THE UNIVERSITY OF NEW SOUTH WALES

SCHOOL OF ELECTRICAL ENGINEERING AND TELECOMMUNICATIONS

Characterising Wireless LAN Transmission Characteristics

Submitted in fulfilment
for the requirements
of the degree of
BE (Telecommunications)

Author: **PETER TZANNES**
Student Number: 3060440
November 2005

Supervisor:

Dr. Tim Moors
Senior Lecturer
School of Electrical Engineering & Telecommunications
University of New South Wales

Assessor:

Dr Vijay Sivaraman
Senior Lecturer
School of Electrical Engineering & Telecommunications
University of New South Wales

Thesis title: Characterising Wireless LAN Transmission Characteristics

Student Name: Peter Tzannes **Student ID:** 3060440 **Topic number:** TM35

A. **Problem statement**

This thesis is concerned with the analysis of signal strength and loss pattern (error rates) of IEEE 802.11g wireless LANs at the packet level. The efforts of which involves analysing a large quantity of data, collected at varied locations and times, using a consistent and reliable framework, so as to establish a confidence in the distribution of observable behaviour.

In the past, wireless trends have been investigated, where an attempt to capture, analyse and draw conclusions has been of primary importance. These trends have questionable relevance to the modern domestic and office environment, due to either the small collected data set, or biased experiments being performed in a single location within a single environment. This thesis tests a variety of hypotheses that are assumed within the wireless community, with the intent of exploring and determining a relationship (if any) from the data collected.

B. **Objective**

Analyse a large sample of data and determine the effects of signal strength and loss rates by segmenting the collected data into different propositions. Proceed by testing each hypothesis, with the intent of determining a relationship (if any), from the data collected. Analyse and segment the temporal variations of signal strength and PER. Produce a Markov model that contributes to the wireless community by understanding and relating packet loss to signal strength.

C. **My solution**

C programs were written that extracted and corrected the experiential data.
Use MATLAB to collate all produced C files
Use the weighted line of best fit method to incorporating the accuracy of router position and the distribution of data.
Use correlation, y-intercept and confidence intervals to analyse distributions
Use MATLAB to graph the variance of signal strength and PER
Produce an exponential distributed 2-state Markov model of the PER segmented by signal strength.

D. **Contributions** (at most one per line, most important first)

Create C and MATLAB programs to automate the extraction and analyses of data
Creation of spreadsheet so students can easily and efficiently enter data
Exponential distributed 2-state Markov Model
Incorporate the accuracy of router location into the weighted line distribution
Signal Strength and PER with observable trends including summary
Analysed and made conclusion from the graphed CI, y-intercept and correlation
Data collection period and accuracy of
Performed experiments to analyse the variability in distributed data

E. **Suggestions for future work**

Further C and MATLAB programs that analyse and determine the attenuation of different object, including wall type, metallic objects … Extend to include angle of incidence through walls (already calculated). Determine the precise amount of variability in the temporal variation of signal strength and PER.

While I may have benefited from discussion with other people, I certify that this thesis is entirely my own work, except where appropriately documented acknowledgements are included.

Signature: ________________________________ **Date: 31 / 10 / 2005**

Thesis Pointers

List relevant page numbers in the column on the left. Be precise and selective: Don't list all pages of your thesis!

8	Problem Statement and Objective
21-23	Reasons and Advantages

Theory (up to 5 most relevant ideas)

51	Weighted line of fit
58	Correlation, y-intercept, gradient and confidence intervals
25,27	Markov model with equilibrium probabilities
18-20 and 40	wireless impairments with ARF and MAC.
16	Shannon's information capacity theorem

Method of solution (up to 5 most relevant points)

45	C programs that extracted and corrected the experiential data.
51	Use MATLAB to collate all produced C files
44-45, 51-53	Incorporate the router accuracy into weighted line distribution
58,59	Use correlation, y-intercept, gradient and confidence intervals to analyse graphed distributions
55	Use MATLAB to graph the variance of signal strength and PER
56, 85	Produce an exponential distributed 2-state Markov model of the PER segmented by signal strength.

Contributions (most important first)

84-87	Exponential distributed 2-state Markov Model
44-45, 51-53	Incorporate the router accuracy into weighted line distribution
74-78, 79-84	Signal Strength and PER with observable trends including summary
78	Data collection period and accuracy of
89-99	Performed experiments to analyse the variability in distributed data
45-56	Create C and MATLAB programs for automation
33,126-128	Create spreadsheet so students can easily and efficiently enter data

My work

26, 56,	System block diagrams/algorithms/equations solved
89	Description of procedure (e.g. for experiments)

Results

60, 79, 84, 87, 89, 100, 106	Succinct presentation of results and significance of results

Conclusion

106	Conclusions from work
108	Suggestions for future research

Literature: (up to 5 most important references)

65, 70, 93	[14] Eckhardt, P., Steenkiste, P. 2003
80	[26] Arauz, J. 2003
38	[27] Joshua Bardwell 2004
29	[16] Haowei, B., and Mohammed A, 2003

Abstract

Wireless signals are omnidirectional in nature, and thus the environment in which wireless signals propagate may ultimately hinder network transmissions, resulting in an increase of lost and erroneous packets. An understanding of what produces these irregularities is essential due to their effect on network throughput, protocol design and in determining the location of access points.

This thesis is concerned with the analysis of signal strength and loss pattern of IEEE 802.11g wireless LANs at the packet level. The efforts of which involves analysing a large quantity of data, collected at varied locations and times, using a consistent and reliable framework, so as to establish a confidence in the distribution of observable behaviour.

In the past, wireless trends have been investigated, where an attempt to capture, analyse and draw conclusions has been of primary importance. These trends have questionable relevance to the modern domestic and office environment, due to either the small collected data set, or biased experiments being performed in a single location within a single environment. This thesis tests a variety of hypotheses that are assumed within the wireless community, with the intent of exploring and determining a relationship (if any) from the data collected.

The analysis is complimented by a range of further experiments aimed at testing possible reasons for the variability of the collected data.

Acknowledgements

The students enrolled in TELE4363, Session 1 of 2005, collected the data used within this thesis. Without their participation, this thesis would not have been possible. So firstly, I would like to thank them for their effort and allowing me to use the collected data within this thesis.

I would like to especially thank my supervisor, Tim Moors, who had the patience in explaining many detailed concepts, and for providing advice and feedback where appropriate. His continual support, and challenging my critical thinking was always interesting and in some cases entertaining.

“There is nothing like looking, if you want to find something.

You certainly usually find something, if you look,

but it is not always quite the something you were after.”

J.R.R. Tolkien: The Lord of the Rings

Table of contents

List of Figures

List of Tables

List of Abbreviations

AES - Advanced **E**ncryption **S**tandard

AP - Access **P**oints

ARF - Auto **R**ate **F**allback

Bps - Bits **p**er **s**econd

BSSID - Basic **S**ervice **S**et **ID**entifier

CI – Confidence **L**evel

CSMA/CD - Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection

DHCP - **D**ynamic **H**ost **C**onfiguration **P**rotocol

DSSS - Direct **S**equence **S**pread **S**pectrum

FEC - Forward **E**rror **C**orrection

FHSS - Frequency **H**oping **S**pread **S**pectrum

GUI - **G**raphic **u**ser **I**nterfaces

IBSS - Independent **B**asic **S**ervice **S**et.

IEEE - Institute of **E**lectrical and **E**lectronics **E**ngineers

IP - Internet **P**rotocol

IPO – Input, **P**rocess, **O**utput

LOS – Line **O**f **S**ight

MAC - Media **A**ccess **C**ontrol

MAC - Medium **A**ccess **C**ontrol

Mbps - Mega**b**its **p**er **s**econd

MIMO - Multiple **I**nput **M**ultiple **O**utput

MP - Measurement **P**oint

OFDM - Orthogonal **D**ivision **M**ultiplexing

OSI - Open **S**ystem **I**nterconnection

PER - Packet **E**rror **R**ate

QOS - Quality **O**f **S**ervice

RMSE - Root **M**ean **S**quare **E**rror

RSSI - Received **S**ignal **S**trength **I**ndication

SNR - Signal-to-**N**oise **R**atio

SSID - Service **S**et **ID**entifier

TCP - **T**ransmission **C**ontrol **P**rotocol

UDP - **U**ser **D**atagram **P**rotocol

WEP - **W**ired **E**quivalent **P**rivacy

WLANs - Wireless **L**ocal **A**rea **N**etworks

WPA - Wi-Fi **P**rotected **A**ccess

WPA-PSK - Wi-Fi **P**rotected **A**ccess **P**re-**S**hared **K**eys

1. Introduction

One major trend in the implementation of networking is the increased adoption of wireless networks, primarily due to the advantages it offers over its wired brethren. Current generation of wireless networking is considerably slower than conventional wired networks, limited by Shannon's information capacity theorem. More important, is wireless signals susceptibility to the electromagnetic propagation in an omnidirectional manner. This gives rise to the characteristics of wireless propagation (e.g. interference and attenuation) and the resulting objects (e.g. metallic objects and other unlicensed 2.4Ghz products) that can hinder or impair wireless network transmissions. This ultimately results in higher loss rates, which reduces the bandwidth available to the end user. Thus understanding wireless characteristics is fundamental for improving transport protocols leading to a reduction in errors and resulting in increased network throughput and determining an optimum position to achieve maximum wireless performance.

To confidently characterise wireless propagation, a large data set was collected from the students enrolled in TELE4363 as part of the practical component of the course. Using a consistent and reliable framework was fundamental for the success within the analyses phase, where the large data set was collected at varied locations and times, as to establish a confidence in the distribution of any observable behaviour.

The focus within this thesis is the analyses of wireless LAN characteristics through the collection of a large data set, which can be divided into three separate stages:

1) *Pre-Analyses:* before the analyses could be begin, the preparation and alteration into a suitable form was critical. C programs were written that extracted, corrected and collated the experiential data to establish a single location that contained all information from a single sample.
2) *During-Analyses:* Once the C programs had been written, MATLAB programs that extracted the data within the created C files were produced. The weighted line of best fit was used incorporating the accuracy of router position and the distribution of data. Other MATLAB programs that accurately produced trends were also graphed.
3) *The analyses:* The analyses phase consisted of three separate tasks:
    1) The static modelling of signal strength and packet error rates. This incorporated determining the relationship (and distribution) of signal strength and packet errors including the examination of interference, room type, humidity, ducted air-conditioning and the amount of people within the dwelling.

2) The temporal variation of signal strength and packet error rates. This included observing any trends over time and incorporated the relationship between signal strength and packet error as a Markov model.
3) Experimental data was collected where two objectives were prominent:
    - Analyse potential causes of variability in data collection.
    - Analyse other general transmission characteristics to the wireless community.

The structure of this report is organised as follows:

The **second** section is an overview of wireless LANs outlining the fundamental operation, architecture and standards.

The **third** chapter continues by explaining why the study of WLANs was chosen, outlining the advantages, the current maximum transmission rate limit, then proceeds to give a brief description for the reason of loss within a wireless network by describing wireless impairments, then proceeds to explain the advantages of understanding wireless characteristics.

The **fourth** chapter gives an overview of Markov modelling, including the process used to calculate the transitional probabilities and the equilibrium probabilities.

The **fifth** chapter provide an overview of past works and presents the approach of this thesis.

Chapter **six** outlines the collection process in three sections: the preparation, the mapping of the dwelling, and finally an overview of the data collection process.

The **seventh** chapter outlines the preparation before the analyses can begin and includes extracting relevant data and an explanation of the produced C and MATLAB programs.

Chapter **eight** outlines the analyses process including the distribution of signal strength and loss rates, interference from 802.11 sources, the impact of room type, air-conditioning, humidity and the amount of people within the dwelling are explored. The temporal variation of signal strength and packet loss is also investigated including the creation of a two-state Markov model.

Chapter **nine** explores the potential reasons for the large variability of data that exists and includes the variation of other wireless characteristics by performing a variety of experiments.

The **final chapter** provides general conclusions along with future works.

2. An overview of the Wired Free Network

A **Wireless Local Area Network (WLAN)** is a transmission system that uses radio waves as a carrier for the propagation of data, hence the origin of the expression a "wired free network". A WLAN (also referred to as a wireless network in its primary form) can be identified by consisting of the following three fundamental components:

- ***Wireless hosts*** are the end-systems where wireless communication is sent from or transmitted too.
- ***Base stations*** or ***access points*** are responsible for sending packets to and from the connected wireless hosts, and acts as a bridge between the wireless and wired networks.
- A ***wireless link*** is the physical wireless (transparent) connection that bridges the gap between the wireless hosts and base station.

The components above are illustrated in figure 1, below:

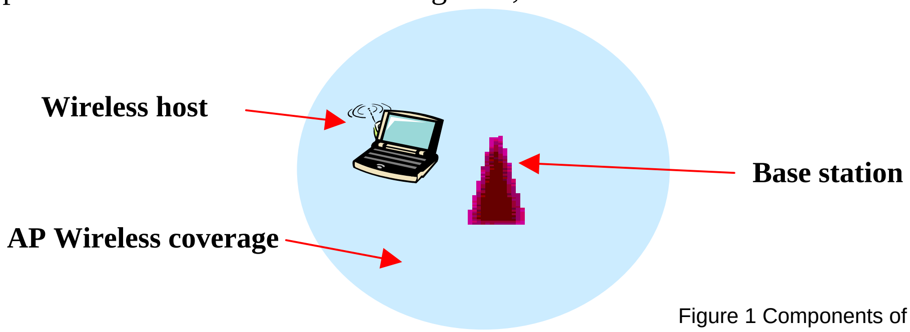


Figure 1 Components of an 802.11 WLAN

If the above components are to communicate successfully, a wireless standard was needed to ensure the harmonious interoperability and compatibility of devices among manufacturers. The Institute of Electrical and Electronics Engineers (IEEE) ensured that this could occur with the 802.11 standard. This globally recognised association has provided and ratified all 802.11 standards for the past two decades.

The characteristics of these 802.11 standards are briefly outlined in table 1:

Characteristics	**Description**
Frequency bands	2.4Ghz or 5Ghz
Maximum Transmission rates	11 Mbps (11b), 54Mbps (11a/11g)
Range	From 10 meters up to 100 meters
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hoping Spread Spectrum (FHSS), Orthogonal Division Multiplexing (OFDM)
Data and Network Security	WEP, WPA, WPA-PSK. (AES considered for 802.11i) Authentication and integrity
Advantages	No cables, ease of installation, flexibility, mobility, competitively priced.
Disadvantages	Unlicensed spectrum thus more interference - higher error rates, performance, security attenuation.

Table 1 Brief description of the characteristics of the 802.11 standard.

2.1 Wireless LAN architecture

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network [1].

In **Infrastructure mode** wireless hosts communicate with a base station which allows the broadcasting, forwarding, coordination, synchronisation and bridging of packets. The area covered by an AP (a cell) is technically referred to as a **Basic Service Set (BSS)**. A **Service Set Identifier (SSID)** identifies every BSS, and is ultimately the identification given to devices within a specific cell to enable wireless communication. A SSID however, need not be unique and thus a **Basic Service Set Identifier (BSSID)** was needed, which uniquely identifies an access point, and is usually the AP's **Media Access Control (MAC)** address.

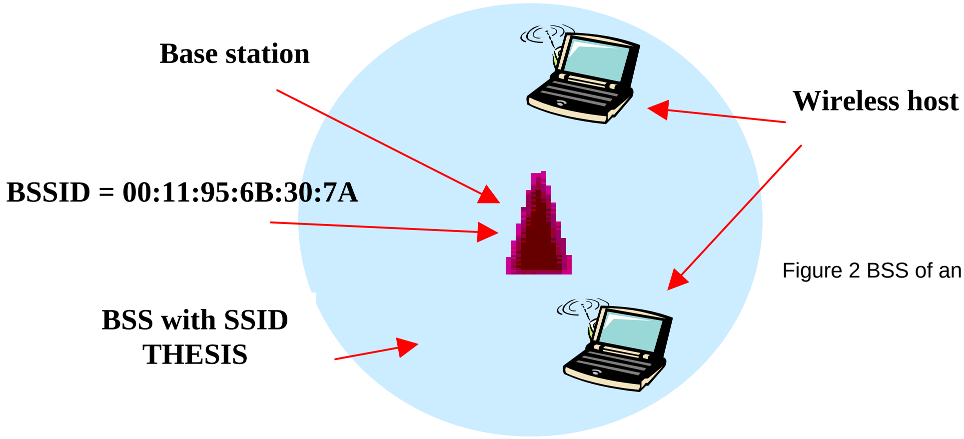


Figure 2 BSS of an infrastructure network

In an **Ad hoc** network, (called an **Independent Basic Service Set (IBSS)** by the 802.11 standard), allows a group of 802.11 wireless stations to communicate with each in peer-to-peer mode without the need for an access point.

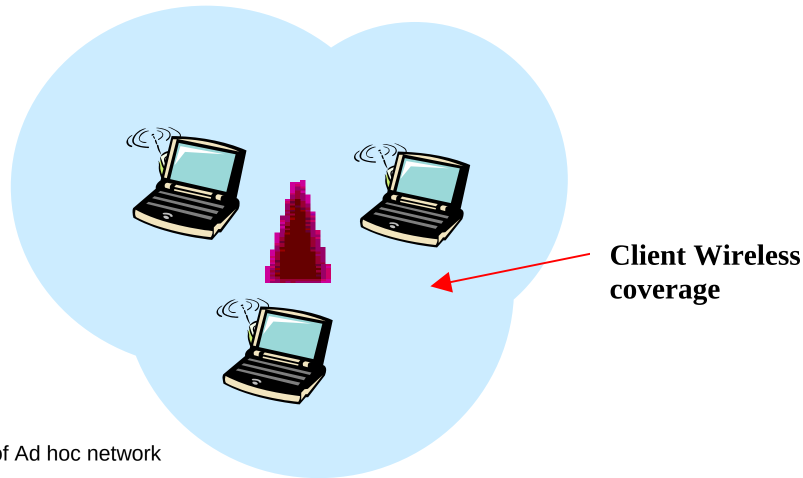


Figure 3 BSS of Ad hoc network

This thesis will only focus on infrastructure network, due to their predominant use.

2.2 802.11 and the OSI reference model

The **OSI (Open System Interconnection)** reference model is a worldwide standard that defines the framework for implementing protocols in seven layers. The exact physical operation within each layer is not described and thus the exact services and protocols are not prearranged. The OSI reference model describes the purpose and reason for existence of each layer within a given protocol construct. The fundamental advantage of creating a standard is the ability to completely modify or change a given layer without the need to alter any other layers within the overall system. The seven layers of the OSI architecture are:

Layer	Level
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Table 2 The seven OSI layers

Because of the widespread adoption of the OSI model, the primary functions of the 802.11 standard operate within the final two layers.

2.2.1 The Physical layer

The four modulation techniques defined in the 802.11 standards include:

- Infrared at 850-950nm
- FHSS in the 2.4 GHz band
- DSSS in the 2.4 GHz band
- OFDM in the 2.4GHz and 5GHz band for 802.11g/a networks respectively.

The physical layer determines if a wireless standard is interoperable with other wireless standards. FHSS and DSSS are not interoperable, however OFDM and DSSS are.

2.2.2 The Data Link layer

The data link layer is divided into several sublayers, which include:

Layer	Description
Driver interface	Linux wireless Extension, Windows Network Device Interface Specifications
LLC	Logical Link Control
802.11 bridging	Uses only in Access points. And example is the Spanning tree protocol
Security	e.g. WEP, WPA
MAC	Medium Access Control
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent

Table 3 The sublayers of the data link layer in wireless LANs

The most important of these layers is the Medium Access Control sublayer. This sublayer is designed to coordinate the use of the physical medium by controlling the transmission of packets from multiple stations, where a station is either a host or an AP. This is accomplished by using the random access protocol- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**. As the name implies, a station that wishes to transmit a packet first needs to ‘sense’ the channel. If the channel is busy, the station defers the transmission for a random period. If no activity is detected however, the station proceeds to transmit the packet (after waiting a small random period of time). If the received packet is intact, the receiving station proceeds to send an acknowledgement back to the sender. If the sender does not receive this packet in a finite length of time, the sender assumes that the packet has been lost and proceeds to retransmit the assumed lost packet. The retransmission of lost packets is a concern for this thesis, as will interfere with any legitimate measurements and thus will pollute collected results.

2.3 Discovering wireless LANs

All wireless devices need to discover and communicate with an AP within a BSS. This occurs through either of the following methods:

1) AP can be configured to periodically broadcast **beacon frames**. These frames can be received by all stations within the broadcast region.
2) The wireless device can send a **probe packet** attempting to find any AP.

Both of the above discovery methods need to indicate such information as the SSID, potential wireless channels and potential transmission rates. The 802.11 MAC layers are responsible for the above association process. Once the association process has occurred, a logical mapping exists between the AP and the host. Each host however, can only associate with a single AP at a given instance in time, conversely an AP can associate with numerous hosts.

Kismet is a program that can capture and report to the user all collected beacon frames, and thus is a good method of detecting other WLANs in the vicinity. Kismet will thus be used to discover potential sources of interference.

2.4 Wireless LAN Standards

The first 802.11 standard was created as a method of extending the 802.3 (wired Ethernet) to venture into the wireless domain. The 802.11 standard, also referred to as Wi-Fi, as it is the Wi-Fi alliance (an independent organisation) that provides Wi-Fi certification to products that conform to the 802.11 standard. Current 802.11 standards that have been certified and are in use include:

Standard	Data Rate	Frequency	Modulation Scheme	Range	Security	Certified
802.11	1 or 2Mbps	2.4Ghz	FHSS or DSSS	< 25m	WEP & WPA	1997
802.11a	Up to 54Mbps	5GHz	OFDM	< 20m	WEP & WPA	1999
802.11b	Up to 11Mbps	2.4GHz	DSSS	< 100m	WEP & WPA	1999
802.11g	Up to 54Mbps	2.4GHz	OFDM above 20Mbps, DSSS below 20Mbps	< 100m	WEP, WPA & WPA-PSK	2003

Table 4 Current 802.11 certified standards.

The following standards either have been unapproved or are currently under development.

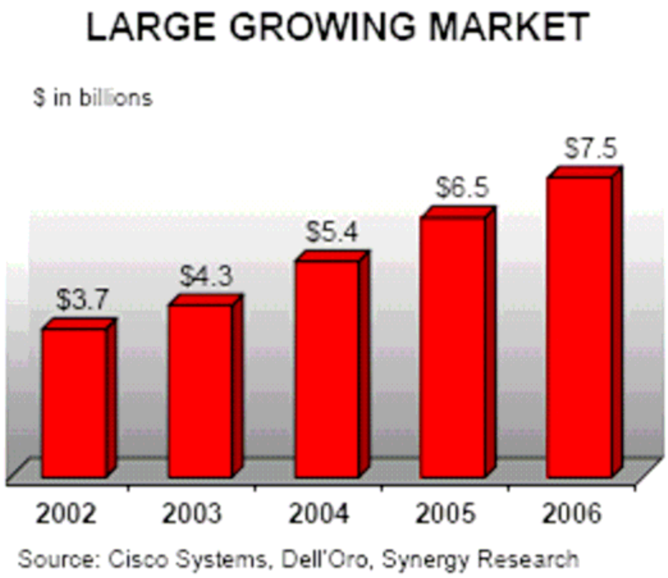
Standard	Brief Description
802.11d	International (country-to-country) roaming extensions.
802.11e	Enhancements: QoS, including packet bursting
802.11F	Inter-Access Point Protocol (IAPP)
802.11h	5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control (TPC) for European compatibility
802.11i	Enhanced security - (ratified 24 June 2004)
802.11j	Extensions for Japan
802.11k	Radio resource measurements
802.11l	Reserved
802.11m	Maintenance of the standard; odds and ends.
802.11n	Higher throughput improvements
802.11o	Reserved
802.11p	WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
802.11q	Reserved
802.11r	Fast roaming
802.11s	Wireless mesh networking
802.11T	Wireless Performance Prediction (WPP) - test methods and metrics
802.11u	Inter-working with non-802 networks (e.g., cellular)
802.11v	Wireless network management
802.11w	Protected Management Frames

Table 5 Unapproved or currently under development 802.11x standards [2]

3. Why the examination of Wireless LANs?

The uptake of WLANs has increased in recent years as shown in the figure below, where the trend within the wireless market is a steady increase in sales from consumer demand. From this graph, it is evident that wireless technology is the future because of the simple fact that many consider wireless a better and more convenient solution than a wired network. However, this does not answer the essential question as to why this uptake has occurred. The answer to this question lies in a number of reasons. Fundamentally, wireless networks share the standard advantages with its wired counterpart namely the ability to share files, multimedia, peripherals and an Internet connection, but also provides many more advantages that conventional wired networking lacks. These include:

Figure 4: Growth of the Wireless Market



- Ease of installation –no cable infrastructure needed.
- Flexibility – Not limited to a specific desk that is located close to a wall jack, but rather the user has the ability to connect to a network anywhere within the wireless coverage area.
- Mobility and Convenience – Can physically move around within the wireless coverage area and still maintain network access.
- Price – wireless devices are competitively priced against wired devices.

From these advantages, wireless technology has certainly matured and as the performance, reliability, and price continues to improve, WLANs will ultimately become more popular in our everyday lives. However, while these advantages for WLANs do exist, they are not the primary reason why WLANs was chosen to be studied.

3.1 The consumer

The consumer at present has only one obsession, the constant and growing demand for higher and higher transmission rates. This speed factor is important for two reasons:

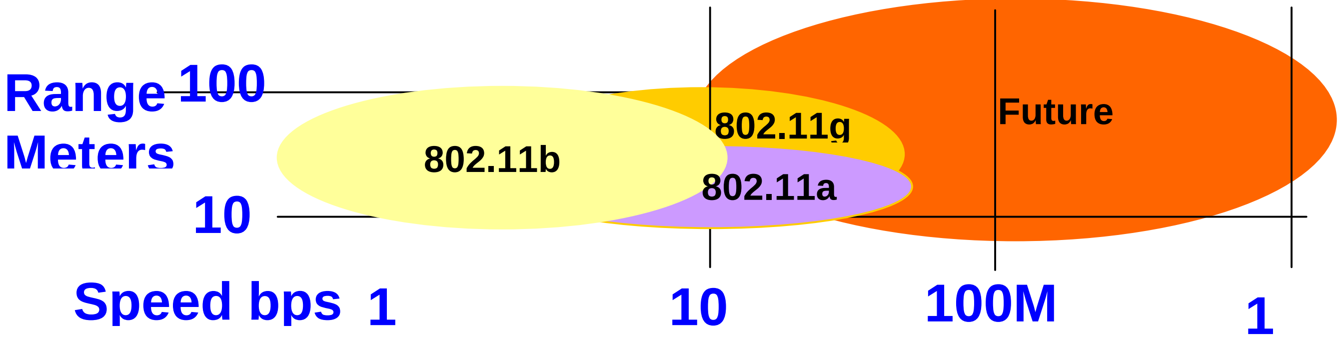
1. Current generation of wireless protocols (shown in the figure 5 below) are considerably slower than conventional wired networks, which are currently operating at a theoretical maximum of 1Gbps. Thus, the need for wireless networks to provide

the same amount of throughput as wired networks has helped the drive for increase throughput.

2. Higher speeds are essential for the new generation of multimedia that will traverse these wireless networks.

The question now becomes, can the transmission speed of wireless networks be increased to achieve speeds that are comparable to wired networks?

Figure 5 Representation of wireless media speeds and potential distances.



3.2 The Problem

Wireless throughput is considerably slower that its 802.3 wired Ethernet counterpart. However, why this limitation has occurred in modern wireless networks is an important and fundamental constraint to the future of wireless networking. The answer to this question lies in Shannon's third and (most famous) theorem, the **information capacity theorem** [3]:

The information capacity of a continuous channel of bandwidth B hertz, perturbed by additive white Gaussian noise of power spectral density $N_0/2$ and limited in bandwidth to B, is given by:

$$C = B \times \log(1 + \frac{P}{N_0 B}) \text{ bits per second}$$

where P is the average transmitted power and we are operating in log to the base 2.

The above theorem implies that, assuming Gaussian noise and given, the bandwidth of the communication channel along with the transmitted power of the signal then it is physically impossible to achieve a higher transmission rate than C bits per second. Thus, the information capacity theorem defines an upper bound on the transmission rate for a given channel assuming an error-free transmission. Consequently, the capacity of a communication channel can be improved by either increasing the channel bandwidth or by increasing the transmitted power. The transmitting power of a signal however, is limited as instructed by the 802.11 standard. Thus, the bandwidth is consequently the only other alternative than can be altered. The 802.11 standard however, segregates the unlicensed frequencies. For example, the 2.4GHz band is divided into 14 separate channels, ranging from channel one at 2.412GHz to channel fourteen at 2.484GHz where adjacent channels

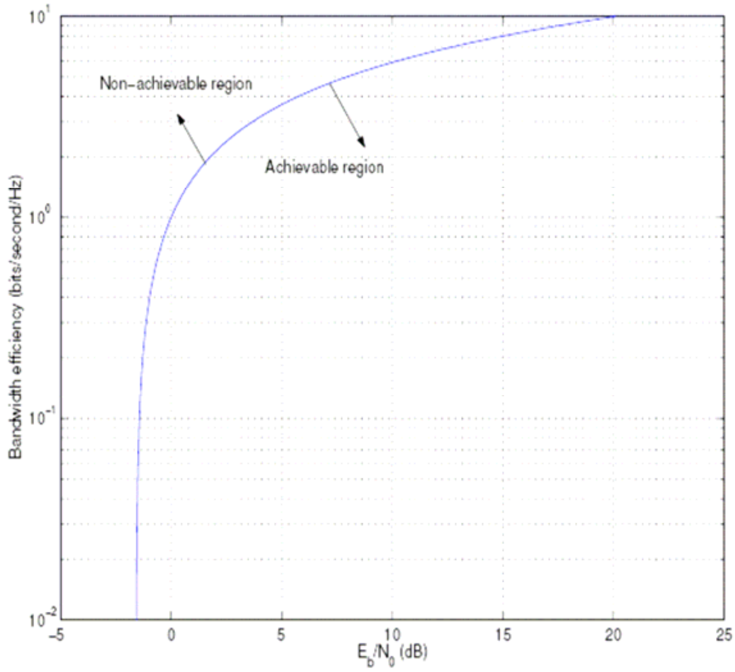


Figure 6. Limit of wireless communication. (Diagram taken from [3])

are separated by 5Mhz. The 802.11b/g standard, that use the 2.4GHz band, requires 22MHz for each channel to operate with minimal interference. [4] Thus, given the 22Mhz separation between channels, this results in only three channels that can exist simultaneously (for example, channels 1, 6 and 11) to provide a minimal of interference. Thus, increasing the bandwidth per channel will result in a further increase to interference.

Shannon's information capacity theorem (given above) uses *P* as the average transmitted power. However, the transmitted power of a signal can be composed of the transmitted bit energy multiplied by the capacity, that is:

$$P = E_b \text{ (energy/bit)} \times C \text{ (bits/second)}$$

The information capacity theorem can be rewritten as:

$$C = B \times \log(1 + \frac{E_b C}{N_o B})$$

Using the above formula, a graph can be drawn (figure 6) that illustrates the achievable regions and non-achievable regions of today's wireless networks. Currently a low energy per bit value and modest bandwidth efficiency, places today's wireless networks relatively close to the graphed blue line. Thus, the peak in terms of capacity per channel has effectively been reached. From here two options exist:

1. Increase the amount of antennas in the system, where all antennas send and receive data simultaneously, this is referred to as a MIMO (Multiple Input Multiple Output) system. This has been proven to increase the capacity of the system [5 6, 7].
2. Study better methods of channel utilisation.

This thesis pursues the second option, where the characteristics of errors are attempted to be analysed and understood. The reasons for which are discussed below.

3.3 Wireless LANs and characteristics

It is common knowledge that today higher transmission error rates are a common and fundamental feature of wireless networks. **From here on, I shall refer to errors rates, as packets that are transmitted over a wireless network that are ultimately not received by the receiver, that is, the data sent is completely lost**. Higher error (loss) rates occur, because unlike the wired world where transmission occurs through a guided media, wireless signals radiate in an omnidirectional manner. This leads to wireless media being susceptible to the properties of wireless propagation (refer to 3.4.1) and vulnerable to objects within the physical environment (refer to 3.4.2). Both of these aspects will ultimately result in a degradation of signal strength, and ultimately an increase of lost packets can result. These higher loss rates are a hindrance to wireless networks and need to be overcome, but before this is achievable the detailed characteristics of wireless errors needs to be understood.

A complete understanding of errors, that is, when errors occur and their reason for occurrence, is an extremely complex task. The method used currently to enhance the understanding of the behaviour of errors within an environment is the creation of statistical models. The aim of such mathematical model is to accurately characterise the behaviour and events of a system as a set of variables, states, and/or set of equations. Thus, a successful statistical model is a complete and accurate representation of the actual behaviour of a wireless network.

3.4 Properties that affect wireless propagation – wireless impairments

Wireless networking provides a convenient and flexible solution to networking without cables, however, with this freedom comes a sacrifice. This sacrifice is the inability to control the path of the wireless signal, as current generation of wireless signals are transmitted in an omnidirectional manner. This gives rise to the characteristics of wireless propagation and the resulting objects that can interfere or impair wireless network transmissions, and include:

3.4.1 Characteristics of wireless propagation.

These impairments are due to the fundamental and physical method in which a wireless signal propagates and include:

Atmosphere absorption contributes to impairments due to water vapour and oxygen.

Noise can be divided into thermal noise and surrounding noise.

- Thermal noise is the motion of electrons caused by heat. This is present in all electronic equipment and cannot be eliminated, only reduced.
- Surrounding noise, as the name implies includes noise from the surrounding indoor and outdoor environment. When the noise maintains a level that is significantly higher that the received signal, errors will be produced.

Interference encompasses three aspects:

- Multi-path interference can be destructive or constructive where obstacles reflect and or scatter the transmitted wave, which could result in multiple copies with varying delays at the receiver, or
- Other devices sharing the same frequency spectrum, or
- Inter-symbol interference results when multiple signals are received at the same time, and the receiver cannot reliably distinguish between these two signals, resulting in interference, which can cause errors.

Attenuation is the loss of a transmitted signal.

- Antennas in wireless LANs are omnidirectional (transmit a signal in all directions) as apposed to directional antennas. The transmitted energy that is transmitted by the sender decreases by the inverse square of the distance travelled by the wave.
- Due to objects being situated in the path from the transmitter to receiver, where each can potentially absorb the signal and a loss in signal strength can result.

Reflection, diffraction, and scattering due to objects that exist in the physical environment.

- Reflection occurs when the transmitted signal bounces back of a conducting object, such that the angle of incidence equates to the angle of reflection. If many waves are reflected, it is referred to as multipath fading, and the signal is often referred to as a Rayleigh distributed.
- Diffraction, (mathematically and physically explained by Hugen’s principle), occurs when there is no direct Line of Sight (LOS) from sender to receiver and the signal encounters an impenetrable body (opaque) and the signal changes path and direction and continues travelling around the impenetrable object.
- Scattering occurs when the radio channel contains objects of dimensions that are on the order (or less) of the electromagnetic wavelength, causing the signal from the transmitter to be radiated in more than one direction.

Doppler shift occurs when the transmitter and/or receiver are physically moving and causes the frequency to shift, and thus complicates the reception of the signal.

Note: the above impairments were combined from sources [8, 9, 10]

3.4.2 Physical properties within the environment

Objects within the path of a wireless signal can fundamentally alter the characteristics of the signal. The table below outlines the varying attenuation, noise sources and interference for a variety of different objects.

Attenuation factor	**Objects**
Very high	Metallic objects, Reinforced concrete
High	Concrete
Medium	Water, Bricks, Stone
Low	Glass, Plaster, Wood
Minimal	Air
Noise sources	
Indoor	Motors, Microwaves
Outdoor	Power lines, railway
Environment	Lightning, Solar flares
Interference	
Unlicensed Spectrum	Other WLANs, Bluetooth devices, cordless phones
Multipath Interference	Reflection/diffraction/scattering of metallic objects

Table 6 Degree of Attenuation for some objects [9]

3.4.3 Fresnel zones

It is a common misconception that only objects within the line of sight between the sender and receiver will affect the transmission characteristics and impair the wireless transmitted signals. However, many if not all of the above-mentioned impairments can have varying affects on the transmitted wireless signal. The question however, is to what extent objects surrounding the line of sight between sender and receiver are considered a threat to the transmitted signal. The answer derived and founded from optics by the physicist Augustin-Jean Fresnel is the use of Fresnel zones.

The Fresnel zone is the physical propagation path of the signal, which are radii of the concentric ellipsoids around the LOS path between sender and the receiver's antennas. The maximum cross sectional radius (r) at the midpoint (see figure 7), that is, the largest outer zone boundary radius (at the midpoint), between the direct LOS can be calculated by [11]:

$$r = 13.1979\sqrt{(6.2137\times 10^{-4})d/(4\times f)}$$

where:

r = Radius in meters

d = Distance in meters

f = Frequency in GHz

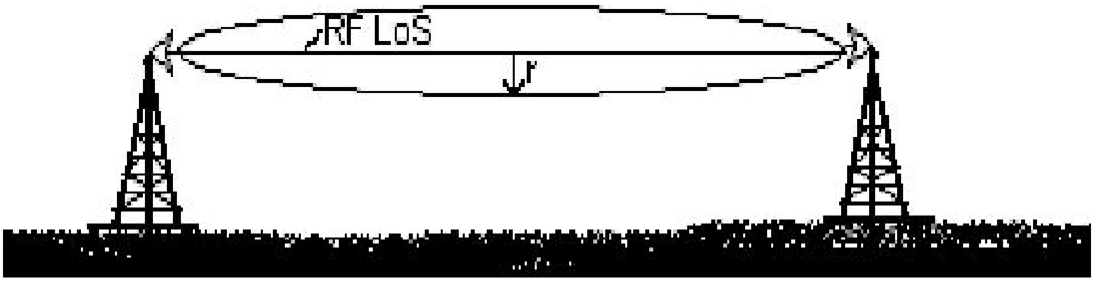


Figure 7 Fresnel zone between two antennas indicating the largest outer zone boundary radius [12].

The fundamental reason for the introduction of Fresnel zones is because all objects within the calculated radius need to be considered when analysing the transmission path between two points. For objects to be clear from interfering with wireless signal, then 60% of the 1st Fresnel zone (calculated by r) needs to be clear in DSSS transmitted systems and 80% of the 1st Fresnel zone needs to be clear for FHSS systems [13]. Some calculations assuming DSSS are given in table 7.

However, based on the table produced the radius of the 1st zone is too narrow, only 0.2 at 10 meters from the router, and thus is too narrow to be of significance compared to the accuracy of data collected.

Meters	**r (meters)**
1	0.06
2	0.09
3	0.11
4	0.13
5	0.14
6	0.15
7	0.17
8	0.18
9	0.19
10	0.2

Table 7 Fresnel Zone Clearance Calculations for a DSSS transmitting system

3.5 Reasons and Advantages of the Characterisation of Errors

Less information is available on the error rates in wireless networks compared with their wired counterparts as the characterisation of the error environments in wireless networks are very complicated. When signals propagate through space, many more factors (as outlined above) can influence the transmitted signals than when the signal propagates through an electrical conductor or fibre [14]. Moreover, since WLANs are a relatively new technology, many protocols were designed for wired networks and thus an increased understanding of transmission error characteristics is essential for the development and alteration of current standards to fit into the new era of wireless networking. Furthermore, when wireless protocol developers are designing new protocols, they do not have the luxury to use network simulation packages such as OPNET, as the current generation will essentially assume a free space like model [15]. That is, the region between the transmitter and receiver is assumed free of all objects that might absorb or reflect the propagation of the wireless signal, and only high attenuation devices (within table 6) are taken into consideration. Obviously, this model is not an accurate representation of the real world.

Currently, wireless engineers are using wireless loss models to predict path propagation loss, for example the Lee model. This ensures an accurate estimation of path loss to help select locations of base stations [16]. This method obviously does not account for many other objects within the path from sender to receiver. However, it is worth noting that current wireless network designers and research groups do have a number of schemes for improving wireless communication, some of which include:

1) In the physical layer:
   - The use of modulation techniques to deal with multipath interference. An example is the use of OFDM in 802.11g wireless networks and is used as a method of dealing with multiple signals with differences phases.
   - The use of Forward Error Correction (FEC) as a technique for error control, which is used by the receiver to improve error rates.

2) Use multiple antennas:
   - To increasing transmission speeds (such as the use of MIMO)
   - For antenna diversity or redundancy. The receiving station can obtain multiple observations of an incoming signal. When demodulation occurs, only a single packet is used from the multiple observations. The technique used is a proprietary one based on the brand of the wireless receiver.

3) Techniques to improve TCP performance in the presence of errors that are in current used or based on theory. These techniques are used to improve performance and can be classified based on the nature, of the action taken: [4]
   - Hide error losses from the sender. This includes techniques such as Snoop, Split Connection approach, Delayed Duplicate Acknowledgements and Link Layer Retransmissions.

- Inform sender of packet loss, which includes techniques such as Explicit Notification and Sender based Discrimination.

Most importantly however, are what advantages would exist if an understanding of error characteristics could be attained?

1. Improve the amount of resilience needed. This could include innovative modulation techniques or transport layer protocols that can adapt to varying needs of wireless communications, which could result in meeting the demands of different operating environments or meeting Quality of Service (QOS) requirements.
2. High error rates can significantly reduce the throughput of wireless networks. Reducing the amount of errors will result in an increase of successful packets that traverse the network, which will ultimately increase the throughput. Thus, understanding, controlling and minimising error rates are crucial.
3. Improve the location of AP. One of the most important characteristics of the propagation environment is the path (propagation) loss. An accurate estimation of the propagation loss provides a good basis for a proper selection of base station locations and a proper determination of the frequency plan. By knowing propagation losses, one can efficiently determine the signal strength, signal-to-noise ratio (SNR) and carrier-to-interference which could ultimately maximise network coverage.

Due to the above theoretical advantages, there is an increasing and growing interest especially among wireless manufactures to iron out and characterise the loss of packets within wireless networks. Network protocol developers and algorithm designers are especially interested in packet errors, since most of the higher-layer applications (running on top of the link layer) exchange blocks of data between peers [16]. Thus the understanding and the characterising of these errors is important for the development of new protocols and the increase of throughput for the new age of multimedia that will traverse wireless network. Ultimately a solution for improving wireless communication should be dependent on the nature of the error pattern, and thus an understanding of the occurrence of errors along with a knowledgeable comprehension of signal strength and path loss analysis is fundamental to the future of wireless communication.

4. Mathematical Modelling

The objective of a mathematical model is to accurately characterise the behaviour and events of a system. Thus, the mathematical model describes the components of a system as a set of variables, states, and/or set of equations and establishes the affiliations between these components. A problem arises when deciding on the form of a model, as each can be classified depending on system characteristics including: linear or non-linear, deterministic or probabilistic, static or dynamic, time varying or time-invarying, continuous or discrete.

In many instances, the output of a system can be characterised into a finite number of states. A widely used model within the wireless community is the 2-state Markov model first introduced by Gilbert [17] then extended by Elliot [18], and is known as the Gilbert-Elliot model. It is this model that has been widely used to **statistically** analyse **packet loss within wireless networks**. Empirical observations of wireless networks, have resulted in [17], [18], [19], [20], [21] and [22] using a 2-state model as an approximation to the loss of packets within a wireless network.

4.1 The Markovian Process

The easiest method of understanding the Markov process is by an example, the easiest of which is the coin toss example illustrated in [23]:

Two rooms exist R1 and R2, where a person is placed within each room, P1 and P2 respectively. A barrier is placed between the rooms, thus the person in room one (P1 in R1) cannot see what is happening within room two (R2). The person in room 2 performs a coin tossing experiment, where he informs P1 of the results of the coin toss. Thus, P1 is only given a sequence of observations (O_1, O_2 …. O_i) that are either heads (*H*) or tails (*T*).

$$O = O_1\, O_2\, O_3\, O_4\, O_5\, O_6$$
$$= T\; H\; H\; T\; H\; T\; T$$

If P1 assumes that a single unbiased coin is being used, (the probability of heads is the same as tails), then two states (S_1 *and* S_2) can be used, where each state corresponds to a side of a coin.

$$S = S_1 \text{ and } S_2$$

These states correspond to the two circles in figure 8 where the arrows between the states represent the unbiased transitional probabilities. The transitions may lead to another state, or back to the same state. From this diagram however, it is evident within any Markovian process the probability of a certain observation q_i at time i is only dependant on the observation at q_{i-1} at time i-1, and does not dependant on other previous observations q_{i-2} q_{i-3}

… q_1. That is, the past is irrelevant in calculating the next state, and is only conditionally dependant on the present state, and so:

$$P(q_i|q_{i-1}, q_{i-2}\ldots q_1) = P(q_i|q_{n-1})$$

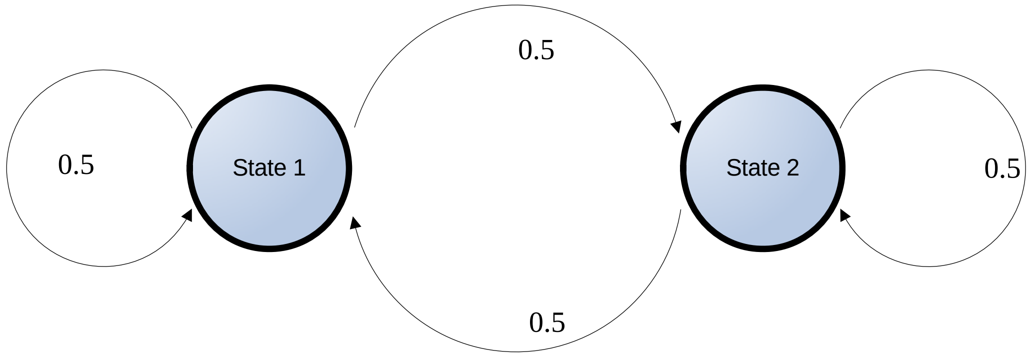


Figure 8 An example of a two-state Markov Model

For the modelling of packet errors within wireless networks, two states exist, and correspond to a **successfully received state**, **the good state**, and **a lost state**, **the bad state**. The number 1 will identify a successfully received packet from here on, while a 0 will identify a lost packet. Thus, it is these observations, the 1's and 0's that will be used to create the two-state Markov model.

