phi^j[f] = \Phi(Y_s^j[f] - X_s[f])$, $\forall f \in \mathcal{F}$
  end
end
else
  for *each subcarrier* $f \in \mathcal{F}$ **do**
    $L^c \subset L$ s.t. $\forall l \in L\ l \in L^c$ if $\mathcal{A}(l - \text{Centroid}(\hat{X}_s[f])) < \mathcal{R}$
    $X_s[f] = \underset{l \in \mathbb{L}^c}{\text{argmax}} \quad \mathcal{P}(l|\hat{X}_s[f])$
  end
end

Algorithm 2: CPRecycle

Algorithm 1 shows the overall procedure followed by CPRecycle receiver from putting the above components together. When CPRecycle receiver receives a preamble, it computes the number of ISI free samples in the CP to determine P. The P segments in the preamble are used to generate a unique probability density function for each subcarrier. These probability density functions are constantly updated when subsequent preambles are received. Once the interference is modeled, the subsequent OFDM symbols are decoding using the maximum likelihood decoder. The set of lattice points over which the maximum likelihood detector searches for the transmitted symbol is computed using the radius R which is an input parameter to the CPRecycle receiver.

Note that from the above description it is clear that CPRecycle receiver does not need to explicitly know the precise nature of interference (e.g., adjacent channel interference, co-channel interference). It can leverage the preambles used for channel estimation. The effectiveness of CPRecycle relies on the extent to which channel and interference characteristics seen from a preamble apply to the subsequent OFDM symbols with data. For rapidly varying or sporadic interference, more frequent preambles are needed to accurately model the interference.

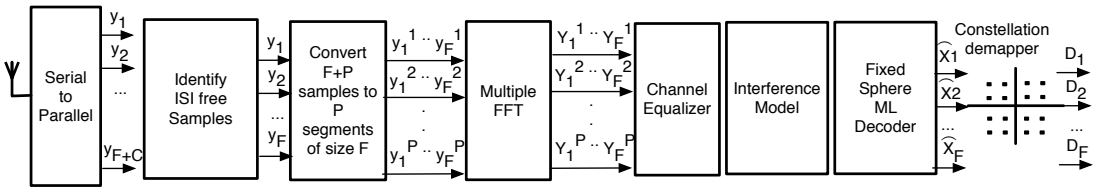

Figure 3.11: Block diagram of CPRecycle receiver as implemented.

3.6 Experimental Evaluation

In this section, we experimentally evaluate the effectiveness of CPRecycle in mitigating different types of interference that can be mapped to practical scenarios.

3.6.1 Implementation

We have implemented a prototype of the CPRecycle receiver using the USRP radio platform [94], Ziria [95] an SDR programming environment, and the GNU Radio software package [96].

CPRecycle Receiver: We implement two variants of the CPRecycle receiver to run on the USRP: (i) IEEE 802.11g receiver (ii) A generic configurable OFDM baseband receiver. For the IEEE 802.11g receiver, we modify the GNU Radio based receiver [96] as shown in Fig. 3.11. Instead of discarding the CP, the ISI free portion of the CP is used to generate P segments that are then passed on to the FFT block to generate P values for each subcarrier corresponding to the signal transmitted on an individual subcarrier. The maximum likelihood decoder then detects the signal transmitted on the subcarrier using the interference model generated with the preambles for each subcarrier.

IEEE 802.11g Setting : The CPRecycle receiver is applicable to IEEE 802.11a/g/n radios which are based on an OFDM PHY. For our experiments we use an off-the-shelf 802.11g Linksys access point running tomato firmware. Each 20MHz channel is composed of 64 subcarriers, spaced 312.5 KHz apart, of which 52 subcarriers are used for data and 4 subcarriers for pilots. Each OFDM symbol has a duration of 4μsec. and each data payload is preceded by a long training field that contains two OFDM symbols for a duration of 8μsec, to enable synchronization and channel estimation. The variation of the signal in different segments in this long training field is used to create the interference model. For our experiments, we choose three MCS modes, QPSK 1/2 (9 Mbps), 16-QAM 1/2 (24 Mbps), and 64-QAM 2/3 (36 Mbps).

3.6.2 Results

We now evaluate the performance of CPRecycle in the presence of adjacent channel interference and co-channel interference.

3.6.2.1 Adjacent Channel Interference

Single Interferer. For the adjacent channel interference case, we use an off-the-shelf 802.11g access point (Linksys) that continuously transmits 400 byte packets, in channel 11 (2462MHz). To generate interference, we use a USRP (B210) to continuously transmit 802.11 traffic in an overlapping channel, in this case channel 8 (2447MHz). A CPRecycle receiver running on another USRP B210, that is capable of decoding 802.11g packets is placed in a fixed location. To choose the appropriate SNR for each MCS, the Linksys router is re-positioned from the receiver until that MCS mode has the highest throughput. Once the SNR for the MCS mode is fixed, the SIR is varied by moving the interferer that generates 802.11 packets in the adjacent channel. We transmit a total of 2000 packets for each scenario and the average values for packet success rate is shown in Fig. 3.12.

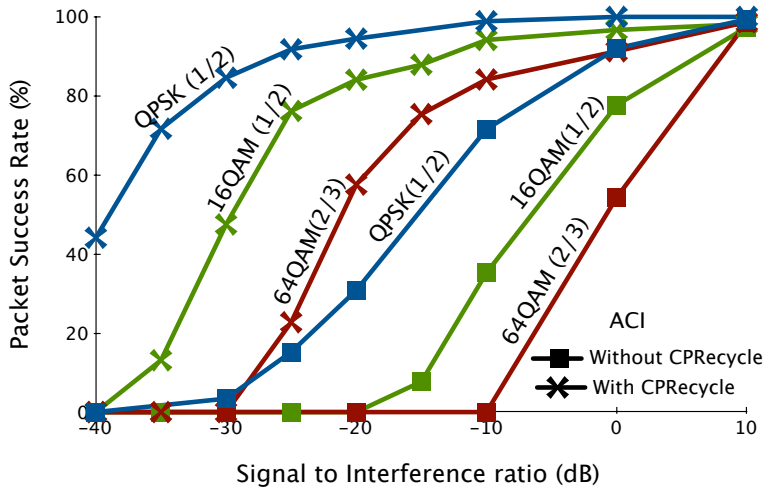

Figure 3.12: Packet success rates for different modulation and coding schemes with one adjacent channel interferer

The severity of the effect of adjacent channel interference on the packet success rates can be seen from the figures. At an SIR value of 0dB, where the power of the signal and the interference is the same, the success rates of packet delivery drops significantly for all MCS modes. Being the highest rate, 64QAM suffers almost 50% packet

loss and is unable to transmit a packet when SIR is -10dB. This effect is slightly less pronounced for the lower modulation schemes such as QPSK, however, the increase in packet loss rate with SIR is still steep, and becomes unusable when SIR decreases to 10dB.

With the CPRecycle receiver, the packet success rates are significantly improved for all the MCS schemes with similar packet success rates achieved with atleast 15dB of adjacent channel interference and in several cases upto 25dB of adjacent channel interference for lower modulation schemes. Considering the packet success rates at -10dB, for example, it can be observed that for all MCS modes the improvement in packet success rates is significant and with higher modulation schemes communication is made possible (with almost 80% packet delivery rate) that would not have otherwise been possible without CPRecycle receiver.

Multiple Interferers. The effect of two interferers creating adjacent channel interference on either side of the channel allocated to a transmitter is shown in Fig. 3.13. For this experiment, the Linksys access point is allocated channel 10 (2457MHz) and the interferers are allocated channels 7 (2442MHz) and 13 (2472MHz) respectively. This is a common scenario in dense deployments of WLANs where overlapping channels has to be allocated to neighboring access points. The packet success rates is noticeably lower for all the modulation schemes, since the number of subcarriers that are affected by adjacent channel interference is almost doubled. However since the interference model is maintained independently per subcarrier, it does not have a significant impact on the performance of the CPRecycle receiver. For example, when the SIR is -10dB, CPRecycle is able to decode more than 80% of the packets successfully in most of the cases.

Guard band needed with adjacent legacy OFDM transmitter. The effect of adjacent channel interference with different sizes of guard-bands for 16QAM is shown in Fig. 3.14 respectively. For this experiment, the set of subcarriers assigned for the first transmitter is fixed and the set of contiguous subcarriers assigned to the second transmitter is varied to generate settings with different guard-bands between the two transmitters. It can be observed that with CPRecycle the amount of guard-bands required to achieve the same packet success rates is significantly lower for both the modulation schemes. This shows that with CPRecycle , a cognitive radio can be allocated frequencies much closer to a licensed band achieving a significantly more efficient use of the wireless spectrum. For example, considering the case with 16QAM, if a cognitive user is allocated a cluster of subcarriers adjacent to a licensed TV transmitter, whose

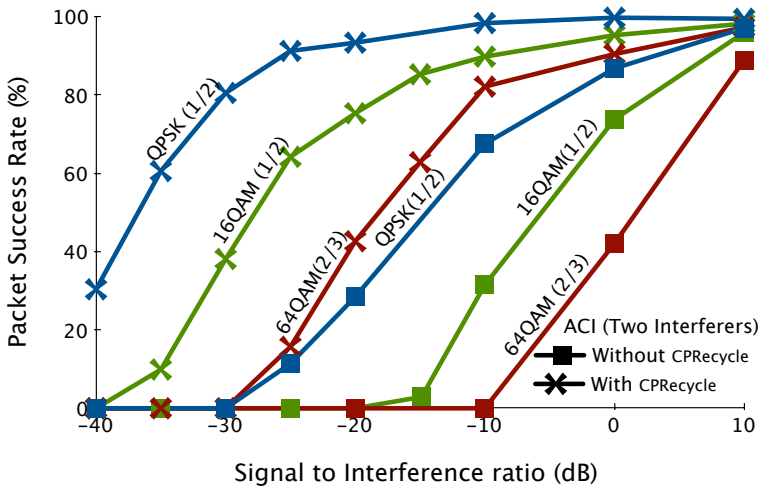

Figure 3.13: Packet success rates with two adjacent channel interferers

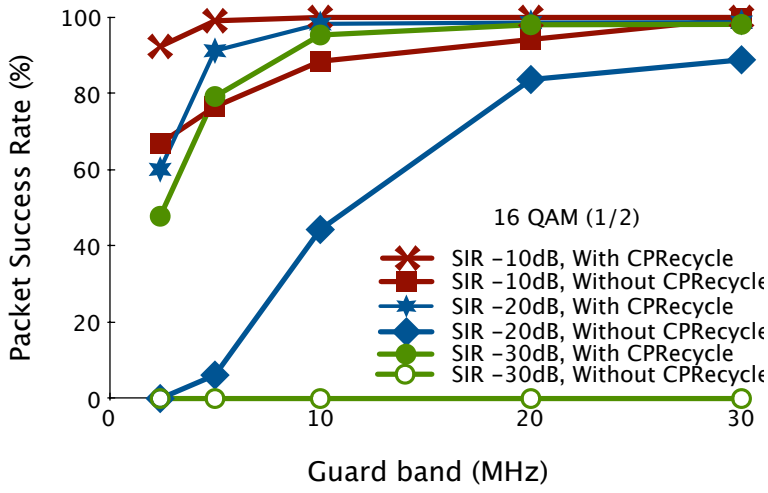

Figure 3.14: Packet success rates with varying guardband sizes with adjacent legacy transmitter

signal is 10 times stronger, then the required guard-band would be reduced from about 15MHz to less than 5MHz to achieve a similar packet success rate.

3.6.2.2 Co-Channel Interference

Single Interferer. To generate co-channel interference, we use a setup that is similar to the adjacent channel interference scenario, except, we use a USRP 802.11 transmitter. This is so clear channel assessment can be turned off to enable simultaneous use of the same channel by both the transmitter and the interferer. Similar to the adjacent

channel interference case, the SNR for each MCS mode is chosen such that any higher modulation scheme would result in a lower throughput. In total, 2000 packets of size 400 bytes, are transmitted for each scenario for each MCS mode and a given SIR setting, and the average packet success rates are computed. The results are shown in Fig. 3.15.

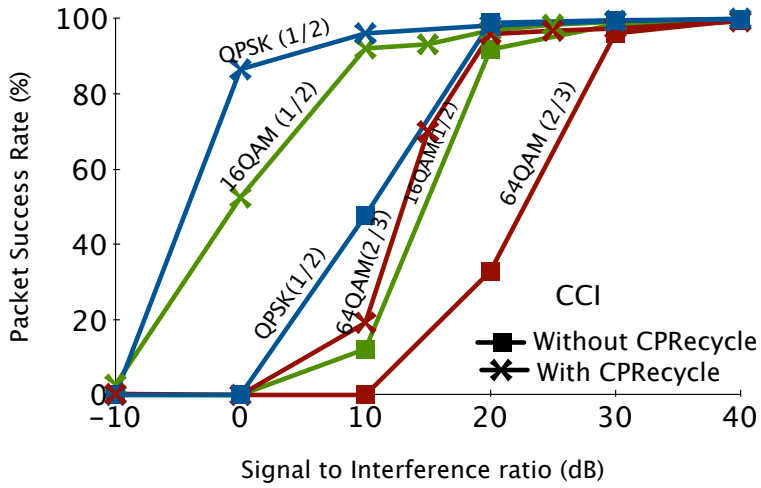

Figure 3.15: Packet success rates for different modulation and coding schemes with single co-channel interferer

As expected, the effect of co-channel interference on 802.11 WLANs is far more severe than adjacent channel interference, which is evident from the figures. Even with SIR 10dB, when the signal of interest is three times stronger than the interference, the packet reception rate drops steeply for all the MCS schemes. This is mainly due to two reasons. (i) Unlike adjacent channel interference, the co-channel interference is in-band. (ii) The number of subcarriers affected by interference is much higher in the co-channel interference scenario. In most cases all the subcarriers used by the transmitter is affected by strong interference.

Another observation is the steepness of the drop in packet reception rates with increasing co-channel interference. The range of co-channel interference tolerated by both with and without CPRecycle receiver is about 15dB in most cases, where as it was about 30dB of adjacent channel interference for most MCS modes. This is mainly due to the significantly higher number of subcarrier affected by interference when compared to adjacent channel interference. However, CPRecycle is able to recover most of these errors since it maintains a separate interference model for each subcarrier from the preamble data.

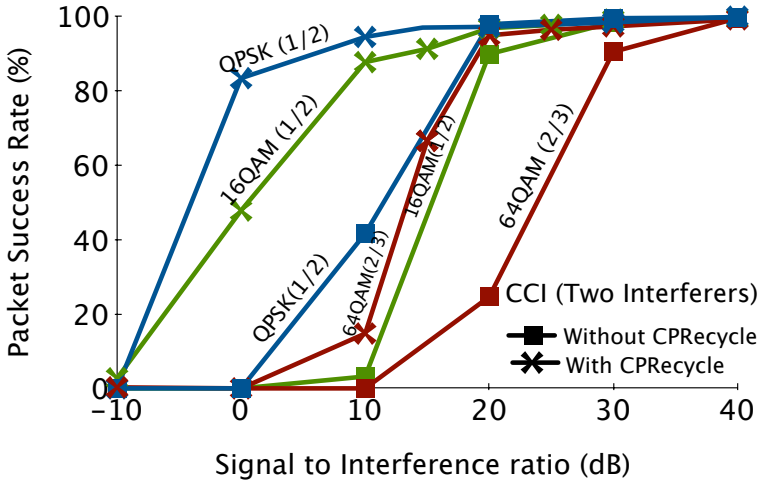

Figure 3.16: Packet success rates with two co-channel interferers

Multiple Interferers. The effect of multiple co-channel interferers is shown in Fig. 3.16. For this experiment, we setup an 802.11 transmitter with carrier sensing disabled, and two interferers in the same channel, placed at the same distance from the transmitter. The SNR is chosen for each MCS mode similar to the other experiments. The SIR is varied by increasing the transmit power in both the interferers. It can be observed that unlike in the case of adjacent channel interference, co-channel interference does not have a significant impact on packet reception. This can be attributed to the fact that the number of subcarriers affected by the higher number of interferers does not change where as it almost doubles in the case of adjacent channel interference. The improvement in packet success rate with CPRecycle is again significant even though the variance of interference is presumably higher with more interferers, while the total power of the interference remains the same. This is primarily due to the nature of the interference model that considers both amplitude and phase changes in the interference to generate the probabilistic model for each subcarrier.

Network Level Improvements. While it is clear that CPRecycle can decode signals even in the presence of strong interference, the network level benefits of this are not obvious. To highlight this, we plot the CDF of number of interfering neighbors for access points in a real indoor office environment shown in Fig. 3.17. From Fig. 3.15, it is evident that with the CPRecycle receiver, the level of co-channel interference that can be tolerated is atleast 15dB for all the MCS modes. This is a direct measure of the increase in energy detection threshold that the CPRecycle receiver would be able to tolerate without additional packet errors.

