A Novel Low-Cost Method for Characterization of Mobile Propagation Channels with Consumer Devices

by

Trevor Gamblin

A thesis
submitted to the University of Ottawa
in partial fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical Engineering and Computer Science

Examining Committee

The following served on the Examining Committee for this thesis.

Supervisor(s):	Sergey Loyka Professor, Dept. of Electrical Engineering and Computer Science, University of Ottawa
Examiners(s):	Halim Yanikomeroglu Professor, Dept. of Systems and Computer Engineering Carleton University
	Claude D'Amours Professor, Dept. of Electrical Engineering and Computer Science, University of Ottawa

Declaration of Authorship

I hereby certify that this thesis is entirely my own original work except where otherwise indicated. I am aware of the University's regulations concerning plagiarism, including those concerning consequent disciplinary actions. Any use of the works of any other author, in any form, is properly acknowledged at their point of use.

Abstract

The latest advancements in mobile device technology are putting ever-higher demands for throughput of wireless networks. This is threatening to outpace the ability of service providers to deploy the necessary infrastructure. Fifth-Generation Mobile Network (5G) technology is experiencing rapid adoption as part of the effort to meet demand, and along with it researchers are continuously seeking new metrics and models for use in predicting the limits of current and future network infrastructure. To succeed, it is key that they have access to methods for simple, effective analysis of the wireless propagation channel in any given location. The typical laboratory test environment lacks the unpredictability and uniqueness of real-world conditions. Additionally, it utilizes equipment whose specifications are often far removed from devices that are actually intended to operate on the mobile network, such as smartphones themselves.

This work focuses on the nature of contemporary path loss models and their ability to accurately predict signal levels, seeking to validate their use against observed path loss behavior in outdoor line-of-sight (LOS) scenarios, where the number of active devices can vary significantly over short periods of time. These conditions are typical of public spaces such as parks and city streets where a large number of users may all simultaneously be accessing high-throughput services. To test their validity, statistics are provided for sets of data collected on foot in public spaces using a novel software utility developed expressly for this purpose. The models we use for comparing against our measured results include both experiential models that are built on other data sets, along with stastically-based, large-scale path loss models. These are compared as a function of distance from the base station (BS), and any unique characteristics of the local network are considered. Finally, a combination of environmental imagery, coverage maps with signal strength overlays, and the aforementioned model comparison are used to estimate the signal source and predict performance in nearby areas.

Acknowledgements

I would like to thank Dr. Sergey Loyka for his insight and encouragement from the beginning of my exploration in electromagnetic theory. His guidance has been invaluable in developing the research concept contained within, and the foundation in wireless communications theory provided by his graduate courses has been similarly pivotal. I cannot thank him enough for taking the time to review the early versions of this work and give helpful suggestions in all aspects of my time in graduate school.

Next I must thank my loving wife Amy, who has been incredibly patient and considerate throughout this long, arduous process. I could not have finished this work without her continuous support. I look forward to us finally spending more time together now that this is complete.

There are many other people in my life who have either influenced this research directly, or assisted me by providing appropriate escapes when breaks were required. These people have also often humored my numerous attempts to explain complex theoretical concepts, design patterns, and industry trends in layman's terms, which collectively have proven invaluable in bolstering my own understanding. In no particular order, thank you to: my longtime friend and philosophical foil Justin, his wife Brittany, and our friends Bovens and Katrina; my childhood friend Brett; my Toronto friends Sonam, Julie, and Nada; my former colleagues Randy, Konrad, Mark, Paul, Jason, and Saul at Wind River Systems; Tim, with whom countless discussions on the wonders and frustrations of working with modern technology were had; my sister Jenny, brother-in-law Umut, father Verdell, my stepmother Roselle, and late mother Elaine; my former advisors Dr. Gohary and Dr. Lambadaris at Carleton University, who helped me get started on this path; and undoubtedly many others whom I am ashamed to have forgotten.

Last but far from least, I cannot forget to thank my four-legged children Stella and Morrison. Their presence has aided me through this journey in countless ways. The unintended insight, constant companionship, and laughter they have provided over the last few years helped to make it all possible.

Table of Contents

Symbols

χ_{σ}^{ABG} Shadowing factor (ABG model) 16, 27

χ_{σ}^{CI} Shadowing factor (CI model) 16, 27

$a(h_{RX})$ Okumura-Hata environment size correction factor 15

α Alpha (ABG model) 16, 41, 42

β Beta (ABG model) 16, 41, 42, 47, 55

c Speed of light 13

D Maximum antenna dimension 7

d Transmitter-receiver distance 6, 13–16

d_0 Reference distance 16, 17

d_c Two-ray critical distance 14, 44, 50

d_{coh} Coherence distance 28, 53

f Frequency 13, 14, 16, 17, 27, 41, 42, 53

G_{RX} Receiver gain 7, 26, 27, 53

G_{TX} Transmitter gain 7, 18, 26, 27, 53

γ Gamma (ABG model) 16, 41, 42

h_{area} Average local area height 24, 25, 31, 36

h_{elev} Local transmitter elevation 24, 25, 31, 34, 36

h_{hgt} Local transmitter height 24, 25, 31–36, 54

h_{RX} Receiver height 14, 18, 27

h_{TX} Effective transmitter height 14, 18, 24, 25, 31, 36, 41, 42

K_r Okumura-Hata suburban correction factor 15

L_0 Average path loss 10

L_L Long-term fading loss 9

L_{meas} Measured path loss 26

L_{PL} Path loss 7, 10, 17

L_{RX} Receiver loss 7

L_S Short-term fading loss 9

L_{TX} Transmitter loss 7

n Path loss exponent (CI model) 16, 41, 42, 47

P_{avg} Average signal power 40–42

P_I Interference power 6

P_{max} Maximum signal power 40, 42

P_{min} Minimum signal power 40–42

P_N Noise power 6

P_{RX} Interference power 6, 7, 24, 26

P_s Signal power 6

P_{th} Threshold power 6

Abbreviations

3GPP 3rd-Generation Partnership Project 3, 5, 16, 23, 65

4G Fourth-Generation 19, 21

5G Fifth-Generation 1, 3–5, 17, 19, 21, 26, 63

ABG Alpha-Beta-Gamma model 15–17, 41, 44, 47, 50, 61

API Application Programming Interface 2, 19

BS Base Station 4, 6

CAD Canadian Dollars 22

CCTM Canadian Cellular Towers Map 22–24, 26

CGI Cell Global Identifier 4

CI Close-In model 16, 17, 41, 44, 47, 50

CIF CI model with a frequency-weighted path loss exponent 17

CIRA Canadian Internet Registration Authority 1

CRTC Canadian Radio-television and Telecommunications Commission 1

DL Downlink 4, 5

EIRP Effective Isotropically Radiated Power 23

EWABG Extended Weighted ABG 17

GPS Global Positioning System 2, 18, 23, 25, 53, 55, 61

ISED Innovation, Science, and Economic Development Canada 23

ISP Internet Service Provider 4–6, 19, 23, 26, 64

ITU International Telecommunications Union 3

LAI Location Area Identification 4

LOS Line-of-Sight 8, 18, 22, 25, 28, 41, 45, 47–50, 52, 53, 55, 61

LTE Long-Term Evolution 1, 4, 5, 11, 17–19, 21, 58, 60, 63, 66

MCC Mobile Country Code 4

MIMO Multiple-Input-Multiple-Output 10

MMSE Minimum Mean-Square Error 16

MNC Mobile Network Code 4

MSP Mobile Service Provider 1

NLOS Non-Line-of-Sight 8, 18, 25, 41, 48–51, 55, 61

OSI Open Systems Interconnection 3

PLE Path Loss Exponent 16

RSRP Reference Signal Received Power 5, 18–22, 25, 26, 42, 47, 49, 51, 52, 60, 62, 66

RSRQ Reference Signal Received Quality 5, 19, 56, 62

RX Receiver 18

SINR Signal-to-Interference-Plus-Noise Ratio 6

SNR Signal-to-Noise Ratio 6

TAC Tracking Area Code 4

T-R Transmitter-Receiver 6, 13–16, 55

TS Technical Standard 5

UE User Equipment 3, 21, 22, 26, 58

UL Uplink 4, 5

UMa Urban Macrocell 17

UMi Urban Microcell 17

Chapter 1

Introduction

Canadians are experiencing ever-greater reliance on mobile devices, with users exceeding an average of 4.4 hours per day using mobile applications in 2021 [1]. In 2019, the Canadian Radio-television and Telecommunications Commission (CRTC) estimated [2] that 88% of Canadian households subscribe to mobile services, while the Canadian Internet Registration Authority (CIRA) reported [3] that 75% of users in Canada accessed the internet via mobile device, with 90%, 60%, and 58% spending online time responding to emails, using social media, and accessing news updates, respectively. Reports from major industry players, such as the 2022 Ericsson Mobility Report [4], likewise predict that 91% of the North American cellular market will have adopted Fifth-Generation (5G) technology by 2028, and that 80% of mobile data already consists of video traffic. It is reasonable to assume that more complex and demanding use-cases are yet to be realized. Fortunately, the ongoing transition from 4G to 5G standards offers wireless speeds previously only obtainable through wired networks and specialized test equipment, expanding the range and quality-of-service available to users.

However, obstacles to improving the cellular experience are often counterintuitive challenges. For example, previous efforts by Mobile Service Provider (MSP) to expand their networks and meet demand have sometimes resulted in even greater congestion, as users take advantage of higher speeds to use more demanding services and at greater frequency [5]. Wireless networks are also increasingly being selected to host critical infrastructure services. The CRTC requires service providers to broadcast emergency messages as part of the National Public Alerting System [6], which includes mobile devices with access to Long-Term Evolution (LTE) infrastructure. This raises the need not only for better speed and coverage, but also relability. A BC Hydro report [7] from November 2021 highlights consumer reliance on mobile devices in emergency situations, suggesting that 70% of British

Columbia's residents consider cell phone access "important" or "very important" in such scenarios. Similarly, in 2018 the CBC published an article [8], which outlined the vulnerabilities of local wireless infrastructure, and the increased network congestion experienced in 2018 by the cities of Ottawa and Gatineau, in the wake of a severe storm. The latter article states that the capacity of backup batteries for mobile systems varies widely, from "two hours to four hours" from typical installations, up to 24 hours for critical infrastructure, depending on network traffic. Although other vulnerabilities may play a role, these alone suggest that collection and publication of detailed network quality statistics at the local, regional, and national levels may improve response to future disasters.

Testing and measurement of wireless systems is typically performed in a laboratory environment. Under these conditions, the research group has a fine-degree of control over an experiment. Access to combinations of expensive, advanced tools including anechoic chambers, software-defined radio modules, vector network analyzers, propagation modeling software, and prototype equipment allow precise measurement of mobile channel characteristics, offering a clear picture of the user experience under ideal conditions. However, real-world environments are subject to numerous additional factors that are not organically produced in the lab (e.g. distance, multi-directional interference, and obstructions), and which may play a significant role in system performance. The aforementioned use of costly measurement devices also means that fewer total test suites and configurations may be available.

Using cell phones in lieu of more specialized test equipment provides a few advantages. First, it allows collection of data as the mobile device itself sees it, rather than idealized or simulated versions. Second, smart phones' ubiquity and portability enable more varied, frequent tests, with relatively little prior setup or planning required compared to network analyzers and other hardware. Finally, it also significantly reduces the experiment's cost, due the aforementioned availability of cell phones and access to mobile applications that are inexpensive compared to commercial test systems. The data produced by this approach can then be used in novel applications, including being automated or analyzed with artificial intelligence algorithms to draw new insights.

A notable example which collects data in this way is Google Maps and its many associated Application Programming Interface (API) options. Crowdsourced device positions, velocities, Global Positioning System (GPS) accuracy, and other location metrics are used in real-time applications to monitor traffic delays, suggest alternative routes, track deliveries, and plan travel, while databases allow browsing of historical trends. Programs revealing low-level system characteristics such as received signal power by position also exist with corresponding public databases. Using these tools' outputs in conjunction with theoretical analysis of the results via modern path loss models is the subject of this thesis.

1.1 Cellular System Architecture

Efforts to predict and overcome the radio propagation channel's influence on user experience are ubiquitous in wireless communications research, with applications including television, navigation, and satellite communications. A variety of concepts and equations have evolved from this research to allow increasingly-sophisticated cellular systems to be designed. Much contemporary research is focused on the growth of Fourth-Generation (4G) and (5G) mobile networks, which are in turn defined by organizations such as the 3rd-Generation Partnership Project (3GPP) and International Telecommunications Union (ITU).

Mobile systems are intended to provide Internet services to users by maximizing coverage and performance for connected devices. This is achieved by deployment of wireless infrastructure strategically in target areas. The exact manifestation of this is influenced by numerous factors. Some of these include user density, environmental properties, proximity of other telecommunications infrastructure, industry standards, aesthetics, and purpose (e.g. shopping or business parks, public events). Figure 1.1 shows the Open Systems Interconnection (OSI) model for computer technology. Despite extensive attention given to functions such as encoding, device authentication, etc. found in the upper levels, the propagation environment (part of the physical layer) remains a primary challenge for mobile systems performance, and is the focus of this thesis.

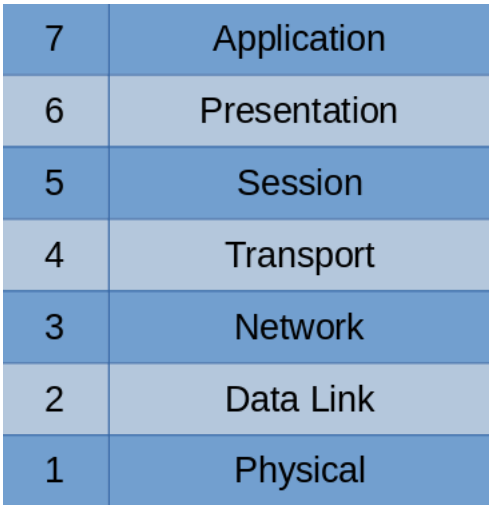


Figure 1.1: OSI Model Layers

Figure 1.2 shows a high level view of the cellular system. A User Equipment (UE) (also

referred to as "nodes") represents mobile devices such as cell phones and tablets. A Base Station (BS) consists of one or more wireless transceivers. Radio transmissions between the BS and UE are bidirectional, i.e. both Downlink (DL) and Uplink (UL) occur. These cell sites can be located within or adjacent to their designated coverage zones, situated on existing or standalone structures (e.g. residential buildings or "masts"). They are connected by cable or wireless links to the core network, which is comprised of devices that manage the overall system, providing services such as device authentication, performance monitoring, and connectivity to the wider internet.

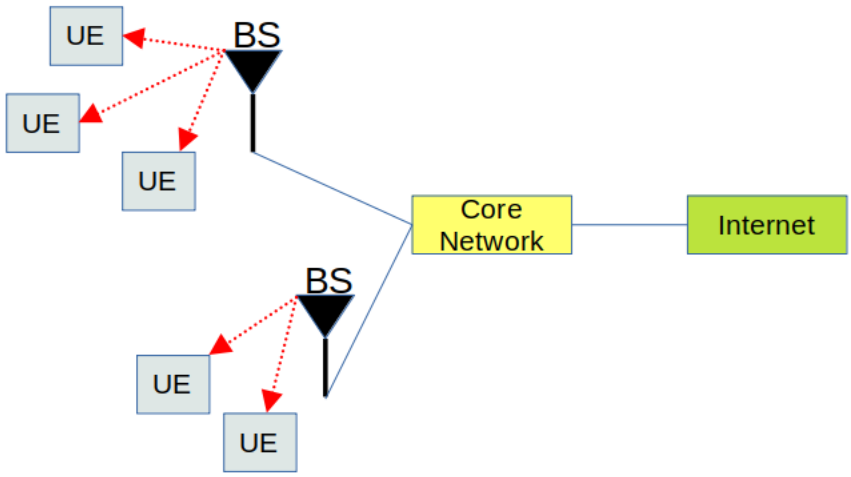


Figure 1.2: Cellular System Diagram

An LTE or 5G base station's coverage can vary with the Internet Service Provider (ISP) and their requirements for a given service area. A cell tower often hosts multiple co-located transceivers that serve adjacent cells. One way in which each cell is distinguished by the network (and the user device) is with the use of a Cell Global Identifier (CGI) [9], which is a composite of four separate identifiers: Mobile Country Code (MCC) which indicates the operating country; Mobile Network Code (MNC) which identifies the specific ISP's infrastructure; Tracking Area Code (TAC) (alternatively, Location Area Code or LAC), indicating a local area within the mobile network; and Cell Identity (also referred to as a Cell ID), which denotes the actual base station. The first three codes may collectively be referred to as the Location Area Identification (LAI). The combined CGI is a globally-unique ID.

Several identifying characteristics are associated with the CGI, but a particularly important one is the cell's operating band, which is associated with fundamental signal characteristics such as the carrier frequency and bandwidth. In practice, most of these signal

bands sit within a small spectrum of frequencies and have separate ranges for DL and UL operations; however, for simplicity a single carrier frequency is often used in analysis. 3GPP publishes the standard mapping between the operating band, frequencies, and bandwidth in [10]. Examples of some cell bands used in Ottawa, Canada are given in Table 1.1.

Table 1.1: Common Cell Bands in Ottawa, Canada

Band	f (MHz)	UL (MHz)	DL (MHz)
2	1900	1850-1910	1930-1990
4	2100	1710-1755	2110-2155
7	2600	2500-2570	2620-2690

In outdoor environments, there are typically four cell sizes [11]:

1. Femto (10 m to 50 m)
2. Pico (100 m to 300 m)
3. Micro (250 m to 1 km)
4. Macro (over 1 km radius)

The rapid expansion of LTE and 5G networks has spurred increased interest towards smaller cell sizes to aid ISPs in providing reliable service to customers. Compared with the macrocell, small cells have numerous advantages, from lower power consumption to higher network capacity, in addition to being more easily integrated into their environment. These cell ranges are only typical values, and in practice UEs will not always experience consistent service quality from the same base station. Although network loading due to excessive device counts or system outages can be responsible, this is often a consequence of the cell environment influencing the radio signal.

Regardless of cell type, development and measurement of network parameters that can indicate the wireless system's health are critical. Contemporary mobile devices track a number of performance metrics for nearby cells. One of these is the Reference Signal Received Power (RSRP), defined in 3GPP Technical Standard (TS) 36.214 as "the linear average over the power contributions (in [W]) of the resource elements that carry cell-specific reference signals within the considered measurement frequency bandwidth" [12, p. 9]. This quantity is used to calculate Reference Signal Received Quality (RSRQ) [12, p. 10],

which factors into handover procedures between cells when thresholds are met according to the ISP network's configuration [13].

With the growing complexity of mobile networks, system designers must be efficient in deploying the necessary infrastructure. Modeling of the wireless propagation channel provides a means to predict system behavior and determine whether proposed BS location, signal power, antenna configuration, cell band, and other parameters will be sufficient for users' needs. What follows is an overview of the theory behind radio propagation, along with the challenges presented by the conditions wireless systems operate under.

1.1.1 Threshold Effect and Receiver Sensitivity

Cellular systems are designed with a minimum expected signal strength for operation. Below this value, the system performance is degraded and an outage may occur. This is a threshold effect, where the Signal-to-Noise Ratio (SNR) is compared against a threshold value to determine if minimum system requirements are met. The SNR is defined as:

$$SNR = \frac{P_s}{P_N} \tag{1.1}$$

where P_s is the signal power and P_N is the environment's noise power. A more complete measure which accounts for the contribution of interfering signals (P_I) is the Signal-to-Interference-Plus-Noise Ratio (SINR) ratio:

$$SINR = \frac{P_s}{P_I + P_N} \tag{1.2}$$

For a given system's threshold power P_{th}, satisfactory behavior is achieved when received power $P_{RX} \geq P_{th}$, or equivalently $SINR \geq SINR_{th}$. The situation where P_{RX} falls below the threshold is called an outage event.

The lowest level where a signal can be received is known as the receiver sensitivity [14]:

$$P_{sens} = kT_nBN_f \tag{1.3}$$

where $k = 1.3806504 \times 10^{-23} J/K$ is Boltzmann's constant, T_n is the temperature in Kelvin, B is the bandwidth, and N_f is the noise figure of the system. For example, assuming $T_n = 290$ K, $B = 5$ MHz, and $N_f = 9$ dB, $P_{sens} = -98$ dBm.

1.1.2 Link Budget

Modeling the factors affecting the SNR of a cellular system is key to predicting performance. The simplest model for wireless propagation is a radio signal with carrier wavelength λ (in meters), propagating away from the antenna towards a similar receiving antenna located at a distance d (known as the Transmitter-Receiver (T-R) distance), as shown in Figure 1.3.

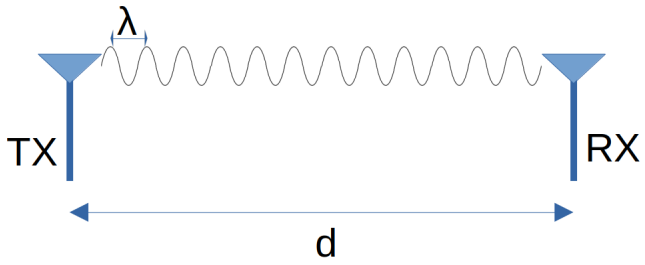


Figure 1.3: Transmitter-Receiver Propagation Diagram

In the "far field" of propagation $d \gg \frac{2D^2}{\lambda}$, where D is the maximum antenna dimension, this scenario is governed by the Link Budget Formula:

$$P_{RX} = P_{TX} \frac{G_{TX} G_{RX}}{L_{TX} L_{RX} L_{PL}} \quad [\text{W}] \tag{1.4}$$

where P_{TX} and P_{RX} are the transmit and received powers in W, G_{TX} and G_{RX} are the respective antenna gains, while L_{TX} and L_{RX} represent losses such as impedance mismatch at the transmitter and receiver, respectively. The last term, L_{PL}, is the path loss, defined as "the reduction in power density of a radio wave as it propagates through the channel" [15]. Figure 1.4 shows the block diagram for a wireless system, where each component is labeled with the corresponding parameters from Equation (1.4). Radio signals emitted from the transmitter are first transformed (shifted) by the losses when connecting via cable to the antenna array. It is modified again by the propagation channel before reaching the receiver, where (following similar losses due to the equipment) it is processed.