An example:

Given the following packet observations with high packet loss, the derivations of all transitional probabilities can be calculated and a two-state model created:

0, 1, 0, 1, 1, 0, 0, 0

By observing the given sample, **four** different **transitions** are possible:

1. 0 -> 0 (lost packet to a lost packet)
2. 0 -> 1 (lost packet to a received packet)
3. 1 -> 0 (received packet to a lost packet)
4. 1 -> 1 (received packet to a received packet)

Assuming the **initial** Markov state is 1, the sample input then becomes:

1, 0, 1, 0, 1, 1, 0, 0, 0

with transitional probabilities:

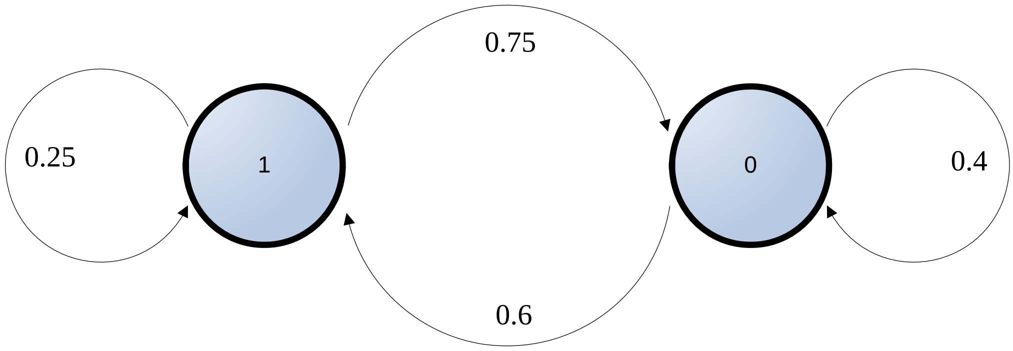
$$P(0|0) = P(0 \to 0) = \frac{\text{number of } (0 -> 0) \text{ transitions}}{\text{total number of } 0\text{s}} = \frac{2}{5} = 0.4$$

$$P(1|0) = P(0 \to 1) = \frac{\text{number of } (0 -> 1) \text{ transitions}}{\text{total number of } 0\text{s}} = \frac{3}{5} = 0.6$$

$$P(0|1) = P(1 \text{->} 0) = \frac{\text{number of } (1\text{->}0) \text{ transitions}}{\text{total number of 1s}} = \frac{3}{4} = 0.75$$

$$P(1|1) = P(1 \text{->} 1) = \frac{\text{number of } (1\text{->}1) \text{ transitions}}{\text{total number of 1s}} = \frac{1}{4} = 0.25$$

where the corresponding Markov model is diagrammatically represented as:



The calculated transitions can also be represented by a **transitional matrix**, in the following form:

$$\begin{pmatrix} P(0|0) & P(0|1) \\ P(1|0) & P(1|1) \end{pmatrix} = \begin{pmatrix} 0.4 & 0.75 \\ 0.6 & 0.25 \end{pmatrix}$$

that is: $P(0|0) + P(1|0) = 1$ => (the sum of all columns must add to 1)

or more generally: $P(0|s_j) + P(1|s_j) = 1$

$$p_0\, s_j \;+\; p_1\, s_j \;=\; 1$$

where the sum of the columns must add to 1.

However, while the transitional probabilities are fundamental to the Markov process another set of probabilities can be derived referred to as the **equilibrium or stationary probabilities**, denoted by p_o and p_1, for the states S_0 and S_1 correspondingly. What these probabilities mean, is no matter the initial state, **after a large number of iterations, the probability that the process is in state S_i is p_i** [24]. The method used to derive these probabilities is given in [24] and is adapted as follows:

Assuming that equilibrium has been reached and you are moving from the q^{th} position to the $(q + 1)^{th}$ then:

$$\begin{aligned} p_i &= P(S_i \text{ in position } q + 1) \\ &= P((0\ x\ S_i) \text{in position } q^{th} \text{ and } (q + 1)^{th} \text{ position}) \\ &\quad + P((1\ x\ \overline{Si}\ ) \text{ in position } q^{th} \text{ and } (q + 1)^{th} \text{ position}) \\ &= P(S_i \text{ in } (q + 1)^{th} | 0 \text{ in } q^{th}) P(0 \text{ in } q^{th}) \\ &\quad + P(S_i \text{ in } (q + 1)^{th} | 1 \text{ in } q^{th}) P(1 \text{in } q^{th}) \end{aligned}$$

$$= P(Si|0)P(0) + P(Si|1)P(1)$$

$$= p_{i0}p_0 + p_{i1}p_0 + p_{i0}p_1 + p_{i1}p_1$$

$$= (p_{i0} + p_{i1})p_0 + (p_{i0} + p_{i1})p_1$$

thus $p_i = \mathbf{p} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ and by observing the final result closely it can be seem that

p = (transitional matrix) **p**

= **Mp** **(**where **M** is the transitional matrix)

Thus, two equations exist:

$p_0 + p_1 = 1$ (since **p** is a probability vector)

$(\mathbf{M} - \mathbf{I})\mathbf{p} = 1$ (since pi = **Mp** and thus pi is an eigenvector with eigenvalue equal to 1)

where I is the 2 *x* 2 identity matrix

The two given equations can be placed into a single matrix as follows and solved algebraically:

$$\begin{pmatrix} 1 & 1 \\ P(0|0) & P(0|1) \\ P(1|0) & P(1|1) \end{pmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

This will produce the vector in the following form:

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} \text{equilibrium 0 state} \\ \text{equilibrium 1 state} \end{pmatrix}$$

This mathematical model will be used briefly when analysing the PER for the collected data (8.2.3).

4.2 Summary of Markov Models

- Markov modelling has been used to model the error characteristics within wireless networks.
- A two-state Markov model is the most common form Markov model.
- For any Markovian process the probability of a certain observation q_i at time i is only conditionally dependant on the observation at q_{i-1} at time i - 1.
- The sum of the transitional probabilities leaving a state always sum to 1.
- The equilibrium probabilities assume that after some time, each state will ultimately converge to a stationary probability.

5. Previous works

In this section, a brief summary of a range of previous works that encapsulates the overall entity of this thesis. The experiments performed along with the details and methods including results and conclusions where appropriate will be given.

5.A. Link-level Measurements from an 802.11b Mesh Network. [22]

Agugo, Bicket, Biswas, Judd, and Morris studied the performance of a multi-hop wireless network. They analysed the packet loss of 38 nodes over a three-kilometre radius. Each node was a PC that contained an 802.11b network card connected to an omni-directional antenna, placed on the roof. They made a number of conclusions:

- Links with intermediate loss rates are common with no sharp transition between high and low packet loss.
- Inter-node distances are not strongly correlated with whether nodes can communicate.
- Most links have non-bursty loss patterns.
- Links with very high signal strengths are likely to have low loss rates, but in general, signal strength has little predictive value.
- A link is likely to have significant loss rate at its optimal 802.11b bit-rate.
- Multi-path fading greatly affects outdoor links and helps explain intermediate loss rates.

5.B. Propagation Measurements of the 5.2Ghz Radio Band in Commercial and Domestic Environments. [25]

Beach, Hafezi, Lawton and Wedge performed wireless measurements in five different environments at 5.2Ghz using both omnidirectional and directional antennas. It was found that directional antennas achieved a better RMS delay spread when compared to an omnidirectional antenna for four out of the five rooms. They also conducted experiments and concluded that the size of the physical environment, the objects within that environment, wall construction, and even moving people played “an important role on the variations of the RMS delay”. Only a very limited number of experiments were performed and no mathematical model was produced.

5.C. Measurement and Analysis of the Error Characteristics of an In-Building Wireless Network. [14]

Eckhardt and Steenkiste discuss the reasons for studying and characterising errors within WLANs and proceed to give an overview of the sources that cause wireless errors. A number of experiments in different environments including direct line of sight, through walls, multiple objects and the human body were tested. The conclusions were: the attenuation through plaster and concrete walls was slight but noticeable, different construction materials have different effects on propagation, and the human body. in direct line of sight has a varying affect on signal propagation. Wireless interference from other similar frequency devices were tested such as 900MHz cordless phones where the conclusion was that the location of the phone, relative to the transmitter or receiver is extremely important in determining packet loss. Potential interference from other operating WLANs was tested and confirmed as a source of packet errors. The experimental data including the amount of packet error rates for all experiments are analysed and presented within the paper. All experiments were performed using AT&T WaveLAN standard at 2Mb/s running in the 900Mhz or 2.4Ghz spectrum. Depending on the final frequency used through the experiments, the reliability of results is questionable for modern networks.

5.D. Experimental evaluation of wireless simulation [15]

This technical paper reviews six of the most common assumptions within wireless network publications, simulations and models, namely:

1) The world is flat.
2) A radio's transmission area is circular.
3) All radios have equal range.
4) If I can hear you, you can hear me (symmetry).
5) If I can hear you at all, I can hear you perfectly.
6) Signal strength is a simple function of distance.

A series of experimentations are performed in an outdoor environment. The six assumptions are then reviewed independently, and demonstrate the weakness and inadequacies of these assumptions within the wireless networking community. It places an emphasis on the necessity of produced simulations and models to incorporate the "sensitivity of results" of any assumptions made. This is imperative and needs to be considered throughout the analysis phase of this thesis.

5.E. Error Modelling Schemes for Fading Channels in Wireless Communications: A Survey. [16]

Bai and Atiquzzaman firstly outline the many complex factors that hinder the accurate modelling of errors within all wireless communications. They then proceeded to outline the main objective of the paper: conduct a survey of existing error modelling methods from a range of published papers. There approach was to analyse the work performed by researchers and classify the models based on the modelling approach. The classifications of these models were either analytical models (the simplification of a model under different operating conditions results in a dependency to the general operating environment), or an empirical distribution-based model (which deals with models where high accuracy and meticulousness is needed for a complete understanding of operating condition). This paper is exceptional as a guide on the various models for wireless environments in either large-scale or small-scale fading.

5.F. Markov Modelling of 802.11 Channels. [26]

Arauz and Krishnamurthy aim was to validate a two-state Markov Model. To do this, wireless experimental data was collected using the 802.11a and 802.11b wireless standards within an office environment. They calculated a Markov model for varying transmission rates and frame sizes. They compared their experimental results to simulated theoretical results and found that a large difference existed, “the differences were typically in the order of 1000%”, and thus a two-state Markov model was found to be inadequate. However, they conducted the experiment in a fixed office environment using a single setup at unknown distances, and so their results might not be reproducible for other wireless networks with different variables or different environments.

5.G. Markov-based Modelling of wireless LAN. [21]

Khayam and Radha perform 802.11b experiments at 2, 5.5 and 11 Mbps transmission rates. Experimentation started using direct LOS, however loss rates were very low and so a continuation of specific experimentations simulations was used, including business, classroom and home environments. The exact differences between these setups were not given and the amount of collected data is not known. Markov models of both bit and packet loss using a new technique referred to as the “Entropy Normalised Kullback-Leibler” is used. The derivation, explanation and quantification of the use of this new technique is analysed using information theory. A Hierarchical and Hidden Markov Models were proved to be inadequate for errors in the physical layer, however a two-state Markov Model was proved to be adequate for packet error analysis.

5.H. 2002 UNSW undergraduate Thesis

Dhanani and Tuli in 2002 were the first thesis group to begin the 802.11b wireless measurement project. They developed software that captured full 802.11 wireless frames by modifying the Linux software drivers for the chosen wireless network cards. This enabled access to all frame types including data, control, and management, and an analysis of error characteristics and throughput could then be made. Software was created that determined the percentage of errors at the physical layer, and while this software did produce results; the results were unreliable due to buffer overruns. An in-depth analysis of errors was not given however a general review of several crucial test results was given. A mathematical model of the observed errors was not applied.

5.I. 2003 UNSW undergraduate Thesis

Chen and Siew, for their thesis in 2003 furthered the work done by Dhanani and Tuli. They solved the buffer overflow problem that Dhanani and Tuli faced, and collected both 802.11a and 802.11b data as a frame and at the bit level. This data was then used to find the probability of errors, along with error correlation for a variety of places including indoor and outdoor and within a variety of environmental condition, including through walls and water effects such as through rain and over a pool. For each experiment, an explanation, and the interpretation of results was given, however a comprehensive set of data was not obtained. Again, a mathematical model of the observed errors was not completed.

5.J. 2004 UNSW undergraduate Thesis

Lo and Ngai for their 2004 thesis extended previous works regarding the wireless measurement project. They modified the software developed by students doing thesis of previous years, and creating a mathematical model of the observed errors by using an n-state Markov model. A Java implemented Markov Modelling program, Jahmm was used, even though Lo and Ngai had to overcome several limitations in its implementation. An analysis at both the bit level and packet level, for a variety of environments including such conditions as the effect of walls, rain, and foliage were modelled. This was extended to include modelling of the orientation of a wireless adapter and the effect of multipath interference. However, while a model was produced for all environments, no comparison of these results were produced, and due to the lack of a comprehensive data set, confident analysis of wireless characteristics was not possible.

5.1 Action because of previous works

Many past papers that performed experiments and analysed wireless LAN behaviour, only collected a relatively small data set and generally in limited environments. A question thus arises as to whether the collected data is sufficient to understand and characterise the nature of errors within a WLAN. To accurately and confidently perform thorough characterisation and ultimately better understand WLANs characteristics, a comprehensive set of data from different locations and at varying times needs to be collected. Two methods exist:

1. Analyse numerous measurements from different published papers. The obvious problem – different papers potentially obtained their data using different system models, and thus the published measurements will differ in numerous ways.
2. Perform experiments in a consistent framework where a large amount of data can be collected and analysed.

The second option was chosen, and from here on referred to as the TELE4363 project, where once the data has been collected it will be analysed where individual hypotheses concerning the characteristics of wireless propagation will be investigated.

6. The Experiment

The growing emergence of wireless LANs in the last few years has influenced a growing demand for home wireless networks, where the important goals of such networks are to enable two or more users to share Internet access, printers and fundamentally, data. Wireless manufactures have capitalised on this market, creating simple and easy-to-use products with simple graphic user interfaces (GUIs) that the general consumer can configure. Using this simplicity to our advantage and the fact that a large collection of data was needed, the TELE4363 project was created.

This project comprised of creating a concise and consistent experimental plan so that all students enrolled into the TELE4363 subject would perform measurements as part of their practical component of the course. The final experimental plan - the instructions given to the students, is attached in Appendix 1. A brief overview and summary of the instructions will now be given, divided into the two consecutive phases that the project encompasses:

6.1 Phase 1: Preparation

Firstly, the students need to choose a dwelling to perform all experiments. This dwelling needs to consist of a minimum of four rooms and in particular, a room to locate the router that remains secure and undisturbed for the duration of the experiments. Once a dwelling was chosen (usually the students home), the next task involved the allocation of equipment to students. There were five **measurement kits** (an example is shown in figure 5), each containing:

- Laptop computer (with laptop bag)
- Measuring tape (to measure details of the house)
- UTP lead (upload collected data)
- Linksys WRT54G wireless router
- Quick cam (take a picture of the dwelling)
- D-Link DWL-AG660 wireless LAN card.

The measurements were conducted from week 5 to week 14 inclusive, in a bath of **3 slots per week**. This produced a schedule so that all students of TELE4363 could perform the experiments.

Figure 9 An example of a measurement kit (appendix 1)

6.2 Phase 2: Mapping of dwelling

As mentioned previously, the majority of layers above the link layer exchange packets of information so this is the most relevant data that needs to be collected. Thus, a method needs to be introduced to record the details within the students dwelling where the experiments are performed. This method is crucial, as the distances from the router to objects and measurement points along with all the objects within the dwelling that can hinder wireless signal propagation (addressed in section 3.4.2) need to be documented. Thus, there is a need to collect and record information such as the lengths of rooms, floor type and wall construction, and collect and record metallic objects such as filing cabinets, fridges and washing machines, electronic equipment such as televisions, microwaves and computers, communication devices such as cordless phones, operational WLANs and Bluetooth devices are to name but a few.

Two methods were chosen for the collection of this data.

1. A rough orthogonal top view, drawn by hand of the dwelling. This drawing is intended as a reference and as an easily identifiable visualisation of the dwelling. The drawing should contain the numbered rooms corresponding to the data entered into the spreadsheet (explained in method 2 below), the dimensions of each room, along with doors, windows, cupboards and large metallic objects given as D, W, R and M respectively. An origin also needs to be introduced, this will be used as a reference for the entering of data into the spreadsheet. A computer drawn example is given in appendix 2.
2. A spreadsheet. Attempting to calculate distances from the router to all measurement points for example from the rough hand sketch is time consuming, and ultimately does not scale. A spreadsheet however, is machine-readable and ultimately, programs can be written to manipulate the data. Specific instructions pertaining to the entering of data into the spreadsheet was given to students as an attempt to dictate the data that should be recorded and the format of this data.

6.2.1 The Spreadsheet

A spreadsheet that can be easily attained, understood and used by all students was needed, so data can be entered in a consistent and reliable framework. Many hours were spent creating and altering the spreadsheet so that students can enter all relevant data with the minimum amount of effort by choosing the relevant response from a drop-down menu. The spreadsheet that was created went through a number of revisions, where each revision added additional detail, criteria or fields that were requested or suggested through feedback from students. Throughout the experiment, the most recent version of the spreadsheet was made available for download on the subject’s webpage. Each revision of the spreadsheet was an attempt to be compatible with all previous versions, so the minimal amount of programs can be written for extracting the data within the spreadsheets. Screenshots of the final version are shown in appendix 2. The spreadsheet created consisted of four different sections, each containing fields where data needs to be entered. These sections along with a brief explanation include:

6.2.1.1 Exterior of building (figure 1 of appendix 2)

- Student number: Allow the unique identifications of data collected.
- Postcode:
  - Allows a rough estimate of the dwelling construction, based on when region was built. With a photograph of the dwelling (which students needed to take) will give a more accurate description of the construction material. This was not used for any analyses
  - A program was created that downloads weather data from the Australian Bureau of Meteorology. The program stores the weather conditions based on postcode.
- Roof Construction
- Number of floors in dwelling, including the highest and lowest floor. This is to determine what sort of dwelling (house or apartment) the experiments were performed in.
- Neighbouring constructions within 20 meters of dwelling in all directions.
- If the dwelling contained air-conditioning, the amount of people within the dwelling during the experiment and the 802.11 channel used was also asked.

6.2.1.2 Interior of dwelling (figure 2 of appendix 2)

Students were told to split there dwelling into a number of rectangular rooms where each room contains a consistent front, back, left and right side, and is identifiable by a unique a room number. These aspects are shown in figure 44 in appendix 2. The room number on the spreadsheet corresponds to the room number on the hand drawn sketch of the house.
For each room the following need to be recorded:

- Room type
- Room size (in metres)
- Room co-ordinates, relative to the origin.
- If the room was accessible
- The floor structure and its finish
- The ceiling type and height
- The wall construction for the left, right, back and front sides.

6.2.1.3 Room Contents (figure 3 of appendix 2)

The contents contained within documented room, were split into 4 object classes:

1) Objects that may **affect wireless propagation** such as metallic and water objects.
2) **Communication devices** such as cordless phones, operational WLANs and Bluetooth devices
3) Objects that can potentially **cause interference** including all electronic equipment.
4) **Communication socket** devices potential locations for wireless router.

Ideally, the exact location of every object should be recorded, however to save labour, only the exact location of all Communication Devices and potential objects that may affect wireless propagation are recorded.

For each object, the following needs to be recorded unless specified otherwise:

- Room number
- The Object Class: objects affecting wireless propagation, electronic equipment, communication devices or communication sockets.
- The Object Type: A range of objects have been included in the drop-down list.
- In default-state: Each electrical object includes a default state in parenthesis. The default state field needs to be changed if it defers from the parenthesized value.
- The start information in relation to bottom left corner of the room. The x, y and z-axis measurements are to be given, however only for "Objects affecting radio" and "Communication devices" are to be recorded.
- Length information is the length of the objects along the x, y and z-axis, however only for "Objects affecting radio propagation” need to be recorded.

An “other” field was placed in the majority of drop-down menus in the final version of the spreadsheet. Students were told to choose the “other” field, if the drop-down menu did not contain an appropriate field and to explain the meaning of “other” in the appropriate “Explanation of Other” cell.

6.2.1.4 WLANs detected by Kismet

All WLANs detected by Kismet need to be recorded. (As previously discussed can potentially be a source of interference.)

6.3 Phase 3: Collection of data

The goal of this phase is to collect data at the packet level, which will allow the determination of the signal strength along with the amount of packets lost. However, before detailing the experiments that were performed, a brief overview outlining some important and essential characteristic elements is given for a better understanding pertaining to the experimental procedure.

6.3.1 The Hardware setup

The chosen Linksys WRT54G wireless router internally runs a distribution of Linux that permits software to be uploaded and executed. Using this feature was the fundamental reason for choosing this router. The experimental setup is as follows: the router is placed in the geographical centre of the dwelling to maximise signal coverage. All users, before beginning the experiment, are instructed to re-upload the software stored on the laptop to the router. This ensures that all students perform the experiment using the same unaltered program. Once the software has been uploaded, the user can proceed to telnet into the Linksys router and run the precompiled uploaded program.

The configuration settings used for the router are:

- Default IP address – Within the 192.168.1.255/24 subnet
- WAN/Internet interface: IP address - 10.0.0.1, Subnet mask: 255.0.0.0 and Gateway: 10.0.0.2
- Wireless Network Mode – 802.11g only
- Wireless Channel – 6 (2.437 GHz), the standard channel for wireless devices
- DHCP Server – Enabled
- SSID – “THESIS”
- Wireless SSID Broadcast – Enabled
- Wireless Security – Disabled. Impeded network performance
- Other settings were left at Default value

All Laptops were dual-boot systems with Linux Fedora Core 3 and Windows XP installed. Windows contained Logitech’s proprietary quick-cam software (experiment 5, 6.5.5.5), while Linux was loaded with kismet (experiment 1, 6.5.5.1), the spreadsheet for the entering of data, OpenOffice, and the emit and observe programs (section 6.3.2).

The configuration settings used for all laptop’s are:

- Local IP subnet -by DHCP
- Wireless Network Mode – 802.11g only
- Wireless Channel – 6 (2.437 GHz), the standard channel for wireless devices
- SSID – “THESIS”
- BSSID – routers MAC address
- Wireless Mode – Infrastructure
- Wireless Security – Disabled
- Other settings were left at Default value

6.3.1.1 Why 802.11g

The 802.11g standard was selected for all experiments. This standard was chosen as is the maximum speed provided by current 802.11 wireless standards, and ultimately, is the preferred standard that is currently being deployed in wireless networks around the world. However, experiments will be performed to determine if any differences exists between the signal strength and transmission rates (see chapter 9.2). If no significant changes exist, then the results of any transmission rate used can be generalised to fit all other transmission rates.

6.3.2 Running the Programs

The fundamental program called the emit program (written by Tim Moors) constantly emits UDP packets that have the same physical length (100 bytes) at a constant interval from the router. The packets are sent to the broadcast address, which will be configured by the students using DHCP to be in the 192.168.1.255/24 subnet. The router and laptop are set to their maximum possible transmission speed of 54Mbps. Antenna diversity was enabled on the router for all experiments; to enable a consistent framework and minimise any discrepancy in distances.

The receiving laptop needs to be configured to capture the emitted packets. The receivers first priority however, is to determine if the packets are indeed from the wireless router, and not from a different subnet. Once the link layer has determined that the packet is indeed from the accompanying wireless router, the signal strength and amount of lost packets need to be determined.

The use of error detection is needed to detect when a packet has been lost, which is accomplish by using sequence numbers that accompany the transmitted UDP packets. The observe program on all laptops is the program that receives all incoming packets, the user however, needs to inform the observe program of the room number and the measurement point. The room number will correspond to that in the spreadsheet, and the measurement point will be either the: top left (10), top right (2), bottom left (7), bottom right (5) and the centre of the room (0) relative to the front of the dwelling (as shown in the figure 44 in the appendix 2). The numbers in brackets correspond to the numbers that are entered as inputs into the observe program. Once the user has entered the room number and measurement point, packets will be collected in a group of 100 or for a 30 second interval, whichever arrives first. The output of the observe program creates two files, the strength file and the packets file, a screenshot of each is given in appendix 3.

6.3.2.1 Packets file

The strength file contains one line for each measurement point, where the first number indicates the room number and the second the measurements point (0, 2, 5, 7 or 10). After this is a sequence of “1”s indicating a successful packet observation or “0”s indicating a missed packet, with long strings of “0”s condensed to the form “[### pkts missing]”. An example is attached in appendix 3 (figure 46).

6.3.2.2 Strength File

The strength file contains multiple lines per measurement point, where each line is split into 10 columns, the columns indicate the:

1. Time in seconds since January 1st 1970.
2. Room number.
3. Measurement point.
4. Number of successful packets that contributes to the current measurement. Once 101 packets have contributed, a new line is formed.
5. Number of missed packets during the current measurement.
6. Number of total packets received on the wireless interface before measurements on this line.
7. Number of packets received on the wireless interface after measurements on this line.
8. Channel quality.
9. The RSSI (Received Signal Strength Indication).
10. Noise level.

Note: An example is attached in appendix 3 (figure 45)

Columns 6 and column 7 of the strength file indicates the number of packets captured at the driver level. Whereas, columns 4 and 5 refer to packets being captured at the application layer. Due to this difference in layer collection, a possibility for the exact number of packets to be detected at the application layer could be different to the driver level. This is due to the fundamental reason that packets might be lost and thus the driver would not have observed the packet. The application layer however, knows of missing packets due to the inclusion and the use of sequence numbers. Thus, the sum of columns 4 and 5 (the amount of lost packets and successful packets) might not be the same as the difference between columns 7 and 6 (the number of packets received on the wireless interface after measurements on this line and before measurements on this line).

The IEEE 802.11 standard describes a technique to indicate the power of the received signal strength in a wireless environment, known as the RSSI value. It is this numeric value that **only** reflects the "energy observed at the receiving antenna" [27] where all measurements have an allowable range between 0 to 255. The 802.11 standard does not describe how these RSSI values should be determined, and thus each developer uses their own proprietary method. Thus, it is not possible to compare different vendors RSSI values, as they are most probably being measured using different methods. This is the fundamental reason as to why all wireless cards used in this experiment are from the same vendor. Another subtle reason

is the use of the Atheros chipset (the chipset used within the wireless cards) has a high degree of precision and uses all 256 RSSI values. One important aspect through observing the strength file in appendix three shows the RSSI value constantly changing over time. This is due to the varying combination of mentioned impairments in section 3.4. The end result is the signal strength will fluctuate significantly when a lack of line of sight between MP and router and this fluctuation will occur with respect to time and distance between the two communicating bodies.
Note: To convert the RSSI value into dBm, **subtract 256**.

The RSSI value only measures the energy received at the antenna input, and does consider the potential accuracy of the received data. It is the channel quality that attempts this, and is generally used as a metric to indicate the amount of corruption in the environment between the access point and the client [27]. Thus, the intent of signal quality is to indicate the "goodness" of a wireless link. However, it was later discovered that this calculated value is actually the RSSI subtracted by the noise level (161). Due to this bug, **the perceived channel quality is not used in any of the analysis phases**.

The noise level (the 10th column of the strength file) in all experiments is constant, at the numeric value of 161. This invariability is because the measured noise level indicates that of the internal electrical equipment, which as previously mentioned are all identical.

Note:
- Contained within the attached instructions (appendix 2) indicates that the strength file should contain 11 columns, where the forth column denotes, "whether the laptop was facing the front (F) or back (B) of the dwelling". This additional column for all experiments was not recorded.
- A bug has been identified within the observe program, which directly affects the strength file. The "number of total packets received on the interface before the start of a measurement " on a particular line (column 6) is always the same as the "number of total packets received on the interface after a measurement" (column 7) on the previous line. While this does not affect the collection of data within a 30 second period, it does affect the collection process between measurement points as data at the driver level is still being collected.

6.3.3 The variables

Many variables exist both in the physical environment and within a wireless network. To produce experimental results that are meaningful, many wireless variables and environmental variables need be remain constant for the duration of the experiment. To observe and successfully analyse a specific characteristic of a wireless network, other network variables need to be maintained and objects with the physical environment need to controlled.

6.3.3.1 Wireless variables (ARF and MAC)

A few functions within WLANs operations can complicate the experiment and ultimately hinder a much needed common standard.

- Auto Rate Fallback (ARF)

Auto Rate Fallback also referred to, as Automatic Rate Control or Auto-Fallback is a method used by wireless devices to provide the best transmission rate at any given instant of time. The faster a device transmits data, results in a shorter period for each bit being transmitted and ultimately results in less energy per bit. Thus, higher transmission rates have an increased chance of being errored because they are more susceptible to the physical properties within the environment and the characteristics of wireless propagation. Thus, the chosen transmission rate at any given time is determined based on a proprietary algorithm that considers both the signal strength and error rates. The trick for wireless developers is creating an algorithm that maximises the throughout, while minimising error rates. This is cause for concern, because the minimisation of errors is not wanted, but rather the observation of errors at varying distances and signal strengths is what is required. If the transmission rate is allowed to alter, then the calculated error rates will ultimately reflect the rate of transmission. To observe the errors at and signal strength at varying distances, then the only alternative is to fix the transmission rate (where the chosen rate was 54Mbps). If the transmission rate is fixed, then the error rate will potentially be a function of the distances and the changing signal strength.

- Medium Access Control (MAC)

Due to the increased amount of errors in wireless LANs, the MAC layer is designed to appear to upper layers as a wired network (802.3), thus attempting to effectively minimise the amount of lost packets. To accomplish this task, all WLANs implement their own acknowledgements of frames and proceed to retransmit frames when errors do occur. If these acknowledgements and retransmission are to occur in this project, they ultimately they will affect the accuracy of the results. Thus, the solution is to disable retransmission and acknowledgements. The solution that solves this problem is the use of UDP as apposed to TCP within the transport layer (explained in section 6.3.4).

6.3.3.2 The environmental variables

Many variables exist within the home environment that need to be controlled for the duration of the experiment. Most important is the orientation of the equipment. A summary of variables that were kept constant include:

- All doors are to remain **closed** for the duration of the experiment.
- All mobile phones are to remain **stationary** for the duration of the experiment.
- Students are to hold the laptop at **waist height** when collecting the data.
- The router is to be placed in the physical **centre** of the dwelling to maximise coverage, and needs to be recorded in the spreadsheet.
- The router is to kept **parallel** with the front of the house for the duration of the experiment
- The router contains two antennas (for diversity) and must remain **vertical** for the duration of the experiment.

6.3.4 The use of UDP as opposed to TCP

The emit and observe programs use UDP rather than TCP for the following reasons:

1. UDP is characteristically an unreliable protocol, and thus does not implement acknowledgements. TCP however implements its own congestion control, (unlike UDP), which requires the use of acknowledgements for each frame sent. Furthermore, TCP's congestion control is the primary reason for performance degradation in wireless networks. This is because, when errors occur within a TCP wireless network, TCP **always** assumes that the errors are due to congestion within the network, and not due to any other sources of impairments. TCP's response to the assumed congestion is to employ a back off algorithm, which reduces the transmission rate.
2. When using TCP and a packet it lost, TCP will retransmit the missing or potential lost packet. UDP however, does not implement any retransmission mechanism. The retransmission of packets will interfere with the legitimate measurements of the experiment.
3. UDP permits the broadcasting of packets, which allows packets to be sent to the 192.168.1 subnet. This is needed because the laptop is given an IP address using DHCP, and will be within the 192.168.1 subnet.

6.3.5 The Experiments

In total, each student performed five experiments. They include:

6.3.5.1 Experiment 1: Sniffing for sources of interference

While performing all experiments, other 802.11 wireless equipment can potentially affect any results obtained. Thus, the aim of this experiment is to identify other potential 802.11 causes of interference using a wireless sniffer. A wireless sniffer is a program that has the ability to capture and report to the user all packetised traffic (including beacon frames) that traverses in free space. One such program is Kismet. The students were instructed to walk around the perimeter of their dwellings while running Kismet on the laptop. If any 802.11 wireless devices were found, students were instructed to turn these devices off (if possible), and recorded these devices in the spreadsheet (shown in appendix 2, figure 43)

6.3.5.2 Experiment 2: Signal propagation

The aim of this experiment is to determine the signal strength and the amount of loss throughout the dwelling. Students will take measurements at the five measurement points in each room by running the observe program (discussed in section 6.3.2). This program will capture the emitted packets from the router, and record data to the packets and strength file.

6.3.5.3 Experiment 3: Student's Own experiment

Students can conduct any experiment they choose, examples are given in appendix 2, section 3.6. The aim of this experiment is to allow students to create a hypothesis, and then proceed to test this hypothesis. Once the experiment has been performed, hopefully an accurate conclusion can be drawn. If multiple students arrive with the same conclusion, then further investigation could be justifiable or possibly general conclusion drawn.

6.3.5.4 Experiment 4: The Time Variance

The exact variance over time of the signal strength and PER is unknown. This experiment aims to determine if the signal strength and ultimately the error rates alter drastically over time. Students chose any measurement point relatively close to the router (ensuring packets will be received by the wireless host) and run the program for as long as possible.

6.3.5.5 Experiment 5: Photograph your dwelling

The construction material of a dwelling can drastically affect the nature of wireless signals, and although the students have recorded this information within the spreadsheet, a photograph in combination with the dwellings postcode will be given to an expert who can potentially give a more accurate description of the construction material. The students can either use the given Logitech quick-cam that works in Windows, or use their own digital camera for taking the photograph.

6.3.6 Uploading the data

Once the students have completed the experiments during their allocated slot, the collected data from all four experiments is then uploaded using a wired connection in G16 to an Electrical Engineering server. The files that are uploaded include:

- The Kismet files
- The spreadsheet
- The files from experiment 2 and 5 (strength, packets and Ethereal)

7. The Preparation

Before any data could be analysed, the collected data needed to be collated and extracted. Only then could programs be written efficiently.

7.1 The Extraction

All students that completed the experiment, as previously described, uploaded their data to the electrical engineering server (the uluru server). From the collected data all relevant files needed to be extracted, this included the strength, packets and Kismet files along with all excel forms (some forms were saved in the open office format). The method that was predetermined even before the commencement of data collection was the creation of computer programs for data analyses. While the strength file is easily readable due to its native text format, excel (or open office files) do not provide this luxury. Thus, all forms were resaved to a comma separated value (.csv extension) file format, which is a non-proprietary format consisting of text or numbers separated by commas.

All the files and forms as mentioned above (the strength, packet, Kismet and excel form) were extracted for all students. Each specific file type was then renamed for each sample in a successive manner. For example, the .csv file, strength, packets and Kismet files for a particular student contained the same prefix – form1.csv (for the .csv file) and strength1 (for the strength file) packets1 (for the packets file) and finally Kismet1. The ’i’th students files were form’i’.csv, strength’i’ packets’i’ and Kismet’i’. This ensured that all files of a particular prefix uniquely identified a sample and ultimately allowed written programs to be more efficient.

The collected data consists of 114 strength, packets and Kismet files along with 102 forms. If any of the sample files were altered, a list of these altered samples and reason for alteration is given in appendix 4.

7.2 The Programs

The primary task before any data analyses was to determine the version of the spreadsheet used and determine if a router was recorded within the spreadsheet for each sample. The results are given below:

Version	1	2	3	4	5	6	7
Number of samples	11	3	4	33	1	19	30

Table 8 Number of samples corresponding to version number

It is to be noted that version 1 and 2 of the spreadsheet were not used in the analyses, due to the substantial differences in form design from versions 3 to 7.

Number of total forms	102
Number of potential forms for data analyses	88
Forms with no router within objects	24
Forms with no router location	13
Number of total initial form samples	51

Table 9 Total forms with the subset containing potential samples and initial 'correct' samples.

Once the above information was known, the fundamental requirement was for the router position to be determined, as the exact router location is fundamental in the analysis phase. Because of the relative small size in usable samples, the hand drawn maps were then used to determine router location, as students were instructed to record the exact router location on these hand drawn maps. The router object was then entered manually into the relevant forms. This however, only led to a small increase in useable samples. It was then decided that an e-mail from Tim Moors (my supervisor and TELE4363 lecturer) would be sent to students that lacked the required router information. If a response was received, the router location was entered manually into the appropriate spreadsheet. With the new information, table 8 altered and produce table 10 below:

Number of total forms	102
Number of potential forms for data analyses	88
Forms with no router	17
Forms with no router position	5
Form where router was placed in unmeasured room or contained no strength file	9
Number of total samples used in experiment	57

Table 10 Form information after email response

The total samples of data that were not used in the analyses phase coincide with one of the following categories.

- Router position was not recorded.
- Spreadsheet version 1 or 2.
- No strength or packets file was uploaded.
- Router was placed in a room that was not contained within the spreadsheet

When entering router position into the forms it became evident that the exact x, y and z coordinates were often not very precise and sometimes one or even two coordinates were lacking. Due the varying confidence of this data it was decided that a confidence meter was needed that depicts the reliability of router location. This confidence meter would vary depending on how accurate the coordinates of router position, derived either from the hand drawn map or from students e-mail replies. The confidence meter (table 11, page 46), is effectively a series of numbers, where the increasing confidence values result in a decrease in confidence, thus a less accurate router position

Confidence Value	Explanation
1	Unaltered spreadsheets
2	Edited with exact router location
3	Edited with 2 known coordinates
4	Edited with 1 known coordinates
5	Edited using estimation of location from MAP
6	Router not found or coordinates were in error

Table 11 The confidence meter including a brief description

While altering data into the spreadsheets the relevant confidence values were also entered at the end of the document. This was so latter C programs could distinguish between the different levels of confidence in the forms. Forms that were not altered were assumed to be free from error.

Note: If the x or y coordinate was not known, the estimated value entered into the form was the centre coordinate of the room containing the router. However, if the z coordinate was not known, then the average of the heights of all rooms within the dwelling was used.

For all written computer programs here on, if more information regarding the exact nature including operation, input or output is sought after, refer to the relevant comments contained within each program in the relevant folders on the attached CD-ROM.

7.2.1 C programs

Note:

- For all written C programs, the screen output continually indicates the number of processed files.
- For exact compilation, instructions consult header within corresponding file.

7.2.1.1 editforms.c

Specific instructions pertaining to the entering of data into the forms was given to students as an attempt to dictate the data that should be recorded and the format of this data. However, the assumption that students strictly followed the written instruction was not a possibility, and thus to minimise the unexpected behaviour of data input and to eliminate potential crashes of any written program, a C program (editforms.c) was written to remove any ambiguity of the saved excel (csv) forms. The program detects and corrects:

- The ambiguity of the object coordinate system. All objects within all rooms should be measured from the bottom left corner in relation to the coordinate system of the room containing the object. This program corrects objects measured from the absolute origin and deduces the correct coordinates in relation to the bottom left corner of the room.
- The use of centimetres or millimetres where detected and corrected for all measurements within the room and objects sheet of the spreadsheet.
- The differences between object numbers within all forms. That is, all forms where altered to use the same object numbers in line with version 1.7.

The inputs to the editforms.c program are all collected csv files. The corresponding output for each .csv file is the editform'i'.txt. This text document is in the form of csv file with the mentioned corrections.

7.2.1.2 strength.c

A program was needed that analysed the experimental results of experiment two and proceeded to collate the recorded data within the **strength** file into a meaningful and compact information set. This information set, calculated by the strength.c program, determines: the humidity during the experiment and then proceeds to record for each measurement point the packet error rate, the average signal strength, the total number of packets collected and finally the number of packets missed. The program outputs this information on a single line along with the room number and measurement point (0,2,5,7 or 10). A further explanation will be given below.

The base program was written by Dylan Syme for the TELE4363 project, but was fundamentally altered to perform the needed tasks on all samples.

The first line of all strength'i'.txt files contains a humidity value. As mentioned previously, the weather was recorded at 10 minute intervals from the Australian Bureau of Meteorology's website for a number of suburbs around Sydney for the duration of the session. Postcodes were instructed to be recorded by students within their spreadsheet. The assumption used however, is the humidity in Sydney is constant. This simplified the programming, otherwise the postcode needed to be extracted from the forms and then cross-referenced with the closest suburb that the Australian Bureau of Meteorology recorded. The closest suburb that was centred around UNSW and away from the ocean (Observatory Hill), was chosen. The time and humidity values at 10-minute intervals was extracted (using: for (i=3; i<7; ++i) ; do grep DATA 0$i* | grep Observatory | cut -d\, -f2,6) and saved into a single file. The issue now was determining when the experiments were run. This is easily found within the strength file, as the first column of all files indicates the time (in seconds since 1970) when the file was saved and thus when the program was run. The relevant time was then calculated, assuming the correct times existed within the strength file, and were cross-referenced with the time of the humidity. Once the closest value was determined, the corresponding humidity value was extracted.

After the humidity (on the first line of all files) contains successive single line containing the information set for each measurement point. This information set calculated by the strength.c program will now be described:

The average signal strength as the name describes is the arithmetic mean of the signal strength of each measurement point.

The packet error rate as the name describes is the number of lost packets (column 3 of all strength files) divided by total number of collected packets (column 4 of all strength files). However, the characteristics of the strength file made this task considerably harder than first thought. Some characteristics within the strength file that needed to accounted for included:

1 The inclusion of experiment 5 within the strength file.
2 Students manually altering the strength file and adding their own text. (A list of altered forms and reason for alteration is given in appendix 4).
3. Measurement points or room numbers that contained typing mistakes. It was found that writing a program to take all permutations of typing mistake was considerably difficult. For example it was instructed “If you knowingly make a mistake … use “999” for the next room/measurement to indicate the previous measurement is erroneous.” However, students also used 999 when they accidentally missed typed a room number, and thus the previous measurement was indeed reliable. So writing a program that flagged and corrected the number 999 was considerably harder and time-consuming. The more efficient and ultimately more reliable solution was to manually open the files and determine the mistake on a case-case basis.

Further to this, a number of fundamental aspects of the packet file also needed to be factored into all calculations, namely:

1. If fewer than 10 packets are received in a given line, then this line is ignored, as 10 or more packets are needed for correct and meaningful statistics (such as RSSI) on any given line.
2. The first line of all files was ignored for all calculations because the number of received packets at the driver level is unknown.
3. As mentioned previously, a bug has been identifies in the observe program, which directly affects the strength file. This bug allows data at the driver level to be collected between measurement points even though the observe program is not active, and so the exact amount of packets collected on the first line of all measurement points is unknown. Because of this uncertainty as to the amount of received packets, there is an unknown level of confidence in this data, and so was removed for all calculations.
4. A degree of confidence for the entire sample was used, however a further degree of confidence for each measurement point (each line within the outputted file) is also needed. This is because the number of packets received at the driver layer (column 7 subtracted from column 6) could differ drastically from the number of packets received at the application layer (column 4). If a variation at the different layers does indeed occur, this is an indication that the collected packets are from other operating wireless LANs. Thus, lines that contain a greater difference need to be given less weight. That is, if the two layers differ, then a reduction in confidence of that data is needed. This is because packets from other operating wireless LANs are included in any measurements taken at that measurement point, such as the calculation of the RSSI value. The method to calculate the confidence for each line is explained below:

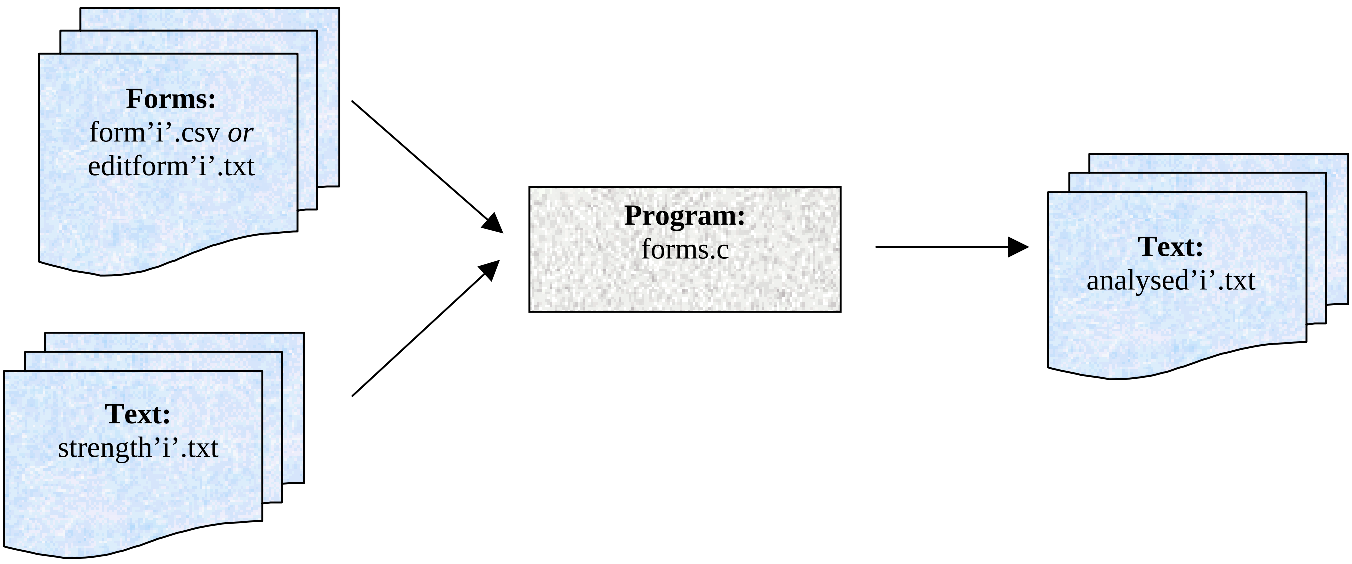
The degree of confidence (reasons for which are explained above) are used in the analysis phase by calculating for each measurement point, firstly, the total number of packets collected at the application layer, which is the sum of column 3 for each measurement point. The second aspect is the number of excess packets per measurement point, this is calculated by the difference between column 7 and 6 subtracted from column 3. These two numbers are then divided to produce a higher fraction for data that is of lesser confidence. Thus, measurement points that have a high confidence level for each measurement point need to have a smaller effect on the overall distributions and trends within the graphical analysis phase. The method to calculate this is explained within the MATLAB programming section.

The overall output of the strength.c program for each input analyses t**he strength file for each student and produces a corresponding strength text** file in a comma separated value form in the following order for each MP: PER, Room, MP number, number of excess packets, number of total received packets, and the average RSSI value. If no strength file for a sample existed, one was created with the single word "EMPTY" within.

7.2.1.3 forms.c

A program was needed that perform two functions: **analyse the spreadsheets** within the collected samples and c**ollate this data with the strength file** (the output of the strength.c program). Thus, this program does the majority of detective work to produce an informative text based file with all information necessary and so all relevant information for each sample is combined in a single file can be used in the analytical phase.

This program was the most challenging, due to the sheer number of tasks that needed to be performed and then continuously meticulously altering aspects of the program to produce an outcome that was robust and reliable while minimising any ripple effects in any other functions. The inputs and outputs to the program are displayed graphically below:



When viewing the output file, it contains the following structure:

1. The first line contains the confidence value as indicated in table 10. If a particular sample does not contain a router within the objects section of the spreadsheet, or the coordinates were not entered and left as the three tuple (0,0,0) or a particular sample does not contain a strength file then the confidence value is set to –9.
2. The second line identifies the number of operating wireless LANs. This was calculated by the number of WLANs detected by Kismet, subtracted by the number of WLANs that were disabled during the experiment, identifiable within the (experimentation) spreadsheet (appendix 2).
3. The third line identifies if the dwelling in which the experiment was performed contained ducted air-conditioning. The number zero's indicates that no air-conditioning was present and a one indicates the converse.