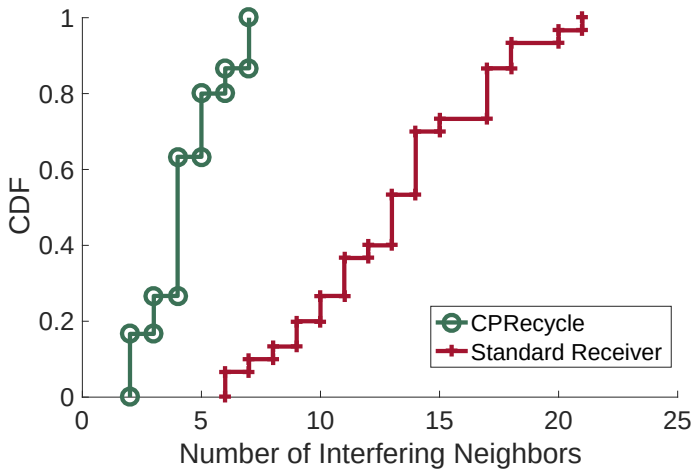

Figure 3.17: CDF of number of interfering neighbors for access points in a real office environment with and without CPRecycle receiver.

We consider our office building [97] which has five floors with a large atirum and most of the walls are made of glass. There are 40 access points deployed in the building with mostly the same place for access points in each floor. We measure the signal strength of access points that can be detected at each of these locations and determine the number of neighbors for the access points by reducing the threshold by 15dB derived from Fig. 3.15. It can be seen that the number of neighbors with CPRecycle is significantly reduced. For instance, with a standard receiver, more than 80% of access points have atleast 12 interfering neighbors where as with CPRecycle more than 80% of the access points have utmost 6 neighbors. This shows how CPRecycle can significantly improve the network capacity of a dense WLAN by reducing the potential interferers in the network.

3.7 Discussion

Detecting ISI free portion of CP : Several methods [98–101] have been proposed in the literature for the detection of ISI-free region in the cyclic prefix. In each of these schemes a correlation coefficient is computed between samples in a given window and a threshold is used to estimate the range of ISI free samples in the CP.

The effect of the duration of the ISI free region over the performance of CPRecycle is shown in Fig. 3.18, where the number of FFT segments represents the duration of the ISI free region. A key observation here is that even when a portion (about 40%) of the

cyclic prefix is unaffected by ISI, CPRecycle is able recover a significant percentage of the erroneous packets. This suggests that CPRecycle can even be used in multipath environments with a significant delay spread.

Computational Complexity and Oversampling: The computational complexity of CPRecycle is O($PN_p^2 f$), where P is the number of ISI free samples in the CP, N_p is the number of preambles and f is the number of subcarriers. Since the number of preambles is not a configurable parameter, we study the effect of P, the number of samples. We conduct experiments for the ACI scenario with varying number of FFT samples, with five preambles to observe the behavior of CPRecycle .

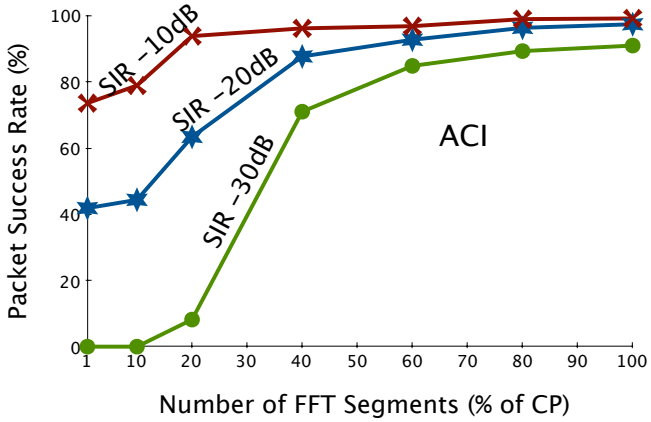

Figure 3.18: Packet success rates with varying number of FFT segments

The packet success rate for three different SIR conditions with 16QAM modulation is shown in Fig. 3.18. An interesting behaviour we observe with the number of FFT segments is that, the benefits of the increasing the number of FFT segments for interference modelling saturates when P reaches about 60% of the samples even at very high interference (SIR -30dB). With lower levels of interference, even 20% of the CP is enough to reduce the packet error rates significantly. There are two advantages to this behaviour with CPRecycle : (i) scenarios with high multi-path delays where the number of ISI free samples in the CP is limited, can still make use of CPRecycle to improve the performance of the receivers. (ii) on devices with limited computational capability the number of FFT segments can be tuned to the capabilities of the device, which gracefully degrades to a standard OFDM receiver with one FFT segment, in the worst case. Hence it can be used in a wide variety of hardware configurations with varying computational capabilities.

When unconstrained by computational capability, it is also beneficial to increase

P beyond the number of ISI free samples available in the CP. This is possible through oversampling with new devices that support higher sampling rates.

3.8 Summary

In this chapter, we presented CPRecycle, an improved OFDM receiver that improves spectral efficiency by decoding packets in the presence of interference. Cyclic prefix is typically unused at the receiver and results in a significant overhead. Exploiting the fact that OFDM based wireless standards over-provision the cyclic prefix (CP) that is meant for preventing inter-symbol interference, we presented a novel OFDM receiver design called CPRecycle that takes advantage of the redundant portion of the cyclic prefix towards interference mitigation. Specifically, CPRecycle models the effect of interference in each subcarrier using a Gaussian kernel density function using the preamble symbols and uses a fixed sphere maximum likelihood detector to decode the following data carrying OFDM symbols subject to interference. Using off-the-shelf IEEE 802.11g transmitters and interferers, we experimentally show the effectiveness of CPRecycle for mitigating adjacent-channel interference and co-channel interference. We also show that two preambles and small portion of cyclic prefix are sufficient to realise significant benefits in terms of packet success rate with CPRecycle .

Chapter 4

Privacy in Home WiFi Networks

4.1 Introduction

Home networks have become an unremarkable part of our lives [102]. The IEEE 802.11 a/g/n/ac standards, or commonly referred to as WiFi [103] are among the most popular solutions for creating personal area networks in homes. The latest standard IEEE 802.11ac can support a throughput in the upwards of 1 Gbps using techniques such as channel aggregation and multiple-input multiple-output. It can support bandwidth hungry in-home applications such as 4K TV that requires about 32 Mbps data rate, or wireless virtual reality headsets that can require several 100 Mbps of bandwidth for a seamless user experience [104].

A typical home network is composed of a WiFi access point to which one or more WiFi clients are connected to. The access point is in turn connected to the Internet and creates a wireless local area network that is used to connect devices such as smart phones, televisions and computers. The WiFi network can be configured to use encryption to keep the communication private. There are however, two problems this approach. Not all data is encrypted as management frames are sent in clear text, which can be used to identify devices present in the environment. Second, the size preserving nature of encryption mechanisms used in WiFi, reveals the traffic characteristics in the network. This information can in-turn be exploited to determine private activities of the home occupants.

In this chapter, we explore the challenges in encrypted home WiFi networks to preserve privacy of its home occupants. Specifically, we study the possibilities of determining the occupancy state of a home and the activity of its occupants, using passively sniffed encrypted WiFi traffic from that home environment. First, a background on

various passive attack vectors is presented followed by the results of experiments conducted in dual-income homes over a two week period. A manual analysis of the signal collected in these home environments shows that this information can be used to reveal occupancy states and some activity classes such as watching television and sleeping. With this insight, we propose *WiFi Glass*, an attack vector that uses deep learning to identify the occupancy state and activity of a home (limited to three activity classes). Evaluation of WiFi Glass shows that it achieves high accuracy in determining, both, the occupancy state and activity class of a home, from only passively collected WiFi signal. The chapter is concluded with a short discussion about promising directions for countermeasures.

4.2 Background

In the past, several attack vectors [105] on home WiFi networks have been identified. In this section we discuss some of these attack vectors that have significant impact in the security of home WiFi networks. They can broadly be classified into active and passive attack vectors. Active attacks involve transmitting some signal either to crack encryption, gain access or to disrupt communication between legitimate devices. We limit our scope to passive attack vectors and for a discussion of active attack vectors on WiFi networks, refer to [106].

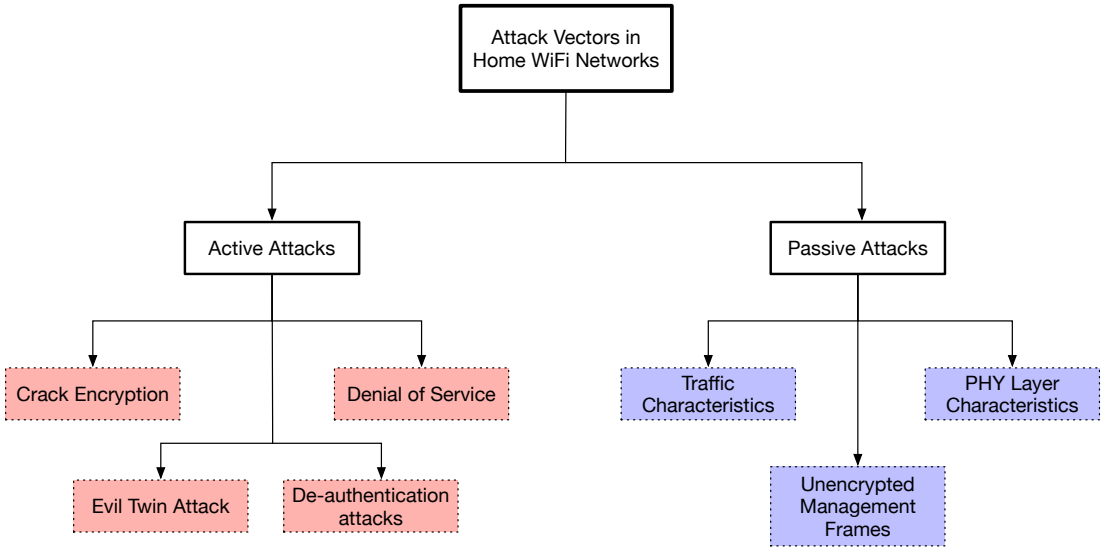

Figure 4.1: Attack vectors relevant to WiFi networks in home deployments

4.2.1 Passive Attacks

Passive attacks in WiFi networks involve scanning the wireless medium and attempting to gain information from the sniffed packets. In WiFi, a packet transmitted by a device can be received by any other device, provided it is with in range of the transmitter. WiFi clients that receive these packets check the MAC address in the destination address of the received frame and drop them if it is not intended for them. However, WiFi sniffers that work in ”monitor” mode can ignore this MAC address check and pass along all the received WiFi frames up the network stack. Tools such as Wireshark [107] and Kismet [108] can be used to decipher these packets and are available for free in the Internet.

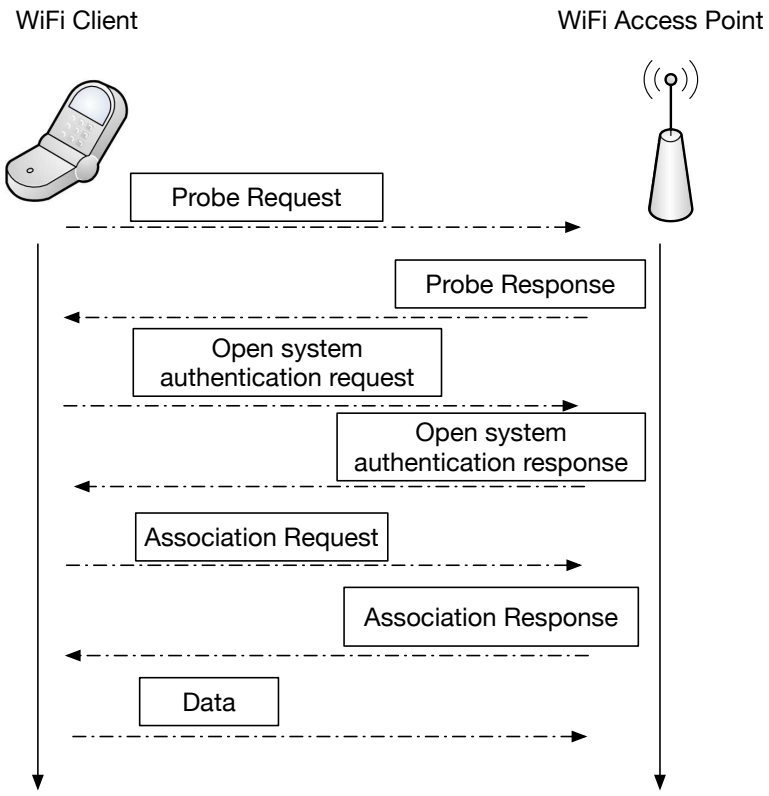

Figure 4.2: Illustration of Active Scanning by WiFi Clients.

One of the main vulnerabilities that are available for an adversary using passive attacks are the unencrypted management data transmitted in the control packets. WiFi uses three types of frames for communication, namely, data, control and management frames.

- The data frames are used to carry encrypted data across the shared medium.

- The control frames are used to coordinate communication among different clients and the access point, which include the Request-to-Send and Clear-to-Send and ACK messages.

- The management frames are used for network management tasks such as association, authentication and de-authentication.

The control and management frames are not encrypted and the information in these frames can be used to decipher side channel information about the network and its users.

4.2.1.1 WiFi Probe Requests

WiFi clients can passively listen for beacons from nearby access points to discover and connect to them [109]. However, the demand for cloud services on smart phones creates a need for a constant connection to the Internet. In order to enable client devices to actively discover WiFi access points in their environment, IEEE 802.11 defines a service discovery process that uses management frames called probe requests. The client device can either transmit *undirected* (broadcast) or *directed* (unicast) probe request frames and would wait for the access points in the vicinity to respond with a probe response. The devices then proceed to exchange authentication and association requests to establish a connection as illustrated in Fig. 4.2. Once the connection is established the client is able to send and receive encrypted data with the access point.

The probe request messages can be either broadcast or unicast to specific access points. Unicast probe request messages are used to connect to WiFi networks that do not broadcast their SSIDs. Whereas, broadcast probe request messages would be answered by any access point. In general, unicast probe request messages are rare when compared to broadcast probe messages [2]. In case of a lack of response, the client device periodically broadcasts the probe request frames until it receives a response as illustrated in Fig. 4.3.

There are several ways in which WiFi probe request messages improve quality of service. First, service discovery using beacons from access points are slow and requires the clients to keep their radio on for a much longer duration leading to high energy consumption [110]. With the use of probe messages, the client only need to keep the radio on for a few milliseconds (to wait for a probe response) before turning it off the save power. Otherwise, the client needs to keep the radio on until a beacon

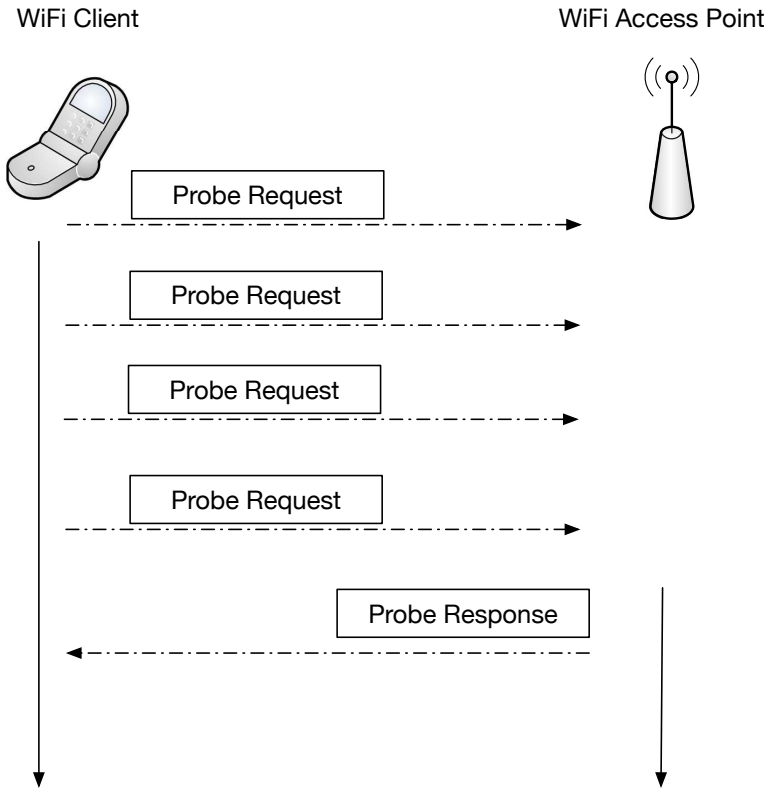

Figure 4.3: Illustration of Active Scanning showing periodic probe request messages by WiFi Clients.

is received from the access point leading to high energy use. This is also helpful for mobile clients to quickly switch access points to maintain an uninterrupted connection.

Second, WiFi probe request messages enable a mobile phone to stay connected to the access point even when its in sleep mode. The regular WiFi probe request messages are used as keep-alive beacons that lets the access points know that the client is still connected. Finally, the only way to connect to (hidden) WiFi networks that do not broadcast their SSID, is to use probe request frames, since the access point does not send beacons for service discovery. While this provides the access point certain degree of privacy compared to broadcasting, the SSID is in the open. However, this has unintended consequences, since the onus of privacy is now transferred to the mobile clients who need to transmit probe request messages with the SSID of the access point. Hence the WiFi probe request is a standard feature in most existing WiFi chipsets and is also enabled by default.