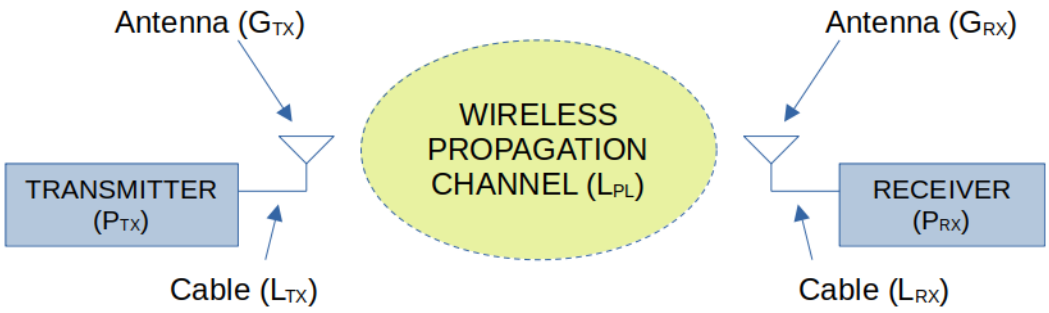


Figure 1.4: High-Level Wireless System Diagram

1.1.3 Propagation Mechanisms

The direct Line-of-Sight (LOS) propagation scenario in Figure 1.3 is an idealized case that does not fully represent the effects real-world environments. Under realistic conditions, a radio wave may encounter multiple obstacles between the transmitter and receiver. There are three additional propagation modes that affect the received signal:

1. Reflection/Refraction
2. Scattering
3. Diffraction

Figure 1.5 shows an example of reflection in the case where a LOS path between the transceivers is available. The ground in this scenario causes the signal reflection, but any sufficiently large surface could serve the same role. In addition to the direct signal path, the wave may be reflected, causing multiple versions of the original signal to be detected by the receiver. Depending on the transmit frequency, the radio signal may also be refracted (i.e. bent) relative to its original path when encountering a change in the propagation medium (e.g. different layers of the atmosphere). Scattering effects behave similarly to reflection at a smaller scale, in that lesser objects with size less than the wavelength can reflect the signal in multiple directions.

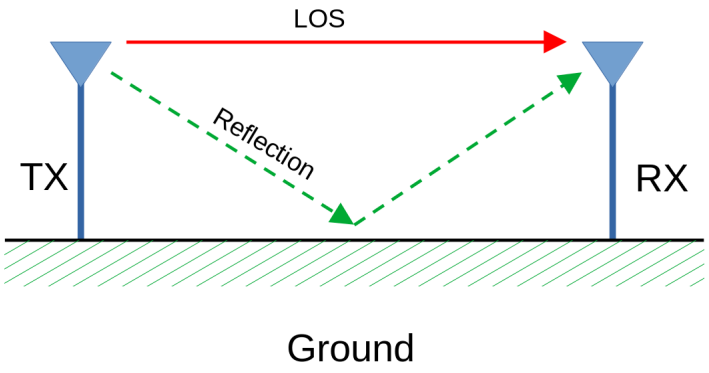


Figure 1.5: Two-Ray (Ground Reflection) Propagation Diagram

A depiction of reflection and diffraction is given for the Non-Line-of-Sight (NLOS) scenario in Figure 1.6. As before, reflected signals arrive at the receiver from an indirect path, while the direct line is blocked. Diffraction occurs in this environment where edges of obstructions (e.g. buildings) are found. While the obstacle is too large for the signal to penetrate it and may be reflected or absorbed, sufficiently sharp edges of the structure can bend the signal, allowing continued propagation on the other side.

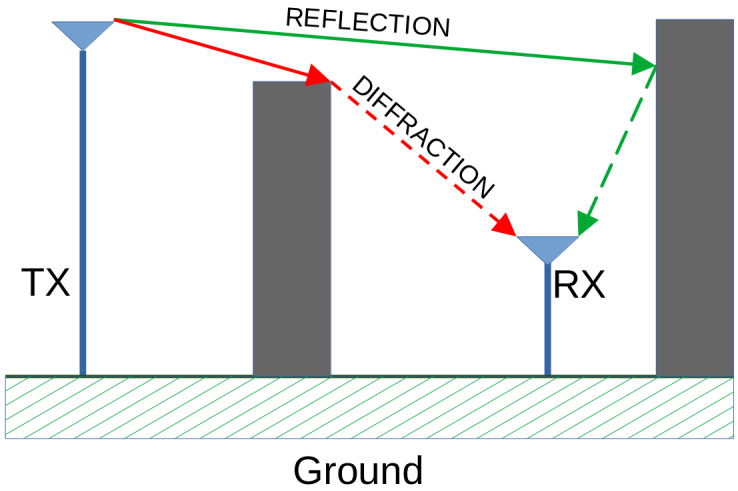


Figure 1.6: NLOS Propagation Diagram

1.1.4 Fading

Real-world environments often incorporate a combination of the propagation conditions from Figure 1.5 and Figure 1.6, along with other interfering channel phenomena. As a consequence, the final signal characteristics at the receiver can deviate drastically from the original transmission. "Fading" is the term for fluctuating received signal power caused by changes propagation conditions (such as path length and frequency) between transceivers. There are two main types of fading effects on the propagation channel from the time-domain perspective:

1. Short-term (L_S)
2. Long-term (L_L)

In Figure 1.5 and Figure 1.6, as a consequence of the various paths taken by the radio wave, the received transmission is a composite of multiple phase-shifted and attenuated versions of the original signal. Constructive and destructive interference resulting from their sum can drastically alter the power observed at the receiving antenna. Short-term fading, also known as "multipath" or "small-scale" fading, is the term for how this effect varies over time for the propagation channel. Depending on how quickly the transceivers are moving, multipath fading can be observed over seconds or less (alternatively, on the order of the carrier wavelength [16, p. 10]).

Long-term fading, also called "large-scale" or "shadowing", is the time-varying influence of large obstacles and environmental characteristics on the received signal power. Structures that are many orders of magnitude greater than λ (e.g. buildings, earthworks) affect the propagation channel in this way. The result is a gradual fluctuation in observed power, in addition to multipath effects and the expected free-space attenuation due to distance. Figure 1.7 provides an example of how long-term and short-term effects may influence a signal's amplitude as a function of time.

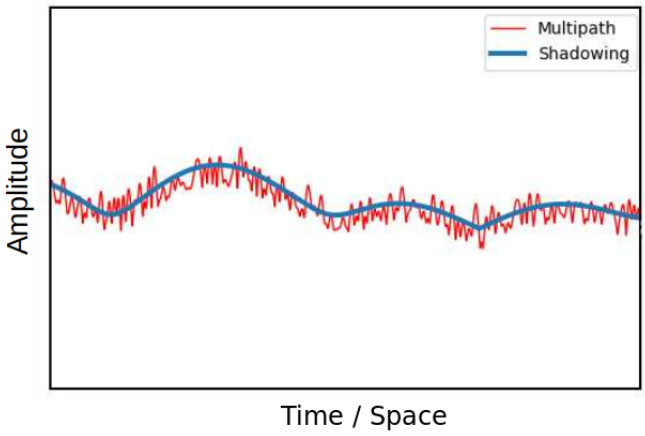


Figure 1.7: Effects of Fading on Signal Amplitude

Both fading effects are part of L_{PL} in Equation (1.4) along with the "average" (e.g. free space) loss, L_0 as in [17]:

$$L_{PL} = L_0 L_S L_L \tag{1.5}$$

From the user's perspective, the influence of fading effects can result in reduced throughput and signal quality. These phenomena are largely out of system designers' control, as the propagation environment typically cannot be altered in order to guarantee LOS conditions and a lack of reflecting and/or scattering obstacles. However, there are ways to compensate for these effects. One mitigation technique is the use of Multiple-Input-Multiple-Output (MIMO) technology [18], which uses a combined space-time signal processing approach by incorporating multiple transmit and receive antennas (along with the appropriate coding and/or modulation schemes), ultimately reducing the influence of some channel effects, and improving data rate and signal quality.

1.2 Summary of Contributions

There were three main contributions derived from this work. The first was to design and test an experiential technique for collecting and validating the end-user experience of devices served by mobile networks. This method focused on using a smartphone as the measurement device, exporting signal data obtained using a freely-available Android-based

mobile application, and comparing the results against common, industry-standard path loss models. As a consequence of the data acquisition method, the experiment is low-cost and low-complexity, since the only equipment required is one or more Android mobile devices with LTE support, which are widely available and significantly less-expensive than typical laboratory measurement equipment. With this technique, a qualitative validation of the models was performed as seen by devices that are representative of the real user experience. This demonstrated the method's accessibility for mobile communication systems research and provided a blueprint for expansion with additional analytic tools such as machine learning algorithms. While there were no new models presented as a result of the research, this method showed the possibility for developing them using mobile devices in the future.

The second contribution was a simplified version of the technique, organized as an undergraduate research laboratory, which may be piloted at the University of Ottawa. This lab will provide students with a practical understanding of challenges to wireless network design by enabling them to compare real-world measurements against contemporary propagation models. In addition to the advantages this realistic experimental method provides for learning purposes, it has the secondary benefit of being easily extendable to larger projects and research concepts.

The third and final contribution was a prototype software tool for analyzing the collected data, known as Routesignal. This is an open-source, freely-available application with a permissive license allowing for potential extension and modification, written using the popular Python 3 programming language. Routesignal provides a blueprint for how the aforementioned data and theory can be combined by researchers to gain new insight into mobile network design.

1.3 Thesis Outline

The organization for this thesis is as follows:

Chapter 2 provides a brief review of common path loss models used as part of this research. Theoretical and experimental varieties are presented, including any functional limitations. Finally, a recent publications in the field are reviewed, focusing on outdoor propagation model usage and cellular system performance as observed by a mobile device.

Chapter 3 details the experimental method used in the thesis. Criteria for data acquisition, mobile infrastructure identification, and environment characterization are provided, including limitations and value of different spaces (e.g. urban vs rural) for the experiment. A tactic for validating infrastructure observations is given. Similar options are provided

for comparing observed cells against online databases, while acknowledging that such data is not always guaranteed to be available.

Chapter 4 covers the extensive results obtained using the method of Chapter 3, for two different environments in Ottawa, Canada. Statistics for the primary data are tabulated, along with relevant geolocation metrics. A subset of the observed cells is chosen, then described in order of sample size. This includes comparison between subsequent cells where appropriate. An attempt is then made to qualitatively match the calculated path loss for each cell to the models touched on in Chapter 2. This is done using visual approximation of the models' parameters using the Routesignal user interface.

Chapter 5 provides an outline for how the method of Chapter 3 could be condensed into a format for hardware-based lab experiments such as those in the course ELG4179: Wireless Communication Fundamentals at the University of Ottawa. This takes advantage of the technique's convenience to provide students with realistic data from a representative source, instead of requiring laboratory equipment that is often unavailable. Suggestions for preliminary questions and study are also given. A more detailed example (contained in the appendices) is then referenced.

Chapter 2

Review of Propagation Channel Models

2.1 Theoretical Models

2.1.1 Free Space Model

The simplest propagation model is the free space model as described in Equation (2.1) [14]:

$$L_{FS} = \left(\frac{4\pi d}{\lambda}\right)^2 \tag{2.1}$$

where λ is the wavelength and d is the T-R distance (both in meters). It describes the signal's attenuation with distance from the transmitter, in the absence of interference, obstacles, or contributing factors, and is used as an ideal-case model for radio propagation. It may also be expressed as a function of frequency f (Hz) as:

$$L_{FS} = \left(\frac{4\pi df}{c}\right)^2 \tag{2.2}$$

where c is the speed of light in m/s.

2.1.2 Two-Ray Model

A common alternative to the free-space model for path loss is the two-ray or ground reflection model [14]:

$$L_{TR} \approx \frac{d^4}{h_{TX}^2 h_{RX}^2} \tag{2.3}$$

where d, h_{TX} and h_{RX} are all in meters. This considers the influence of both the direct LOS path and a single dominant reflection in the received signal shown in Figure 1.5. The two-ray model is an approximation, valid beyond a critical distance d_c defined as:

$$d \geq d_c = \frac{4\pi h_{RX} h_{TX}}{\lambda} \quad \text{[m]} \tag{2.4}$$

where λ is the signal wavelength, again in meters.

2.2 Semi-Empirical Models

2.2.1 Okumura-Hata Model

The empirically-based Okumura-Hata model (also known simply as the Hata model) was developed by Hata in 1980 [19]. It is based on measurements collected by Okumura in 1968 [20], and attempts to account for the effects of propagation conditions such as those in Figure 1.5 and Figure 1.6 due to large obstacles in urban and suburban areas. For the urban propagation scenario, it is expressed as:

$$\begin{aligned} L_{urban} = {} & 69.55 + 26.16\log(f) - 13.82\log(h_{TX}) \\ & -a(h_{RX}) + (44.9 - 6.55\log(h_{TX}))\log(d) \end{aligned} \quad \text{[dB]} \tag{2.5}$$

where:

- f is the frequency (MHz)
- h_{TX} and h_{RX} are the base station and mobile device heights (m)
- d is the T-R distance (km)

- $a(h_{RX})$ is the correction factor

The correction factor is determined based on the urban environment's size:

$$a(h_{RX}) = \begin{cases} 3.2(\log(11.75h_{RX})^2 - 4.97, & f \geq 400 \\ 8.29(\log(1.54h_{RX}))^2 - 3.69, & f \leq 200 \end{cases} \tag{2.6}$$

with $a(h_{RX}) = 0$ for $h_{RX} = 1.5$ m. In a small city, $a(h_{RX})$ is

$$a(h_{RX}) = (1.1\log(f))h_{RX} - 1.56\log(f) + 0.8 \tag{2.7}$$

The Okumura-Hata model also has correction factors for suburban and rural environments K_r and Q_r, which result in the expressions:

$$L_{suburban} = L_{urban} - 2(\log\frac{f}{28})^2 - 5.4 \quad [\text{dB}] \tag{2.8}$$

and

$$L_{rural} = L_{urban} - 4.78(\log(f))^2 + 18.33(\log(f)) - 40.94 \quad [\text{dB}] \tag{2.9}$$

The Okumura-Hata models are considered valid under the following conditions:

$$\begin{cases} 1 \leq h_{RX} \leq 10 & \text{m} \\ 30 \leq h_{TX} \leq 200 & \text{m} \\ 1 \leq d \leq 10 & \text{km} \\ 150 \leq f \leq 1500 & \text{MHz} \end{cases} \tag{2.10}$$

2.2.2 Alpha-Beta-Gamma Model

The statistical Alpha-Beta-Gamma model (ABG) [21] [22] is a mathematical solution (rather than being based on physics or empirical measurements) designed for predicting large-scale path loss:

$$L_{ABG} = 10\alpha\log\frac{d}{1\,\text{m}} + \beta + 10\gamma\log\frac{f}{1\,\text{GHz}} + \chi_\sigma^{ABG} \quad [\text{dB}] \tag{2.11}$$

where:

- d is the 3D T-R distance, with $d \geq 1$ m

- α is the distance-dependence coefficient
- β is an offset parameter in dB
- γ is the frequency-dependence coefficient
- f is the frequency in GHz
- χ_σ^{ABG} is the shadowing factor, represented as a Gaussian random variable with mean zero and standard deviation σ in dB

The ABG model is an extension of a previous model without the γ parameter, known as the alpha-beta (AB; alternatively "floating intercept") model, and is used as part of 3GPP channel simulation [23]. Neither is based on theoretical or experimental results, and instead "are determined by finding the best fit values to minimuze the error between the model and measured data" [22]. Unlike the two-ray and Okumura-Hata models, the ABG's inclusion of χ_σ^{ABG} allows it to depict shadowing effects over distance as well.

2.2.3 Close-In Model

The Close-In model (CI) model is a statistical model like the ABG [22]:

$$L_{CI} = L_{FS}(f, 1\text{m}) + 10n \log(d) + \chi_\sigma^{CI} \quad [\text{dB}] \tag{2.12}$$

where:

- n is the Path Loss Exponent (PLE), which is determined according to [24]
- d is the T-R distance in meters
- χ_σ^{CI} is the shadowing factor as with Equation (2.11)
- $L_{FS}(f, 1\text{m})$ is the free-space path loss with reference distance $d_0 = 1$ m

Unlike the ABG, however, the CI model has a physical basis. Its PLE parameter is determined from a Minimum Mean-Square Error (MMSE) fit to the measured data and is inspired by the presence of exponents in the free-space and two-ray models. If α of the ABG model is set equal to n in the CI, $\beta = 20 \log \frac{4\pi}{c}$, and $\gamma = 2$, then the two models are equivalent. The model's frequency dependence is well within the antenna near-field

when $d_0 = 1$ m[1], and is shown to provide good accuracy for outdoor scenarios and various frequencies in [21] [22].

2.3 Modern Models

Many publications on mobile communications in recent years have been focused specifically on the validation of path loss models for simulating LTE and 5G performance. In Sun et al [21] [22], the aforementioned ABG, CI, and CI model with a frequency-weighted path loss exponent (CIF) models are evaluated for their stability in modeling various indoor and outdoor signal measurements. Other recent examples are the CIF [25] and Extended Weighted ABG (EWABG) [26], both of which are variations on models previously described (CI and ABG, respectively). Additionally, there are other path loss models published by standards bodies, such as 3GPP, for specific propagation scenarios, e.g. Urban Microcell (UMi), Urban Macrocell (UMa) models for street canyons with base stations nearby and below roof height, and open spaces with roof-mounted cells at greater distances, respectively [27]. The UMa data came from two campaigns by Nokia/Aalborg University (AAU) in Denmark and the University of Texas at Austin (UT Austin), respectively; while UMi measurements were acquired by Qualcomm and NYU; collectively they covered a range of frequency bands from 2 to 73 GHz. The data's environment was described as a typical urban space, with base station heights (mounted on buildings) up to 25 m in the first scenario and 36 m in the second. Their conclusion was that all three models provide similarly good estimations of the channel behavior, with at most 1.2 dB difference between their respective standard deviations, and with the CI model being particularly appealing for its single-parameter dependency and stability across propagation frequencies. Considerable time is spent in each paper justifying the latter's use of $d_0 = 1.0$ m as being based on the same physical principles (i.e. frequency dependence) as the Friis equation, described earlier in this chapter, while also noting that older propagation models used reference distances of 100 m or even 1 km, based on less-obstructed environments and wider coverage areas [21].

Additional research by the same authors [23] [24] [28] [29] involved similar validations of these propagation models. In particular, Haneda et al [29] highlights the degree of interest and industry involvement in this approach, with fifteen different organizations and corporations included in the author list (as well as over 30 individual contributors). Although focused primarily on frequencies above 6 GHz, which are beyond the capabilities of most current consumer devices, the technique presented (along with what lower-frequency

[1] where the free space path loss at $f = 2600$ MHz (for example) is $L_{PL} = 40.74$ dB.

results are given) remains useful. This experimental methodology is fairly well-defined. In the Aalborg University portion of the data (which was the only campaign where sub-6 GHz frequencies were tested), a van-mounted receiver traversed the chosen campaign area at a known pace and compared received signals against known transmissions at multiple distinct locations and frequencies. Notably, they also used imagery from Google Maps to classify the measured data as LOS or NLOS.

Similarly, in Milanovic [30], the Walfich-Ikegami, Ericsson, and SUI models' predictions are compared against data collected in the city of Osijek, Croatia over mixed urban and suburban conditions similar to those discussed earlier. Fairly typical parameters for h_{TX} ($22 - 50$ m), h_{RX} (1.7 m), P_{TX} (40W), and G_{TX} (16-17.5 dBi) were observed for an LTE signal operating at 1800 MHz. A modest total of 78 RSRP measurements were taken using Rohde & Schwarz "drive-test" equipment across the city, with a software tool "Cellular Expert", and then plotted in logarithmic form against the models over distance. While this work successfully incorporates realistic environments and wireless infrastructure (from an unknown service provider), it again makes use of specialized test equipment to achieve this, and is vague on the path and rate of progression.

While such work implies the usefulness of these modern path loss models in predicting urban propagation behavior, the procedures used in the experiments are not from the perspective of an actual mobile device and involve significantly different hardware. These papers, and the initial Aalborg University study [31], describe the measurement setup as consisting of two Receiver (RX) dipole antennas (one static at 2 GHz, the other variable) mounted atop the campaign vehicle, where the received signal is sampled (along with GPS data) at 10 samples per second using a specialized radio network analyzer. Although adjusted such that some parameters (e.g. RX height versus that of the typical mobile device) are comparable, there are still many points where this technique may be more idealistic than what is experienced by the real end-user. For example, while the received signal in the Aalborg scenario is measured in a representative urban environment and may be influenced by any number of other nearby wireless services operating on similar frequency bands, the test setup doesn't necessarily account for the variability caused, for example, by loads both on the real mobile network and the user device themselves. Additionally, the general design, acquisition, and/or deployment of the test configuration may be hampered by the need to calibrate it against realistic usage scenarios, such as with the operational height and antenna setups mentioned previously. This validation process could be made more useful by being made more easily replicable.

The use of cell phones to obtain coverage data was previously explored by Al-Shasimi [32]. In that work, the authors carried out a comparison between measurements collected with two mounted and stationary smartphones, and a scanner in flat, suburban surround-

ings. Data was obtained using a mobile application for the devices known as "LTENetScan" and a statistical analysis was performed using MATLAB. The findings show that the smartphones under test reported average received power levels slightly lower (approximately 2 dB) than the scanner with LTENetScan, but also that they generally provided accurate and stable RSRP measurements. The conclusion is ended by suggesting the development of coverage maps with such measurements as a low-cost, easier process than using traditional drive-test methods for the same purpose.

Measurements available via cell phones' low-level signal APIs appear to allow a more comprehensive study of LTE and future 5G network performance, without necessarily requiring the drive-test equipment seen in other examples. Their ubiquity and standalone designs make them much simpler to design test campaigns around. These reasons alone may lead to better insight when validating new models and network algorithms; but there are other applications as well. Open databases such as [33] and [34] provide identification, coverage, and other performance data for wireless networks as reported by user devices. Although their respective presentations differ and focus on different characteristics, such approaches offer up considerable amounts of data up for analysis, and represent an interesting heuristic for validating propagation models if the channel environment can be properly described.

Previous research on crowdsourced (also "crowdsensed") mobile network performance [35] [36] gives some insight. [36] focused primarily on spectrum usage for Fourth-Generation (4G) networks and urban deployment status by ISPs (here called Mobile Network Operators or MNOs) for the London, UK area in 2017. However, it also measured and analyzed the RSRP and RSRQ, finding that the former performed better at higher frequencies and the latter showing an inverse relationship with network usage (i.e. RSRQ was higher with less cell traffic). The CellMapper database [33] and associated mobile app were utilized to obtain this result, displaying the potential usefulness of smartphones as surveying tools. Raida et al [35] is an older (but more relevant) crowdsourcing example, exploring the general utility and tradeoffs of using mobile devices for cell network testing. Specifically, it highlights the as-of-yet undiscussed downsides of doing so, such as bias of users against using limited data resources on benchmarking tests or the number of possible distinct test scenarios ($30 \cdot 10^{12}$) at play when all predictors are considered. The authors performed simulations and measured real data to conclude that network throughput prediction was made more reliable by the inclusion of crowdsourced data, avoiding unrepresentative measurements in the process (such as what might be caused by only measuring at certain times of day or user speeds). Once again, various mobile applications are used to obtain this information, however, the time scale for the experiment is on the order of months.