4. The fourth line identifies the number of people that where in the dwelling during the experiment. A zero however, indicates that greater than 9 people were within the dwelling, whereas all other numbers correspond to the amount of people present.
5. The rest of the output file consists of rows each corresponding to a unique measurement point in the form of: <Room> <MP> <Distance> <RSSI> < Number of excess packets > <Number of total received packets> <Room type> <Angle of Incident> and the <PER>, where the “<>” identifies the use of columns.

Note: This program was initially written for the original .csv forms, and thus it is recommended to use these, as apposed to the edited forms.

A Description of the Columns:

The RSSI, number of excess packets, number of total received packets and the PER columns are the unaltered values calculated and transferred from the output of the strength.c program.

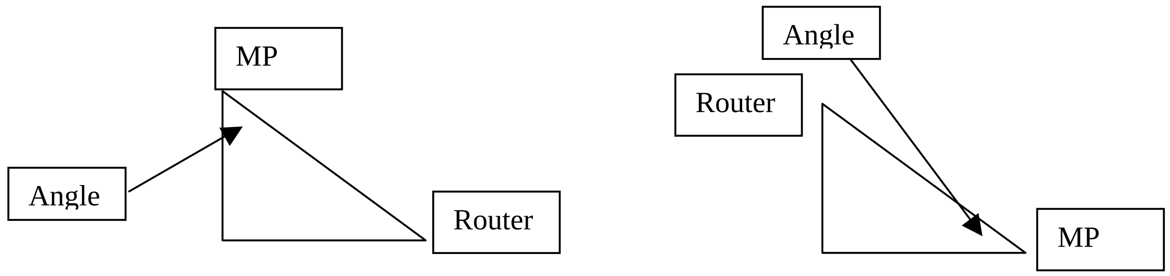
The distance column is the calculated distance (in meters) from the router to all measurement points. This was the primary function and most important objective of this program. It was this task where the majority of time and effort was spent. Undertaking this task however, did require a number of aspects to be assumed:

1. The exact corner of all rooms were used to calculate the distance, however, it is unknown if students actually placed their router in this exact location.
2. All measurement points were taken to be at a height of 1.0 meter from the dwellings floor during the data collection phase.
3. When determining the height of the router specifically dwelling that contained multiple storeys, the thickness of the floor and the thickness of the ceiling cavity between floors was neglected.
4. The router was instructed to be placed on the highest level of the dwelling, thus the height of the lower level (underneath the router) was needed. This information cannot be determined directly from the spreadsheet, and so the average of all lower level floor heights was calculated and used.

The final calculated distance is given in metres using a floating-point numbers to six decimal places thus attempting to maximise accuracy.

The room type (column 7) as the name describes is the type of room identifiable from the spreadsheet.

The second last column identifies the angle of incidence as the acute angle between the router and the measurement point. Two cases exist, when the measurement point is higher than the router, or when the measurement point is lower than the router. Diagrammatically the calculated angle is shown below:



The final line of all created analysed’i’.txt contains the word “END”.

7.2.2 MATLAB programs

The function of the created MATLAB programs is numerous: to collate all collected samples, produce graphs of different variables which includes determining the variability of the graphed y-values with certain x-values and ultimately fit a curve to the graphed data to examine the test hypothesis.

The curve-fitting task is fundamental for the analysis phase, and most importantly all written MATLAB programs will use the same curve fitting method. The confidence values from the first line of the analysed’i’.txt and the degree of confidence for each measurement point within the analysed’i’.txt (as discussed in the strength.c section) need to be considered. The problem now lies in the task of finding a method to successfully minimise the effects of data where less confidence has been predetermined. A commonly used statistical technique to accurately fit data is referred to as least-square curve fitting. This method chooses the parameters of a function to minimise the mean-square error between the curve and the measured values, that is it minimises the *chosen value* by:

$$\textit{chosen value} = \textit{data} - \textit{fit}$$

Using this method however, assumes all values to be of equal quality. This assumption in this experiment is violated and thus the fit would be influenced by poor and inaccurate data, and so a number of techniques were tried that gave weighting to data that had a higher degree of confidence, these include:

- Counting data multiple times that had a higher confidence level. The problem with this method was attempting to find a mathematical reason for the multiples used.
- Using the correlation of data. Using this method however required knowledge of a correct correlation, and ultimately involved coercing data to a preconceived graph type.

The main problem or issue with this thesis is determining that amount of weight that should be given to each sample. The final method uses the variability in router position as an indicator on the trustworthiness of data for each sample, where the weighted least squared method is used, which uses an additional scaling factor, a weight, in the fitting process. The *chosen value* determines how important a particular measurement point is when the curve is parameterised, and thus, the *chosen value* is multiplied by the scaling factor, which ultimately influences the final fit. Thus, a high quality data set plays a higher level of coercion in the final fit, that a point that is of lesser quality.

The weights for the different confidence levels (table 11) still need to be determined and justified, and so the final method used is as follows. The only sample that is knowingly 100% reliable is the sample that I myself collected, this data was then altered to determine the variability for a given condition, where the conditions are the same as those in the confidence table (given in table 11). That is, for the different confidence levels the most reliable sample was altered so it incorporated the confidence criteria. For example, confidence value 3 describes the router with only two known coordinates. To simulate this, the router position was altered to reflect this criterion, where two known values where kept constant, while the third was altered. The x or y room size values that contained the router was changed either by 3 meters (this was considered an average room size) or by the width of the room (whichever was smaller), and the z value was altered from zero, to the height of the room. To determine how the output varies while changes at the input, the correlation coefficient identifies if a linear relationship exists between the x and y graphed data is calculated. For the given example, the correlation coefficient for the three different alternatives (x and y known while z unknown, x and z known while y unknown and finally y and z known while x is unknown) was calculated and then the average was taken. The absolute value of the average (weighting needs to be positive to be meaningful) produces the weighted value 0.6377. This was done for all confidence levels, excluding confidence level 1 and 2, as these were given a full 100% weighting. The following table shows the confidence levels with the corresponding weightings used.

Confidence Level	**Weighting used**
1	1
2	1
3	0.6377
4	0.79
5	0.7502
6	0

Table 12 Confidence Level with corresponding weight

While the above method does take into consideration the variability of router position the assumption that all lines within the strength file are identical is again not a valid statement. To dismiss this assumption, the number of excess packets is divided by the total number of collected packets (as described in the strength.c section). An acceptable limit was then set at

10%. If the calculated value is above the 10% limit, then this value is used as a weighting. However, if a particular measurement point is above the predefined 10% limit, and is also a samples that as a low confidence level (3, 4 or 5), then both numbers are multiplied to produce the new weighted value for that measurement point.

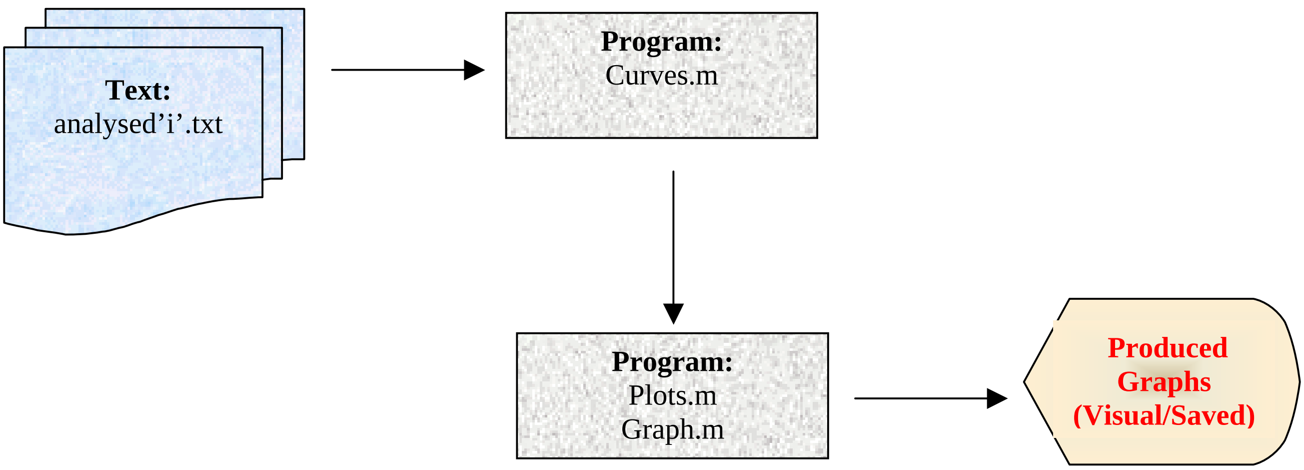
Once a distribution has been graphed, the weighted line of best fit is determined using the weighted method described.

Note: Only fundamental programs are explained.

7.2.2.1 Curves.m

Extracts data from all analysed'i'.txt samples and determines the confidence of the data and the corresponding weighting needed. Data from all measurement points for each successive sample is then loaded into on large matrix for easy extraction. The matrix contains nine rows of the following arrangement: number of WLANs, PER, distance, average RSSI, sample weighting, room type, air-conditioning, the number of recorded people and lastly the humidity.

The remaining part of the program is split into a number of sections such as room type, number of operating WLANs … Within each of these sections the Plots.m or Graph.m programs are called where the corresponding graphs are be produced. Since the vast number of total graphs that will be produced, each line is commented out, however if a graph needs to be produced, then the corresponding line needs to be uncommented.



7.2.2.2 Plots.m

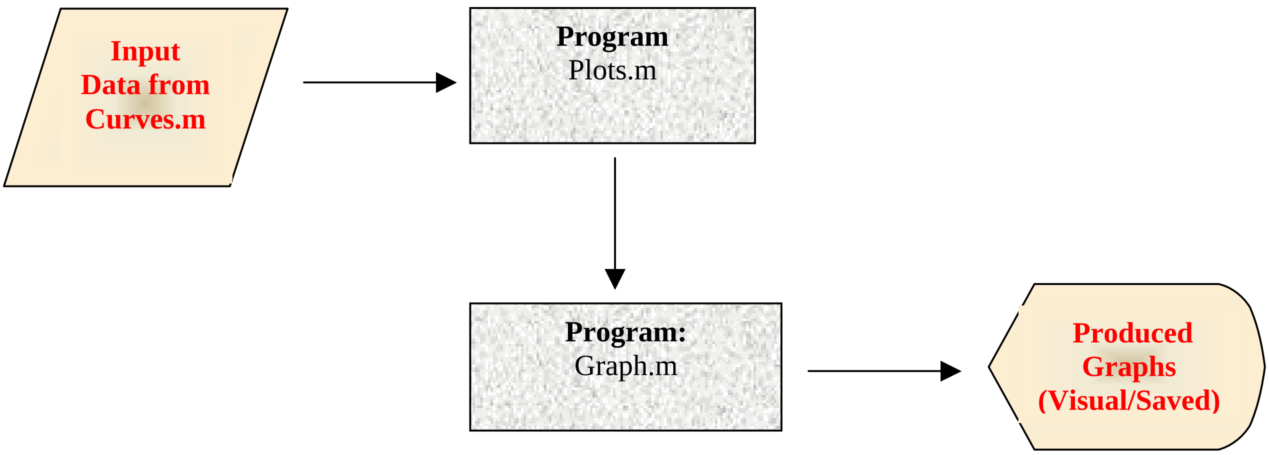
For the single created matrix of elements of nine rows, this function extracts the relevant x, y and weight values, determines (using the switch and case method) the corresponding title of the extracted data and calls the function Graph.m. The function arguments Plots.m include: the sorted matrix (as the original matrix is produced on successive samples), the matrix is sorted based on the x-data that is to be graphed.

The rest of the arguments include: a number indicating the first sample to be graphed, the total number of samples that are to be graphed. This is followed by the x-axis label, y-axis label, graph heading, the colour of the linear fit, the colour for the data, the type of data to be analysed and the corresponding row of data that is to be graphed within the original matrix.

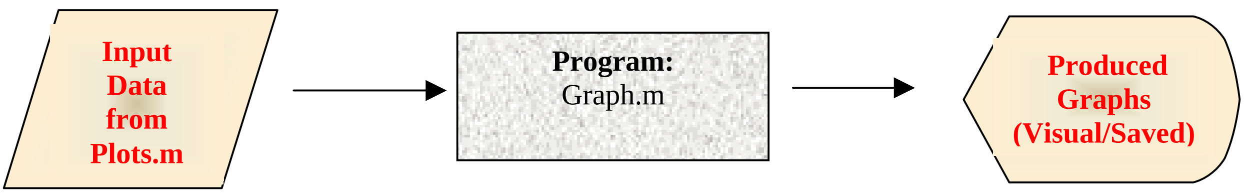
Distances were limited to 12 meters for all drawn graphs as it was assumed that the average length of a house does not extend the 12 metre mark, and thus the most likely cause of these occurrences are student errors when entering room sizes into the spreadsheet.

7.2.2.3 Graph.m

A single function call which includes all necessary elements to graph the x and y arguments and create the linear line of best fit in a single figure. The x-axis, y-axis and title are also passed as arguments and the final figure is saved with the filename of the saved figure matching the title of the created figure. The function arguments include: x-axis data, y-axis data, weights of data, x-axis label, y-axis label, graph heading, the colour of the linear fit, the colour for the data, if RSSI is used (alter axis accordingly), is PER is used (alter axis accordingly) and if a line of best fit is desired in the created figure. The figure is saved as a jpeg with the filename the same as the title of the figure.



The flow diagram of Plots.m is given above, whereas the Graph.n is given below:



The rest of the MATLAB files in this section deal explicitly with experiment 4.

7.2.2.4 StrengthTime.m

Takes as input the strength'i' file, where 'i' is the input argument to the program. The program finds experiment five within the strength file, then proceeds to collect 10 RSSI values, which it then averages and calls the function Stats.m to calculate some statistics and shows the signal strength over time. Individual RSSI values against time produced a graph that was too compressed and it was extremely difficult to see any effects. The time over which the analysis is done is the time within the strength'i' file. The programs ErrorTime.m, PacketLoss.m, Autocorrelation.m and Markov.m are also called. Thus, all information regarding experiment 4 for a chosen sample can de determined by running this program with the corresponding integer argument.

7.2.2.5 Stats.m

The standard deviation, mean and range are calculated for the strength'i' file. The graph of the average of 10 RSSI values over time is then produced.

7.2.2.6 ErrorTime.m

Called from the program StengthTime.m, and passed the same 'i' input argument the corresponding packets file is opened and experiment five found. The error rate for 1000 packets is then calculated and graphed.

7.2.2.7 PacketLoss.m

Called from StrengthTime.m with the same argument, where the corresponding packets file is opened and experiment five found. The program then collects different bursts loss sizes to graph the frequency of the bursts on the y-axis with the burst length on the x-axis. The log of the frequency of the bursts was used, as the burst size for smaller numbers was found to be extremely large. The program also calculates the loss rate. With only a simple alteration (documented in the program) an alteration is possible to graph the burst size for received packets.

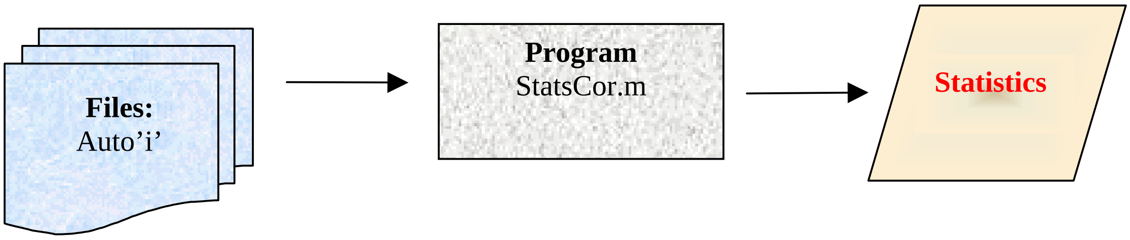
7.2.2.8 Autocorrelation.m

Called from StrengthTime.m and passed the 'i' input argument, the original signal strength values as found within the strength'i' file and the lag used for the autocorrelation. A rough estimate of the lag is used since an approximate gap between each successive line is 2 seconds. Thus, if a 30 second lag is wanted, then the integer 15 is used. The output of this file is auto'i', with the corresponding autocorrelation as a floating-point integer within the file.

To show how all the files and programs interact for a single sample a flowchart is given below, and is executed by StrengthTime('i') where 'i' indicates an integer.

7.2.2.9 StatsCor.m

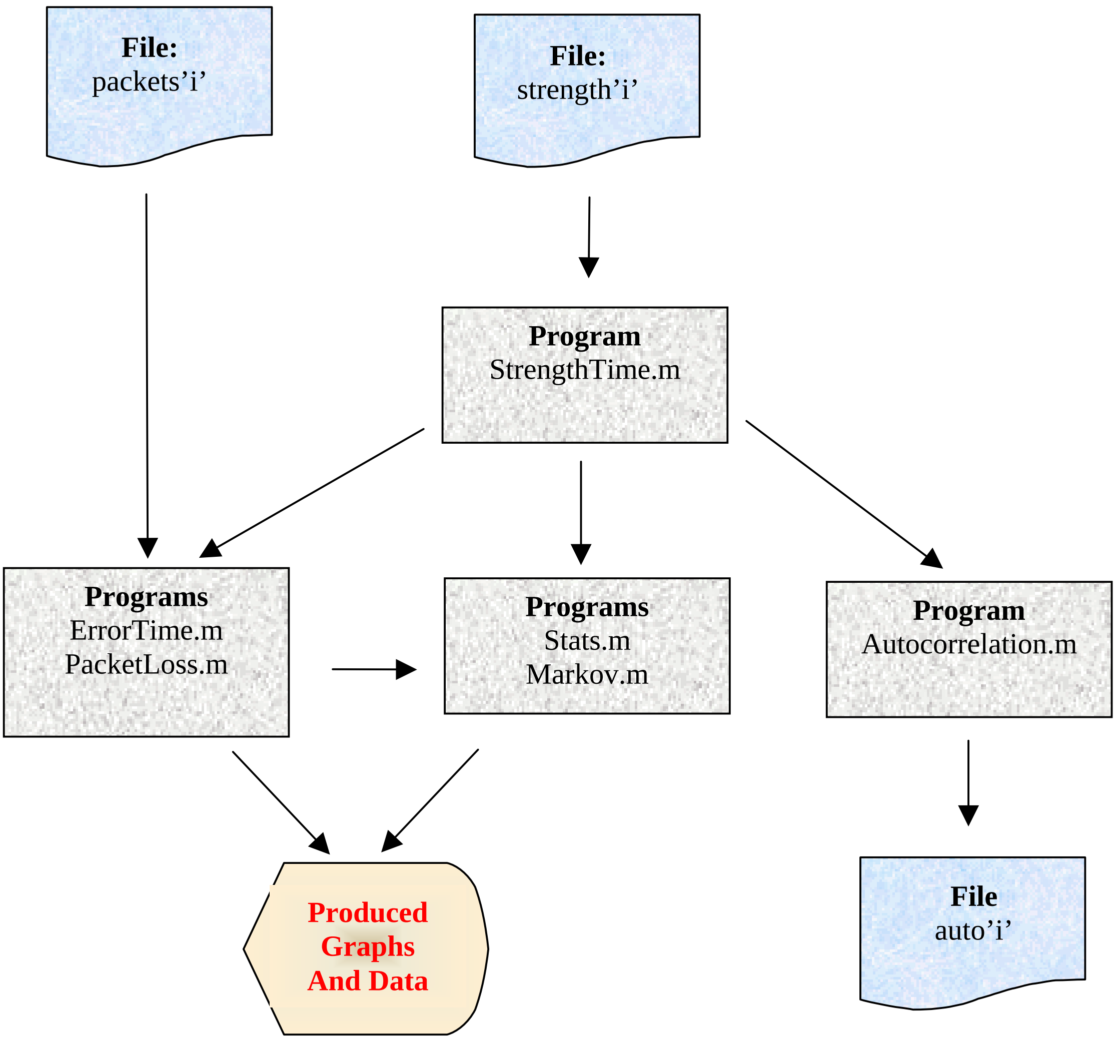
The program calculates the mean and standard deviation of all autocorrelation data within the auto'i' files. An integer argument is given as the input, which corresponds to the maximum number of files for analyses.



7.2.2.10 Markov.m

The program takes as input the 'i' input argument and calculates the transitional probabilities which are displayed as transitional matrix (see chapter 4 page 26). The equilibrium probabilities are calculated and displayed as a vector (for format see page 27)

A flowchart for experiment 4 is given below:

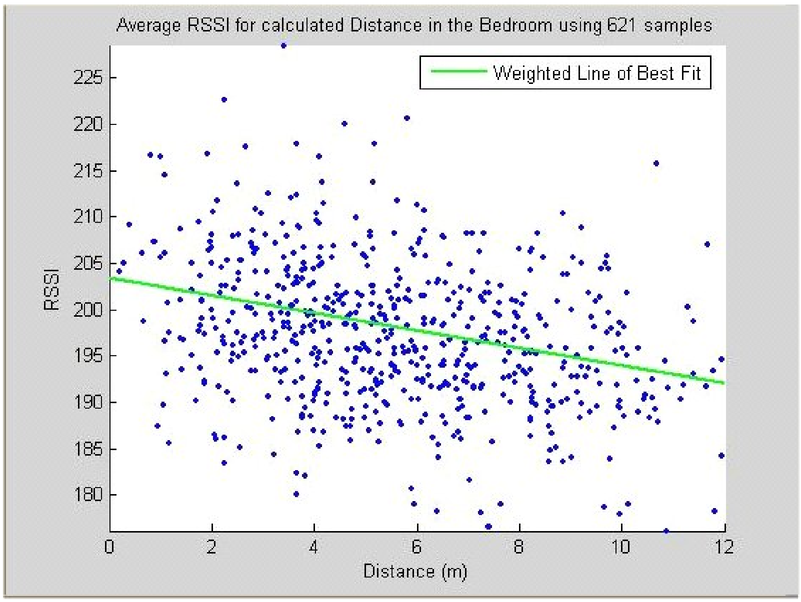


8. The Results

Much data has been collected, and it is only through analyses of this collected data that any hypotheses can be tested. Thus, this section has been segmented into different propositions each carrying individual hypotheses, with the intent of investigating and determining a relationship (if any), from the data collected.

8.1 Signal Propagation

A problem was found when analysing the figures created within MATLAB. The problem with creating individual graphs for comparison, produces the difficulty of observing any relationship. For example, the weighted fits of signal strength for the bedroom and kitchen are given below. Just by observing these figures, it is extremely difficult to observe any relationships (if any). This process becomes more difficult as the number of individual graphs increase.



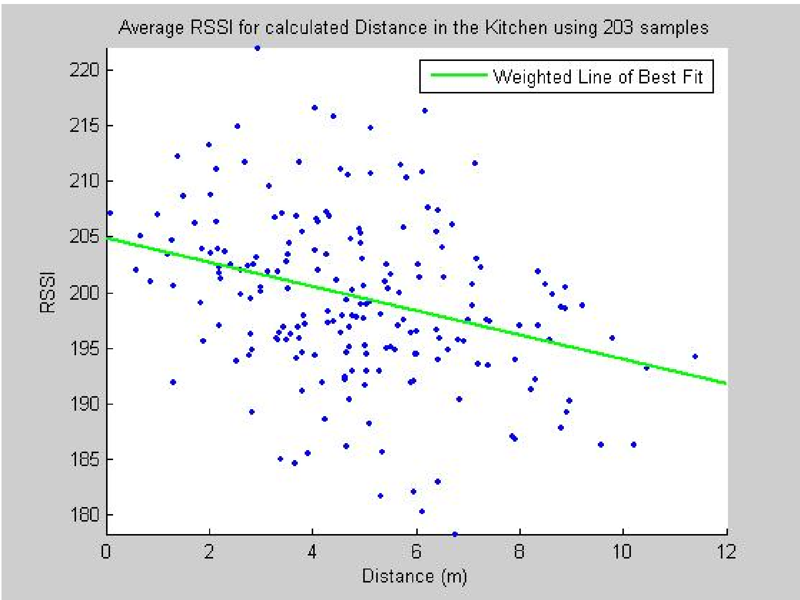


Figure 10 Two Graphs of RSSI vs. distance, are they the same. How different are they?

The next logical step was combining all weighted lines of best fit into a single figure, as shown in figure 11. While this method does work for small samples, attempting to ascertain any relationship is still difficult due to the large number of lines within a single figure.

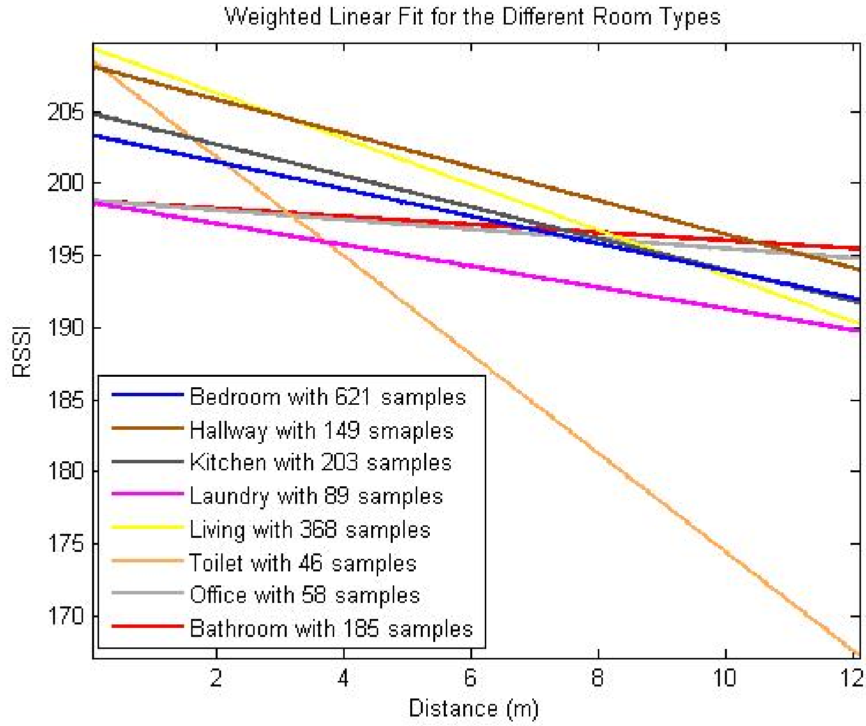


Figure 11 The weighted linear fit for all room types.

Thus, a graphical method was needed to compare similar graph types, which combines all information into a one-stop shop to observe relationships (if any). If a large sample of graphs are needed to be compared, a number of different statistics of each individual linear weighted graph were combined into a single figure. Each of the following statistics was calculated and graphed as a subplot (using a bar graph):

1) **Gradient with 95% confidence interval**: The rate in decline of signal attenuation over distance.
2) **Y-intercept with 95% confidence interval**: Designed to indicate where a graph starts. All weighted figures are produced using a linear line of fit and so the gradient is not a sufficient indicator, as graphs with similar gradients can have any range of different starting points. Although theoretically, at distances of 0, all y-intercept graphs should effectively be the same, this was not case, and thus was included in the statistical analyses. The best case is a room with a non-steep gradient and high Y-intercept.
3) **Correlation:** A number between –1 and 1, which describes the relationship, in particular the amount of spread of the data to the line of best fit. A perfect linear relationship with negative slope produces a correlation of –1, and indicates that

as one variable increases, the other decreases by the same ratio. A correlation of 0 indicates that no relationship is evident.

The gradient and y-intercept graphs show the 95% confidence interval as red bars on the bar graphs. A confidence interval is used as many cases vary with the number of samples, and therefore is a good indicator as to the sample size. Just using the gradient and y-intercept gives only a rough prediction of the confidence bounds, because the bounds vary based on the number of samples at each particular point. Thus, the 95% CI is only are linear estimate, and the exact 95% CI graphs will be graphed and shown in the relevant appendix.

Note: All graphs produced will be a function of distance unless otherwise stated.

Using the RSSI values recorded in experiment two, which can infer two aspects, firstly the wireless signal coverage across the dwelling and secondly the calculated packet error rates. All information collected regarding a sample is recorded within the analysed'i'.txt. Using this many hypotheses can be analysed within the dwellings with the ultimate goal of determining if a particular assumption is valid within the wireless community.

8.1.1 The General Spatial Distribution of Signal Strength and Loss Rates

The most common interest within the wireless community is the relationship between the three tuple: signal strength, packet error rates and distance. While the most widespread and commonly known RF-model in free space is the path loss model, where the received signal strength decrease logarithmically with distance [22, 28]. In spite of this, figure 12 shows the distribution with a linear line of best fit of the calculated distance from the router to each measurement point, plotted against the average signal strength. The weighted linear line of best fit was found to be the most accurate and is shown on the same graph. One might expect to see an exponential decrease in signal strength as the distance increases, this however was not the case. The graph indicates an attenuation due to distance of approximately **3dBm per meter**, which is substantially different to [14, 15, 26] and the free space experiment (see chapter 9 category two) where an exponential decrease was found.

A fixed transmission speed was used and consequently the potential to observe a key relationship between another key interest within the wireless community, that is, the signal strength and the amount of packet loss (errors). Figure 13 reveals two aspects: firstly, that the majority of packet loss was less than 0.1, which results in a contribution of 72% of collected samples at a signal strength value of between 201 and 198. Secondly, and most importantly, a linear correlation between signal strength and errored packets is evident, where **a 5dBm decrease in signal strength corresponds to a packet rate loss of 0.2**, which is very significant for modern protocols. Therefore, a direct correspondence does exist between signal strength and PERs, and so signal strength can be used as a direct predictor of PERs (the converse can also be used). As mentioned, however, a 5dBm decrease in signal strength corresponds to a packet rate loss of 0.2, if distance is also considered, an increase of **1m only increases the PER by 0.01,** (as shown in figure 14), a lot smaller variation than the RSSI. The general conclusion can be made by which based on the collected data, **the signal strength at a particular location has a more predominant role in establishing the PER, than the physical displacement from the router.**

One important aspect to note from all created graphs especially figure 12 is the **large cloud of data points**, that is, the data points have a large range for all distances. This is significant, and shows distance alone cannot be used for an accurate estimate of signal strength. The reason for this clouds existence is of significant importance. A range of experiments were performed (category one within chapter 9) that might explain the significance of this clouds.

For reference, the corresponding weighted linear equations with a 95% confidence bounds are:

Figure	Coefficients Curve fit (p1*x + p2) with 95% confidence bounds
RSSI vs. Distance (figure 11)	p1 = -1.078 (-1.227, -0.9284) p2 = 204.6 (203.8, 205.5)
RSSI vs. PER (figure 12)	p1 = -22.66 (-25.28, -20.04) p2 = 200.5 (200.1, 200.9)
PER vs. distance (figure 13)	p1 = 0.006768 (0.00418, 0.00935) p2 = 0.02887 (0.0141, 0.0436)

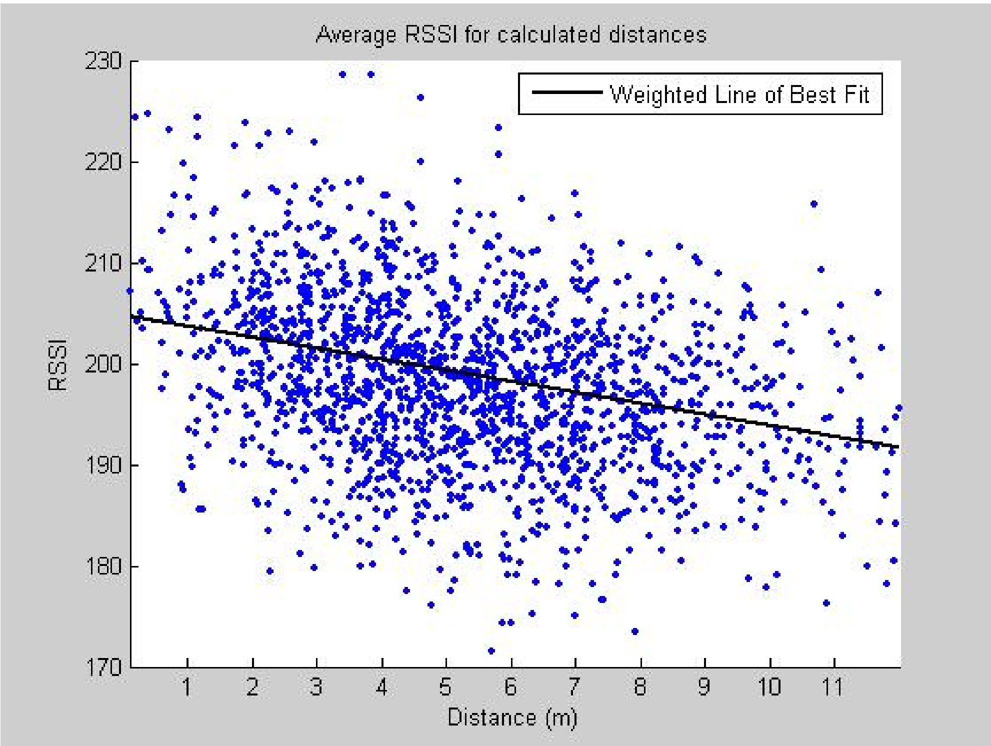


Figure 12 The Average RSSI and Distance for all samples

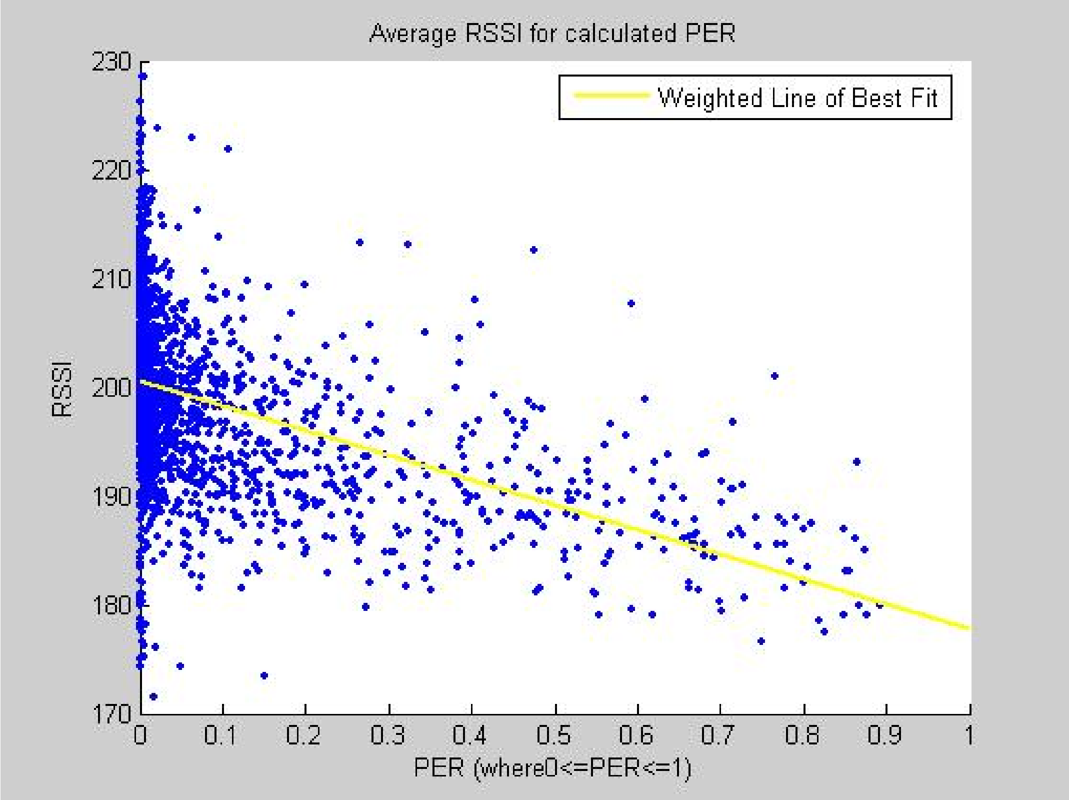


Figure 13 The average signal strength showing the amount of loss in packets

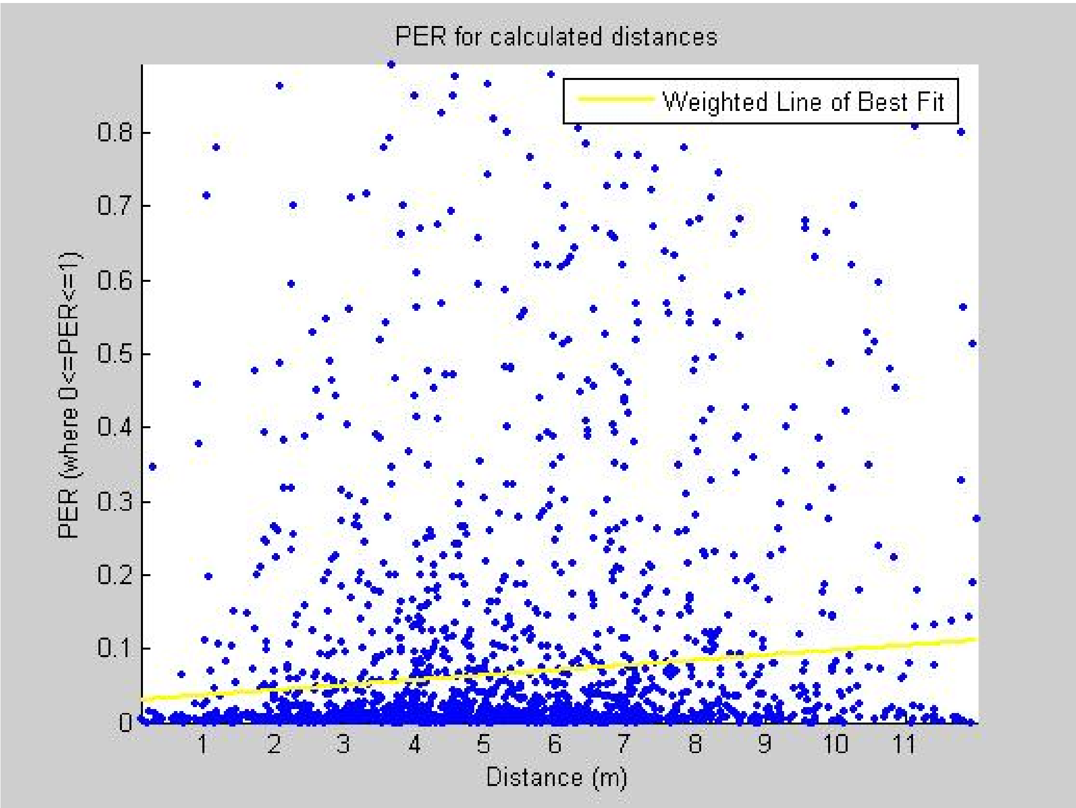


Figure 14 Packet Error Rates at corresponding distances.

8.1.2 Effect of type of room on signal strength

Different rooms within a dwelling contain a variety of different objects with varying degrees of attenuation (3.4.2). Using this as a building block, all measurement points that were collected within a specific room type were graphed to determine if a varying degree of correlation between signal strength and distance along with PER and distance exists based on room type.

Note:

- *The room type 'recess' was not used as contained a very small number of samples (three). All other room types contained no samples.*
- *The complete set of confidence interval bounds are given in appendix 5.*

The final produced graph showing gradient, y-intercept and correlating is given in figure 15. The weighted linear graph showing all room types on a single graph is given in appendix 5. Table 13 gives the correlation with the number of samples, the RMSE along with the line of best fit with the 95% confidence bounds.

Room type	**Correlation**	**Number of Samples**	**RMSE**	**Coefficients Curve fit *(p1*x + p2)* with 95% confidence bounds**
Bathroom	-0.0827	185	6.253	p1 = -0.2765 (-0.711, 0.1581) p2 = 198.8 (196.3, 201.3)
Bedroom	-0.3114	621	6.839	p1 = -0.9449 (-1.166, -0.7242) p2 = 203.4 (202, 204.7)
Hallway	-0.3814	149	7.699	p1 = -1.17 (-1.686, -0.6541) p2 = 208.2 (205.3, 211)
Kitchen	-0.3395	203	6.598	p1 = -1.088 (-1.543, -0.6327) p2 = 204.9 (202.5, 207.2)
Laundry	-0.1804	89	7.397	p1 = -0.7378 (-1.636, 0.1602) p2 = 198.7 (193.8, 203.5)
Living	-0.4512	368	7.709	p1 = -1.587 (-1.924, -1.249) p2 = 209.5 (207.6, 211.4)
Toilet	-0.5341	46	7.461	p1 = -3.422 (-4.954, -1.891) p2 = 208.6 (202.2, 215)
Office	-0.2365	58	4.63	p1 = -0.3332 (-1.173, 0.5064) p2 = 198.8 (193.8, 203.9)

Table 13 All room types with correlation, number of samples, RMSE and the curve fit indicating gradient and Y-intercept with 95% CI.

From the graphed data, the room type that contains the smallest gradient along with a high correlation (in absolute terms), and a high y-intercept is the ideal room to locate wireless devices. The bathroom and laundry both contain a low correlation, this is understandable due to the variable RF conditions. Each also contains a low gradient, likely caused by the low correlation. However, these two room types have a large CI. One of the largest is for the laundry, indicating an extremely high variability of collected data, again likely due to the variable RF conditions. An interesting result is the large difference between the bathroom and the toilet, where the toilet contains the highest correlation and gradient, though again the confidence interval is one of the largest. Only 46 samples were collected, and consequently a larger collected sample might potentially alter its statistics and reduce the current outcast status. The high correlation of the toilet is offset by the fact that this room has the steepest gradient, and it is this steep gradient that contradicts the general trend of all other room types where smoother gradient is relevant. Based on the collected samples the low gradient and y-intercept of the laundry and bathroom along with the steepness of the toilet prove to be the group of room and are the worst. The biggest surprise however, is the office, which has a considerably low gradient and correlation, which is an extremely important location for wireless media. This low correlation is potentially caused by computers and other electrical devices that are associated within an office space. One positive aspect however, about the office is modest y-intercept.

Just by observing the confidence intervals of each room type, they all have the potential to be rearranged and thus produce different results. However, based on the data collected, the laundry, toilet and office are the worst with the largest confidence intervals and thus a large variance in the gradient and y-intercept is prominent. This is followed by the bathroom, hallway and kitchen, and finally the smallest confidence interval is in the living room, followed by the bedroom. This small confidence interval in the living and especially the bedroom indicates that these are one on the safest and most reliable places for wireless equipment. The living in particular can be argued is the best room for wireless media; however do not let the high gradient allow you to conclude otherwise. The gradient is one of the steepest, however it also has the highest y-intercept, and by observing figure 47 (in appendix 5) it can be seen that the living is indeed one of the highest located graphs compared to all other rooms. In addition, the correlation of the living is the highest (behind the toilet), and so a relationship between RSSI and distance is definitely prominent. This high correlation along with a relative high y-intercept and a small width in the confidence interval allows the **living** to be the number **one** spot for wireless media.

Another interesting result is the similarity between the kitchen and the bedroom, which contain extremely similar gradients, correlation, and y-intercept; they also have extremely similar RMSE values. The number of samples is significantly different - the kitchen contains three times as many samples and thus the confidence interval will be slightly tighter compared to the kitchen. Based on the statistics the kitchen and bedroom are essentially identical, which is interesting considering the amount of variability in objects that exist within each room, then again, due to the smaller confidence, the bedroom, (compared to the kitchen) shows a smaller degree of variation, and therefore can be considered better than the kitchen.

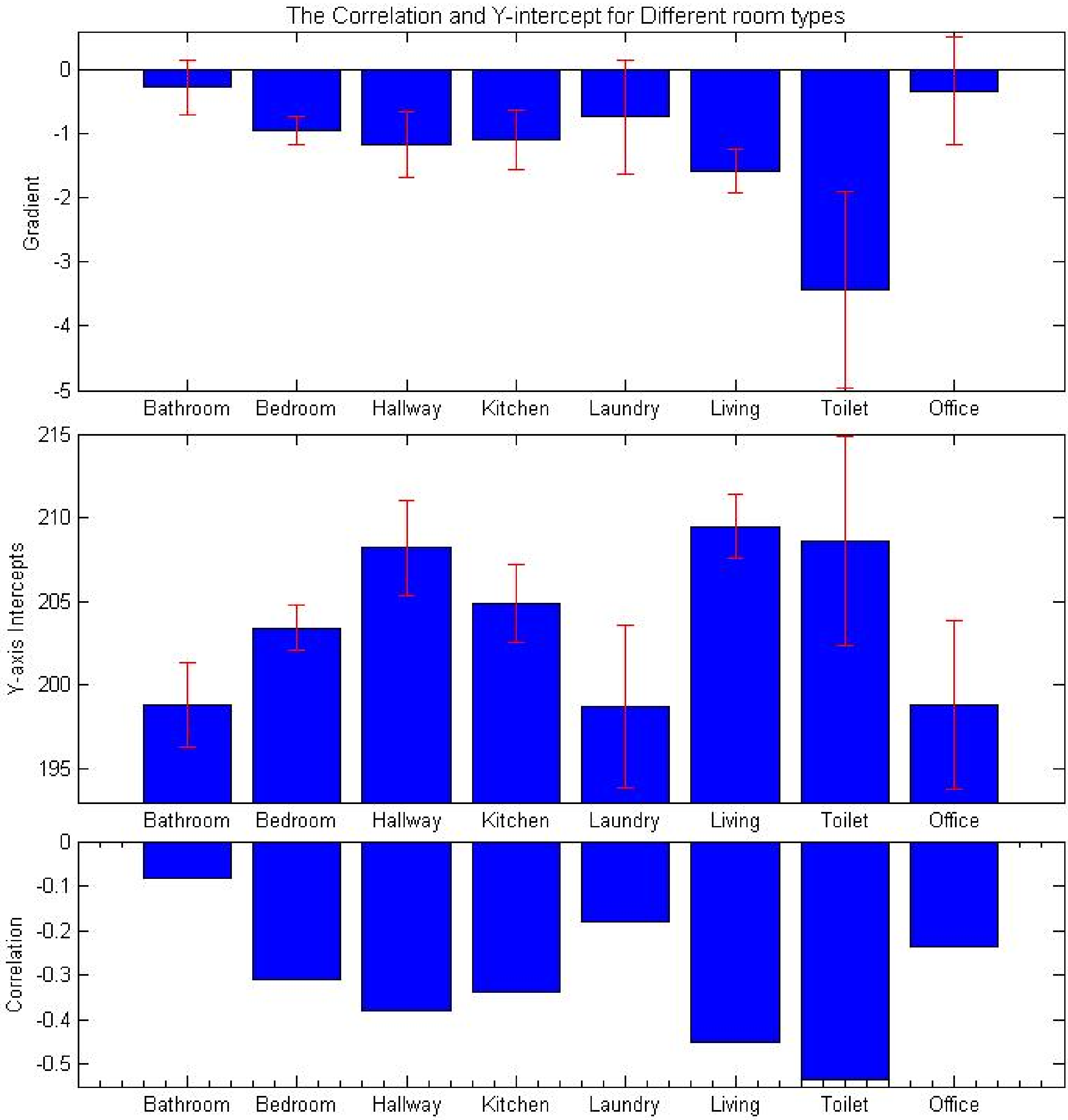


Figure 15 The Correlation with the Gradient and Y-intercept showing a 95% confidence interval for different room types.