The service discovery process in WiFi networks cannot be encrypted since no cryp-

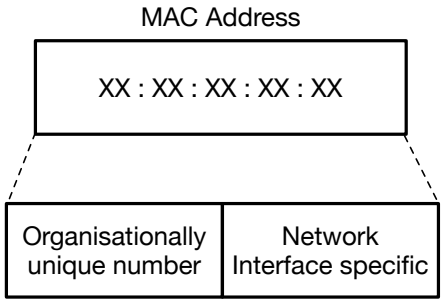

Figure 4.4: 48 bit MAC Address

tographic key has been shared prior to association [111]. Recently, WiFi probe request frames have generated a lot of interest [1, 2, 112–127] and the transmission of unique MAC address in WiFi probe frames has been shown to lead to various information leaks. Smart phones transmit an alarming number of WiFi probe request packets that can lead to loss of privacy among other problems [1]. On average some smart phones can transmit about 55 WiFi probe messages every hour, increasing upto 2000 probe request messages in some cases.

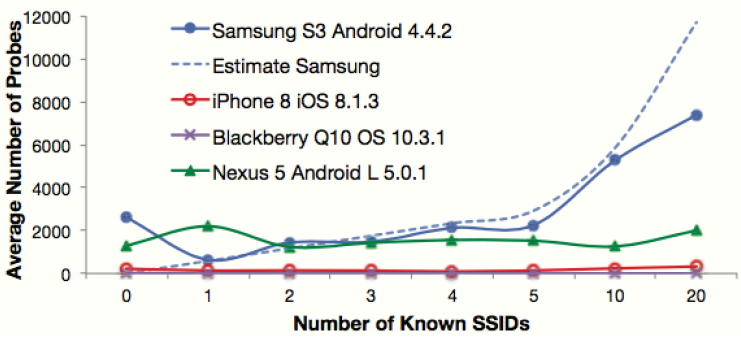

Figure 4.5: Frequency of probe request frame reproduced from [1]

The frequency of WiFi probe request frames are not defined in the IEEE 802.11 standards and is left for the vendors to decide. The frequency of probe request frames transmitted by a smart phone depends on various factors, such as its manufacturer, IEEE 802.11 implementation, and the state of the smart phone (display on/off, WiFi on/off ..etc). Since the transmission characteristics of the WiFi probe request messages has a strong correlation with the state of the device, this information can be used by an adversary to determine the state of the smart phone. For example, Jamil et al [119],

with more than 93% accuracy, is able to determine the (on/off) state of display on the smart phone by analysing the pattern of WiFi probe request messages emanating from the phone.

4.2.1.2 MAC Address and Preferred Networks

WiFi probe requests are considered a security vulnerability due to the fact that they include the MAC address of the client devices in clear text. A MAC address is a 48 bit number that uniquely identifies a network interface [128]. The allocation of MAC address is managed by IEEE Registration Authority [128], and is typically done in blocks of 2^{24} addresses. The first 24 bits represent the Organisational Unique Identifier (OUI) and the last 24 bits represents the network interface card specific identifier. Manufacturers are allocated a MAC address large block (MA-L) that is composed of a 24 bit unique OUI and the right to generate various extended identifiers with the allocated OUI. Hence the first 24 bits can be used to identify the device manufacturer, for example, "Apple" or "Samsung". The MAC address "FF:FF:FF:FF:FF" is reserved for broadcast messages. Most client devices use this unique global identifier as their MAC address. This method of allocation opens an attack vector, where an adversary is able to infer information about the device from just the MAC address. For instance Martin et al, [129] analyse a dataset of 2 billion MAC address of devices and propose a method where the MAC address alone can be used to infer significant information about the device.

The MAC address embedded in the WiFi probe request messages has been exploited for several types of invasion of privacy, such as tracking people [122, 130]. For instance, in the UK, trash cans equipped with WiFi receivers were use to track the movement of shoppers [118]. Several tracking systems have been deployed in public shopping centres to track the movement of customers to gain more understanding. Identifying the MAC address of a mobile device and linking it to its owner are two different problems, with the latter being far more difficult due to the presence of other devices and protection schemes such as MAC randomisation. Cunche [122], shows how a MAC address can be used to link a mobile device to a person/identity in the real world. This can be used to set WiFi booby traps where an action is triggered if a person enters a particular area. This can be performed by simply monitoring the wireless activity and checking for the MAC address in the source address field of the header. Such attacks can be used for various purposes ranging from pranks to proximity weapons.

MAC Randomisation: A common strategy employed by most smart phone and

computer operating systems is to randomise the MAC addresses. While the general principle is the same, the details differ depending on the operating system and the manufacturer. Some device change MAC addresses every 20 minutes and some every few hours. This can provide some protection against MAC address profiling attacks, for instance, in cases the OUI of the MAC address is used to determine the manufacturer. However, all implementation of MAC address randomisation has been shown to fail in providing adequate privacy protection [131]. Using unique fingerprints such as probe burst rate, known SSIDs and pattern of IEs, it is possible to identify the device and link it to the MAC addresses. In the network stack made of several interworking components, the original MAC address is sometimes leaked, for instance, it was recently discovered that the Access Network Query Protocol (ANQP) request on Linux and Windows OSs used the original MAC address in their messages. Such developments have showed the limitations of MAC randomisation in protecting the MAC addresses of WiFi devices.

4.2.1.3 Probe request bursts

Since access points can be allocated any of the WiFi channels, the probe request messages must be sent out in all the channels that the client is allowed to use in the geographical location. Hence the probe messages are usually sent out in bursts in successive channels to enable discovery of access points in these different channels. While this ensures that access points of interest would hear the probe request messages irrespective of the channel they occupy, it also exposes a new side-channel for attack.

The algorithm a client uses to send probe bursts across different WiFi channels varies from one client device model to another. In particular this depends significantly on the operating system and the WiFi chipset in use [132]. For instance, the algorithms used by Samsung Galaxy S5 and Apple iPhone 4 can be visualised from Fig. 4.6. It can be seen how the device sweeps the WiFi channels with its probe request frames. The probe request burst characteristics can be used to accurately fingerprint a device since there is a strong correlation between the burst characteristics and the device model.

4.3 Observations from monitoring Home WiFi networks

In order to understand the severity of information that can be manually inferred from passive sniffing of encrypted home WiFi networks, experiments are conducted in three

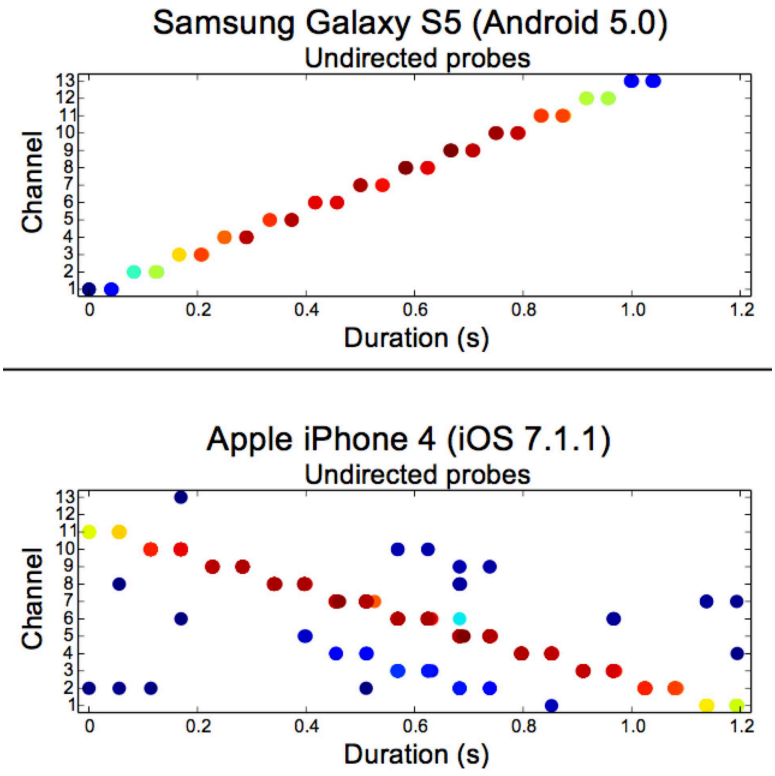

Figure 4.6: Frequency of probe request frame reproduced from [2]

dual-income family homes using passive WiFi sniffers, correlated with ground truth activity information. In this section, we discuss different facets of private information that can be manually inferred from the passively sniffed signal.

4.3.1 Experimental Methodology

To investigate the current state of security in home WiFi networks, we design a portable WiFi sniffer that is capable of monitoring a home WiFi network. We deploy it in the homes of three dual-income families for one week along with a feedback device through which they are able to provide information about various activities such as sleeping, cooking, and watching TV.

We design a portable sniffer that is capable of collecting the encrypted WiFi signals. A schematics diagram illustrating various components used in the device is shown in Fig. 4.7. The sniffer uses Odroid-XU4 [133], an octa-core single board computer that can power a BLADE-RF [134] software defined radio. The Odroid-Xu4 is a good choice for the experiments since it has USB 3.0 ports, supports eMMC storage, and

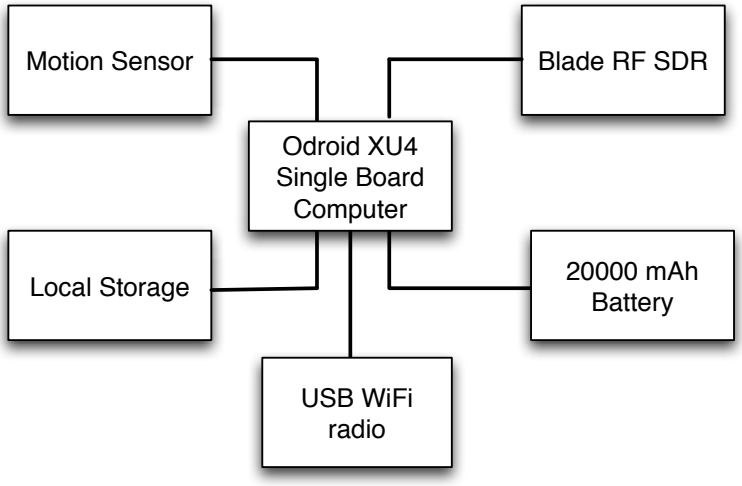

Figure 4.7: Schematics of WiFi sniffer used by a typical rogue agent

is powered by ARM Cortex A15 and A7 octa-core processors. The BLADE-RF pairs well with the Odroid-XU4 single board computer and they are connected through the USB 3.0 port. It is capable of receiving 12-bit 40 MSPS and can be used to scan up to 40MHz of spectrum. We run a modified IEEE 802.11 GNURadio receiver [96] on the Odroid-XU4 with modified firmwares, capable of storing frames to an external storage at line rate.

In order to measure ground truth about home occupancy we include two additional components, 10mm X 10mm push buttons and a pyro-electric infrared sensor (PIR) sensor. The PIR sensor is capable of detecting human presence within its line of sight and has about 135 degrees of wide coverage.

We deploy this device in three family homes in the UK for two weeks. We intentionally choose three families with dual-incomes. The dynamics of home occupancy and activity is significantly different for dual-income families [135]. For instance, most dual-income family homes are unoccupied at regular timings each day, which is not the case with single income homes. Kids tend to stay home alone more in the case of dual-income families. The devices are placed in an easily assessable location and the sniffer is separated from the WiFi access point by two walls or more in all the homes, as illustrated in Fig. 4.8.

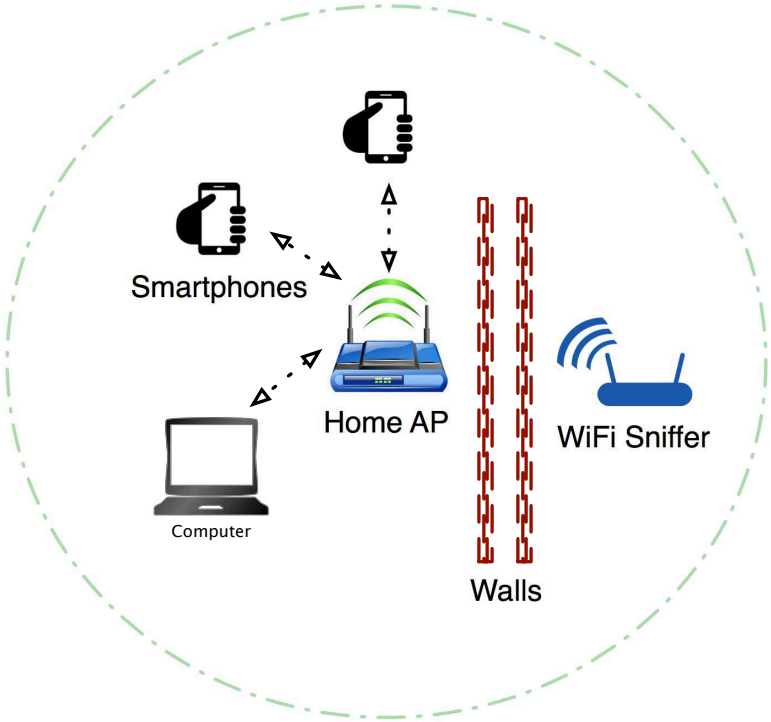

Figure 4.8: Deployment of sniffer in home WiFi network

ID	Income Type	Occupants	WiFi Devices
A	Dual Income	32 years male and 32 years female	9 devices; IPad tablet, IPod music player, ROKU TV, Chromecast dongle, PS3, two laptops, and two apple iPhones.
B	Dual Income	38 year male, 35 year female with two kids, 8 year old boy and 2 year old girl	6+ devices; IPad tablet, Nintendo WII, Smart TV, two laptops, two smartphones and some WiFi enabled toys.
C	Dual Income	30 year male and 28 year female	7 devices; IPad tablet, Sony PSP, chromecast HDMI streamer , two laptop and two smartphones.

Table 4.1: Information about homes involved in the experimental study

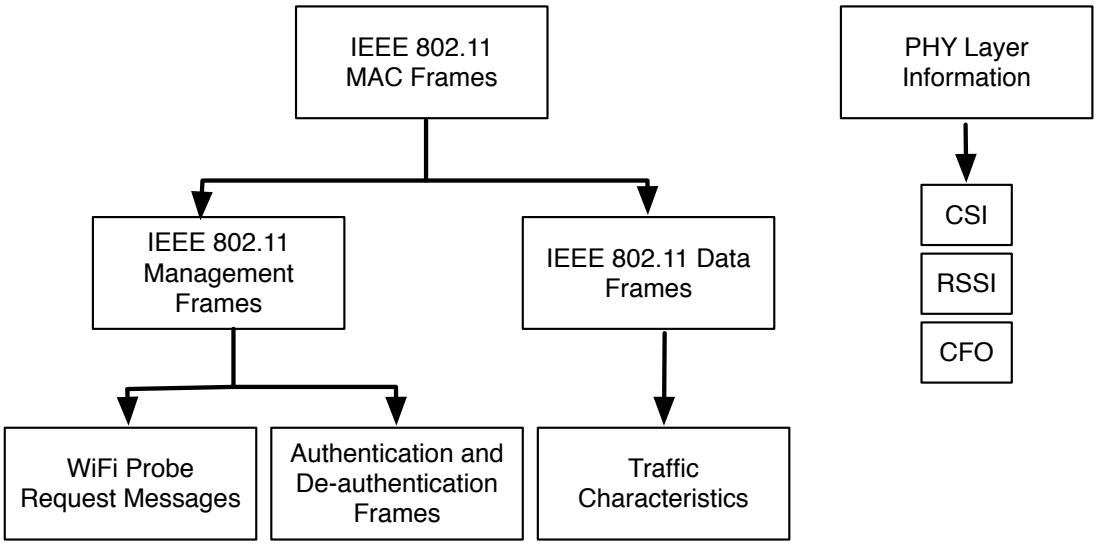

Figure 4.9: Information collected through the sniffer

4.3.1.1 Information Collected with the WiFi Sniffers

The information collected by the WiFi sniffer is classified in Fig .4.9. The IEEE 802.11 MAC frames are processed for management frames and data frames. The data frames are encrypted and hence no useful information can be obtained from the data itself. However, the encrypted data frames can be used to measure traffic characteristics of the home WiFi network which in turn can be used to infer the number of active devices and their activity. This is made possible with the use of encryption schemes that retain the original size of the data. The data frames are processed on the device and the traffic metrics are extracted. We retain all the IEEE 802.11 management frames. In the management frames, of particular interest, are the WiFi probe request/response messages and authentication/de-authentication messages. The WiFi probe messages and its frequency can be used to extract information about the availability and activity of mobile WiFi clients such as smartphones.

We also collect other non-wireless information for ground truth measurements about the occupants presence and activities. The PIR motion sensor provides information about the occupancy of the home. We also provide push buttons on the device for the home occupants to provide ground truth for events such as going to bed, waking up, leaving home, arriving home, and watching TV. We use this information to identify the presence of correlation between the events and the wireless activity.