Given calibration methods for mobile signal data (such as described in [32]), control of

an application that can perform tests and report outcomes, and knowledge of propagation models developed by industry standards bodies, a novel technique for wireless network validation appears possible. One remaining obstacle to these databases and applications is access to the raw data as reported by the device. CellMapper, for example, focuses on uploading new measurements to the crowdsourced platform and therefore limits the parameters and/or binning that researchers could use in their analysis. An alternative called Network Cell Info Lite [37] provides this capability, allowing export of received signal and cell data in multiple database formats. Using this to collect received power data over a local area and then analyzing the measurements with an appropriate software tool may be a more direct means to compare the models' performance against actual RSRP values for a given environment, device, network configuration, etc. within the wireless propagation environment as observed by devices that everyday users possess.

With possession of such a simple technique, received signal data would be readily obtainable, and the process could be easily repeated over many different environments, conditions, and time intervals to obtain very large datasets. Statistical analyses, visualization, and cutting-edge analysis tools such as machine and deep learning algorithms could then be applied to large amounts of data crowdsourced this way, providing realistic insight into mobile systems' performance in specific conditions and the prediction thereof. This could also have unconventional applications as well, e.g. detection and mitigation of false base stations (as described in Karacay et al [38]) and other information security risks. A template for combining these experimental concepts will be presented and explored in the following chapters.

Chapter 3

Methodology

The purpose of these experiments is to validate common radio propagation models using the most representative data source - i.e. mobile phones and existing network infrastructure. To do this, we will measure the device's RSRP over an extended walk through an accessible area. The smartphone's camera will be used to collect imagery of possible base stations for cross-referencing against Google Maps or other services for location validation. With a sufficient number of RSRP observations, the observed path loss can then be compared against the models of Chapter 2. Coverage maps can also be generated with the RSRP data to infer specific surroundings' effects on the results and provide an alternative perspective.

3.1 Setup

3.1.1 Device Selection

Test equipment is selected based on three criteria:

1. Relevance
2. Portability
3. Cost

Using LTE-capable cell phones means that the UEs have representative hardware specifications and utilize recent wireless network services (i.e. 4G and 5G) in the area. This

reduces the researcher's control over the environment in comparison to a more typical wireless test lab setup, but as a result it provides a way to check path loss models for real-world scenarios. This also achieves the portability requirement, as most devices are pocket-sized and therefore require no special fixtures, while the base stations are already present and require no setup from the user. Finally, they also make the process inexpensive (in contrast to the specialized equipment of the laboratory environment) for the same reasons, with cell phones available at $200 Canadian Dollars (CAD) or lower.

3.1.2 Data Acquisition

A software application is required to access the UE's low-level network API and expose received signal characteristics for study. The same general requirements for device selection also apply here. At minimum, this would include tracking time series of RSRP and other performance metrics, with accompanying geolocation data. Datasets collected in this manner also must be exportable in a format that can be processed and visualized. Additional features such as bitrate, cell site info, and coverage prediction, while not required, are highly desirable.

3.1.3 Base Station Identification

This experiment is heavily-dependent upon accurate estimation of the signal origin. There are two possible approaches:

1. Manually record tower locations and their surrounding environment using the built-in camera;
2. Use resources such as Google Maps to locate entries in the Canadian Cellular Towers Map (CCTM) [39]

The manual approach may be the more reliable option, since the latter is not guaranteed to provide up-to-date imagery and therefore may not reflect the same environmental context (e.g. new construction blocking LOS at a certain distance). A reasonable assumption is that cell towers in suburban and rural areas (which tend to be large, brightly-colored and standalone structures) are easiest to identify. In urban zones, transceivers may be mounted independently, on rooftops, or the sides of buildings as required. Some equipment may also be camouflaged for aesthetic reasons, increasing detection difficulty.

3.1.4 Urban, Suburban, and Rural Environments

Urban areas offer the highest potential user density, are typically readily accessible by public transport, and feature extensive pedestrian space. This would make them the default choice, if the relative difficulty in tower identification were not a factor. Where urban environments are especially built-up (e.g. numerous high-rise buildings, or street canyons), the accuracy of GPS measurements may be lower. Rural environments tend to host fewer base stations servicing wider areas, which are more recognizable among the surroundings. Suburban environments appear to possess characteristics of both, with the highest likelihood of stand-out cell towers, reduced density, green space and pedestrian walkways, and public transit routes. However, other areas should still be studied where possible - especially urban areas, as the potential user density demands performant and reliable infrastructure. One compromise would be to identify the transition zone between one or more area types within which to run the experiment. Data from this campaign can then be reviewed as a whole or separately.

3.2 Analysis

3.2.1 Tower Data

Observed cell tower positions are required for calculating path loss, and should be verified against other sources. Additionally, we also require values for transceiver height, carrier frequency, and transmit power. In Canada, The Spectrum Management System Database published by Innovation, Science, and Economic Development Canada (ISED) [40] contains physical infrastructure data reported by service providers. The Canadian Cellular Towers Map [39] overlays this information on OpenStreetMap data, color-coded for the associated ISP and providing characteristics such as transceiver height, elevation, antenna azimuth (i.e. what sector around the tower it covers) and carrier frequency. An example is shown in Figure 3.1. A variety of factors influence the rate at which new tower information becomes available in the database, however, so it is possible that some towers may be detected with no match.

The CCTM database's help page notes that the "Power" value represents Effective Isotropically Radiated Power (EIRP), however the data is inconsistent due to each ISP reporting values in a different manner; therefore, the column is not feasible for a P_{TX} estimate. Instead, each base station could be assumed to use the 3GPP maximum for transmission power [41] and/or commercial antenna specifications to estimate actual power

transmitted. Using the industry maximum for P_{RX} means that any discrepancy will appear as a constant shift in the path loss at all distances (assuming that actual P_{TX} is constant).

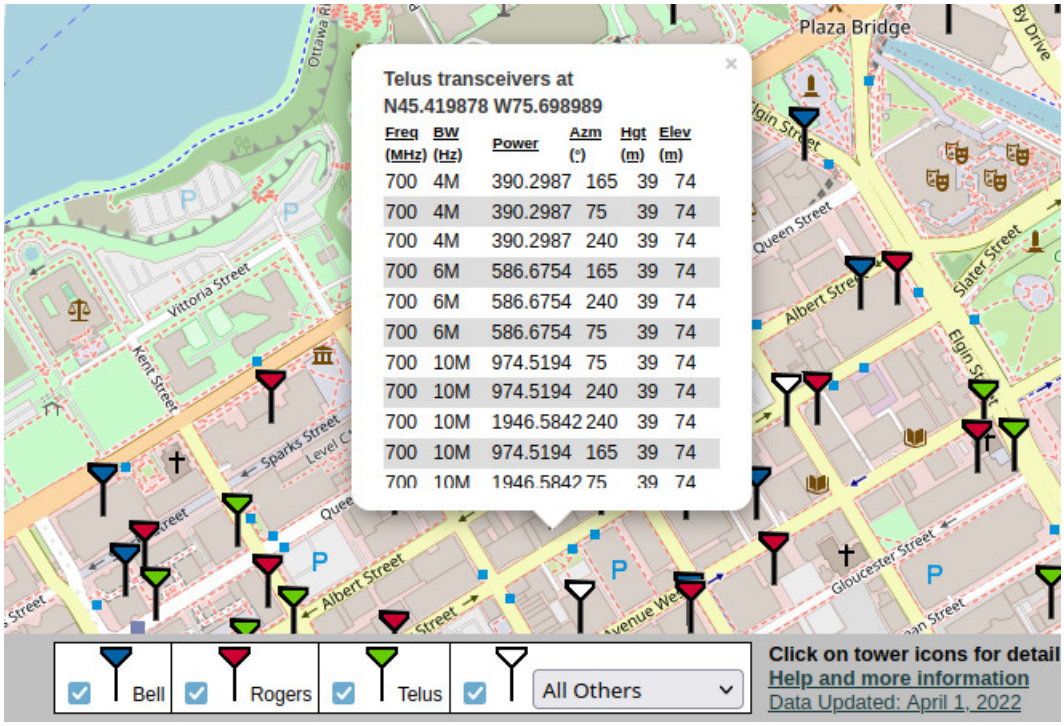


Figure 3.1: Canadian Cellular Towers Map in Downtown Ottawa, Canada

The second transceiver characteristic of note is the height, for both the tower itself and elevation of the surrounding area (above sea level). Since elevation can vary widely across a given zone, a simple approximation for use in calculating path loss is needed. The average of all elevations for the area's towers reported by CCTM h_{area} should be determined. The height h_{TX} for each base station is then calculated as:

$$h_{TX} = h_{hgt} + h_{elev} - h_{area} \quad [m] \tag{3.1}$$

where h_{hgt} and h_{elev} are the CCTM values under "Hgt" and "Elev", respectively. This relationship is depicted in Figure 3.2. Effectively, any part of the tower's local environment above h_{area} (e.g. hill or building) is considered to be part of the mast.

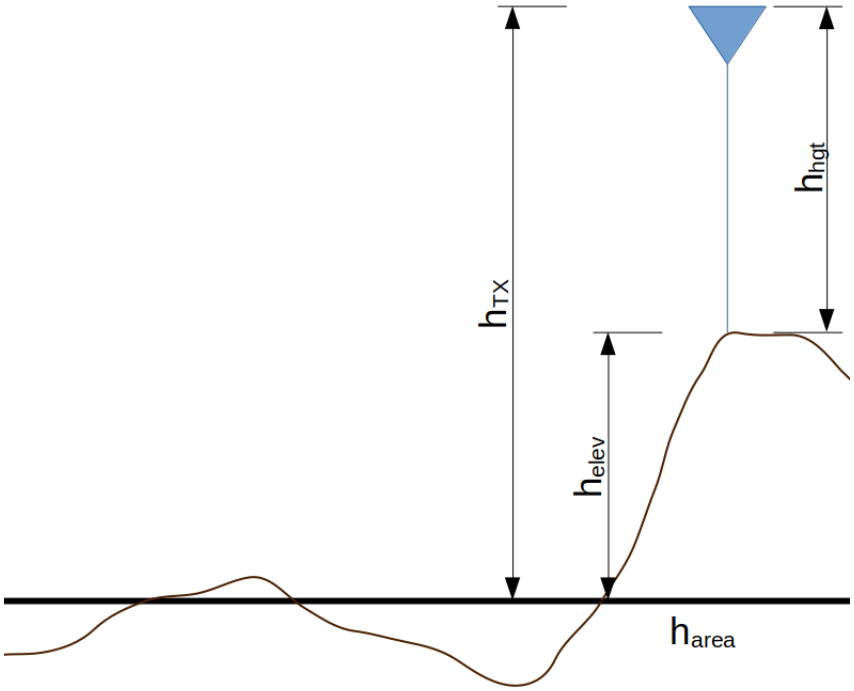


Figure 3.2: Comparison of h_{TX}, h_{hgt}, h_{elev}, h_{area}

3.2.2 RSRP Coverage Maps

In this experiment, RSRP data is sorted according to mobile network IDs, particularly Cell ID, and then compared against cell tower locations. This is ideally done by mapping signal power as an overlay for overhead and/or satellite imagery, such as OpenStreetMap [42]. The composite image can then be reviewed along with similar captures obtained on foot to determine environmental context. With awareness of the LOS and NLOS conditions present in the campaign area, the RSRP overlay can be evaluated for each cell against identified base station locations on a per-cell basis to attempt triangulation of the source. Overlays featuring unusual position readings relative to the actual route may additionally provide indication of GPS coverage loss for that space, which should be factored into the analysis. Environmental phenomena such as shadowing caused by large structures along the route should be discernable for the proper cells; absence of such behaviors may be evidence that the cell under analysis originates at a different location.

3.2.3 Cell Verification

Given that the experiment intends to analyze RSRP by cell, verification of measured data is important to ensure accurate interpretations. The CellMapper project [33], which aggregates user-contributed data from the CellMapper mobile application, provides an online resource to cross-reference observations against. Similar to the CCTM, information is sorted and displayed by ISP. Each cell includes details on parameters such as operating band, last user observation, tower verified/unverified status, and 5G capability among others. Some cells additionally provide a coverage overlay that can be compared directly against the measured positions from the experiment.

3.2.4 Path Loss Modeling

The final analysis step is to compare measured path loss against the theoretical and experiential models from Chapter 2. Assuming beam steering at the antennas and no other losses from cables or similar sources for simplicity, by rearranging the link budget in Equation (1.4) for path loss (referred to here as L_{meas}) and converting to logarithmic form we obtain:

$$L_{meas} = P_{TX\_est} - P_{RX} + G_{TX} + G_{RX} \quad \text{[dB]} \tag{3.2}$$

where P_{TX_est} is the estimated transmitter power, P_{RX} is the received power in dBm as measured by the UE; and G_{TX} and G_{RX} are the antenna gain at the transmitter and receiver, respectively. Equation (3.2) represents the average behavior of the path loss data, without being sufficient to predict path loss at a particular location. Given that cell phone antennas typically have low gain, G_{RX} is set to 0 dB. Gain specifications for numerous commercial transceiver models are available online; however, Table 4.3 in [41] suggests 15 dBi (which actually includes input losses) as an appropriate alternative. Note that any deviation in P_{TX_est}, P_{RX}, G_{TX}, or G_{RX} results in a constant shift in the resulting array of L_{meas}, so adjustments are simple to make.

Model parameter values need to be estimated from the environment or from trends in the plotted data itself. A qualitative approach where input parameters are manually adjusted to approximate the observations is a simple solution for testing the method, although it is less rigorous. While this may leave the analysis open to multiple competing best-fit configurations of the models or other deviations, it may also provide greater insight towards applying the models, as each "solution" to the data obtained can have its parameters validated against known propagation behaviors.

Chapter 4

Results

4.1 Overview

The devices utilized were the Samsung Galaxy S8 and the Motorola Moto G 5G, which are characterized in Appendix A. For both phones, the network service provider was Rogers Communications. The application that will be used for this experiment is Network Cell Info [37] (specifically the free Lite version of the app). It provides an array of useful features and information, including readouts of power and signal quality for the serving cell and nearest neighbors, speed testing, performance visualizations, and other abilities. In particular, it allows the user to export measured data in a variety of formats. For this experiment, the OpenCelliD [43] data format will be used. Measurements were recorded in approximately three-second intervals while traversing the campaign area, and the results from individual sessions (which each spanned multiple cells covering the route) were combined and organized into composite data sets on a per-cell basis. Each session was exported as an OpenCelliD database to a computer workstation for analysis. Images and screenshots were obtained during data collection where appropriate, with post-processing to ensure anonymity for other persons and businesses. Graphical analysis of OpenCelliD data was performed with the custom tool **Routesignal** (Appendix B), designed specifically for this research, from which maps of signal data overlaid on exported OpenStreetMap [42] imagery and plots of comparisons with path loss models were generated.

Routesignal allowed adjustment of each parameter separately, with the limitation that the same value is used for both the χ_σ^{ABG} and χ_σ^{CI}. Frequency f was always set according to the corresponding band in Table 1.1. The values for G_{TX} (15.0 dB), G_{RX} (0.0 dB), and $h_{RX} = 1.6$ m (i.e. the approximate height of the smartphone during tests) were static

throughout. Due to the uncertainty of CCTM power data[1], $P_{TX} = 43$ dBm was used for all cells, with the understanding that actual transmit power may not actually be constant. The coherence distance, d_{coh} represents the interval length over which the large-scale fading is assumed constant (for this experiment, 5.0 m), rounded-up from the GPS accuracy for mobile devices of ± 4.9m[2]. Effectively, this experiment assumes the modeled fading is constant within 5.0 m of a single measurement.

For each cell ID in turn, the detected base stations that had LOS along some or all of the route were provided to Routesignal and the distance for each measured point was computed. The model parameters were then adjusted to approximate the observed path loss. The test ranges for this experiment consisted of two different areas in Ottawa, Canada:

1. The "Carling" area, a suburban space made up of sidewalks, bike paths, parking lots, cul-de-sacs, and residential buildings in the Nepean area;
2. The "Sparks" area, an urban street canyon environment in the downtown core surrounded by tall buildings.

Figure 4.1 shows a map of the Carling Area and surroundings, with added markers for important locations. The area featured a mixture of small businesses, schools, and housing - primarily single-family homes and apartment buildings four storeys or lower at the western extent; a mixture of residential and commercial buildings (some of 10+ storeys) bordering the eastern and southern areas; and public parks followed by a waterway (the Ottawa River) to the north. Traffic was moderate-but-consistent at street level while there were few pedestrians present. However, the quantity of private dwellings in sight of the observed cell towers suggested that a significant number of user devices could be active within the service area at any given time.

Carling area points of interest are listed in Table 4.1, where the position values were manually selected from the data files by comparing locations using Google Maps, then truncating to four data points (which provides accuracy to approximately 11m or ± 5.5m). Data collection sessions began at L1, progressing either towards L6 before returning, or immediately toward L2. The space between L1 and L2 was open and relatively flat, flanked by highway infrastructure at the southern extent; lower-elevation parks and waterways on the north; and with mixed green and residential spaces at the east and west. From L1 to L6 there was significant reduction in long-range visibility due to multiple highway overpasses and numerous light poles, then a similar open area flanked on either side by denser green space, which continued between L6 and L7.

[1] See in Section 3.2.1.

[2] According to https://www.gps.gov/systems/gps/performance/accuracy/.

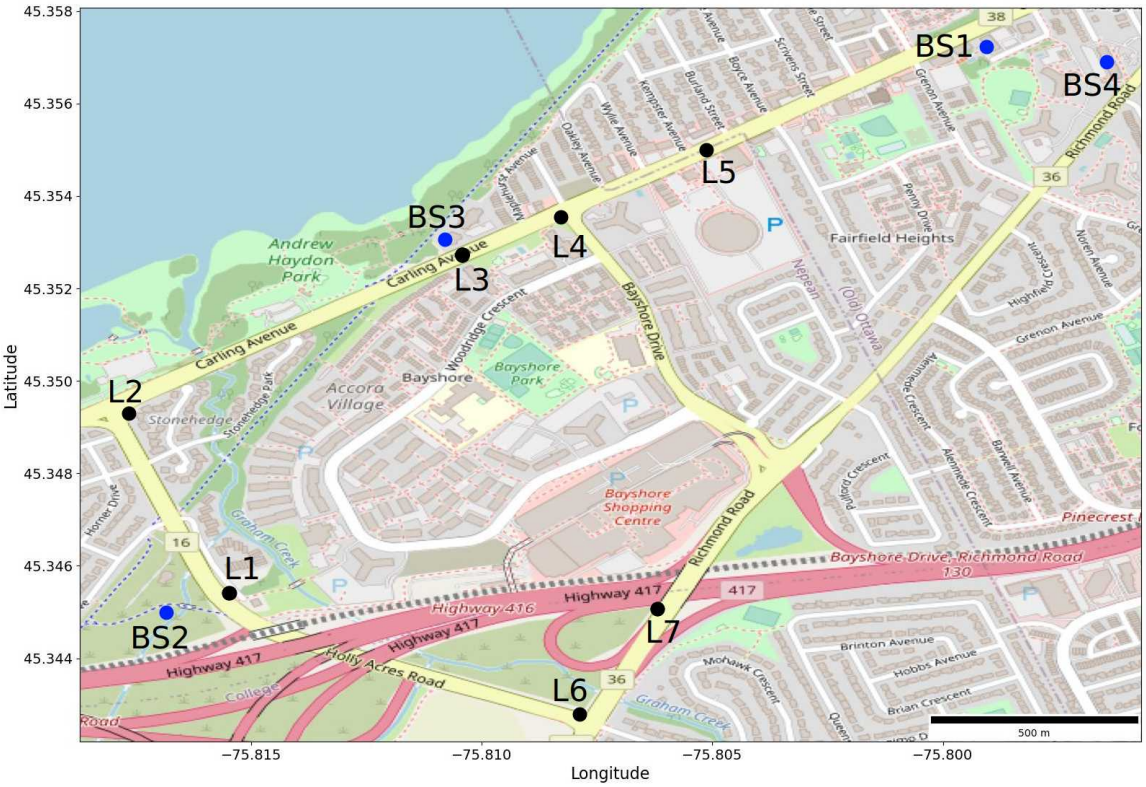


Figure 4.1: Carling Route Map

Table 4.1: Carling Area Reference Locations

Point	Latitude	Longitude
L1	45.3461	-75.8160
L2	45.3492	-75.8177
L3	45.3524	-75.8103
L4	45.3533	-75.8084
L5	45.3548	-75.8050
L6	45.3428	-75.8079
L7	45.3451	-75.8061

From L2 to L3, the line-of-sight view to possible base stations varied depending on which side of the road was traversed. The approach also featured a gradual decline in elevation, which became an incline again prior to arrival at L3. This location was also

approximately where line-of-sight to base station candidates ceased being blocked intermittently by telephone and light poles. From L3 to L4 (and L5) the environment took on a more urban nature, with several high-rise and commercial structures lining the roadway boundaries, and corresponding to an increase in user density.

Figure 4.2 shows a map of Sparks Street and surroundings. This test range was a "street canyon" business area for pedestrians and cyclists in downtown Ottawa, Canada intersected by north-south auto routes. In contrast to the Carling campaign, structures in this environment could approach 90 meters[3]in height. The area was devoid of ground-level obstacles, other than sporadic street lights and flag poles. The route was bordered by the aforementioned structures on both sides, occasionally broken up by north-south streets a few scattered lower-elevation buildings. There was also a gradual decrease in elevation between L7 and L9.