8.1.3 Interference from 802.11 Sources

The number of operational WLANs, calculated by the number of WLANs that were disabled during the experiment (identifiable within the spreadsheet) subtracted from the number of WLANs detected by Kismet is an important factor during the collection of data. Eckhardt and Steenkiste, [14], performed a similar experiment where WLAN interference was confirmed as a source of packet errors, however, Aguayo and this team, [22], found little correlation between the number of WLANs and packet loss. This section deals with extracting the relevant data and determining if any correlation exists between the number of operational WLANs with the signal strength and PER.

Table 14 shows the frequency of operational WLANs along with RSSI and PER statistics. The gradient, y-intercept with 95% CI along with the correlation are graphed incorporating the RSSI and PER in figures 16 and 17 respectively.

Operation WLANs	**Freq**	**RSSI**			**PER**		
		Correlation	**Gradient**	**Y-intercept**	**Correlation**	**Gradient**	**Y-intercept**
1	16	-0.2810	-0.9522	203.4	0.1641	0.008574	0.04295
2	2	-0.6048	-2.206	208.6	0.3229	0.02498	-0.02876
3	7	-0.4428	-1.659	207	0.3964	0.0146	-0.0206
4	10	-0.2828	-0.8991	204.2	0.0441	0.002486	0.03846
5	2	-0.7036	-1.805	203.6	0.5690	0.0316	-0.05935
6	4	-0.4957	-1.575	209.6	0.2500	0.005535	0.0123
7	4	-0.6562	-2.403	210.4	0.0601	-0.00093	0.04141
8	5	0.0687	0.1253	199.3	-0.0660	-0.00233	0.07829
11	2	-0.3309	-0.6795	206.1	0.3107	0.00442	0.0358
13	1	-0.2959	-0.7602	204.5	0.4089	0.02211	-0.0543
15	2	-0.1494	-0.3822	203.3	0.1187	0.003234	0.0221

Table 14 Number of Operational WLANs indicating frequency with RSSI and PER statistics.

From figure 16, as the number of operational wireless LANs increase, there is no observable trend in the gradient, y-intercept or correlation. Even incorporating the confidence intervals, still no obvious trend can be found. Removing the low frequency samples from the analyses, which include two, five, eleven, thirteen and fifteen (operational WLANs) still no trend emerges. If only the high frequency samples are used including one, three and four (operational WLANs), the only trend that exists is that a single WLAN contains the lowest gradient, lowest y-intercept and lowest correlation, while three operation WLANs contains the highest statistics, and the fourth is in the middle. This trend in gradient, y-intercept and correlation seems more of a coincidence, however, using two samples that contain the same frequency, six and seven (operational WLANs) the trend is still evident. A trend does indeed seem to occur, though the trend is not evident in samples that contain a small frequency, and so would seem more of a coincidence.

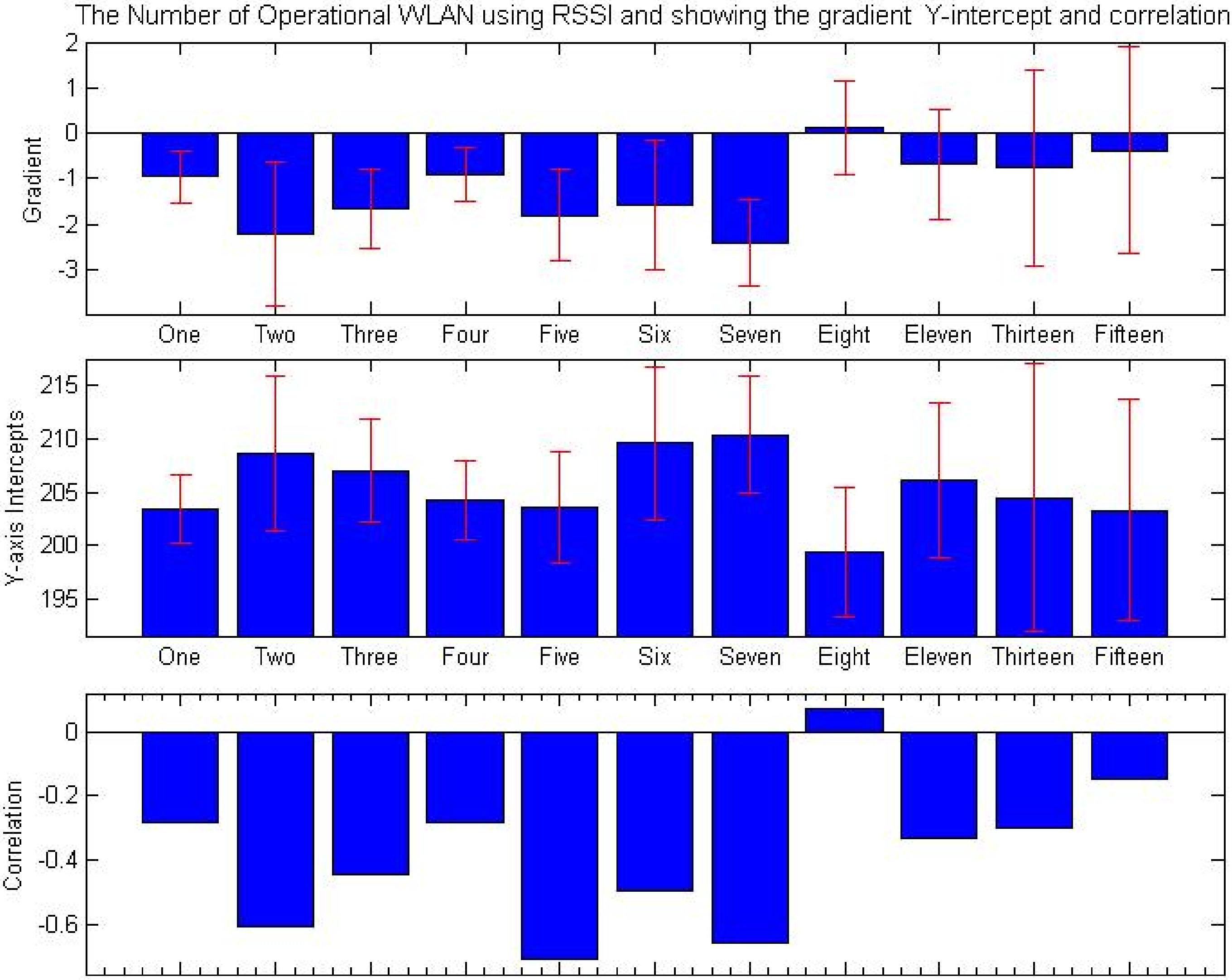


Figure 16 The Correlation with the Gradient and Y-intercept showing a 95% confidence interval for different number of operation WLANs using RSSI.

According to the 802.11 standard: the RSSI is described as **only** the "energy observed at the receiving antenna", and therefore is a measurement of the power of the signal regardless of how clear or concise the signal is. Even though RSSI only measures the power of the observed signal, and therefore does not consider the amount of interference within an environment. Determining if the number of operational WLANs does cause any harm should be more evident when observing PERs. So, the gradient, Y-intercept and correlation where calculated for the PERs within each operational WLAN. The 95% confidence interval was very large and so was not placed in figure 17, but is shown in appendix 6.

As the number of operational WLANs increase, a relatively sound hypothesis might dictate that the PER should also increase thus producing a steeper gradient. In spite of this, figure 17, does not incorporate the channels used by any WLANs. A histogram of only the channels used by potential sources of interference is shown in figure 18, where the first channel is zero in dark blue, and an unknown channel is shown last in brown. If kismet does not have enough packets to determine the exact channel of a wireless LAN, it assigns the channel 0. This channel will be discarded from analyses, as each could potentially be operating on any channel between 1 to 12. In addition, a few WLANs were detected that contained extremely high operating channels, these WLANs are operating on the 802.11a standard and shown on the graph as errors. Since 802.11a does not operate within the 2.4 GHz band it will be discarded from analyses.

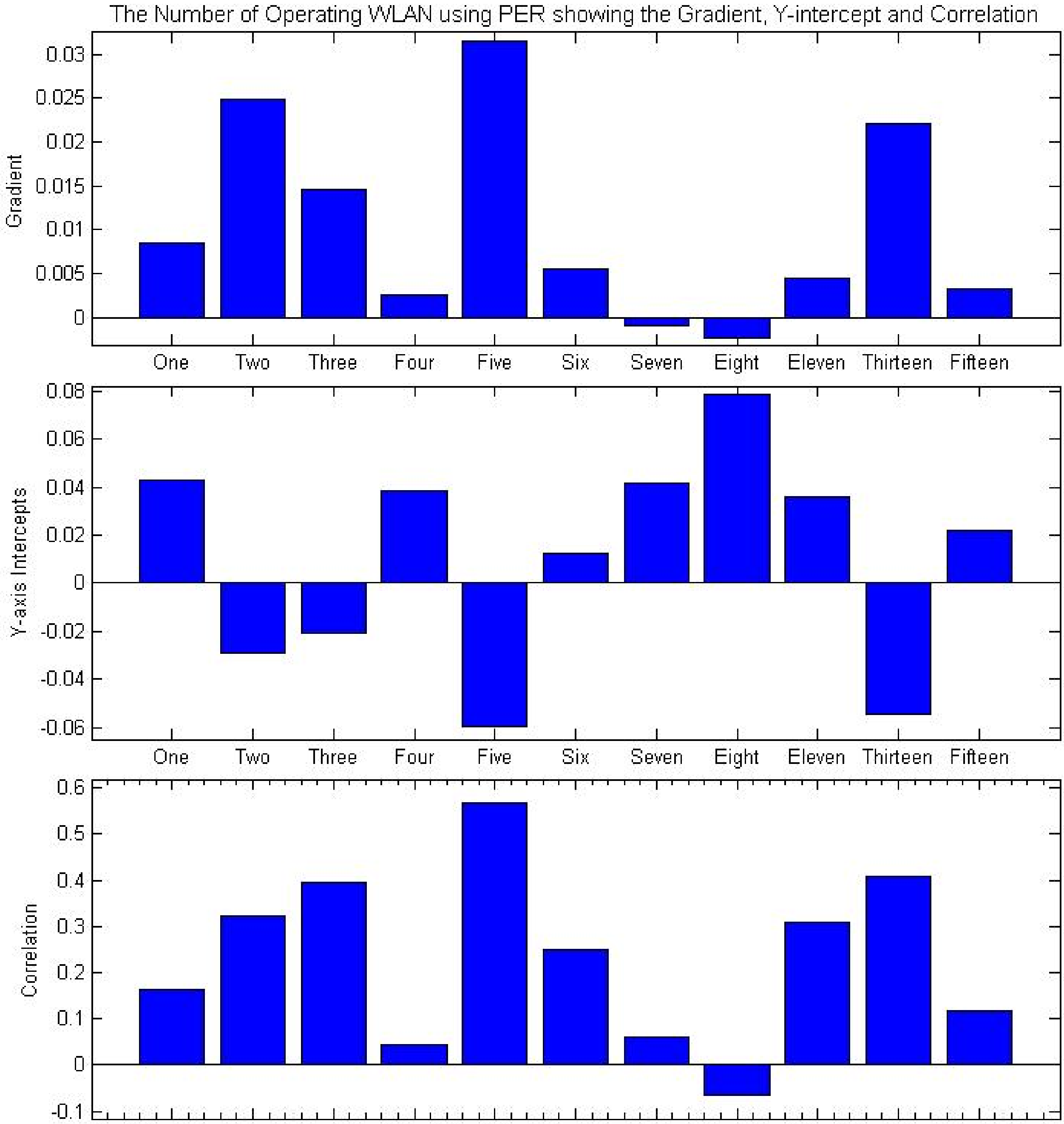


Figure 17 The Correlation with the Gradient and Y-intercept showing a 95% confidence interval for different number of operation WLANs using PER.

The channel used in the experiment is channel 6, and based on theory (explained in section 3.2) all other channels except channels 1 and 11 are a potential source of interference. Using this fact, samples that contain a higher number of interfering channels should produce more packet errors and contain stepper gradients. Sample eight has the highest number of interfering channels, but is one of only two samples that contains a negative gradient, and is the only sample that contains a negative correlation, which shows a decrease in PER over distance. The next potential highest amount of interference, is from sample fifteen, this sample however, has a positive correlation. Therefore, **no conclusive results** can be determined based on the PER and the amount of interfering WLANs.

One aspect of the graph that is important is the y-intercept values. Some of these values are negative, and obviously, a negative PER cannot occur. This is an indication that not enough samples were collected. Thus, based on the collected no trend can be found.

The channel utilisation histogram shows a general trend where channel 6 and channel 11 are the channels that have the highest frequency. This might be an indication that many persons operating WLANs do know of the potential interference from other operating WLANs in the vicinity, and are attempting to minimise any potential interference.

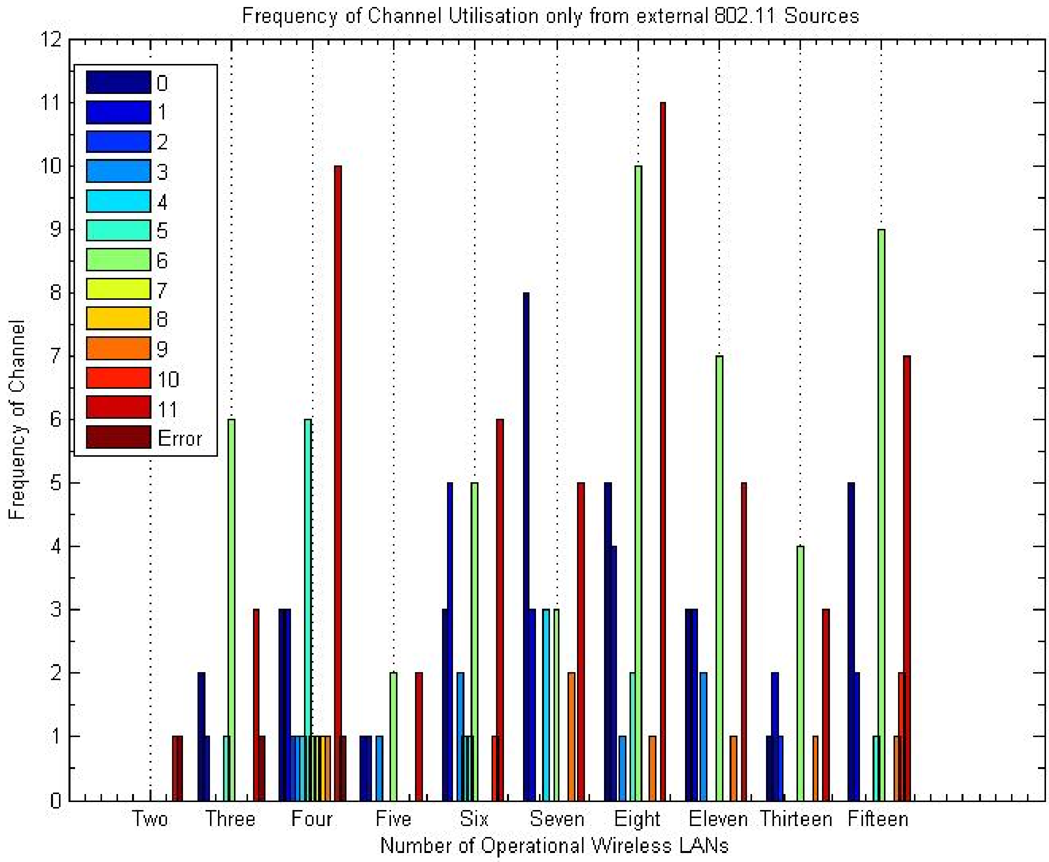


Figure 18 A histogram of channels used by external operating WLANs

8.1.4 Air-conditioning

Ducted air-conditioning within a dwelling is an interesting field to study, due to the amount of metal contained within a single dwelling can be quite substantial. Therefore attenuation, diffraction and reflection can all occur and can potentially cause a loss of signal strength and possibly a reduction of PER. Figure 19 shows the variation of signal strength of dwellings that contain and lack ducted air-conditioning whereas figure 20 shows the variation in PER.

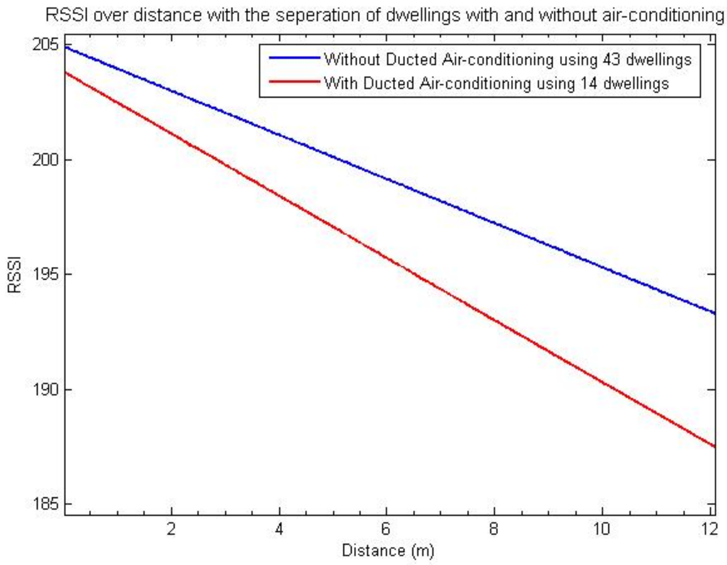


Figure 19 (left) Separated dwellings with and without air-conditioning showing the variation of RSSI over distance

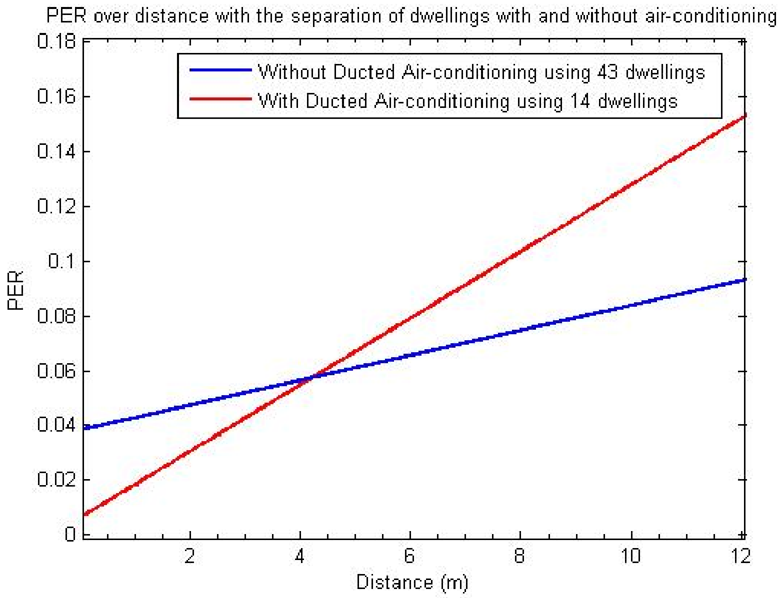


Figure 20 (right) Separated dwellings with and without air-conditioning showing the variation of PER over distance

The confidence intervals in each case shows roughly the same distribution and so was removed from this figure, but is attached in appendix 7. From figure 19, it is evident that dwellings that **contain** ducted-air-conditioning have lower **signal strength** to distance graph, which is indeed intuitive due to the overall worsened conditions caused by the attenuation, diffraction and reflection of the air-conditioning components. From this graph, and based on our previous discovery, the dwellings that lack ducted air-conditioning should also produce an overall better PER, where the PER graph has been calculated and shown in figure 20. According to this graph, this is not 100% true, as dwellings that **do not** have ducted air-conditioning initially have a lower PER. This, **alters at 4.2 meters** where the converse it true. A possible reason for the changeover at 4.2 metres could be due to the average room size for the 14 dwellings that contained air-conditioning, as ultimately, measurements taken within the same room might have a reduced effect on the transmitted signal as less attenuation, diffraction and reflection occurs. More over, the more likely explanation for the changeover at the 4.2-metre mark is a mere coincidence and there is no literal and meaningful justification.

Based on the statistics for both the PER and RSSI (table 15) the correlation for PER is extremely low in both cases, which indicates that there is no real association between the dependence on air-conditioning and the PER, also the RSSI shows a relatively small correlation. However, dwellings that contain air-conditioning have roughly double the correlation than dwellings without, so **signs** do indeed exist that the **signal strength and PER are impacted by air-conditioning**, though further investigation is needed for a more **conclusive answer**.

	Freq	RSSI			PER		
		Correlation	Gradient	Y-intercept	Correlation	Gradient	Y-intercept
Without Air	43	-0.2856	-0.9608	204.9	0.1149	0.004553	0.03824
With Air	14	-0.4057	-1.352	203.8	0.2507	0.01215	0.006133

Table 15 Statistics for RSSI graphs for dwellings with and without air-conditioning

8.1.5 People

The amount of people that were within a wireless environment was also investigated to determine if any side effects were induced. The usual trends existed in all graphs, such as a decrease of PER over distance and a decrease in signal strength over distance. A sample of a few signal strength graphs is given in appendix 8. Finding any correlation as the number of people increase with PER and RSSI was **not** evident, this process made more difficult due to the large CI present in all graphs. The lack of results is somewhat understandable considering the dimensions of an average human body is not much larger than, for example, a filing cabinet. If a large amount of people were present, then these results might change, such as in [14], where signal strength and packet error rates were sightly impaired when a person "bends over to examine the laptop screen". To determine if an individual does indeed attenuate signal strength, further experiments will be performed, (category one in changer 9). Regardless, if relatively small amounts of people are present during the operation of WLANs, then **no** effect on RSSI and PER is evident.

8.1.6 Humidity

Humidity is a measure of the quantity of water vapour within the air, while relative humidity is given as a percentage, which identifies the ratio of water vapour divided by the amount of water the air can hold [29]. Therefore, a humidity of 50% indicates that the air can hold double the current water vapour. A 100% relative humidity indicates that no more water can be held and so rain occurs, however, most of the time the air below the clouds and on earth is not saturated. Thus, rain only originates from saturated clouds, and can pass through unsaturated drier air particles, and so the relative humidity on the ground could be as low as 90 [30].

The wavelength corresponding to 2.4 GHz is about 4.5 inches in length, and so a dipole is in the order of a couple of inches in length, which is a lot bigger than a water molecule, and so the potential for attenuation is minimal [ECMpuke, 29]. Many mixed opinions exist about the effect on humidity on RF signals. Therefore, does the humidity have any impact on signal strength and PER within wireless networks? This experiment tries to determine if any correlation exists between humidity and the attenuation of wireless signals.

Since rain can occur even as low as 90, the humidity was separated into 10 discrete intervals, where figure 21 shows the gradient, y-intercept and correlation of the signal strength over distance. From this figure, as the humidity increases, there is no obvious relationship with the gradient, y-intercept or correlation. In fact as the humidity increases the gradient acts somewhat as a step function, altering between low gradient, then high, then back to low and so on. However, the greatest outlier is the set 41-50; this is the outlier in all RSSI measurements. It is both this set along with the 51-60 set that contains the least amount of samples, with 51-60 showing the greatest range of CIs in both the gradient and y-intercept. Even though the CI might be large, this **is not** an indicator of low correlation, as the sample 41-50 bucks this trend. Thus, from the data collected 41-50 and 51-60 are the outliers.

The last three sets (71-80, 81-90 and 91-100) do contain a large range of samples (over 350 each) but still no gradient relationship is evident. The 91-100 set does contain the lowest gradient with the lowest y-intercept, however is also the sample that contains essentially no correlation at close to zero, and so no trend is evident, thus the gradient and y-intercept values are not that reliable.

From the samples collected, the only conclusion is the humidity **does not attenuate** signal strength, and so is not a factor to hinder the received signal power. However, a direct experiment on humidity and its effects is given in category one chapter 9.

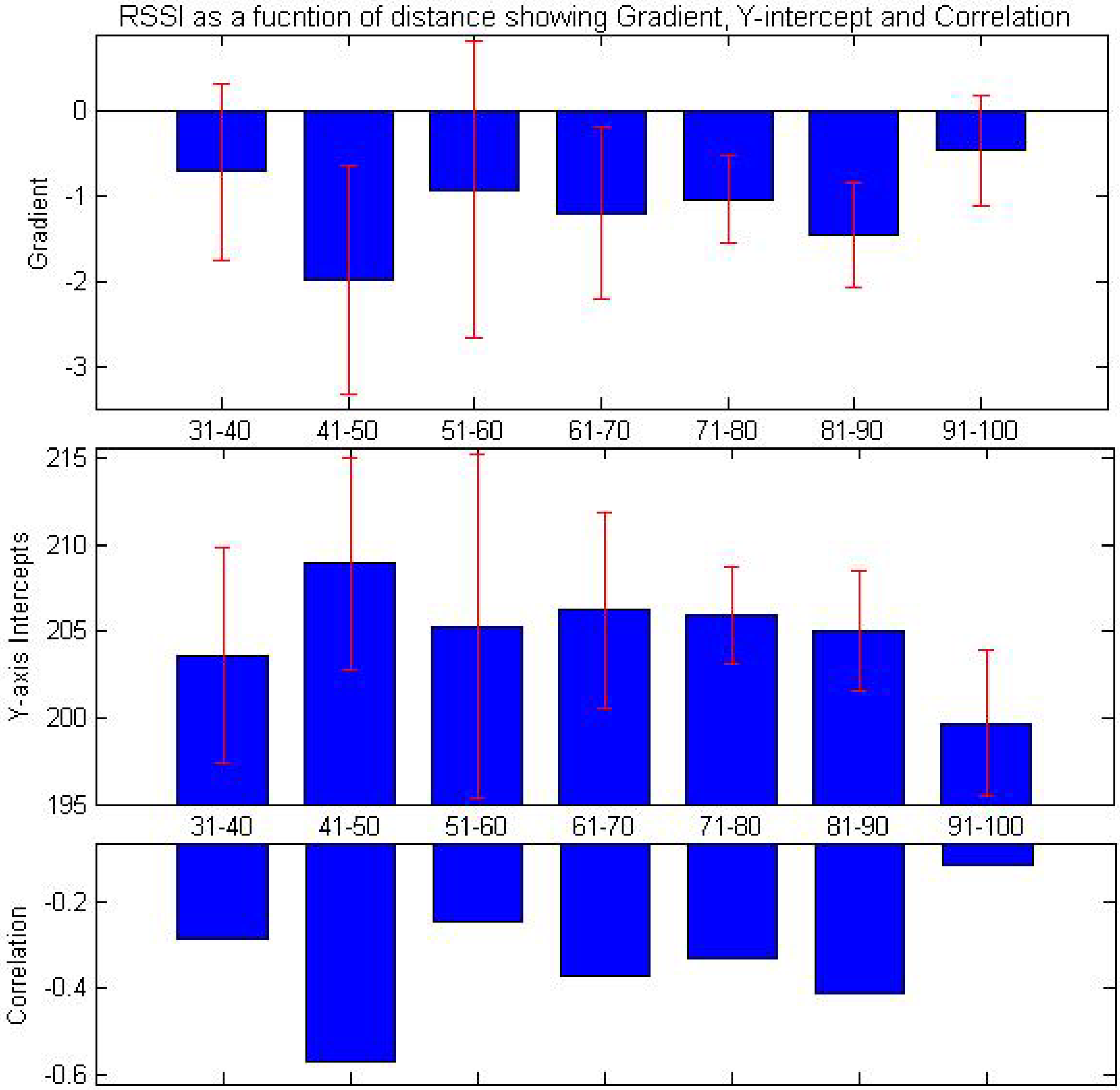


Figure 21 The Gradient, Y-intercept and Correlation using RSSI as a function of Humidity separated into groups of 10.

Humidity	Freq	RSSI			PER		
		Correlation	Gradient	Y-intercept	Correlation	Gradient	Y-intercept
31-40	107	-0.2842	-0.7132	203.6	0.0619	0.0006054	0.05257
41-50	61	-0.5726	-1.982	208.9	-0.1405	-0.004986	0.07473
51-60	60	-0.2442	-0.9241	205.3	-0.0340	-0.000428	0.0447
61-70	149	-0.3700	-1.202	206.2	0.1439	0.006461	0.02571
71-80	570	-0.3294	-1.039	205.9	0.1927	0.008375	0.02724
81-90	464	-0.4131	-1.45	205	0.1490	0.008157	0.03628
91-100	357	-0.1111	-0.4567	199.7	-0.0063	-0.002445	0.1185

Table 16 Statistics for RSSI and PER over distance for a range of different Humidity sets

The PER produced a worse relationship, where all samples are graphed in a single figure and shown in appendix 9, though statistics are given in figure 22. No CI were used as these were large, but are attached in appendix 9. Examples of the gradient increasing, decreasing and essentially straight. The same trend is prominent within the correlations, which indicates the same **relationship** between the **spread** of collected data and the **steepness** of the weighted line of best fit.

The CI is also another aspect to notice, where the sets that are increasing have a smaller CI compared to other samples in which the PER remains constant or decreases as the PER increases. So latitude remains, if a large sample were to be collected better results might entail, however, based on the data collected no trend at all exists within the gradient or y-intercept, and thus based on the data collected the humidity **does not** alter or coerce the PERs.

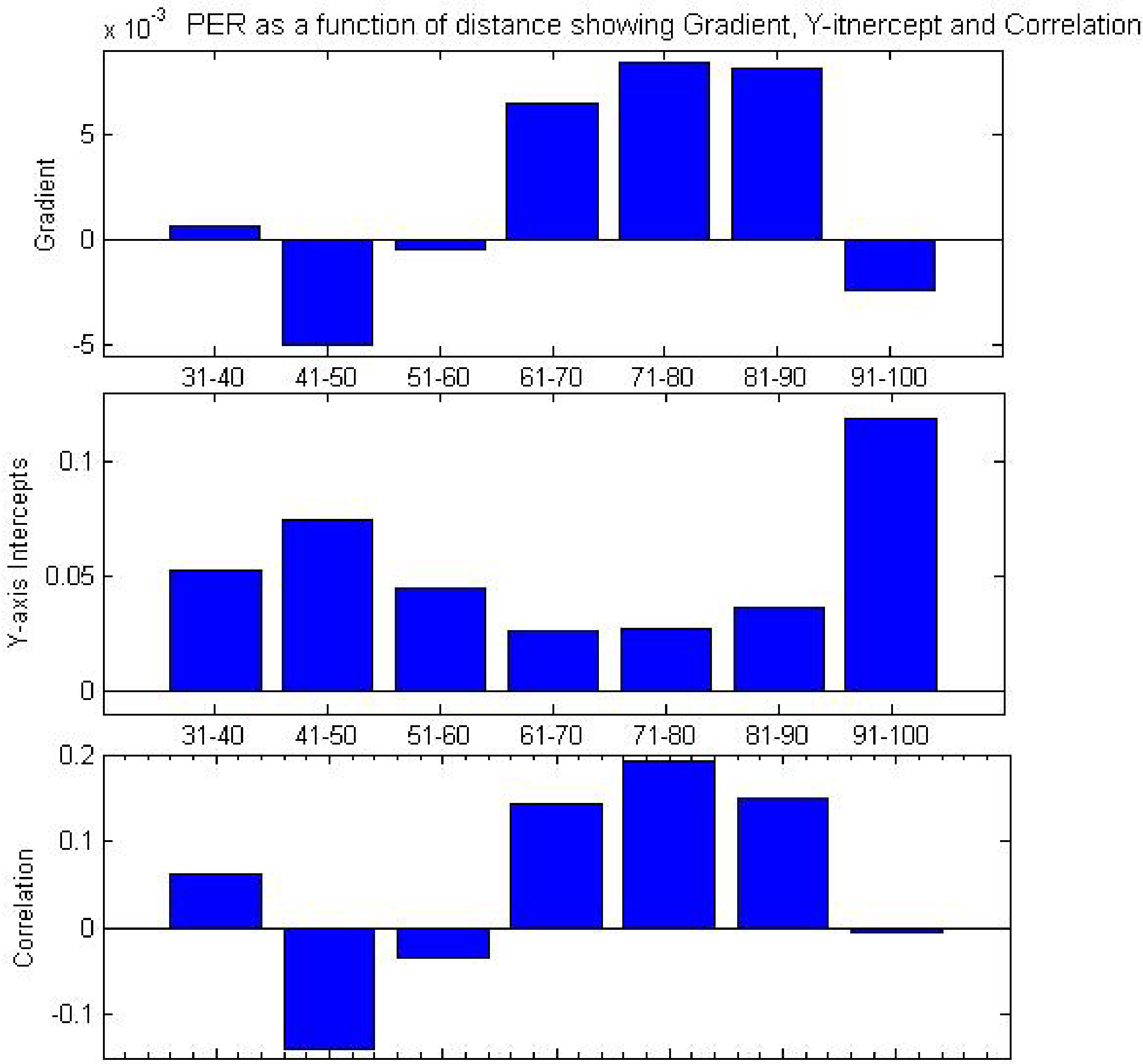


Figure 22 The Gradient, Y-intercept and Correlation using PER as a function of Humidity separated into groups of 10.

8.1.7 The Best Location?

From the results collected, the logical question and what ultimately is of most importance to the end user is **choosing the optimum position to achieve the best wireless performance** for all wireless devices within a network. Steps that the wireless user should incorporate include:

1) A rough guideline could be to place the AP in the geographical centre of all users that require wireless network access. This ensures the signal will radiate omni-directionally to all users and maximise coverage over the dwelling. **However**, signal strength has a more predominant effect on PER that the attenuation due to distance. Thus, the need to choose a location for both the AP and the end user that has higher signal strengths is considered more significant. This can be done by:
   - Using Kismet, which can detect the Signal Strength.
   - Avoid rooms such as the laundry, toilet, and bathroom, which produce the worst RSSI measurements.
   - The best locations include the hallway and living.
2) Place the router as high as possible to minimise the attenuation due to objects.
3) Attempt to reduce the amount of vertical planes that the transmitted signal needs to traverse through, this includes walls, ceilings doors, and/or floors.
4) Avoid placing wireless devices near objects that cause interference, especially microwaves (see microwave section within chapter 9), and try to avoid objects that creates reflections, diffraction or scattering.
5) If a single AP does not provide adequate coverage for all wireless devices or poor wireless performance is experienced, additional APs can be added to wireless network that increase range and performance.

Given the above criteria, the router and end user locations can be shifted to reduce the amount of errors and to maximise signal strength. In most cases the optimum position based on the above criteria might not be viable or sensible, possibly due to the lack of facilities such as power or Cable/ADSL outlet, and so the closest rational location should be chosen based on the criteria mentioned.

8.2 Time variation

The temporal behaviour of two wireless features over time are investigated: the signal strength and the error rate.

8.2.1 Signal Strength

Observing the strength file in appendix three indicates the signal strength constantly changing over time. The primary reason for this is due to the varying combination of mentioned impairments in section 3.4. The end result is that the signal strength will fluctuate between the measurement point and router and this fluctuation will occur with respect to time and distance between the two communicating bodies. However, the fundamental question is: **how long does one need to observe the signal strength to be confident in its mean value**. This question is extremely important for this thesis, as all data for each measurement point, was collected for a 30-second interval, and the essential question then is: does this 30-second interval capture the entire variance of the signal strength over time, and ultimately how accurate are the results presented within this thesis.

8.2.1.1 The Observed Trends

From observing the different variations of signal strength graphs, produced by StrengthTime.m (7.2.2.4), each can be categorised into one of **four classes**:

1) No variation of signal strength.
2) Variation occurs in discrete phases
3) Intermediary and subtle changes in signal level.
4) Cannot determine category, as experiment was not run long enough to observe any trends.

1) No variation of signal strength

These samples show **no substantial variation** of signal strength over time for the collection process, and account for approximately **22%** of data collected. An example is shown in figure 23, where the collection process lasted approximately 7.5 hours with a mean of –66.23dBm (shown in red) and a standard deviation of 1.02dBm.

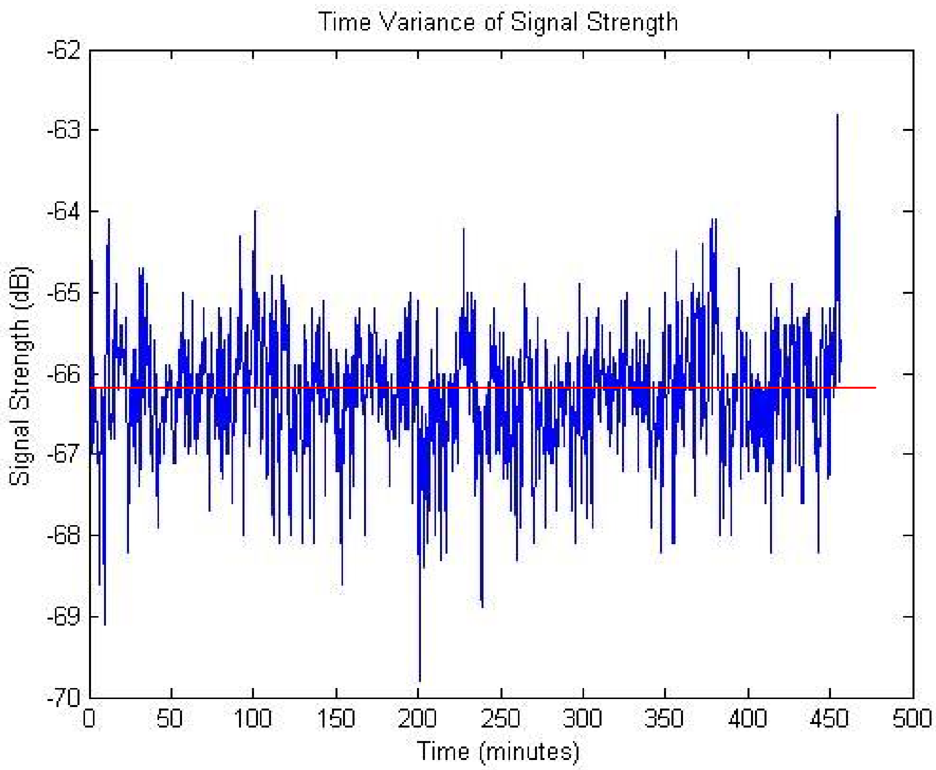


Figure 23 An example of no variation of signal strength

2) Variation occurs in discrete phases

Figure 24 shows a sample where the signal strength constitutes **discrete phases**. These phases are identified from sections of the graph that contain different mean and standard deviations values. For figure 21, the two separate phases are circled in red and green, where the first phase (red) occurs from 0 to 6.6 hours with a mean of -54.25dBm, while the second occurs from 6.6 hours to the finish with a mean of -50.9dBm. Thus a difference in averages of about 3.35dBm. However, one important issue with these measurements is the durations of the phases, and since the experiment was stopped by the user, the exact duration is unknown as generally only a single transition was captured (as in figure 21). From observing multitudes of graphs, the phases seem to be completely random, that is:

- The phases occur over multiple hours.
- The phases can occur anywhere within the received signal.
- The amount of noise within each phase can vary.
- The exact pattern of the phases is random. That is, the graph could start in a high phase, and then go low, or the graph could take the form of the converse.

From the collected data, about **35%** contains some form of discrete variation in phase. From this subset of data, a general analysis is that the ranges exist from **5-10dBm, and the period of the duration lasts in the order of hours.**

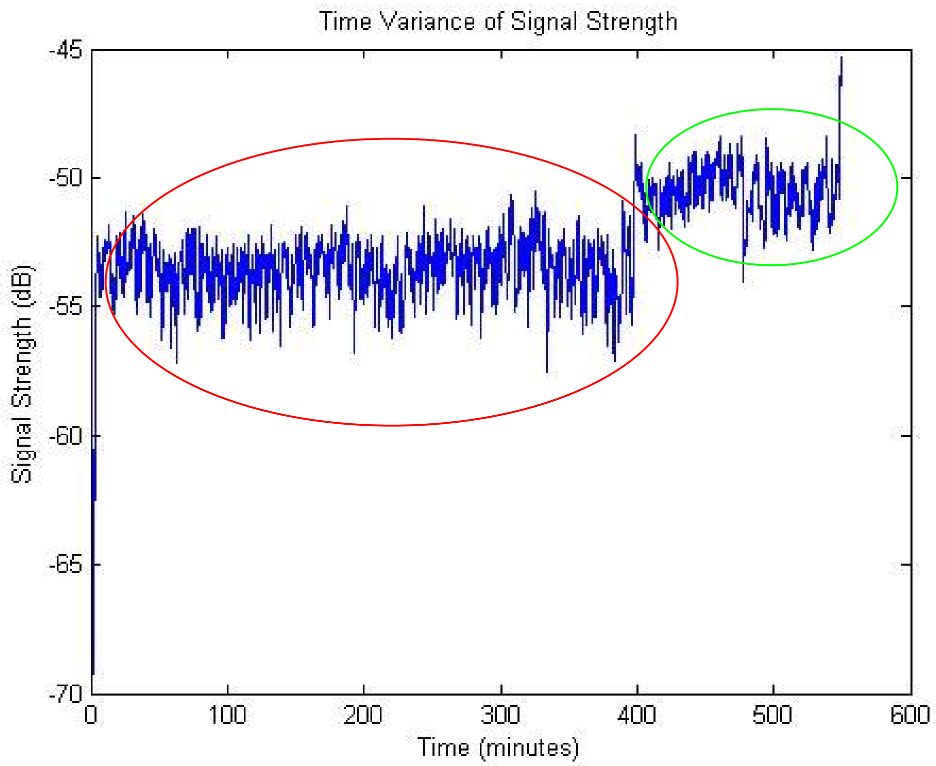


Figure 24 Time Variance of Signal Strength Over in discrete phases

3) Intermediary and subtle changes in signal level.

This class of signal strength graphs **do vary over time** and thus are not classified within class one and do not maintain a constant mean over discrete phases, as in figure 24, and so are not classified within class two. An example of one such graph is shown in figure 25, where from the start to 3.5 hours a linear increase in signal strength is observed (shown in red), from here on, a constant signal strength with mean -56.2dBm (shown in green). This class of signal strength variation accounts for **33%** of collected data.

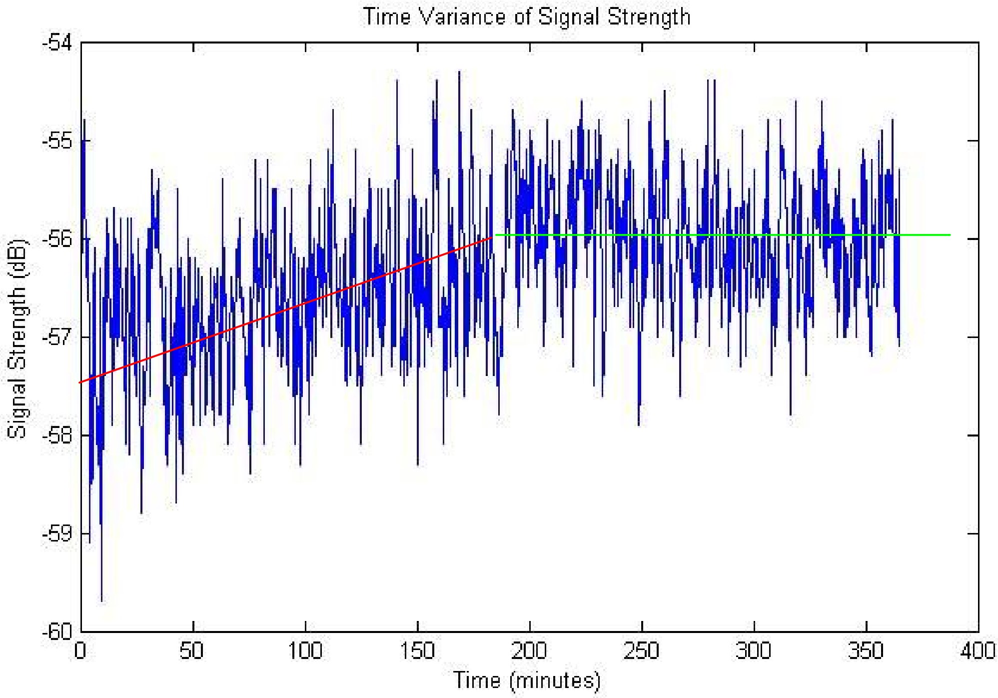


Figure 25 Intermediary and subtle changes in Signal Strength over time

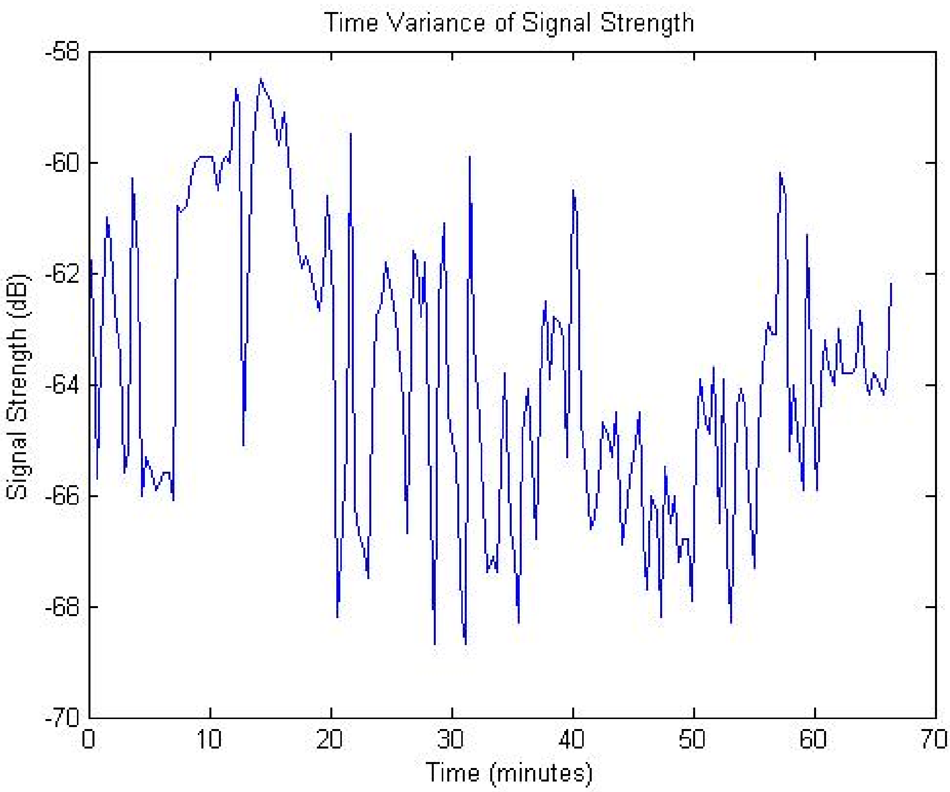


Figure 26 No trend in Signal Strength over time

4) Other Various

This final class of signal strength types do not belong to any of the other three classes as the collection process was stopped before any observable trend could be seen, an example is given in figure 26. The duration of the collected data was for no more than 1.5 hours, which is low compared to the other categories of collected data and a potential longer period is needed for any trend to arise. More importantly, all examples within this category display a high degree of variance of signal strength over time. This group contributes about **10%** of the collected data.