4.3.2 Information Leaks

In this section, two types of private information that can be inferred from the passively sniffed wireless signal, namely, home occupancy and in-home activity are discussed.

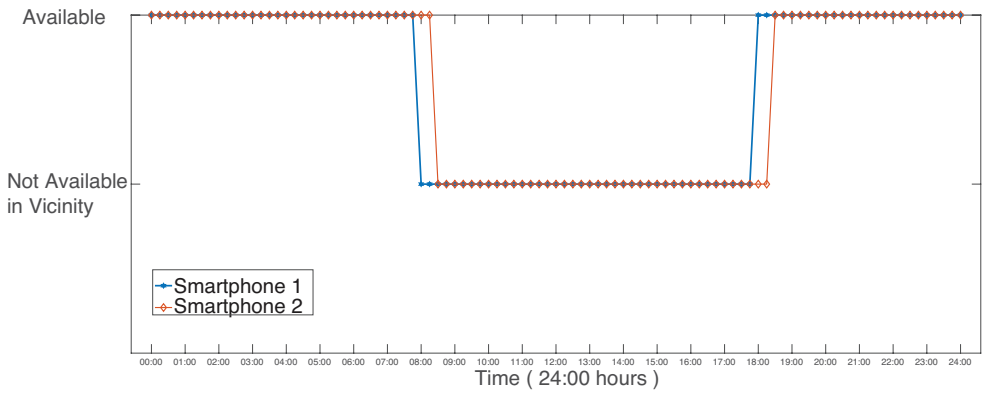

Figure 4.10: Presence of smart phones in vicinity of Home A in a 24 hour period

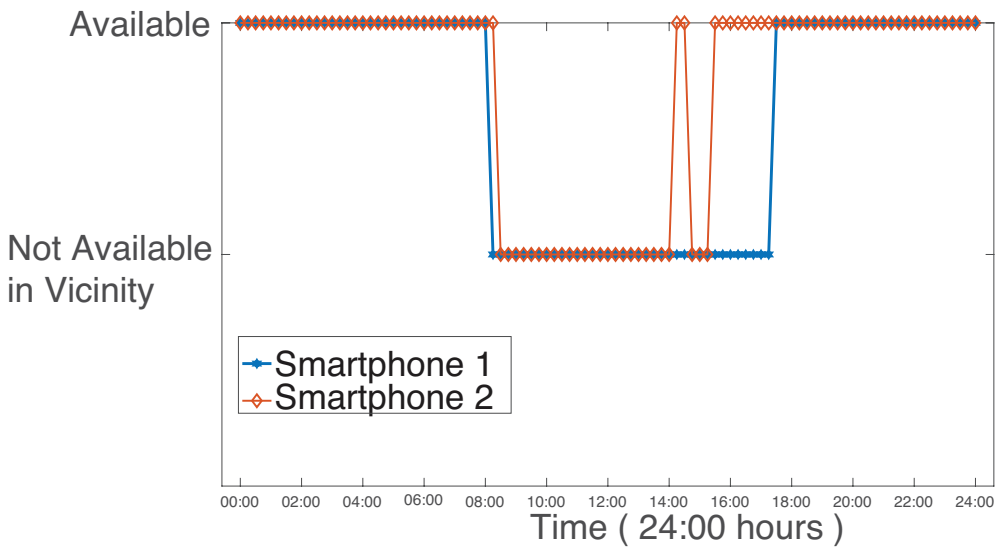

Figure 4.11: Presence of smart phones in vicinity of Home B in a 24 hour period

Home occupancy refers to a set of information related to the current occupancy state of homes. This is privileged information which an adversary could use to target a particular home or its occupants for abuse. The knowledge that a home is unoccupied may increase the number of home burglaries. For instance, an offender could surf the

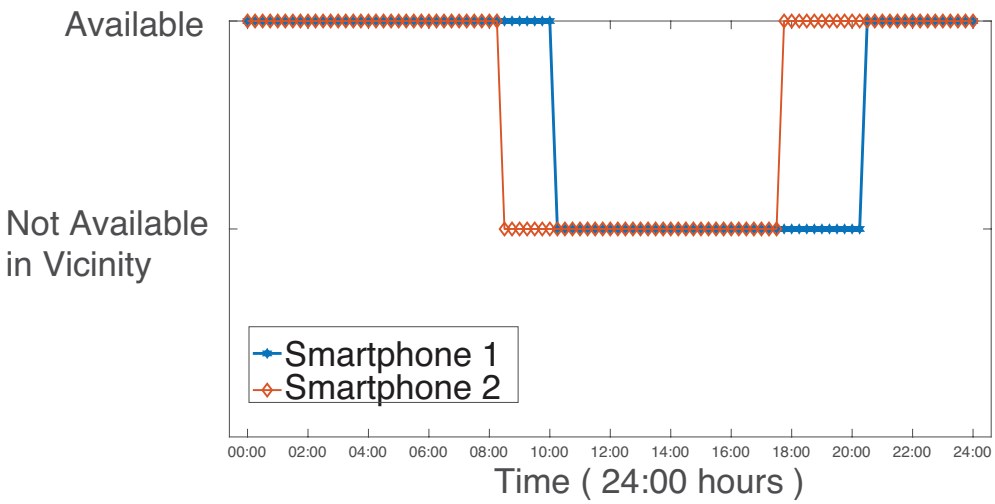

Figure 4.12: Presence of smart phones in vicinity of Home C in a 24 hour period

streets with a portable WiFi scanner or enter a higher rise building (such as a residential flat with multiple units), to identify an unoccupied house to target.

To identify home occupancy, the active devices in the home environment is identified from the sniffed signal data using the management frames. The availability of smartphone in the home environment over a 24 hour period in homes A, B and C are shown in Fig. 4.10, Fig. 4.11, and Fig. 4.12, respectively. We set a duration of 20 minutes of silence from a device to mark it as *not present* in the home. It can be seen that in a 24 hour period, the frequency of WiFi probe request messages can be used to accurately track the presence or absence of the device owner at home. This is helped by the fact that, the smartphones never stop sending WiFi probe request messages, even when they are connected to the home WiFi access point. While this is useful for the smart phone to identify access points with a stronger signal it also enables tracking the presence of smart phones even when they are not in use or in sleep mode.

Another metric that can be used to infer home occupancy without the need to identify devices involves monitoring the traffic between the home access point and the wireless clients in a device agnostic manner. Instead of isolating the smartphones to identify their presence, this method considers the uplink traffic characteristics of the home WiFi access point to the wireless clients. The intuition behind this method is that there is a significant difference in the usage of home WiFi networks when the home is occupied when compared to when its unoccupied. When users are present in the home they generate traffic on the home WiFi network, even when they are not using their

devices due to background activity. We use the notion of active devices to capture this effect. A device is considered active if it receives more than a certain threshold of data within a set period.

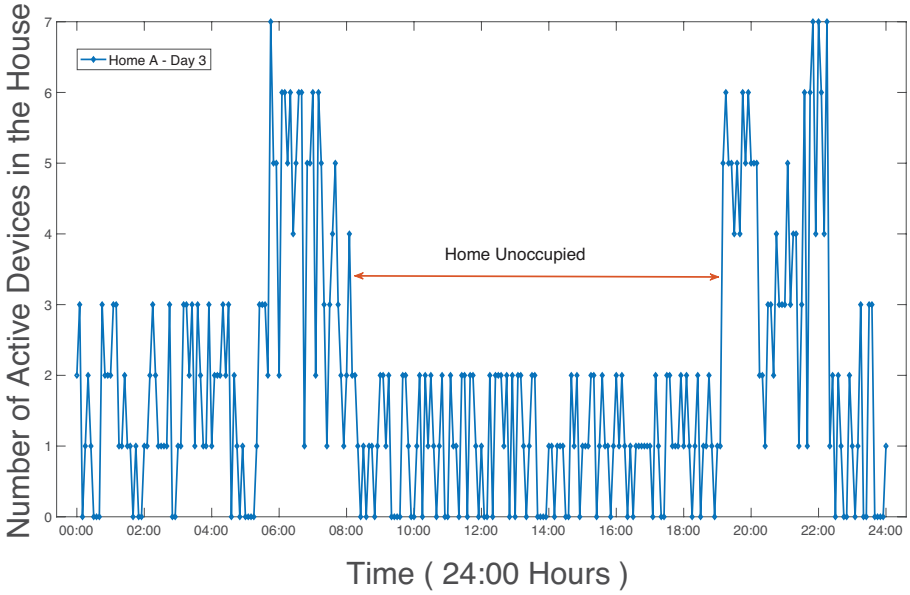

Figure 4.13: Active devices in home A during a 24 hour period

The results collected from the homes show strong correlation between the number of active devices and the number of occupants in all three homes. The number of active devices in a 24 hour time period in homes A, B and C are shown in Fig. 4.13, Fig. 4.14, and Fig. 4.15, respectively. In all three cases, there is a clear drop in the number of active devices when the home is unoccupied, which are due to the smart phones and laptops leaving the home network in these particular cases. It is typical for most people leaving their homes to carry with them some WiFi connected devices such as smart phones, laptops, and music players. This has a clearly observable effect on the in-home network and can be observed by an adversary outside the home premises without the knowledge of the home occupants.

In-home activity such as sleeping or watching television, is private information. One of the basic expectations from the home is that the activities of the occupants are not observable for a stranger from outside. However, the ability of wireless signals to penetrate through walls, while a very helpful feature to provide network coverage for your entire home, it can also be seen by any (rogue) WiFi sniffer just outside the home premises. If the wireless activity can be used to infer physical activities of the

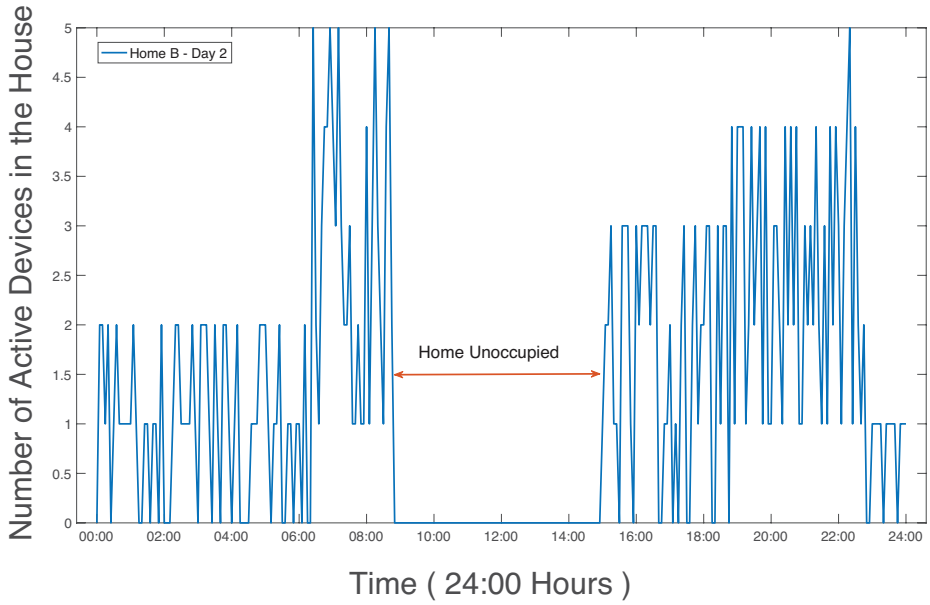

Figure 4.14: Active devices in home B during a 24 hour period

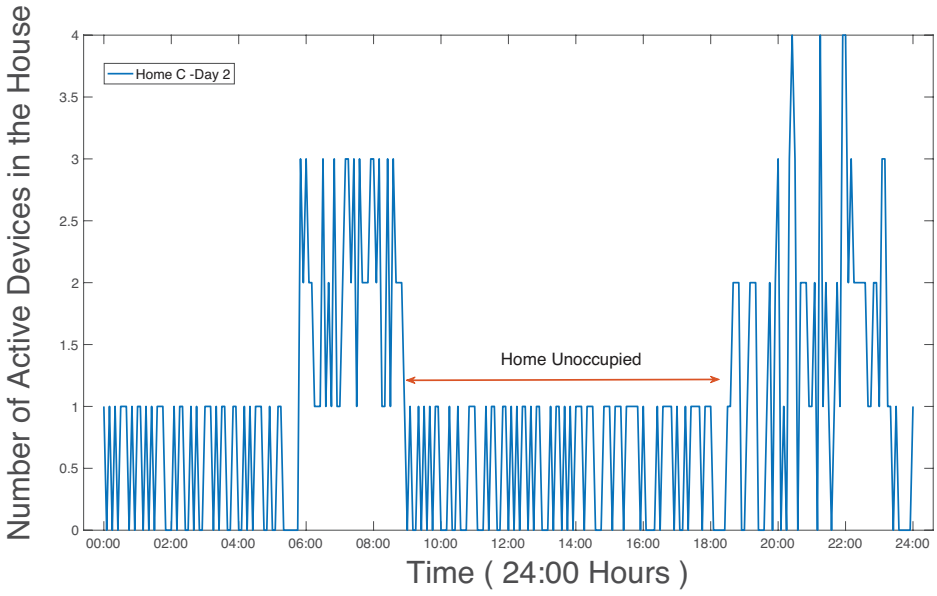

Figure 4.15: Active devices in home C during a 24 hour period

occupants, then that provides an adversary the ability to see through the home walls with a simple WiFi sniffer.

The same concept of active devices can be used to determine some activities such as sleeping. When all the home occupants are sleeping, naturally there is a drop in

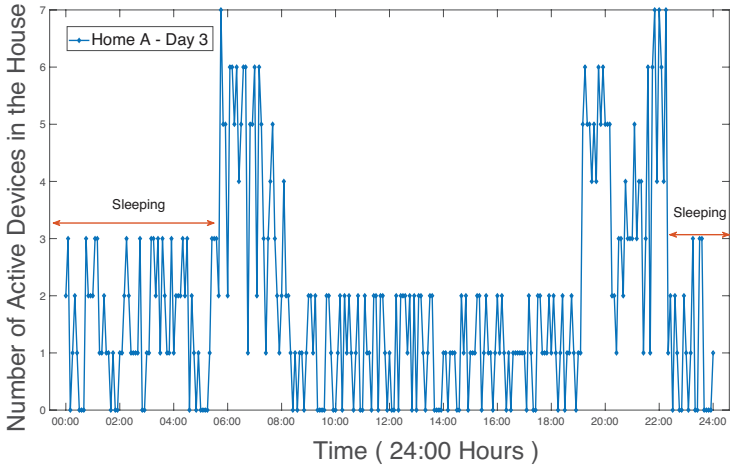

Figure 4.16: Sleep activity in home A

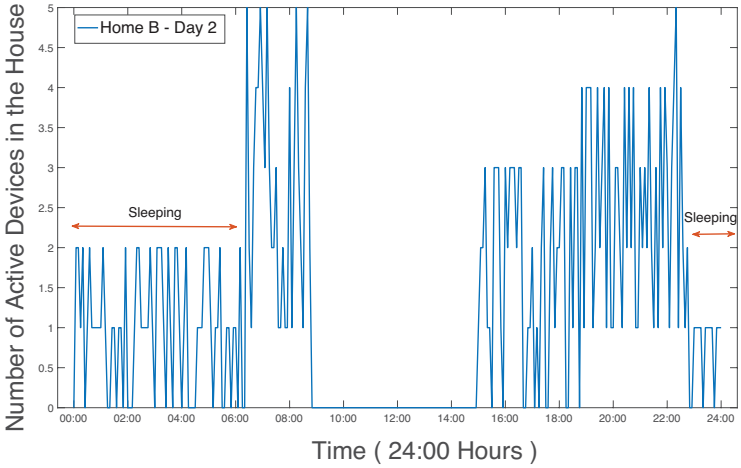

Figure 4.17: Sleep activity in home B

the number of active devices such as televisions and laptops for example. However, smart phones and laptops on standby continue to transmit WiFi probe request messages among other background activity. The number of active devices in a 24 hour period is shown in Fig. 4.16, Fig. 4.17, and Fig. 4.18. In all three cases, the reduction in the number of active devices is clear. Some devices even when not in use continue to transmit WiFi packets due to some background activities while other devices are completely turned off (eg., television) during the time when the occupants are sleep.