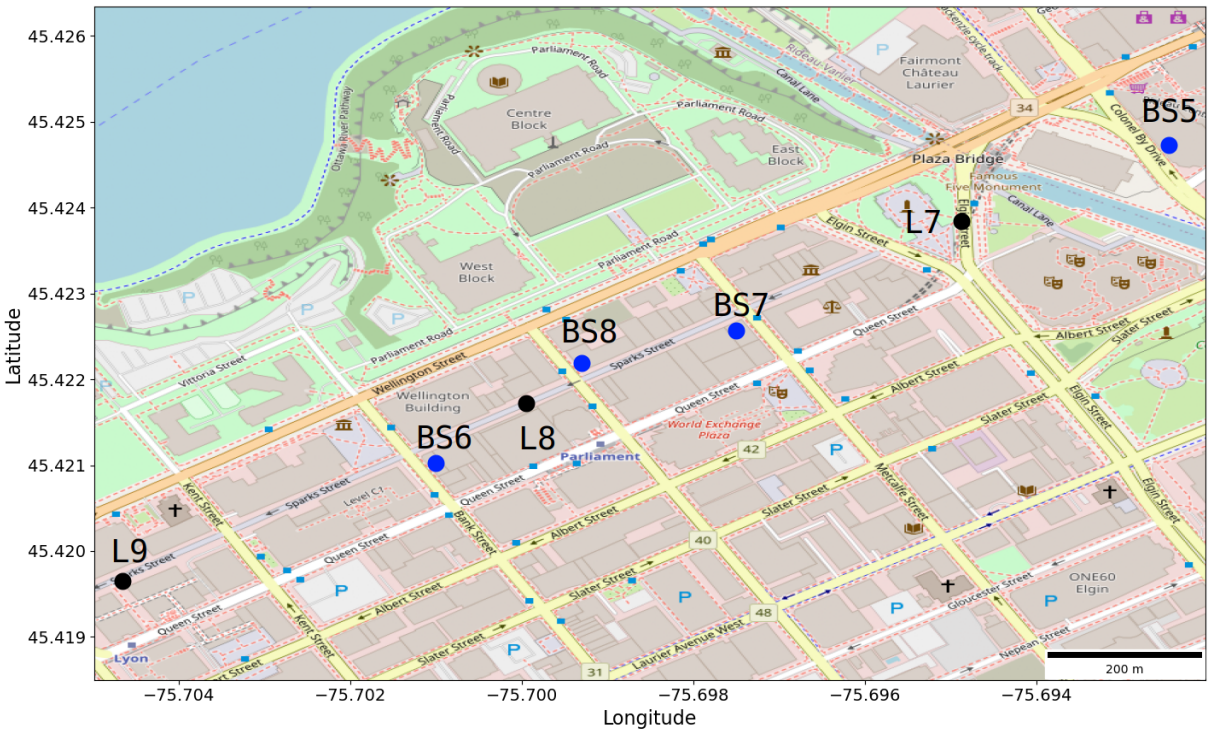


Figure 4.2: Sparks Route Map

Observation took place when visible device density was low in the area itself (like

[3]According to data found at https://skyscraperpage.com/cities/?buildingID=6253

Table 4.2: Sparks Area Reference Locations

Point[4]	Latitude	Longitude
L7	45.4238	-75.6949
L8	45.4218	-75.6997
L9	45.4197	-75.7045

Carling), with similar potential for nearby mobile devices. Table 4.2 lists the locations of interest from Figure 4.2. Unlike the Carling campaign, which progressed in a "loop", observations for Sparks were typically made at the eastern extent and proceeding from L7 through L8 (the midpoint) to L9, before retracing steps to L7. The resulting data set therefore showed the same rough positions twice, at slightly different times of day (on the order of 30 minutes). Deviation from the campaign path was also comparatively limited due to the street canyon environment, with most measurements occurring within ±5 m of the street's centre. Export and examination of measurements was performed in the same manner as with the Carling area.

4.2 Base Stations

4.2.1 Carling Area

Table 4.3: Carling Base Stations

Station	Latitude	Longitude	h_{TX}(m)	h_{elev}(m)	h_{hgt}(m)
BS1	45.357264	-75.799109	53	78	49
BS2	45.345035	-75.816792	28	66	36
BS3	45.352921	-75.810651	44	68	50
BS4	45.456944	-75.796667	55	83	46

Four candidate base stations were identified in the Carling area and are listed in Table 4.3. Latitude and longitude were estimated by positioning the UE next to the station where possible, and otherwise taken as an approximate value from the Google Maps satellite imagery database. The CCTM included position data which was used for verification purposes, along with site elevation (relative to sea level) and transceiver height above ground. h_{TX} was determined from h_{elev} and h_{hgt} according to Section 3.2.1, where h_{area} was determined to be 74 m.

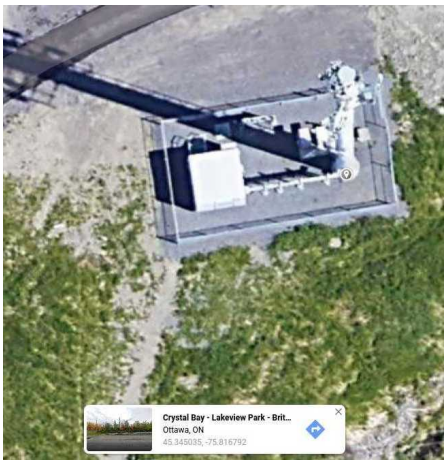


Figure 4.3: BS2 Satellite View.

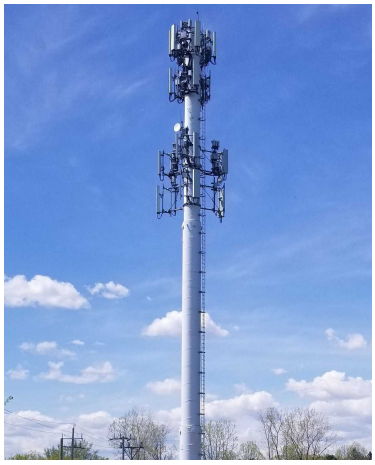


Figure 4.4: BS2 Pedestrian View.

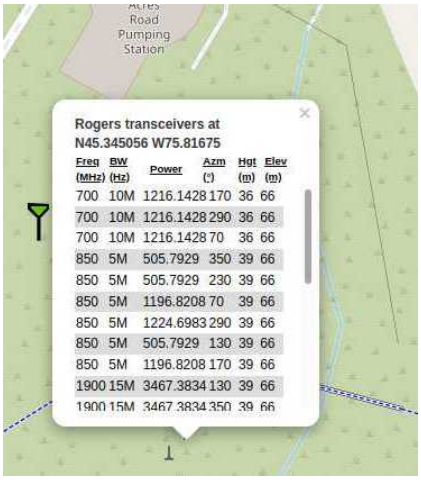


Figure 4.5: Rogers Transceivers Near BS2.

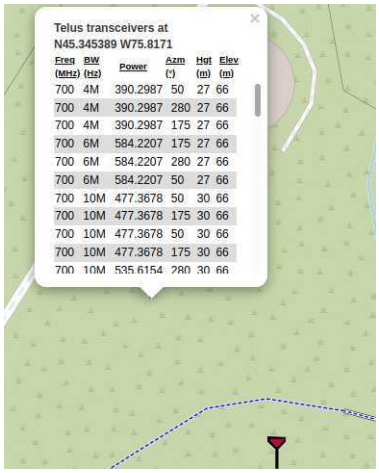


Figure 4.6: Telus Transceivers Near BS2.

Figures 4.3 and 4.4 show the satellite and pedestrian views of the structure referred to as "BS2", which was located near L1 as in Table 4.1. The base station stands out clearly against the background, with a mast hosting multiple sets of transceiver hardware. This structure's height gave it visibility from both L2 and L6. The CCTM shows two sets of transceivers nearby, operating on bands 2, 4, and 7 (Figure 4.5 and Figure 4.6). The first, operated by Rogers Communications, is listed at $h_{hgt} = 36$ m, while the second is operated by Telus Communications, with $h_{hgt} = 30$ m. No obvious second structure was visible, so

it was assumed that they were co-located, and the former's tower position used.

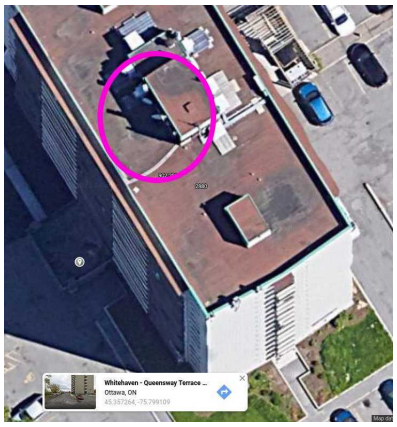


Figure 4.7: BS1 Satellite View.

Figure 4.8: BS1 Pedestrian View.

The next base station, shown in Figure 4.7 and Figure 4.8, is referred to as "BS1". This structure was not adjacent to the campaign path, but it was visible in the distance from L2. Figure 4.9 shows the CCTM data for a tower at BS1's location, with transceivers $h_{hgt} = 49$ m.

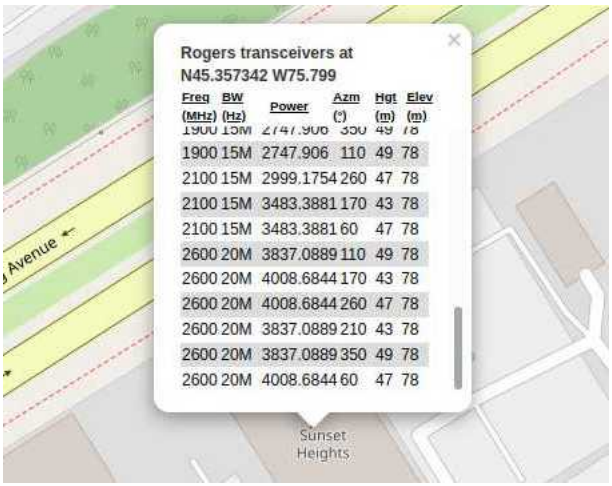


Figure 4.9: Rogers Transceivers Near BS1.

"BS3" is shown in Figure 4.10 and Figure 4.11. While it was adjacent to the route, it had the least-obvious hardware, which appeared to be concealed with paint or other shielding. CCTM data for two sets of transceivers are shown in Figure 4.12 and Figure 4.13.

However, neither provider matched the UE's (Rogers). A variety of transceiver heights were reported between the two providers, so $h_{hgt} = 50$ m was chosen in this instance; both networks operate on band 4. The bandwidth of 0 reported for Videotron along with h_{elev} for Freedom were unusual, and the corresponding rows were avoided in calculations.

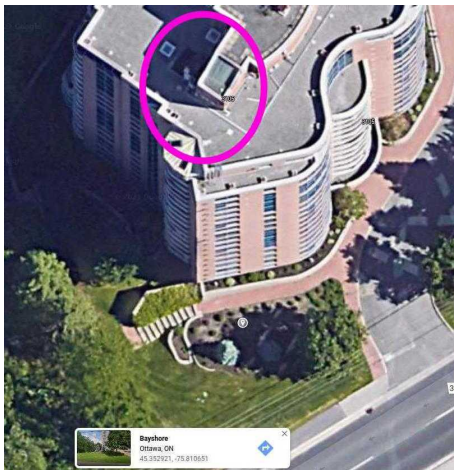
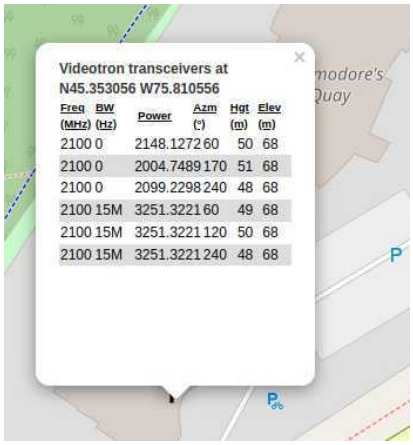


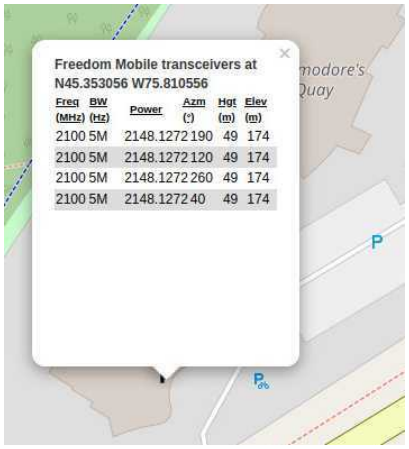
Figure 4.10: BS3 Satellite View.

Figure 4.11: BS3 Pedestrian View.



[39]

Figure 4.12: Videotron Transceivers Near BS3.



[39]

Figure 4.13: Freedom Mobile Transceivers Near BS3.

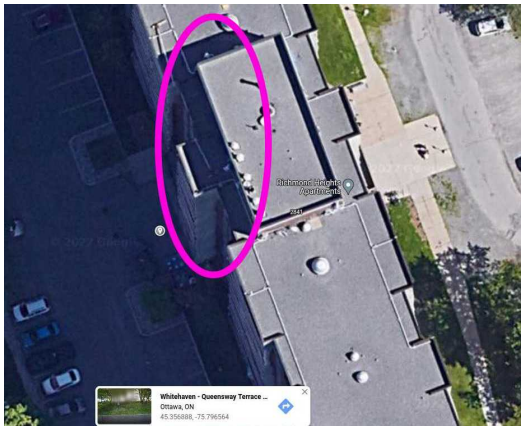
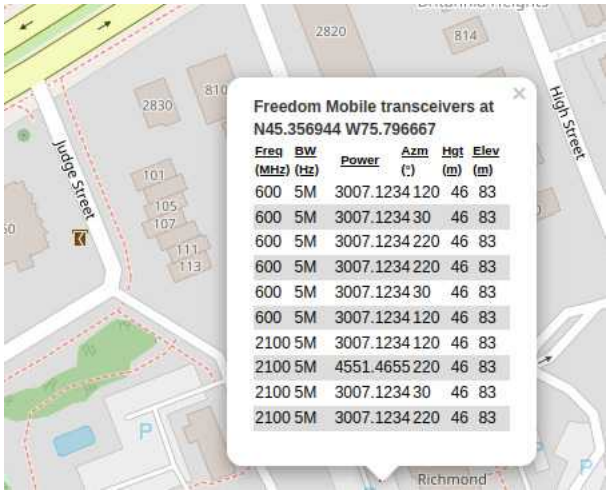


Figure 4.14: BS4 Satellite View.

Figure 4.15: BS4 Pedestrian View.

The final Carling cell "BS4" is shown in Figure 4.14 and Figure 4.15. This base station was the most distant from the campaign route, limited to line-of-sight in the vicinity of L4 and L5. Similar to BS3, it was also less obvious from street level, although its elements were not explicitly camouflaged. CCTM's only transceiver record for this position operated on band 4 with $h_{hgt} = 46$ m. This transceiver is attributed to Freedom Mobile, as shown in Figure 4.16.



Freedom Mobile transceivers at N45.356944 W75.796667

Freq (MHz)	BW (Hz)	Power	Azm (°)	Hgt (m)	Elev (m)
600	5M	3007.1234	120	46	83
600	5M	3007.1234	30	46	83
600	5M	3007.1234	220	46	83
600	5M	3007.1234	220	46	83
600	5M	3007.1234	30	46	83
600	5M	3007.1234	120	46	83
2100	5M	3007.1234	120	46	83
2100	5M	4551.4655	220	46	83
2100	5M	3007.1234	30	46	83
2100	5M	3007.1234	220	46	83

Figure 4.16: Freedom Transceivers Near BS4.

4.2.2 Sparks Area

The Sparks campaign featured significantly more challenging base station identification. The entire route boasted a consistent line-of-sight to BS5, as shown in Figures 4.17 and 4.18. Figure 4.19 shows the CCTM data [39] for the only transceiver in the vicinity operating on band 7 attributed to Rogers. Here, $h_{area} = 72$ m.

Table 4.4: Sparks Base Stations

Station	Latitude	Longitude	h_{TX}(m)	h_{elev}(m)	h_{hgt}(m)
BS5	45.425036	-75.692309	76	66	82
BS6	45.421182	-75.701126	21	72	21
BS7	45.422627	-75.69757	44	68	48
BS8	45.422221	-75.699320	55	83	46

Figure 4.17: BS5 Satellite View.

Figure 4.18: BS5 Pedestrian View.

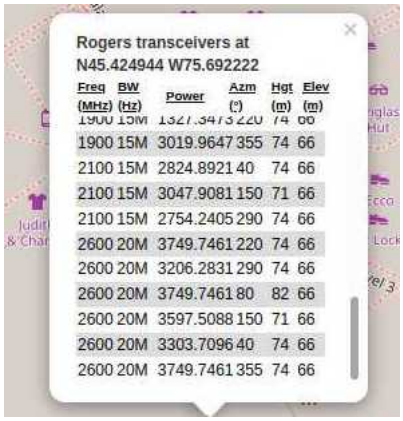


Figure 4.19: Rogers Transceivers Near BS5.

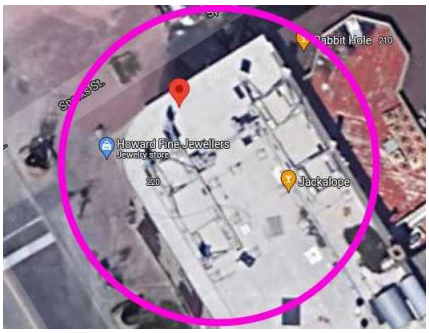


Figure 4.20: BS6 Satellite View.

Figure 4.21: BS6 Pedestrian View.

Figures 4.20 and 4.21 show the BS6 base station, a series of antennas placed on the roof of a four-storey building at the corner of an intersection, approximately (45.421178, -75.701120). The elements cover an arc that gives an overview of Sparks Street in both directions. Given their low, rooftop positioning at the corner, this array seemed an obvious choice for providing coverage to the intersection and nearby street. As shown in Figure 4.22, this station was attributed to Telus (not Rogers) in the CCTM database.

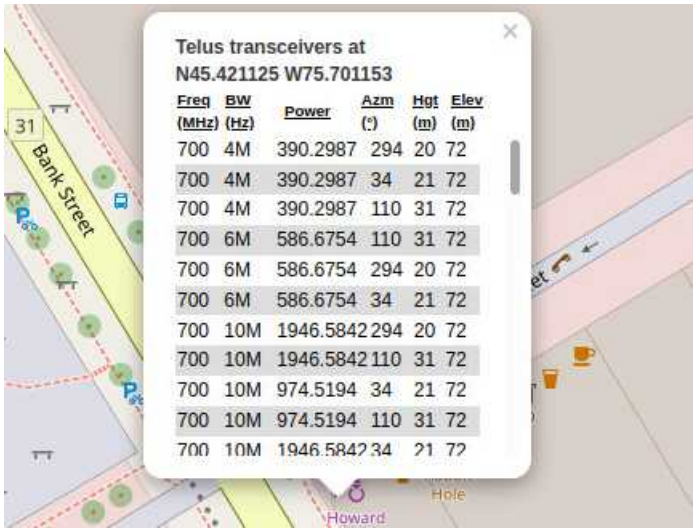


Figure 4.22: Telus Transceivers Near BS6.

The BS7 base station was less apparent, as the antenna elements' color matched the superstructure and could be mistaken for heating, ventilation, or other components (Figure 4.24). This array appeared to have a limited, westward view of Sparks Street, although

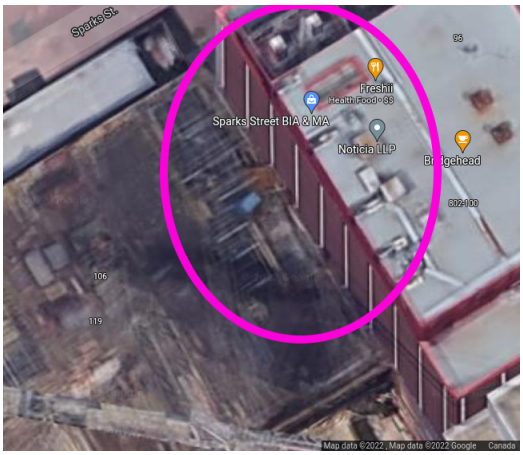


Figure 4.23: BS7 Satellite View.

Figure 4.24: BS7 Pedestrian View.

its proximity to L7 meant that this covered the vast majority of the route. Numerous temporary construction scaffoldings and other objects were present in its vicinity, that may have caused temporary propagation obstacles. Figure 4.25 reveals that this base station is also a Telus array, making it less likely to be a source for the measurements.

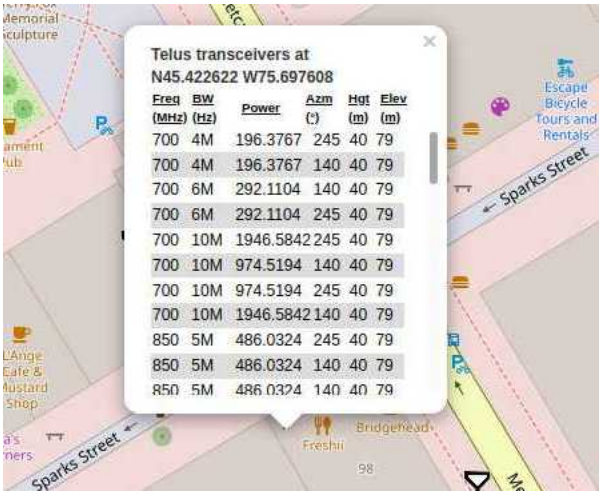


Figure 4.25: Telus Transceivers Near BS7.

Similar to the BS7 base station, the BS8 candidate was situated along the top of a building near the route's origin, but it was clearly visible against the structure. This array had possibly the shortest exposure along the Sparks environment when considering both

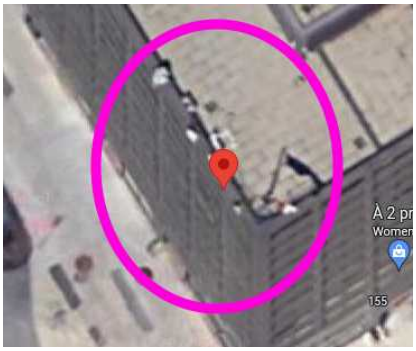


Figure 4.26: BS8 Satellite View.

Figure 4.27: BS8 Pedestrian View.

directions, since its view was nearly at the midpoint and appeared to have been oriented strictly westward. The BS6 base station was the only other candidate array to which it had line-of-sight. This base station was attributed to Rogers according in the CCTM database (Figure 4.28).

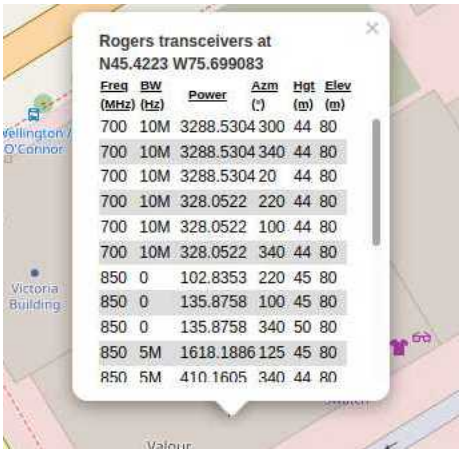


Figure 4.28: Rogers Transceivers Near BS8.