Conclusion

The running of this experiment required students to run the observe program within a 10 meter radius of the router for a prolonged period. From the produced classes **1 in 10** samples of data shows no indication of any observable trends (class four) however this data class does indicate a higher degree of variance in signal strength. **Twenty-two precent** of data shows that the signal strength does **not** alter over time (class one), whereas **58%** (classes two and three) show that a variation is **evident**. Ultimately though, it depends on what your definition of stationary is. If you consider a **5-10dBm** high, (as in class two which counted for **23%**), then the signal strength does indeed alter over time. If for whatever reason a 5-10dBm is not considered a drastic change, then the signal strength is relatively stationary over time. Nonetheless, regardless of stationarity, this experiment shows **that the signal strength can alter randomly for no apparent reason and at any given time**, and so performing experimentations where observing signal strength requires hours of data collection only to incorporate signal fluctuations is time consuming and generally cannot be done. Nevertheless, this experiment revealed that if an accurate measurement is needed where all fluctuations are incorporated, then the data suggests the collection process take place over multiple hours. While the long-term alteration in signal strength is evident, the alteration of signal strength in the short term, that is, from the current 30-second period to the next 30-second period still needs to be explored.

8.2.1.2 The Experiment Period

From observing the signal strength over a prolonged period of time, the alteration within a 30-second period is the logical next step, which raises a fundamental question: how similar (or different) is a current 30-second measurement period to the next 30-second interval? To calculate this, the autocorrelation function using the signal strength data is used with a lag of 30 seconds.

The autocorrelation with a 30-second lag was calculated for all samples to be on average 0.363 with a standard deviation of 0.225. This average value does seem low, indicating that no real correlation exists between different 30-second periods, and then raises the issue that the 30-second period might not be long enough to capture the variability of signal strength. However, for comparison, a single lag was calculated to have an average of 0.625 with standard deviation of 0.236. This puts the initial 30-second lag calculation into more perspective, as even a single lag shows a relatively high degree of alteration in signal strength. On the other hand, all measurements taken incorporated this 30-second period and since the correlation falls significantly short of the maximum one value, the question of accuracy is then raised, namely how accurate is the signal strength for the 30-second period? Through observing the many signal strength graphs over a 30-second period, a rough approximation is that the **signal strength for a 30-second period has a resolution of ± 2dBm. Therefore, all collected data throughout this thesis is accurate to within ± 2dBm.**

- **Signal Strength Conclusion**

The analysis of signal strength for a prolonged period indicates that signal strength can alter unpredictably for no apparent cause and at any given moment. More importantly, if any fluctuations in signal strength need to be identified then the collected data proposes that multiple hours of data is crucial. However, all experimental measurements incorporate a 30-second period, where the accuracy of this measurement corresponds to a precision of ± 2dBm at each measurement location. This 30-second period is thus an approximate estimate of the signal strength at a particular point in time. Gradually, over a prolonged period (many hours) this 30-second capture will:

- Stay constant for multiple hours then alter at a rate of 5-10dBm with a probability of 0.35.
- Change minimally over time with 0.33 probability.
- Change drastically in a small time frame with probability of 0.1.
- The ideal outcome, not alter at all with probability 0.22.

8.2.2 Packet Error Rate

A simple linear relationship between the signal strength and PER has already been discussed (8.1.1), where an alteration in signal strength did alter PERs, however the potential variation of PERs at a stationary location and the quantity of packet bursts at a constant location while stationary over time has not been addressed.

8.2.2.1 The Observed Trends

From the PacketLoss.m MATLAB program (7.2.2.6), a sample of a **typical graph** showing the frequency of the error bursts is illustrated in figure 27. This graph shows:

1 The majority of packet loss occurs when the burst size is small.

2 More importantly, is the general trend, which indicates as the burst size increases, the frequency of packet length decreases, in an **exponential** manner. This experimental discover was also found by [26]. This exponential decrease will be investigated further as used within the Markov model.

3 A third aspect to note is that errors seem to occur in rough bursts of five, evident in the tail end of the graph, (at burst sizes greater than 30). From this result, an important question is raised, namely, why does this occur? The answer to this, could lie within the emit program, where its primary function was to send out packets uniformly, that is, with a constant interval between the transmitted packets. At the receiver side, however, packets were received in rough bursts of five, which is hinted at graphically in figure 27. This trend is even more prominent when the experiment 5 capture is opened and examined within Ethereal.

This burstiness can potentially cause problems, **namely packets are more susceptible to the external randomness of noise independent from the transmitted system**. Because if noise were to occur instantaneously for a finite amount of time, it will ultimately have a greater impact on packets that are grouped together, in bursts, than packets that are evenly distributed. The worst-case scenario occurs when the noise is synchronised onto the packet bursts and potentially all packets will be lost. Thus, the observation at the output (receiver) is effected by the timing at which packets are transmitted by the sender (at the input).

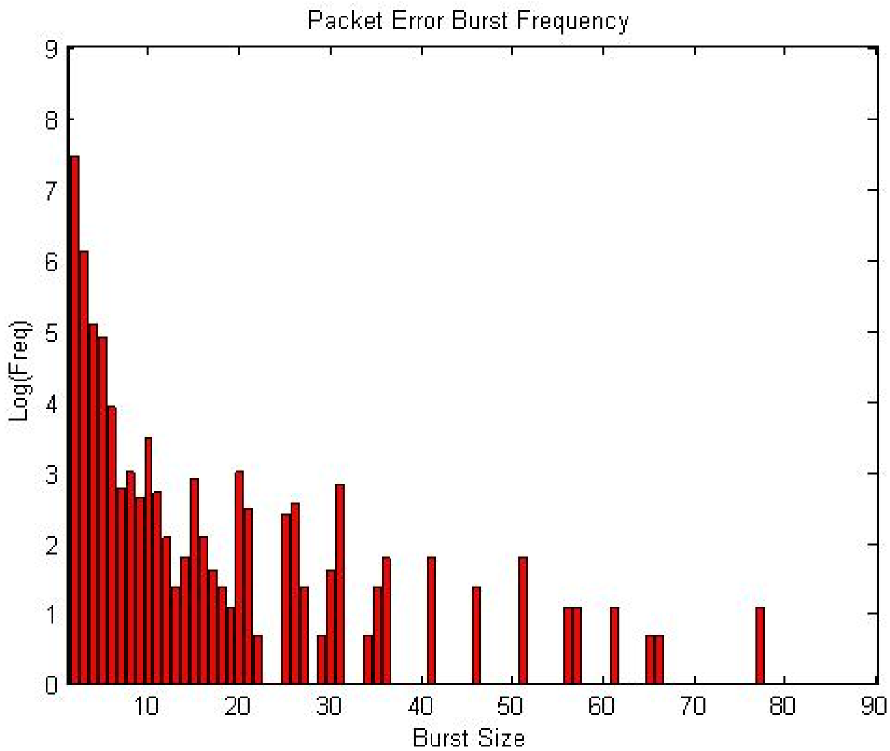


Figure 27 Packet Error Bust Frequency of a typical sample

This burstiness could have a number of causes namely:

1. A bug within the source program.

2. The router could be buffering the transmitted data and sending the packets in bursts.
3. The receiver, in particular the NIC could be buffering the data before passing the data to higher layers.

It was initially thought that bursts always occurred in groups of five. However, by observing the sequence numbers within Ethereal it was found that this hypothesis was false. Nonetheless, packets were being received in **approximate bursts of five**. Because of the burstiness an attempt was made to combine packets in busts from the packets file and graph the error rate, thus incorporating the means by which data was sent. However, the output did not prove to be useful, for two reasons:

1. The graphed packets within the packets file might not be synchronised with the actual burst packets within Ethereal. An attempt was made to permutate the packets file with the Ethereal file so the correct burst sequence could be used, however this task was extremely difficult and ultimately seemed too ambitious.
2. The data collection process was run for a prolonged period. Thus, dividing all collected packets into multiples of 5, and graphing this data resulted in plots where no trend was evident as the plots contained too many data points. Zooming in on a particular section did not help due to the reason given above.

Ultimately, it is the variation of packet loss over time that is of significant interest, and from observing the different variations of PER graphs produced by ErrorTime.m (7.2.2.6), each can be categorised into one of four classes:

1) No variation in PER.
2) No variation in PER, including some random peaks where the error rate drastically alters.
3) Slight variations in PER, including random peaks where the error rate drastically alters.
4) Variation in PER is obvious.

1) No variation in PER

Figure 28 is an example of how PER does not alter over time for the duration of the collected data. The red line on the figure indicates the mean PER of 0.198. This class of no variation in PER only contributes less than **1%** of all collected data.

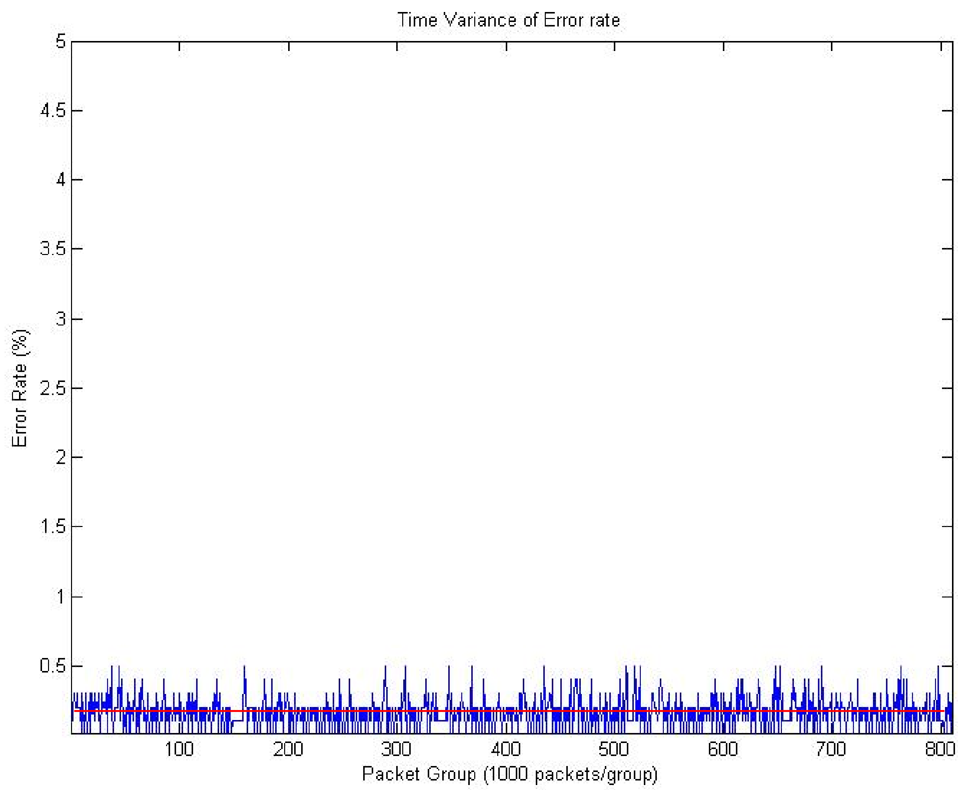


Figure 28 No variation of signal strength over time

2) No variation in PER, including some random peaks where the error rate alters.

Figure 29 shows a sample where the PER for the majority of the collected packets remains constant at an invarying mean; however, this category of data contains random peaks where the error rate alters. An example of this alteration is circled on the graph where the error rate alters from the mean of 0.23 to approximately 1 and 3.75 for an extremely short period of time (approximately a couple of groups of 100 packets). From observing multitudes of graphs, these peak error rates have a wide range from as low as few percentage to as high as 100%. However, the peak is *always* more than 4 times the mean of the invarying graph. The position of the error rates within the error stream however seems to be completely random, that is, they occur anywhere within the received packet stream. The duration of these peaks last on average no more than a handful of collected groups of 1000, and thus the **duration of these peak error rates last on average no more than a 2-minute duration.**

This class of data contributes **45%** of collected data.

3) Moderate variation in PER, including random peaks where the error rate alters

This category of graphs contains PERs that vary gradually over time, and thus does not show a drastic alteration for the entire data collection process. Figure 30 is an example where the PER does not remain constant, but varies moderately (shows as red arrows) and includes a peak error rate that is considerably different to the remaining data. This category of PER variations accounts for **16%** of collected data.

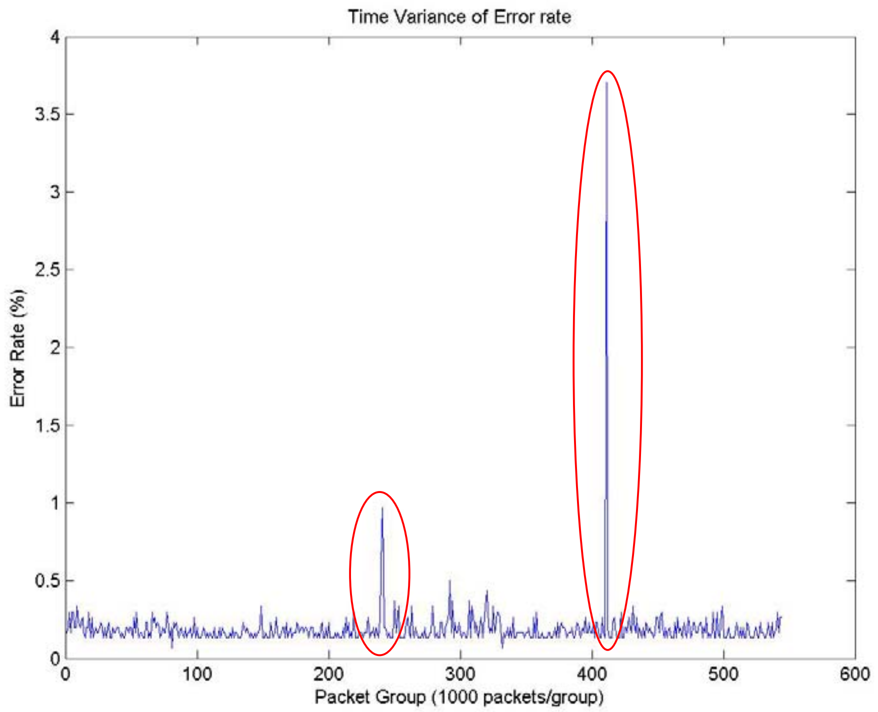


Figure 29 An example of random peaks error rates occurring for a short amount of time

4) Variation in PER is obvious

The final category of collected PER shows a drastic alteration for the entire duration of accumulated data (figure 31). This category contributes about **38%** of all data.

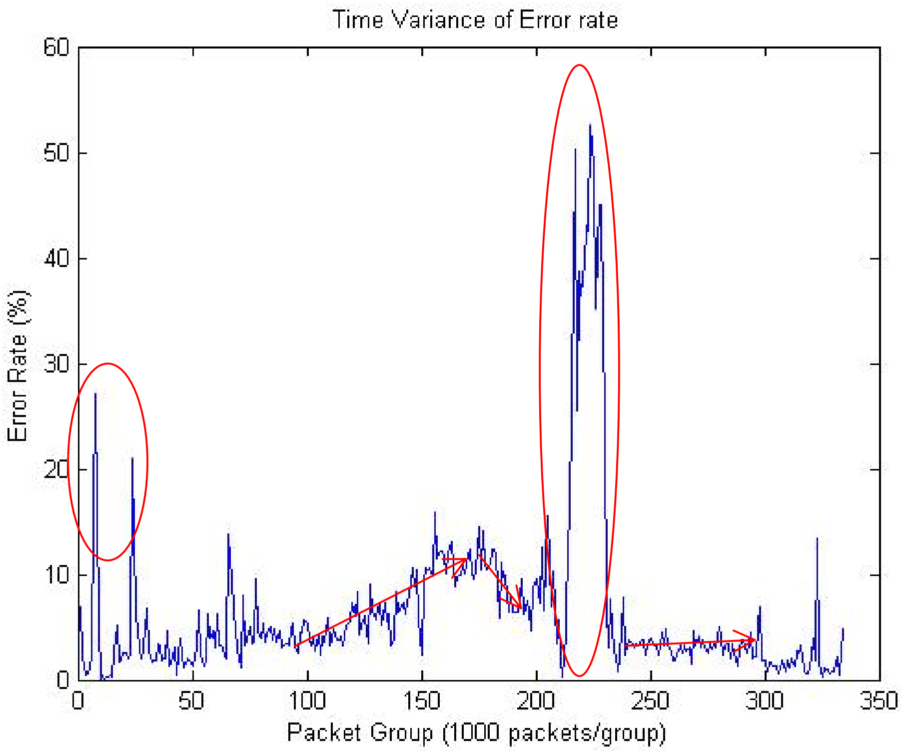


Figure 30 Slight variations in error rate including a peak

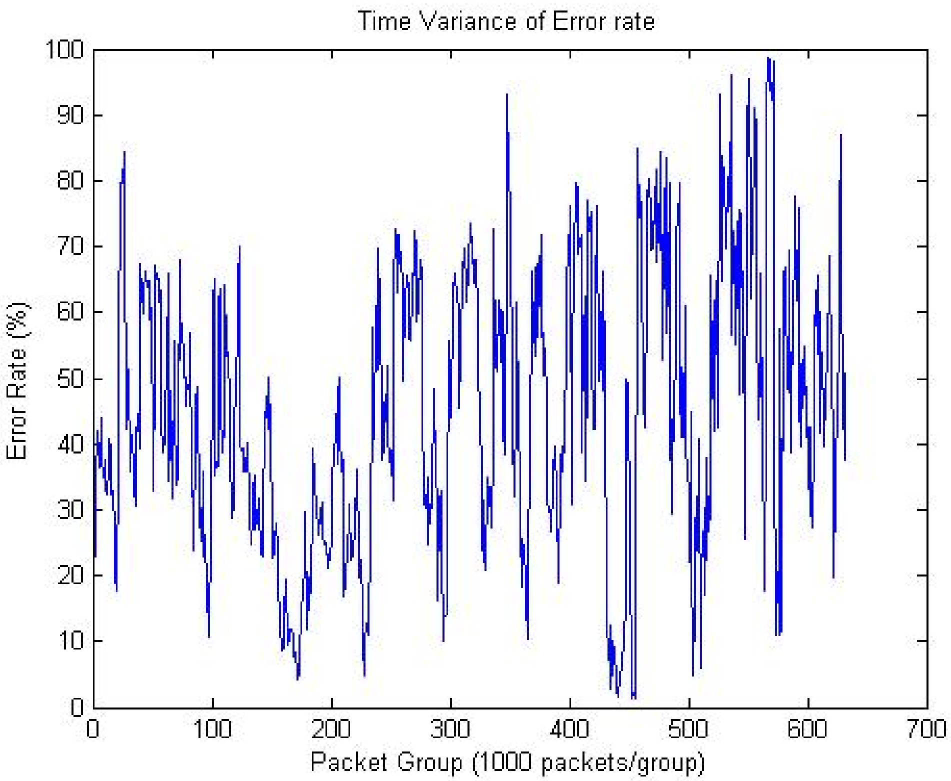


Figure 31 The temporal variation of PERs

Conclusion

From the four different categories 38% of data shows a high degree of variation of PER, while 16% shows a moderate change, 45% indicates no variation however does demonstrate random peaks where the error rates do alter on average for a 2-minute period, finally less than 1% shows no change. Therefore, based on the collected data, the PER, just as signal strength, **can alter randomly for no apparent reason and at any given time**, and with less than a single percent of collected samples where error rates do remain stationary, the main consensus is that PERs do indeed vary over time at a stationary location. The majority of this variance only occurs at instantaneous peak alterations for a minute amount of time. These peak alterations are most likely due to interference and not noise within the physical environment, such as altering the wireless path causing multipath interference for example when the door is opened or due to the attenuation of the user when they check on the operability of the laptop.

8.2.3 Relationship between Signal Strength and PERs (The Markov Model)

As previously indicated, figure 27 shows a typical set of results where an exponential relationship between the packet **error** burst size and the frequency of each error burst. Plotting the **received** packet burst frequency (figure 32), a similar exponential relationship is also established. If an exponential were to be fitted to both the errored and received packet data, this exponential curve would summarise the magnitude of packet bursts and indicate the decay of packet bursts.

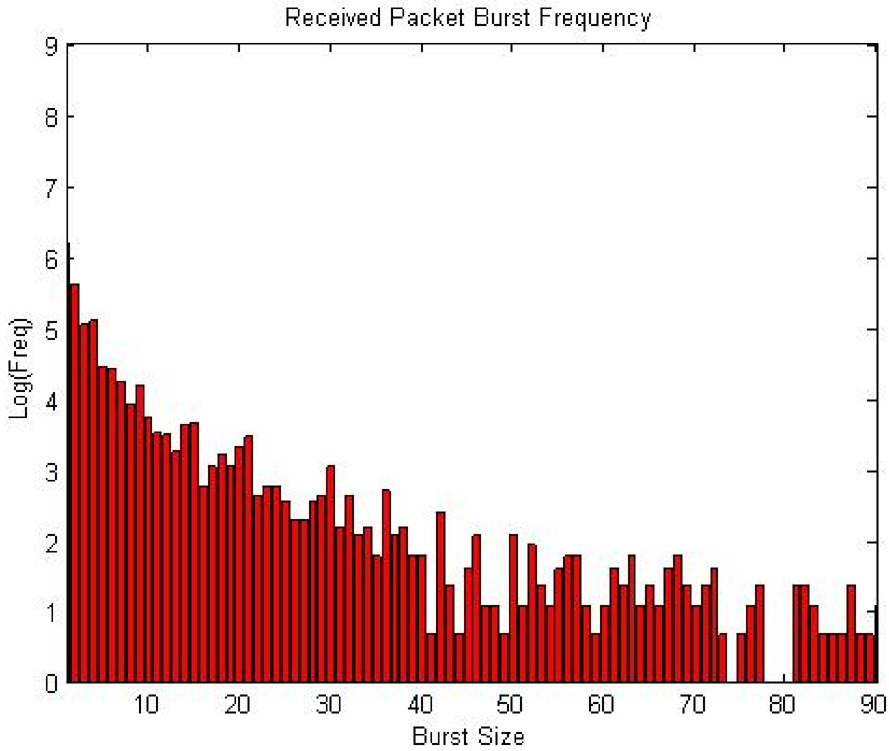


Figure 32 A typical sample of Received Packet Bust Frequency.

A simple relationship has already been found where the PER is a linear function of signal strength (8.1.1) and thus different signal strengths will produce different PER, and so the hypothesis being that different exponentials potentially exist for different signal strengths. The method to test this hypothesis is the mean signal strength was calculated then rounded to the nearest dBm for all experiment 4 data that remained constant over the collection process. The experiment 4 data within the packets file was then combined for all samples that had identical rounded mean signal strength values. The exponentials for the burst size of both packet loss and packets received was calculated along with a 95% CI. Once the exponentials were calculated, they can be used to determine the approximate burst size within each state when using a two-state Markov model, where each state corresponds to a successful or errored packet. The exponential curve used to fit the data is of the form:

$$a\,e^{-bx}$$

where a indicates the y-intercept and thus the frequency of a single packet loss or single packet received, whereas b indicates the rate of decay, where values closer to 0 represent a slower decay, and it is this b value that identifies the potential size of packet bursts based on the burst length (the x value).

A two-state Markov model for all combined data was then calculated, where the four transitional probabilities (0 -> 0, 0->1, 1->0 and 1->1) and the two equilibrium probabilities for the two states (bad and good) were determined based on the method described within Chapter 4. The results are given in table 17.

Starting with the exponential curve in the **bad state**, the value of *a* shows as the signal strength increases, single bursts (y-intercept) increases, this is an indication the start of packet bursts will be more frequent. Combining this with the *b* value, which starts close to 0 and decreases as the signal strength increases, thus indicating **faster decay**, and thus overall indicating a high probability of **shorter bad bursts as the signal strength increases,** which is a significant finding.

For the **good state,** the trends are a lot less subtle, but trends do exist. Taking firstly the values of *a,* which decrease with **increasing signal strength,** thus indicating that **shorter single received bursts will have a low probability**. The *b* value (although subtle) increases towards 0 with increasing RSSI, thus indicating **the received burst length and frequency increases as the signal strength increases.** Both the *a* and *b* results makes logical sense, as longer burst lengths are wanted when receiving packets and thus minimal single packets are wanted. The transitional probabilities did not show any obvious trends, thus a further indication that the transitional probabilities cannot be used in isolation to determine the relation between signal strength and PER.

The **equilibrium probabilities, further confirmed the results of the exponential distributed findings**. As the signal strength increases the probability of existing within the bad state decreases, and conversely for the good state, as the strength increases the probability being within the good state also increase. Again, this is a significant finding and based on collected data.

Signal Strength with a distribution of packet length with Markov transitional Probabilities and Equilibrium Probabilities

RSSI	Exponential in the form a*exp (b*x) with 95% CI		Transitional Probabilities				Equilibrium probabilities	
	Bad (0)	**Good (1)**	**0 -> 0**	**0 > 1**	**1 -> 0**	**1 -> 1**	**Bad (0)**	**Good (1)**
187	a = 6.544 (6.064, 7.023) b = -0.0644(-0.0709, -0.0579)	a = 5.145 (4.832, 5.459) b = -0.02455(-0.0268, -0.022)	0.7897	0.2074	0.0056	0.9945	0.0259	0.9741
190	a = 7.327 (6.82, 7.833) b = -0.0417 (-0.0454, -0.0379)	a = 7.746 (7.638, 7.854) b = -0.00658(-0.0069,-0.0062)	0.4120	0.5857	0.0191	0.9810	0.0315	0.9685
196	a = 8.55 (7.48, 9.62) b = -0.0894 (-0.1032, -0.0755)	a = 7.129 (6.954, 7.304) b = -0.01059(-0.012, -0.0099)	0.4014	0.5796	0.0121	0.9883	0.0198	0.9802
197	N/A	a = 10.23 (8.7, 11.76) b = -0.4776 (-0.556, -0.3994)	0.2397	0.7603	0.0003	0.9997	0.0004	0.9996
199	a = 8.894 (7.746, 10.04) b = -0.1354 (-0.1556, -0.1152)	a = 5.536 (5.321, 5.752) b = -0.0046(-0.0054, -0.0038)	0.2807	0.7074	0.0094	0.9908	0.0129	0.9871
200	a = 11.85 (10.49, 13.22) b = -0.4603 (-0.5189, -0.4016)	a = 1.369 (0.8569, 1.88) b =0.00092(-0.00615, 0.0079)	0.30529	0.69326	0.001555	0.99845	0.00223	0.9978
205	a = 7.098 (6.622, 7.573) b = -0.07286 (-0.0795, -0.067)	a = 5.491 (5.049, 5.933) b = -0.0323(-0.0360, -0.0285)	0.73050	0.25009	0.003152	0.99708	0.01156	0.9884
208	a = 11.07 (9.57, 12.58) b = -0.5347 (-0.6116, -0.4578)	*a = 1.011 (0.6548, 1.367)* *-b = -0.0179 (-0.0289, -0.007)*	0.19362	0.80637	0.001032	0.99897	0.00128	0.9987
215	a = 14 (12.13, 15.86) b = -0.6071 (-0.6893, -0.5249)	*a = 0.3422 (0.1338, 0.5505)* *-b = 0.0019 (-0.0093, 0.01324)*	0.09219	0.90781	0.001225	0.99877	0.00135	0.9987

Table 17 Signal Strength with packet loss analysis

N/A = Not enough samples to create a curve that accurately models the data. *Italicized text* = Not an ideal exponential fit, however data still showed a rough exponential trend.

8.2.4 Summary

- From the collected data, signal strength over a prolonged period is categorised by either no variation (22%), variation occurring in discrete phases (35%), intermediary and subtle changes (33) or no trend is evident (10%).
- Each measurement point within the dwelling collected data for a 30-second period. The resulting signal strength has accuracy to within ± 2dBm.
- Over an extended collection phase, the PER either shows no variation at all (1%), no variation, however includes some random peaks (45%), slight variations in PER (16%) and the variation in PER is obvious (38%).
- Signal strength and PERs can alter randomly for no apparent reason and at any given time.
- As the burst size increases the frequency decreases producing an exponentially distributed function.
- The exponential distributed curves resulted in conclusive data that indicated as the signal strength increases the probability of shorter bursts in error decreases. While for successful packets, as the signal strength increases the probability of higher bursts size was evident.
- The equilibrium probabilities also confirmed the findings of the exponential distribution. As the signal strength increases the probability of existing within the bad state decreases, and conversely for the good state, as the strength increases the probability being within the good state increase.

9. Other Experiments

A number of other individual experiments were performed; these experiments can be separated into two categories:

1) An alteration of a number of static characteristics within the wireless project that may contribute to the high variability of received data.
2) General experiments aimed at testing the transmission characteristics of WLANs.

All experiments were performed at least twice for a 30-second interval so a comparison of the results can be made. In both instances, the range, mean and standard deviation of the signal strength are determined.

Note: - All experiments performed during Session 1, were performed in vacant rooms on Level 2 of the Electrical Engineering building on UNSW campus.

- Only a small set of data was collected, therefore making it difficult to generalise results.

9.1 Category one

For the first category of experiments, a venue was sort that contained the minimal set of properties that affect wireless propagation, and so was effectively a free space like environment. After thoroughly exploring all local parks, the best location was the local soccer field. Performing experiments in this free space like environment ensures that the signal strength is guaranteed to be caused explicitly by the fundamentals of wireless propagation and not altered by any physical environmental properties. Because of the open space environment all experiments were performed in direct LOS between the router and the receiving station.

In the 4363 experiment an attempt was made to control as many variables as possible. However, some variables may have been inadvertently altered by the end user, which could potentially contribute to the large **cloud of data that was recorded,** (discussed previously however an example is shown again in figure 33, where a large range in signal strength exists for all distance). Hence an attempt is made to capture and record any potential variations that exist.

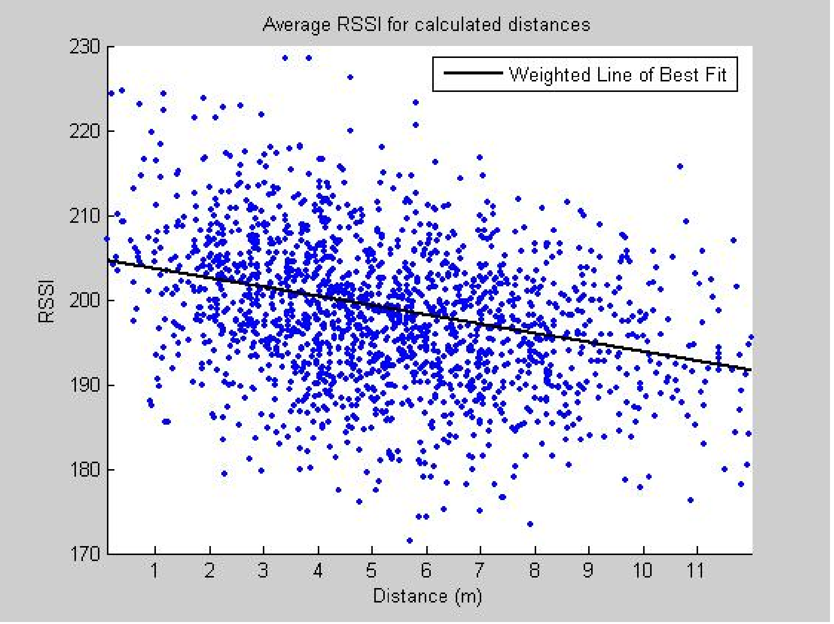


Figure 33 The blue cloud of data

- **Moving while Collecting Data**

When collecting data, small movements of the laptop can potentially modify the signal strength. This experiment attempts to determine if the signal strength is drastically altered by these small movements in the x, y and z direction. To try to simulate movement, a distance of 30 centimetres, which corresponds to a couple of wavelengths was used, to move the laptop back and forth at a constant velocity for the 30-second period. Since the experimental setup involved holding the laptop in the direct line of sight at a distance of 1 meter, moving the laptop the 30-centimeters will not likely alter the distance by a large amount, and thus not alter the signal strength, and therefore all variations are due to the laptops movements. Five sets of data were collected:

1) Placing the laptop on a solid object at waist height.
2) Holding the laptop stationary at waist height.
3) Moving the laptop slowly 'left and right' in the x direction.
4) Moving the laptop slowly 'up and down' in the y direction.
5) Moving the laptop slowly 'forward and backward' in the z direction.

The results of performing the experiment twice are given below:

Measurement	Mean			Standard Deviation		Range	
	First	Second	Average	First	Second	First	Second
1	217.53	219.99	218.76	1.36	1.33	5	5
2	216.40	214.79	215.595	1.34	1.9	6	8
3	210.45	218.06	214.255	2.88	1.98	7	7
4	214.06	216.06	215.06	2.05	2.25	6	4
5	217.34	214.98	216.16	2.21	3.01	5	7

Table 18 Comparison of Results when moving during data collection.

The results indicate that moving the laptop while collecting data **does alter the signal strength**. This is demonstrated when comparing all measurement points with the first, which was placed on a stationary object for data collection. Even **unintentional movements** of the laptop (set two) show an alteration in signal strength by an average of **3.165dBm,** when compared to the stationary object. **This difference is significant** as all experimental data was collected while students where holding the laptop**,** and therefore if students placed the laptop on a rock solid object, the wireless device would be completely stationary, and based on the collected data an elevation on average of about 3.165dBm **could potentially** result. However, since this experiment was only performed a few times, the difference could be a result of background noise.

If the laptop was moved in any of the x, y or z plane, the RSSI is slightly affected, furthermore the standard deviation shows an even more prominent variance. The exact reason for this higher variance is somewhat of a mystery, a potential reason is due to the varying signal of the router, as the laptop moves to locations that have a better or worse signal strength, which causes a higher variance. It seems that the mean signal strength and standard deviation are affected during the data collection phase by movements and thus does contribute to the cloud of recorded data, however this contribution is **small at best**. This experiment demonstrates that any movements need to be kept to a minimum for an accurate representation of signal strength, however a larger sample is needed for a more conclusive outcome.

- **Omnidirectional**

The wireless routers used (and all wireless routers for that matter) are omnidirectional in nature and thus ideally are capable of transmitting in all direction. Thus, the amount of power sent in all directions should be the same, and therefore the RSSI should be the same. If the router was found to be lacking the omnidirectional trait, then the exact orientation of the router and laptop also needs to be incorporated when analysing any set of data.

The wireless router and laptop were placed at the same constant height, where the router was positioned in its usual operating mode, that is, the antennas were vertical and the front of the router was facing position 12, thus the distance of both antennas to position 12 is identical. The laptop for all measurements was placed facing the router at a radius of 2 meters at all the o’clock positions from 1 to 12, as shown in the diagram below:

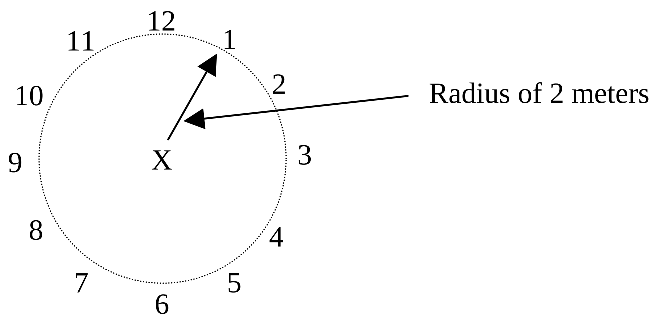


Figure 34 Omnidirectional testing at o’clock measurement points on the same plane

From the results (table 19), the variability of the mean, standard deviation and range between the first and second measurements for all positions are relatively similar, with an average variability of 0.998, 0.246 and 0.917 respectively. While the variability between the first and second measurements is small, the variability between the different o’clock positions is definitely more prominent, where the smallest signal strength was at 12 o’clock with 200.65 and the highest at 5 o'clock with 208.8. The 12 and 6 o'clock positions are the samples that are essentially outliers with the highest standard deviation and the highest range, which is interesting because these samples are directly in front and behind the router. One explanation of the variance is the lack of antenna diversity, as both of these positions have the exact same length to both antennas on the wireless router, whereas all other positions have varying length. This varying length allows the router to choose the best signal from one of the two antennas, and thus because of this varying length the results indicate that antenna diversity does improve the signal strength, where the small separation of the antenna's on the router (roughly a single wavelength), causes the router to distinguish between different signal strengths and choose the most ideal.

When incorporating all positions, the variability between all o'clock positions shows that the signal strength changes **at an average of approximately 2.5dBm**. This indicates that the omnidirectional nature of the wireless router shows a substantial unevenness at equidistant radii from the router, which could also be a cause of the large range of data samples present. This 2.5dBm could be considered **small** as even the difference between the first and second measurements have a variability of **0.998dBm.**

Position (o'clock)	**Mean**			**Standard Deviation**		**Range**	
	First	**Second**	**Average**	**First**	**Second**	**First**	**Second**
12	202.92	200.65	201.785	1.91	2.07	6	7
1	205.33	204.13	204.73	0.49	0.92	1	2
2	207.53	209.13	208.33	0.52	0.92	1	3
3	204.13	204.13	204.13	0.64	0.74	2	2
4	206.67	207.07	206.87	0.49	0.46	1	2
5	208.8	207.87	208.335	0.56	0.64	2	2
6	205.66	204.8	205.23	1.05	1.68	4	5
7	207.67	206.3	206.985	0.62	0.72	2	3
8	204.9	205.6	205.25	0.65	0.85	3	2
9	205.4	206.5	205.95	0.85	0.54	2	1
10	208.1	206.9	207.5	0.71	0.50	3	2
11	205.3	206.8	206.05	0.56	0.86	2	1

Table 19 Comparison of signal strength at the corresponding o'clock positions at a 2 meter radii

The above experiment was conducted on the same plane as the router, and thus different heights were not considered. To simulate this, the router was then turned 90 degrees, and an experiment, which emulated upstairs and downstairs could be used. Four measurements points were chosen, two upstairs (1 and 2) and two downstairs (3 and 4), shown in figure 35, where each measurement point (1, 2, 3 and 4) is equidistance from the router. This again would test if the router does emit in an omnidirectional manner as in the following figure:

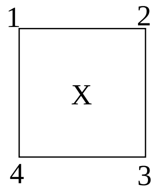


Figure 35 Measurement points where 1, 2 emulate upstairs and 3, 4 downstairs.

The results are given in table 20:

Position	**Mean**			**Standard Deviation**		**Range**	
	First	**Second**	**Average**	**First**	**Second**	**First**	**Second**
1	203.1	204.2	203.65	0.75	0.85	2	3
2	202.2	204.3	203.25	0.74	0.69	4	3
3	203.5	202.3	202.9	0.68	0.76	2	3
4	202.1	203.4	202.75	0.75	0.46	2	1

Table 20 Comparison of signal strength positions at a 2-meter radii simulating height

From the simulated results, upstairs shows a slightly higher signal strength compared to downstairs, only by an average 0.625dBm, which is insignificant. Thus based on the collected results, the simulation of upstairs and downstairs gives extremely similar results, and thus the omnidirectional nature at different height can be assumed.

- **Human body**

The amount of people within a wireless dwelling during the experiment was found to have no impact on the RSSI and PER (see relevant section in 8.1.5). A question still remains, does the human body attenuate signal strength. Eckhardt, and Steenkiste, [14], performed a similar experiment where the human body did attenuate signal strength, thus the current experiment aims to validate this. The router and laptop were placed at the same height (1 meter) and separated by 1.5 meters. Two sets of data was then collected, one implementing a direct line of sight between the router and laptop, the other impaired by a person directly in front of the laptop. The results are given in the table below:

	Direct Line of Sight			Impaired		
	First	Second	Average	First	Second	Average
Mean	213.4	214.79	214.095	207.53	208.13	207.83
Standard Deviation	1.24	1.39	1.315	1.51	1.46	1.485
Range	4	5	4.5	5	5	5

Table 21 Comparison of signal strength when impaired by human body

The results indicate that a difference of approximately 6dBm between the impaired and direct line of sight is apparent, the amount of spread of the signal strength is slightly higher when the body is inserted directly into line of sight. From these results placing the human body between the direct of line sight of the router and laptop produces an **attenuation factor of 6dBm.** Thus, if the person was impairing the signal during the data collection phase then a difference of 6dBm is expected. This result is significant as if students complied with the experimental instructions, then the human body should not be attenuating the signal strength, however, no method of determining if students followed these instructions is possible. **Thus, if students did not follow instructions, a 6dBm variance within the cloud of data can be contributed to the attenuation due to the human body.**

- **Door**

Most students when performing the experiments were not the only inhabitants of their dwellings, and so people moving about while the experiment is being carried out is nevitable. Thus, the potential for doors to be left open is a possibility, and could be a contribution to the variability of results. This experiment tests the effect of an average household door on signal strength.

An average household single door has dimensions 0.71m (W) x 2.5m (H) x 3.5 cm (D), and made from hollow wood. This door was tested multiple times both open and closed at a symmetric distance of 0.5 meter from the door; the results are given below:

	Door Open			Door Closed		
	First	Second	Average	First	Second	Average
Mean	210.66	209.99	210.325	209.56	207.97	208.765
Standard Deviation	1.59	1.6	1.95	1.23	0.8	1.015
Range	3	5	4	4	3	3.5

Table 22 Comparison of signal strength when door is open and closed

From these results, when the door is opened the mean is slightly higher showing a 1.5dBm increase, and the standard deviation is also a bit elevated, showing on average a 0.94 increase. From this simple experiment using the best possible location for the router and laptop, **a slight increase in both the mean and standard deviation are observed**, but not a drastic alteration. However, one student performed a similar experiment across the entire dwelling incorporating 40 measurement points, and compared the results to when all doors where opened and closed. They found an extremely similar mean, with a 0.367 difference along with a slight increase in the standard deviation, at 0.322. It is unknown the exact number of signals that essentially passed directly through the opened or closed doors. Since these numbers are extremely close, no real conclusion can be given. Based on the collected experimental data, when the signal passed directly through opened and closed doors, a potential valid conclusion is that doors **do affect signal strength**, though the relative differences are relatively **small**. For a consistent measurement framework, all doors should be consistently opened or closed.

Note: This experiment was done within a dwelling

- **Antenna Orientation**

The orientation of the router's antenna for the experiment was to be vertical. However, if students did not place them in their vertical nature, does an alteration in signal strength arise? The aim of this experiment attempts to determine if any alteration occurs based on a fixed location.

For all experiments, the setup is as follows: the router and laptop were placed in front of each other and in direct line of sight, at a height of one meter, and 1 meter apart. The orientation of the 2 antennas would be altered simultaneously, where data would be collected for 10 minutes in each different orientation. Three orientation experiments were performed:

Orientation One

The angle used for the first experiment is shown in figure 36, where a photograph was taken using an orthogonal side view (showing an angle of 90 degrees). No angles less than 90 degrees need to be tested as the router does not allow for such angles to occur, that is, the antenna's could only be moved for angles greater than 90 degrees. The results are given in table 23:

Antenna Orientation (Degrees)	Mean	Standard Deviation	Range
90	212.68	1.33	5
120	210.54	1.94	6
150	207.94	2.89	10
180	210.8	1.54	7

Table 23 Experiment One: Angle Orientation with mean, standard deviation and range

Orientation of the
router's antenna

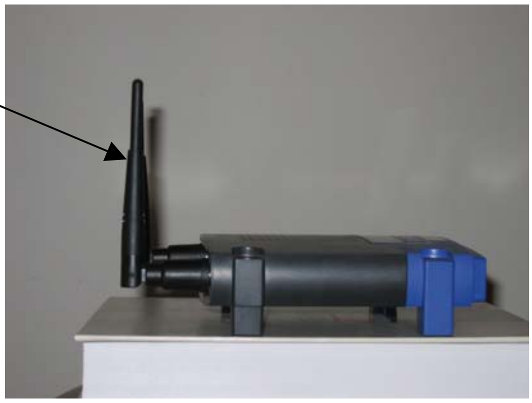


Figure 36 The orientation of the antenna from a side view indicating the angle used.
Where 90 degrees indicates that the antenna's are vertical, and 180 degrees that they in line with the router

From the above table the first three orientations indicates a trend, where, as the angle increases the mean, standard deviation and range also produce an increase of just over 2dB. The final angle however, opposes this trend. Moreover, this experiment indicates that altering the angle in a single direction does alter the signal strength.

Orientation Two

Looking at the router from the orthogonal front view (figure 37), the two antennas can be moved either left or right. This experiment alters the orientation of both antennas simultaneously in the same direction. Results are given in table 24.

Figure 37 The orientation of the antenna from a front view showing the 110-degree angle used.
Where 90 degrees indicates that the antenna's are vertical.

From the symmetric movements of the antennas, the mean signal strength, standard deviation and range all indeed change. This change is most evident when the orientation is both parallel with the router (0 and 180 degrees), which has the highest mean signal strength at 215.76 and 217.14 respectively compared to the norm 212.68. The 45 and 135 degree orientation, show an extremely similar mean (209.87 and 209.47), however, have a vastly different range, and a slight difference in standard deviation. In conclusion extreme changes in symmetric antenna orientation does show a drastic alteration in all calculated statistical characteristics, although these positions during data collection are extremely unlikely, even at 45 and 90 degrees signal strength was altered.

Antenna Orientation (Degrees)	Mean	Standard Deviation	Range
0	215.76	2.86	12
45	209.87	1.32	8
90	212.68	1.33	5
135	209.47	2.71	16
180	217.14	2.66	13

Table 24 Experiment Two: Angle Orientation with mean, standard deviation and range

Orientation Three

Looking at the router from the orthogonal front view (figure 38), the two antennas can be moved either left or right. The third experiment alters the orientation of both antennas to produce different angles with the router. Results are given in table 25.

Figure 38 The orientation of the antenna from a front view showing antenna 1 at 110 and antenna 2 at 90 degrees

Table 25 Experiment Three: Angle Orientation with mean, standard deviation and range

Antenna Orientation Antenna 1, Antenna 2 (Degrees)	Mean	Standard Deviation	Range
90,90	212.68	1.33	5
85,95	212.62	2.43	10
95,85	211.35	2.39	14
135,45	214.69	1.81	9
45,135	213.04	2.96	15

The results indicate that signal strength does alter, but the results are only small.