Some activities such as watching television can be inferred from fingerprinting the WiFi devices. In our case, the television in the three homes were equipped with

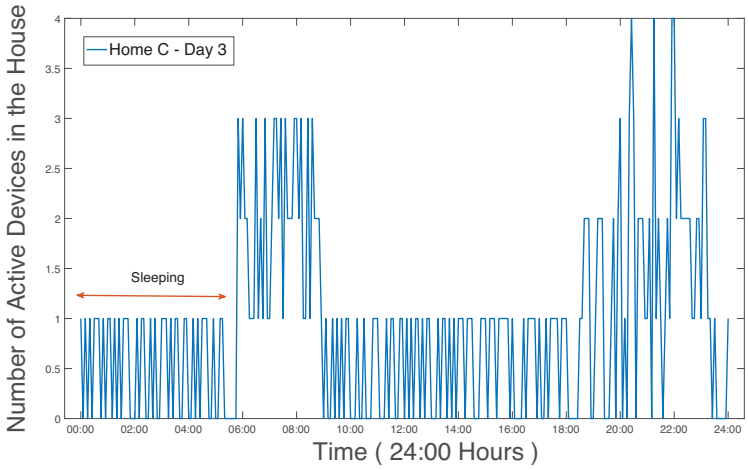

Figure 4.18: Sleep activity in home C

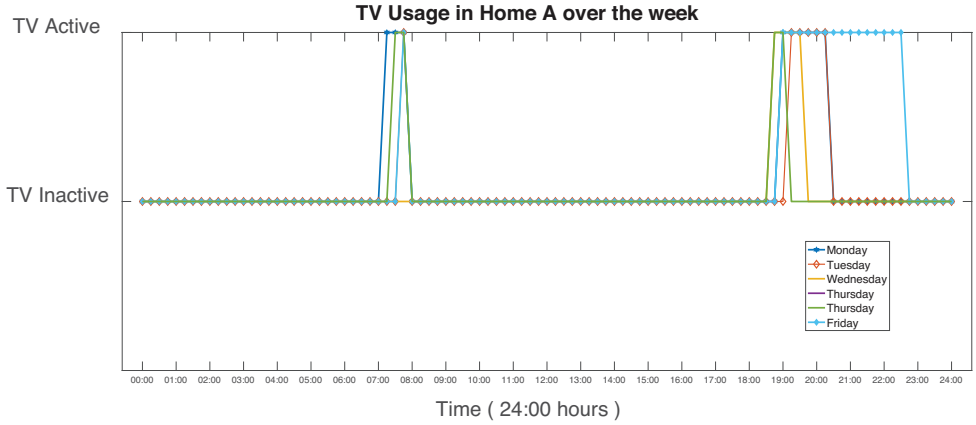

Figure 4.19: Television use in home A

WiFi, either integrated as part of the television or as an accessory such as a streaming player. The MAC addresses were not randomised and unlike smart phones they are not switched on all the time, so it is straight forward to identify the device from the headers. The weekly usage of television in home A is shown in Fig. 4.19. The activity detected from the chromecast corresponds precisely to the periods when the television was on. The granularity can be further improved by reducing the buffer timer for the alive counter.

4.4 WiFi Glass

In this section, we present a systematic method to perform this inference from the wireless signal information, using convolutional neural networks with deep learning. A brief introduction to deep learning is presented, followed by the description of the proposed scheme, referred to as WiFi Glass.

4.4.1 Machine Learning for classification

Recently, machine learning has been shown to solve a variety of pattern recognition and classification problems [136], in some cases, surpassing human ability. In general, the objective of machine learning is to find a function g, that defines the relationship between the set of inputs X and set of outputs Y, given by,

$$g : X \rightarrow Y \tag{4.1}$$

The key difference between legacy pattern recognition techniques and machine learning is that, the model is obtained from data rather than domain knowledge. Specifically, the inputs $X \in \mathcal{R}$ consists of k discrete samples and can be represented as,

$$\mathcal{X} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} \tag{4.2}$$

where, $x_i \in \mathcal{R}^j$ is the feature vector consisting of j observations corresponding to each sample, denoted as,

$$x_\alpha = \left[x_{\alpha 1}, x_{\alpha 2}, \ldots, x_{\alpha j},\right], \alpha = 1, \ldots, k \tag{4.3}$$

Similarly, the outputs corresponding to j samples is given by,

$$Y = \left[y_1, y_2, \ldots, y_k\right] \tag{4.4}$$

The goal of the machine learning algorithm is to learn the mathematical model for the function g from Eq.4.1. Real world observations in the form of,

$$\mathcal{D} = \{(x_1, y_1), \ldots, (x_k, y_k)\} \tag{4.5}$$

are used to train the learning algorithm to determine g.

The accuracy of the learning algorithm is significantly influenced by the choice of features used to train it. In practice, this is a significant limitation, as feature engineering is well known to be both difficult and expensive. As an alternative, *feature learning* is a machine learning technique that allows the system to discover the features automatically, alleviating the need for manual feature engineering. Feature learning can be performed in a supervised or unsupervised setting. In supervised learning, the system learns the features using labeled input data, where as, in unsupervised learning, the system learns using unlabelled input data.

In recent years, deep artificial neural networks also known as, *Deep Learning*, have won numerous contests in pattern recognition and classification using supervised learning. It has been applied to various problems such as image classification, speech recognition, medical imaging analysis and game play. In wireless communication, it has been applied for indoor localisation [137], human activity detection using on body sensors [138], signal modulation [139], and radio burst classification. Refer to [140] for an overview of the application of deep learning in networking.

The basis of most deep learning algorithms is the artificial neural network. An artificial neural network (ANN) consists of three layers (input, hidden and output), each made up of many simple, connected units called neurons, each producing a sequence of real-valued activation a with parameters $\mathcal{P} = \{\mathcal{W}, \mathcal{B}\}$, where $\mathcal{W}$ is the set of weights and $\mathcal{B}$ a set of bias. The activation at neuron t at layer l is give by,

$$a_t = \sigma(\mathcal{W}x + b) \tag{4.6}$$

where, σ is the transfer function, typically a sigmoid or hyperbolic tangent function. The transfer function introduces non-linearity which enables multiple layers to be stacked on top each other. Activation functions that are commonly used in layers are the ReLU, sigmoid and the softmax functions. The rectified linear unit (ReLU) [141], just removes all negative values in the vector and replaces them with zero. It is defined as,

$$\sigma(x_i) = max(0, x_i) \tag{4.7}$$

The sigmoid function produces a curve with a 'S' shape and is a real-valued differ-

entiable function and its derivate can be easily computed to determine gradients. The function is given by,

$$\sigma(x_i) = \frac{1}{1+e^{-x_i}} \tag{4.8}$$

The softmax function is typically used as the last layer of the network. It is used to convert a k dimensional vector of arbitrary real values to a k dimensional vector of values in the range [0,1] whose sum is 1. This vector represents a probability distribution over k possible outcomes. The softmax function is given by,

$$softmax(x;\mathcal{P}) = \frac{e^{\mathcal{W}_i x+b_i}}{\sum_{q=1}^{j} e^{\mathcal{W}_q x+b_q}} \tag{4.9}$$

Deep learning refers to a set of machine learning techniques that uses many hidden layers to learn multiple representations of the data, as illustrated in Fig. 4.20. With multiple layers, the function g becomes,

$$g(x;\mathcal{P}) = \sigma(\mathcal{W}_\infty \sigma(\mathcal{W}_\in \ldots(\mathcal{W}_\gamma x + b_\gamma)) + b_1) \tag{4.10}$$

The objective of training the algorithm is to minimise the loss function given by,

$$L_i = \frac{1}{K}\sum_{r=1}^{K} l(y_r^*, y_r) \tag{4.11}$$

where, y_r^* is the output obtained by the neural network and y_r is the actual output obtained from the labeled training data. Deep neural networks can be trained using simple stochastic gradient descent technique as long as the units are relatively smooth functions of their inputs and weights. Using back-propagation, which is essentially an application of the chain rule for derivatives, the gradient of the function can be computed and used as a measure to adjust the weights. The key insight in back-propagation is that, the derivative of the loss function with respect to the input layer can be computed by working backwards from the gradient with respect to the output layer. This technique can be applied recursively to compute gradients for all the layers, simplifying the training process.

There are several successful deep neural network architectures, such as, Recurrent Neural Network (RNN), Deep Belief Network (DBN) [142], Convolutional Neural Network (CNN), and auto-encoder (AE). A Recurrent Neural Network (RNN) is made up of neurons with feedback connections and use long short-term memory units. It has been shown to be very successful in text compression, speech recognition and

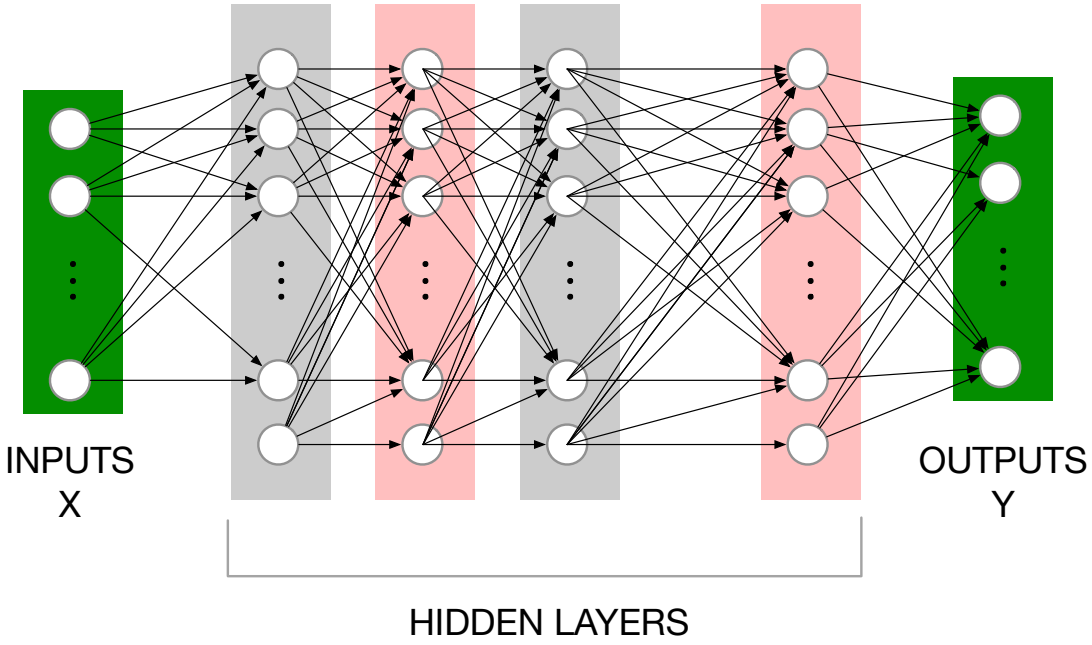

Figure 4.20: Deep Neural Network architecture showing input, output and dense hidden layers

handwriting recognition tasks. A Deep Belief Network (DBN) is a stack of restricted Boltzmann machines, which is a undirected connected bipartite graph consisting of feature-detecting units. They were primarily proposed to solve the vanishing gradient problem, which however can also be solved with the use of a Rectified Linear Unit (ReLU) function. Autoencoder (AE) is an unsupervised technique that learns a latent representation of the input value using hidden layers which is modelled as an encoding-decoding process. **Convolutional neural networks** (CNN) use convolution to extract features and were originally proposed [143] for image classification. Convolutional neural networks are of particular interest to us, due to three key properties, namely, weight sharing, translation invariance and pooling.

A typical CNN is composed of many layers for both feature representation and classification. A convolution layer consists of a set of learned F kernel weights to generate a feature map Y from an input matrix X using a convolution operation. The role of the convolution process is to detect local conjunctions of features from the previous layers. This enables the extraction of local features around each window. The convolution layers are followed by a pooling layer which is used to reduce the spectral variance in the input features. Several pooling algorithms have been proposed with max, sum and average pooling being the most popular for recent applications. With

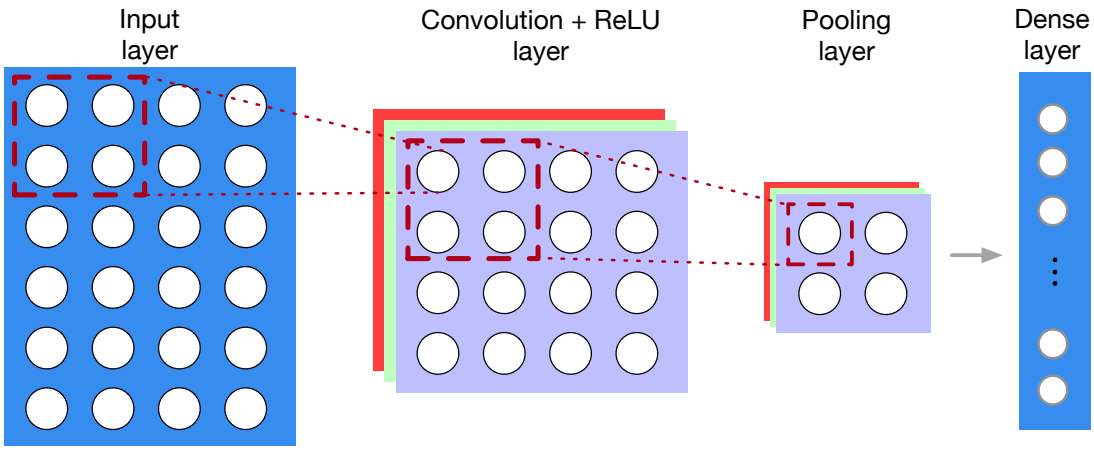

Figure 4.21: Convolutional Neural Networks architecture showing convolution layers, pooling layers followed by dense layers

max-pooling for example, the maximum value of a local patch of units is identified and neighbouring pooling units take inputs from patches that are shifted by one row or column, reducing the dimensions and resulting in translation invariance. The output of the pooling layer is passed onto fully connected layers, finally ending with the softmax layer. We use multiple convolution and pooling layers, linked to dense layers to extract the occupancy and activity information.

4.4.2 WiFi Glass architecture

In this section, we describe WiFi Glass, a deep learning technique for identifying home occupancy and activity using passively sniffed WiFi signals. This technique involves an information collection phase, a training phase and a deployment phase as illustrated in Fig. 4.22.

The **information collection phase** involves sniffing WiFi signal, collecting ground truth information about activities and preprocessing that data into the appropriate input vectors for the deep learning phase. The WiFi signal in the home environment is processed at line rate to recover the information discussed in Section 4.3.1.1. In order to combine the information of different modalities we use an information fusion layer, that involves a sliding window technique to combine and segment the time series information into a collection of equal sized vectors. The physical layer parameters are combined as illustrated in Fig. 4.23. The channel state information is averaged over bins to reduce the number of subcarriers with a configurable step value. The traffic

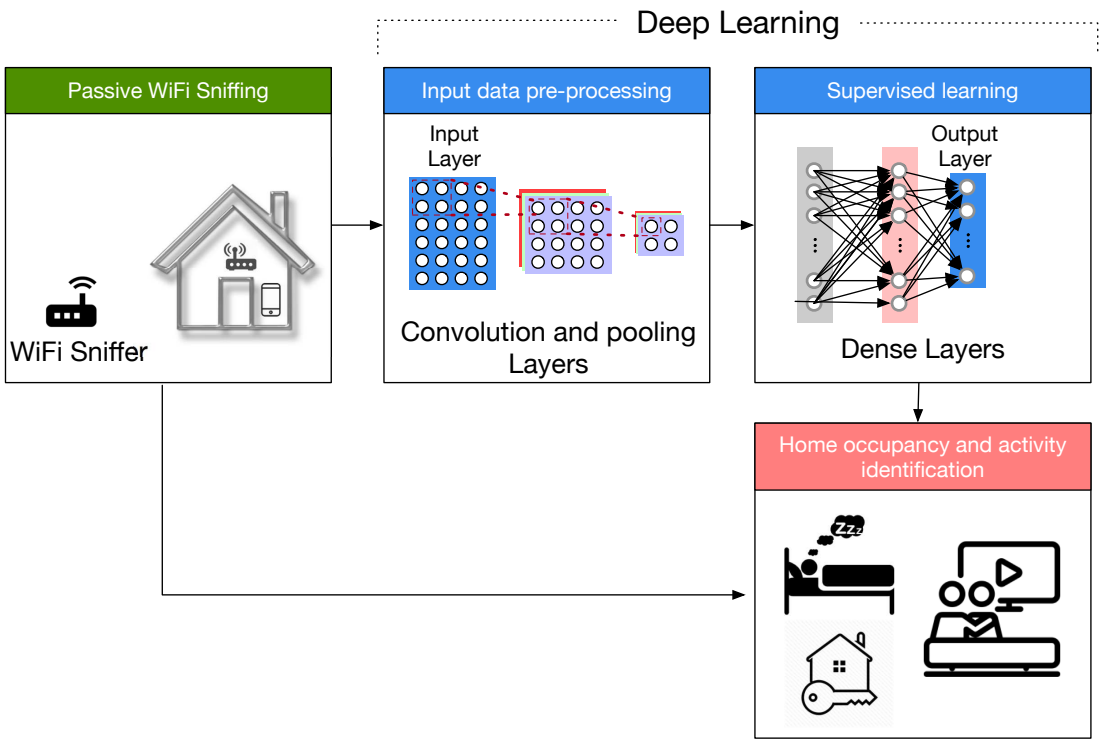

Figure 4.22: WiFi Glass : showing three key phases. 1. Information collection phase (Green) 2. Training Phase (Blue) 3. Deployment phase (Red)

characteristics and the device activity computed from decoding the management packets as described in Section 4.3, are used to form an activity vector whose size depends on the total number of devices being tracked. Using this technique, instead of simply concatenating the vectors, we use a fully connected layer to combine the data. The position of these vectors are kept constant to aid the temporal nature of the convolution process.