4.3 Analysis

The key statistics for the Carling cells' measured data are given in Table 4.5, where all but C6 showed mean received power values greater than -100 dBm. Both the average and standard deviation were calculated directly from the dBm values, rather than converting to linear and averaging before returning to dBm. This was to remain consistent with the standard deviation calculations of the Appendix in [21], which average the logarithmic path loss directly. Six cells (C2, C3, C4, C5, C7, C10) reported peak values exceeding -70 dBm (except C5) over at least 100 data points (other than C1). Interestingly, the peak power for cells C3 and C4 were the only instances where our measurements were within 3 dB of those in the CellMapper database [33] - observations for C5-7 were significantly higher (-96.0, -108.0, and -78.0 dBm, respectively), while C9-10 (-85 and -72 dBm) and C1-2 (-93 and -88 dBm) were significantly lower. It is possible they may have been measured in a different part of the base station's coverage zone; that the environment may be substantially different; and that more extreme variations could yet be observed. Assuming a noise figure of 9 dB [44], $T_n = 290$ K and 5 MHz bandwidth (the minimum for band 7) in Equation (1.3), the receiver sensitivity $P_{sens} = -98$ dBm. 3GPP specifies the lowest channel bandwidth at 1.4 MHz, which would suggest $P_{sens} = -103$ dBm. All but C1 and C9 had minimum measurement values below this figure, suggesting that the mobile device may be reporting values according to a different calculation, or reading noise. However, the 3GPP reference sensitivity is listed as -108 dBm [41], so some actual signal reception may still have occurred if the true device sensitivity more closely matches the model.

Table 4.5: Carling Measured Statistics by Cell

Cell (ID)	Points	Band	P_{avg}(dBm)$\pm\sigma$ (dB)	P_{max}(dBm)	P_{min}(dBm)
C1 (9241603)	48	4	-73.8 ± 5.1	-65.0	-84.0
C2 (9391383)	192	2	-85.8 ± 9.5	-68.0	-100.0
C3 (9391431)	275	7	-89.8 ± 6.8	-68.0	-104.0
C4 (9391433)	203	7	-96.4 ± 5.2	-85.0	-113.0
C5 (9748502)	192	2	-89.0 ± 6.7	-78.0	-105.0
C6 (9748552)	6	7	-106.0 ± 3.2	-103.0	-110.0
C7 (9748553)	832	7	-87.4 ± 8.5	-66.0	-108.0
C8 (9755670)	14	2	-94.4 ± 4.4	-88.0	-100.0
C9 (26317826)	10	4	-75.1 ± 3.0	-71.0	-81.0
C10 (26317827)	120	4	-67.4 ± 8.5	-52.0	-113.0
Overall	1892	N/A	-87.2 ± 10.0	-52.0	-113.0

Table 4.6: Carling Model Parameters by Cell

Cell	Source	f (MHz)[5]	h_{TX} (m)	Points	Dist. Range (m)	α	β (dB)	γ	n	σ (dB)
C7	BS1	2600	53	832	352-1698	4.0	0.0	2.2	3.4	6.8
C3	BS2	2600	28	275	113-819	1.6	70.0	6.3	4.0	6.8
C4	BS2	2600	28	203	199-511	1.6	70.0	6.3	4.0	6.8
C5	BS1	1900	53	192	839-1674	4.2	0.0	1.8	3.3	5.2
C2	BS2	1900	28	192	152-744	4.4	0.0	0.9	3.6	6.8
C10	BS3	2100	44	120	195-646	3.9	0.0	1.8	2.9	5.5

Table 4.6 contains summarized model inputs by cell based on the measured data, excluding those without at least 100 measurements. This exclusion was made to help ensure that analyzed cells provide a reasonable minimum sample size from observations made over wider ranges, and avoid cells only witnessed briefly at the campaign boundaries. Curve fitting was done manually by loading all Carling measurement files with the Routesignal tool, providing cell tower coordinates collected from Google Maps overlays along with supplementary area map images generated from OpenStreetMap's website. The controls were then adjusted manually to visually approximate each model's curve to the observed path loss for each cell.

These parameter results were generally higher than those reported for the 2 GHz UMa LOS scenarios' ABG model in [21] (often appearing closer to the NLOS examples), with exceptions in α (1.6) for C3 and C4. Likewise, β (70.0 dB), n (for the CI model) and the various σ values for both exceed those listed there ($\beta = 19.6$ dB, $n = 2.8$, $\sigma_{CI} = 3.5$, $\sigma_{ABG} = 3.2$). Only γ for C5 (1.8) was similar to the UMa (1.9) result. In subsequent sections, cells C7, C3, and C2 are reviewed (in order from largest to smallest sample count) and compared against a rough fitting of the path loss models. This is used to qualitatively estimate how likely a particular base station is to be the cell source.

Correspondingly, the key statistics for the Sparks area are given in Table 4.7. Despite the more challenging environment, the cells detected in this campaign had mean and maximum signal powers exceeding those in the Carling area, with P_{avg} over 7 dB higher. Additionally, no values for P_{min} fell below the -100 dBm mark. This could be attributed to the relatively short distances (excluding BS5) under examination. Overall, the Sparks data set is much smaller (400 versus 1892 total measurements), and all five cells share the

[5]Converted from the bands in Table 4.5 using 3GPP TS 36.104 [10].

same transmission band (7). Using the same critieria to select cells for analysis, only C13 was chosen for further inspsection. The parameters used are shown in Table 4.8.

Table 4.7: Sparks Measured Statistics by Cell

Cell (ID #)	Points	Band	P_{avg} (dBm) $\pm$ σ (dB)	P_{max} (dBm)	P_{min} (dBm)
C11 (8227657)	54	7	-80.5 $\pm$ 4.3	-75.0	-89.0
C12 (9438791)	56	7	-81.4 $\pm$ 5.8	-66.0	-97.0
C13 (9438792)	242	7	-79.2 $\pm$ 6.4	-59.0	-90.0
C14 (9567817)	6	7	-86.5 $\pm$ 0.8	-85.0	-87.0
C15 (9569609)	42	7	-80.3 $\pm$ 3.3	-75.0	-88.0
Overall	400	N/A	-79.9 $\pm$ 5.9	-59.0	-97.0

Table 4.8: Sparks Model Parameters by Cell

Cell	Source	f (MHz)	h_{TX} (m)	Points	Dist. Range (m)	α	β (dB)	γ	n	σ (dB)
C13	BS5	2600	55	832	26-501	3.9	0.0	2.7	3.4	6.8

4.3.1 C7

In Figure 4.29, the CellMapper database's entry for C7 is shown. The coverage outline is a narrow area running along Carling Avenue and crossing through L2, L3, L4, and L5 in Figure 4.1. Interestingly, the listed maximum RSRP (-78 dBm) is significantly lower than what was observed in the experiment (-66 dBm). Figure 4.30 shows the environment between L2 and L5 from one side of the campaign route, with the locations of BS3 (left) and BS1 (right) circled in pink. The measured area consists of a suburban green space and commuter route. Density and size of structures increased between L3 and L5, where the UE passed below the superstructure for BS3.

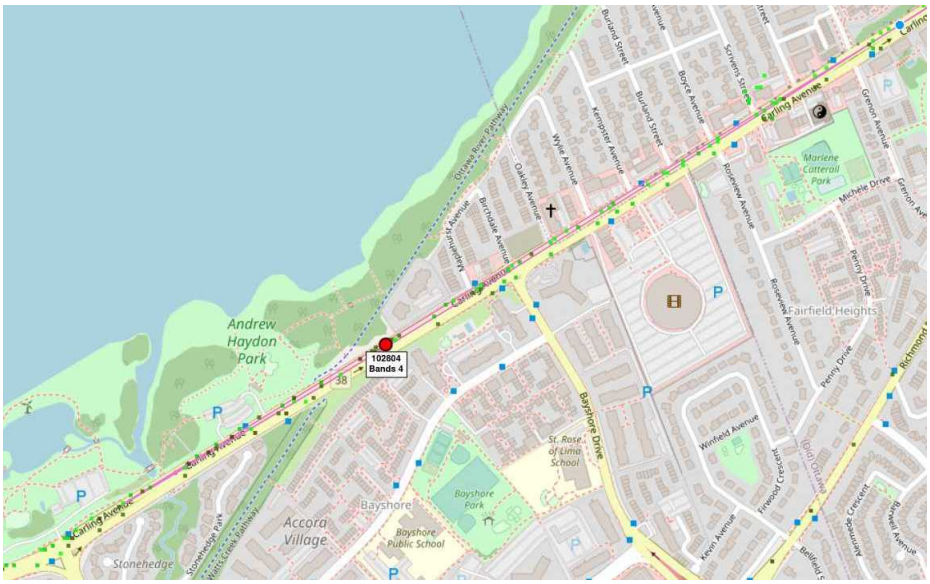


Figure 4.29: C7 CellMapper Data

Figure 4.30: L2, Facing L3-5 (Left Side)

The received power map for C7 is shown in Figure 4.31. Measurements were collected monotonically toward BS1, beginning from L2 in Figure 4.1. There was a clear overall increase in received power over the section, with intermittent variation that could be attributed to environmental factors such as changes in elevation along the route, or brief obstruction by street lights. BS3 is also located along the campaign path, but Figure 4.31's power values when approaching and receding from it suggest that this is not the source, unless the coverage is either uneven by design, or some other phenomenon is affecting its performance.

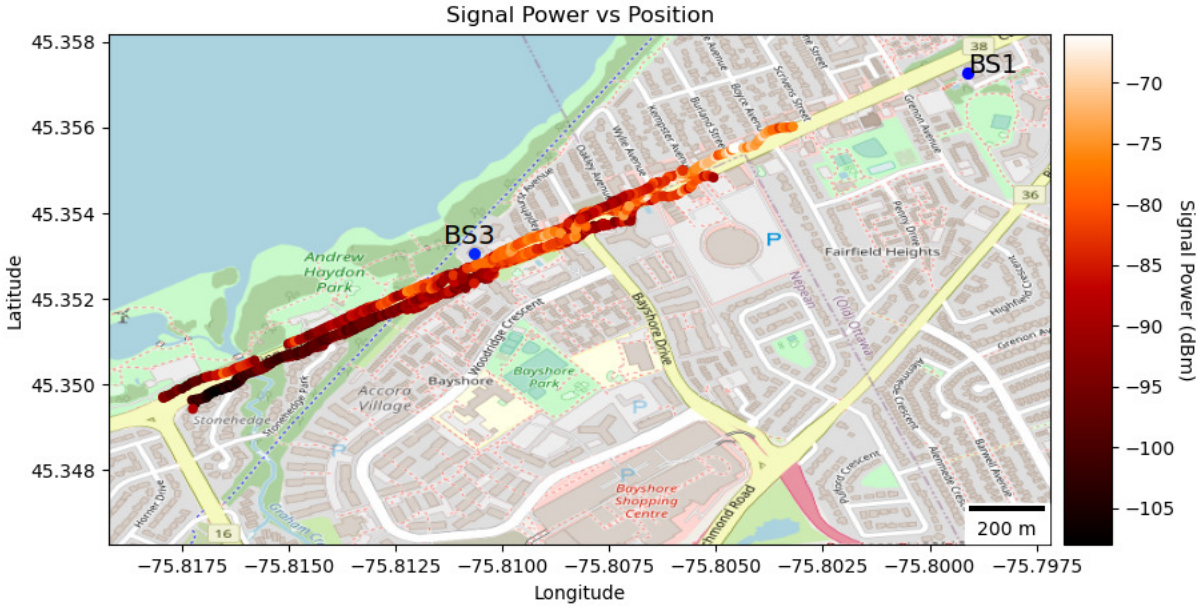


Figure 4.31: C7 Received Power Map vs BS1, BS3

Figure 4.32 shows the measured path loss (relative to BS1). We find that the ABG and CI models both result in close fits. The free space and two-ray models overshoot the data as a whole regardless of position - given that the critical distance d_c for the two-ray model with these parameters is 9687 m, this is not surprising. The Okumura-Hata urban and suburban models appear to undershoot and overshoot the data's average, respectively (or alternatively provide bounds for it); the rural version is a poor fit. This is reasonable given that they do not account for log-normal shadowing and are not intended for use above 1500 MHz.

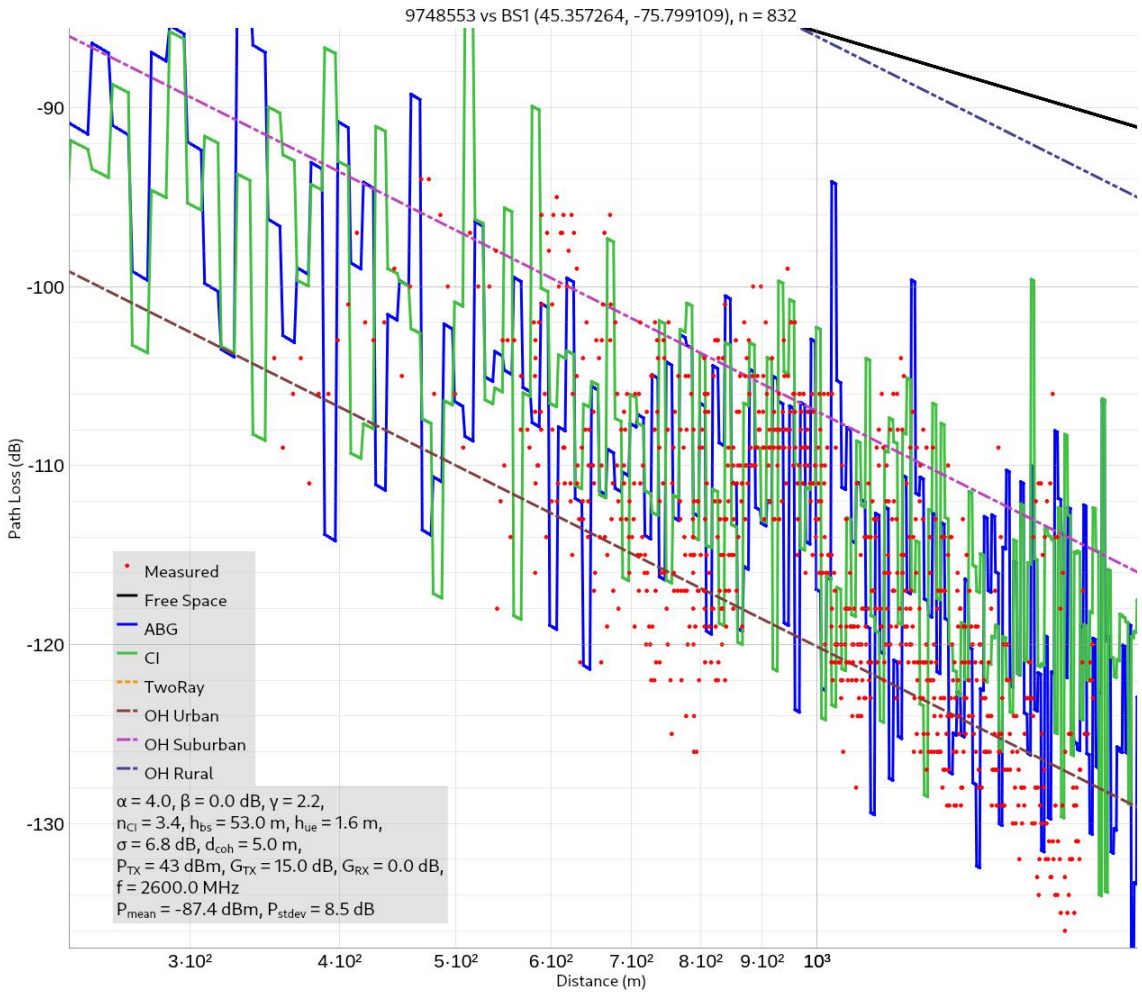


Figure 4.32: Path Gain for C7 vs BS1

4.3.2 C3

The CellMapper data for C3 in Figure 4.33 shows no apparent overlay for the cell (although the others could obscure one near L6 and L7). Environmental characteristics for C3 are shown facing BS2 (from L2) in Figure 4.34, with large sections where LOS is maintained. Immediately south of L1 was an overpass preceded by dense street and traffic lights, which would have severely obstructed that area between L1 and L6. Unlike C7, where progression was consistently in the assumed base station's direction, C3's dataset is comprised of multiple sets acquired while moving between different combinations of L1, L6, and L2.

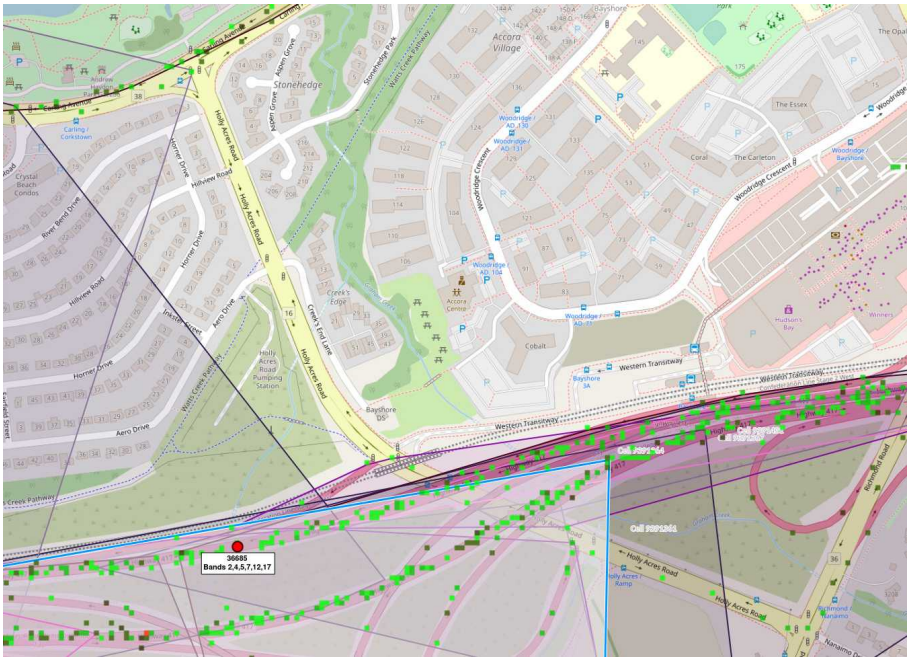


Figure 4.33: C3 CellMapper Data

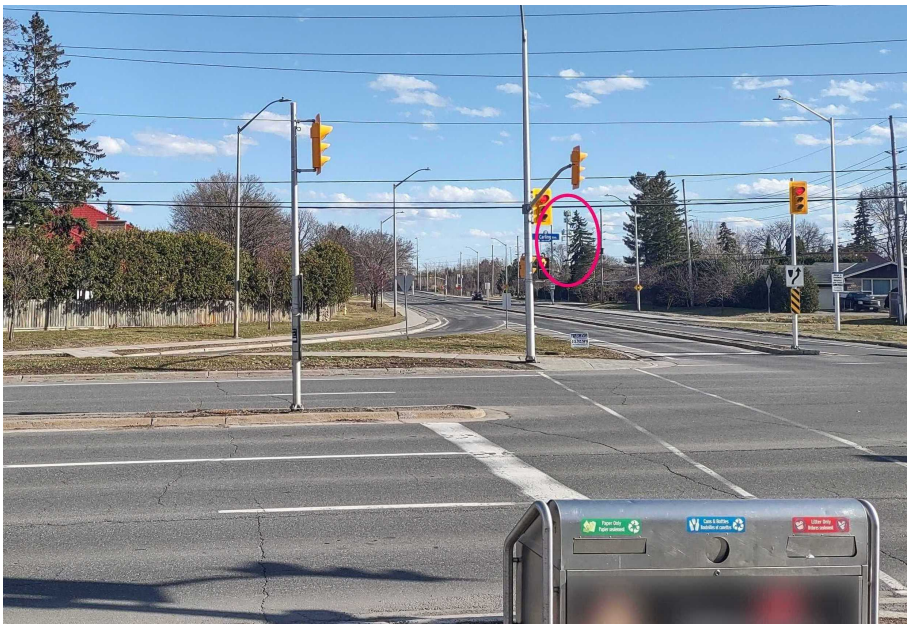


Figure 4.34: Near L2, Facing L1

The received power map for C3, Figure 4.35 shows a gradual path loss increase heading north (i.e. between L1 and L2), while the southern progression (towards L6) is much more rapid - likely as a result of the aforementioned overpass - before the RSRP appears to stabilize below -95 dBm for the duration (even long after LOS to BS2 is reacquired). In Figure 4.36, this is represented by the path loss falling by more than 20 dB over roughly 50 m, with some outliers. The models predictably show a poorer fit to this behavior than they did for C7. The ABG model provided arguably the best fit, using a high β value to compensate for the nearly flat RSRP curve. The CI model with $n = 4.0$ overestimates the measured path gain at close-range, overshooting the results until around 500 m. All other models fall short of the observations, with the Okumura-Hata Urban model providing an upper bound.

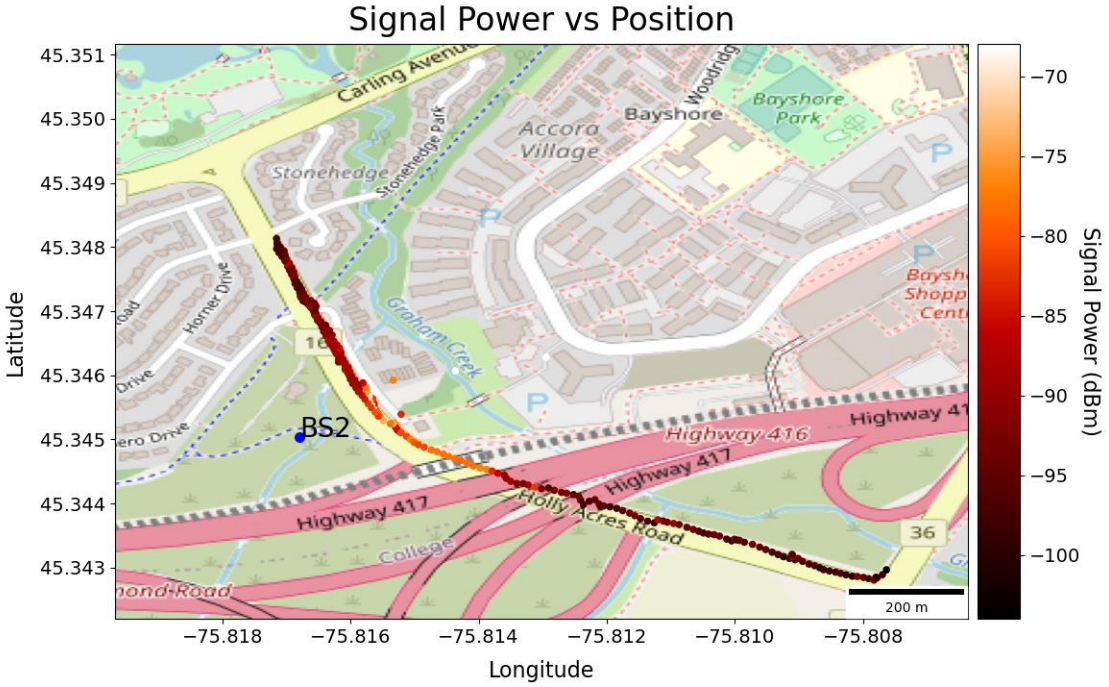


Figure 4.35: C3 received power map vs BS2

The curve's shape and variance within 200 m of BS2 are reasonably at odds with the large-scale models, considering their design for LOS conditions, and omitting NLOS measurements may have resulted in a better fit. The near-constant path loss at higher distances could be explained by variable transmit power at BS2, if P_{TX} were increasing with distance (unlike our static P_{TX_est} in Equation (3.2)). Additional data at medium- and long-range (where available) could be used to verify this by looking for a critical distance beyond which path loss falls off more rapidly.