The intention of this experiment is to determine: if altering the antennas from its vertical position, in any direction, when collecting data from a single location, will affect the signal strength. From the three different experimental orientations, each indicates that an **alteration in mean signal strength occurs. This alteration varies based on the angles of the antennas**, **where an increase and a decrease in signal strength has been observed.**

Ultimately, the exact orientation of the antennas will intimidate the signal strength in different ways, sometimes the signal strength does not change, other times it can change drastically. The signal strength will also be different depending on the exact location relative to the antenna’s position, thus for the antenna’s to remain within the experiment as a constant variable, they need to remain vertical.

- **Humidity**

Within section 8.1.6, humidity was found to have no effect on the signal strength. However, in this experiment a more direct approach will be taken, where severe humidity will be introduced. The router and laptop were placed one meter apart where a plastic sheet was placed over the electronic equipment to cover from any accidental water leakage. Water was then sprayed between the two communicating bodies, where the results with water and without water can be compared. The experiment was run twice over a 1-minute period.

	No Water			**Water**		
	First	**Second**	**Average**	**First**	**Second**	**Average**
Mean	213.6	214.27	213.935	211.4	211.73	211.565
Standard Deviation	0.63	0.59	0.61	1.24	1.53	1.385
Range	2	2	2	3	5	4

Table 26 Difference in results when water was introduced between the two communication bodies

The differences in statistics indicate when water was introduced the mean signal strength difference was **2.37dBm lower**. The standard deviation and range are also slightly higher, at a difference of 0.775 and 2 respectively. Thus, from the collected data, severe humidity, that is physically inducing water between the laptop and router does have an impact at a separation distance of 1 meter by 2.37dBm.

The impact on humidity was also tested within the 4363 experiment (section 8.1.6); the results indicate that humidity was not affected. The most likely reason for the discrepancy, is because of the differences in the exact experimental procedure, namely, directly introducing humidity between the sender and receiver does have an impact. This impact on signal strength is not constant, and would alter according to distance. For example, assuming constant humidity at a distance of 10 meters, an extreme approximation based on the data collected is a signal strength difference of 23.7dBm (as 2.37dBm for a single meter). This is definitely severe, and according to [31], the attenuation of 0.01dB/km at 55mm/h to approximately 0.02 dB/km at 150mm/h is the norm. Thus completely different to the experimental results obtained, further indicating that more data needs to be collected for a better conclusion.

Throughout the 4363 experiment, the humidity would obviously change, and thus based on the above experiment severe humidity does influence the signal strength. However, severe humidity was not directly introduced during the data collection process, furthermore according to [31] the results will be insignificant and thus the effects of humidity as concluded in section 8.1.6 would not be a factor in the cloud of collected data.

9.1.1 Summary

During the collection of data in the 4363 experiment, an attempt was made to control as many variables as possible. The end user may have inadvertently altered some variables. The large range in many of the produced graphs could manifest this alteration. An attempt was made to explain the existence of the large variance in the collected data by performing experiments and analysing the resulting changes in signal strength. It was found that:

- Physical movements of the laptop during the collection process did alter the mean signal strength however its contribution is small at best.
- The omnidirectional nature of the router was tested and a substantial unevenness at equidistant radii from the router was found, where on average a 2.5dBm difference between all measurement points were found.
- The human body has an attenuation factor of 6dBm.
- The variability due to doors being left opened or closed was tested, where a difference was found, however this difference was extremely small.
- Depending on the orientation of the antennas, an increase and a decrease in signal strength has been observed, and in one instance a variance of over 4.4dBm was found.
- Experimental data concluded that severe humidity lowers signal strength by 2.37dBm per meter. Other evidence indicates humidity is insignificant

9.2 Category Two

The second category of experiments were general in nature and performed to test the transmission characteristics of WLANs.

- **Signal Strength and Transmission Rate**

The project was conducted at a single transmission rate (54Mbps), where the assumption was that **signal strength would not change for different transmission rates**. This is important because if an alteration does not , then the results within this thesis can then be generalised for other transmission rates. Thus, the question is does altering the transmission rate affect the signal strength?

Initial experiments were performed during Session 1; the results indicated that lower transmission rates had slightly higher signal strengths. However, the experiment was repeated in a 'free space' like environment for different transmission rates at different distances. Each distance was only calculated once; the results are given in table 27, and the mean signal strengths are graphed in figure 39:

Distance (meters)	Mean				Standard Deviation				Range			
	54	36	18	6	54	36	18	6	54	36	18	6
0.2	227.4	227.53	228.06	228	0.91	1.13	1.58	1	3	4	5	3
1	212.32	214.13	214.46	214.73	2.87	0.74	1.46	0.96	8	2	5	3
2.5	201.26	201.73	202.86	204.2	1.1	0.7	1.36	1.01	4	2	5	3
4	194.93	196.67	196.47	197.4	1.28	0.72	0.83	0.74	4	3	3	3.
5.5	192	191.13	194.32	195.53	1.20	1.41	1.13	1.41	3	4	6	5
7	188.09	187	191.26	188.39	1.04	0.93	2.12	1.76	3	4	4	6
8.5	189.49	187.93	185.32	186.06	1.65	1.33	2.26	1.91	5	5	7	6
10	186.75	185.6	184.26	183.19	0.71	0.83	1.87	1.61	2	3	5	5

Table 27 Mean, standard deviation and range for four different transmission rates

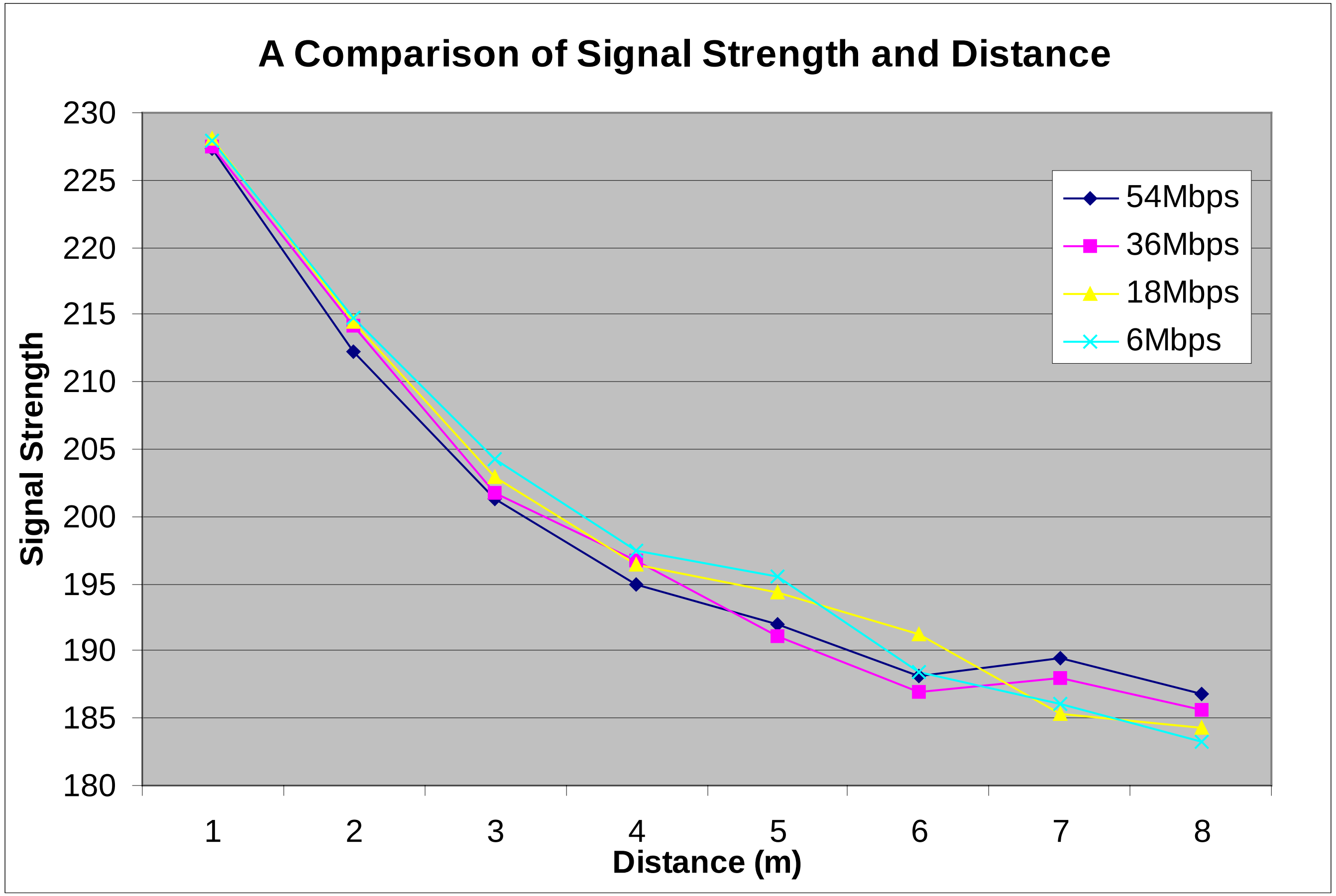


Figure 39 Comparison of RSSI and Distance for four different transmission rates.

Only the number of **received packets** is used to calculate the signal strength. However, if packets are being lost then signal strength alone is not a clear indicator for comparing the different transmission rates. Thus, the PER needs to be investigated. However, upon examining the loss rates, no lost packets were found at the highest distances for all transmission rates. Thus, from the data collected, the signal strength is an accurate representation of the received packets and is the only characteristic that needs to be considered.

From the graphed data, points less than 4 meters show a trend, that the higher transmission rates have slightly lower signal strength. This difference is extremely small, at approximately 1dBm. According to the omnidirectional experiment, each sample at a particular distance can vary by up to 1dBm at a constant transmission rate, indicating the trends less than 4 meters is effectively inert. On the other hand, data points greater than 4 meters do not indicate any trends. Thus, the general conclusion is that at different transmission rates the signal strength is extremely similar, and therefore any significant conclusions within this thesis can be generalized to other transmission rates.

What is also evident from all transmission rates is the exponential trend, which is substantially different to the calculated linear weighted curve that was produced based on the analysed data (8.1.1). The difference in results could be because:

1) This experiment was done within a free space environment and thus contained the minimal set of properties that would affect wireless propagation.
2) Due to the large cloud of data that existed within the analysed set of data, an exponential curve could exist, but is masked by the variability in collected data.

- **Symmetry test and height**

  Transmission characteristics need not be symmetrical, so it is possible that the wireless router can hear the laptop but the laptop not hear the wireless router, or vice versa. Many reasons for this occur including:

  1) Signals may not traverse the same path from sender to receiver and back, and so factors within the environment can affect the wireless propagation of the signals.
  2) 802.11 MAC layer (2.2.2) includes its own acknowledgement and retransmission feature. Thus, the network layer does not perceive a frame as successfully delivered unless symmetric reception is possible. [15]
  3) The different use of antenna diversity in different equipment, e.g. a wireless router may have antennas that are further separated than is possible on a card bus NIC and so provide better choice of signal strength based on the signal from each of the multiple antennas.

This experiment was done within a dwelling, where the direct path between the laptop and AP was 2.5 meters and the signal passed through two walls and through varying in-house furniture. The router was placed in one room, and the laptop in the other. Once the collection of data was completed in one location (position one), the wireless devices were then swapped (position two), and the symmetry of the collection process could then be compared.

The above process was completed twice for two different heights: on the floor and at a height of 1 meter. This was to determine if the difference in height alters signal strength.

	Mean			Standard Deviation		Range	
	First	Second	Average	First	Second	First	Second
Floor - position one	199.79	201.49	200.64	2.21	2.54	7	6
Floor - position two	204.25	201.73	202.99	1.12	2.34	9	5
Height - position one	206.16	208.26	207.21	1.28	1.39	5	4
Height - position two	213.54	212.67	213.105	2.76	2.25	3	9

Table 28 Comparison of symmetry (position one and two) at different heights

This simple symmetry experiment shows that when both the laptop and router were placed on the floor, the signal strength varied on average with a 2.35dBm difference. Using this experiment in isolation, it in would seem that symmetry might exist. Upon altering the heights to 1-meter however, showed a completely different tale (potentially due to sheer luck), where the average signal difference turned out to be 5.895dB. This difference is indeed significant, and thus, a situation exists in which symmetry fails, and thus **symmetry cannot be assumed** in any wireless devices or in the creation of wireless protocols. This finding is inline with that of [15] where experiments were performed in a ‘free space’ like environment, for a variety of distances up to 250 meters.

Comparing the different heights shows **that height also plays a significant role** in optimising wireless coverage. The improved signal strength, regardless of laptop and router location was always higher when the router and laptop were at greater heights. This is most likely due to the fewer obstacles that the wireless signal must pass through, therefore resulting in less attenuation of the signal. So ultimately, height **does** need to be considered when placing the router within a dwelling.

- **Microwave**

Many sources of interference exist for WLANs operating in the popular unlicensed 2.4 GHz spectrum. The unlicensed nature of this band implies frequency overlap and thus the possibility of adversely affecting packet loss, increasing packet errors and the direct influence of the signal strength on receivers is a genuine threat to WLANs. One such appliance within the home is the microwave. Thus, this experiment aims to determine if microwave ovens affects the transmission characteristics of wireless networks in a home environment.

The microwave tested operates (according to the user manual) at 2445 MHz, which is between channel seven and channel eight. The WLAN was set to operate at channel six, which equates to a moderate level of interference. The microwave was situated within the kitchen, and was moved to the center of the room, and was set to operate in its standard operating mode while I collected data at the measurement points for the majority of surrounding and adjacent rooms. The experiment was done with the microwave running and then with the microwave off at the same measurement points so a comparison can be done.

Once the first set of data was collected, which was directly in front of the microwave, it was evident that microwaves have a direct impact on transmission characteristics due to the large amount of packets that were being lost despite the apparent use of shielding within the microwave. Once the data was collected it was evident **that the microwaves did cause packet loss**, where the packet loss was bursty in nature.

For the room that contained the operational microwave, a **burst of 4-6 packets** was evident; this was then followed on average by a burst of 13 lost packets. The distance and burstiness for each measurement points is displayed in table 29 where a ‘Yes’ indicates that the packet loss is bursty, a ‘No’ indicates that the results were similar to when the microwave was turned off and a maybe indicates that the comparison between results were somewhat different, but not entirely bursty.

Rooms	**2**	**5**	**7**	**10**	**0**
Office	2.5	5.1	5.3	3	3.5
Kitchen	2	3	3	2	0
Living	8	4.3	2.2	7.3	5.3
Living	4.1	6.3	5.5	3.5	3.5
Rooms	**2**	**5**	**7**	**10**	**0**
Office	Maybe	Yes	No	No	No
Kitchen	Yes	Yes	Yes	Yes	Yes
Living	Yes	Yes	Yes	Maybe	Maybe
Living	No	Maybe	Maybe	No	No

Table 29 Measurement points indicating distance and the possibility of burstiness

The most important aspect for WLANs is the physical loss range due to the microwave. If a comparison between the possibility of burstiness and distance is made, then **burstiness is affected up to approximately 5 meters**. After this, the interference from the microwave becomes imperceptible and the ‘normal’ wireless characteristics and environmental factors become dominant. One aspect of this experimental data that is interesting is the signal strength values are higher when the microwave is turned on. An example is given of the in table 30.

Rooms	2	5	7	10	0
Microwave on	-53.6667	-46.2727	-33	-50	-46
Microwave off	-56.1667	-59.3333	-54.8667	-58	-59

Table 30 Comparison of RSSI values in dB

When the microwave was turned on, it was in close proximity to wireless receiver (the laptop), thus the microwave signal was stronger that the wireless router. The wireless card records this increase in signal strength, however this signal is the incorrect signal, which ultimately causes interference, and thus a loss of packets is the outcome.

The question now is, how can users combat microwave interference? The obvious solution is to avoid using wireless networks in close proximity to a microwave, even though the actual impact will be temporary, as microwaves are generally operational for a few minutes at a time. If working near a microwave is unavoidable, then the first solution is to enable “microwave oven robustness” on your wireless card (if supported). This ensures that the loss of packets will be sustained over a longer period of time before a reduction in speed occurs. Another option is to alter the wireless channel of the wireless network to one that is at least 22 MHz away from the operating frequency of the microwave oven.

9.2.1 Summary

- At different transmission rates the signal strength is extremely similar and thus the results within this thesis can be generalised to all transmission speeds.
- The symmetry of wireless devices should not be assumed, as symmetry does not exist.
- Height plays a significant role in signal strength variability.
- Based on the results of a single microwave, when turned on, the microwave induces packet loss in bursts, where wireless receivers up to approximately 5 meters were affected.

10. Conclusions including Future Work and Improvements

This thesis presents the extraction and collation of a large collected data set at the packet level within IEEE 802.11g wireless LANs using C and MATLAB. Based on my experience performing these tasks, much of the collected data had small discrepancies within. To make the task of programming easier for any future work, a potential solution when uploading the collected data might be to incorporate an error checking facility. An example of some major tests could be to check if coordinates are correct and/or to check if the spreadsheet contained a router.

The analysis of the collated data involves the study of signal strength and loss patterns. Here I will merely provide a brief summary of the conclusions found, and if further analysis is wanted, please see the relevant section within this thesis. The overall analyses can be divided into three separate but interrelated phases:

1) Static experiments.
2) Temporal variation of signal strength and PER.
3) Causes of variability in data collection with the analyses of general transmission characteristics.

Based on the signal strength and PER graphs, the signal strength has greater effect in establishing the PER than the physical distance from the router. However, the signal strength, PER and distance all interrelate and have a direct impact and influence on each other. Nevertheless, the results indicate that signal strength is of primary important, and distance comes secondary when determining packet loss.

Signal strength may be a good indicator in determining the optimum location of wireless media. However, the temporal variation of the signal strength at a particular location must be considered. The main conclusion is that signal strength can vary at any given time and for no apparent reason. More importantly, the autocorrelation with a single lag shows a high degree of change, with the calculated value of 0.625. This indicates that even over a few seconds, the signal strength can show a high degree of variation. Since all collected data was collected for a 30-second period, it was determined that the data collected was accurate to within $\pm$ 2dBm. Observing the signal over prolonged periods revealed that if an accurate measurement is needed where all fluctuations are incorporated, then the data suggests the collection process take place over multiple hours. The packet loss also shows the same general trend where an alteration can occur randomly for no apparent reason and at any given time, were approximately half of the alterations in PER occur randomly with peak losses lasting a few minutes. Based on the data collected, the PER and signal strength both vary, with each having an approximate probability of a half that minimal alterations will occur.

The 4363 experiment procedure required a number of wireless and physical characteristics that needed to be constant. However, the data collected contains a high degree of variability. To explain this variability a number of experiments were performed. While most experiments did hint at small alterations in signal strength, where on average an approximate 5dBm could be attributed to students introducing inconsistent samples. The more probable reason of the high variability confirms previous findings that the signal strength alters randomly, then again, since the collection process was only for 30-second, the more likely reason is the amalgamation of samples from different physical environments.

Regardless of the variability of signal strength and PER, one important and fundamental finding is the exponential distribution of burst length for both lost and received packets. This exponential curve indicates three burst aspects: the magnitude, the decay and the length. When the signal strength increases, the probability of error bursts occurring decreases, and therefore, lower signal strength produces errors that are clustered together. The successfully received packets indicate that as the signal strength increases, the probability of larger bursts sizes was evident, and therefore higher bursts are associated with higher signal strength. This exponential distribution was incorporated into a two-state Markov model, and therefore the time spent within each state will be exponentially distributed. The produced transitional probabilities did not show any trends, however the produced equilibrium probabilities revealed a trend, which makes it the better candidate for determining the time spent within each state.

Although this thesis performed experiments at 54Mbps, it was found through experimentation that different transmission rates produce signal strengths that are extremely similar. It would be reasonable therefore that the results within this thesis can be generalised to all transmission speeds. It was also found that symmetry and height play an important role in wireless networks. Firstly, symmetry does not exist and should not be assumed when creating wireless protocols, and secondly, the higher from the ground a signal originates, the better the signal strength that results due to the reduction in objects that the signal traverses.

From the data collected other conclusion were:

- For room type:

  - The laundry and bathroom are statistically the worst rooms, likely due to the variable RF conditions.
  - The office, which is an important location for wireless media, was one of the worst rooms for wireless media, potentially caused by computers and other electrical devices that are associated within an office space.
  - The living room, statistically, proved to be the best room for wireless media.
- No conclusive results based on interference from other 802.11 wireless devices.
- Evidence indicates signal strength and PER are slightly lower when dwellings contain ducted air-conditioning.
- The number of people within a dwelling indicated no alteration in PER and RSSI, which is understandable considering the dimensions of an average human body.

10.1 Future work

Work that could be performed in the future include:

1) Writing further C programs that:
   - Determine the number of object and object type between each measurement point and router.
   - Find measurement points that pass through objects.
   - Incorporate the angle of incident that was calculated in the program forms.c and find the distance through walls
2) Writing further MATLAB programs that:
   - Determine the reduction in signal strength for different object types.
   - Determine if the signal strength passing through metallic objects is lower.
   - Calculate the attenuation factor for different objects such as wall types.
   - Draw a graph of signal strength vs. distance and PER vs. distance so a comparison can be made between different objects, for example, metallic objects, walls and even doors, to determine their affect.
   - Write a program that determines the exact amount of variation that exists within signal strength and find the duration of any mean periods that may exist (8.2.1.1). This can then be extended to include PER.
3) Additional experimentations to identifying further reasons for the variability in collected data.
4) Dualities of experimental results exist, one within experiment 2 (30-seconds) and experiment 4 (prolonged period). A comparison of these results could be done, and potentially use to find any correlations.

11. References

[1] Tan, T.K. Bing, Benny. *World Wide Wi-Fi. Technological Trends and Business Strategies* John Wiley & Sons, 2003, ch. 1, pp 20-15.

[2] *Wikipedia*. IEEE 802.11. (n.d.). Retrieved July 27, 2005, from Answers.com Web site URL: *http://www.answers.com/topic/ieee-802-11*.

[3] Hayken, S. *Communication System,* 4th Edition, 2000, pp 599 – 603

[4] Avaya *Wireless Based LANs Course,* Retrieved July 27, 2005, URL: *http://wireless.ictp.trieste.it/school_2002/lectures/ermanno/interference.ppt*

[5] Hanlen, L., Fu, M. *Multiple Antenna Wireless Communication Systems: Limits to Capacity Growth* IEEE Wireless Communications and Networking Conference, Orlando, 2002.

[6] Goldsmith, A., Jafar, S.A., Jindal, N., Vishwanath, S. *Capacity limits of MIMO channels* IEEE Vol 21, No 5, June 2003, pp 684 – 702

[7] Jensen, M.A., Wallace, J.W. *A review of antennas and propagation for MIMO wireless communications*. IEEE. Vol 52, No 11, Nov. 2004 , pp 2810 – 2824

[8] Haowei, B., and Mohammed A. *Error Modelling schemes for fading Channels in Wireless Communications: A survey* IEEE Vol 5, No. 2 2003, pp2-9.

[9] Moors, T. (2004) Tele4363 Lecture notes, Week 1 Lecture 3. URL: *http://uluru.ee.unsw.edu.au/~tim/courses/tele4363/lec/*

[10] KaryGiannis, T., Owens, L. (2002) "*Wireless Network Security 802.11, Bluetooth and Hand-Held devices.* National Institute of Standards and Technology, U.S Department of Commerce, November 2002. pp10-13

[11] Ohrtman, F., Roeder, K. *Wi-Fi Handbook – Building 802.11b Wireless Networks,* 2003 pp 214- 215.

[12] *Wikipedia*. Fresnel Zones Diagram Retrieved August 20, 2005, from Answers.com Web site URL: *http://en.wikipedia.org/wiki/Image:Fresnel.JPG*

[13] Fresnel Zones, Retrieved August 20, 2005, URL: *http://www.radiolan.com/cgi-bin/fresnel.cgi*

[14] Eckhardt, P., Steenkiste, P. *Measurement and Analysis of the Error Characteristics of an In-Building Wireless Network.* SIGCOMM August 1996 Standford, CA.

[15] Kotz, D., Newport, C., Gray, R., Liu, J., Yuan, Yougu. *Experimental evaluation of wireless simulation assumptions*. Dartmounth Computer Science Technical Report, 2004, pp 1-20.

[16] Haowei, B., and Mohammed A. *Error Modelling schemes for fading Channels in Wireless Communications: A survey* IEEE Vol 5, No. 2 2003 pp2 - 9.

[17] Gillbert. E.H. *Capacity of a Bursty-Noise Channel" Bell Systems, Technology Journal* Vol 39, No 10, 1960, pp1537 - 1548

[18] Elliot, E.O. *Estimates of Error Rates for Codes on Bursty Noise Channels* Bell Systems, Technology Journal Vol 42, No 9, 1977, pp1977 – 1997

[19] Zorzi, M., and Rao, R.R. *Lateness of Probability of a Retransmission Scheme for Error Control on a Two-State Markov Channel*. IEEE Vol 47, No. 10 Oct. 1999, pp 1537 - 1548

[20] Tang, c., and McKinley, P. *Modeling Multicast Packet Losses in Wireless LANs.* Session San Diego, 2003 pp 130 - 133

[21] Hayher, R., Syed, A. *Markov-based modelling of Wireless Local Area Networks*. ACM Mobicom International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), September 2003.

[22] Aguayo, D., Bicket, J., Biswas, S., Judd, G., Morris, R., Link-*level Measurements from an 802.11b Mesh Network* Carnegie Mellon University. M.I.T. Computer Science and Artificial Intelligence Laboratory 2004.

[23] Rabiner, L.R. *A tutorial on Hidden Markov Models and Selected Applications in Speech Recognition* IEEE Vol 77, No. 2, 2003 pp 257 - 286.

[24] Trenerry, D. *Information Codes and Ciphers Maths 3411*. 2005, pp57 – 59

[25] Hefazi, P., Wedge, D., Beach, M. A., Lawton, M. *Propagation Measurements of the 5.2 GHz Radio Band in Commercial and Domestic Environments*' HP Labs Technical Report July 1987.

[26] Arauz, J. *Markov Modelling of 802.11 Channels*. IEEE, 2003, pp 771 – 775

[27] Joshua Bardwell "You Believe You Understand What You Think I Said…" The Truth about 802.11 Signal and Noise Metrics 2004, pp 13-16

[28] Zhou, Z. G, CONNECTED - Mechanisms for Improving Wireless Connectivity in Mobile Computing Environments. UNSW, 2004 PHD Thesis, pp106 - 110

[29] Humidity, Retrieved September 2005, URL:*http://www.schneier.com/blog/archives/2005/08/wireless_interc.html*

[30] Humidity Retrieved September 2005, URL:F*http://wgntv.trb.com/news/weather/weblog/wgnweather/archives/001189.html*

[31] Australian Government, Australian Communication Authority. *60 GHz Band Millimetre Wave Technology*. December 2004, pp 11.

12. Appendix

Appendix 1 (Project Instructions)

Phase 1: Preparation

1.1 Select a dwelling

You should select a dwelling that has at least four rooms that you can access, and one that is secure for keeping the equipment for the duration of the Data Collection phase. The dwelling will likely be where you live, but that is not necessary, and you should try to ensure that the dwelling is different from the dwelling used by other TELE 4363 students (e.g. in case you live together).

We will use your student number to identify the dwelling for your project, so it is important that you **email** `tele4363adminATee.unsw.edu.au` **before Mon. Mar. 7 if you intend to use the same dwelling for the project as another TELE 4363 student.** In this case, please request slots that are separated by at least one month. This should provide some protection in case the specification changes over time. Also, the subsequent measurements may be cancelled by the lecturer if we are running out of time*resources – students who scheduled to make those measurements should use the data collected from the first measurement of that dwelling.

1.2 Check dwelling layout

In the Data Collection phase of this project, you will be required to map your dwelling. **Before Mon. Mar. 21**, you should check that your dwelling can be reasonably characterised by the method described in Section 1.1, and if not suggest in the webCT “Project: Suggestions for improvement” forum how the method should be modified to allow characterisation of your dwelling.

1.3 Slots for using equipment

In each week (from week 3 to 14, including the mid-session break and w12 seminar week), there will be 3 “slots” for use of the equipment, in the early, middle, and late parts of the week. The table below shows when the equipment can be picked up, and when it must be returned for each slot (through the EE&T store – room G18 of the EE&T building).

	Early	**Middle**	**Late**
Pick up Between 1pm and 5pm	Monday	Wednesday	Friday
Return between 9am and 11am	Wednesday	Friday	Monday

Due to public holidays, there will be no pickup on: Friday, 25 March (Good Friday) Monday, 28 March (Easter Monday) Monday, 25 April (Anzac Day) Friday, 10 June (due to the Queen’s Birthday)

Pickups on the following dates have exceptional return dates (but normal return times of between 9am
and 11am): Wednesday, 23 March return Wednesday 30 March Friday, 22 April return Wednesday 27 April

When collecting the equipment:

- You should check that the kit contains a complete set of equipment
- As early as possible, you should check the charge on the laptop’s battery, and if it is not fully charged, then plug in the mains adapter.

You will need some graph paper for drawing the layout of your dwelling. You can download a graph paper pattern from http://uluru.ee.unsw.edu.au/~tim/courses/tele4363/project/graph.pdf and print it out in lab G16 when you collect the equipment.

The deadline for returning equipment (11am) is also the deadline for uploading your data (Section 6.12) and submitting your drawing (Section 5.1).

1.4 Kits of equipment

Do not attempt to open the casing of any equipment. If you're interested in the inside of the wireless router, then look at http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=6 Do not expose the equipment to adverse conditions (e.g. moisture, humidity or dust if testing the effect of these on wireless transmission).

Most kits include 8 items, plus a bag: 1 laptop bag 1 measuring tape 1 Unshielded Twisted Pair (UTP) patch lead 1 laptop computer (details below) 1 Linksys WRT54g wireless router 1 Quickcam 2 power packs (one for the laptop and another for the wireless router) 1 D-Link DWL-AG660 wireless LAN card

The kit of equipment is self-contained, in that you need no other networking facilities in order to collect your data. We are using the wireless router not for its ability to interconnect networks, but as a cheap programmable wireless emitter. The photo shown in figure 8 shows a typical kit of equipment:

FYI: Security: Some of the equipment used in this project is configured to be slightly insecure so as to facilitate studies of wireless transmission. It is not intended to be a guide as to how to configure a secure wireless network. e.g. frame encryption complicates the mapping from physical transmission errors to bits as received by applications, and firewalls impede network performance monitoring software.

Phase 2: Mapping your dwelling

It is important to map your dwelling so that the distance between the wireless router and measurement points, and the objects placed within that distance, is known. Dwellings can vary substantially in organisation, so these guidelines may not be appropriate in all cases.

If you have a measuring tape, then you can map your dwelling before your slot for using the equipment. Doing so will provide you with more time during your slot for experimentation. However, you should update your map when you do the experimentation (e.g. to reflect the state of electronic equipment at the time of experimentation, rather than during original mapping).

2.1 Hand-drawn map

Manually draw a rough map of your dwelling on graph paper available from http://uluru.ee.unsw.edu.au/~tim/courses/tele4363/project/graph.pdf . If your dwelling has many floors, then use one sheet of graph paper per floor, and staple the pages together. The drawing must show the rooms (number each room) and their dimensions. Mark the locations of the following objects with the corresponding letters: doors (D), windows (W), robe/cupboard (R), large metallic objects such as fridges and sinks (M). This map does not have to be meticulous – its purpose is to facilitate visualisation (both by yourself and the teaching staff) of the map data that will be entered in the spreadsheet. In particular, the map doesn't have to be to scale – just draw the measurements on the rooms.

Submit the hardcopy of your map through the school assignment box with "TELE 4363. Dr Moors. 1234567" clearly written on the top right hand corner, where 1234567 is your student number. You *should* submit your map by the end of your slot for using the equipment, but the teaching staff won't mind if you are a couple of days late (up to 3).

2.2 Orientation

For the purposes of this project, we will consider dwellings to consist of a number of rectangular areas ("rooms") that are aligned with a front/back ("y-axis") direction (relative to the "front" of the dwelling) and a left/right ("x-axis") direction. You can choose an arbitrary side of your dwelling to be the "front", but you may want to consider that the front left corner of the dwelling will be used as the origin for measurement coordinates, and that the laptop will face the front or back for measurements. Figure 3 provides an example of two rooms. Note that the orientation (left/right and front/back) is the same for all rooms relative to the origin. The floating point measurements near the arrows indicate the dimensions of the rooms, and the integers in Room 1 identify Measurement Points (Section 6.5). The "W" and "D"s in boxes indicate the locations of window and two doors. Ideally, every detail of your dwelling would be recorded, but that would be onerous. Instead, we will aim to capture the significant parts of your dwelling, by measuring room sizes and objects that may affect radio propagation. The detailed mapping of your dwelling can be done at the same time as Experiment 2, in which you will move around your dwelling to take measurements. However:

- You must have some idea of the rough layout of your dwelling in order to locate the wireless router (Section 6.1).
- You should quickly scout around your dwelling to identify electrical devices and turn them on/off according to Table 5 as far as possible prior to Experiment 2.
- Since the measuring tape is metallic, you should not have it extended when performing the measurements of Experiment 2.
- If you map your dwelling before your allocated slot for using the kit of equipment, then you will have more time during your slot to spend on using the equipment and making measurements.

To allow machine processing of the data that you collect, you will use a spreadsheet to store data about the dwelling, rooms, and their contents. A template for the spreadsheet is available. You can use the Start-Menu->Office->OpenOffice.orgCalc spreadsheet tool under Linux to enter this data.

Spreadsheet extensions: Please do not extend the spreadsheet yourself – if you think it needs to be extended, then make a posting saying so to the "Project: Suggestions for improvement" discussion topic of webCT, and you could earn a bonus mark!

Object codes: To ensure some consistency in describing the construction and contents of dwellings, the spreadsheet uses, and the tables in this section provide, a set of codes for common types of construction materials and contents.

Repetitive selections in spreadsheet: It can be tedious to have to select the same value in many list boxes (e.g. to state that the ceiling for each room is plaster). A shortcut is to directly manipulate the coded data that the list boxes manipulate. The "Data" sheet stores this information, with essentially one room or object described in each row, and the columns providing attributes of that room/object, with the default code being 1 (indicating nothing yet entered). To directly manipulate this data, manually use the list box to specify the value for one room/object (e.g. one room has a plaster ceiling). Then check the “Data” sheet for where the corresponding coded value is stored, e.g. cell P3 for the ceiling of room 1. Then you can copy the value there (e.g. 3 for plaster) to the values for other rooms/objects in other rows to quickly replicate the value without having to enter it manually with the list boxes.

Measurements must be accurate to within 10cm, and preferably to within 1cm. If a parameter is variable, e.g. the height of a ceiling that slopes at an angle, then include your estimate of the mean value.

2.3 Exterior of your dwelling

Note that we distinguish between a building and your dwelling, e.g. an apartment (dwelling) may be part of a building.

FYI: The spreadsheet asks for your

- Student number: This (combined with knowledge of which students share dwellings) allows us to uniquely identify each dwelling.
- Postcode: This allows a rough guess at the type of construction of your dwelling (e.g. given when different areas were developed) and also to test the extent to which the class is representative of “typical” home wireless users.

Roof: What material is used for the roof of the building containing your dwelling? See Table 3 for codes. Purpose: Several roofing materials (corrugated iron and reinforced concrete) contain appreciable amounts of metal which may affect radio propagation. **Floors**: Select one floor as being at “ground” level. (In some buildings, e.g. the EE&T building, there may be a choice of ground.) Use consecutive integers to identify floors, with ground=1, and more positive means higher.

Number of floors in your building: The number of floors at ground level or above.
Lowest floor of your dwelling
Highest floor of your dwelling Purpose: For identifying probability of interfering sources above/below Measurement Points, and for understanding layout of rooms within dwelling.

Neighbouring constructions.
Identify any other constructions within 20m of your dwelling by recording their type, and their distance from the perimeter of your dwelling. Use “outdoors” if there is no such construction. If your dwelling spans multiple floors, then each floor may have different neighbours (e.g. a fence for the ground floor, and a more distant building for the 2nd floor). To cater for this, you can enter neighbour information for both the lowest and highest floors of your dwelling.

Purpose: This is intended to identify possible reflectors (e.g. metallic fences) or sources of interference (e.g. electronic equipment in neighbouring dwellings).

Value	Roof / ceiling	Neighbouring structures
0	none	
1	plaster / gyprock	outdoors
2	tile	indoor public space (e.g. corridor)
3	corrugated iron	indoor private space (e.g. another dwelling)

4	concrete	fence – wood
5		fence – metallic (e.g. colourbond)
6		fence – other material

Table 3: Codes for dwelling exteriors.

The following issues strictly relate to the interior of your dwelling, but encompass the overall dwelling, and so are raised here:

Does your dwelling have ducted air conditioning? Purpose: Air conditioning ducts often have large metallic surfaces which may reflect or absorb signals. While it would be ideal to map their location, they are often inaccessible. Recording whether they exist should help compare measurements from like buildings.

How many people were in your dwelling (more correctly, measurement space) during the experiment? Purpose: More people suggests an increased chance of people moving through the line of sight from laptop to router during the experiment.

2.4 Interior of your dwelling

The basic idea is to describe the layout in terms of rectangles, since most rooms are composed of rectangular parts. If a living space that you use as one "room" consists of multiple rectangular parts (e.g. an L-shaped room) then record each part (2 for an L-shaped room) as a separate "room". On your hand drawing, you may want to show the division between parts of a room using dashed lines. Measure the width and depth of the room. Do not include cupboards or built-in-robes as part of the distance measurements. If a rectangular area has a side that is longer than 10 metres, then divide it into smaller areas with sides no longer than 10 metres. (This ensures that Measurement Points will not be too widely spread, e.g. in open-plan dwellings with large open spaces.)

Choosing rooms: In Experiment 2 you must make measurements in at least 4 rooms, and preferably would make measurements in all rooms of your dwelling, although you are not required to make measurements in more than 10 rooms. You should record the construction (this Section) and contents (Section 5.5) of all rooms that you make measurements from, plus all rooms between the router and rooms that you make measurements from. You may not be able to access all rooms (e.g. they may be locked), in which case you should note this and guess their construction and contents.

Too many rooms?: If it is not feasible to make measurements in all rooms (e.g. if there are more than 20), then try to choose rooms that:

1. Would most likely contain computing or communications equipment (e.g. give preference to living rooms and offices over bathrooms).
2. Are the larger rooms (e.g. give preference to hallways over recesses) Represent all floors of your dwelling. e.g. if your dwelling has multiple floors, then make measurements in at least one room on each floor.

Too few rooms?: Assuming that a minimal dwelling has a living room and bathroom, treat those as two rooms, and make measurements from two "rooms" outside your dwelling: one a corridor or balcony through which you access your dwelling, and another an outside area preferably on the opposite of your dwelling to the corridor. If you don't live on the ground floor then this second outside area may be floating above the ground. For these outside areas, try to make measurements at points adjacent to your dwelling, and at a distance of up to 10m away from your dwelling.

What to record:

- **Room number**: Use consecutive positive integers starting with 1 to number rooms
- **Room type**: Implies typical contents and construction – e.g. metal fridge/sink in kitchen. Used for consistency checking of rooms in dwelling, and contents of rooms.
- **Notes about room**, Textual e.g. name of room (for your reference only – more user friendly than a number), whether it is non-rectangular, any structural features that may affect propagation (e.g. staircase in corridor room)
- **Room size**: left-to right for the width, and front-to-back for the depth. Measurements should be accurate to within 10cm.
- **Room Coordinates**: The location of the front-left corner of the room relative to the origin of your measurements. For example, in Figure 2, Room 1 has coordinates x=0, y=1.1 (offset from the origin), and Room 2 has coordinates x=5.5 (width of room 2 which separates it from the origin), y=0. The z coordinate is the floor number of the room.
- **Accessible**? Could you enter the room? If not, make guesses for the type of floor, ceiling and walls, and of what objects are within the room.
- **Floors**: The structure gives the floor strength, and the finish is what covers the structure as you view it from above. If you know the structure, then select floorboards, concrete, brick as appropriate. If you don't know the structure then try knocking on it to determine whether it sounds hollow or solid. If knocking is inconclusive (e.g. carpet covers floorboards, resulting in little sound) then select "unknown". Select the finish from tile, carpet or polished.
- **Ceilings**: Use the roofing codes from Section 5.3. For most dwellings, you should only need to measure the ceiling height once for each floor, and visually check that ceilings in adjacent rooms are at similar heights (if not, remeasure). For our purposes, we'll ignore ceiling cavities, and just measure the height of the lowermost layer of the ceiling relative to the floor. Codes:

Value	Room type	Floor structure	Floor finish	Wall
0		unknown		none
1	Bathroom	floorboards	tile	double brick
2	Bedroom	concrete	carpet	single brick
3	Hallway	brick	polished	fibro
4	Kitchen	generic - solid		concrete
5	Laundry	generic - hollow		plaster
6	Living			timber
7	Recess (e.g. built-in- robe)			cupboards
8	Toilet			built-in-robe
9	Office			generic solid
10	Unknown (only if inaccessible)			generic - hollow

Table 4: Codes for room data

Walls: Comments:

- **Openings in walls**: Doors and windows should be described as objects that appear “in” the room, as per Section 5.5.
- **Wall types**: It is hard to determine the type of wall without pulling it apart, which we don’t expect! For outer walls, exposed brick on the outside suggests that the wall is either single brick (if it sounds hollow when knocked from inside) or double brick (otherwise). You may gain insight into the construction of your dwelling by comparing it to similarly shaped neighbouring dwellings (e.g. if your building is cement rendered and you can’t determine what is under the cement, but it has the same shape as neighbouring buildings that are all brick, then you’d guess that there is brick under the cement) – this is one reason for taking a photograph of your dwelling. If all else fails, knock on it and indicate if it sounds solid or hollow.
- FYI: Some plaster walls are based on a wire mesh and are reported (e.g. http://www.intel.com/support/wireless/wlan/pro2100a/userguide/ENU/trouble.htm#3) to significantly affect wireless propagation.
- FYI: The redundancy in describing both sides of a wall that separates two rooms provides a consistency check and allows for rooms that adjoin multiple other rooms with differing dividers. When two rooms have inconsistent descriptions for a shared wall, we can assume that the description of wall for the room that is shortest along this wall correctly describes the common wall, and that the description of the wall for the other room describes the remainder of the wall for that other room.

2.5 Contents of rooms

Objects of interest are:

- Those that affect propagation (metal, water)
- Those that may create interference (electronic equipment, particularly wireless equipment)
- Communication outlets (potential locations for wireless router)
- Communication devices (phone, computer, etc)

Ideally, we would record the *location* of each of these objects, but to save labour, we will merely record their existence. Exceptional objects, whose exact location *will* be recorded, are Communication Devices and any metallic or water “Objects affecting radio propagation”.
Purpose: The location of such objects indicates whether they are in the line of sight to wireless router for various Measurement Points, and so could significantly affect the results.
Objects affecting radio propagation are gaps in walls (doors/windows) and those that contain large amounts of metal (absorber and reflector) or water (absorber).

- **Emphasise interior gaps**: It is most important to record gaps in walls through which the line of sight from router to laptop may pass (e.g. interior doors) but less important to record other gaps (e.g. exterior doors/windows on rectangular dwellings).
- **Close doors**: The state of doors may affect measurements (e.g. if open the door essentially an area of free space) but recording this introduces too many parameters (e.g. is the door hinged or sliding?, which side is the hinge on?, how far does it open?, etc) so **we assume for this project that doors are closed wherever possible**.
- **Metallic electronic objects**: Some metallic appliances (e.g. refrigerators and computers) could also be rightly considered to be electronic equipment, but we’ll just record them once as metallic objects.
- **Minimum cross-section**: The aim is to identify any object with an appreciable cross-section (more than 30cm by 30cm along any axis) that could significantly attenuate the signal (or reflect signals). To limit the number of measurements, we’ll omit objects that do not have large cross-sections. This includes objects that contain large amounts of non-planar metal, e.g. window frames, or a bed which may have metallic beams and even mattress springs. *Do* include objects such as fridges, filing cabinets, computers with

metallic cases, sinks, metallic insect/flyscreens and blinds on windows, etc.

State of electronic equipment: It is important to record the state of activity of all electrical equipment (Electronic equipment, Communication devices, and some Objects affecting radio propagation) since they may affect RF noise levels. The type of each electrical object includes a default state in parenthesis, e.g. “Computer (on)”. Set the “Default state” column entry for the object to reflect whether the object will be in this default state (on for a computer) for the duration of Experiment 2.

FYI: The state of electrical equipment could change during other experiments, which may lead to variability in results, but it is impractical to freeze everything in a living household. A possibility for Experiment 4 is to test whether the changing the state of such equipment affects the results obtained in Experiments 2, 3 or 5.

Try to determine whether wireless communication devices use the 2.4GHz band. Examples of products that do are 802.11 and Bluetooth networking equipment, and some DECT cordless phones.

Because the number of objects in a room may vary by room, the list of objects may be arbitrarily long. The list must consist of sets of 5 pieces of information about each object:

- the type of object
- Where it starts (closest point to the floor on the front-left corner of the room) on the “x”, “y” and “z” axes
- It’s length along the “x”, “y” and “z” axes

For these measurements, the z axis refers to a distance from the floor (c.f. other measurements where it indicates which floor). It is only necessary to provide

- **Start information** for Communication Devices and any metallic or water “Objects affecting radio propagation”.
- **Length information** for “Objects affecting radio propagation” – just use 0s for the lengths of other objects.

For other objects, you can leave these cells blank.

Note that one of the objects that you record must be the wireless router used in the experimentation.

Section 6.1 gives instructions for locating the router.

Value	**Objects affecting radio propagation**		**Electronic equipment**	**Communication devices**	**Communication sockets**
0		none	none	none	none
1	Wall openings	door	Dish washer (off)	Wireless router (on!)	phone / DSL
2		window	Fluorescent lights[2] (on)	Computer (on)	cable TV
3	Passive metallic objects	Filing cabinet	Microwave oven [5] (off)	Phone – wired (on)	TV antenna
4		Metal shelving	Minor appliances (clocks, plug-in lights) (don’t care about state)	Phone – 2.4GHz cordless	
5		Other (e.g. metallic flyscreens)	Stereo (off)	Phone – cordless (on but not being used for voice)	

6	Metallic appliances	Clothes dryer (off)	Television (off)	Phone – mobile (on but not being used for voice)	
7		Clothes washing machine (off)	Air conditioning (including fans and heaters) (off)	RF wireless devices (off) (baby monitor, remote controlled toys, etc)	
8		Refrigerator (on)	Combined electrical equipment (e.g. TV, VCR, stereo etc all in one cabinet) (off)	Known 802.11 devices	
9		Other			
10	Water bodies	Aquarium			
11		Other			

Table 5: Codes for room contents

Phase 3: Experimentation with equipment

Summary of measurements:

- Sniffing for other WLANs (Experiment 1)
- Signal strength from Measurement Points in each room (Experiment 2)
- Transmission errors (Experiment 3)
- Daytime photograph of exterior of dwelling The experiments would likely be conducted in the order listed above, although the only hard constraint is that the sniffing be done before other experiments so that possible sources can be disabled before subsequent experiments. Since Experiment 5 takes a long time, but little labour, it is likely that you will run it overnight

If resources permit, some students will be randomly selected to repeat the Data Collection phase towards the end of session. This is intended to check the repeatability of the Data Collection. Selected students will be notified by Fri. May 13th 2005.