The pre-processing learning process consists of a convolution layer followed by a regularisation layer, a ReLU in our case and finally a pooling layer to reduce the size of the image. This batch of three layers is repeated as many times as necessary depending on the hierarchy of the features being captured, as illustrated in Fig. 4.24. In the convolution layers, the previous layers features are convolved with kernels and adjusted with a bias value to activate the current layer. The ReLU layer is used to normalise the data and remove negative values from the system using the function $f(x) = max(x,0)$. In the pooling layer, the adjacent units are combined to reduce the size of the images and to increase the invariance of the features to distortions of the input data. In order to map the feature represented in the convolution layers, the output

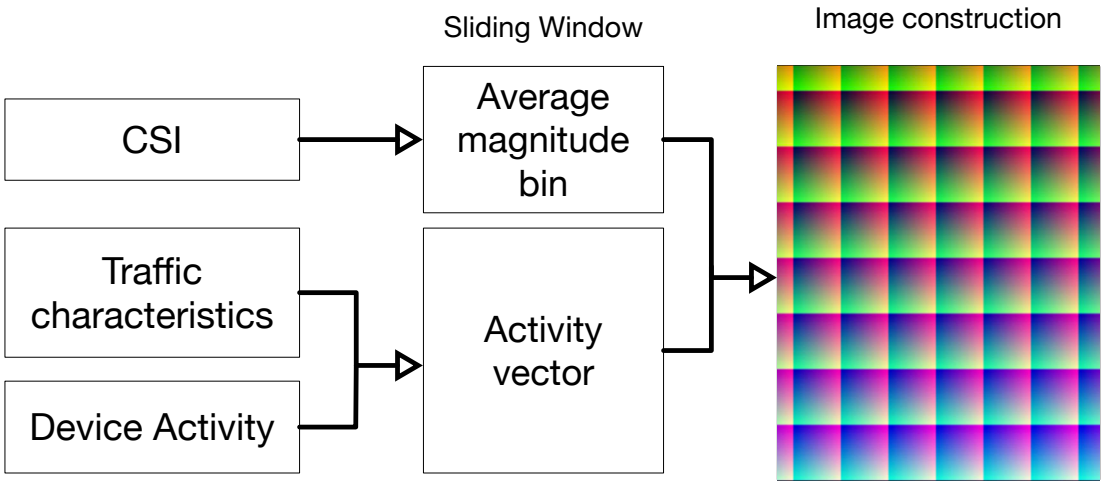

Figure 4.23: Constructing image from the collected information for the convolution operation

from this network is fed into a fully connected network.

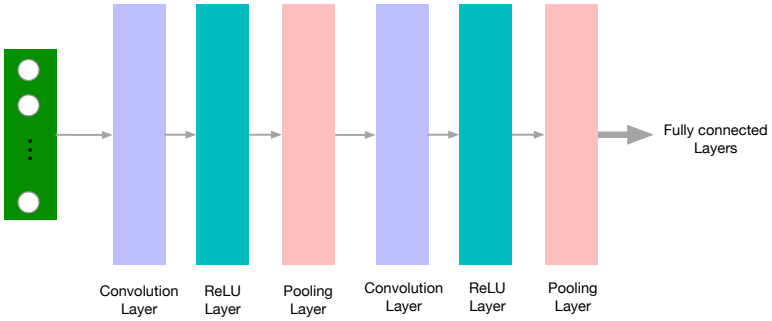

Figure 4.24: Architecture of CNN used in WiFi Glass, showing alternating convolution and pooling layers

The fully connected network is a standard multilayer perceptron neural network as described in Section 4.4.1 used to map the latent features into various classes of activities and home occupancy states. For our experiments we use two sets of output classes, namely occupancy and activity. In the dense network used to map occupancy, we use two states, namely, occupied and unoccupied. In the dense network used to map activity use use three states, namely, television, sleeping, and other. A *softmax* function is used to convert the activations in this layer into a posterior probability of the output classes, which is directly used to determine the activity or occupancy state.

Some of the hyper-parameters that needs to be tuned to improve the accuracy of

Table 4.2: Hyperparameters involved in the deep learning process

Hyperparameter	Influenced component	Value/Range
Pool Size	Max Pooling Layer	1x2 to 1x7
Pool Stride	Max Pooling Layer	3 to 5
Number of layers	Fully Connected Layers	1 to 5
Weight Decay	Back Propagation	0.00001
Output Classes	Last Layer	2 to 3
Dropout Probability	Dropout	0.7
Kernel Size	Convolution Layers	1x2 to 1x7
Loss Function	Back Propagation	$\mathcal{L}$
Stopping Criteria	Back Propagation	$\lvert\mathcal{L}^t - \mathcal{L}^{t-1}\rvert < \tau$

the classification process are listed in Table.4.2 along with the component they influence. During training phase, the various parameters such as the weights and bias that minimise the loss function needs to be identified. This is a non trivial task as the loss is a function of hundreds of parameters. A popular technique to solve this problem is called back propagation using steepest gradient descent.

In order to prevent over-fitting of data to the training set, regularisation methods such as L1 and L2 regularisation are employed to penalise some parameters. Dropout is a popular technique [141] employed to prevent over-fitting. Instead of modifying the cost function, dropout reduces co-adaptations between hidden units by randomly dropping some hidden units. In other words, dropout reduces the value of a unit to zero with probability p. This forces the hidden units to not depend on a few other units increasing the number of paths through which activation happens, enabling the network to learn redundant features.

4.5 Evaluation

In this section we evaluate the performance of the proposed scheme, WiFi Glass. In particular, we evaluate the classification accuracy with both activity and occupancy classes. In addition to the performance results, we also present some interesting behaviour of the CNN with respect to some key parameters such as kernel size, number of layers and pool size. Finally, to understand the time a rogue agent needs to spend capturing wireless information to carry out this attack, we evaluate the performance of the proposed scheme with respect to the sniffing duration.

4.5.1 Training the model

To tune hyperparameters, we employ a greedy method where in the number of layers, kernel size, pool size are adjusted while retaining the best configuration from the previous step. We arrived at a layer size of four, as the classification accuracy plateaus. The learning rate used is 0.02 and a weight decay value of 0.00001 is used. Training is performed for a high number of epochs (2000) for each scenario and is stopped if the error change is less than the set threshold.

The data used to train the model is derived from the WiFi signal data collected from the three homes using passive sniffing. This data corresponds to different scenarios and are categorised based on the activity at the time. Furthermore, for training and evaluation they are separated into two categories, namely, training set and evaluation set. The signal collected on one of the days (selected in random) is separated from the training data to be used for evaluating the trained classifier. In total, 420 observations spanning between 5 minutes and upto 45 minutes were used for evaluation.

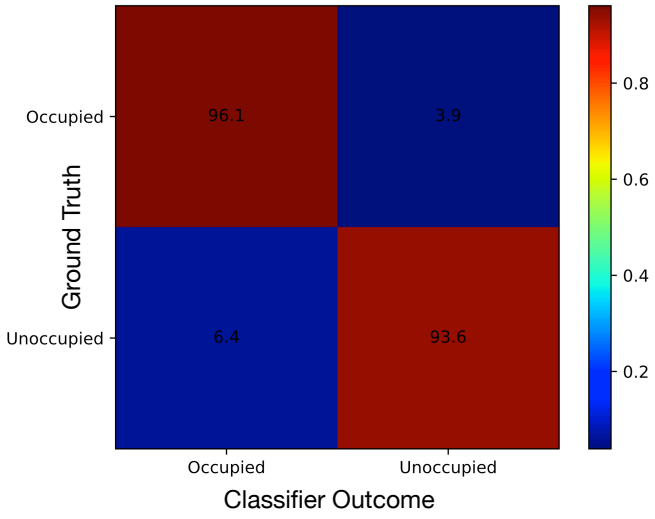

Figure 4.25: Confusion matrix representing the classification accuracy of occupancy detection

The trained model is ready to be used to identify home occupancy and activities based on the evaluation WiFi signal set. The input signal is used to construct a set of images which is then passed as an input to the CNN layers. The final layer outputs the probability of the house being occupied. In case of activity detection, the final layer

outputs the probability of the activity being performed at the house, which in our study is limited to sleeping, watching television, and other activities.

4.5.2 Occupancy and Activity Recognition

The mean classification accuracy of WiFi Glass for occupancy detection across three home environments is represented as a confusion matrix in Fig. 4.25. The proposed scheme achieves a very high accuracy (94.85%) in detecting the occupancy states across all three environments. It identifies unoccupied states with 93.6% probability and unoccupied scenarios with 96.1%. The false detections of occupied and unoccupied states are at 3.9% and 6.4% respectively. Analysis of these erroneous detections revealed that most of the scenarios resulting in a false positive occurred within a short period of time after a state change and most scenarios that resulted in false negative were due to smart phones being turned off either deliberately or due to lack of power. It seems possible to improve the accuracy of the scheme by collecting training data around these edge cases.

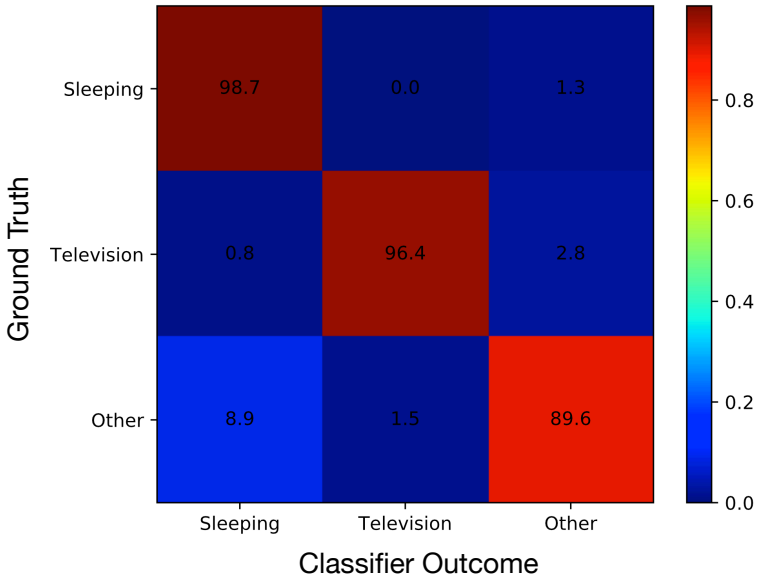

Figure 4.26: Confusion matrix representing the classification accuracy of activity detection

The confusion matrix for activity detection, classifying them into three activity classes, namely, sleeping, watching television and other activities, is shown in Fig.

4.26. All three activity classes are classified with high accuracy in the three environments, with the average accuracy of 94.5%. Most of the erroneous detections are when activities belonging to the other activities class are identified as belonging to the sleeping activity class due to the similarity of traffic characteristics. Analysis of these errors show that most of them occur when there is insufficient information about the presence of smart phones and high reliance on the traffic characteristics. The accuracy of the activity classification can be further improved by tuning the hyper-parameters, particularly, the dropout parameters to reduce the reliance on traffic characteristics.

4.5.3 Hyper-parameters

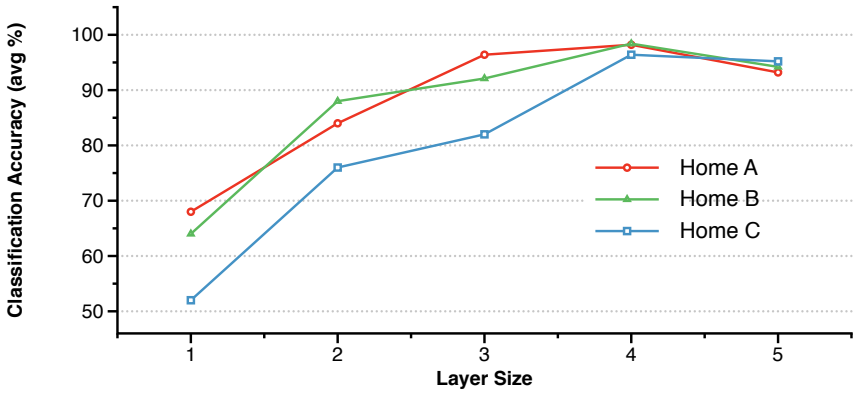

Figure 4.27: The effect of number of layers on the performance of the CNN

We now analyse the performance of WiFi Glass with respect to key hyper-parameters such as the number of layers, kernel size, and pool size. The classification accuracy of the CNN with varying number of layers in the network starting from one and incrementally increasing it up to five layers, as shown in Fig. 4.27. The accuracy of the classification scheme peaks with four layers suggesting that the four layers are able to capture the hierarchy of features required for both occupancy and activity detection. With a higher number of layers, the problem of overfitting becomes more pronounced and the accuracy of the testing set decreases.

The classification accuracy of the CNN with varying pool size is shown in Fig. 4.28. The pooling layer is used to reduce the spatial size of the representation and the pool size refers to the number of units that are consolidated into a single unit. We incrementally vary the pool size from 1x2 to 1x5. The classification accuracy of the

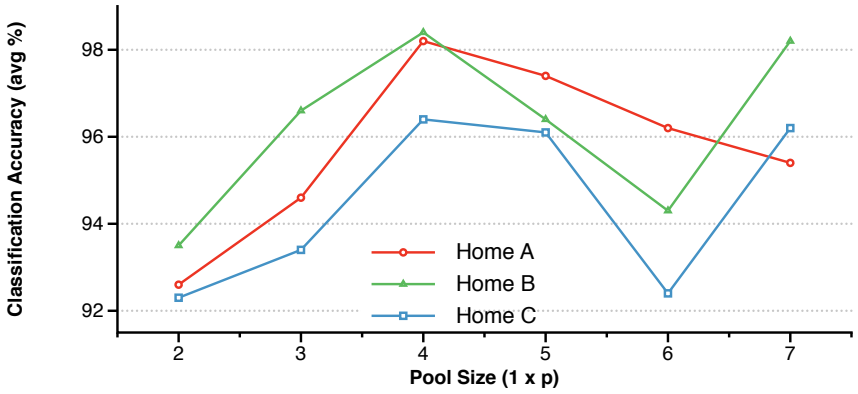

Figure 4.28: The effect of pool size on the performance of the CNN

CNN does not follow a clear trend and hence the pool size does not seem to have any potential to improve it.

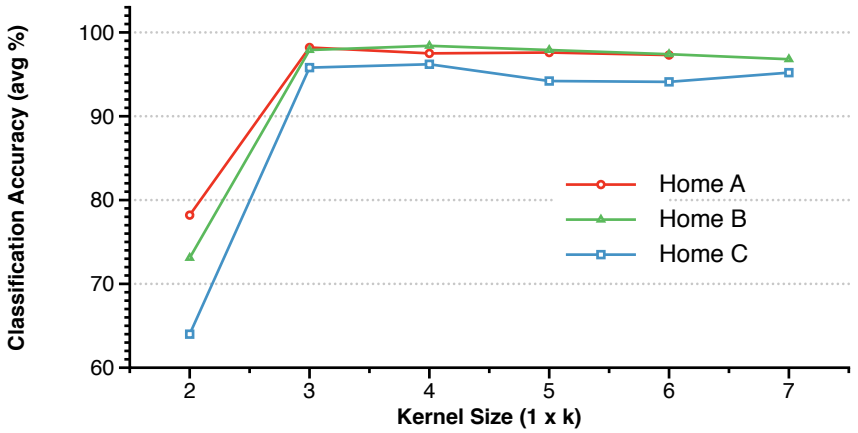

Figure 4.29: The effect of convolution kernel size on the performance of the CNN

The classification accuracy of the CNN with varying kernel size is shown in Fig. 4.29. The convolution layers convolve a kernel of size 1xk with the input layer before passing it to the pooling layer. The size of the kernel affects the temporal range of feature dependencies and hence needs to be tuned to the input data. The accuracy of classification increases when the kernel size increases from 1x2 to 1x3, however, beyond that, the classification accuracy saturates, suggesting 1x3 as an efficient kernel size.

In order to understand the practical implications of the amount of time a rogue agent has to sniff the data for training and classification, we train the network with

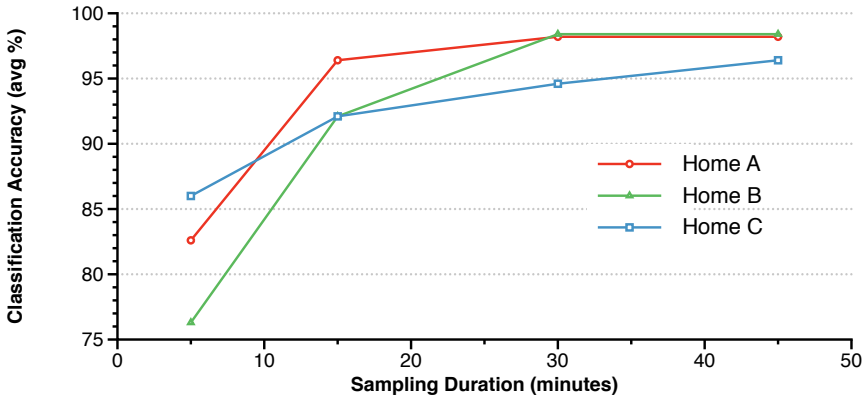

Figure 4.30: The effect of sampling duration on the classification accuracy

varying amounts of labeled data from two days to 6 days of sniffing duration. For classification, we use sliding windows of intervals ranging from 5 minutes to 45 minutes. This sliding window duration translates to the time spent by a rogue agent with a passive WiFi sniffer in the home environment in order to determine its occupancy state. The classification accuracy with increasing sniffing duration is shown in Fig. 4.30. As expected, the classification accuracy increases with increasing sniffing duration. However, in all the environments, a sniffing duration of around 15 minutes is enough to determine occupancy with more than 90% certainty. And, a sniffing duration of 30 minutes achieves a near perfect classification accuracy in two of the three home environments, highlighting the practicality of this attack vector.