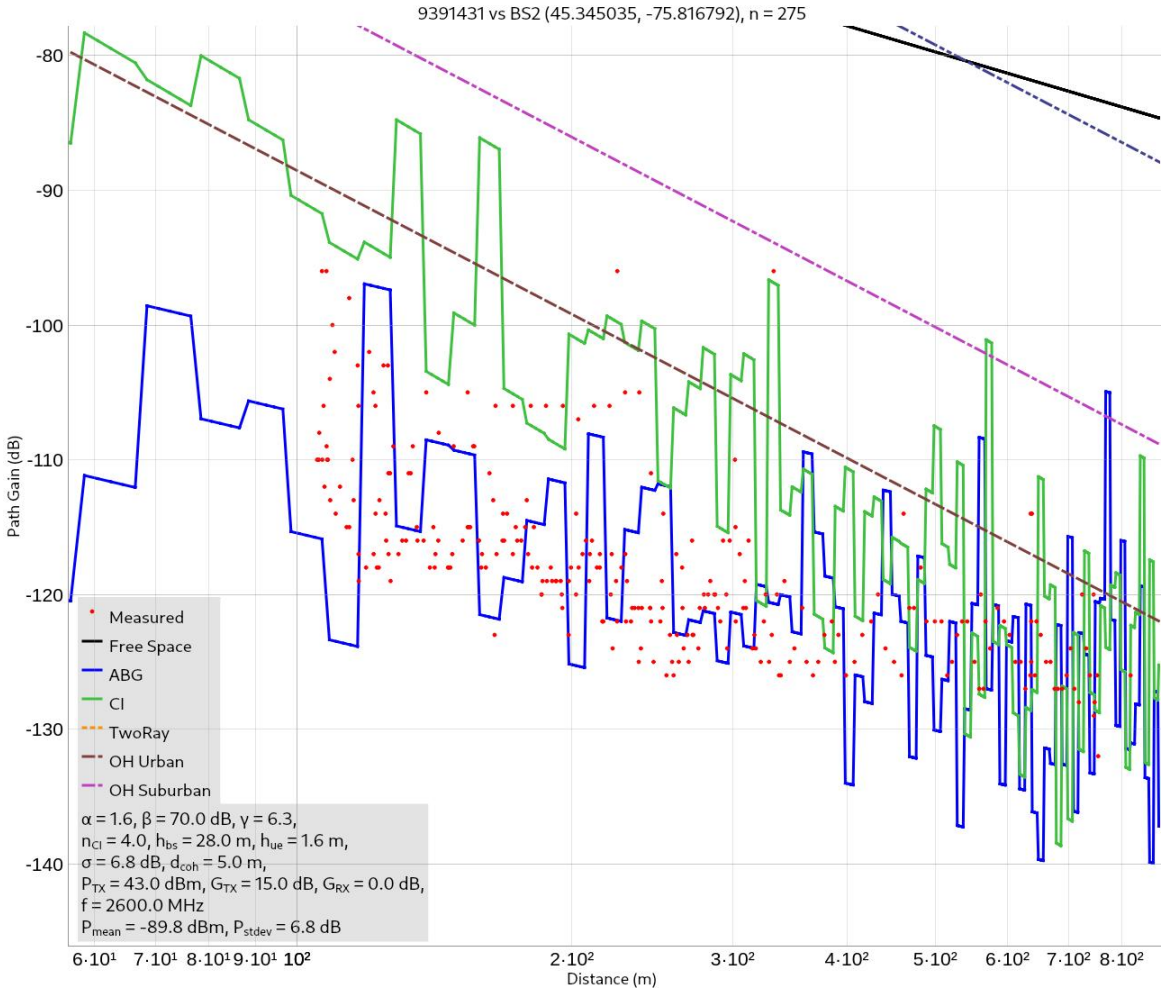


Figure 4.36: Path Gain for C3 vs BS2

4.3.3 C2

C2 operates on band 2, unlike the previous two cells. The data was collected while proceeding strictly away from the base station (BS2). After reaching L2, the vast majority of data was obtained from the right side of the route. Figure 4.38 shows the measured RSRP relative to BS2 and BS3. The obvious drop in RSRP after the smartphone lost LOS to BS2 meant that the transceiver was assumed to be located there. Figure 4.37 shows the CellMapper database entry for C2, including a bowl-shaped coverage overlay that is consistent with observations along the L2-L3 portion of the campaign route. Curiously, this overlay does not include the L1-L2 segment, where the strongest RSRP values were measured. The contradictory operating band for C2 (2, versus the BS3 transceivers' band 4) along with the database's maximum RSRP (−88 dBm versus observed −68 dBm) both cast some doubt on BS3 as the probable transmission source. Additionally, Figure 4.37 shows that BS3 is located at one corner of the coverage area according to crowd-sourced data.

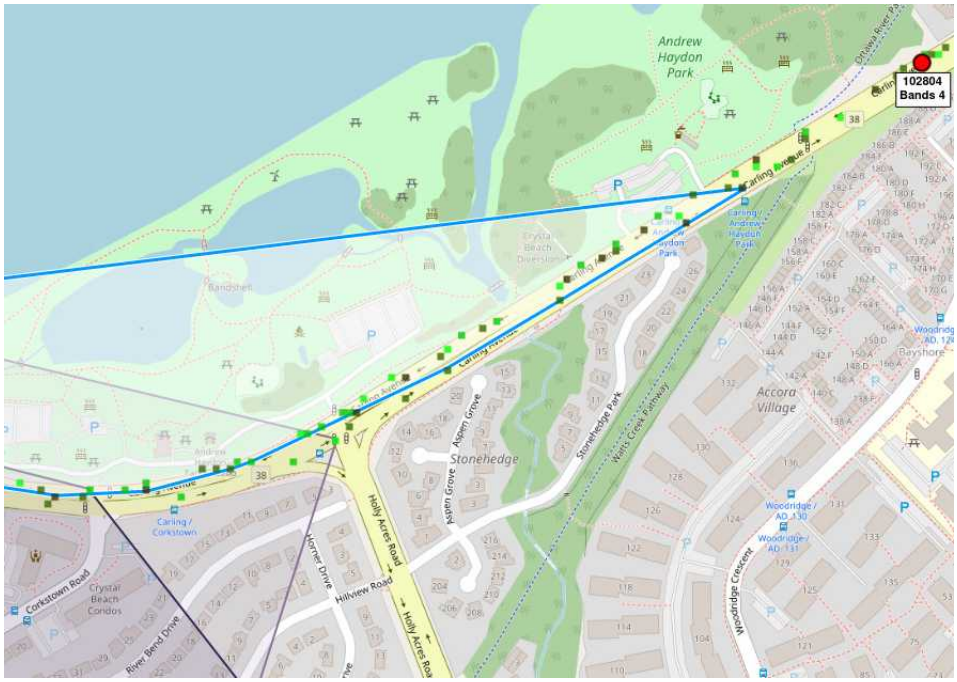


Figure 4.37: C2 CellMapper Data

In Figure 4.39, C2 is compared against the same LOS models, despite using mixed LOS/NLOS data in the path loss calculation. This influenced the cell-wide variance value,

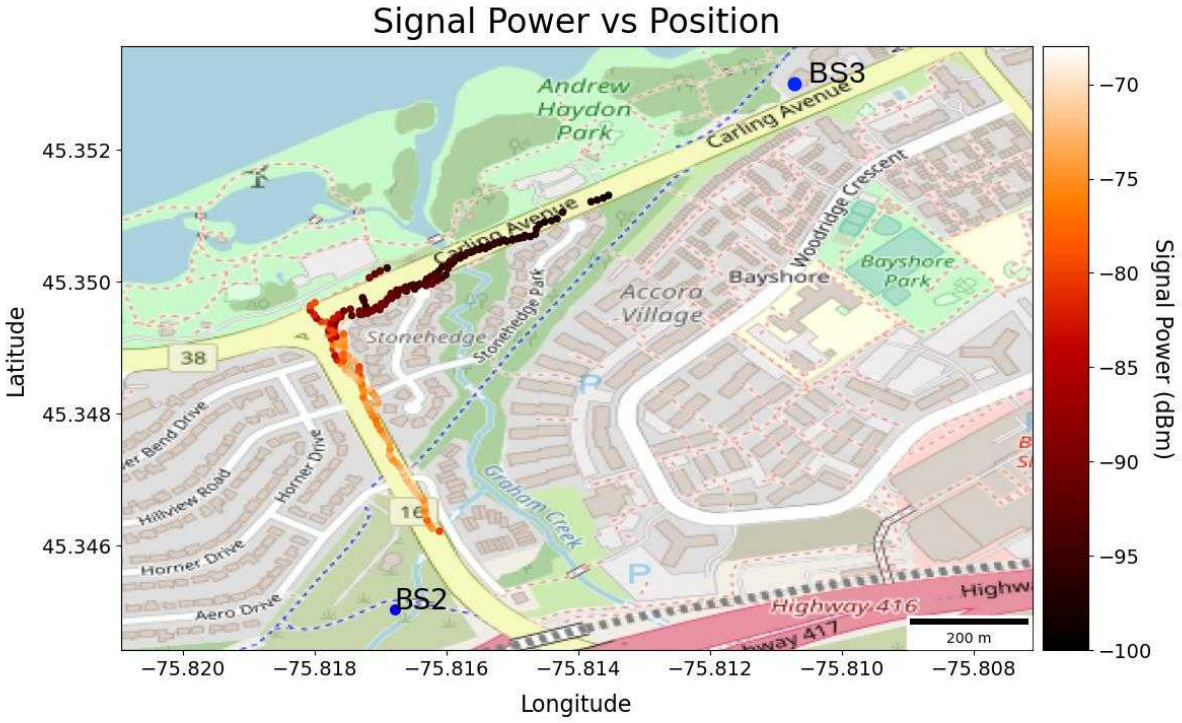


Figure 4.38: P_{TX} for C2 vs BS2, BS3

and therefore both the ABG and CI models overestimate the true variance shown in the observations. As before, the ABG, CI, and Okumura-Hata urban/suburban models provide the most relevant results. Along the LOS portion, the ABG and CI fail to account for a small number of measurements in proximity to BS2, while the Okumura-Hata models do the same while again serving as upper and lower bounds for the majority of data. There is a predictably sharp downturn in path gain beyond 300 m, corresponding to progression around the corner at L2 and out of LOS for the tower. However, the data returns to a relatively flat slope again after the transition, suggesting that the LOS models could be adjusted to approximate the NLOS portion as well. The measured distances are again within the two-ray model's critical distance $d_c \approx 3520$ m, so a poor fit is reasonable.

Although BS3 has LOS to the second portion of the cell data, it appears highly unlikely

that it is C2's source, as the received power follows an inverse trend to the distance and visibility expected for the environment. A large number of measurements were collected in the NLOS region well into the same area covered by C7. Interestingly, no handover occurs to any other cells, despite very low RSRP values, but more detailed analysis would be required to understand why. Based on these results, one might expect similarly-low RSRP measurements when proceeding northwest of L2 once BS2 is no longer visible, provided no other nearby cell provides better service.

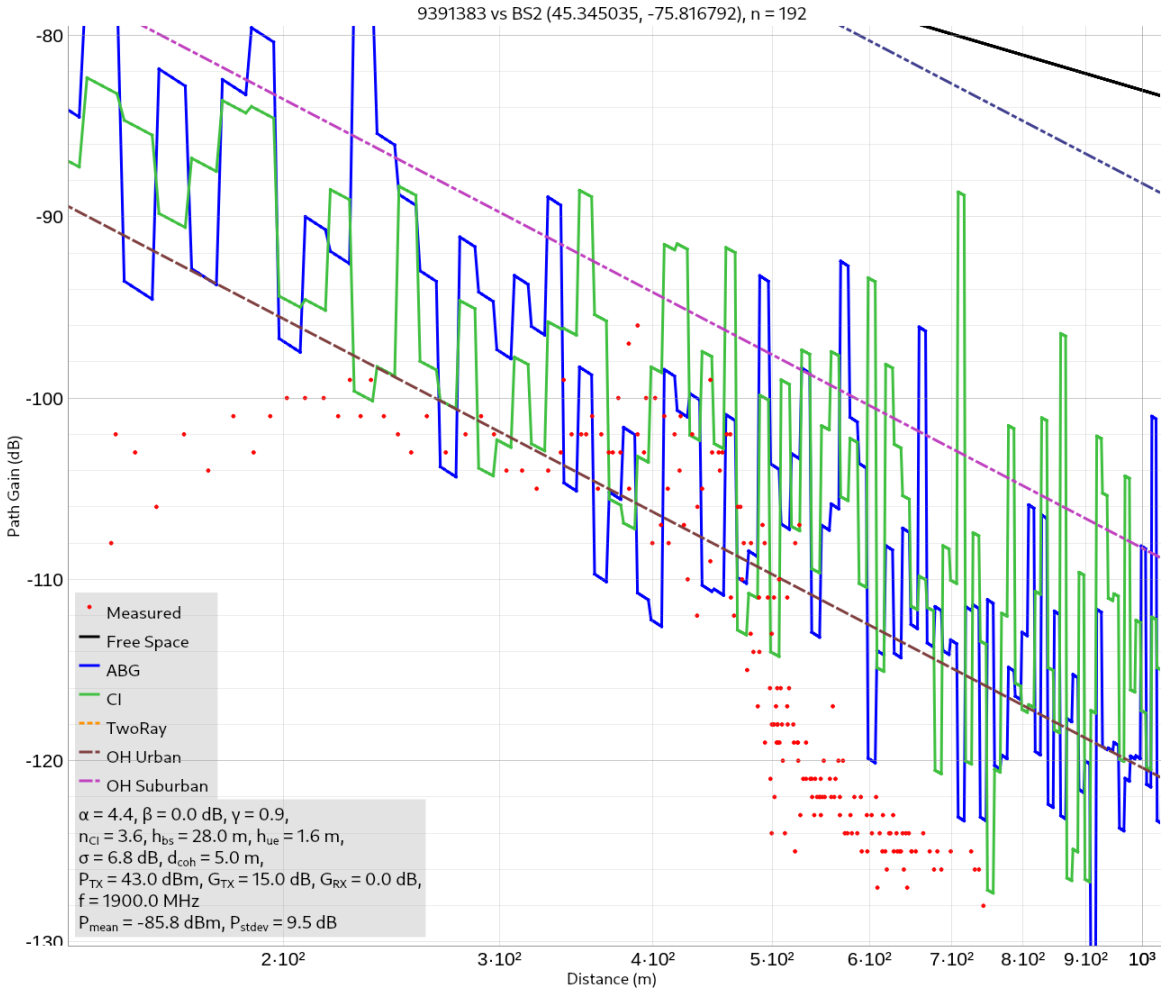


Figure 4.39: Path Gain for C2 vs BS2

4.3.4 C13

As stated above, the Sparks data was not as amenable to the experimental technique described in Chapter 3. Notably, the CellMapper [33] database did not contain any apparent information for C13, which prevented verification of cell band and coverage area in this way. The received power data for C13 is shown in Figure 4.40. BS5 was initially assumed to be the cell's transmission source, since the transceiver location roughly matched the tower info in Figure 4.19. Given BS5's distance from the data, it would be reasonable to expect the results in Figure 4.40 to feature low RSRP that declined consistently while proceeding away from the tower. However, the observations show that the highest received power values occur near the route's end, within at least partial view of all four base stations. Given that measurements for C13 are low east of BS6 and nonexistent earlier than the approximate location of BS8, this would imply a focused cell designed to support a tiny subset of the area, despite possessing adequate LOS conditions to its entirety. Alternatively, when comparing the data against BS8 in Figure 4.40 we see a (possibly superficial) resemblance to the close-range decrease in signal power for C10 in the Carling area, for a transceiver location that should in theory experience significantly-lower propagation loss.

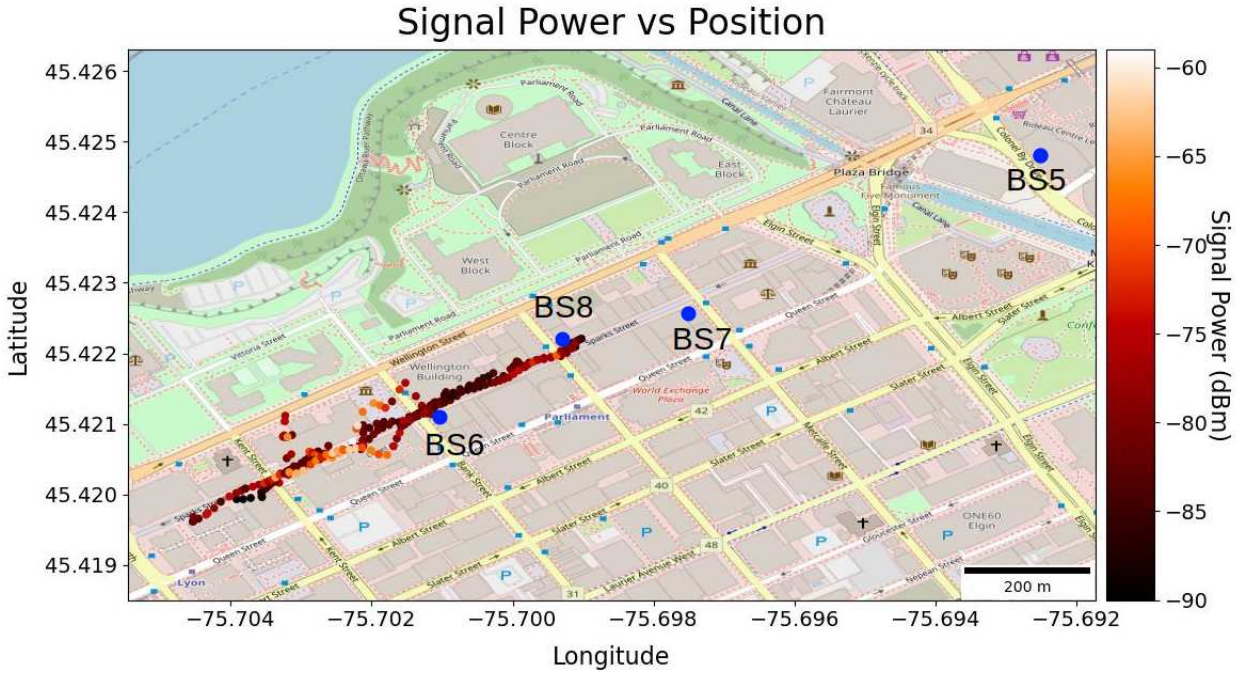


Figure 4.40: C13 Received Power Map vs BS5, BS6, BS7, BS8

Figure 4.41 shows calculated path loss for C13 versus the LOS model suite and referenced to BS5's location. As before, f= 2600 MHz, G_{TX} = 15.0 dB, G_{RX} = 0.0 dB, P_{TX} = 43.0 dBm, and d_{coh} = 5.0 m. Although there is a hint of the flatness seen in C3, the gain varies by 10 dB or more between 750 and 850 m, and had the highest values at the extremes relative to BS5. Some of this inconsistency is visualized in Figure 4.40 as values that were seemingly recorded inside the adjacent buildings - this is likely caused by surrounding structures' height impacting GPS satellite accuracy.

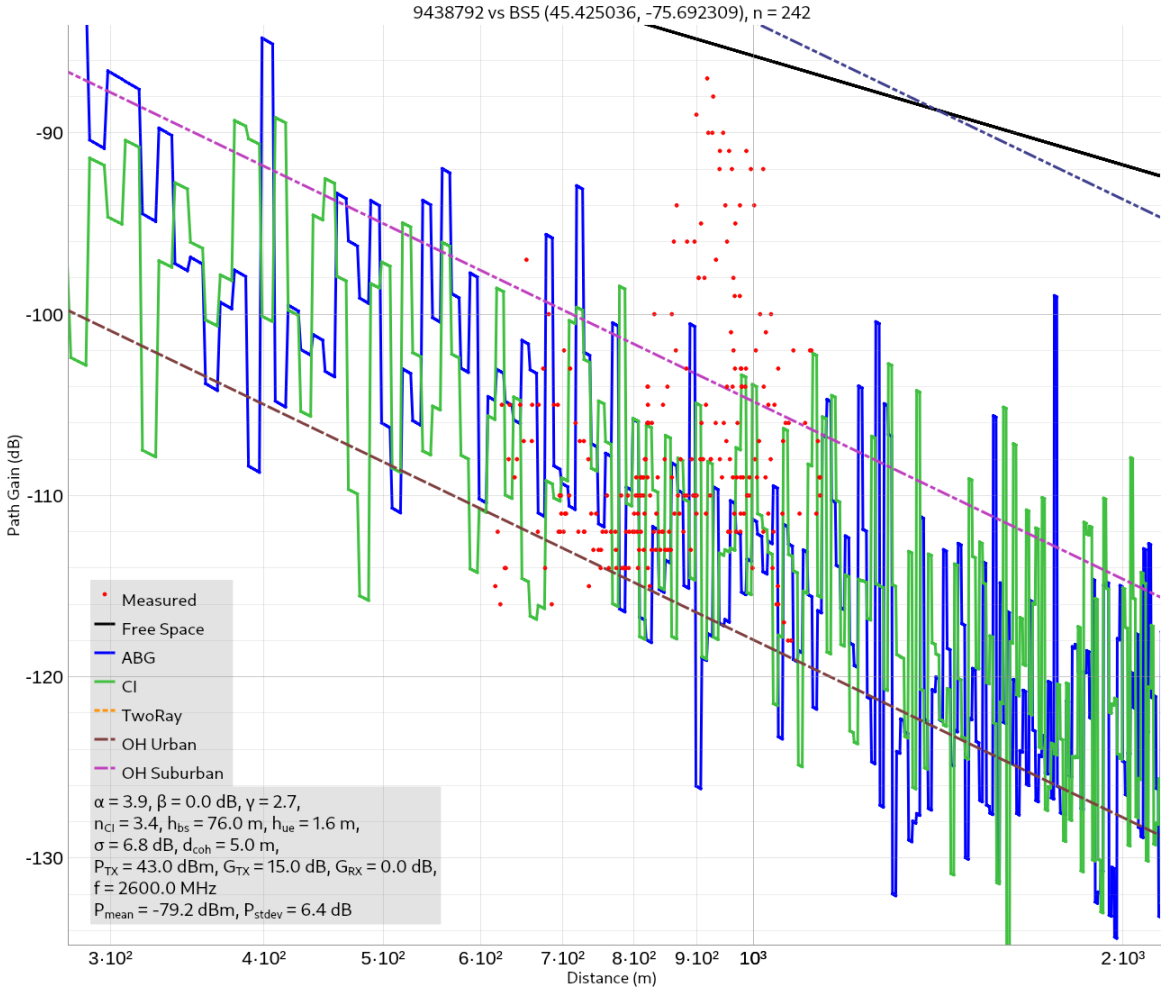


Figure 4.41: Path Gain for C13 vs BS5

As with the Carling results, the σ = 6.4 dB value is influenced by several outlying measurements incorporated in the calculation, but is still comparable to data available in

the literature. If data between $800 - 1100$ m that was most egregious were excluded from Figure 4.41, then a hint of decrease in path loss over distance could be argued. Based on previous observations, if the measurements were all collected in close proximity to the transceiver (i.e. under 200 m) then this would make sense; however, the opposite is true for BS5. The general trajectory appearing downward might suggest that C13's assumed source is incorrect, or some other unknown input is affecting the propagation channel.