3.1 Locating the router

You should locate the wireless router as close as possible to the geographic centre[3] of your dwelling (in terms of horizontal dimensions), subject to the constraint that its power lead can reach a mains outlet. This location is a first approximation of a location that should maximise coverage throughout your dwelling. Of course, other locations are also reasonable.

Height of equipment:

- Locate the **wireless router** as high as possible in the centre of the dwelling. This is because of gravity: most obstructions are on the floor, so elevating the wireless router can raise it above obstructions. For multi-story dwellings "as high as possible" implies that the router should be located on the top floor of your dwelling.
- Measurements from the **laptop** should be as close as possible to waist height (for convenience and approximation of desk height). ([6] claims that "node height also

significantly influenced link quality.")

Note that the router's location must be recorded amongst the objects in the spreadsheet (Section 5.5), and make sure that the wireless router's antennae are vertical.

3.2 Orientating equipment

The relative orientation of devices can significantly affect the quality of communication between them, as shown by [7] for wireless nodes in sensor networks, and [1] for 802.11 devices. Ideally, the wireless router and laptop would have the same orientation for all Measurement Points, however this would be cumbersome (requiring adjustments to the router for each measurement), and error prone (aligning devices when there is no line of sight). Instead, we will control orientation of the router and laptop so that their orientation is known.

The **wireless router** must be orientated so that its two antennas form a line that is parallel with the left-right axis of the dwelling, and are closer to the far side of the dwelling than is the side of the router with the LEDs.

Hold the **laptop** so that the up/down direction of the keyboard (e.g. from letter w on keyboard to letter z) is parallel to the line extending along the front/back directions of the dwelling. The observe program which makes measurements will ask you whether the LCD screen was facing the front of the dwelling or the back of the dwelling for each Measurement Point. The choice of orientation creates variability in the measurements but is intended so that you can see the screen and enter data on the keyboard. Furthermore, you must ensure that the laptop is between your body and the wireless router, otherwise the measurements will be complicated by variable inclusion of your body (which will absorb signals – see [8] and [6]) in the line of sight between laptop and wireless router.

3.3 Instructions for resetting the wireless router

You can login to the laptops under either Linux (Fedora Core) or Windows with the username "tele4363" and password "43634me". You should login under Linux for this part of the project.

Due to the need to connect a UTP cable between laptop and router, you may need to relocate the router lower than its position from Section 6.1. Please return it to that position when you have disconnected the UTP cable.

Connect the laptop to one of the 4 numbered ports on the router (not the fifth "Internet" port). Turn power on to the router. Press the reset button on the back for approximately 10 seconds until the power LED flashes or all 4 numbered LEDs light up. Wait a couple of seconds, and obtain from the router an IP address for the laptop's Ethernet (probably 192.168.1.100): In a Linux terminal:

$ sudo ifconfig ath0 down *ensure that the WLAN interface is down* (if the wireless card isn't inserted, which is OK, then you might get an error message.) Note that ath0 refers to the wireless interface, and eth0 refers to the Ethernet interface, and the last character of both names is a zero, not a capital O.

$ sudo ifconfig eth0 up *ensure that the Ethernet interface is up*

$ sudo dhclient eth0 *Use DHCP to obtain an IP address*

The router's default IP address is 192.168.1.1. Enter the router's IP address in the address field of a web browser on the laptop (e.g. Start Menu -> Internet -> Web Browser) to access the web-based interface to the router. The router will identify itself (WRT54G) and ask for a user name and password. Leave the user name blank, and use "admin" as the password.

The web interface starts with a “Setup” page. Kludge time: The software for accessing Linux on the router will only work if the router’s WAN/Internet interface has been “configured”. To do this, on the Basic Setup page:

Select “Static IP” from the drop-down box that by default is set to “Automatic Configuration –DHCP”. In the Internet IP address field, enter: 10.0.0.1 with Subnet mask: 255.0.0.0 and Gateway: 10.0.0.2

After clicking the “Save Settings” button (at the bottom of the window), you should see another window “Settings are successful”. Click “Continue”

While using the web interface, go to the “Status” tab (top right with black background) and click on the “Wireless” tab (with blue background on the right). This page should show which channel the router is using (which should be 6). If it does not show the channel, then check that you clicked on the blue “Wireless” tab (and don’t have the blue “Router” tab highlighted). If it does not show that the router is using Channel 6, then use the “Basic Wireless Settings” tab under the “Wireless” tab to set the channel to 6. From the Status -> Wireless tab, look at the MAC address of the wireless interface of the router.

On the laptop, make sure the wireless LAN card is inserted, and run:

$ sudo ifconfig ath0 up *ensure that the interface is up. If you get an error “No such device” then try reinserting the WLAN card.*

$ sudo iwconfig ath0 channel 6 *to match that used by the router*

$ iwlist ap *list visible access points (wireless routers)*

One of the MAC addresses (a string of six numbers separated by colons, where each number consists of two hex digits) listed for the ath0[4] interface should match the wireless MAC address of the router that is displayed on the Wireless Status web page. The display for this MAC address should also indicate a higher signal level than of other wireless devices, indicating the proximity of the router to the laptop. Copy this MAC address and paste it when you direct the wireless card to associate with the router:

$ sudo iwconfig ath0 ap <MAC address>

e.g. $ sudo iwconfig ath0 ap 00:60:1D:01:23:45 and then get an IP address for the wireless interface

$ sudo dhclient ath0 *get an IP address for the wireless interface* The output from dhclient should end with a line “bound to 192.168.1.102” or a similar number, which is the IP address of the wireless interface. If this number differs from 192.168.1.102, then make a note of it, and replace occurrences of 192.168.1.102 in these instructions with the address that you have. You should now also be able to disconnect the UTP cable connecting the router and laptop, and wirelessly communicate between laptop and router. Mark the Ethernet interface as down so that the laptop uses the wireless interface (rather than trying to use the disconnected wired interface) to communicate to the 192.168 subnet:

$ sudo ifconfig eth0 down

You should then be able to run the software that installs the interface with Linux on the router:

$ cd ~tele4363/wrt54g-0.51

$ ./wrt54g.sh The script should end with “You can connect a browser to ...”. If you get an error “ttcp status, status is 1” then you need to reset the router and configure the WAN interface as described above.

You should then be able to telnet into the router:

$ telnet 192.168.1.1 and see a command prompt (#). Note that commands in these instructions are prefaced by the # command prompt if they are to be run on the router; otherwise they are to be run on the laptop.

cd /tmp/var/bin/options and see the programs that you'll use in this directory.
netperf *performance testing client*
netserver *performance testing server*
emit *emits a series of packets – used for signal measurements*

3.4 Experiment 1: Sniffing for sources of interference

Wireless transmission characteristics will depend on what sources of interference exist. The intent of
Experiment 1 is to try to detect (using Kismet) other 802.11 equipment in the environment, in case it
might affect the results obtained in subsequent experiments.
Using Kismet:

- To invoke Kismet, type "kismet" from the command line of a terminal running on the laptop (e.g. with a $ prompt).
- Kismet logs the data that it collects in files in the directory from which it was invoked, so ensure that you invoke it from a directory to which you have write access (otherwise you'll get an "Unable to open dump file" error). The files have names of the form "Kismet-<date>-<invocation>.<extension>" and we are most interested in the .csv file containing information about networks that Kismet found (the first line of the .csv file describes the format, and the .network file contains a more human-friendly format of this data) and the .dump file which capture frames of interest that were observed on the networks.
- Kismet is a keyboard-orientated program. Windows (such as the opening "Welcome to Kismet" message) can be closed by pressing "x". Press "h" in any window for help. In large windows (such as the help window), use PgUp/PgDn to scroll up/down, and the left/right arrow keys to scroll left/right.
- Wander around the perimeter of your dwelling with the laptop running Kismet to survey for 802.11 wireless equipment.
- Type "Q" (note uppercase) to quit Kismet. If you detect any such equipment, then try to turn it off for Experiment 2 to Experiment 5.

What to submit:

- The .csv and .dump files for your run of Kismet
- If you detected wireless devices using Kismet, enter on the "Experimentation" sheet of the spreadsheet information about any devices that you were able to disable during the experimentation.

3.5Experiment 2: Signal propagation

The intention of Experiment 2 is to determine the coverage area of the wireless router across the dwelling. For our purposes, coverage will be inferred from the signal strength and noise level at positions around the dwelling. The wireless router will continuously transmit frames and the laptop will record the Receive Signal Strength Indication (RSSI) and noise level. Try to ensure that mobile phones are stationary during Experiment 2 (e.g. do not carry one yourself). FYI:

- Transmission characteristics need not be symmetrical, so it is possible that the wireless router can hear the laptop but the laptop not hear the wireless router, or vice versa. One reason for this is the different use of antenna diversity in different equipment, e.g. a wireless router may have antennas that are further separated than is possible on a cardbus NIC and so provide better choice of signal strength when selecting one antenna to receive a signal that is suffering multipath interference.
- A by-product of measuring signal strength is that the laptop will receive frames during this period and these can contribute to the body of data for studying transmission errors (Section 6.8).

The signal strength may depend on the transmission rate (and hence type of modulation) used. To control this, set the transmission rate for both the router and laptop to 54Mb/s:
On the router:

wl rate 54 *sets the unicast transmission rate*
wl mrate 54 *sets the multicast (and subnet broadcast) transmission rate*

On the laptop:

$ sudo iwpriv ath0 mode 3 *fixes the card in 802.11g mode (without this, it will switch to 802.11a which the router does not support)*
$ sudo iwconfig ath0 rate 54M *set the rate to 54Mb/s*

To collect data about signal strength. On the router:
cd /tmp/var/bin/options
./emit 192.168.1.255 100 123 200 10000000 54
The parameters for emit indicate:

- the destination address,
- the UDP packet length. FYI: The value of 100 (bytes) should ensure that frames aren't too long to have negligible chance of getting through. You can also estimate the bit error rate by knowing the frame error rate (from the "strength" file produced by observe) and knowing this packet length (plus the lengths of overheads: 8B for UDP, 20B for IP, plus 28B for the 802.11 MAC header).
- the seed for the randomly generated packet content. FYI: This value is arbitrary.
- the interval between packets (in us). FYI: The value of 2ms is long enough to give time for the 100B UDP packet to be transmittedat the lowest possible rate (1Mb/s).
- the number of packets to send. The value of 10 million should keep it going for long enough.
- the transmission rate (this only records the rate in packets – it doesn't affect the actual rate)

On the laptop:
$ cd ~tele4363
$ rm strength packets *Erase any previous records*
$ ./observe ath0 192.168.1.255 *Observe packets broadcast to subnet 192.168.1. on interface ath0*

The software to measure the signal strength needs to be informed of which room you are making the measurement in, and which **Measurement Point** within that room is being measured. It will first ask you to identify the room (using the number corresponding to that used in Section 5.4) and will then ask you to identify the Measurements Points as it makes the measurements. In each room, you should measure the signal strength at five Measurement Points identified as "2 o'clock" (back right corner), "5 o'clock" (front right corner), "7 o'clock" (front left corner), "10 o'clock" (back left corner), and the centre of the room. For example, in Figure 2, integers mark the positions of Measurement Points in the corners of Room 1. The software will ask you to identify the Measurement Point (2, 5, 7, 10, or 0 for the centre). It will also ask you whether the laptop's screen is facing the front or back of your dwelling, and will then measure the signal strength from the wireless router for 30 seconds. It may then beep, and will ask for details about the next Measurement Point. Move to the next Measurement Point, and repeat.

Typing mistakes: If you knowingly make a mistake when typing in a room number or measurement point then continue to collect the signal strength information as normal for that measurement point, but use "999" for the next room/measurement point so that the files record that the previous measurement was erroneous. Then continue as normal.

To help you understand the output for your analysis: observe sends output to the screen and to two files, “strength” and “packets”. Both files can be viewed from the command line by using “more”, e.g. “$ more strength”. The screen and “packets” output are essentially the same, with a “1” indicating a successful packet observation and “0” indicating a missed packet, with long strings of “0”s condensed to the form “[### pkts missing]”. The screen and “packets” output differ in how they show the room and measurement point numbers: these appear interactively on the screen, but appear on the beginning of each line of the “packets” file. The “strength” file has at least one line for each measurement point, with each line containing 11 comma-separated values:

1. Time (in seconds since Jan. 1 1970)
2. Room number
3. Measurement point number FYI: observe writes a line to the strength file for each 100 packets that it observes, possibly leading to multiple lines for the same measurement point. These lines can indicate the temporal variation of the signal strength. The channel statistics are averaged over the previous 10 packets, so if fewer than 10 packets have been observed, then these statistics will be polluted with values from the previous measurement point.
4. Whether the laptop was facing the front (F) or back (B) of the dwelling.
5. Number of packets that contributed to the measurement on this line FYI: The channel quality (see below) is measured over 10 frames, so is only meaningful if this value exceeds 10.
6. Number of packets received on the ath0 device ***before*** measurements on this line
7. Number of packets received on the ath0 device ***after*** measurements on this line FYI: if columns 6 and 7 differ by more than 100, then the difference is caused by extraneous packets which may not have come from the router, so may pollute the channel readings in terms of their use as indicators of the channel from the router.
8. Channel quality (See http://www.mattfoster.clara.co.uk/madwifi-4.htm#3 for details)
9. Channel signal level
10. Channel noise level.

For both the signal and noise levels, subtract 256 to get the value in dBm.
Note that Experiment 5 will append further measurements to the “strength” and “packets” files.

3.6 Experiment 3: Your own experiment

The exact form of Experiment 4 is up to you: Create, and conduct, your own experiment to test the transmission characteristics of wireless LANs in home environments.
Some ideas:

- Effect of fluorescent lights or microwave ovens
- Effect of height of equipment
- Absorption by bodies – insert varying numbers of people between line of sight path; test how signal strength depends on the presence of the “Objects affecting radio propagation” listed in Section 5.5.
- Repeat Experiment 2 or Experiment 5
  - using a different rate or channel

    To set the laptop’s wireless LAN card’s:
    - Rate:
      - List available rates: “iwlist ath0 rate”
      - Choose one of the rates: “sudo iwconfig ath0 rate 36M” (use “auto” instead of a number to specify that the rate should be selected automatically).
    - Channel:
      - List available and current channels: “iwlist ath0 channel”
      - Choose one of the channels (preferably channel 1, 6 or 11): “sudo iwconfig ath0 channel 6”

- o with antenna diversity disabled

  To control antenna diversity on the wireless router:

  • Choices are “0” (force use of antenna 0), “1” (force use of antenna 1) or “3” (automatically select best antenna).

  • Diversity can be controlled for reception using “# wl antdiv” and transmission using “# wl txant”.

  • To view the current setting, just run the above commands on the router, e.g. “# wlantdiv”

  • To control antenna diversity, follow the above commands with the value to use, e.g.“# wl antdiv 0”
- o outdoors (include a map of the area, as per Section 5)

Although you will only have access to your own dwelling for this experiment, try to describe how the experiment would operate across multiple dwellings, e.g. to test the effect of variations amongst dwellings.

If you wish to use the emit and observe programs for your experiment, then for the duration of this experiment, you should ensure that the “strength” and “packets” files are renamed so that your experimental data is not placed between the output of Experiment 2 and Experiment 5. Save the results of your experiment in a subdirectory exp4/*.

3.6 Experiment 4: Transmission errors

Because of the long duration of this experiment, you will need to plug the laptop into mains power. This may limit the choice of Measurement Point.

In Experiment 5, you will place the laptop at a Measurement Point used in Experiment 2 that is (as lose as possible) 10 metres from the router. Run the “emit” program on the router:

```
# ./emit 192.168.1.255 100 123 200 10000000 54
```

transmit many packets over the wireless medium. Run “observe” on the laptop to hopefully capture some episodes of transmission error. Add the number “1” as a third parameter when running “observe”
to force it to observe indefinitely (until you press ^C):

```
$ ./observe ath0 192.168.1.255 1
```

Also capture the frames using Ethereal, and in Ethereal’s “Capture” dialog box, set “Stop capture” after 10MB. Run this experiment for at least one hour, and preferably as long as possible.Save the packets captured by Ethereal in a file “exp5”.
The “observe” program appends additional packet and strength measurements to the end of the files created in Experiment 2.

Appendix 2 (Hand-Drawn and Spreadsheet Screenshots)

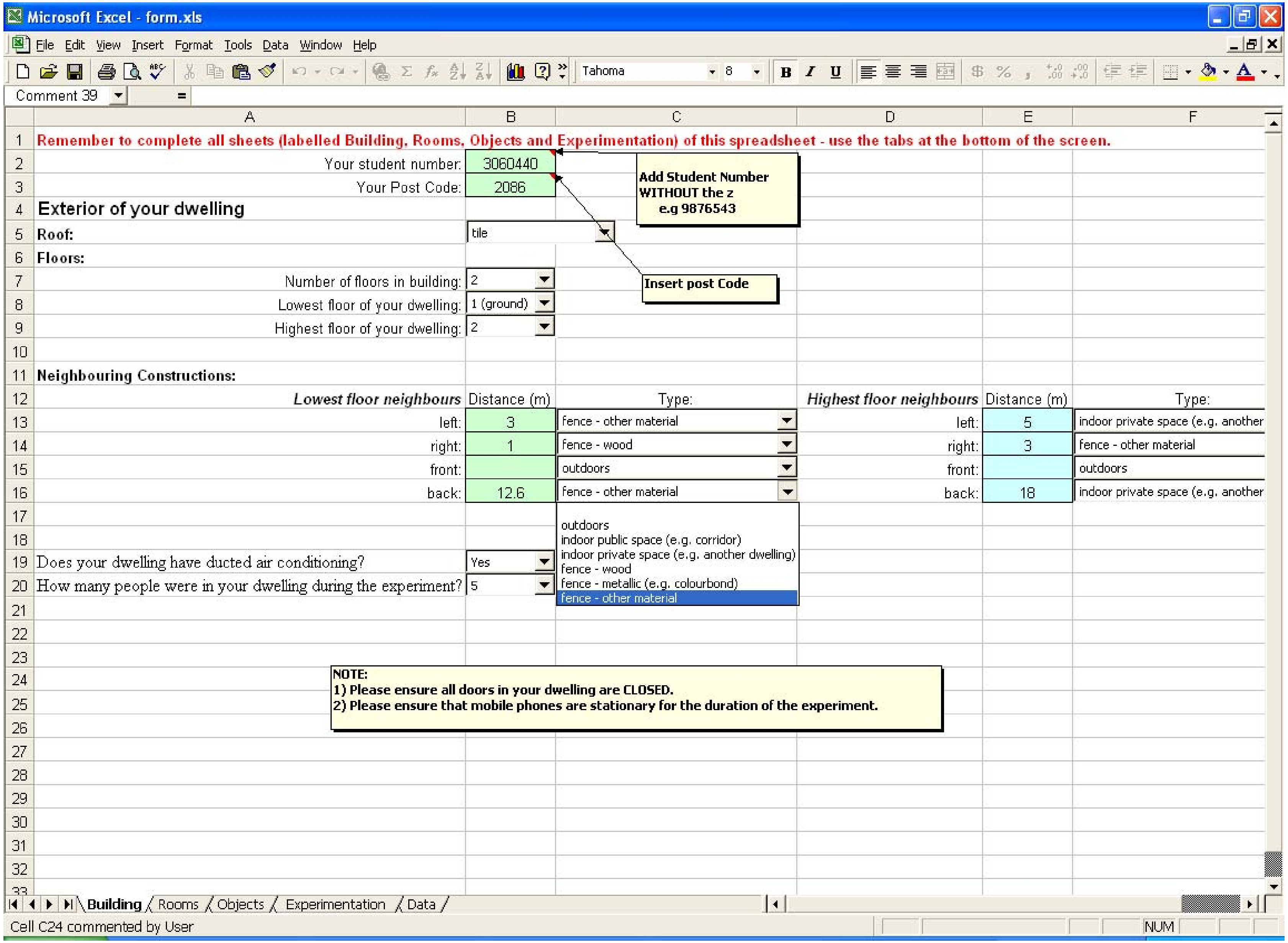
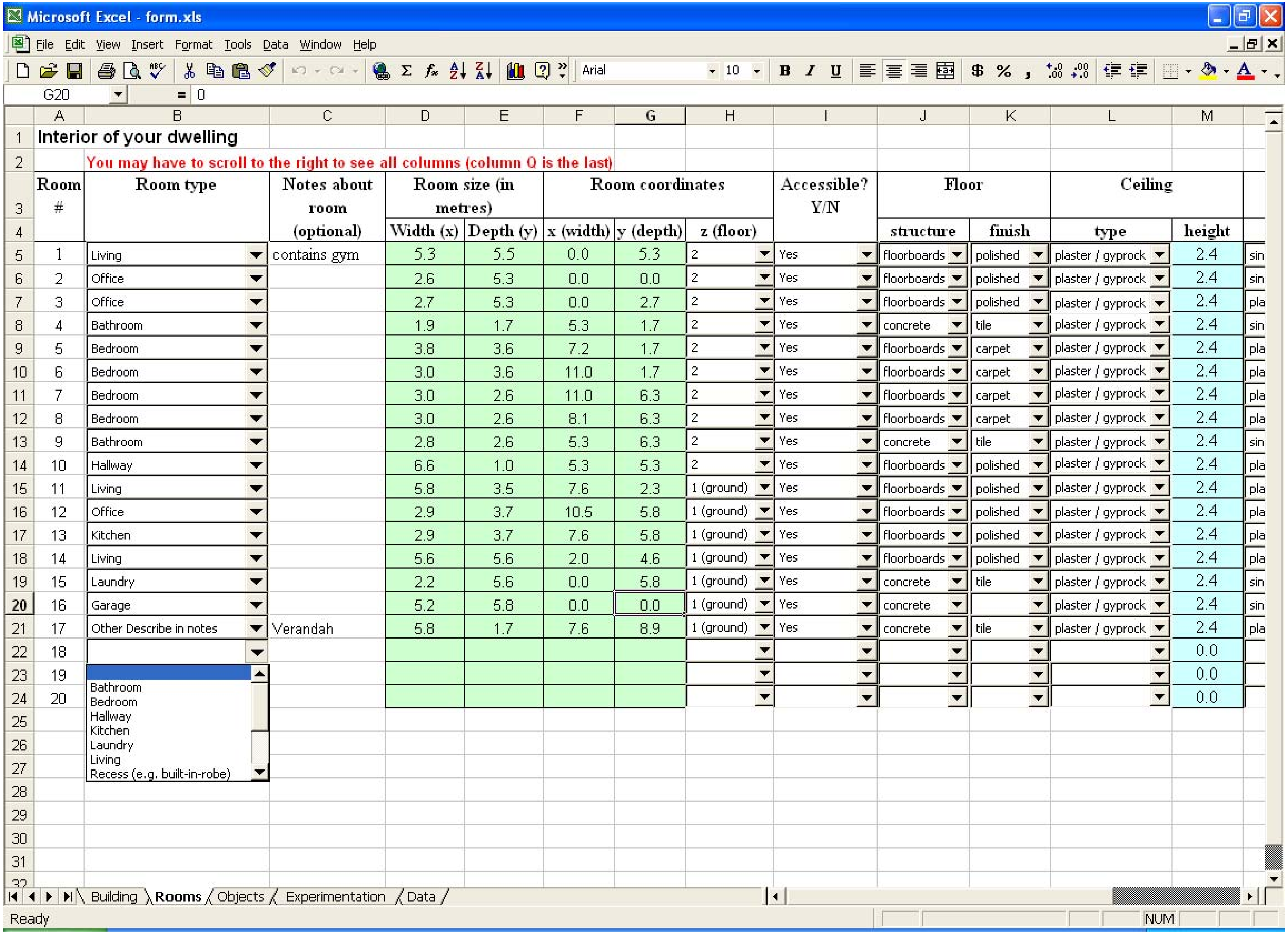


Figure 40 Screenshot of the Building form



Microsoft Excel - form.xls

File Edit View Insert Format Tools Data Window Help

G20 = 0

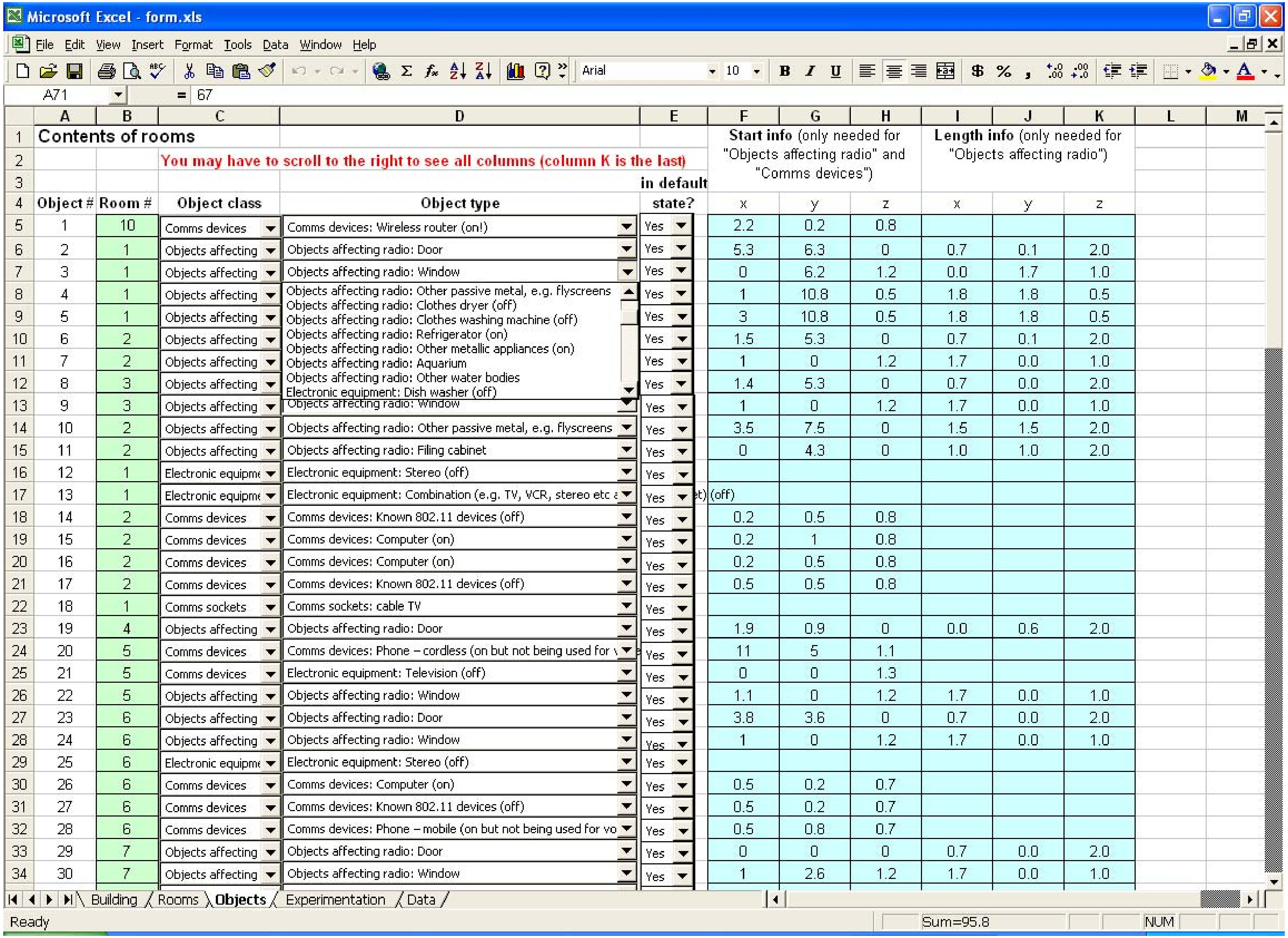
	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	Interior of your dwelling													
2		You may have to scroll to the right to see all columns (column O is the last)												
3	Room #	Room type	Notes about room	Room size (in metres)		Room coordinates			Accessible? Y/N	Floor		Ceiling		
4			(optional)	Width (x)	Depth (y)	x (width)	y (depth)	z (floor)		structure	finish	type	height	
5	1	Living	contains gym	5.3	5.5	0.0	5.3	2	Yes	floorboards	polished	plaster / gyprock	2.4	sin
6	2	Office		2.6	5.3	0.0	0.0	2	Yes	floorboards	polished	plaster / gyprock	2.4	sin
7	3	Office		2.7	5.3	0.0	2.7	2	Yes	floorboards	polished	plaster / gyprock	2.4	pla
8	4	Bathroom		1.9	1.7	5.3	1.7	2	Yes	concrete	tile	plaster / gyprock	2.4	sin
9	5	Bedroom		3.8	3.6	7.2	1.7	2	Yes	floorboards	carpet	plaster / gyprock	2.4	pla
10	6	Bedroom		3.0	3.6	11.0	1.7	2	Yes	floorboards	carpet	plaster / gyprock	2.4	pla
11	7	Bedroom		3.0	2.6	11.0	6.3	2	Yes	floorboards	carpet	plaster / gyprock	2.4	pla
12	8	Bedroom		3.0	2.6	8.1	6.3	2	Yes	floorboards	carpet	plaster / gyprock	2.4	pla
13	9	Bathroom		2.8	2.6	5.3	6.3	2	Yes	concrete	tile	plaster / gyprock	2.4	sin
14	10	Hallway		6.6	1.0	5.3	5.3	2	Yes	floorboards	polished	plaster / gyprock	2.4	pla
15	11	Living		5.8	3.5	7.6	2.3	1 (ground)	Yes	floorboards	polished	plaster / gyprock	2.4	pla
16	12	Office		2.9	3.7	10.5	5.8	1 (ground)	Yes	floorboards	polished	plaster / gyprock	2.4	pla
17	13	Kitchen		2.9	3.7	7.6	5.8	1 (ground)	Yes	floorboards	polished	plaster / gyprock	2.4	pla
18	14	Living		5.6	5.6	2.0	4.6	1 (ground)	Yes	floorboards	polished	plaster / gyprock	2.4	pla
19	15	Laundry		2.2	5.6	0.0	5.8	1 (ground)	Yes	concrete	tile	plaster / gyprock	2.4	sin
20	16	Garage		5.2	5.8	0.0	0.0	1 (ground)	Yes	concrete		plaster / gyprock	2.4	sin
21	17	Other Describe in notes	Verandah	5.8	1.7	7.6	8.9	1 (ground)	Yes	concrete	tile	plaster / gyprock	2.4	pla
22	18												0.0	
23	19												0.0	
24	20												0.0	

Bathroom
Bedroom
Hallway
Kitchen
Laundry
Living
Recess (e.g. built-in-robe)

Building | Rooms | Objects | Experimentation | Data

Ready NUM

Figure 41 Screenshot of the Rooms Form



Microsoft Excel - form.xls

File Edit View Insert Format Tools Data Window Help

A71 = 67

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Contents of rooms					Start info (only needed for "Objects affecting radio" and "Comms devices")			Length info (only needed for "Objects affecting radio")				
2			You may have to scroll to the right to see all columns (column K is the last)										
3					in default								
4	Object #	Room #	Object class	Object type	state?	x	y	z	x	y	z		
5	1	10	Comms devices	Comms devices: Wireless router (on!)	Yes	2.2	0.2	0.8					
6	2	1	Objects affecting	Objects affecting radio: Door	Yes	5.3	6.3	0	0.7	0.1	2.0		
7	3	1	Objects affecting	Objects affecting radio: Window	Yes	0	6.2	1.2	0.0	1.7	1.0		
8	4	1	Objects affecting		Yes	1	10.8	0.5	1.8	1.8	0.5		
9	5	1	Objects affecting		Yes	3	10.8	0.5	1.8	1.8	0.5		
10	6	2	Objects affecting		Yes	1.5	5.3	0	0.7	0.1	2.0		
11	7	2	Objects affecting		Yes	1	0	1.2	1.7	0.0	1.0		
12	8	3	Objects affecting		Yes	1.4	5.3	0	0.7	0.0	2.0		
13	9	3	Objects affecting	Objects affecting radio: Window	Yes	1	0	1.2	1.7	0.0	1.0		
14	10	2	Objects affecting	Objects affecting radio: Other passive metal, e.g. flyscreens	Yes	3.5	7.5	0	1.5	1.5	2.0		
15	11	2	Objects affecting	Objects affecting radio: Filing cabinet	Yes	0	4.3	0	1.0	1.0	2.0		
16	12	1	Electronic equipme	Electronic equipment: Stereo (off)	Yes								
17	13	1	Electronic equipme	Electronic equipment: Combination (e.g. TV, VCR, stereo etc a	Yes	t) (off)							
18	14	2	Comms devices	Comms devices: Known 802.11 devices (off)	Yes	0.2	0.5	0.8					
19	15	2	Comms devices	Comms devices: Computer (on)	Yes	0.2	1	0.8					
20	16	2	Comms devices	Comms devices: Computer (on)	Yes	0.2	0.5	0.8					
21	17	2	Comms devices	Comms devices: Known 802.11 devices (off)	Yes	0.5	0.5	0.8					
22	18	1	Comms sockets	Comms sockets: cable TV	Yes								
23	19	4	Objects affecting	Objects affecting radio: Door	Yes	1.9	0.9	0	0.0	0.6	2.0		
24	20	5	Comms devices	Comms devices: Phone – cordless (on but not being used for v	Yes	11	5	1.1					
25	21	5	Comms devices	Electronic equipment: Television (off)	Yes	0	0	1.3					
26	22	5	Objects affecting	Objects affecting radio: Window	Yes	1.1	0	1.2	1.7	0.0	1.0		
27	23	6	Objects affecting	Objects affecting radio: Door	Yes	3.8	3.6	0	0.7	0.0	2.0		
28	24	6	Objects affecting	Objects affecting radio: Window	Yes	1	0	1.2	1.7	0.0	1.0		
29	25	6	Electronic equipme	Electronic equipment: Stereo (off)	Yes								
30	26	6	Comms devices	Comms devices: Computer (on)	Yes	0.5	0.2	0.7					
31	27	6	Comms devices	Comms devices: Known 802.11 devices (off)	Yes	0.5	0.2	0.7					
32	28	6	Comms devices	Comms devices: Phone – mobile (on but not being used for vo	Yes	0.5	0.8	0.7					
33	29	7	Objects affecting	Objects affecting radio: Door	Yes	0	0	0	0.7	0.0	2.0		
34	30	7	Objects affecting	Objects affecting radio: Window	Yes	1	2.6	1.2	1.7	0.0	1.0		

Objects affecting radio: Other passive metal, e.g. flyscreens
Objects affecting radio: Clothes dryer (off)
Objects affecting radio: Clothes washing machine (off)
Objects affecting radio: Refrigerator (on)
Objects affecting radio: Other metallic appliances (on)
Objects affecting radio: Aquarium
Objects affecting radio: Other water bodies
Electronic equipment: Dish washer (off)

Building / Rooms / Objects / Experimentation / Data /

Ready Sum=95.8 NUM

Figure 42 Screenshot of the Objects Form

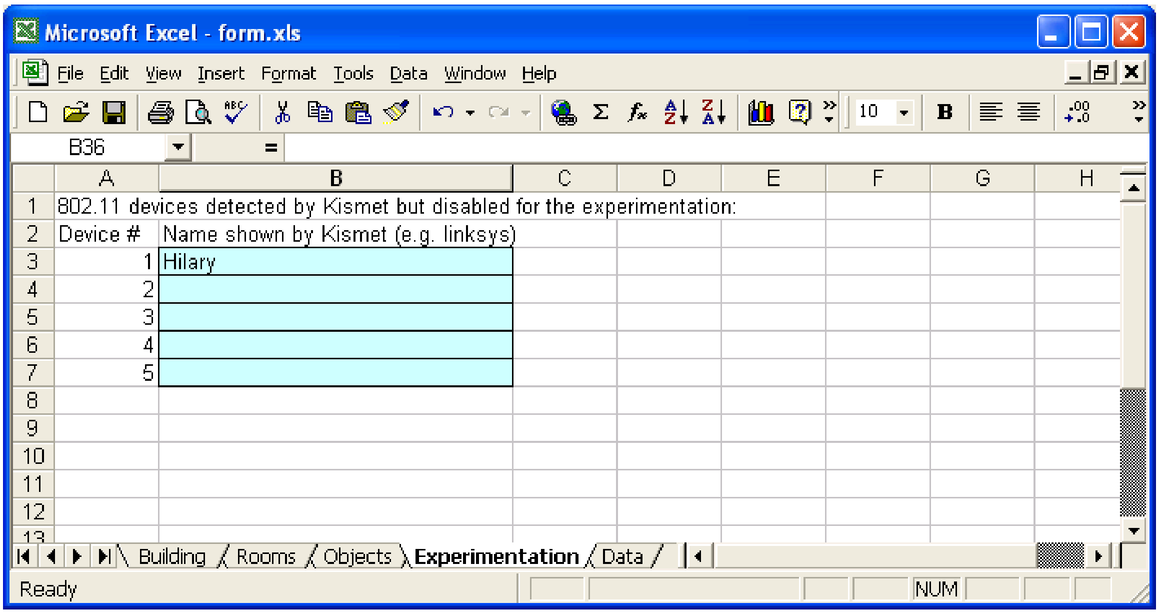
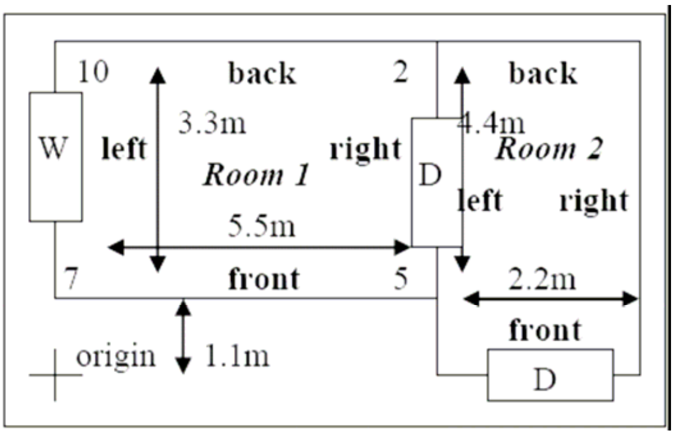


Figure 43 Screenshot indicating other Wireless LAN devices detected by Kismet

Figure 44 Computer drawn example of the contents that are required in the hand drawn



Appendix 3 (Strength and Packets Screenshots)

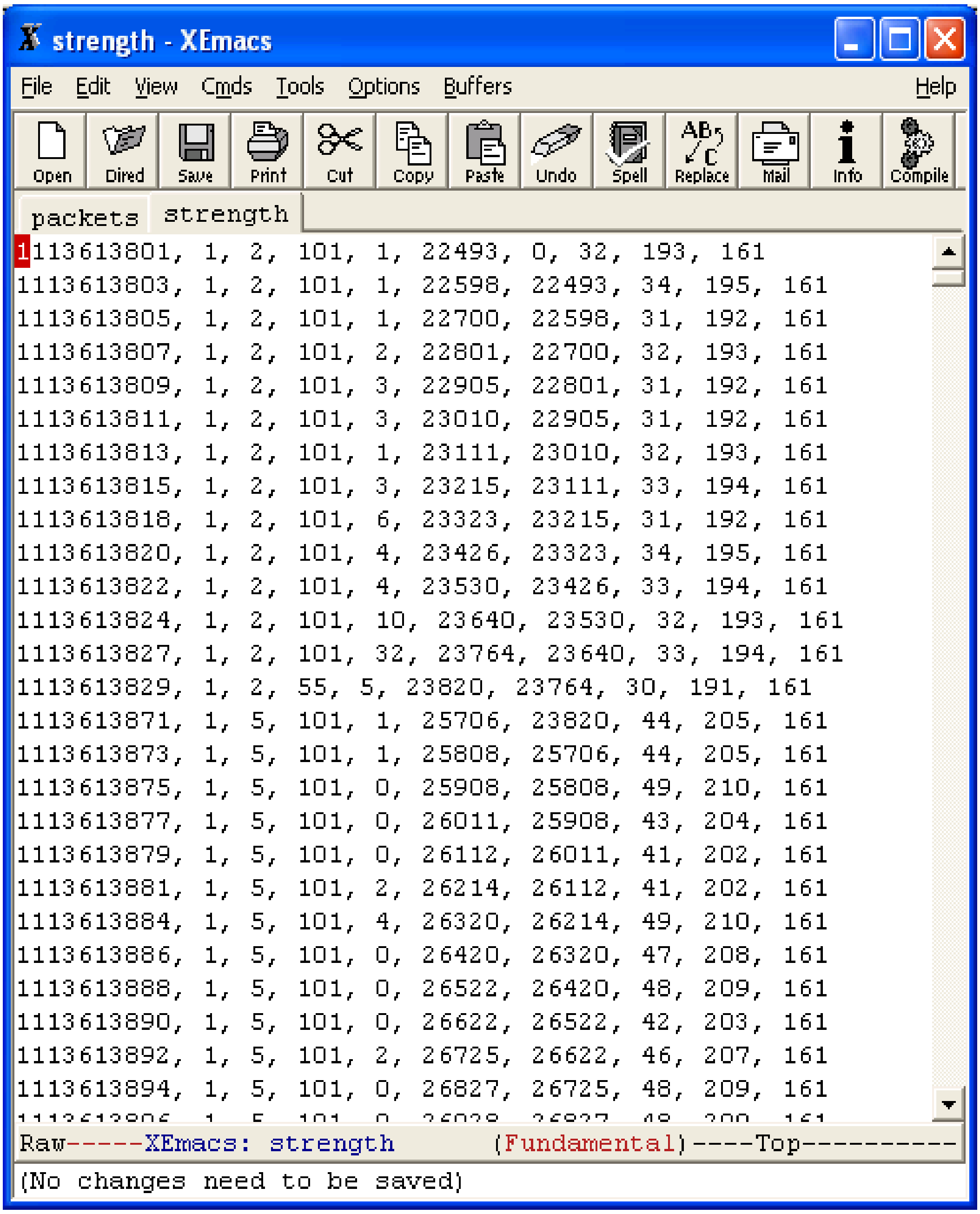


Figure 45 An extracted section of the Strength File

The Strength File contains 10 columns:
1 - time stamp
2 - room number
3 - measurement point
4 - number of packets contributed to measurement
5 - number of missed packets
6 - number of total packets received after measurement
7 - number of total packets received before measurement
8 - received signal strength indicator – noise level
9 - received signal strength indicator (0-255)
10 - noise level - 161

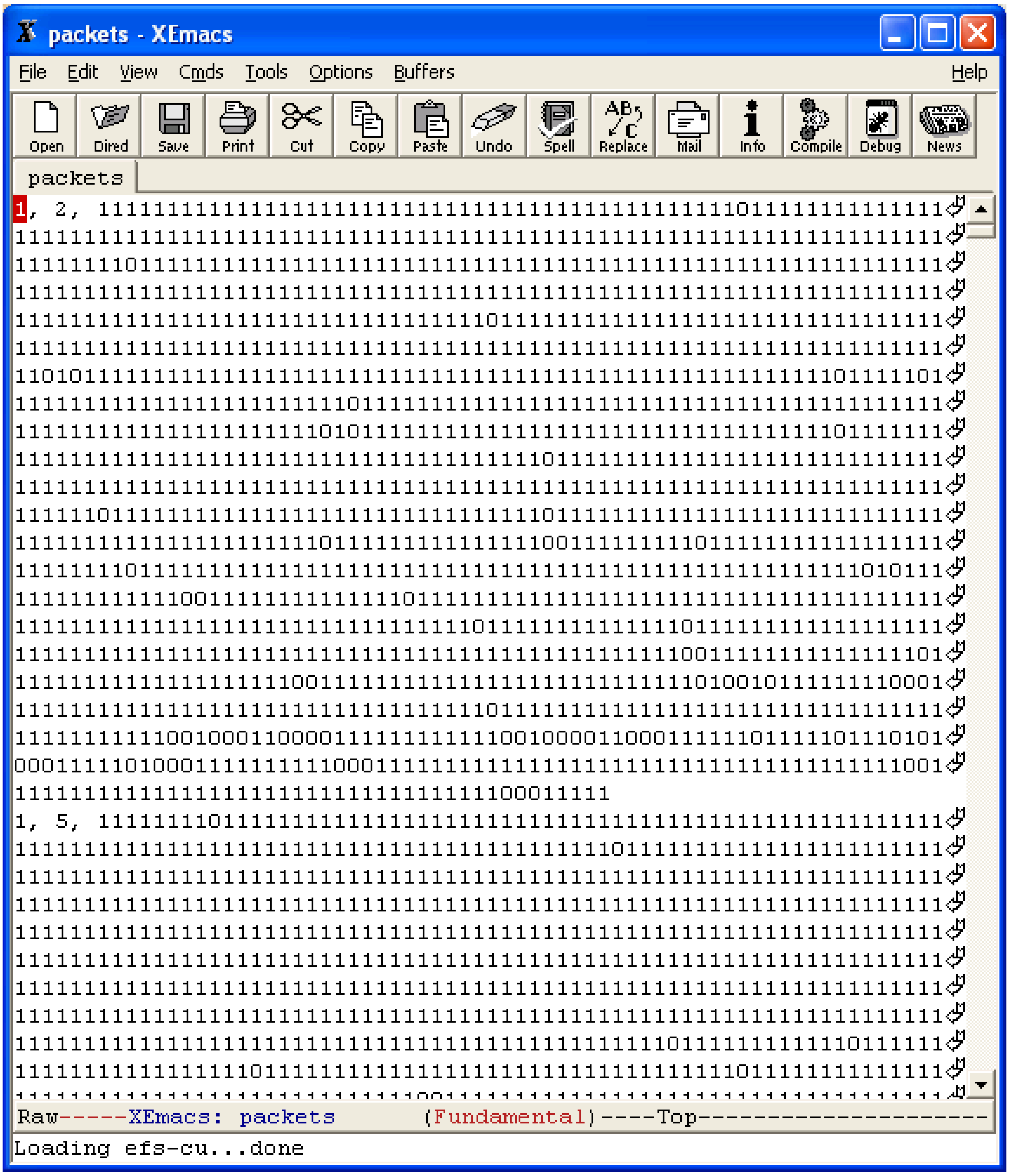


Figure 46 An extracted section of the Packets file (with word wrap enabled)