4.6 Promising Countermeasures

So far only a few attempts have been made using deep learning on passively sniffed encrypted WiFi signal to reveal private behaviour about its users. It seems inevitable that the use of deep learning would continue to further challenge the preservation of privacy in an encrypted home WiFi network. Hence it is of crucial importance to identify countermeasures to such attack vectors. Several promising directions for countermeasures to WiFi Glass exist for further research, such as use of encrypted management frames, Obfuscation of traffic characteristics and using fake wireless transmissions.

Encrypted Management Frames: In IEEE 802.11 management frames send unencrypted information over the un-secure wireless medium. While this design choice did not pose a concern two decades ago, now with new handoff mechanisms, radio

resource management, and service discovery processes, the management frames have come to contain sensitive information that must be protected. Additionally, the lack of authentication of management frames lead to vulnerabilities which can be exploited in de-authentication and disassociation attacks. The IEEE 802.11w protocol amendment proposes Protected Management Frames (PMF), a specification for communicating with encrypted management frames that can provide protection against the protocol based attacks that use information in the management frames. This specification is a mandatory requirement in order to obtain the certification for IEEE 802.11ac, the latest WiFi standards for WLANs.

Obfuscation of traffic characteristics: In WiFi the data transmitted over the unsecure wireless medium is encrypted. However, the 128-bit AES block cipher used to encrypt the data preserves the original size of the plaintext data. This exposes a range of side-channel information that an adversary could exploit, for instance, Akinson et al, propose a mechanism that can detect the presence of Skype traffic with around 97% accuracy using only the inter-arrival time between frames and frame size distributions [144]. Traffic analysis has been shown to enable an adversary to infer the identity of websites that the user travels to [145]. Our experimental study demonstrated that the traffic characteristics may indeed be used to infer personal information about home occupants. Hence it is clear that such information must be obfuscated, for example, by padding to change the original size of the clear text.

4.7 Summary and Conclusion

Communications over the home WiFi network is considered private when encryption and a strong passphrase is used. In this chapter, we showed that private information can indeed be inferred from encrypted home WiFi networks using traffic analysis. We presented WiFi Glass, an attack vector on home WiFi Networks that can be used to determine the occupancy state of the home and some activity classes with high accuracy. Moreover, to determine such information in most cases, a rogue agent would only need to spend around 15 mins, highlighting the practicality of the attack. The two most promising avenues for countermeasures are obfuscation of traffic characteristics and encrypted management frames. With the continuing proliferation of deep learning techniques, it is crucial that countermeasures are developed for such attacks.

Chapter 5

Summary

5.1 Summary of Contributions

This thesis discussed three issues related to efficient use and privacy of wireless spectrum use. Specifically, we proposed,

- **GAVEL**, a strategy-proof auction mechanism for short-term spectrum access that improves spectral efficiency
- **CPRecycle**, an improved OFDM receiver that mitigates interference using information in the cyclic prefix to improve spectral efficiency
- **WiFi Glass**, an attack vector on home WiFi networks that reveals private information about occupancy states and human activity using passively sniffed WiFi signal.

First, we considered short-term spectrum auctions. Existing auction mechanisms do not satisfy the requirements for a dynamic short-term spectrum market. Since the first strategy-proof short-term auction mechanism, VERITAS, was proposed in 2008, several problems have surfaced and several auction mechanisms have been proposed. We identify that the root cause of all these problems may be due to the underlying auction format (the sealed-bid auction format) and not the winner/price determination strategies. With this insight, we proposed a truthful auction mechanisms, GAVEL, for the Licensed Shared Access market, based on the ascending-bid auction. Performance evaluations of the auction mechanism show that GAVEL improves revenue for the auctioneers while achieving better utility for the bidders.

Second, we investigated the use of cyclic prefix to decode data in the presence of interference improving spectral efficiency. The cyclic prefix contains useful information and can be utilised for interference mitigation. Through experiments involving USRPs, we observed the effects of the received signal in the cyclic prefix in the presence of different types of interference. This led us to the key insight, that while the cyclic prefix only contains redundant information about the signal of interest, the presence of interference in the environment turns this information unique and useful to decode the signal of interest in the presence of interference. Using this insight, we designed CPRecycle, an improved OFDM receiver that is capable of using the information in the cyclic prefix to mitigate various types of interference such as adjacent channel interference and co-channel interference. Performance evaluations using off-the-shelf WiFi routers and USRPs, showed that CPRecycle is able to decode the signal of interest even in the presence of strong interference in various deployment scenarios. Furthermore, CPRecycle receiver only require modifications at the OFDM receiver and hence can support the millions of smart phones and laptops that are already in use today.

Third and finally, we investigated the privacy of encrypted WiFi networks in home environments. Using experiments in three dual-income family homes, we observe that passively sniffed signal in the home environment can be used to infer highly private information such as home occupancy and activities inside the home. We presented WiFi Glass, an attack vector that uses deep learning to determine occupancy status of a home and some activities of its occupants. Evaluations using real data shows that such private information can be inferred with high accuracy and in most cases only requires about 15 minutes of sniffed data. This highlights the need for countermeasures as such attacks using deep learning would only get more capable in time. We briefly discussed some promising avenues for countermeasures, covering, traffic characteristics obfuscation and encrypted management frames.

5.2 Future Work

Spectrum Auctions: GAVEL, the auction mechanism proposed in this thesis is the first time ascending-bid auction format has been used as the basis for a dynamic short-term spectrum auction mechanism that is strategy-proof. The nature of ascending-bid auctions while it solves several problems associated with sealed-bid auction mechanisms, opens other issues for consideration. For instance, the nature of sealed-bid auction format avoided collusion by enforcing the secrecy of the bid. In the ascending-

bid, the bidders are able to infer their competitors bids based on the demand curve. This may open avenues for collusion and requires further investigation. GAVEL has not been shown to maximise the social welfare, either exactly nor approximately, or to be Pareto-efficient. This is due the distributed nature of channel assignment in GAVEL and requires further investigation.

CPRecycle: There are two aspects of CPRecycle that needs further investigation. Just as in with single antenna receivers, with MIMO, CPRecycle provides multiple redundant copies of the signal received a few microseconds apart that could have suffered from a different level of interference. Furthermore, along with spatial multiplexing streams, CPRecycle offers another dimension of redundancy that can be exploited in the decoding process. This requires further investigation. Second, further evaluation of performance of CPRecycle with varying packet length, modulation schemes, different interference sources, environments, and communication standards is left for future work. Modern standards such as IEEE 802.11ac have a much longer duration of cyclic prefix and the performance of cyclic prefix in such systems require further investigation.

Privacy of encrypted home WiFi networks: With the continuing proliferation of deep learning techniques, it is inevitable that techniques such as WiFi Glass would only get better at extracting private information from encrypted WiFi networks based on the context of their deployment. Hence, it is crucial to develop countermeasures for such attacks to preserve privacy on home WiFi networks. In particular, the traffic characteristics and the unencrypted management frames are promising avenue for such countermeasures and requires further investigation.

Bibliography

[1] Julien Freudiger. How talkative is your mobile device? In *the 8th ACM Conference*, pages 1–6, New York, New York, USA, 2015. ACM Press.

[2] O Waltari and J Kangasharju. The Wireless Shark: Identifying WiFi Devices Based on Probe Fingerprints. In *Proceedings of the First Workshop on Mobile ...*, 2016.

[3] Ralph Cassady. *Auctions and auctioneering*. Univ of California Press, 1967.

[4] Xia Zhou, Sorabh Gandhi, Subhash Suri, and Haitao Zheng. ebay in the sky: Strategy-proof wireless spectrum auctions. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 2–13. ACM, 2008.

[5] Xiaojun Feng, Yanjiao Chen, Jin Zhang, Qian Zhang, and Bo Li. Tahes: A truthful double auction mechanism for heterogeneous spectrums. *Wireless Communications, IEEE Transactions on*, 11(11):4038–4047, 2012.

[6] Fan Wu and Nitin Vaidya. Small: A strategy-proof mechanism for radio spectrum allocation. In *INFOCOM, 2011 Proceedings IEEE*, pages 81–85. IEEE, 2011.

[7] I. Kash, Rohan Narayana Murty, and David C. Parkes. Enabling sharing in auctions for short-term spectrum licenses. *Mechanisms and Games for Dynamic Spectrum Allocation*, 2013.

[8] Zhenzhe Zheng and Guihai Chen. A strategy-proof combinatorial heterogeneous channel auction framework in noncooperative wireless networks. *Mobile Computing, IEEE Transactions on*, 14(6):1123–1137, 6 2015.

[9] A Peled and A Ruiz. Frequency domain data transmission using reduced computational complexity algorithms. ... *IEEE International Conference on ICASSP'80 ...*, 1980.

[10] S B Weinstein. The history of orthogonal frequency-division multiplexing [History of Communications]. *IEEE Communications Magazine*, 2009.

[11] Eldad Perahia and Michelle X Gong. Gigabit wireless LANs: an overview of IEEE 802.11ac and 802.11ad. *ACM SIGMOBILE Mobile Computing and Communications Review*, 15(3):23–33, November 2011.

[12] Marja Matinmikko, Hanna Okkonen, Marko Palola, Seppo Yrjola, Petri Ahokangas, and Miia Mustonen. Spectrum sharing using licensed shared access: the concept and its workflow for lte-advanced networks. *Wireless Communications, IEEE*, 21(2):72–79, 2014.

[13] Pierce Rixon. Licensed Shared Access. *Whitepaper IEEE TCCN*, 2014.

[14] Milind Madhav Buddhikot. Towards a virtual cellular network with variable grade spectrum: challenges and opportunities. In *Proceedings of MOBICOM*, pages 369–374. ACM, 2013.

[15] P. Klemperer. *Auctions: Theory and Practice*. Princeton University Press, 2004.

[16] S. de Vries and R. V. Vohra. Combinatorial auctions: A survey. *INFORMS Journal on Computing)*, 15(3):284–309, 2003.

[17] P. Cramton, Y. Shoham, and R. Steinberg. Introduction to Combinatorial Auctions. MIT Press, 2006.

[18] Dejun Yang, Xiang Zhang, and Guoliang Xue. Promise: A framework for truthful and profit maximizing spectrum double auctions. In *INFOCOM, 2014 Proceedings IEEE*, pages 109–117. IEEE, 2014.

[19] Xia Zhou and Heather Zheng. Trust: A general framework for truthful double spectrum auctions. In *INFOCOM 2009, IEEE*, pages 999–1007. IEEE, 2009.

[20] Mojgan Khaledi and Alhussein Abouzeid. Adaptive: A dynamic index auction for spectrum sharing with time-evolving values. In *WiOPT, 2014 12th International Symposium on*, pages 513–520. IEEE, 2014.

[21] Qinhui Wang, Baoliu Ye, Bin Tang, Tianyin Xu, Song Guo, Sanglu Lu, and Weihua Zhuang. Aletheia: Robust large-scale spectrum auctions against false-name bids. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 27–36. ACM, 2015.

[22] Ming Li, Pan Li, Linke Guo, and Xiaoxia Huang. Pper: Privacy-preserving economic-robust spectrum auction in wireless networks. INFOCOM, 2015.

[23] Ruihao Zhu, Zhijing Li, Fan Wu, Kang Shin, and Guihai Chen. Differentially private spectrum auction with approximate revenue maximization. In *Proceedings of the 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '14, pages 185–194, New York, NY, USA, 2014. ACM.

[24] He Huang, Xiang-Yang . Y. Li, Yu-e . E. Sun, Hongli Xu, and Liusheng Huang. Pps: Privacy-preserving strategyproof social-efficient spectrum auction mechanisms. *Parallel and Distributed Systems, IEEE Transactions on*, 26(5):1393–1404, 5 2015.

[25] Qianyi Huang, Yixin Tao, and Fan Wu. Spring: A strategy-proof and privacy preserving spectrum auction mechanism. In *INFOCOM, 2013 Proceedings IEEE*, pages 827–835. IEEE, 2013.

[26] Ian /A/ Kash, Rohan Murty, and David C. Parkes. Enabling spectrum sharing in secondary market auctions. *Mobile Computing, IEEE Transactions on*, 13(3):556–568, 3 2014.

[27] Gaurav S. Kasbekar and Saswati Sarkar. Spectrum auction framework for access allocation in cognitive radio networks. *IEEE/ACM Transactions on Networking (TON)*, 18(6):1841–1854, 2010.

[28] Wei Li, Xiuzhen Cheng, Rongfang Bie, and Feng Zhao. An extensible and flexible truthful auction framework for heterogeneous spectrum markets. In *Proceedings of the 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '14, pages 175–184, New York, NY, USA, 2014. ACM.

[29] Yanjiao Chen, Jin Zhang, Kaishun Wu, and Qian Zhang. Tames: A truthful auction mechanism for heterogeneous spectrum allocation. In *INFOCOM, 2013 Proceedings IEEE*, pages 180–184. IEEE, 2013.

[30] Yanjiao Chen, Peng Lin, and Qian Zhang. Lotus: Location-aware online truthful double auction for dynamic spectrum access. In *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pages 510–518. IEEE, 2014.

[31] Zhenzhe Zheng, Fan Wu, Shaojie Tang, and Guihai Chen. Unknown combinatorial auction mechanisms for heterogeneous spectrum redistribution. In *Proceedings of the 15th ACM international symposium on mobile ad hoc networking and computing*, MobiHoc '14, pages 3–12, New York, NY, USA, 2014. ACM.

[32] Sorabh Gandhi, Chiranjeeb Buragohain, Lili Cao, Haitao Zheng, and Subhash Suri. Towards real-time dynamic spectrum auctions. *Computer Networks*, 52(4):879–897, 2008.

[33] Miao Pan, Jinyuan Sun, and Yuguang Fang. Purging the back-room dealing: Secure spectrum auction leveraging paillier cryptosystem. *Selected Areas in Communications, IEEE Journal on*, 29(4):866–876, 2011.

[34] Debasis Mishra and David C. Parkes. Ascending price vickrey auctions for general valuations. *Journal of Economic Theory*, 132(1):335–366, 2007.

[35] Christer Andersson, Ola Andersson, and Tommy Andersson. Sealed bid auctions versus ascending bid auctions: an experimental study. *Review of Economic Design*, 17(1):1–16, 2013.

[36] Peter Cramton. Ascending auctions. *European Economic Review*, 42(3):745–756, 1998.

[37] Lawrence M. Ausubel. An efficient dynamic auction for heterogeneous commodities. *The American economic review*, pages 602–629, 2006.

[38] Chunchun Wu, Zuying Wei, Fan Wu, Guihai Chen, and Shaojie Tang. Designing differentially private spectrum auction mechanisms. *Wireless Networks*, pages 1–13, 2015.

[39] Kun Tan, Ji Fang, Yuanyang Zhang, Shouyuan Chen, Lixin Shi, Jiansong Zhang, and Yongguang Zhang. Fine-grained channel access in wireless lan. *ACM SIGCOMM CCR*, 41(4):147–158, 2011.

[40] Eduard Garcia Villegas, Elena Lopez-Aguilera, Rafael Vidal, and Josep Paradells. Effect of adjacent-channel interference in ieee 802.11 wlans. In *CROWNCOM*, pages 118–125, 2007.

[41] Jens Nachtigall, Anatolij Zubow, and Jens-Peter . P. Redlich. The impact of adjacent channel interference in multi-radio systems using ieee 802.11. In *In Proceedings of IWCMC*, pages 874–881, 2008.

[42] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of MobiCom*, pages 114–128, 2004.

[43] A. Zubow and R. Sombrutzki. Adjacent channel interference in IEEE 802.11n. *WCNC 2012*, 4 2012.

[44] Yong Ding, Yi Huang, Guokai Zeng, and Li Xiao. Channel assignment with partially overlapping channels in wireless mesh networks. In *Proceedings of ICWI*, page 38, 2008.

[45] Kunxiao Zhou, Xiaohua Jia, Liming Xie, Yanan Chang, and Xing Tang. Channel assignment for wlan by considering overlapping channels in sinr interference model. In *Proceedings of ICNC*, pages 1005–1009. IEEE, 2012.

[46] Yan Li, Xiaowen Wang, and Syed Aon Mujtaba. Cochannel interference avoidance algorithm in 802.11 wireless lans. In *Proceedings of VTC*, pages 2610–2614, 2003.