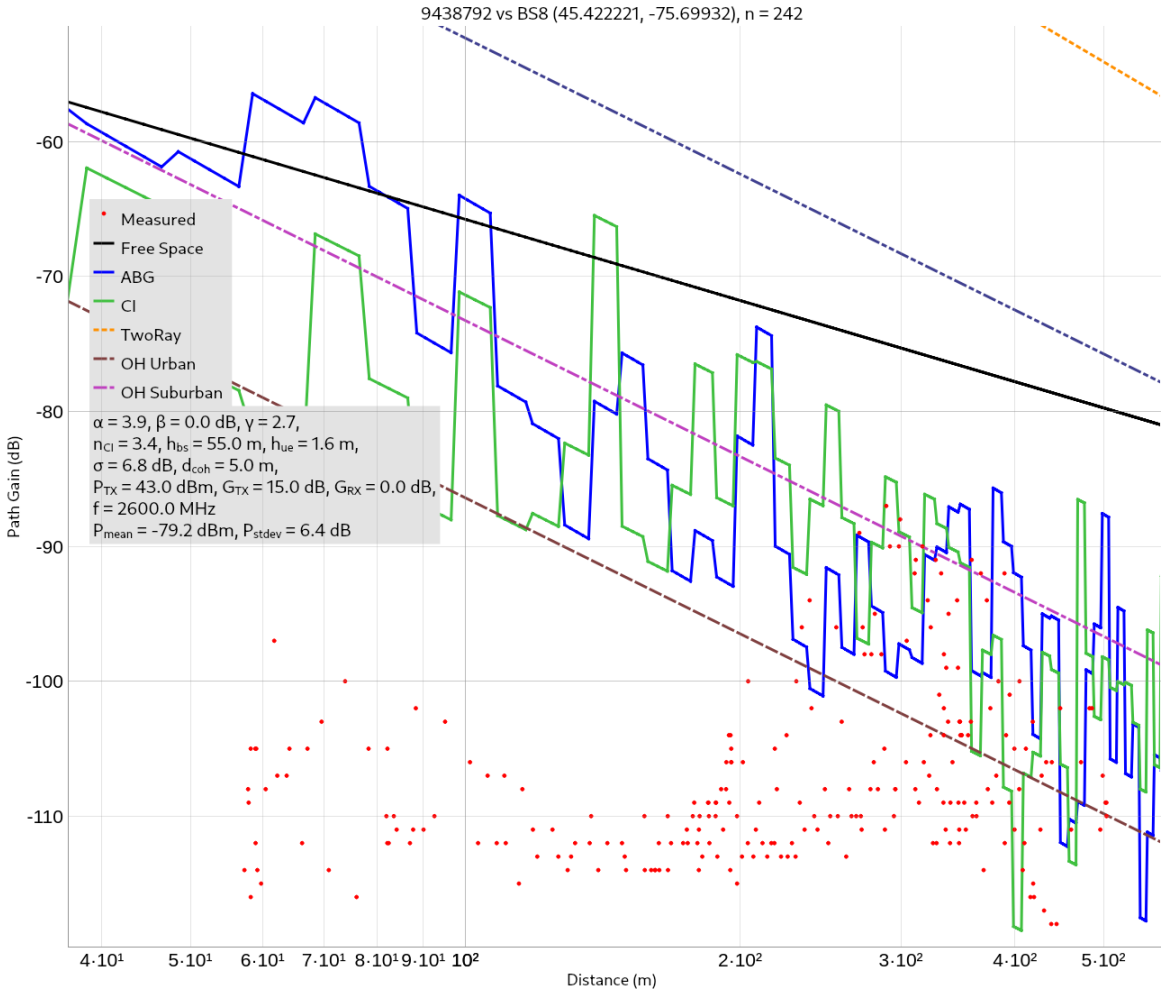


Figure 4.42: Path Gain for C13 vs BS8

Figure 4.42 compares the data against BS8's location (with no adjustments to the models). The data is shifted horizontally, placing all but the more anomalous measurements out of the models' reach. Given $h_{hgt} = 55$ m, it seems reasonable that those measurements

would be at a large viewing angle relative to the array orientation in Figure 4.27, and that multipath propagation would play a greater role than LOS transmission. While the ABG model could be used to approximate the close-range measurements with high β, it would likely have unusual values for the other parameters, and the other models would not be capable of matching the majority of observations. It is not clear from these results if either base station is the correct signal source.

4.4 Summary

The previous sections showed that path loss models could be easily compared against mobile system data observed in a realistic outdoor scenario, then processed and visualized with Routesignal or a similar tool. The most effective models for curve fitting were the ABG and CI, both of which could be adjusted to align with large portions of the measurements for C7, C3, and C2. In particular, the ABG approximated C3's data despite a large number of NLOS signals, although a discrepancy like seen with the CI would be expected for LOS models. Since the ABG is more adjustable, it appears to be a helpful tool whose β parameter may help indicate when environmental assumptions are mismatched to the data. Okumura-Hata urban and suburban forms were the only others to be relevant in most examples. For C7 and C13, they provided apparent lower and upper bounds, respectively to the data. For the other cells, urban nearly provided an upper limit for C2, C3, and C13's (when compared against BS8) observations. C13 had an unusual increase in path gain at greater distances from BS5, suggesting highly-focused coverage or another possible base station. For BS8, the models (with the same parameters) were a total mismatch. The free space and two-ray models did not approximate the observations in any case, suggesting that while they are useful for theoretical purposes they may not be practical for validating real-world mobile systems performance.

Given the analysis' poor fit to both tower locations, the data for C13 could be influenced by other environmental conditions, or the signal may originate from a different base station. It could also be a consequence of GPS inaccuracy at the mobile device in the street canyon environment resulting in incorrect T-R distances. This could be aided by a supplemental device and/or technique providing position correction, particularly when similar experiments occur in other areas with varying levels of NLOS sections. While the other cell environments were more open, such an adjustment could still prove useful in other outdoor locations such as series of obstructions for C3 and BS2. Manual inputs for σ typically appeared to be more accurate than the calculated values, but this is consistent with the variety of environments traversed, including some NLOS areas. Even so, better

estimations (for example, by binning the measurements over appropriate intervals) could be made, potentially leading to different results for the other parameters.

As a whole, the results show many opportunities for expansion and more detailed analysis. Improved (including AI-assisted) curve fitting methods, statistical calculations, and fusion with other metrics such as RSRQ and data rate could aid in detecting patterns, model mismatches, and other insights, including finding alternate parameter sets that align with cell data where it shows a roughly monotonic progression (i.e. all except C13). They would also be testable for trends with many other characteristics, such as observation time/date, device load and system specifications, area population, weather conditions, channel bandwidth, or available cell bands.

Chapter 5

Teaching Laboratory

The methods and experiences of the previous chapters could be easily repurposed for teaching wireless communications concepts in courses such as ELG4179 at the University of Ottawa. Using a mobile device as test equipment was informative to how the propagation environment causes real-world performance to deviate from theory. For education purposes, it has numerous advantages:

- Students have ready access to required equipment (mobile devices) and environments (pedestrian spaces)
- Measurements are easy to obtain in short time intervals and in nearly any location
- Data can be compared against (and added to) public signal coverage databases
- Shows practical examples for wireless communications, with real-world limitations
- Introduces mobile network design and operation concepts
- Equipment used also generates useful complementary information (photos, screenshots)

The following sections outline how such a teaching laboratory could be written.

5.1 Preparation

This section's most immediate and important goal is to ready the target audience to understand the measurements they will make. Some basic conceptual questions should be required, e.g. regarding LTE technology definitions or types of propagation fading. Calculations of key results for hypothetical scenarios such as the free space path loss at 1 m for a range of frequencies, or more specific questions about the UE's device specifications, could also be appropriate. The section must additionally include instructions on any software or extra tooling required for the particular scenario.

5.2 Data Collection

Instructions and/or an algorithm for collecting measurements should be given here. This includes selection of the campaign environment itself, which ideally has at least one clearly-identifiable base station present for which to acquire location data. Clear information on any special characteristics to watch for and gather supplementary data on (e.g. taking photographs depicting relative locations of detected base stations) is also essential. The steps should fully explain how to operate the mobile application to acquire the desired performance metrics.

5.3 Analysis

Guidelines for analyzing and preparing the observations for submission as a gradeable report should go here, including how to combine and/or relate them to the Preparation section's questions. Instructions on which sources to use for verification of quantities such as tower positions should be given (if a specific source is prefered). There should also be some guidance on reasonable assumptions to make about unknown system parameters where needed, such as transmit power or antenna gain. At minimum, the analysis requirements should incorporate plots of the measured data over time, distance, or another appropriate reference, along with a critical review of the results. Other presentations of the data such as coverage maps may provide additional insight for the student and be simple enough to generate.

5.4 Example

A sample laboratory designed according to this outline is provided in Appendix C.

Chapter 6

Conclusion

6.1 Thesis Summary

This thesis set out to provide a blueprint for effective wireless network analysis using only mobile devices, existing infrastructure, and the appropriate processing of observations and environmental characteristics. Its intended audience spanned industry, academic, hobbyist, and emergency management groups and individuals. The free Android application Network Cell Info Lite was selected for data collection based on its ability to export measurements in popular formats on a per-session basis. The local area was then canvased for accessible outdoor spaces with multiple widely-visible cell towers. Each potential transceiver's location was recorded either on-foot (using the mobile device itself) or via the Google Maps service, then verified in the Canadian Cellular Towers Map database, along with key properties such as downlink frequency, service provider, and height relative to the campaign route.

Two contrasting environments were ultimately chosen: one suburban area with mixed residential, commercial, and green space, along with a decidedly urban street canyon. Geolocated RSRP measurements and contextual images of LTE network infrastructure were obtained by traversing them repeatedly at convenient intervals. The custom software tool Routesignal was developed for overlaying estimated tower positions and received signal data (by cell) on OpenStreetMap imagery, as well as providing a convenient means to compare the path loss models of Chapter 2 against the results. Suspected base stations observed during the walk were compared against detected cells' signal power map and each model to determine their validity.

Knowledge of the propagation environment - particularly where local obstructions resulted in NLOS conditions - along with cell band info was essential too, and used to predict the source for each cell. This was supplemented with analogous information in the online CellMapper database to improve matching confidence. A final comparison was performed between calculated path loss and common propagation models' expected loss as a function of distance, again considering NLOS conditions and other environmental factors where the results differed.

The ease in identifying network infrastructure was readily apparent in the Carling area. Base stations generally stood out against the buildings that hosted them or were standalone, making geolocation trivial with the aid of a mobile phone's GPS, or popular online mapping tools. Received power maps of each area portrayed results consistent with shadowing and NLOS channel expectations, and some extreme examples revealed signs of poor-coverage zones worth analyzing further. The online resources used to compare cell data, when combined with user measurements, showed the simplicity involved in performing further experiments and characterizing other spaces with wireless network coverage. This was despite a lack of careful control in many factors such as time of day, user density, movement speed, or brief deviations from the path over subsequent sessions.

Characterizing a cell was shown to be more challenging in the urban environment, with the visualized data showing much more variance in places; a probable outcome of adjacent structures blocking line-of-sight to one or more GPS satellites. This contributed to the difficulty in predicting which (if any) observed base station was the source. Significantly larger datasets may be required to better understand the urban scenario, and additional metrics may need consideration to achieve the same level of apparent utility.

Parameter models utilized were typically at odds with those reported in the literature for outdoor, LOS environments. Many factors could play a role, but a common theme was that the data's variance was excessive for most cells due to being calculated for the entire dataset, rather than binned or otherwise divided into more local analyses. This was also partially a consequence of inconsistency in campaign execution, including wandering between LOS and NLOS conditions over intermediate segments of the route. These results could be improved by using localized and/or windowed averages over binned subsets of the data, especially with manual adjustment of their size.

Another recurring observation was of higher-than-expected received power in close-range measurements, where all except the ABG model (due to its use of a non-physical offset) were inadequate. This was consistent with shadowing and angle-of-incidence when located near the cell site's base. Although unlikely to compensate for systematic user errors, a short-range correction factor added to the models may improve accuracy near

the transceiver. Similarly, all model parameters may have benefitted from the ability to represent variable transmit power, as the flatness of some cells' path loss curves suggested that such adjustments (by the network) may be playing a significant role for at least some areas.

The devices' receiver sensitivity may have played a role in the conclusions drawn about the data. Measured values for minimum power among most cells in the Carling area were below the $P_{sens} = 98$ dBm threshold calculated using Equation (1.3). Some variation may be expected depending on the operating bandwidth of a given channel and the environment's temperature, but it is also possible that the devices' reporting method includes other factors. Further investigation into the origin of this discrepancy, such as comparing outputs of different cellphone models against the same cell (for hardware variations) may provide correction factors or insight into other phenomena.

Based on the thesis outcomes, a laboratory template for use in educational environments was created. Basic questions about wireless propagation and modern standards were selected, followed by a condensed version of the experimental design employed for the aforementioned data collection. The experiment's simplicity made it highly valuable a teaching tool, as many important wireless propagation concepts were encountered in real-world situations that could then be compared against detailed online resources for validity. Its reliance on cell phones for data acquisition meant that no costly, immobile, and/or unrepresentative equipment would be required for adoption into school curricula, as despite the platform-dependent availability of the measurement software, a critical mass of students in college and university environments is likely to have access. Additionally, for institutions with such sophisticated test hardware, it provides an external technique to calibrate the laboratory test environment.

It is important again to emphasize the simplicity of this process. Using only personal mobile devices, free Android applications, widely-available standards, crowdsourced reference databases, and a prototype Python-based plotting tool, the method's potential for characterization of future network infrastructure, system performance, and propagation conditions was shown. This focused almost exclusively on the RSRP measured by the user devices. Inclusion of other metrics from RSRQ to speed tests and performing these measurements under different regimes and propagation conditions should only prove the value of this technique further, both as a complement to more traditional laboratory setups and as a reference in its own right.

6.2 Future Work

6.2.1 Optimization and Extension of Results

This research was conducted on a narrow scope of campaign environments and network characteristics, chosen based on convenience and proximity to the author. While this provided a wealth of data to review and interpret, some gaps in the results could potentially be overcome by more careful execution of the research method. Many more propagation channels with unique characteristics could also be identified, measured, and analyzed in a similar manner. This would provide a more complete picture of the technique's limits and potentially indicate how to compensate for them. Given the spread of 5G-capable devices, corresponding wireless infrastructure, and the Network Cell Info Lite tool's support, another obvious extension would be to perform the same experiment in areas with more extensive 5G coverage and with more mobile device platforms that support the capability, as the bands tested here all operated below 5 GHz. There are also numerous other metrics for the propagation channel in the literature which were not mentioned here and could be analyzed, e.g. outage probability and bitrate statistics.

6.2.2 Revisiting Previous Research Concepts

The catalyst for this research was a similar experiment performed under very different circumstances. The original objective was to analyze LTE signal propagation in tunnel environments, which would have used the same Network Cell Info Lite and Routesignal tools to collect signal quality measurements while riding metropolitan subway systems in cities such as Ottawa, Toronto, and Montreal. The COVID-19 pandemic's early-2020 arrival in Canada meant restrictions on access to such spaces, and an associated increase in safety risks. Given these obstacles' unknown duration, an alternative research concept (i.e. the one presented here) had to be developed. The subway tunnel analysis could be revisited using a process similar to the one provided, with appropriate adjustments based on the environment and associated literature.

6.2.3 Replication of Published Experiments

The literature showcased experimental setups that were used to confirm applicability of various path loss models, or investigate other propagation behaviors in specific environments. A core argument of this thesis is that they used methods that are less accessible

and more idealized than the experience of using end-user equipment. A useful study may be to survey these same areas using the process contained in this thesis (where possible), with appropriate tracking of environmental changes (if possible) since the original works' publication dates. Any significant deviations from the previous outcomes could provide suitable foundations for related research, including future graduate students' undertaking similar theses. Other well-known experiments would also be reasonable choices to begin calibrating the procedure's use with various mobile devices.

6.2.4 Academic and Industry Implications

Condensation of wireless network analysis into such a simple method has many implications for future research. The outlined process requires the analyst to be aware of the common challenges of wireless propagation and the consequences for signal quality, but provides a portable and repeatable means of collecting data for studying these phenomena. For teaching purposes, this could mean highly-flexible delivery and execution, e.g. under pandemic-influenced lockdown or other remote learning conditions, along with minimal preparation from the administrative side. Individual student reports could be incorporated into larger studies, including multi-year projects that analyse longer-term changes in wireless network performance, or large-scale signal mapping initiatives for the municipalities and regions that institutions are located within.

Support for uploading collected data in Network Cell Info Lite and the CellMapper mobile application means that students and faculty researchers alike can contribute directly to community-maintained public resources. In some cases, this even implies compensating for gaps in these databases, which this work has shown exist. Furthermore, should an academic institution be determined to procure and control the equipment themselves, rather than relying on the mobile devices in students' possession, then they can do so at a fraction of the price attached to more standardized equipment, while having confidence in the representative nature of the devices and access to a variety of models with distinct specifications.

Telecommunications companies also benefit from employment of the ideas presented here. Pragmatic verification and validation techniques could be developed for purposes such as identifying performance and coverage gaps in existing systems, tracking these metrics under specific environmental conditions (e.g. adverse weather) or system loads (e.g. public events), and testing of new deployments. ISPs may be able to provide event planning services to commercial customers who require consistent coverage at a venue (e.g. a large sporting event or national holiday celebration), which could be based on data

acquired with this technique. An example could be an application akin to a combination of CellMapper and Google Maps to provide real-time updates and predictive services for users.

With sufficient simplification and/or documentation, the wider public could also have access to as-of-yet nonexistent, derived software for testing actual signal quality and performance against that which is advertised by their provider in unusual ways. Telecom companies may wish to be cognizant of and able to provide an adequate response for discrepancies that users may report. Smaller competitors to the dominant network providers may stand to benefit for the same reason, where strategic analysis of such datasets could reveal new opportunities to capitalize upon.

Finally, the insights and discrepancies witnessed via this technique may aid in ongoing research by 3GPP and other bodies to develop new propagation models. The analysis of Chapter 4 suggested that close-range signal behavior deviates from the predictions of widely-accepted models, and simple correction factors may be obtained by more careful investigation of the results collected in this way. Alternatively, such phenomena could also lead to new, specialized use-cases for models that are considered to be of limited value in more controlled contexts. This may be true even if the fitting is not necessarily based on physical principles (such as with the ABG and the flat curve of C3).

6.2.5 Improved Software

The Routesignal application was designed as a simple prototype for analyzing exported OpenCelliD datasets, but it has limited functionality. It may serve as a blueprint for more comprehensive, open-source or proprietary tools, or as inspiration for new features in other existing software suites. If it is maintained as its own utility, there are numerous improvements to the user interface, performance, and underlying project structure that can be made. In either case, many features and metrics described in the Network Cell Info Lite application and the literature alike could be incorporated as well, including:

- Support for additional data formats, e.g. CMWF v.1.1, which is supported by Network Cell Info Lite and contains metrics such as RSSNR, RSRQ, and CQI
- Additional path loss models
- Windowed/localized adjustment of some parameters, e.g. variance and transmit power

- Sorting/analysis by proximity to a location, time of day, data rate, RSRP/RSRQ-versus-time, etc. in addition to cell ID
- Import and export of cell tower profiles
- Automatic acquisition of other artifacts, e.g. OpenStreetMap imagery, based on provided datasets' characteristics
- Tracking of online resources' information for analysis of selected cells
- Verification/validiation against expectations from industry standards, e.g. 3GPP specifications
- Use of machine learning algorithms to estimate model parameters and filter erroneous data

Considering that this experiment focused almost exclusively on RSRP and path loss, the capabilities of Network Cell Info Lite and other tools may also not be fully explored. Similar software could be developed with more specific objectives or based on new data standards which could further improve accessibility. Despite being selected for its relative ease-of-use, one limitation experienced with Network Cell Info Lite was the difficulty in consistently acquiring signal measurements at consistent intervals, considering that other artifacts such as environment and base station imagery were required, and that other performance metrics such as bitrate measurements do not use the same interface for acquisition. Features that enable automatic logging of data or even guided user interfaces for collecting the entire suite of information available to a mobile device (including the low-level network API, system diagnostics, and camera outputs) could make this process even more accessible and streamlined.

The utilization of machine learning algorithms is a particularly important possibility. Extremely low measurement values (i.e. ones below the receiver sensitivity) and other anomalies can be filtered from the measurements, provided a big data approach is taken. The method makes collection of large data sets for this purpose feasible and easily comparable. Combining this concept with similar processes applied to environmental data such as Google Maps or other large, public databases of information related to the real user experience may enable rapid system validation and even more sophisticated performance prediction.

6.2.6 Security and Emergency Management

A final perspective to consider this method for: security and resiliency of mobile network infrastructure. Although written with academic and industry applications in mind, this thesis has shown the speed which malicious actors could not only identify the locations of, but also determine the relative importance of cell towers for covering specific areas and services. This phenomenon was alluded to by information published by CBC in 2017 [45], wherein systems known as Mobile Device Identifiers (MDIs) could be used to track and identify cell phones were described. This approach could provide attackers with significant knowledge of local cell services and their users, and critical systems such as Emergency Alert System in Canada, which is transmitted via LTE infrastructure, could even be damaged or rendered non-operational using this insight.