The Packets file:
First number - room number
Second number - measurement point (0, 2, 5, 7 or 10)
1 - successful packet
0 - missed packet

Appendix 4 (Outline of Edited Samples)

Forms that required manual editing:

Forms	Reason for Editing
59	Incorrect room number for router location.
83	Removed incorrect object - consisted of N/A lengths and room and type.
66	Incorrect room coordinates.
28	Had x and y coordinates back to front.
88	Changed version number to 1.7
21 and 58	Corrected 802.11 section, had N/A, changed to 0
13	Corrected disabled router section in spreadsheet, contained redundant router names

Strength and/or packets files that required manual editing:

Strength	Reason for Editing
13, 14, 17, 27, 34, 37, 54, 57, 61, 66, 67, 69, 73, 75, 82 and 83	Contained 999 for room or MP within.
69	Saved experiment in wrong order.
19	Contained error within strength file.
22, 25 and 63	Contained headings
6	Removed final dozen lines as all values were zero
52	Incorrect value entered.
Packets	**Reason for Editing**
27, 42, 50, 54, 62, 64, 72, 74, 78, 81,87	Contained blank lines.
6	Student edited file
22, 25	Contained headings within file

Final Router Samples:

Samples	Reason for Editing
1,4,5,8,10,20,21,23,25,27,29,30,32,36,37,39,41,43,45,46,47,50,51,53,55,58,59,64,70,72,73,75,76,78,80,82,83,84,85,86,88	Did not alter
7,9,13,14,15,16,17,26,28,31,38,44,48,52,56,62,66,69,74	Altered after receiving reply from e-mail
11,12,18,19,22,24,33,34,35,40,49,54,57,60,63,81,87	No Router
2,3,6,42,61,65,67,68,71,77,79	Incorrect Router coordinates

Samples that contained no strength files:

Samples	Reason for Editing
15,35,74,81	No strength Files

Appendix 5 (Graph for Different Room types)

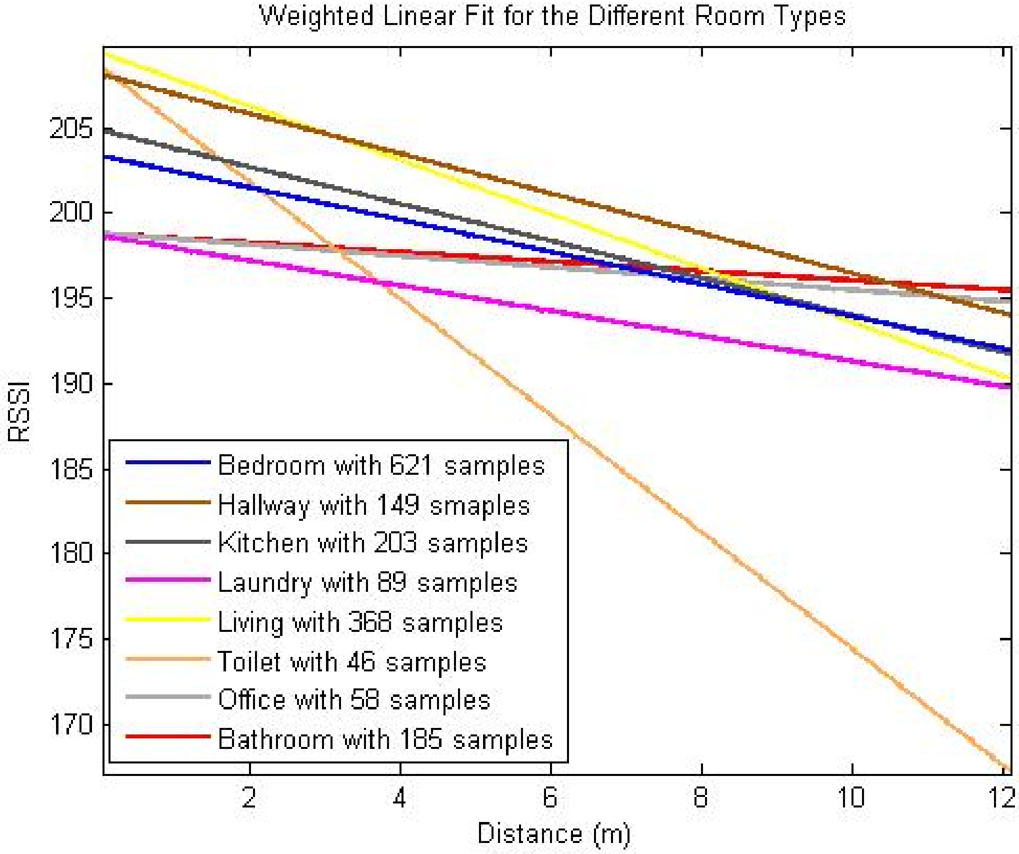


Figure 47 The weighted linear fit for all samples in a room

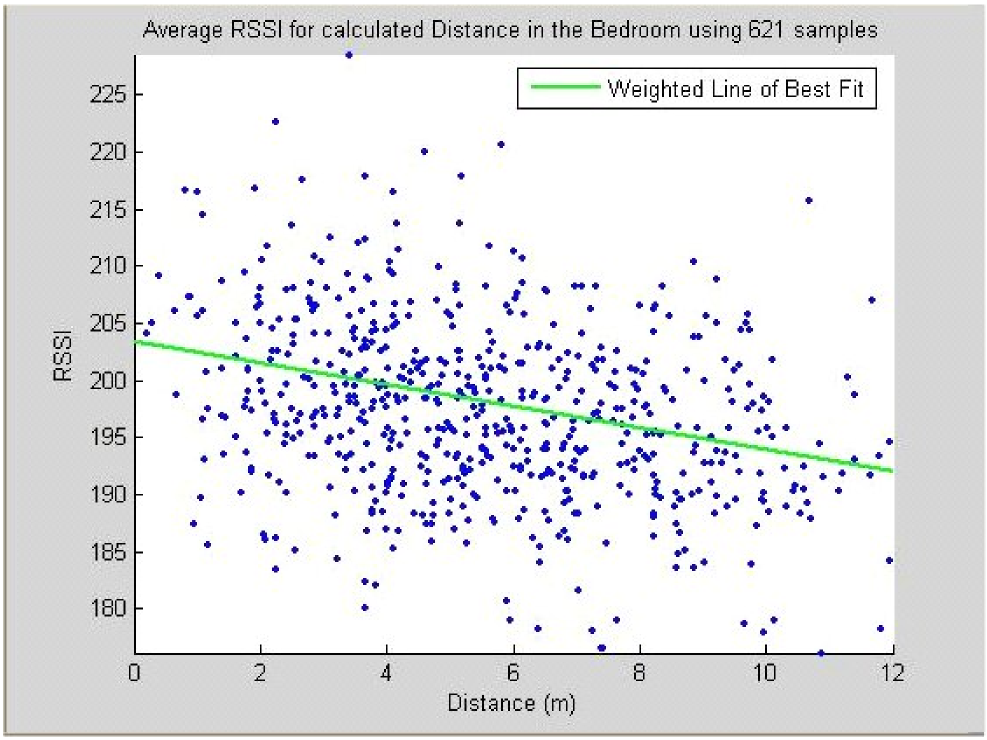
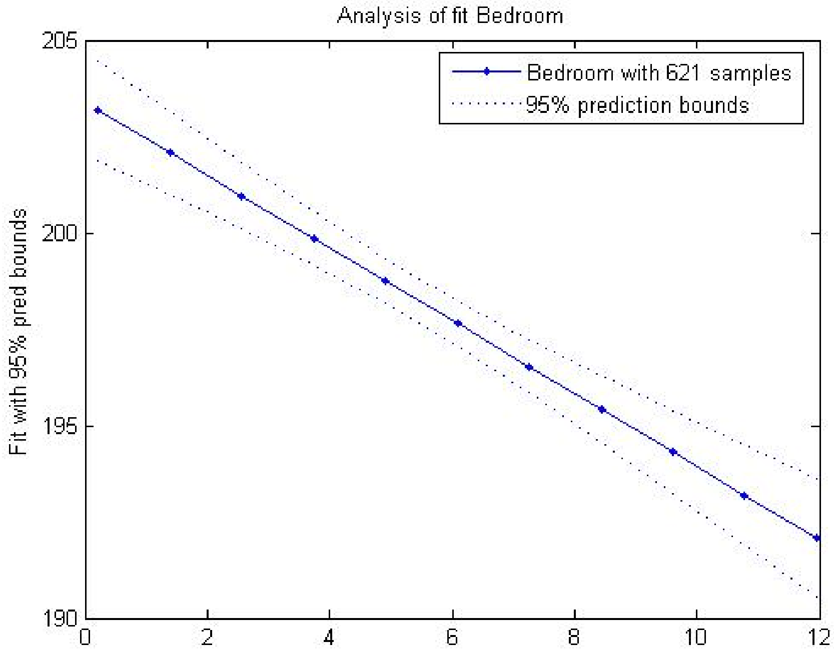
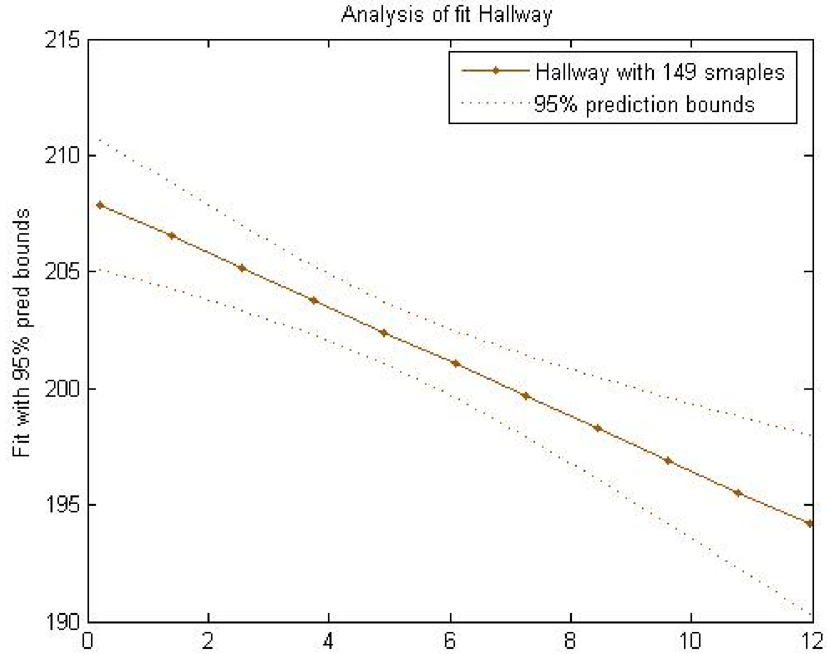
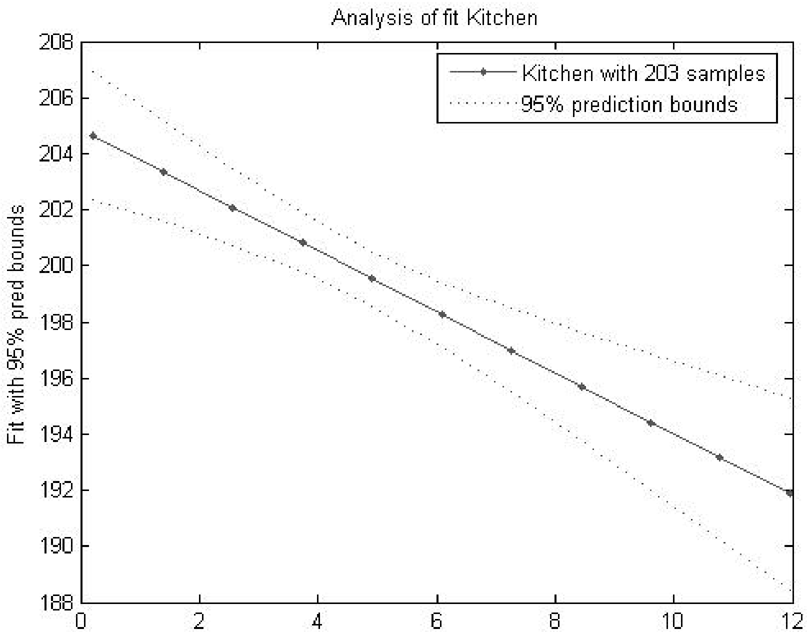
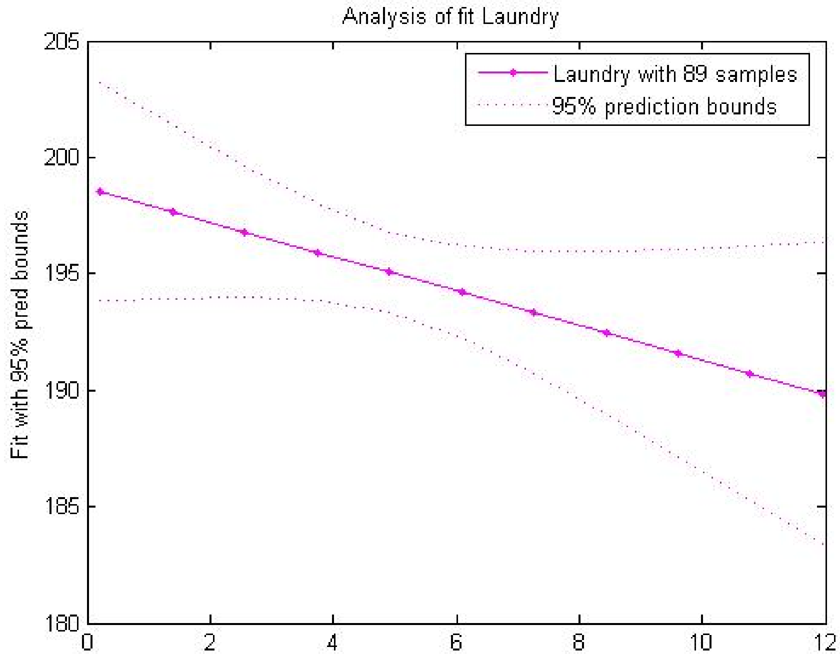


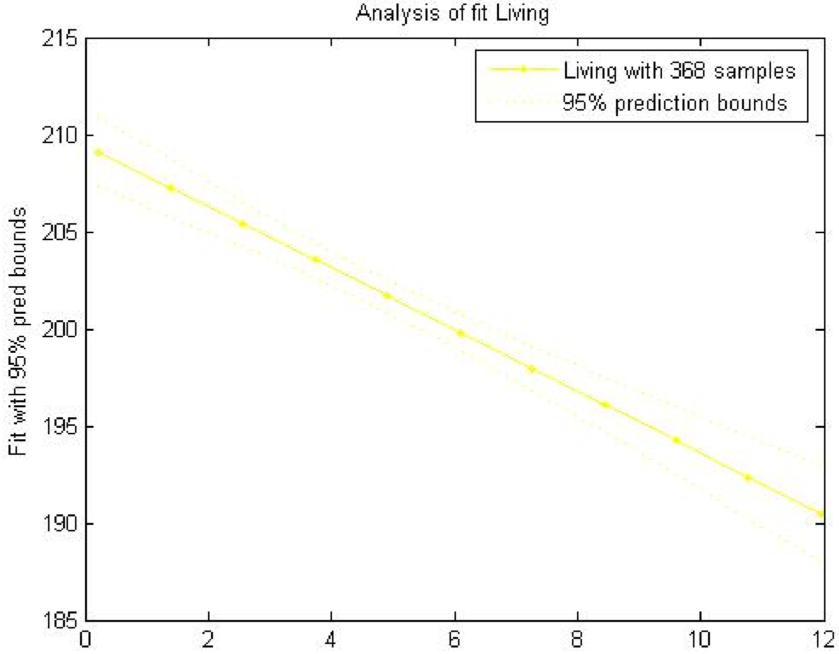
Figure 48 All samples and weighted linear line of best fit for the bathroom


Analysis of fit Bedroom
Bedroom with 621 samples
95% prediction bounds
Fit with 95% pred bounds
205
200
195
190
0
2
4
6
8
10
12


Analysis of fit Hallway
Hallway with 149 smaples
95% prediction bounds
Fit with 95% pred bounds
215
210
205
200
195
190
0
2
4
6
8
10
12


Analysis of fit Kitchen
Kitchen with 203 samples
95% prediction bounds
Fit with 95% pred bounds
208
206
204
202
200
198
196
194
192
190
188
0
2
4
6
8
10
12


Analysis of fit Laundry
Laundry with 89 samples
95% prediction bounds
Fit with 95% pred bounds
205
200
195
190
185
180
0
2
4
6
8
10
12



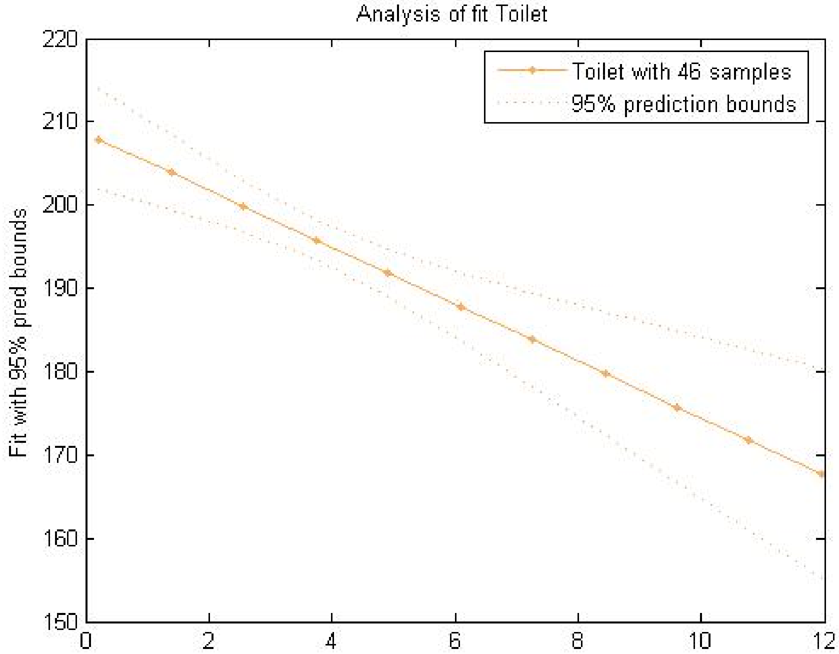
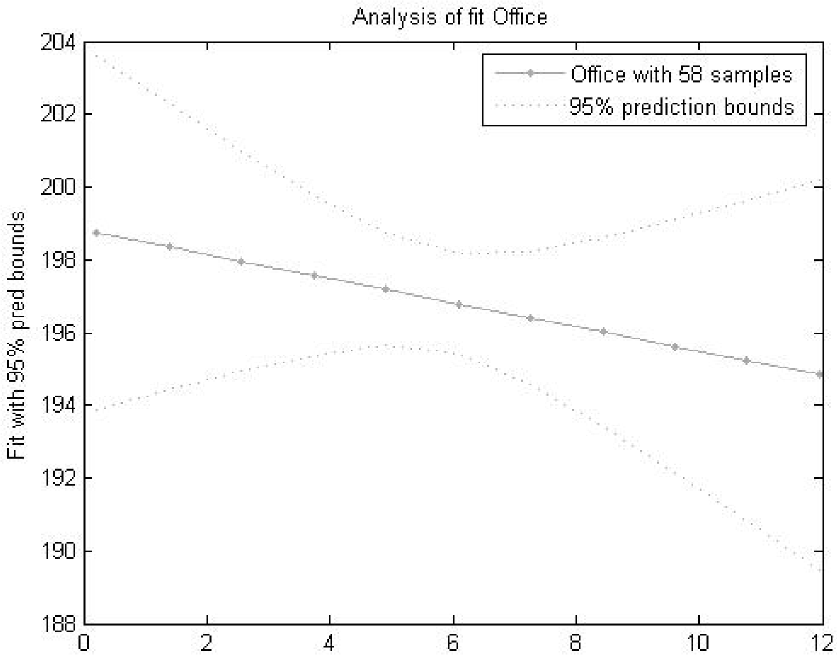
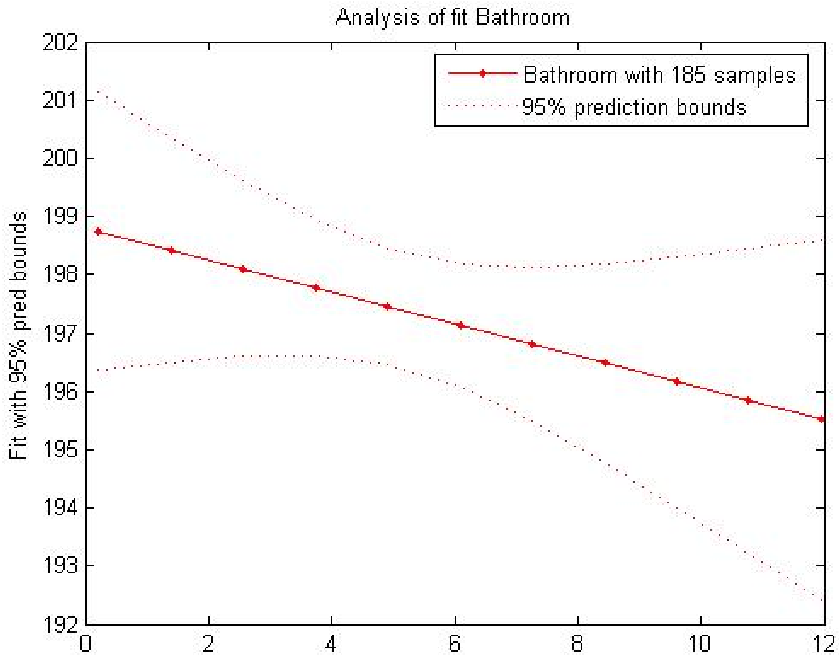


Figure 49 A 95% Confidence Interval for the different room types





Appendix 6 (The PER of Operational WLANs)

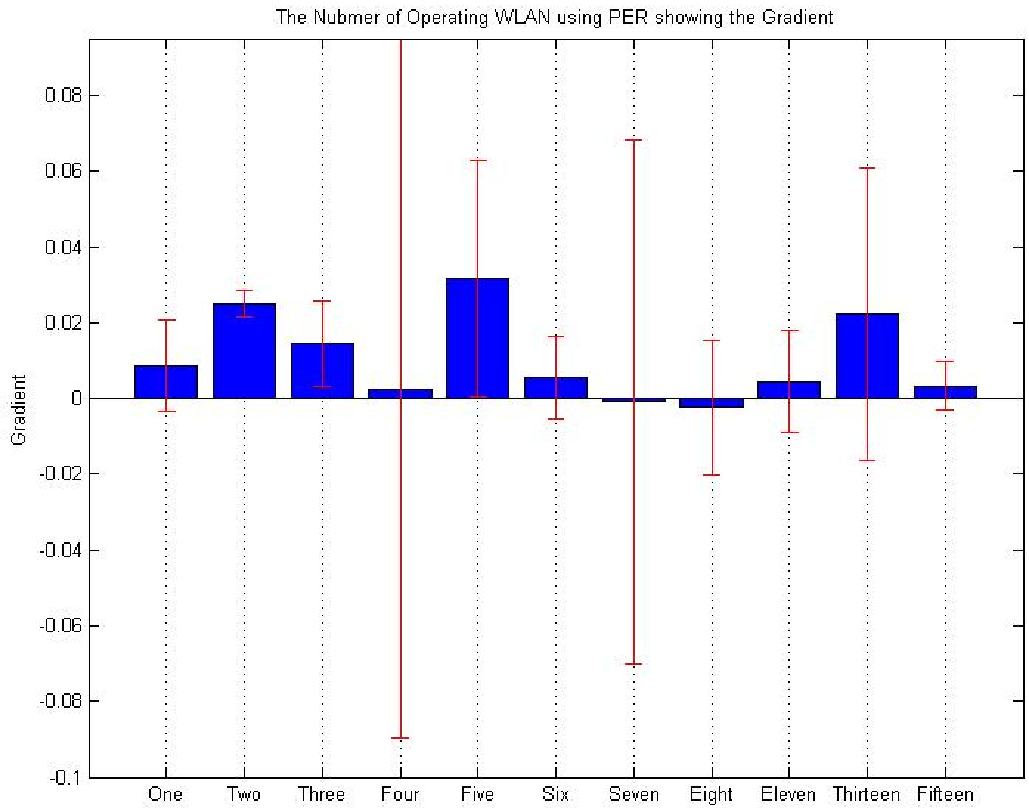


Figure 50 A 95% Confidence Interval of the gradient using PERs

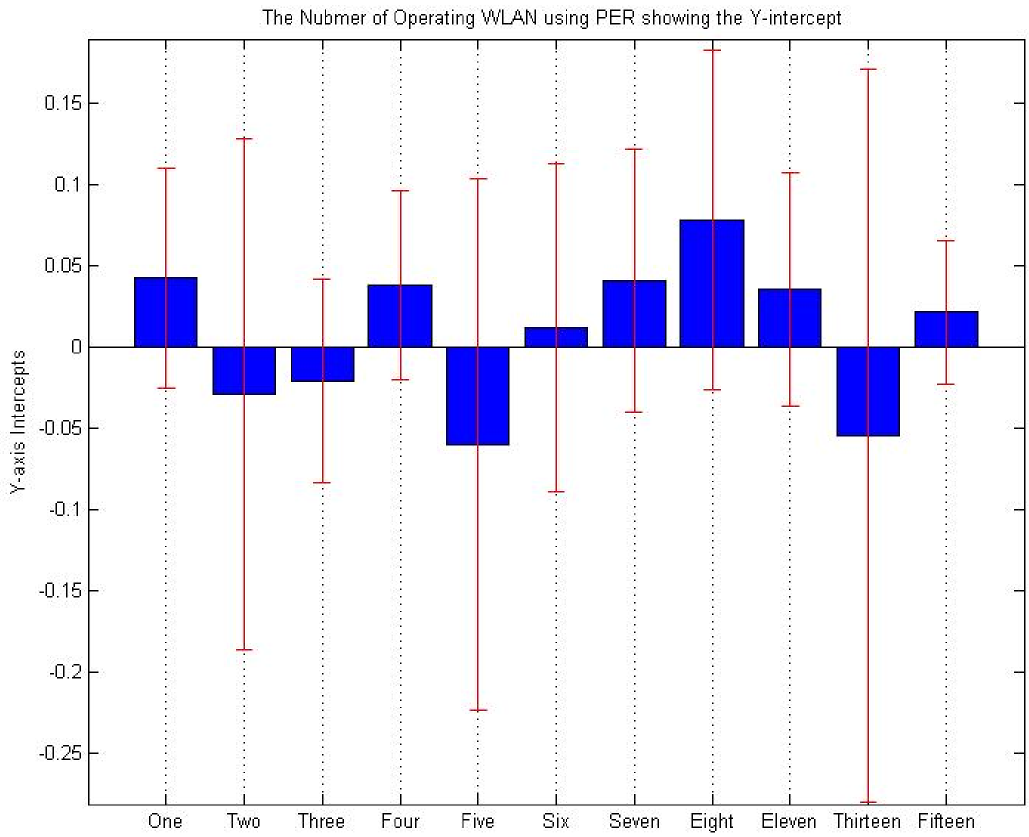


Figure 51 A 95% Confidence Interval of the Y-intercept using PERs

Appendix 7 (Confidence Intervals of Air-conditioning Graphs)

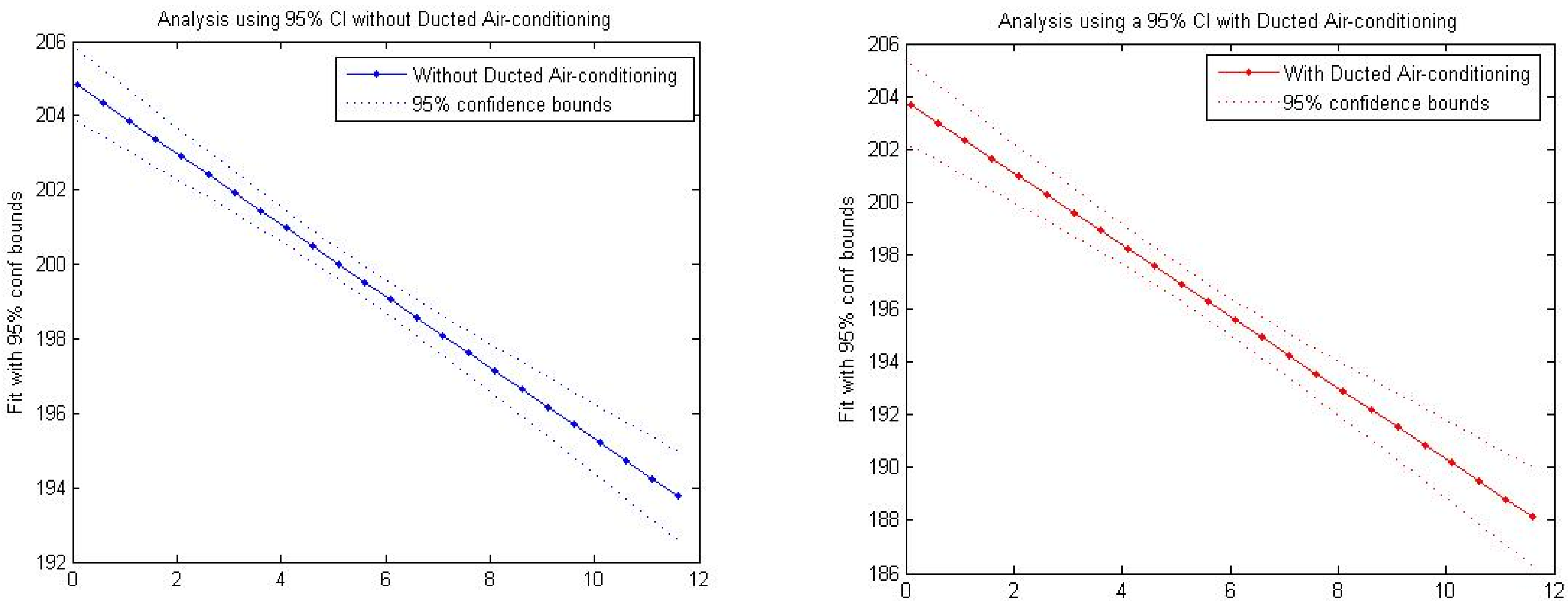


Figure 52 Using RSSI a 95% CI for dwelling without and with ducted air-conditioning

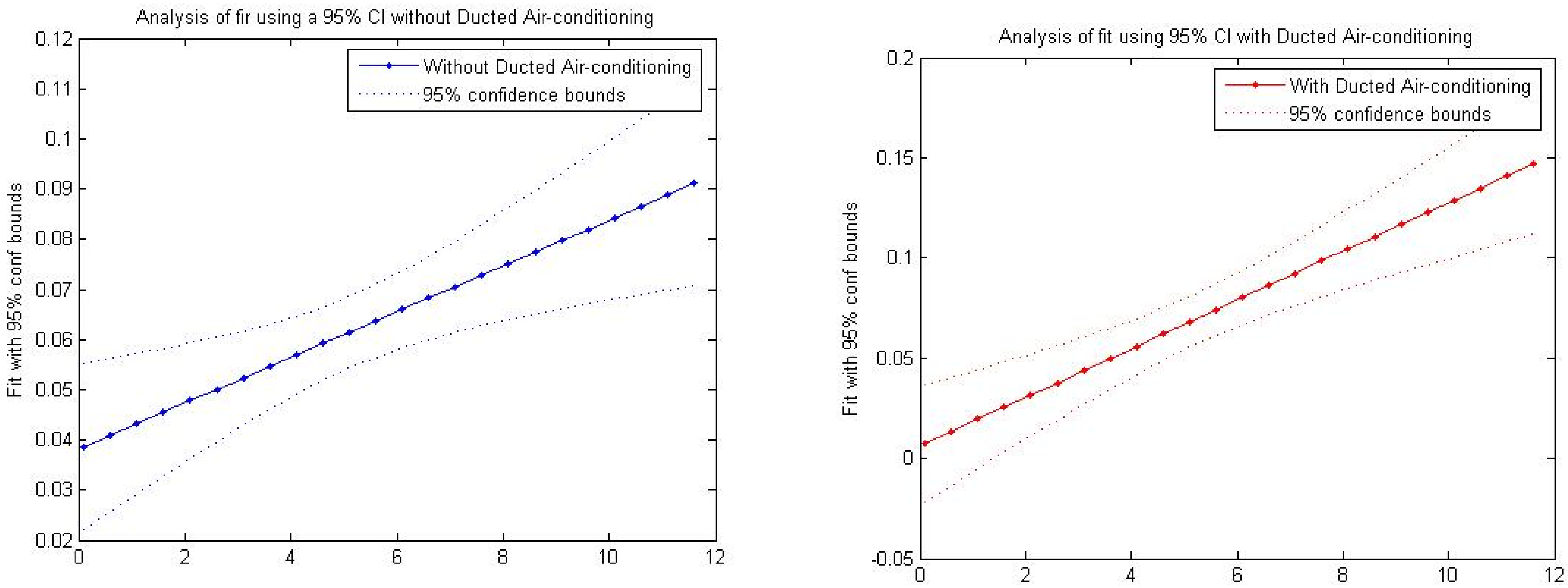
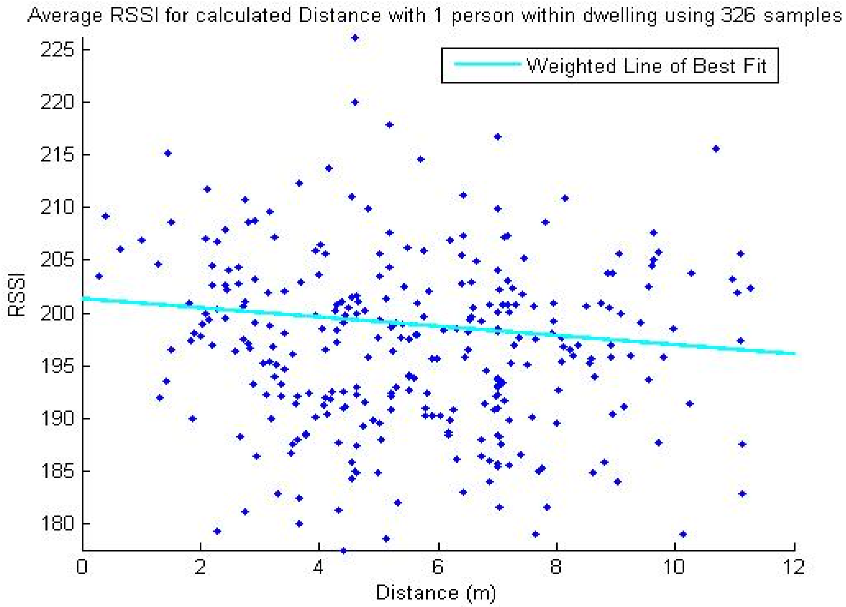
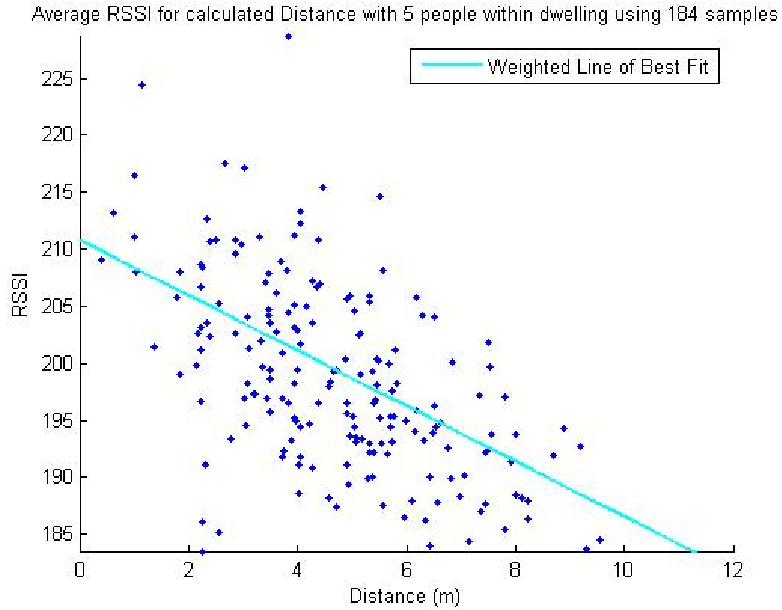


Figure 53 Using PER a 95% CI for dwelling without and with ducted air-conditioning

Appendix 8 (Sample of Graphs with People in the environment)





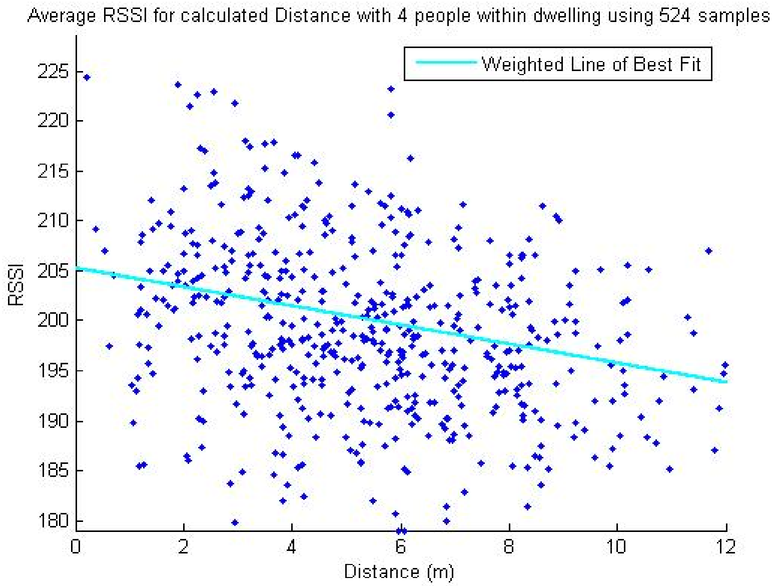
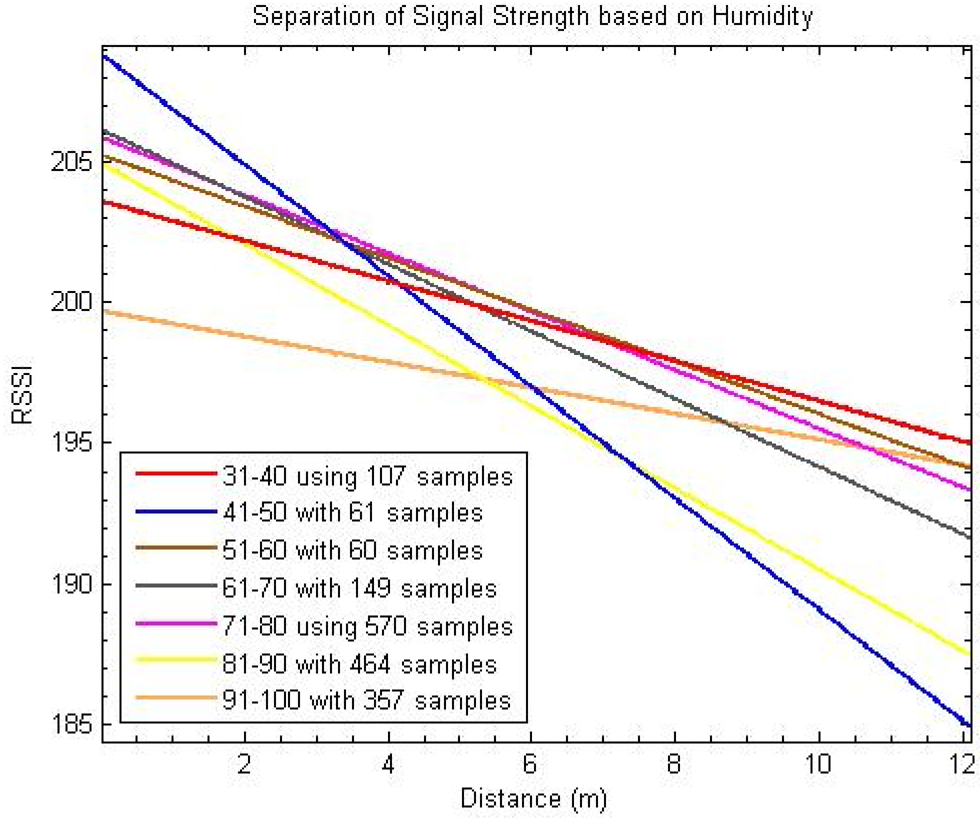


Figure 54 Sample of Signal Strength graphs

separated by the different amount of people within the dwelling

Appendix 9 (Humidity Graphs)



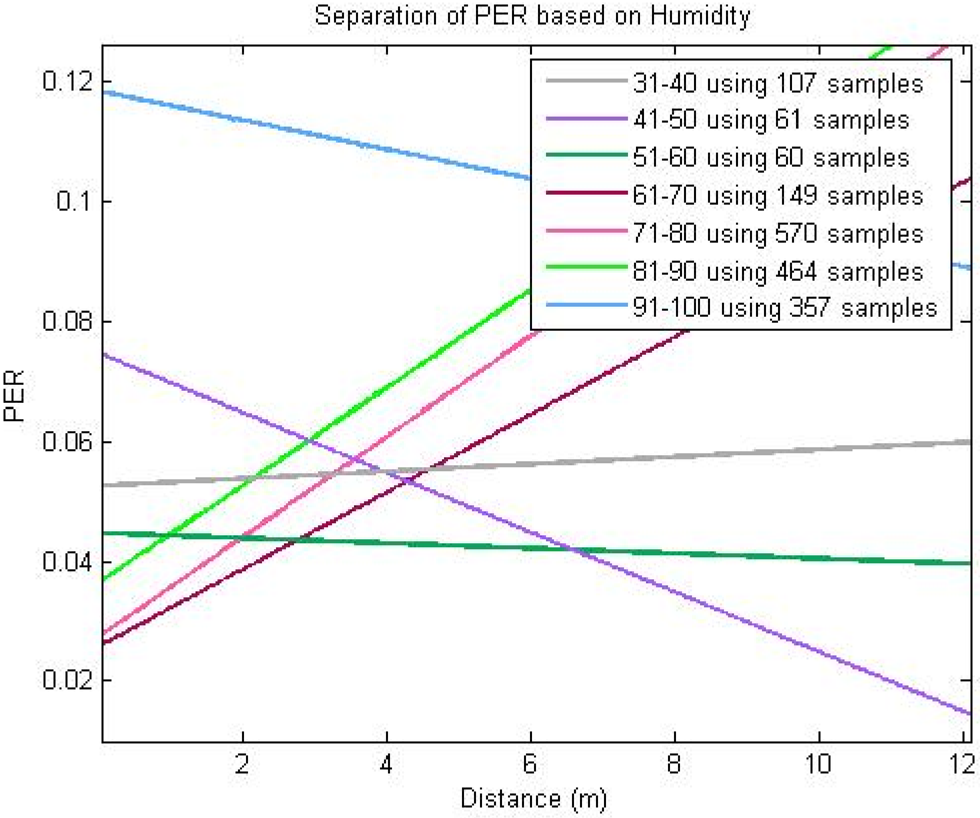


Figure 55 The RSSI and PER as a function of distance separated by humidity values

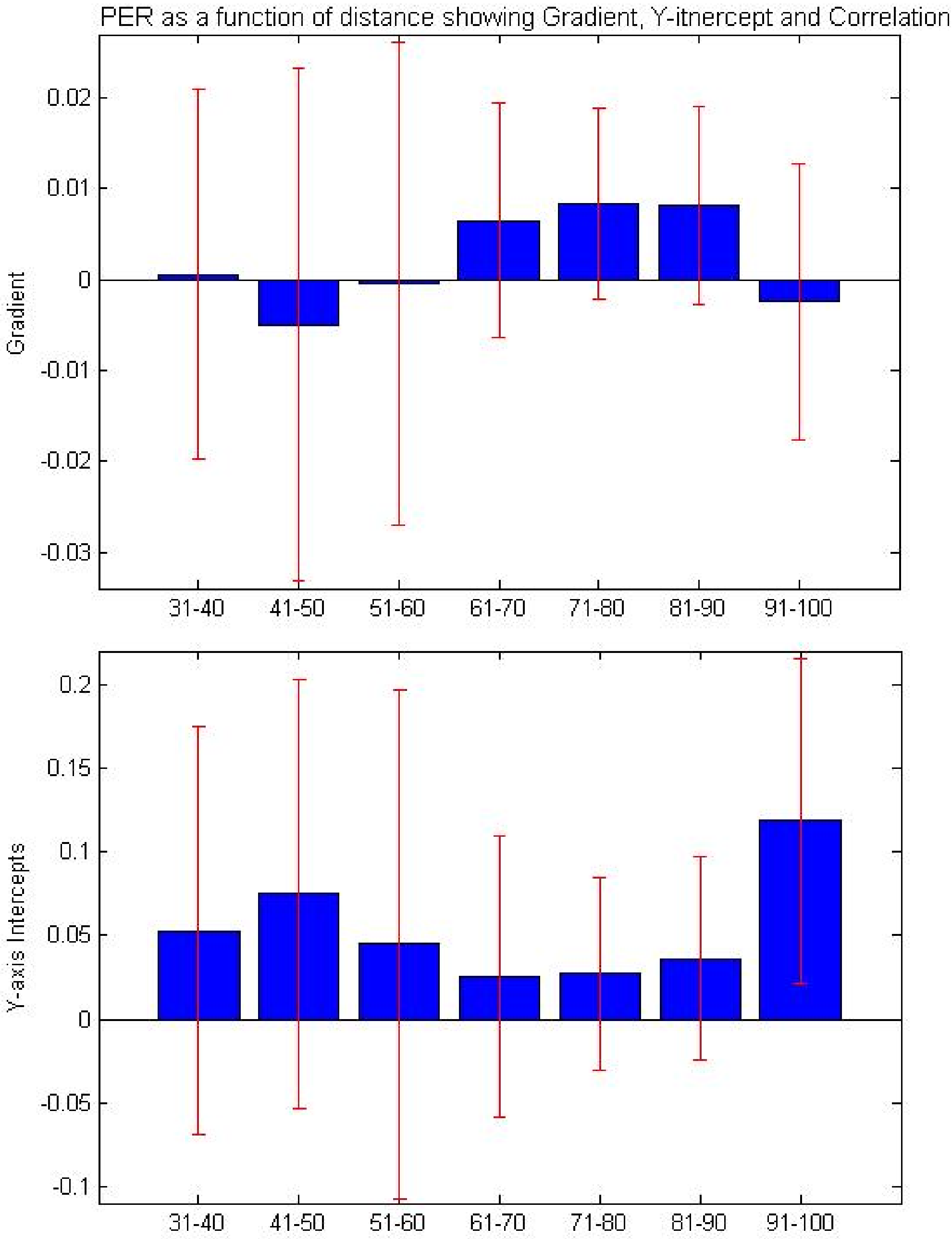


Figure 56 The CI of Gradients and Y-intercept PER as a function of distance