[47] Cheng Feng, Hongyu Cui, Meng Ma, and Bingli Jiao. On statistical properties of co-channel interference in ofdm systems. *Communications Letters, IEEE*, 17(12):2328–2331, 2013.

[48] Azade Farshad, Mahesh K. Marina, and Francisco Garcia. Urban wifi characterization via mobile crowdsensing. In *Proceedings of NOMS IEEE*, pages 1–9, 2014.

[49] Ramakrishna Gummadi, David Wetherall, Ben Greenstein, and Srinivasan Seshan. Understanding and mitigating the impact of rf interference on 802.11 networks. *ACM SIGCOMM CCR*, 37(4):385–396, 2007.

[50] Christina Thorpe and Liam Murphy. A survey of adaptive carrier sensing mechanisms for ieee 802.11 wireless networks. *Communications Surveys & Tutorials, IEEE*, 16(3):1266–1293, 2014.

[51] Nazmus Saquib, Ekram Hossain, Long Bao Le, and Dong In Kim. Interference management in ofdma femtocell networks: issues and approaches. *Wireless Communications, IEEE*, 19(3), 2012.

[52] T. Weiss, J. Hillenbrand, A. Krohn, and F. K. Jondral. Mutual interference in ofdm-based spectrum pooling systems. *IEEE Xplore*, 4:1873–1877 Vol.4, 5 2004.

[53] Ivan Cosovic, Sinja Brandes, and Michael Schnell. Subcarrier weighting: a method for sidelobe suppression in ofdm systems. *Communications Letters, IEEE*, 10(6):444–446, 2006.

[54] Ivan Cosovic and Tiziano Mazzoni. Suppression of sidelobes in ofdm systems by multiple-choice sequences. *European transactions on telecommunications*, 17(6):623–630, 2006.

[55] Ahmed Selim, Irene Macaluso, and Linda Doyle. Efficient sidelobe suppression for ofdm systems using advanced cancellation carriers. In *Proceedings of IEEE ICC*, pages 4687–4692, 2013.

[56] Srikanth Pagadarai, Rakesh Rajbanshi, Alexander M. Wyglinski, and Gary J. Minden. Sidelobe suppression for ofdm-based cognitive radios using constellation expansion. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pages 888–893. IEEE, 2008.

[57] Hisham Mahmoud and Hüseyin Arslan. Sidelobe suppression in ofdm-based spectrum sharing systems using adaptive symbol transition. *Communications Letters, IEEE*, 12(2):133–135, 2008.

[58] Pawel Kryszkiewicz, Hanna Bogucka, and Alexander M. Wyglinski. Protection of primary users in dynamically varying radio environment: practical solutions and challenges. *EURASIP Journal on Wireless Communications and Networking*, (1):1–20, 2012.

[59] Yann Léost, Moussa Abdi, Robert Richter, and Michael Jeschke. Interference rejection combining in lte networks. *Bell Labs Technical Journal*, 17(1):25–49, 2012.

[60] Daewon Lee, Hanbyul Seo, Bruno Clerckx, Eric Hardouin, David Mazzarese, Satoshi Nagata, and Krishna Sayana. Coordinated multipoint transmission and reception in lte-advanced: deployment scenarios and operational challenges. *Communications Magazine, IEEE*, 50(2):148–155, 2012.

[61] Daiming Qu, Zhiqiang Wang, and Tao Jiang. Extended active interference cancellation for sidelobe suppression in cognitive radio ofdm systems with cyclic prefix. *Vehicular Technology, IEEE Transactions on*, 59(4):1689–1695, 2010.

[62] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications . Technical report, 1997.

[63] Kyle Jamieson and Hari Balakrishnan. Ppr: Partial packet recovery for wireless networks. *ACM SIGCOMM CCR*, 37(4):409–420, 2007.

[64] Grace R. Woo, Pouya Kheradpour, Dawei Shen, and Dina Katabi. Beyond the bits: cooperative packet recovery using physical layer information. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 147–158. ACM, 2007.

[65] Shyamnath Gollakota, Samuel David Perli, and Dina Katabi. Interference alignment and cancellation. In *ACM SIGCOMM Computer Communication Review*, volume 39, pages 159–170. ACM, 2009.

[66] Tarun Bansal, Wenjie Zhou, Kannan Srinivasan, and Prasun Sinha. Robinhood: sharing the happiness in a wireless jungle. In *Proceedings of ACM HotMobile*, page 22, 2014.

[67] Fadel Adib, Swarun Kumar, Omid Aryan, Shyamnath Gollakota, and Dina Katabi. Interference alignment by motion. In *Proceedings of the ACM MobiCom*, pages 279–290, 2013.

[68] Swarun Kumar, Diego Cifuentes, Shyamnath Gollakota, and Dina Katabi. Bringing cross-layer mimo to today's wireless lans. In *ACM SIGCOMM CCR*, volume 43, pages 387–398, 2013.

[69] Linghe Kong and Xue Liu. In *In Proceedings of ACM MobiCom*. ACM, 2015.

[70] Shyamnath Gollakota, Fadel Adib, Dina Katabi, and Srinivasan Seshan. Clearing the rf smog: making 802.11 n robust to cross-technology interference. *ACM SIGCOMM CCR*, 41(4):170–181.

[71] Yubo Yan, Panlong Yang, Xiang-Yang . Y. Li, Yafei Zhang, Jianjiang Lu, Lizhao You, Jiliang Wang, Jinsong Han, and Yan Xiong. Wizbee: Wise zigbee coexistence via interference cancellation with single antenna. *Mobile Computing, IEEE Transactions on*, 14(12):2590–2603, 2015.

[72] Sachin Katti, Dina Katabi, Hari Balakrishnan, and Muriel Medard. Symbol-level network coding for wireless mesh networks. In *ACM SIGCOMM Computer Communication Review*, volume 38, pages 401–412, 2008.

[73] Allen Miu, Hari Balakrishnan, and Can Emre Koksal. Improving loss resilience with multi-radio diversity in wireless networks. In *Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 16–30, 2005.

[74] Grace R. Woo, Pouya Kheradpour, Dawei Shen, and Dina Katabi. Beyond the bits: cooperative packet recovery using physical layer information. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 147–158, 2007.

[75] Jun Huang, Guoliang Xing, Jianwei Niu, and Shan Lin. Coderepair: Phy-layer partial packet recovery without the pain. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pages 1463–1471, 2015.

[76] Mahanth Gowda, Souvik Sen, Romit Roy Choudhury, and Sung-Ju . J. Lee. Cooperative packet recovery in enterprise wlans. In *INFOCOM, 2013 Proceedings IEEE*, pages 1348–1356, 2013.

[77] Kyle Jamieson and Hari Balakrishnan. Ppr: Partial packet recovery for wireless networks. *ACM SIGCOMM Computer Communication Review*, 37(4):409–420, 2007.

[78] Kate Ching-Ju . J. Lin, Nate Kushman, and Dina Katabi. Ziptx: Harnessing partial packets in 802.11 networks. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 351–362, 2008.

[79] Christopher L. Holloway, Michael G. Cotton, and Paul McKenna. A model for predicting the power delay profile characteristics inside a room. *Vehicular Technology, IEEE Transactions on*, 48(4):1110–1120, 1999.

[80] Chan-Ping . P. Lim, John L. Volakis, Kubilay Sertel, Rickie W. Kindt, and Achilleas Anastasopoulos. Indoor propagation models based on rigorous methods for site-specific multipath environments. *Antennas and Propagation, IEEE Transactions on*, 54(6):1718–1725, 2006.

[81] Tadeusz A. Wysocki and H-J . J. Zepernick. Characterization of the indoor radio propagation channel at 2.4 ghz. *Journal of telecommunications and information technology*, pages 84–90, 2000.

[82] Saravana Manickam Rathinakumar, Bozidar Radunovic, and Mahesh K. Marina. Shiftfft: An efficient approach to mitigate adjacent channel interference in ofdm systems. In *Proceedings of the HotWireless in Conjunction with MobiCom*, pages 11–15, 2015.

[83] Thierry Pollet, Mark Van Bladel, and Marc Moeneclaey. Ber sensitivity of ofdm systems to carrier frequency offset and wiener phase noise. *Communications, IEEE Transactions on*, 43(2/3/4):191–193, 1995.

[84] J Stott. The effects of phase noise in cofdm. *EBU technical Review*, pages 12–25, 1998.

[85] Songping Wu and Yeheskel Bar-Ness. Ofdm systems in the presence of phase noise: consequences and solutions. *Communications, IEEE Transactions on*, 52(11):1988–1996, 2004.

[86] Cheng Feng, Hongyu Cui, Meng Ma, and Bingli Jiao. On statistical properties of co-channel interference in ofdm systems. *Communications Letters, IEEE*, 17(12):2328–2331, 2013.

[87] David W Scott. *Multivariate density estimation: theory, practice, and visualization*. John Wiley & Sons, 2015.

[88] George R. Terrell and David W. Scott. Variable kernel density estimation. *The Annals of Statistics*, pages 1236–1265, 1992.

[89] Simon J. Sheather. Density estimation. *Statistical Science*, 19(4):588–597, 2004.

[90] M. Chris Jones, James S. Marron, and Simon J. Sheather. A brief survey of bandwidth selection for density estimation. *Journal of the American Statistical Association*, 91(433):401–407, 1996.

[91] Emanuele Viterbo and Joseph Boutros. A universal lattice code decoder for fading channels. *Information Theory, IEEE Transactions on*, 45(5):1639–1642, 1999.

[92] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

[93] Mohamed Oussama Damen, Hesham El Gamal, and Giuseppe Caire. On maximum-likelihood detection and the search for the closest lattice point. *Information Theory, IEEE Transactions on*, 49(10):2389–2402, 2003.

[94] Matt Ettus. Usrp users and developers guide. *Ettus Research LLC*, 2005.

[95] Gordon Stewart, Mahanth Gowda, Geoffrey Mainland, Bozidar Radunovic, Dimitrios Vytiniotis, and Doug Patterson. Ziria: language for rapid prototyping of wireless phy. In *Proceedings of the 2014 ACM conference on SIGCOMM*, 2014.

[96] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. An ieee 802.11 a/g/p ofdm receiver for gnu radio. In *Proceedings of Software radio implementation forum*, 2013.

[97] Barbara Majecka. Statistical models of pedestrian behaviour in the forum. *Master's thesis, School of Informatics, University of Edinburgh*, 2009.

[98] Xuejun Chen, Chenchen Zhang, and Yuan Luo. Low-complexity isi-free region detection for ofdm systems in high-mobility fading channels. In *In Proceedings of IEEE HWMC*, 2014.

[99] Karthik Ramasubramanian and Kevin Baum. An ofdm timing recovery scheme with inherent delay-spread estimation. In *In Proceedings of IEEE GLOBECOM*, volume 5, pages 3111–3115, 2001.

[100] Chorng-Ren . R. Sheu and Chia-Chi . C. Huang. A novel guard interval based isi-free sampling region detection method for ofdm systems. In *Proceedings of IEEE VTC 2004*, volume 1, pages 515–519.

[101] Chenchen Zhang, Xuejun Chen, and Yuan Luo. Threshold optimization for isi-free region detection in high-mobility fading channels. In *In Proceedings of IEEE HMWC*, 2015.

[102] A Crabtree, R Mortier, T Rodden, and P Tolmie. Unremarkable networking: the home network as a part of everyday life. In *Proceedings of the . . .*, 2012.

[103] WiFi Alliance. www.wi-fi.org.

[104] Y Qi, M Hunukumbure, and M Nekovee. Quantifying data rate and bandwidth requirements for immersive 5G experience. . . . *(ICC)*, 2016.

[105] O Nakhila, A Attiah, and Y Jinz. Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. . . . *Conference*, 2015.

[106] O Nakhila, A Attiah, and Y Jinz. Parallel active dictionary attack on WPA2-PSK Wi-Fi networks. . . . *Conference*, 2015.

[107] Wireshark. www.wireshark.com.

[108] Kismet. kismetwireless.net.

[109] G Castignani, A Arcia, and N Montavont. A study of the discovery process in 802.11 networks. *ACM SIGMOBILE Mobile . . .*, 2011.

[110] Genevieve Bartlett, John Heidemann, and Christos Papadopoulos. *Understanding passive and active service discovery*. ACM, New York, New York, USA, October 2007.

[111] M Abadi and C Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, 2004.

[112] M V Barbera, A Epasto, A Mei, and V C Perta. Signals from the crowd: uncovering social relationships through smartphone probes. In *Proceedings of the 2013 . . .*, 2013.

[113] Y Singh. WIFI espionage using a UAV. 2016.

[114] L Mikkelsen, R Buchakchiev, and T Madsen. Public transport occupancy estimation using WLAN probing. ... *(RNDM)*, 2016.

[115] Y S Kim, Y Tian, and L T Nguyen. LAPWiN: Location-aided probing for protecting user privacy in Wi-Fi networks. ... *and Network Security (* ..., 2014.

[116] A Di Luzio, A Mei, and J Stefa. Mind Your Probes: De-Anonymization of Large Crowds Through Smartphone WiFi Probe Requests. 1.

[117] A Mashhadi, G Vanderhulst, and U G Acer. An Autonomous Reputation Framework for Physical Locations based on WiFi Signals. In *Proceedings of the 2nd* ..., 2015.

[118] B Bonné, A Barzan, and P Quax. WiFiPi: Involuntary tracking of visitors at mass events. *World of Wireless*, 2013.

[119] Shuja Jamil, Sohaib Khan, Anas Basalamah, and Ahmed Lbath. *Classifying smartphone screen ON/OFF state based on wifi probe patterns*. ACM, New York, New York, USA, September 2016.

[120] E G Vattapparamban. People Counting and occupancy Monitoring using WiFi Probe Requests and Unmanned Aerial Vehicles. 2016.

[121] A A Aldan, O Cerrahoglu, E Topalli, and X Soriano. Marauder's Map: Sniffing MAC addresses in the MIT wireless network. *courses.csail.mit.edu*.

[122] M Cunche. I know your MAC Address: Targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques*, 2014.

[123] A Dabrowski and E R Weippl. Mobile Phone's WiFi Presence for Continuous Implicit Secondary Deauthentication. *sba-research.org*.

[124] Levent Demir. Wi-Fi tracking : what about privacy. page 25, September 2013.

[125] Kai Li, Chau Yuen, Salil S Kanhere, Kun Hu, Wei Zhang, Fan Jiang, and Xiang Liu. SenseFlow: An Experimental Study for Tracking People. June 2016.

[126] E Vattapparamban and K Akkaya. Indoor occupancy tracking in smart buildings using passive sniffing of probe requests. ... *Workshops (ICC)*, 2016.

[127] N Cheng, X O Wang, and W Cheng. Characterizing privacy leakage of public WiFi networks for users on travel. *INFOCOM*, 2013.

[128] Guidelines for 48-Bit Global Identifier (EUI-48) .

[129] J Martin, E Rye, and R Beverly. Decomposition of MAC address structure for granular device inference. In *Proceedings of the 32nd Annual Conference ...*, 2016.

[130] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. *Analysing the privacy policies of Wi-Fi trackers*. ACM, New York, New York, USA, June 2014.

[131] M Vanhoef, C Matte, M Cunche, and L S Cardoso. Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *Proceedings of the 11th ...*, 2016.

[132] J Franklin, D McCoy, P Tabriz, and V Neagoe. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. *Usenix ...*, 2006.

[133] Odroid XU4. http://www.hardkernel.com/.

[134] Blade RF. http://www.nuand.com/.

[135] L Leung and R Zhang. Mapping ICT Use at Home and Telecommuting Practices: A Perspective from Work/Family Border Theory. *Telematics and Informatics*, 2016.

[136] Francisco Pereira, Tom Mitchell, and Matthew Botvinick. Machine learning classifiers and fmri: a tutorial overview. *Neuroimage*, 45(1):S199–S209, 2009.

[137] T O'Shea, J Hoydis IEEE Transactions on Cognitive, and 2017. An introduction to deep learning for the physical layer. *ieeexplore.ieee.org*.

[138] H Ye, G Y Li, BH Juang IEEE Wireless Communications, and 2017. Power of deep learning for channel estimation and signal detection in OFDM systems. *ieeexplore.ieee.org*.

[139] T Wang, C K Wen, H Wang, F Gao China, and 2017. Deep learning for wireless physical layer: Opportunities and challenges. *ieeexplore.ieee.org*.

[140]

[141] J Schmidhuber Neural networks and 2015. Deep learning in neural networks: An overview. *Elsevier*.

[142] Geoffrey E Hinton. Deep belief networks. *Scholarpedia*, 4(5):5947, 2009.

[143] Yann LeCun et al. Generalization and network design strategies. *Connectionism in perspective*, pages 143–155, 1989.

[144] J S Atkinson, M Rio, J E Mitchell, and G Matich. Your WiFi Is Leaking: Ignoring Encryption, Using Histograms to Remotely Detect Skype Traffic. In *2014 IEEE Military Communications Conference (MILCOM)*, pages 40–45. IEEE, 2014.

[145] K P Dyer, S E Coull, and T Ristenpart. Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. *2012 IEEE Symposium . . .* , 2012.