Similarly, extreme weather and long-term climate change effects have already revealed the population's dependency on vulnerable wireless networks, which will only grow as greater portions of users' needs are obtained online. The experimental method's accessibility is again a benefit to researchers in this field, as it provides a basis for determining which parts of a wireless network are highest-priority for restoration in disaster scenarios, based on signal quality and usage statistics combined with knowledge of existing emergency response strategies.

References

[1] CTV News, "Canadians spent 4.4 hours on mobile apps a day in 2021: report," 2022.

[2] Canadian Radio-television and Telecommunications Commission (CRTC), "Communications Monitoring Report 2018," Jul 2019.

[3] Canadian Internet Registration Authority (CIRA), "Canada's Internet Factbook 2019," 2019.

[4] Ericsson, "Ericsson Mobility Report," Nov 2022.

[5] C. Nguyen, "Verizon Blames Video Consumption for Slow 4G LTE Speeds," Dec 2013.

[6] Canadian Radio-television and Telecommunications Commission (CRTC), "Emergency Alerts and the National Public Alerting System," Jan 2022.

[7] BC Hydro, "Lower Mainlanders less prepared for storm season than other British Columbians," Nov 2021.

[8] CBC News, "Canada's cellphone system vulnerable in disasters, say experts," 2022.

[9] European Telecommunications Standards Institute (ETSI), "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification," *ETSI TS 123 003 V16.3.0 Release 16*, 2020.

[10] 3rd Generation Partnership Project (3GPP), " Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception," *Tech Rep TR 36.104 V17.7.0 Release 17*, 2022.

[11] Fujitsu, "High-Capacity Indoor Wireless Solutions: Picocell or Femtocell?," 2013.

[12] 3rd Generation Partnership Project (3GPP), "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements," *Tech Rep TR 36.214 V15.2.0 Release 15*, 2020.

[13] K. Dimou et al, "Handover within 3GPP LTE: Design Principles and Performance," in *2009 IEEE 70th Vehicular Technology Conference Fall*, pp. 1–5, 2009.

[14] S. Salous, *Radio Propagation Measurement and Channel Modelling*. Wiley, 2013.

[15] S. Sun, T. S. Rappaport, M. Shafi, P. Tang, J. Zhang, and P. J. Smith, "Propagation Models and Performance Evaluation for 5G Millimeter-Wave Bands," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8422–8439, 2018.

[16] D. Tse, *Fundamentals of Wireless Communications*. Cambridge University Press, 2016.

[17] S. Loyka and A. Kouki, "Using two ray multipath model for microwave link budget analysis," *IEEE Antennas and Propagation Magazine*, vol. 43, no. 5, pp. 31–36, 2001.

[18] D. Gesbert, M. Shafi, S. Da-shan, P. J. Smith, and A. Naguib, "From theory to practice: an overview of MIMO space-time coded wireless systems," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 3, pp. 281–302, 2003.

[19] M. Hata, "Empirical formula for propagation loss in land mobile radio services," *IEEE Transactions on Vehicular Technology*, vol. 29, no. 3, pp. 317–325, 1980.

[20] Y. Okumura et al, "Field strength and its variability in UHF and VHF land-mobile radio service," *Rev. Elec. Commun. Lab*, vol. 16, 1968.

[21] S. Sun et al, "Investigation of Prediction Accuracy, Sensitivity, and Parameter Stability of Large-Scale Propagation Path Loss Models for 5G Wireless Communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 2843–2860, 2016.

[22] T. S. Rappaport et al, "Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks—With a Focus on Propagation Models," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, pp. 6213–6230, 2017.

[23] T. S. Rappaport, G. R. MacCartney, M. K. Samimi, and S. Sun, "Wideband Millimeter-Wave Propagation Measurements and Channel Models for Future Wireless Communication System Design," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3029–3056, 2015.

[24] S. Sun et al, "Propagation Path Loss Models for 5G Urban Micro- and Macro-Cellular Scenarios," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–6, 2016.

[25] G. R. MacCartney, T. S. Rappaport, S. Sun, and S. Deng, "Indoor Office Wideband Millimeter-Wave Propagation Measurements and Channel Models at 28 and 73 GHz for Ultra-Dense 5G Wireless Networks," *IEEE Access*, vol. 3, pp. 2388–2424, 2015.

[26] D. Casillas-Perez, D. Merino-Perez, S. Jimenez-Fernandez, J. A. Portilla-Figueras, S. Salcedo-Sanz, "Extended Weighted ABG: A Robust Non-Linear ABG-Based Approach for Optimal Combination of ABG Path-Loss Propagation Models," *IEEE Access*, vol. 10, pp. 75219–75233, 2022.

[27] 3rd Generation Partnership Project (3GPP), "Study on channel model for frequencies from 0.5 to 100 GHz," *Tech Rep TR 38.901 V16.1.0 Release 16*, 2020.

[28] S. Sun, T. A. Thomas, T. S. Rappaport, H. Nguyen, I. Z. Kovacs, and I. Rodriguez, "Path Loss, Shadow Fading, and Line-of-Sight Probability Models for 5G Urban Macro-Cellular Scenarios," in *2015 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, 2015.

[29] K. Haneda et al, "5G 3GPP-Like Channel Models for Outdoor Urban Microcellular and Macrocellular Environments," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–7, 2016.

[30] J. Milanović, G. Šimac, and K. Mazor, "Performance analysis of empirical propagation model for long term evaluation (LTE) network," in *2016 International Conference on Smart Systems and Technologies (SST)*, pp. 69–74, 2016.

[31] H. C. Nguyen et al, "An Empirical Study of Urban Macro Propagation at 10, 18 and 28 GHz," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2016.

[32] H. Al-Shamisi, H. Al-Shamsi, I. Kostanic, and J. Zec, "Verifying Measurements of Reference Signal Received Power (RSRP) on LTE Network using an App on Android Smartphones," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 372–377, 2018.

[33] CellMapper, "Cellular Coverage and Tower Map." https://www.cellmapper.net.

[34] U. Labs, "OpenCelliD - Largest Open Database of Cell Towers and Geolocation." https://www.opencellid.org.

[35] V. Raida, P. Svoboda, M. Lerch, and M. Rupp, "Crowdsensed Performance Benchmarking of Mobile Networks," *IEEE Access*, vol. 7, pp. 154899–154911, 2019.

[36] Z. Frias, L. Mendo, and E. J. Oughton, "How Does Spectrum Affect Mobile Network Deployments? Empirical Analysis Using Crowdsourced Big Data," *IEEE Access*, vol. 8, pp. 190812–190821, 2020.

[37] M2Catalyst, LLC., "Network Cell Info Lite." https://www.m2catalyst.com/network-cell-info-lite.

[38] L. Karaçay et al, "A Network-Based Positioning Method to Locate False Base Stations," *IEEE Access*, vol. 9, pp. 111368–111382, 2021.

[39] S. Nikkel, "Canadian Cellular Towers Map." https://www.ertyu.org/steven_nikkel/cancellsites.html.

[40] ISED Canada, "Spectrum Management System Data." https://sms-sgs.ic.gc.ca/eic/site/sms-sgs-prod.nsf/eng/h_00010.html.

[41] 3rd Generation Partnership Project (3GPP), "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) system scenarios," *Tech Rep TR 36.942 V17.0.0 Release 17*, 2022.

[42] "OpenStreetMap." https://www.openstreetmap.org.

[43] Wilysis, "Payload legend (OpenCelliD API)." https://wiki.opencellid.org/wiki/API#Payload_legend.

[44] European Telecommunications Standards Institute (ETSI, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception," *ETSI TS 136 101 V15.9.0 Release 15*, 2020.

[45] CBC News, "RCMP reveals use of secretive cellphone surveillance technology for the first time," 2017.

APPENDICES

Appendix A

Mobile Devices

A.1 Samsung Galaxy S8

The Samsung Galaxy S8 is a 4G LTE-capable device with the following specifications[1]:

- Mobile Phone Model: SM-G950W
- Released April 2017
- 4G Bands: 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 29, 30, 38, 39, 40, 41, 66
- 3G Bands: HSDPA 850 / 900 / 1700(AWS) / 1900 / 2100
- 2G Bands: GSM 850 / 900 / 1800 / 1900

[1] Obtained from https://www.gsmarena.com/samsun_galaxy_s8-8161.php

A.2 Moto G 5G

The Moto G 5G is a 5G-capable device with the following specifications[2]:

- Mobile Phone Model: Moto G 5G
- Released December 2020
- 5G Bands: 1, 3, 5, 7, 8, 28, 38, 41, 77, 78
- 4G Bands: 1, 2, 3, 4, 5, 7, 8, 18, 19, 20, 26, 28, 38, 39, 40, 41, 42, 43
- 3G Bands: HSDPA 850 / 900 / 1700(AWS) / 1900 / 2100
- 2G Bands: GSM 850 / 900 / 1800 / 1900

[2]Obtained from https://www.gsmarena.com/motorola_moto_g_5g-10577.php

Appendix B

Routesignal

Routesignal is a prototype mapping and analysis tool under continuous development by the author for comparison of OpenCellID data against common path loss models. The program is written in the Python programming language (version 3.9.7+) and uses OpenStreetMap [42] images to generate RSRP coverage overlays. The source code is released freely under the open-source MIT License on GitHub[1], where instructions for installation and usage can also be found. routesignal enables the user to:

- Plot RSRP overlays on mapping imagery using exported OpenCellID databases (Figure B.1)
- Compare data against common path loss models (Figure B.2)
- Review tabulated statistics arranged by data set and cell ID

Examples of the user interface are shown on the following pages.

[1] See https://github.com/threexc/routesignal.

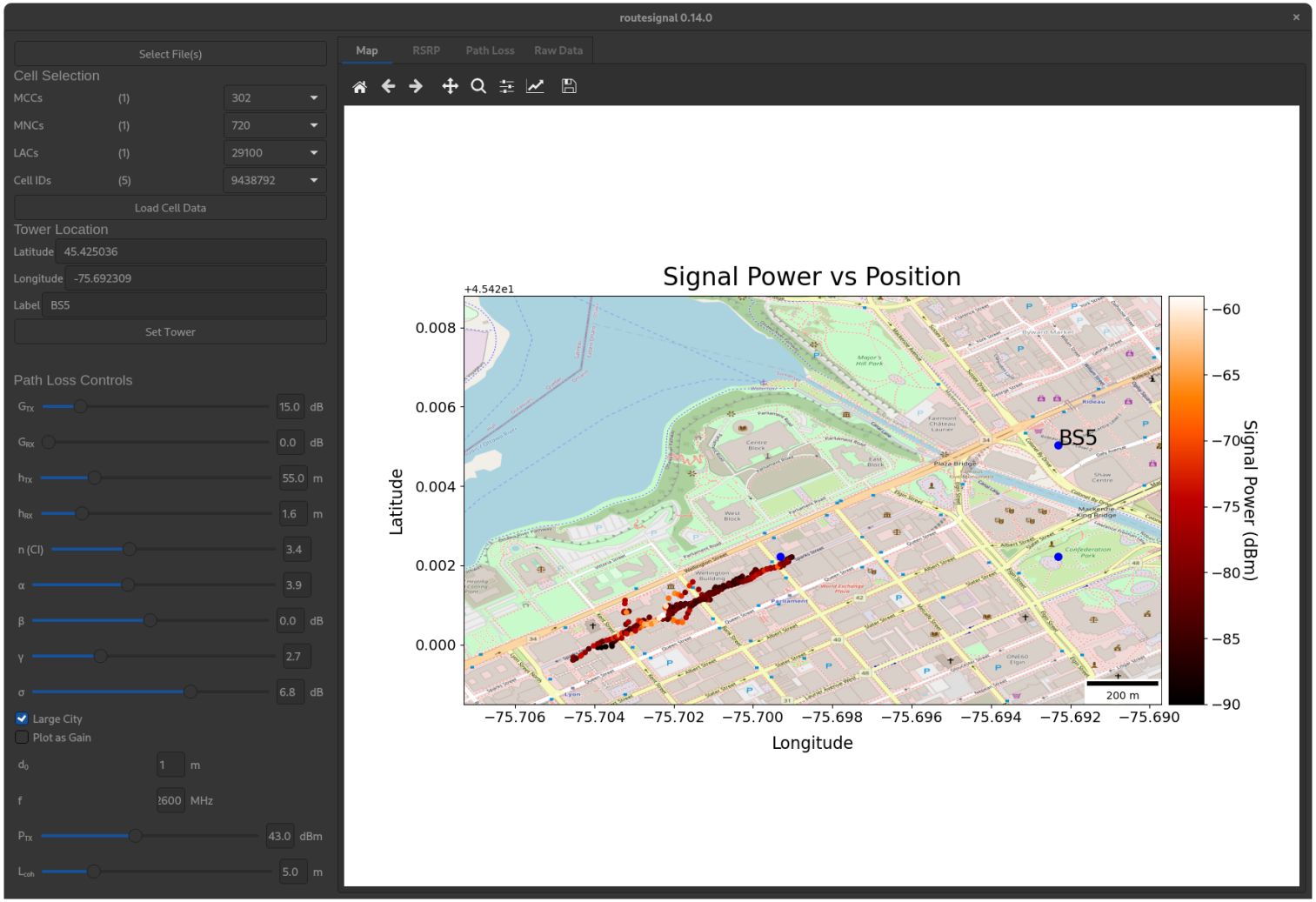


Figure B.1: P_{RX} Map Plot

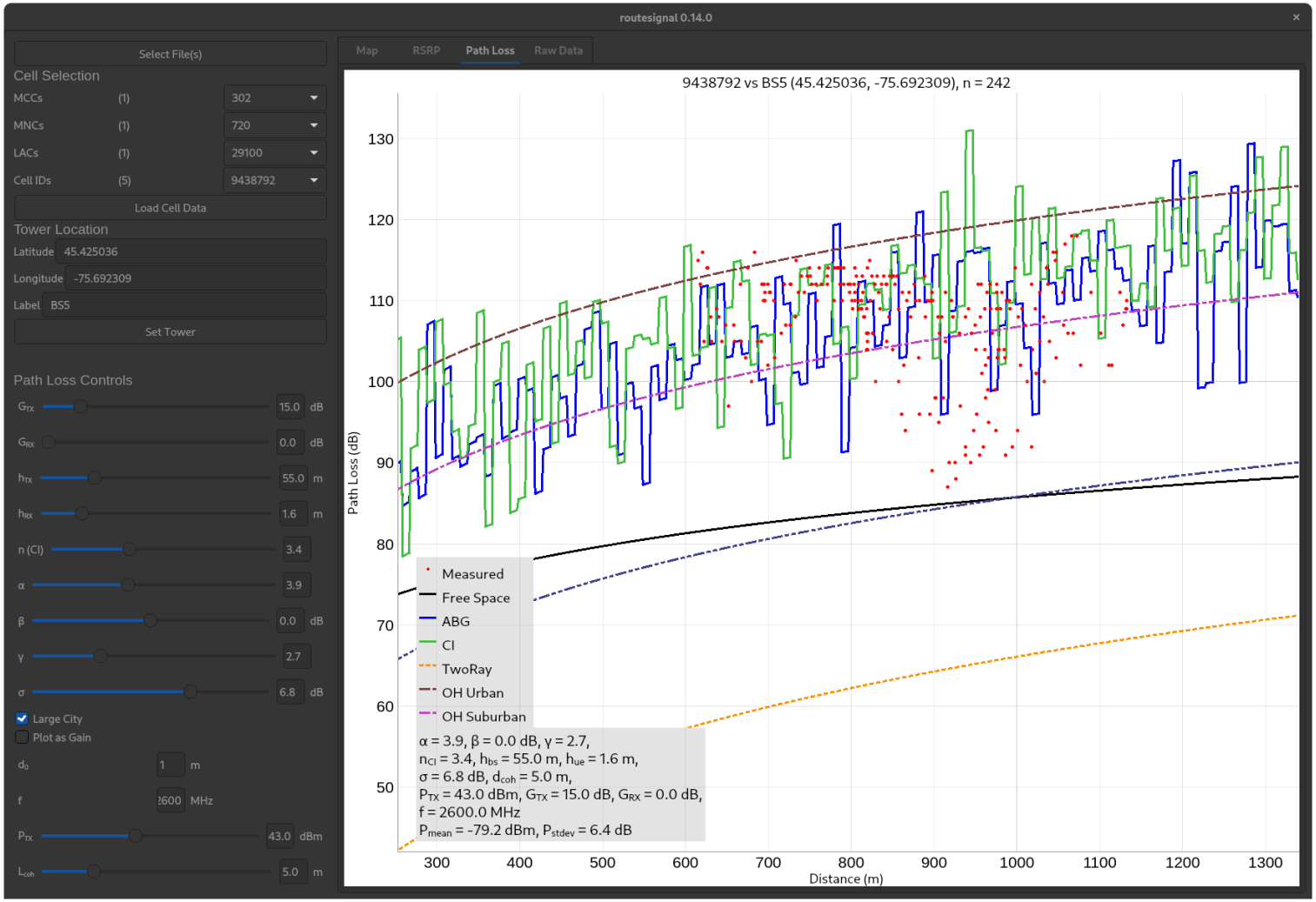


Figure B.2: Path Loss Tab

Appendix C

Undergraduate Laboratory

C.1 Preparation

Note: The mobile app required for this experiment is not available on iOS. You will need to work with someone who has access to an Android phone for this experiment.

1. Provide brief but clear answers for the following questions:
   (a) What is 4G?
   (b) What is 5G?
   (c) What is one major difference between 4G and 5G networks?
   (d) What is the difference between a cell tower and a base station?
   (e) What is multipath propagation?
   (f) What are the two types of fading in wireless systems? How do they differ?
   (g) Which 4G and 5G frequencies/bands does your mobile device support?
   (h) What is the maximum allowed downlink transmit power per channel of an urban cell site according to the FCC, in W and dBm?
2. What is the free space path loss in dB for a 2600 MHz signal, one metre from the source? Assume that both of the transmit and receive gains are zero.
3. What is the typical accuracy of your mobile device's GPS measurements?

4. What is the maximum range for a 4G LTE system? Support your answer with a simple link budget calculation. Assume a transmit power of 43 dBm, a received power of -75 dBm and a transmit antenna gain of 10 dBi. Make reasonable assumptions about cable losses and other factors. What do you think the received antenna gain (i.e. for a cell phone) should be?

5. On your Android device, download and install Network Cell Info Lite. Familiarize yourself with the app and its features before continuing with the lab. Note in particular which cells are detected in nearby areas, along with their operating frequencies/bands, and the range of received powers observed.

C.2 Data Collection

In this Lab, we will measure the characteristics of mobile network signals and study how they vary in space and time.

1. **Ensure that**:
   (a) The battery in your device is fully charged
   (b) Your device has a signal in the area, and it is not connected to a WiFi network
   (c) The chosen area has at least partial line-of-sight with one or more potential base stations you've identified above
2. Choose an accessible outdoor "campaign" area to explore for your experiment, such as a nearby park or your route to/from school. Analyze the chosen environment for possible base stations as you go. These may be tall, easily-visible towers overlooking neighbourhoods and roadways, or smaller antenna arrays mounted on the roofs or sides of buildings. Collect images of them, then etimate their heights, along with their latitudes and longitudes, either by using an online mapping tool (such as Google Maps' satellite view), or by positioning yourself relatively close (within 10-20m of the structure's base) and reading the location as given on the "Map" tab in Network Cell Info Lite. Note the general characteristics of the environment between you and the base station(s), including any large obstructions. If you cannot identify at least two possible transceivers in the area, you must either expand your route or choose a different location.
3. Once you have chosen a campaign area, pick an "origin" and start Network Cell Info Lite. Press the Settings button (the gear icon). Navigate to "Database", then "Export database type" and ensure that it is set to "OpenCellID csv".
4. Open the "Raw" tab, then take a screenshot to capture the serving cell info and the nearest neighbours. Make note of each cell's MCC, MNC, TAC, ECI, and Band.
5. Navigate to the "Map" tab in the app. Begin collecting data by doing the following:
   (a) Navigate to part of your chosen area within line-of-sight of an identified base station, and plan a route through it that breaks LOS with the base station (moves behind a building, hill, etc.) at least once.
   (b) Take a photo of the base station from the origin.

(c) Slowly move along this route while saving measurements by pressing the check-mark button (bottom-left side of the screen) on the map approximately every five seconds for two minutes, generating 20-30 data points. Each successive button press will regenerate .csv file on your device that contains your latest measurement and all of the previous ones for this run. Note: DO NOT press the "X" button on the map tab. This will clear your map markers (you will need them later).

(d) If you reach the end of your route before the two-minute mark, retrace your path until you meet the time requirement.

(e) At the route's end, take a photo of the base station (unless you are at the origin again).

(f) Acquire images of any obstacles that blocked your line-of-sight during the experiment (while facing the base station)

(g) Repeat steps a) through c) five times (if you have identified more than one base station, you can choose a different one). You should have a total of 100-150 data points.

(h) Finally, take a screen capture of the "Map" tab showing your route.

C.3 Analysis

This section will involve using a plotting tool (MATLAB, Python, GNU Octave, etc.) and various online resources to complete.

1. Visit *https://www.ertyu.org/steven_nikkel/cancellsites.html* and locate the area you performed the collection phase in. For each base station you identified, find and record the nearest one shown on the Canadian Cellular Towers Map, then calculate the distance between its location and your estimate.

2. Locate the exported data in your phone's storage (it should be located in "Internal Storage" and then "Network Cell Info Lite", accessible with a File browser app). Export the largest file starting with "OpenCellID" to your computer via email, Google Drive upload, or some other method. Calculate the distances from your suspected base station(s) to the corresponding OpenCellID data. Plot the received power as a function of distance for each base station.

3. Assuming that the transmit power is 30 dBm, the TX gain is 6.0 dBi, and the RX gain is 0.0 dBi, find the propagation path loss for your measurements. Compare it with free space, 2-ray and indoor (such as ITU) models. Make conclusions. You can determine the frequency to use from your data by referencing the cell band list at *https://en.wikipedia.org/wiki/LTE_frequency_bands*.

4. Repeat the previous step with a transmit power of 43 dBm.

5. For each suspected base station, review the corresponding OpenCellID data's "cellid" column. Did it change while collecting each set of measurements? Explain why this might happen.

6. Navigate to *https://www.cellmapper.net* select your cell provider, and search your campaign area's location for red markers containing cell info. Are you able to find the cells you measured? If so, how does your highest measurement value compare to the listed Maximum Signal (RSRP)?

Your report has to provide not only the measurement results, but also a clear comparison with the theoretical models (i.e. free-space, 2-ray and the ITU indoor model).